CHAPTER 2

Essentials of Quantum Mechanics

We begin by building up the basic ingredients of quantum mechanics. This is not meant to be a course on quantum mechanics, and so we will proceed pragmatically and without much fanfare. We will have the luxury of working with finite-dimensional Hilbert spaces (if you do not know what this means, you will soon), since this is the setting of most present applications of quantum learning theory. Our pedagogical approach will be to revisit ordinary probability theory in a suggestive way that naturally generalizes to quantum theory. Our exposition is meant to be accessible to readers with a knowledge of linear algebra and probability theory.

1. Probability theory on vector spaces

1.1. Probability distributions and their transformations

Here we will formulate probability theory on a discrete space, with some additional linear algebraic baggage that will be useful later. If we have a set of size N we can represent a probability distribution over that set as a vector in $\mathbb{R}^N$ given by

$$\vec{p} = \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_N \end{bmatrix}$$

where p_i is the probability of the ith item. We have, out of convenience, chosen an ordering on our set of items so that we can organize the probabilities into a vector, but of course this ordering is arbitrary. As usual, we require $p_i \geq 0$ for all i since probabilities cannot be negative, and also $\sum_{i=1}^N p_i = 1$ so that the probabilities are appropriately normalized. There is a natural way of packaging the normalization condition. To this end, consider the row vector

$$\vec{1}^T = \begin{bmatrix} 1 & 1 & \cdots & 1 \end{bmatrix} .$$

Then $\sum_{i=1}^N p_i = 1$ is equivalent to

$$\vec{1}^T \cdot \vec{p} = 1 ,$$

and we will use this more compact expression henceforth. It will sometimes be useful to consider the *probability simplex* Δ_N which is a subset of $\mathbb{R}^N$, where Δ_N consists of all nonnegative vectors with entries summing to one. Then we can write $\vec{p} \in \Delta_N$.

Next we consider a rudimentary version of *dynamics*. That is, what kinds of transformations on $\vec{p}$ will map it into another valid probability distribution? The

simplest kind of transformation we can imagine is a linear one, so let us examine that first. Letting M be an $N \times N$ matrix, we consider the transformation

$$\vec{p}' = M \cdot \vec{p},$$

so that $\vec{p}'$ is the new probability distribution after the transformation. But what conditions do we need to put on M such that $\vec{p}'$ is a bona fide probability distribution for all initial distributions $\vec{p}$? Well, we need for all entries of $\vec{p}'$ to be nonnegative, and for $\vec{1}^T \cdot \vec{p}' = 1$. To ensure the first property, suppose that $\vec{p}$ is all zeroes except for the jth entry which equals one. (That is, we would sample the jth object with probability 1 and never sample anything else.) To introduce some other notation, let $\vec{e}_j$ be vector which is all zeroes except for the jth entry which equals one. Then we have

$$\vec{p}' = M \cdot \vec{e}_j = \begin{bmatrix} M_{1j} \\ M_{2j} \\ \vdots \\ M_{Nj} \end{bmatrix} .$$

In order for all entries of $\vec{p}^{'}$ to be nonnegative, we evidently require $M_{ij} \geq 0$ for all j, and i fixed. Varying over i as well, we find the requirement that $M_{ij} \geq 0$ for all i, j, and so M must be a matrix with nonnegative entries. Since we also demand that $\vec{1}^T \cdot \vec{p}' = 1$, we find the condition

$$\vec{1}^T \cdot \vec{p}' = \vec{1}^T \cdot M \cdot \vec{e}_j = \vec{1}^T \cdot \begin{bmatrix} M_{1j} \\ M_{2j} \\ \vdots \\ M_{Nj} \end{bmatrix} = 1 .$$

That is, the jth column of M must sum up to one. Since this must hold for every column, we find the condition

$$\vec{1}^T \cdot M = \vec{1}^T . \tag{2}$$

Thus a nonnegative matrix satisfying (2) will send probability vectors to probability vectors. We honor this finding with a definition:

Definition 5 (Markov matrix)**.** *Let M be an $N \times N$ matrix. We say that M is a* ***Markov matrix*** *if $M_{ij} \geq 0$ for all i, j, and $\vec{1}^T \cdot M = \vec{1}^T$. Then M maps probability vectors to probability vectors.*

A few comments are in order. In many treatments of Markov matrices, there is a different convention in which M is taken to act on probability distributions 'to the left', which would give the transpose our definition above. Our conventions here are chosen to align with those of quantum mechanics, as we will see later on.

We immediately notice that Markov matrices behave nicely under composition. Specifically, we have the useful lemma:

Lemma 6 (Composition of Markov matrices)**.** *If $M_1, M_2, ..., M_k$ are Markov matrices, then $M_k \cdots M_2 \cdot M_1$ is also a Markov matrix.*

The proof of this useful fact follows by a short calculation using the definition (which you should do if you have not thought it through before). The upshot of

this lemma is that we can consider transformations like

$$\vec{p}\,' = M_k \cdots M_2 \cdot M_1 \cdot \vec{p}$$

as instantiating a type of 'circuit', with depth k. That is, we could say the words: starting with $\vec{p}$ we apply M_1 followed by M_2 followed by M_3 and so on, and then finally apply M_k.

Before moving on to increasing levels of sophistication, we consider a simple example:

Example 1 (Bernoulli coin, $N = 2$). We now specialize to a two–outcome space and fix the ordering so that the first coordinate is outcome 0 ("success") and the second is outcome 1 ("failure"). A Bernoulli distribution with success probability θ is therefore represented by

$$\vec{p}_\theta = \begin{bmatrix} \Pr[0] \\ \Pr[1] \end{bmatrix} = \begin{bmatrix} \theta \\ 1-\theta \end{bmatrix}, \qquad \theta \in [0,1].$$

Consider the *bit–flip* dynamics with flip probability $\varepsilon \in [0,1]$,

$$M_\varepsilon = \begin{bmatrix} 1-\varepsilon & \varepsilon \\ \varepsilon & 1-\varepsilon \end{bmatrix},$$

whose entries are nonnegative and whose columns each sum to 1, so M_ε is a Markov matrix in our sense. Acting on $\vec{p}$ produces

$$\vec{p}_{\theta'} = M_\varepsilon\, \vec{p}_\theta = \begin{bmatrix} (1-\varepsilon)\theta + \varepsilon(1-\theta) \\ \varepsilon\theta + (1-\varepsilon)(1-\theta) \end{bmatrix} \quad \Longrightarrow \quad \theta' = (1-2\varepsilon)\,\theta + \varepsilon,$$

where $\theta' = \Pr'[0]$ is the new success probability.

Some immediate checks help build intuition. When $\varepsilon = 0$ the map is the identity; when $\varepsilon = 1$ it deterministically flips $0 \leftrightarrow 1$; and when $\varepsilon = \frac{1}{2}$ it sends every input to the uniform distribution $\vec{p}_{1/2} = \begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix}$ in one step. For any $0 < \varepsilon < 1$, the unique fixed point solves $\theta' = \theta$ and is $\theta_* = \frac{1}{2}$. (To see this, simply solve $\theta_* = (1-2\varepsilon)\theta_* + \varepsilon$ for θ_*). Iterating M_ε a total of k times yields exponential mixing toward the fixed point θ_* at rate $|1-2\varepsilon|$:

$$\theta^{(k)} = \big(1-2\varepsilon\big)^k \Big(\theta^{(0)} - \frac{1}{2}\Big) + \frac{1}{2}\,.$$

Finally, the family M_ε of Markov matrices is closed under composition (illustrating the lemma above): a short calculation shows

$$M_\eta\, M_\varepsilon = M_{\varepsilon+\eta-2\varepsilon\eta}\,,$$

and in particular $M_\varepsilon^k = M_{\varepsilon_{\text{eff}}}$ with

$$\varepsilon_{\text{eff}} = \frac{1-(1-2\varepsilon)^k}{2}.$$

This two–state example already displays dynamics, fixed points, and circuit composition within the linear–algebraic language we have been developing.

Moving on, it is useful to recount a few features of probability distributions. If

we have k probability distributions $\vec{p}_1, ..., \vec{p}_k$, then we can form a new probability distribution by forming a convex combination

$$\vec{p}' = \sum_{j=1}^{k} r_j \, \vec{p}_j \tag{3}$$

where $r_j \geq 0$ and $\sum_{j=1}^{k} r_j = 1$. To see this, notice that $\vec{p}'$ has nonnegative entries and that $\vec{1}^T \cdot \vec{p}' = \sum_{j=1}^{k} r_j \, (\vec{1}^T \cdot \vec{p}_j) = \sum_{j=1}^{k} r_j = 1$. We can interpret $r_1, ..., r_k$ as a probability distribution over k items in its own right, and say of (3) that we have a probabilistic mixture of k probability distributions wherein we sample from $\vec{p}_j$ with probability r_j. That is, $r_1, ..., r_k$ is a probability distribution over probability distributions. (You can use this 'meta' statement to impress your friends, if you like.) To make this concrete, consider the following example:

Example 2 (Sampling two coins, $N = 2$). Suppose we have two Bernoulli coins, represented by the probability vectors $\vec{p}_{1/2}$ and $\vec{p}_{1/3}$, respectively. The first one gives heads with probability $1/2$ and tails with probability $1/2$, and the second gives heads with probability $1/3$ and tails with probability $2/3$. Now suppose I have both coins in my pocket in such a way that when I reach in, I grab the first coin with probability $1/4$ and the second coin with probability $3/4$. Then if I reach in and grab a coin and toss it, what is the probability that I would output heads? This is described by the convex combination

$$\frac{1}{4} \, \vec{p}_{1/2} + \frac{3}{4} \, \vec{p}_{1/3} = \begin{bmatrix} 3/8 \\ 5/8 \end{bmatrix},$$

and so evidently the probability of heads is $3/8$.

So far we have only considered *linear* transformations on $\vec{p}$ that map it into another probability distribution. What if we consider nonlinear transformations? One example would be the nonlinear transformation

$$T(\vec{p}) = \begin{bmatrix} \frac{p_1^2}{\sum_{i=1}^{N} p_i^2} \\ \frac{p_2^2}{\sum_{i=1}^{N} p_i^2} \\ \vdots \\ \frac{p_N^2}{\sum_{i=1}^{N} p_i^2} \end{bmatrix}.$$

Another example would be a Bayesian update. There are clearly a vast infinitude of other possibilities as well. Among this infinitude of transformations there is a natural class that interfaces well with convex combinations of probability distributions. In particular, suppose we mandate that T satisfies

$$T\left(\sum_{j=1}^{k} r_j \, \vec{p}_j \right) = \sum_{j=1}^{k} r_j \, T(\vec{p}_j) \tag{4}$$

for any $\vec{p}_1, ..., \vec{p}_k$ and any valid $r_1, ..., r_k$. In words, we are requiring that a transformation of a probabilistic mixture is a probabilistic mixture of transformations (and specifically, the same transformation). Such T's satisfy a nice structure theorem:

Theorem 7 (Mixture-preserving transformations are Markov matrices)**.** *Suppose that $T : \Delta_N \to \Delta_N$ is a mixture-preserving transformation, namely that (4) is satisfied. Then there exists a Markov matrix M such that $T(\vec{p}) = M \cdot \vec{p}$ for all $\vec{p}$.*

PROOF. Write $\vec{p} = \sum_{j=1}^{N} p_j \, \vec{e}_j$. Using the mixture-preserving property of T, we have

$$T(\vec{p}) = T\left(\sum_{j=1}^{N} p_j \, \vec{e}_j\right) = \sum_{j=1}^{N} p_j \, T(\vec{e}_j) \, .$$

Let M be the matrix whose jth column is $T(\vec{e}_j)$. Then $T(\vec{p}) = M \cdot \vec{p}$. Each column $T(\vec{e}_j)$ is a probability vector, so $M_{ij} \geq 0$ and $\vec{1}^T \cdot M = \vec{1}^T$. Thus M is a Markov matrix, as claimed. □

Mixture-preserving transformations are natural from a physical point of view. Imagine a preparation device that, with probabilities $r_1, ..., r_k$, produces one of the distributions $\vec{p}_1, ..., \vec{p}_k$ by consulting some randomly tossed coins you do not get to see. If dynamics could distinguish whether this randomization happened "before" or "after" the transformation, then the timing of the unseen coin flips would be observable from the output statistics alone. Requiring that they not be observable is exactly the statement of (4).

Two simple consequences are worth keeping in mind. First, the admissible dynamics are closed under randomized control: if with probability r_j you implement a Markov matrix M_j, then the overall map is

$$M' = \sum_{j=1}^{k} r_j \, M_j \, ,$$

which is again a Markov matrix since $\vec{1}^T \cdot M' = \sum_{j=1}^{k} r_j \, (\vec{1}^T \cdot M_j) = \vec{1}^T$ and all entries are nonnegative. Second, if one further insists that deterministic states are carried to deterministic states, so that $\vec{e}_j$ never acquires additional randomness, then each column $T(\vec{e}_j)$ must itself be a basis vector. Equivalently, M has exactly one 1 (and zeros elsewhere) in each column. Such matrices are sometimes called *deterministic* or *functional* Markov matrices. If in addition the mapping $j \mapsto i(j)$ is injective (no two distinct columns point to the same basis vector), then M is a permutation matrix.

By contrast, nonlinear updates arise when you condition on a revealed outcome and then renormalize; the rule in that case depends on which outcome was announced, so it is not a single fixed map on Δ_N and does not represent closed-system dynamics. This classical discussion sets the stage for the quantum case, which we will treat soon. (There, the state space becomes the convex set of density operators, mixture-preserving maps become convex-linear "channels," and the role of Markov matrices is played by completely positive, trace-preserving maps.)

1.2. Joint distributions and tensor products

In probability theory it is essential to consider joint distributions. Here we develop the basic operations of joint distributions in a convenient and illuminating linear algebraic notation. First we require some additional tools on the linear algebra side. Specifically, we will upgrade our linear algebraic toolkit to *multi-linear*

algebra. The key operation will be the **tensor product**, which is an operation for joining two or more vector spaces.

We will proceed by motivating the tensor product informally through simple examples, and then give the abstract definition. It is worth paying close attention as the tensor product will serve as an essential piece of mathematical architecture for almost everything in quantum learning theory.

Consider two vectors $\vec{v}, \vec{w}$ in $\mathbb{R}^N$. We denote their tensor product by $\vec{v} \otimes \vec{w}$. To develop what this means, consider the example below.

Example 3. Let $\vec{v} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$ and $\vec{w} = \begin{bmatrix} 3 \\ 4 \end{bmatrix}$. Then their tensor product $\vec{v} \otimes \vec{w}$ is represented by

$$\vec{v} \otimes \vec{w} = \begin{bmatrix} 1 \\ 2 \end{bmatrix} \otimes \begin{bmatrix} 3 \\ 4 \end{bmatrix} = \begin{bmatrix} 1 \cdot \begin{bmatrix} 3 \\ 4 \end{bmatrix} \\ \\ 2 \cdot \begin{bmatrix} 3 \\ 4 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 3 \\ 4 \\ 6 \\ 8 \end{bmatrix} .$$

In words, $\vec{w}$ gets 'sucked in' to $\vec{v}$. Now let us take the tensor product in the other order, namely $\vec{w} \otimes \vec{v}$:

$$\vec{w} \otimes \vec{v} = \begin{bmatrix} 3 \\ 4 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 3 \cdot \begin{bmatrix} 1 \\ 2 \end{bmatrix} \\ \\ 4 \cdot \begin{bmatrix} 1 \\ 2 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 3 \\ 6 \\ 4 \\ 8 \end{bmatrix} .$$

From this we glean that, in general, $\vec{v} \otimes \vec{w} \neq \vec{w} \otimes \vec{v}$. Moreover, since $\vec{v} \in \mathbb{R}^2$ and $\vec{w} \in \mathbb{R}^2$, we notice that $\vec{v} \otimes \vec{w} \in \mathbb{R}^4$. To this end we write $\vec{v} \otimes \vec{w} \in \mathbb{R}^2 \otimes \mathbb{R}^2 \simeq \mathbb{R}^4$.

Example 4. Suppose $\vec{v} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$ and $\vec{w} = \begin{bmatrix} 3 \\ 4 \\ 5 \end{bmatrix}$ so that $\vec{v} \in \mathbb{R}^2$ and $\vec{w} \in \mathbb{R}^3$. Then

$$\vec{v} \otimes \vec{w} = \begin{bmatrix} 3 \\ 4 \\ 5 \\ 6 \\ 8 \\ 10 \end{bmatrix} \in \mathbb{R}^6 ,$$

and we write $\vec{v} \otimes \vec{w} \in \mathbb{R}^2 \otimes \mathbb{R}^3 \simeq \mathbb{R}^6$.

From the previous two examples we see the general rule that if $\vec{v} \in \mathbb{R}^N$ and $\vec{w} \in \mathbb{R}^M$, then $\vec{v} \otimes \vec{w} \in \mathbb{R}^N \otimes \mathbb{R}^M \simeq \mathbb{R}^{NM}$. So upon taking the tensor product of two vector spaces, the dimensions multiply. We can generalize this further by contemplating another example:

Example 5. Let $\vec{v} = \begin{bmatrix}1\\2\end{bmatrix}$, $\vec{w} = \begin{bmatrix}3\\4\end{bmatrix}$, and $\vec{u} = \begin{bmatrix}5\\6\end{bmatrix}$. Then we have

$$\vec{v}\otimes\vec{w}\otimes\vec{u} = (\vec{v}\otimes\vec{w})\otimes\vec{u} = \begin{bmatrix}3\\4\\6\\8\end{bmatrix}\otimes\begin{bmatrix}5\\6\end{bmatrix} = \begin{bmatrix}15\\18\\20\\24\\30\\36\\40\\48\end{bmatrix}$$

and $\vec{v}\otimes\vec{w}\otimes\vec{u} \in \mathbb{R}^2\otimes\mathbb{R}^2\otimes\mathbb{R}^2 \simeq \mathbb{R}^8$.

The above example indicates that

$$\mathbb{R}^{N_1}\otimes\mathbb{R}^{N_2}\otimes\cdots\otimes\mathbb{R}^{N_k} \simeq \mathbb{R}^{N_1N_2\cdots N_k}\,,$$

namely that if we take the tensor product of k vector spaces then the result is a vector space which is the product of the dimensions of the constituents.

We are now ready to define tensor products abstractly, and to really appreciate what it means. Consider the following definition:

Definition 8 (Tensor product)**.** *Let V and W be real vector spaces. A **tensor product** of V and W is a vector space $V\otimes W$ together with a map*

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

that is bilinear in each argument, i.e. for all scalars $a,b,c\in\mathbb{R}$ and vectors $\vec{v},\vec{w},\vec{u}$,

$$(a\,\vec{v}+b\,\vec{w})\otimes\vec{u} = a\,(\vec{v}\otimes\vec{u}) + b\,(\vec{w}\otimes\vec{u}),$$
$$\vec{v}\otimes(b\,\vec{w}+c\,\vec{u}) = b\,(\vec{v}\otimes\vec{w}) + c\,(\vec{v}\otimes\vec{u}),$$

and in particular $(a\vec{v})\otimes\vec{w} = \vec{v}\otimes(a\vec{w}) = a(\vec{v}\otimes\vec{w})$. Concretely, one may construct $V\otimes W$ as the vector space spanned by formal symbols $v\otimes w$ modulo the above bilinearity relations.

To connect this with coordinates, fix bases $\{\vec{e}_i\}_{i=1}^N$ of $\mathbb{R}^N$ and $\{\vec{f}_j\}_{j=1}^M$ of $\mathbb{R}^M$. Then the NM simple tensors $\{\vec{e}_i\otimes\vec{f}_j\}_{i,j}$ form a basis of $\mathbb{R}^N\otimes\mathbb{R}^M$, and so $\dim(\mathbb{R}^N\otimes\mathbb{R}^M) = NM$. If $\vec{v} = \sum_i v_i\,\vec{e}_i$ and $\vec{w} = \sum_j w_j\,\vec{f}_j$, then

$$\vec{v}\otimes\vec{w} = \sum_{i,j} v_iw_j\,(\vec{e}_i\otimes\vec{f}_j)\,,$$

which recovers the stacking rules seen in the earlier examples and realizes the identification $\mathbb{R}^N\otimes\mathbb{R}^M \simeq \mathbb{R}^{NM}$.

Identifying $\mathbb{R}$ with the one–dimensional space spanned by 1, there are canonical isomorphisms $V\otimes\mathbb{R}\simeq V\simeq\mathbb{R}\otimes V$ given by $\vec{v}\otimes a\mapsto a\,\vec{v}$ and $a\otimes\vec{v}\mapsto a\,\vec{v}$. Hence $\mathbb{R}^N\otimes\mathbb{R}^1\simeq\mathbb{R}^N\simeq\mathbb{R}^1\otimes\mathbb{R}^N$.

Linear maps interact nicely with tensor products. If $A:\mathbb{R}^N\to\mathbb{R}^{N'}$ and $B:\mathbb{R}^M\to\mathbb{R}^{M'}$ are linear, there is a linear map $A\otimes B:\mathbb{R}^N\otimes\mathbb{R}^M\to\mathbb{R}^{N'}\otimes\mathbb{R}^{M'}$ defined by

$$(A\otimes B)(\vec{v}\otimes\vec{w}) = (A\vec{v})\otimes(B\vec{w})$$

which in matrix form is the familiar Kronecker product.

Remark 9 (Associativity of tensor products)**.** *For our purposes, it does not matter whether we first form $(V \otimes W)$ and then tensor with U from the right, or first form $(W \otimes U)$ and then tensor with V from the left. There is a canonical identification between*

$$(V \otimes W) \otimes U \quad \text{and} \quad V \otimes (W \otimes U),$$

and so we will simply write

$$V \otimes W \otimes U$$

without worrying about parentheses. This scales to many tensor factors. For a vector space V we write

$$V^{\otimes k} := \underbrace{V \otimes \cdots \otimes V}_{k \text{ copies}},$$

which has dimension $(\dim V)^k$ and a basis $\{\vec{e}_{i_1} \otimes \cdots \otimes \vec{e}_{i_k}\}$. We will use this to model multi–part systems: for example, a register of k N-ary variables naturally lives in $(\mathbb{R}^N)^{\otimes k} \simeq \mathbb{R}^{N^k}$.

As a word of caution, order still matters*. As we explained before, in general we have $\vec{v} \otimes \vec{w} \neq \vec{w} \otimes \vec{v}$. When we want to swap the order of a tensor product we will use the linear map $\mathsf{SWAP} : V \otimes W \to W \otimes V$, acting by*

$$\mathsf{SWAP} \cdot (\vec{v} \otimes \vec{w}) = \vec{w} \otimes \vec{v}\,.$$

In summary, associativity lets us ignore parentheses; SWAP lets us reorder factors when needed.

Going from the abstract back to the concrete, we have the example below:

Example 6. Suppose you are faced with this mess:

$$(a\,\vec{v} + b\,\vec{w}) \otimes (c\,\vec{s} + d\,\vec{t} + e\,\vec{u}) \otimes (f\,\vec{q} + g\,\vec{r})\,.$$

To expand it, what do you do? *Don't panic.* If you have a long list of things to do, just do them *one at a time.* Specifically in this case, use associativity to expand the bracketed terms first:

$$\begin{aligned}&\underbrace{(a\,\vec{v} + b\,\vec{w}) \otimes (c\,\vec{s} + d\,\vec{t} + e\,\vec{u})} \otimes (f\,\vec{q} + g\,\vec{r}) \\ &= (ac\,\vec{v} \otimes \vec{s} + ad\,\vec{v} \otimes \vec{t} + ae\,\vec{v} \otimes \vec{u} + bc\,\vec{w} \otimes \vec{s} + bd\,\vec{w} \otimes \vec{t} + be\,\vec{w} \otimes \vec{u}) \otimes (f\,\vec{q} + g\,\vec{r}).\end{aligned}$$

Now you can multiply through and expand the rest of the terms as

$$\begin{aligned}&acf\,\vec{v} \otimes \vec{s} \otimes \vec{q} + acg\,\vec{v} \otimes \vec{s} \otimes \vec{r} + adf\,\vec{v} \otimes \vec{t} \otimes \vec{q} + adg\,\vec{v} \otimes \vec{t} \otimes \vec{r} \\ &\quad + aef\,\vec{v} \otimes \vec{u} \otimes \vec{q} + aeg\,\vec{v} \otimes \vec{u} \otimes \vec{r} + bcf\,\vec{w} \otimes \vec{s} \otimes \vec{q} + bcg\,\vec{w} \otimes \vec{s} \otimes \vec{r} \\ &\quad + bdf\,\vec{w} \otimes \vec{t} \otimes \vec{q} + bdg\,\vec{w} \otimes \vec{t} \otimes \vec{r} + bef\,\vec{w} \otimes \vec{u} \otimes \vec{q} + beg\,\vec{w} \otimes \vec{u} \otimes \vec{r}\,,\end{aligned}$$

which is the desired expansion.

With some basic tensor product definitions at hand, we can now leverage them to discuss joint probability distributions in a slick vector space formalism.

Respecting historical tradition,[1] suppose we have two urns, where the first urn has N objects and the second urn has M objects. Suppose that the probability that we select one of the N items in the first urn is described by the probability

[1] See *Ars Conjectandi* by Jacob Bernoulli, published posthumously in 1713.

vector $\vec{p} \in \mathbb{R}^N$, and the probability that we select one of the M items in the second urn is described by the probability vector $\vec{q} \in \mathbb{R}^M$. Then if we select an item from the first urn followed by the second urn, what is the probability that we sampled item i from the first urn *and* item j from the second urn? The answer is encoded in the tensor product $\vec{p} \otimes \vec{q}$, and in particular its $(i-1)M + j$th entry:

$$[\vec{p} \otimes \vec{q}]_{(i-1)M+j} = p_i q_j \, .$$

We can extract this entry by dotting $\vec{p} \otimes \vec{q}$ against $\vec{e}_i^{\,T} \otimes \vec{e}_j^{\,T}$, namely

$$(\vec{e}_i^{\,T} \otimes \vec{e}_j^{\,T}) \cdot (\vec{p} \otimes \vec{q}) = p_i q_j \, .$$

The vector $\vec{p} \otimes \vec{q}$ is itself a probability vector living in $\Delta_{NM} \subset \mathbb{R}^{NM}$; thus it is a probability distribution on NM outcomes, as we wanted.

So far we have examined $\vec{p} \otimes \vec{q}$ which is a product distribution, assuming in our example that our sampling from each of the two urns is uncorrelated. Below we show in an example that convex combinations of tensor products can represent a correlated, joint distribution.

Example 7. Suppose the first urn has two items ($N = 2$), say a ring and a watch, and the second urn has three items ($M = 3$), say a tissue, a match, and a rubber band. The urns were prepared by the ghost of Jacob Bernoulli. We are told that with probability $1/3$ he put a ring in the first urn *and* a rubber band in the second urn, and with probability $2/3$ he put a watch in the first urn *and* a match in the second urn. Then the joint distribution over the urns is described by

$$\frac{1}{3} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} + \frac{2}{3} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1/3 \\ 0 \\ 2/3 \\ 0 \end{bmatrix} .$$

This distribution does not factorize into a tensor product of two individual vectors.

We abstract this example in the following remark.

Remark 10 (Joint distributions and multi-index notation)**.** *Given k probability spaces represented by $\Delta_{N_i} \subset \mathbb{R}^{N_i}$ for $i = 1, ..., k$, a distribution on the joint space is represented by*

$$\Delta_{N_1 \cdots N_k} \subset \mathbb{R}^{N_1 \cdots N_k} \simeq \mathbb{R}^{N_1} \otimes \cdots \otimes \mathbb{R}^{N_k} .$$

Product (independent) distributions have the special form $\vec{p}^{\,(1)} \otimes \vec{p}^{\,(2)} \otimes \cdots \otimes \vec{p}^{\,(k)}$, and general joint distributions are convex combinations of such products. For example, if $\vec{p}_i^{\,(j)}$ represents a distribution in $\mathbb{R}^{N_j}$, then

$$\sum_{i_1, i_2, \ldots, i_k} r_{i_1 i_2 \cdots i_k} \, \vec{p}_{i_1}^{\,(1)} \otimes \vec{p}_{i_2}^{\,(2)} \otimes \cdots \otimes \vec{p}_{i_k}^{\,(k)}$$

is a joint distribution so long as $r_{i_1 i_2 \cdots i_k} \geq 0$ for all $i_1, i_2, ..., i_k$ and additionally $\sum_{i_1, i_2, \ldots, i_k} r_{i_1 i_2 \cdots i_k} = 1$. Here we have used a multi-index notation, in which we are putting subscripts on subscripts; this is to avoid notation like $\sum_{a,b,c,\ldots} r_{abc\cdots}$ which do not specify the total number of subscripts, which in our case is k. (Moreover, there are only 26 letters of the Latin alphabet.) Multi-index notation may initially

seem like gross notation, but you will soon grow accustomed to it, like generations have before you.

Joint distributions interface nicely with the $\vec{1}^T$ row vector in a number of ways. For clarity, let us write $\vec{1}_N^T$ to denote the all-ones row vector with N entries. Then we have the nice identity

$$\vec{1}_{N_1}^T \otimes \vec{1}_{N_2}^T \otimes \cdots \otimes \vec{1}_{N_k}^T = \vec{1}_{N_1 N_2 \cdots N_k}^T .$$

Thus if $\vec{p}$ is a joint distribution living in $\Delta_{N_1 N_2 \cdots N_k}$, then we have

$$(\vec{1}_{N_1}^T \otimes \vec{1}_{N_2}^T \otimes \cdots \otimes \vec{1}_{N_k}^T) \cdot \vec{p} = \vec{1}_{N_1 N_2 \cdots N_k}^T \cdot \vec{p} = 1 .$$

We can also use the all-one row vector to formulate a nice way of computing marginal distributions. To illustrate, we proceed with the example below.

Example 8. Consider a joint distribution on $\Delta_6 \subset \mathbb{R}^2 \otimes \mathbb{R}^3$. Let us denote the joint distribution by $\vec{p}_{AB}$ where A represents the first subsystem of two items, and B represents the second subsystems of three items. Then we can write $\vec{p}_{AB}$ as

$$\vec{p}_{AB} = \begin{bmatrix} p_{AB}(1,1) \\ p_{AB}(1,2) \\ p_{AB}(1,3) \\ p_{AB}(2,1) \\ p_{AB}(2,2) \\ p_{AB}(2,3) \end{bmatrix} .$$

Suppose we want to marginalize over the second probability space (the one over three items). Letting $\mathbb{1}_N$ denote the $N \times N$ identity matrix, we marvel at the linear operator $\mathbb{1}_2 \otimes \vec{1}_3^T$ which maps $\mathbb{R}^2 \otimes \mathbb{R}^3 \to \mathbb{R}^2$. We marvel at it because applying the operator to $\vec{p}_{AB}$ we find

$$(\mathbb{1}_2 \otimes \vec{1}_3^T) \cdot \vec{p}_{AB} = \begin{bmatrix} p_{AB}(1,1) + p_{AB}(1,2) + p_{AB}(1,3) \\ p_{AB}(2,1) + p_{AB}(2,2) + p_{AB}(2,3) \end{bmatrix} = \begin{bmatrix} p_A(1) \\ p_A(2) \end{bmatrix} = \vec{p}_A$$

where $\vec{p}_A$ is the marginal distribution on the first subsystem A, which has two items.

The insight in the above example generalizes in the following way.

Remark 11 (Marginalizing any subset of subsystems)**.** *Let $\vec{p} \in \Delta_{N_1 \cdots N_k}$ be a joint distribution on k subsystems with sizes $N_1, ..., N_k$. For any subset $S \subseteq \{1, ..., k\}$, define the linear "marginalization" map*

$$\mathcal{M}_S := \bigotimes_{j=1}^{k} K_j = K_1 \otimes K_2 \otimes \cdots \otimes K_k , \qquad K_j = \begin{cases} \mathbb{1}_{N_j} & \text{if } j \in S \\ \vec{1}_{N_j}^T & \text{if } j \notin S \end{cases} ,$$

and so $\mathcal{M}_S : \mathbb{R}^{N_1 \cdots N_k} \to \mathbb{R}^{Prod_{j \in S} N_j}$. Then $\mathcal{M}_S \cdot \vec{p}$ is the marginal over the subsystems indexed by S.

To summarize, we have recast ordinary probability theory (on discrete probability spaces) in a linear-algebraic language, which has motivated us to develop the fundamentals of multi-linear algebra and tensor products. This mathematical technology certainly illuminates aspects of multi-linearity lurking in ordinary probability theory. But our true motivation was to set up probability theory in such a way as to make (finite-dimensional) quantum mechanics appear as a natural generalization, using many of the same ingredients. In this next section when

we introduce quantum mechanics, we will relentlessly capitalize on parallels with probability theory, but also take care to point out where such parallels break down.

2. Quantum theory in finite dimensions

We begin with a very brief history of quantum theory. Circa 1900 Max Planck studied blackbody radiation, and solved an inadequacy in the extant equations by stipulating that energy is quantized in units of his eponymous constant. Then in 1905, Einstein suggests that light itself is quantized as "photons", providing an explanation for the photoelectric effect. In the ensuing decade, Bohr makes a first pass at quantum theory (the so-called 'old' quantum theory), and correctly predicts the spectral lines of hydrogen. This first pass at quantum theory only goes so far, and a second pass is made in the 1920's. In 1924, de Broglie postulates that a particle with momentum p has 'wavelength' $\lambda = h/p$, which is soon confirmed by electron diffraction experiments. Thereafter, Heisenberg, Born, and Jordan developed matrix mechanics in 1925 (although they did not yet understand the connection to de Broglie). In 1926, Schrödinger leveraged de Broglie's insight to develop wave mechanics, and that same year showed the equivalence with matrix mechanics. That year as well, Born gave a 'probabilistic' interpretation of quantum mechanics which clarified its connections to measurable quantities in experiments. In 1927, Heisenberg wrote down his famous uncertainty principle. Most of the abstract mathematical foundations of quantum mechanics were consolidated by Dirac and von Neumann in the early 1930's, and Einstein-Podolsky-Rosen as well as Schrödinger highlighted the importance of entanglement in 1935. The year after in 1936, Birkoff and von Neumann investigated how quantum mechanics leads to a new form of logical reasoning that goes beyond classical Boolean logic; in hindsight this may be regarded as the first hint of the possibility of quantum computing (although it was not understood as such at the time).

Having completed our brief historical diegesis, we now turn to presenting the axioms of quantum mechanics. There are various ways of 'motivating' the axioms of quantum mechanics, although at some level they were *guessed* by very clever people and experimentally confirmed by very clever people (sometimes in the opposite order). We will, however, give some intuition. But first, a word of caution. When someone asks for a motivation for quantum mechanics in terms of classical mechanics, this is philosophically backwards; it would be like asking for a derivation of special relativity starting from Newton's equations. Indeed, just as special relativity reduces to Newtonian physics in a certain regime of validity, so too does quantum mechanics reduce to classical mechanics in a certain regime of validity. Nonetheless, we will proceed with an idiosyncratic way of 'guessing' some of the axioms of quantum mechanics starting from classical intuitions.

2.1. Mechanics on ℓ^p spaces: from classical to quantum

Let us begin by contemplating the salient mathematical structures undergirding the dynamics of probability distributions discussed above. For this, it is useful to have the following definition:

Definition 12 (Normed vector space)**.** *Let V be a vector space over a field K; we will consider either $V = \mathbb{R}^N$ (with $K = \mathbb{R}$), or $V = \mathbb{C}^N$ (with $K = \mathbb{C}$). A* ***normed***

vector space *is a pair* $(V, \|\cdot\|)$ *where* $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ *is the* ***norm*** *which satisfies the following three properties:*

(1) (Positive definiteness) $\|\vec{v}\| = 0$ *if and only if* $\vec{v}$ *is the zero vector.*
(2) (Absolute homogeneity) $\|a\,\vec{v}\| = |a|\|\vec{v}\|$ *for any* $a \in K$ *and any* $\vec{v} \in V$*.*
(3) (Triangle inequality) $\|\vec{v} + \vec{w}\| \leq \|\vec{v}\| + \|\vec{w}\|$ *for any* $\vec{v}, \vec{w} \in V$*.*

Then we can define a very useful class of norms as follows:

Definition 13 (ℓ^p norms)**.** *The* ℓ^p ***norm****, defined over* $\mathbb{R}^N$ *or* $\mathbb{C}^N$ *for* $p \geq 1$*, is*

$$\|\vec{v}\|_p := \left(\sum_{j=1}^{N} |v_j|^p \right)^{\frac{1}{p}}. \tag{5}$$

One can show that (5) is indeed a norm in the sense of Definition 12 above. (It is immediate to verify positive definiteness and absolute homogeneity; verifying the triangle inequality involves a more delicate proof leveraging Hölder's inequality.)

A special case of the ℓ^p norm is when $p = 1$, giving $\|\vec{v}\|_1 = \sum_{j=1}^{N} |v_j|$. Then when $\vec{p}$ describes a probability distribution, the normalization of probability distributions is equivalent to the condition $\|\vec{p}\|_1 = 1$. Then our characterization of Markov matrices can be equivalently phrased as follows: M is a Markov matrix if and only if

$$\|M \cdot \vec{p}\|_1 = \|\vec{p}\|_1$$

for all $\vec{p}$ describing probability distributions. In fact, using absolutely homogeneity, we also have the slightly weaker statement that M is a Markov matrix if and only if $\|M \cdot \vec{v}\|_1 = \|\vec{v}\|_1$ where all entries of $\vec{v}$ have the same sign. But then we might ask: what are the matrices A such that $\|A \cdot \vec{v}\|_1 = \|\vec{v}\|_1$ for all $\vec{v} \in \mathbb{R}^N$? Interestingly, such matrices A, called ℓ^1-isometries, are highly restricted:

Theorem 14 (ℓ^1-isometries)**.** *Let* $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ *and* $A \in \mathbb{K}^{N \times N}$*. The following are equivalent:*

(1) $\|A \cdot \vec{v}\|_1 = \|\vec{v}\|_1$ *for all* $\vec{v} \in \mathbb{K}^N$*.*
(2) $A = P \cdot \mathrm{diag}(\varepsilon_1, \ldots, \varepsilon_N)$ *where* P *is a permutation matrix and* $|\varepsilon_j| = 1$ *for all* j *(so* $\varepsilon_j = \pm 1$ *if* $\mathbb{K} = \mathbb{R}$*).*

In the proof below, for a vector $\vec{v} = (v_1, \ldots, v_N) \in \mathbb{K}^N$ we write

$$\mathrm{supp}(\vec{v}) := \{\, k \in \{1, \ldots, N\} : v_k \neq 0 \,\}$$

for its *support*. We say two vectors have *disjoint supports* if their supports are disjoint sets.

Proof. Write $\vec{a}_j := A \cdot \vec{e}_j$ for the jth column of A. Then $\|\vec{a}_j\|_1 = \|A \cdot \vec{e}_j\|_1 = \|\vec{e}_j\|_1 = 1$.

Fix $i \neq j$. In the real case,

$$\|\vec{a}_i \pm \vec{a}_j\|_1 = \|A \cdot (\vec{e}_i \pm \vec{e}_j)\|_1 = \|\vec{e}_i \pm \vec{e}_j\|_1 = 2.$$

By the triangle inequality we always have $\|\vec{a}_i \pm \vec{a}_j\|_1 \leq \|\vec{a}_i\|_1 + \|\vec{a}_j\|_1 = 2$; equality of sums forces equality *coordinate-wise*. Thus for every coordinate k,

$$|a_i(k) \pm a_j(k)| = |a_i(k)| + |a_j(k)|.$$

For reals, the '+' equality enforces same sign (or a zero), and the '−' equality enforces opposite sign (or a zero); both can hold only if $a_i(k)a_j(k) = 0$. Hence $\mathrm{supp}(\vec{a}_i) \cap \mathrm{supp}(\vec{a}_j) = \varnothing$.

In the complex case, use

$$\|\vec{a}_i + \vec{a}_j\|_1 = \|\vec{a}_i + i\,\vec{a}_j\|_1 = 2.$$

Again equality is coordinate-wise, so with $z = a_i(k)$ and $w = a_j(k)$,

$$|z + w| = |z| + |w|, \qquad |z + i\,w| = |z| + |w|\,.$$

Each equality in $\mathbb{C}$ holds if and only if the summands share an argument; the first says z and w are collinear, the second says z and $i\,w$ are collinear. This is impossible unless $z = 0$ or $w = 0$. Thus the supports of distinct columns are disjoint in the complex case as well.

We now have N nonempty, pairwise-disjoint subsets $S_j := \mathrm{supp}(\vec{a}_j) \subseteq \{1, \ldots, N\}$. Therefore

$$N \;\le\; \sum_{j=1}^{N} |S_j| = \Big|\bigcup_{j=1}^{N} S_j\Big| \;\le\; N,$$

so $|S_j| = 1$ for all j. Hence $\vec{a}_j = \varepsilon_j\,\vec{e}_{\sigma(j)}$ for some permutation σ and some $\varepsilon_j \neq 0$. From $\|\vec{a}_j\|_1 = |\varepsilon_j| = 1$ we get $|\varepsilon_j| = 1$, and writing P for the permutation matrix of σ gives $A = P \cdot \mathrm{diag}(\varepsilon_1, \ldots, \varepsilon_N)$. The converse is immediate. □

Remark 15. *Equivalently, the ℓ^1-isometries are the **signed permutation matrices** when $\mathbb{K} = \mathbb{R}$ and the **monomial matrices** with unimodular entries (i.e. their absolute value equals one) when $\mathbb{K} = \mathbb{C}$. If one further assumes $A_{ij} \geq 0$, then necessarily $\varepsilon_j = 1$ for all j, so A is a permutation matrix.*

The upshot of Theorem 14 is that the only linear maps that preserve the ℓ^1 norm on all of $\mathbb{R}^N$ (or $\mathbb{C}^N$) are signed-permutation (or monomial) matrices. Thus, if we insist on global ℓ^1–isometries, the dynamics amount only to relabeling coordinates and multiplying by signs (or phases). A nontrivial theory appears when we restrict attention to the positive cone and, in particular, to the probability simplex Δ_N: requiring a linear map M to send probability vectors to probability vectors yields precisely the column–stochastic (Markov) matrices introduced above. Moreover, Theorem 14 generalizes as follows:

Theorem 16 (ℓ^p-isometries for $p \neq 2$)**.** *Let $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ and $A \in \mathbb{K}^{N\times N}$. Then for $p \geq 1$ and $p \neq 2$, the following are equivalent:*

(1) $\|A \cdot \vec{v}\|_p = \|\vec{v}\|_p$ for all $\vec{v} \in \mathbb{K}^N$.

(2) $A = P \cdot \mathrm{diag}(\varepsilon_1, \ldots, \varepsilon_N)$ where P is a permutation matrix and $|\varepsilon_j| = 1$ for all j (so $\varepsilon_j = \pm 1$ if $\mathbb{K} = \mathbb{R}$).

A proof can be found in [**Aar04**] (although the original proof goes back to at least Banach). The theorem above shows that for $p \neq 2$ the only linear $\|\cdot\|_p$–isometries are monomial matrices, so there is no norm-preserving linear dynamics that mixes coordinates beyond permutations (and multiplicative sign or phase factors). The case $p = 1$ is special only in that, after restricting to the positive cone, we can relax from "isometry on all vectors" to the weaker requirement "maps the probability simplex to itself"; this yields the rich class of Markov matrices. For $p > 1$ and not equal to 2, no analogous stochastic family exists. By contrast, when $p = 2$ the isometries form a continuous group providing genuinely nontrivial linear dynamics.

We have already explicated how the $p = 1$ case corresponds to classical mechanics; we will see that the $p = 2$ case corresponds to quantum mechanics.

First let us give a structure theorem for the ℓ^2-isometries. We start with the following definition.

Definition 17 (Orthogonal and unitary groups)**.** *A matrix $R \in \mathbb{R}^{N\times N}$ is an **orthogonal matrix** if and only if it satisfies $R^T R = RR^T = \mathbb{1}$. This set of matrices is closed under multiplication and inverses, and forms the **orthogonal group** $O(N)$. Similarly, a matrix $U \in \mathbb{C}^{N\times N}$ is a **unitary matrix** if and only if it satisfies $U^\dagger U = UU^\dagger = \mathbb{1}$. This set of matrices is closed under multiplication and inverses, and forms the **unitary group** $U(N)$.*

Then our structure theorem for ℓ^2-isometries is as follows.

Theorem 18 (ℓ^2-isometries)**.** *Let $R \in \mathbb{R}^{N\times N}$. The following are equivalent.*

(1) $\|R \cdot \vec{v}\|_2 = \|\vec{v}\|_2$ for all $\vec{v} \in \mathbb{R}^N$.
(2) $R \in O(N)$.

Similarly, let $U \in \mathbb{C}^{N\times N}$. The following are equivalent.

(1) $\|U \cdot \vec{v}\|_2 = \|\vec{v}\|_2$ for all $\vec{v} \in \mathbb{C}^N$.
(2) $U \in U(N)$.

We defer the proof until later, when additional mathematical tools will allow us to present it more simply.

In the same way that

$$\vec{p}\,' = M_k \cdots M_2 \cdot M_1 \cdot \vec{p}$$

for the M_i being Markov matrices constitutes ℓ^1-preserving dynamics on $\Delta_N \subset \mathbb{R}^N$, then e.g.

$$\vec{\Psi}' = U_k \cdots U_2 \cdot U_1 \cdot \vec{\Psi} \tag{6}$$

for $\vec{\Psi}, \vec{\Psi}' \in \mathbb{C}^N$ and the U_i being unitary matrices constitutes ℓ^2-preserving dynamics on $\mathbb{C}^N$. Just as probability distributions $\vec{p} \in \Delta_N \subset \mathbb{R}^N$ play a starring role in classical mechanics, the **wavefunction** plays a starring role in quantum mechanics. In its simplest form, a wavefunction is a vector $\vec{\Psi} \in \mathbb{C}^N$. (The fact that $\vec{\Psi}$ lives on $\mathbb{C}^N$ as opposed to $\mathbb{R}^N$ is an empirical fact with measurable consequences.) In particular, the wavefunction will provide a description of the 'state' of a quantum system, and so often the words 'wavefunction' and 'state' are used interchangeably.

Quantum mechanics is essentially the study of dynamics of the form (6) on $\mathbb{C}^N$, along with additional physical input that relates that dynamics to observable reality. Other physical inputs can constrain the form of the unitaries which are used. Before delving into these 'physical' considerations below, it is first worth explicating a bit more of the mathematical structure of ℓ^2 spaces, since they will be our stomping grounds for the entirety of this book.[2]

So far we have introduced the structure of an ℓ^2 norm on $\mathbb{C}^N$, in Definitions 12 and 13 (taking $p = 2$ in the latter). A nice feature of the ℓ^2 norm is that it gives us a very nice additional structure on $\mathbb{C}^N$, namely an inner product space. We define inner product spaces below, and then explain how the ℓ^2 norm allows us to define a canonical inner product space.

[2]They are also, more generally, the stomping grounds for our physical reality.

Definition 19 (Inner product and inner product space)**.** *Let $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ and let V be a vector space over $\mathbb{K}$. An **inner product** on V is a map*

$$\langle \cdot, \cdot \rangle : V \times V \to \mathbb{K}$$

such that for all $u, v, w \in V$ and $a, b \in \mathbb{K}$:

(1) (Conjugate symmetry) $\langle v, w \rangle = \overline{\langle w, v \rangle}$.

(2) (Sesquilinearity) $\langle u, av + bw \rangle = a \langle u, v \rangle + b \langle u, w \rangle$ *and* $\langle au + bv, w \rangle = \overline{a} \langle u, w \rangle + \overline{b} \langle v, w \rangle$. *Equivalently, the inner product is linear in its* second *argument and conjugate–linear in its first.*[3]

(3) (Positive definiteness) $\langle v, v \rangle \geq 0$, *with equality if and only if $v = 0$.*

*A pair $(V, \langle \cdot, \cdot \rangle)$ is called an **inner product space**. The inner product induces a norm by*

$$\|v\| := \sqrt{\langle v, v \rangle}\,.$$

To fully bring you into the fold, we introduce a slightly more refined notion of inner product spaces due to Hilbert.

Definition 20 (Hilbert space)**.** *A (complex) **Hilbert space** is a complex inner product space $(\mathcal{H}, \langle \cdot, \cdot \rangle)$ that is complete*[4] *with respect to the induced norm $\|v\| = \sqrt{\langle v, v \rangle}$.*

Remark 21 (Finite-dimensional case and notation)**.** *When $\dim \mathcal{H} < \infty$, completeness is automatic, so every complex inner product space is a Hilbert space. In this book we work exclusively with finite-dimensional Hilbert spaces, typically written $\mathcal{H} \simeq \mathbb{C}^N$ equipped with the ℓ^2 inner product. We will often write $\vec{\Psi} \in \mathcal{H}$ for a state vector ("wavefunction"), and linear maps on $\mathcal{H}$ are represented by matrices; those that preserve the inner product are precisely the unitary operators $U : \mathcal{H} \to \mathcal{H}$.*

As such, an inner product space can be thought of as a normed space, with additional structure. Below we explain how the ℓ^2 norm is induced by an inner product.

Definition 22 (ℓ^2 inner product)**.** *On $\mathbb{C}^N$ we take the standard inner product to be the **ℓ^2 inner product***

$$\langle v, w \rangle := v^\dagger w = \sum_{j=1}^{N} \overline{v}_j w_j,$$

which on $\mathbb{R}^N$ reduces to $v^T w$. The induced norm is $\|v\| = \sqrt{\langle v, v \rangle} = \left(\sum_{j=1}^{N} |v_j|^2\right)^{1/2} = \|\vec{v}\|_2$, which is precisely the ℓ^2 norm.

A useful notion is (Hermitian) conjugation, which we define below.

Definition 23 (Conjugation and Hermitian adjoint)**.** *For a complex number $a \in \mathbb{C}$, its complex conjugate is a^*. For a vector $\vec{v} \in \mathbb{C}^N$, write $\vec{v}^*$ for entrywise conjugation and define the **conjugate transpose** (or **Hermitian conjugate**) by*

$$\vec{v}^\dagger := (\vec{v}^*)^T\,.$$

---

[3] This is the convention commonly used in physics. Over $\mathbb{R}$ it reduces to bilinearity.

[4] "Complete" means that every Cauchy sequence in $\mathcal{H}$ (with respect to the metric $d(u, v) = \|u - v\|$ induced by the inner product) converges to a limit *in* $\mathcal{H}$: for all $\varepsilon > 0$ there exists N such that $m, n \geq N$ implies $\|x_m - x_n\| < \varepsilon$, and there is $x \in \mathcal{H}$ with $\|x_n - x\| \to 0$. Intuitively, there are no 'holes' in the space.

For a matrix $A \in \mathbb{C}^{M\times N}$, write A^* for entrywise conjugation and define its ***Hermitian adjoint*** *(conjugate transpose) by*

$$A^\dagger := (A^*)^T \in \mathbb{C}^{N\times M}.$$

Equivalently, using the ℓ^2 inner product $\langle u, v\rangle = u^\dagger v = \sum_{j=1}^N u_j^* v_j$, we have that $A^\dagger$ is the unique linear map satisfying

$$\langle x, Ay\rangle = \langle A^\dagger x, y\rangle \quad \text{for all } x \in \mathbb{C}^M,\ y \in \mathbb{C}^N.$$

The adjoint obeys, for all compatible A, B and scalars $\alpha, \beta \in \mathbb{C}$,

$$(AB)^\dagger = B^\dagger A^\dagger, \qquad (\alpha A + \beta B)^\dagger = \alpha^* A^\dagger + \beta^* B^\dagger, \quad (A^\dagger)^\dagger = A.$$

Over $\mathbb{R}$, complex conjugation is trivial ($a^* = a$), so $A^\dagger = A^T$. Additionally, a matrix H is ***Hermitian*** *(or* ***self–adjoint****) if $H^\dagger = H$.*

Having defined the ℓ^2 inner product as well as the Hermitian adjoint, we can rephrase Theorem 18 as:

Theorem 24 (ℓ^2-isometries, reprise)**.** *Let $R \in \mathbb{R}^{N\times N}$. The following are equivalent.*

(1) $\langle R\vec{v}, R\vec{v}\rangle = \langle \vec{v}, \vec{v}\rangle$ for all $\vec{v} \in \mathbb{R}^N$.
(2) $R \in O(N)$.

Similarly, let $U \in \mathbb{C}^{N\times N}$. The following are equivalent.

(1) $\langle U\vec{v}, U\vec{v}\rangle = \langle \vec{v}, \vec{v}\rangle$ for all $\vec{v} \in \mathbb{C}^N$.
(2) $U \in U(N)$.

With our inner product definitions at hand, we are now equipped to provide a simple proof of Theorem 24 and thus Theorem 18.

Proof. We give the argument for $\mathbb{C}^N$; the real case is analogous with † replaced by ^{T} and i replaced by ± 1.

Assume (1): $\langle U\vec{v}, U\vec{v}\rangle = \langle \vec{v}, \vec{v}\rangle$ for all $\vec{v} \in \mathbb{C}^N$. Write

$$\langle U\vec{v}, U\vec{v}\rangle = \langle \vec{v}, U^\dagger U\, \vec{v}\rangle,$$

so for every $\vec{v}$,

$$\langle \vec{v},\, (U^\dagger U - \mathbb{1})\, \vec{v}\rangle = 0.$$

Set $H := U^\dagger U - \mathbb{1}$. Then $\langle \vec{v}, H\vec{v}\rangle = 0$ for all $\vec{v}$. For arbitrary $\vec{x}, \vec{y}$ we compute (using conjugate–linearity in the first argument and linearity in the second):

$$\begin{aligned} 0 &= \langle \vec{x} + \vec{y},\, H(\vec{x} + \vec{y})\rangle = \langle \vec{x}, H\vec{x}\rangle + \langle \vec{x}, H\vec{y}\rangle + \langle \vec{y}, H\vec{x}\rangle + \langle \vec{y}, H\vec{y}\rangle \\ &= \langle \vec{x}, H\vec{y}\rangle + \langle \vec{y}, H\vec{x}\rangle, \\ 0 &= \langle \vec{x} + i\vec{y},\, H(\vec{x} + i\vec{y})\rangle = \langle \vec{x}, H\vec{x}\rangle + i\langle \vec{x}, H\vec{y}\rangle - i\langle \vec{y}, H\vec{x}\rangle + \langle \vec{y}, H\vec{y}\rangle \\ &= i\langle \vec{x}, H\vec{y}\rangle - i\langle \vec{y}, H\vec{x}\rangle. \end{aligned}$$

Solving these two equations gives $\langle \vec{x}, H\vec{y}\rangle = \langle \vec{y}, H\vec{x}\rangle = 0$ for all $\vec{x}, \vec{y}$. Fixing $\vec{y}$ and taking $\vec{x} = H\vec{y}$ yields $\|H\vec{y}\|^2 = 0$, so $H\vec{y} = 0$ for all $\vec{y}$ and hence $H = 0$. Therefore $U^\dagger U = \mathbb{1}$. In particular, the columns of U are orthonormal, so U is invertible and $U^{-1} = U^\dagger$; hence also $UU^\dagger = \mathbb{1}$ and $U \in U(N)$, establishing (2).

Conversely, if $U \in U(N)$ then $U^\dagger U = \mathbb{1}$, and for all $\vec{v}$,

$$\langle U\vec{v}, U\vec{v}\rangle = \langle \vec{v}, U^\dagger U\, \vec{v}\rangle = \langle \vec{v}, \vec{v}\rangle\,,$$

which is (1). This completes the proof. □

Let us pause to summarize what we have done so far in this Subsection. First, we recognized that dynamics on (finite) probability distributions is dynamics that preserves ℓ_1. We then contemplated what dynamics would look like that preserves ℓ_p for $p > 1$, and found that the only interesting option is $p = 2$, for which unitary dynamics does the job. We then explained that the ℓ_2 is produced by a natural inner product, which also interfaces nicely with unitary dynamics. Below, we will show how ℓ_2-preserving dynamics is essentially (finite-dimensional) quantum mechanics, along with some additional mathematical baggage which relates the dynamics to observable measurements. Then let us commence below with the axioms of quantum mechanics.

2.2. The axioms of quantum mechanics

Quantum mechanics was presented essentially its contemporary form by Paul Dirac in 1930 [**Dir81**] and placed on a rigorous Hilbert space footing by John von Neumann in 1932 [**VN18**]. The reader might be surprised to discover that Dirac's book [**Dir81**] remains foundational for quantum-mechanics courses nearly a century later.

2.2.1. *Bra-ket notation*

Before giving the axioms, we introduce Dirac's famous **bra-ket notation**, much beloved by physicists (and sometimes unfairly despised by mathematicians). Consider the $\mathbb{C}^N$, viewed as a Hilbert space with ℓ^2 inner product. In the future, we will simply say "consider the Hilbert space $\mathcal{H} \simeq \mathbb{C}^N$". Recall that if $\vec{\psi}, \vec{\phi} \in \mathcal{H}$ then their inner product is

$$\langle \vec{\psi}, \vec{\phi} \rangle = \sum_{j=1}^{N} \psi_j^* \phi_j = \vec{\psi}^\dagger \cdot \vec{\phi}\,.$$

The far right-hand side demonstrates that we can think of the inner product as a bilinear map from $\mathcal{H}^* \otimes \mathcal{H} \to \mathbb{C}$, where $\mathcal{H}^*$ is the space of row vectors. There is a canonical isomorphism from $\mathcal{H}$ to $\mathcal{H}^*$ given by Hermitian conjugation. This is all just a fancy way of saying the following: to take the inner product $\langle \vec{\psi}, \vec{\phi} \rangle$ of $\vec{\psi}$ and $\vec{\phi}$, we just take the Hermitian conjugate of $\vec{\psi}$ and dot that with $\vec{\phi}$.

The far left-hand side of 2.2.1 takes the notational form of a 'bracket'. Dirac suggests that we enclose vectors in $\mathcal{H}$ by $|\cdot\rangle$, so that instead of writing $\vec{\phi}$ we write $|\phi\rangle$. Such an object is called a 'ket'. In similar spirit, a column vector $\vec{\phi}^\dagger \in \mathcal{H}^*$ is enclosed by $\langle \cdot |$, so that instead of writing $\vec{\psi}^\dagger$ we write $\langle \psi |$. Such an object is called a 'bra'. Then bras and kets are related via Hermitian conjugation, namely

$$|\psi\rangle^\dagger = \langle \psi |\,.$$

Finally, we can put together bras and kets to form

$$\langle \psi | \phi \rangle := \langle \vec{\psi}, \vec{\phi} \rangle = \sum_{j=1}^{N} \psi_j^* \phi_j = \vec{\psi}^\dagger \cdot \vec{\phi}\,,$$

which is a...(drum roll please) 'bra-ket'! Get it?[5]

[5]Famously, Dirac was not known for his sense of humor.

Besides being somewhat whimsical, Dirac's bra-ket notation is in fact extremely useful. The reason is not so much mathematical, but rather visual. As you yourself will experience, bra-ket notation is visually suggestive of how to organize and manipulate certain equations (especially compared with arrows and daggers), and eases the mind towards simplifying complicated expressions in multi-linear algebra. That is, Dirac found a notation which resonates with the structure of our minds.

Let us develop Dirac's notation a bit further. In addition to forming 'inner products' $\langle\psi|\phi\rangle = \vec{\psi}^\dagger \cdot \vec{\phi}$, we can also form 'outer products' $|\phi\rangle\langle\psi| = \vec{\phi} \cdot \vec{\psi}^\dagger$. Here $|\phi\rangle\langle\psi|$ is evidently a rank 1, $N \times N$ matrix. Then the trace of this matrix is evidently

$$\mathrm{tr}(|\phi\rangle\langle\psi|) = \langle\psi|\phi\rangle\,.$$

Since Hermitian conjugation for a scalar is the same as complex conjugation, we have the useful identity

$$(\langle\psi|\phi\rangle)^\dagger = (\langle\psi|\phi\rangle)^* = \langle\phi|\psi\rangle\,,$$

where we observe that the ψ and ϕ have switched sides.

It is useful to show a few examples to get you fully acquainted with bra-ket notation. Consider the standard orthonormal basis $\{\vec{e}_i\}_{i=1}^N$ of $\mathbb{C}^N$, which we denote by $\{|i\rangle\}_{i=1}^N$ in our new notation. The orthonormality of the basis elements can be expressed as

$$\langle i|j\rangle = \delta_{ij} := \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases},$$

where δ_{ij} is called the **Kronecker delta**. Recalling that the identity matrix is $\mathbb{1} = \sum_{i=1}^N \vec{e}_i \cdot \vec{e}_i^T$, in bra-ket notation we have

$$\mathbb{1} = \sum_{i=1}^N |i\rangle\langle i|\,.$$

Then given a state $|\psi\rangle$, we have

$$|\psi\rangle = \mathbb{1}|\psi\rangle = \left(\sum_{i=1}^N |i\rangle\langle i|\right)|\psi\rangle = \sum_{i=1}^N |i\rangle \underbrace{\langle i|\psi\rangle}_{=:\psi_i} = \sum_{i=1}^N \psi_i |i\rangle\,, \tag{7}$$

where ψ_i are the coefficients of $|\psi\rangle$ in the $|i\rangle$-basis. (Note also that $(\langle i|\psi\rangle)^\dagger = \langle i|\psi\rangle)^* = \langle\psi|i\rangle = \psi_i^*$, and so the coefficients of $\langle\psi|$ in the $\langle i|$-covector basis are ψ_i^*.) Similarly, for a matrix M, we have

$$M = \mathbb{1}\cdot M\cdot\mathbb{1} = \left(\sum_{i=1}^N |i\rangle\langle i|\right) M \left(\sum_{j=1}^N |j\rangle\langle j|\right) = \sum_{i,j=1}^N |i\rangle \underbrace{\langle i|M|j\rangle}_{=:M_{ij}}\langle j| = \sum_{i,j=1}^N M_{ij}\,|i\rangle\langle j|\,, \tag{8}$$

where M_{ij} are the matrix elements of M in the $|i\rangle$-basis. As a check of our notation, let us compute $M|\psi\rangle$ using the far-right hand sides of both (7) and (8):

$$M|\psi\rangle = \left(\sum_{i,j=1}^N M_{ij}\,|i\rangle\langle j|\right)\sum_{k=1}^N \psi_k|k\rangle = \sum_{i,j,k=1}^N M_{ij}\psi_k|i\rangle\underbrace{\langle j|k\rangle}_{=\delta_{jk}} = \sum_{i=1}^N \left(\sum_{j=1}^N M_{ij}\psi_j\right)|i\rangle\,.$$

So we see that the coefficients of $M|\psi\rangle$ in the $|i\rangle$-basis are $\sum_{j=1}^N M_{ij}\psi_j$, exactly as expected using the standard rules of matrix multiplication.

For our final flourish, we present the **spectral theorem** in finite dimensions in bra-ket notation. The spectral theorem will play a crucial role in the formulation of quantum mechanics.

Theorem 25 (Spectral theorem for normal matrices in finite dimensions)**.** *Let $A : \mathcal{H} \to \mathcal{H}$ be a linear operator on a finite dimensional complex Hilbert space $\mathcal{H} \simeq \mathbb{C}^N$. The following are equivalent*

(1) A is normal, meaning $A^\dagger A = AA^\dagger$.

(2) There exists an orthonormal basis of eigenstates $|v_1\rangle, \ldots, |v_N\rangle$ and complex numbers $\lambda_1, \ldots, \lambda_N$ such that $A = \sum_{j=1}^N \lambda_j |v_j\rangle\langle v_j|$ Equivalently, if U is the unitary with columns $|v_j\rangle$ then $U^\dagger A U = \mathrm{diag}(\lambda_1, \ldots, \lambda_N)$.

We will break up the proof into a few lemmas:

Lemma 26. *Let $A : \mathcal{H} \to \mathcal{H}$ be a normal matrix for $\mathcal{H} \simeq \mathbb{C}^N$. Then A has at least one eigenvector $|v\rangle$. Moreover, if $A|v\rangle = \lambda|v\rangle$, then $A^\dagger|v\rangle = \lambda^*|v\rangle$.*

Proof. By the fundamental theorem of algebra the characteristic polynomial $p_A(\lambda) = \det(A - \lambda\mathbb{1})$ has a complex root. If λ is such a root, then $A - \lambda\mathbb{1}$ has a non-trivial nullspace, meaning that A has an eigenvalue λ and at least one nonzero eigenstate $|v\rangle$ with $A|v\rangle = \lambda|v\rangle$. Without loss of generality we take $|v\rangle$ to be normalized so that $\langle v|v\rangle = 1$. Now notice that

$$\underbrace{\langle v|A^\dagger}_{=\lambda^*\langle v|} |v\rangle = \lambda^* \,. \tag{9}$$

Recall that the Cauchy-Schwarz inequality $|\langle\psi|\phi\rangle| \leq \sqrt{\langle\psi|\psi\rangle}\sqrt{\langle\phi|\phi\rangle}$ achieves equality only when $|\psi\rangle$ is proportional to $|\phi\rangle$. Assuming A is normal, we have

$$\begin{aligned} |\lambda| &= |\langle v|A^\dagger|v\rangle| \\ &\leq \sqrt{\langle v|v\rangle}\sqrt{\langle v|A^\dagger A|v\rangle} \\ &\leq \sqrt{\langle v|AA^\dagger|v\rangle} \\ &= |\lambda| \,, \end{aligned}$$

where we have used Cauchy-Schwarz in the first equality and normality of A in the equality thereafter. We thus see that Cauchy-Schwarz is tight in the above setting, implying that $A^\dagger|v\rangle$ is proportional to $|v\rangle$. In light of (9), we find that $A^\dagger|v\rangle = \lambda^*|v\rangle$, and so $|v\rangle$ is an eigenstate of $A^\dagger$ with eigenvalue λ^*. □

Lemma 27. *Let $A : \mathcal{H} \to \mathcal{H}$ be a normal matrix for $\mathcal{H} \simeq \mathbb{C}^N$. If A has two eigenvectors $|v\rangle, |w\rangle$ with distinct eigenvalues λ, μ, then $\langle v|w\rangle = 0$, i.e. $|v\rangle$ and $|w\rangle$ are orthogonal.*

Proof. Without loss of generality we can take $\langle v|v\rangle = \langle w|w\rangle = 1$. Using Lemma 26, $A^\dagger|w\rangle = \mu^*|w\rangle$. Then

$$(\lambda - \mu)\langle v|w\rangle = \langle (A - \mu\mathbb{1})v \,|\, w\rangle = \langle v \,|\, (A^\dagger - \mu^*\mathbb{1})w\rangle = 0 \,,$$

and so we find $\langle v|w\rangle = 0$. Thus eigenstates with distinct eigenvalues are orthogonal. □

Lemma 28 (Invariance of an eigenspace and its orthogonal complement)**.** *Let A be a normal operator on a finite–dimensional complex Hilbert space $\mathcal{H}$ and let*

$$E_\lambda := \ker\big(A - \lambda\,\mathbb{1}\big)$$

be the λ–eigenspace of A. Then E_λ and $E_\lambda^\perp$ are each invariant under both A and $A^\dagger$. In particular, the restriction

$$A\big|_{E_\lambda^\perp}$$

is normal on the Hilbert space $E_\lambda^\perp$.

Proof. By Lemma 26, if $|y\rangle \in E_\lambda$ then $A^\dagger|y\rangle = \lambda^*|y\rangle$. Now let $|x\rangle \in E_\lambda^\perp$ and $|y\rangle \in E_\lambda$. Then we have $\langle y|A|x\rangle = \langle A^\dagger y|x\rangle = \lambda^*\langle y|x\rangle = 0$. Since $\langle y|A|x\rangle = 0$ for every $|y\rangle \in E_\lambda$, we have $A|x\rangle \in E_\lambda^\perp$. Thus A leaves $E_\lambda^\perp$ invariant. The same calculation with A and $A^\dagger$ interchanged shows $A^\dagger$ leaves $E_\lambda^\perp$ invariant as well. Trivially A leaves E_λ invariant and from the first step $A^\dagger$ leaves E_λ invariant too.

Finally set $B := A\big|_{E_\lambda^\perp}$. Since both A and $A^\dagger$ leave $E_\lambda^\perp$ invariant, the adjoint of B with respect to the inner product on $E_\lambda^\perp$ is $B^\dagger = A^\dagger\big|_{E_\lambda^\perp}$. Hence

$$B^\dagger B = \big(A^\dagger A\big)\big|_{E_\lambda^\perp} = \big(AA^\dagger\big)\big|_{E_\lambda^\perp} = BB^\dagger,$$

so B is normal on $E_\lambda^\perp$. □

With the above lemmas at hand, we finally turn to the proof of Theorem 25.

Proof of Theorem 25. We prove (1) ⇒ (2) by induction on N. The case $N = 1$ is immediate. Assume the claim holds for all dimensions smaller than N.

By Lemma 26 the operator A has an eigenvalue λ and a nonzero eigenstate. Let $E_\lambda = \ker(A - \lambda\,\mathbb{1})$ and choose an orthonormal basis $\{|v_1\rangle, \ldots, |v_r\rangle\}$ of E_λ. By Lemma 28 the orthogonal complement $E_\lambda^\perp$ is invariant under both A and $A^\dagger$. Hence the restriction

$$B := A\big|_{E_\lambda^\perp}$$

is a normal operator on the Hilbert space $E_\lambda^\perp$ whose dimension is $N - r$. By the induction hypothesis there exists an orthonormal basis $\{|v_{r+1}\rangle, \ldots, |v_N\rangle\}$ of $E_\lambda^\perp$ consisting of eigenstates of B, hence of A. Together with $\{|v_1\rangle, \ldots, |v_r\rangle\}$ this gives an orthonormal eigenbasis of $\mathcal{H}$. Writing A in this basis yields

$$A = \sum_{j=1}^{N} \lambda_j\, |v_j\rangle\langle v_j|\,,$$

with $\lambda_j = \lambda$ for $j \le r$ and λ_j equal to the eigenvalues of B for $j > r$. This proves (2).

For (2) ⇒ (1) we compute

$$A^\dagger = \sum_{j=1}^{N} \lambda_j^*\, |v_j\rangle\langle v_j| \quad \text{and} \quad A^\dagger A = \sum_{j=1}^{N} |\lambda_j|^2\, |v_j\rangle\langle v_j| = AA^\dagger\,,$$

and so A is normal. This completes the proof. □

Remark 29 (Hermitian and unitary cases)**.** *If $A = A^\dagger$ then every λ_j is real and $A = \sum_j \lambda_j |v_j\rangle\langle v_j|$. If A is unitary then every λ_j has $|\lambda_j| = 1$ and $A = \sum_j e^{i\theta_j} |v_j\rangle\langle v_j|$*

As an application, consider the following definition.

Definition 30 (Projector)**.** *A **projector** P on $\mathcal{H}$ is a Hermitian idempotent: $P = P^\dagger = P^2$. Equivalently, $P \succeq 0$ and its eigenvalues lie in $\{0, 1\}$.*

Hermiticity implies that all of the eigenvalues of P are real and positive semi-definiteness implies that all of the eigenvalues are nonnegative. Then $P^2 = P$ means that the eigenvalues are either 0 or 1. Supposing $\mathcal{H} \simeq \mathbb{C}^N$, we can use the spectral decomposition to write P as

$$P = \sum_{i=1}^{r} 1 \cdot |v_i\rangle\langle v_i| + \sum_{i=r+1}^{N} 0 \cdot |v_i\rangle\langle v_i| = \sum_{i=1}^{r} |v_i\rangle\langle v_i|$$

for some orthonormal basis $\{|v_i\rangle\}_{i=1}^N$, where r is the rank of the projector. Then P is a projector onto the r-dimensional subspace of $\mathcal{H}$ spanned by $\{|v_i\rangle\}_{i=1}^r$. We can check that $P^\perp = \mathbb{1} - P$ is also a projector onto the orthogonal complement.

Having covered the essence of bra-ket notation, we turn to presenting the axioms of quantum mechanics a la Dirac (with some refinements).

2.2.2. *The axioms*

Here we give the standard axioms of quantum mechanics, with some commentary. The axioms describe the basic mathematical objects of quantum theory, and tether them to observable reality. In the form presented below, the axioms may seem somewhat abstract, and we will discuss this unusual feature shortly. We have tailored the axioms to the finite-dimensional setting for clarity.

(1) **(Quantum states fully describe a system at fixed time.)** At a fixed moment in time, a quantum system about which we have maximal information is fully described by some state vector $|\psi\rangle$ with unit norm living in a Hilbert space $\mathcal{H}$.

(2) **(Time evolution of a closed system is unitary.)** If a quantum system is closed (i.e. it is not interacting with any external system) and starts in an initial state $|\psi_0\rangle$, then at any later time T the state $|\psi_T\rangle$ will be related to the original one by some unitary, that is $|\psi_T\rangle = U|\psi_0\rangle$ for some unitary U that may depend on T.

(3) **(Physical properties have associated projectors.)** Any measurable physical property (such as "spin-up along the z-axis", or "the particle is in region R") has an associated projector P. Such an operator P is an example of an **observable**.

(4) **(Measurement and the Born rule.)** Suppose we have a property corresponding to a projector P, and measure whether or not a system with state vector $|\psi\rangle$ (with unit norm) has that property. Then the probability that we measure $|\psi\rangle$ to have the given property is $\langle\psi|P|\psi\rangle$. This is called the **Born rule**. If $|\psi\rangle$ is measured to have the property, then after measurement the new state of the system is

$$\frac{P|\psi\rangle}{\sqrt{\langle\psi|P^\dagger P|\psi\rangle}} = \frac{P|\psi\rangle}{\sqrt{\langle\psi|P|\psi\rangle}},$$

which also has unit norm (assuming $P|\psi\rangle \neq 0$, in which case we would never have measured $|\psi\rangle$ to have the given property anyway.)

Now we have a number of comments to make in order to unpack the axioms. The first two axioms were motivated by our previous discussions, in which quantum mechanics is framed as norm-preserving dynamics on ℓ^2. The first axiom codifies that a (normalized) vector in a Hilbert space contains everything there is to know about a quantum state, and the second axioms explains that the dynamics of an isolated system is described by unitary dynamics. Unitary dynamics is reversible since (i.e. unitary matrices are invertible), and so in a closed system the future is completely determined by the past and the past is completely determined by the future. An interesting feature of the second axiom is that it does not tell us *which* unitaries we should use. Indeed, given a classical system, we might wonder what kinds of quantum unitary dynamics can reproduce the the classical dynamics in the appropriate regime. This is a subtle question which goes beyond the axioms, and requires additional empirical input.

The first axiom's proviso "about which we have maximal information" deserves explanation. Consider flipping an unbiased coin to decide whether to prepare a system in state $|\psi_0\rangle$ or $|\psi_1\rangle$. After the flip, the system is in state $|\psi_0\rangle$ with probability $1/2$ or state $|\psi_1\rangle$ with probability $1/2$. This probabilistic description reflects our classical ignorance, not any fundamental quantum uncertainty. The system is definitely in one state or the other; *we* simply do not know which. There is a useful formalism for handling such incomplete knowledge, which we will introduce later.

The second axiom's restriction to "closed" systems is similarly important. A closed system does not interact with any external environment. If such interactions were present, we would need to account for our incomplete knowledge of the environment, which we will address later. When a system couples to an external environment, its dynamics can become non-unitary: information leaks irreversibly from our system into the environment, where it becomes inaccessible to us. Despite being non-unitary, these dynamics can be nicely characterized.

While the first and second axioms specify the basic mathematical objects at play, the third and fourth axioms tether those mathematical objects to empirical reality. This is differently structured than e.g. Newton's axioms of classical mechanics, which specify properties like position and momentum but do not explain what it means to measure them, or how to do so.[6]

Now we turn to the third axiom. The third axiom assigns yes/no properties of a quantum system to linear subspaces of the Hilbert space, via projectors onto those subspaces. For instance, the property 'the spin points up in the z-direction' corresponds to some projector P. The opposite property corresponds to the projector $P^\perp = \mathbb{1} - P$ onto the orthogonal complement. If we have a collection of properties corresponding to projectors $P_1, \ldots, P_k$, we call them **compatible** if the corresponding subspaces are mutually orthogonal, i.e. $P_i P_j = 0$ for $i \neq j$. This orthogonality implies $[P_i, P_j] = 0$. Under orthogonality, if a state answers 'yes' to one property

[6]Part of the reason is that position and momentum, at least in some informal sense, were already known to empiricists in Newton's time. Thus people already knew how to measure them. Interestingly, as we all know, one can use Newton's laws to build devices to better measure position and momentum. You might wonder if this would lead to a circular argument: can we use devices, built using principles from Newton's laws, to then do experiments to test Newton's laws? In short, the answer is 'yes', if we (correctly) conceive of such experiments as testing the *consistency* of Newton's laws with empirical reality. Indeed, since measurements of quantities in Newton's theory require Newton's theory for their specification and possibly design, and there is no clear sense in which one can use empirical findings to test Newton's laws *ex nihilo*.

(i.e. $P_i|\psi\rangle = |\psi\rangle$), it automatically answers 'no' to all others (i.e. $P_j|\psi\rangle = 0$ for $j \neq i$). The projectors $P_1, \ldots, P_k$ are **complete** if their corresponding subspaces span all of $\mathcal{H}$, which is equivalent to $P_1 + \cdots + P_k = \mathbb{1}$. Completeness means that a state will always answer 'yes' to at least one property. Then compatibility and completeness together mean that the state will answer 'yes' to exactly one property in the list (and thus 'no' to all others in the list). The following remark captures some useful nomenclature.

Remark 31 (Hermitian observables)**.** *Let $P_1, \ldots, P_k$ correspond to compatible and complete properties. Suppose that my detector registers the real number a_j to indicate 'yes' for property j. (For instance, if the jth property is 'the particle is at position j', then the detector might just output the number j for the position.) Then we can construct the Hermitian observable*

$$A = \sum_{j=1}^{k} a_j \, P_j \tag{10}$$

which encodes measurement outcomes with respect to our list of properties. In particular,

$$\langle\psi|A|\psi\rangle = \sum_{j=1}^{k} a_j \, \langle\psi|P_j|\psi\rangle = \sum_{j=1}^{k} a_j \, \text{Prob}[\text{measure outcome } j] \, ,$$

*where in the last equality we used the Born rule from the fourth axiom. The resulting number is the expectation value of the output of our detector. Since by the spectral theorem all Hermitian operators A can be written in the form (10) for some choice of compatible and complete properties, we call Hermitian operators **observables**, with the understanding that their physical interpretation in terms of properties comes from their spectral decomposition.*

A consequence of our discussion above is that certain properties may be *incompatible*, i.e. correspond to non-orthogonal subspaces. For instance, properties corresponding to projectors P and Q are said to be incompatible if $[P, Q] \neq 0$. In this case the two measurements do not admit a common eigenbasis, so in general one cannot ascribe sharp values to both properties simultaneously. Typically, if a state has a definite value for the property corresponding to P, then measuring the property corresponding to Q will yield (in light of the fourth axiom) probabilistic results, and the act of measurement can disturb the system so that P is no longer definite. This lack of joint sharpness is the essence of incompatibility, underlies the uncertainty principle, and is one of the distinguishing features of quantum mechanics vis-à-vis classical mechanics.

The fourth axiom is, in a sense, the most mysterious. While the third axioms abstractly explains the relationship between properties of a system and the quantum state of a system, the fourth axiom tethers these properties to probabilistic observable outcomes. To begin, recall that we said that a state $|\psi\rangle$ has the property corresponding to P if $P|\psi\rangle = |\psi\rangle$, and so not have the property if $(\mathbb{1} - P)|\psi\rangle = P^{\perp}|\psi\rangle = |\psi\rangle$ (or equivalently $P|\psi\rangle = 0$). So far we have accounted for the possibilities $P|\psi\rangle = |\psi\rangle$ or 0, but if $|\psi\rangle$ is neither in the subspace corresponding to P or orthogonal to it, then $P|\psi\rangle \neq |\psi\rangle$ and $\neq 0$. The Born rule tells us that we should interpret the norm squares of the projection of $|\psi\rangle$ into P, namely $\langle\psi|P^{\dagger}P|\psi\rangle = \langle\psi|P|\psi\rangle$, as the probability that $|\psi\rangle$ has that property. More peculiar

is that when we affirmatively measure $|\psi\rangle$ to have that property, the $|\psi\rangle$ assumes the new state $\frac{P|\psi\rangle}{\sqrt{\langle\psi|P|\psi\rangle}}$. This state now *has* the property, since

$$P \cdot \frac{P|\psi\rangle}{\sqrt{\langle\psi|P|\psi\rangle}} = \frac{P|\psi\rangle}{\sqrt{\langle\psi|P|\psi\rangle}}$$

Said another way, if we measure a state to affirmatively have a property (whether or not it definitely had the property before), it subsequently *assumes* that property. This is different from classical mechanics: for example, classical mechanics stipulates that if we measure a particle to have position x then it definitely had position x before. In quantum mechanics, by contrast, measuring a particle to be in position x just tells us that the particle is in position x now, even though it might not 'definitively' have had that property before.

We notice another peculiarity of the fourth axiom, which is that the map

$$|\psi\rangle \longmapsto \frac{P|\psi\rangle}{\sqrt{\langle\psi|P|\psi\rangle}} \tag{11}$$

is not in general unitary (unless $P = \mathbb{1}$ in which case the map is the identity since $|\psi\rangle$ has unit norm). This would appear to violate the second axiom, which necessitates unitary dynamics. However, we were careful in the second axiom to specify that unitary dynamics happens for *closed* systems; in ordinary circumstances, the measurement apparatus is external to the system that it interrogates, and so the non-unitary of (11) is not in conflict with the second axiom. However, the fourth axiom tempts us to consider the following: if we described the detector (which itself is quantum-mechanical) as *part of* the closed system, then the total detector-system dynamics must be unitary; then can the fourth axiom somehow be derived from the other three? This question is both challenging and profound. Its core difficulty is that the first three axioms do not speak of probability whereas the fourth axioms does speak of probability; as such, the question posed would mandate that probability is *emergent* in quantum mechanics. There have been a vast number of attempts to weaken the fourth axiom or to in some sense 'derive' it from the other three (which often involves covertly bringing in a weakening of the fourth axiom anyway). For our purposes, we can think of the fourth axiom is *pragmatic*, in that it tells us what happens, *in practice*, when we measure a quantum system with an external measurement device.[7]

Having abstractly discussed the axioms, some examples are in order.

Example 9 (Dynamics and projective measurements for a single qubit). We work in the two-dimensional Hilbert space $\mathcal{H} \simeq \mathbb{C}^2$ with the *computational basis*

[7]Related to the previous footnote, we might wonder how we can test quantum mechanics as a theory if we require quantum theory to build the measurement apparatus needed for the tests themselves. As before, the answer is that we are testing the *consistency* of quantum mechanics, and its alignment with empirical reality. One cannot generally test quantum mechanics with detectors solely intelligible through Newtonian mechanics, i.e. you cannot solely use classical to test quantum (see [**Mah18**] for a quantum cryptographic wrinkle in this story). But it is fine to use quantum to test quantum, so long as it all works out empirically. And it very much does.

$\{|0\rangle, |1\rangle\}$ where $|0\rangle := \begin{bmatrix}1\\0\end{bmatrix}$ and $|1\rangle := \begin{bmatrix}0\\1\end{bmatrix}$. We introduce the **Pauli matrices**[8]

$$X = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$$
$$Y = \begin{bmatrix}0 & -i\\ i & 0\end{bmatrix} = -i\,|0\rangle\langle 1| + i\,|1\rangle\langle 0|$$
$$Z = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|.$$

They are Hermitian, satisfy $X^2 = Y^2 = Z^2 = \mathbb{1}$, and obey

$$[\sigma_j, \sigma_k] = 2i\,\varepsilon_{jk\ell}\,\sigma_\ell, \qquad \{\sigma_j, \sigma_k\} = 2\,\delta_{jk}\,\mathbb{1},$$

where $(\sigma_1, \sigma_2, \sigma_3) = (X, Y, Z)$. Their eigenvalues are ± 1, with $Z|0\rangle = |0\rangle$ and $Z|1\rangle = -|1\rangle$.

Measuring "spin along z" corresponds to the compatible, complete pair of projectors

$$P_0 = |0\rangle\langle 0| = \frac{\mathbb{1} + Z}{2}, \qquad P_1 = |1\rangle\langle 1| = \frac{\mathbb{1} - Z}{2}.$$

Likewise, "spin along x" has eigenstates $|\pm\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ with projectors

$$P_+^{(x)} = |+\rangle\langle +| = \frac{\mathbb{1} + X}{2}, \qquad P_-^{(x)} = |-\rangle\langle -| = \frac{\mathbb{1} - X}{2}.$$

More generally, for any unit vector $\hat{n} = (n_x, n_y, n_z) \in \mathbb{R}^3$ we have

$$P_\pm^{(\hat{n})} = \frac{\mathbb{1} \pm \hat{n}\cdot\vec{\sigma}}{2}, \qquad \hat{n}\cdot\vec{\sigma} := n_x X + n_y Y + n_z Z,$$

which indeed satisfy the properties of projectors.

For dynamics, consider unitary rotations generated by the Pauli matrices. For any unit vector $\hat{n}$ and real angle θ, define

$$R_{\hat{n}}(\theta) := \exp\!\left(-\,i\,\frac{\theta}{2}\,\hat{n}\cdot\vec{\sigma}\right) = \cos\!\left(\frac{\theta}{2}\right)\mathbb{1} - i\,\sin\!\left(\frac{\theta}{2}\right)\hat{n}\cdot\vec{\sigma}.$$

Physically, $R_{\hat{n}}(\theta)$ is the time-t propagator of a closed qubit with Hamiltonian $H = \frac{\Omega}{2}\,\hat{n}\cdot\vec{\sigma}$ and $\theta = \Omega\,t$. That is, $R_{\hat{n}}(\theta)$ can be written as e^{-iHt} for the above choices of H and t.

Suppose we prepare the qubit in the $+1$ eigenstate of Z, namely $|\psi_0\rangle = |0\rangle$. If the system evolves under the Hamiltonian $H = \frac{\Omega}{2}Y$ for time t, the unitary $U(t) = R_y(\theta)$ acts with $\theta = \Omega\,t$. Acting on $|0\rangle$ and using $Y|0\rangle = i|1\rangle$, the evolved state is

$$|\psi_t\rangle = \cos\!\left(\tfrac{\theta}{2}\right)|0\rangle + \sin\!\left(\tfrac{\theta}{2}\right)|1\rangle.$$

Now consider measuring in the Z basis. The Born rule with projectors P_0, P_1 gives

$$p_Z(0\,|\,t) = \cos^2\!\left(\tfrac{\theta}{2}\right), \qquad p_Z(1\,|\,t) = \sin^2\!\left(\tfrac{\theta}{2}\right).$$

[8]The hardest one to remember is Y, in particular the placement of the minus sign in the matrix elements. High energy physicist Howard Georgi has a useful mnemonic: the 'minus i' is lighter so it floats all the way to the top. Now hopefully you will never forget where the minus sign goes.

If outcome 0 is observed, the state collapses to $|0\rangle$; if outcome 1 is observed, it collapses to $|1\rangle$.

If instead we measure in the X basis, the probabilities are

$$p_X(\pm \,|\, t) = \tfrac{1}{2}(1 \pm \langle\psi_t|X|\psi_t\rangle)\,.$$

Since $\langle\psi_t|X|\psi_t\rangle = \sin\theta$, we find

$$p_X(+\,|\,t) = \tfrac{1+\sin\theta}{2}, \qquad p_X(-\,|\,t) = \tfrac{1-\sin\theta}{2}.$$

To connect with the Bloch sphere, define for any $|\psi\rangle$ the triple

$$\vec{r} = (\langle X\rangle, \langle Y\rangle, \langle Z\rangle) \in \mathbb{R}^3.$$

For the state $|\psi_t\rangle$, we obtain $\vec{r}(t) = (\sin\theta, 0, \cos\theta)$, a unit vector rotating about the y-axis. The Born rule in this language becomes

$$\Pr[\text{outcome } \pm \text{ along } \hat{n}] = \frac{1 \pm \hat{n}\cdot\vec{r}}{2}.$$

Armed with our basic examples, we next examine some additional mathematical structures in quantum mechanics.

2.3. Additional mathematical structures

Here we will introduce some additional mathematical apparatus which we can view as additional tools for the applications of the axioms of quantum mechanics presented above.

2.3.1. *Tensor products and density matrices*

We now carry the tensor–product technology into the quantum setting and introduce the operator language that lets us handle classical uncertainty and open–system effects in a clean way. When two systems are modeled by Hilbert spaces $\mathcal{H}_A \simeq \mathbb{C}^{N_A}$ and $\mathcal{H}_B \simeq \mathbb{C}^{N_B}$, their composite is described by the tensor product

$$\mathcal{H}_{AB} := \mathcal{H}_A \otimes \mathcal{H}_B \simeq \mathbb{C}^{N_A N_B}.$$

Choose orthonormal bases $\{|i\rangle_A\})_{i=1}^{N_A}$ and $\{|j\rangle_B\}_{j=1}^{N_B}$. The product kets $\{|i\rangle_A \otimes |j\rangle_B\}_{i,j}$ form an orthonormal basis of $\mathcal{H}_{AB}$. As in the classical case, linear maps respect tensoring. If X_A acts on $\mathcal{H}_A$ and Y_B acts on $\mathcal{H}_B$, then

$$(X_A \otimes Y_B)\big(|\psi\rangle_A \otimes |\phi\rangle_B\big) = (X_A|\psi\rangle_A) \otimes (Y_B|\phi\rangle_B).$$

Operations on a single part are written $X_A \otimes \mathbb{1}_B$ or $\mathbb{1}_A \otimes Y_B$.

A pure state $|\Psi\rangle \in \mathcal{H}_{AB}$ is called a **product state** if it factors as $|\Psi\rangle = |\psi\rangle_A \otimes |\phi\rangle_B$. Otherwise it is **entangled**. The following normal form is indispensable.

Theorem 32 (Schmidt decomposition)**.** *For any unit vector $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ there exist orthonormal sets $\{|k\rangle_A\}$ and $\{|k\rangle_B\}$ together with nonnegative numbers $\{\lambda_k\}$ that sum to one such that*

$$|\Psi\rangle = \sum_{k=1}^{r} \sqrt{\lambda_k}\,|k\rangle_A \otimes |k\rangle_B, \quad r \le \min\{N_A, N_B\}\,.$$

*The number r is uniquely defined and is called the **Schmidt rank**.*

This is really just another way of stating the linear algebraic fact that every $N_A \times N_B$ matrix (in this case the entries of $|\Psi\rangle$ reshaped into such a matrix) has a singular value decomposition, so we defer the proof until a bit later.

Up to this point, our description of a single system has used a unit vector $|\psi\rangle$. That choice corresponds to maximal information. In many situations there is additional classical uncertainty. Perhaps a device prepares $|\psi_j\rangle$ with probability r_j. It is convenient to package such ensembles into a single object, the **density operator** (or **density matrix**)

$$\rho := \sum_j r_j \, |\psi_j\rangle\langle\psi_j| \in \mathcal{S}(\mathcal{H}), \tag{12}$$

which is Hermitian, positive semidefinite, and satisfies $\mathrm{tr}(\rho) = 1$. In fact, any operator which is Hermitian, positive semidefinite, and satisfies $\mathrm{tr}(\rho) = 1$ can be written in the form (12), and so we define:

Definition 33 (Density operator)**.** *A* ***density operator*** $\rho \in \mathcal{S}(\mathcal{H})$ *is a linear operator on* $\mathcal{H}$ *which satisfies* $\rho = \rho^\dagger$*,* $\mathrm{tr}(\rho) = 1$*, and* $\rho \succeq 0$*.*

We say that a state is **pure** when $\rho = |\psi\rangle\langle\psi|$, equivalently $\rho^2 = \rho$ and $\mathrm{tr}(\rho^2) = 1$, and otherwise it is **mixed**. A pure state corresponds to a rank 1 density matrix, and a mixed state corresponds to rank greater than 1. The Born rule extends linearly. Specifically, for a projector P,

$$\Pr[\text{“yes” on } P \text{ given } \rho] = \mathrm{tr}(P\rho),$$

and for an observable A,

$$\mathbb{E}_\rho[A] = \mathrm{tr}(A\rho).$$

Upon a projective measurement with projectors P_j, two kinds of updates occur. If we condition on the outcome j, then

$$\rho \longmapsto \frac{P_j \rho P_j}{\mathrm{tr}(P_j \rho)}.$$

If the outcome is forgotten, then

$$\rho \longmapsto \sum_j P_j \rho P_j,$$

which removes coherences between the corresponding subspaces.

Joint states admit a notion of marginalization that mirrors our classical $\vec{1}^T$ trick. Given ρ_{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$, the state of A alone is the **partial trace** over B:

$$\rho_A := \mathrm{tr}_B(\rho_{AB}) \in \mathcal{S}(\mathcal{H}_A).$$

In coordinates with respect to any orthonormal basis $\{|j\rangle_B\}$,

$$\mathrm{tr}_B(\rho_{AB}) = \sum_j \big(\mathbb{1}_A \otimes \langle j|\big)\, \rho_{AB}\, \big(\mathbb{1}_A \otimes |j\rangle\big). \tag{13}$$

The map tr_B is characterized by the identity

$$\mathrm{tr}\big[(X_A \otimes \mathbb{1}_B)\rho_{AB}\big] = \mathrm{tr}\big[X_A \,\mathrm{tr}_B(\rho_{AB})\big] \quad \text{for all } X_A\,,$$

so it really is the quantum version of taking a marginal. If ρ_{AB} is diagonal in the product basis, (13) reduces exactly to summing out the B index. The identity $\mathrm{tr}_B(\rho_{AB}) = \rho_A$ is the quantum sibling of marginalization by dotting probability vectors with with $\vec{1}^T$, as appeared in our earlier discussion.

Two corollaries are immediate from the Schmidt decomposition. First, if $|\Psi\rangle$ is a pure vector on AB and $\rho_{AB} = |\Psi\rangle\langle\Psi|$, then $\rho_A = \mathrm{tr}_B(\rho_{AB})$ and $\rho_B = \mathrm{tr}_A(\rho_{AB})$ share the same nonzero eigenvalues. The state $|\Psi\rangle$ is entangled if and only if either reduced state is mixed, equivalently if and only if the Schmidt rank is strictly greater than 1. Second, every mixed state can be realized as the marginal of a pure state on a larger space. Given a decomposition $\rho_A = \sum_k \lambda_k |k\rangle\langle k|$, the vector

$$|\Phi\rangle_{AR} = \sum_k \sqrt{\lambda_k}\, |k\rangle_A \otimes |k\rangle_R$$

on an auxiliary space $\mathcal{H}_R$ satisfies $\mathrm{tr}_R(|\Phi\rangle\langle\Phi|) = \rho_A$. This construction is called a **purification**.

With the above notations at hand, we can finally give a proof of the Schmidt decomposition. As mentioned above, it is really just a repackaging of the singular value decomposition, but it is instructive to go through the argument in the quantum language above.

Proof of Theorem 32. Let $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a unit vector. Form the rank-one projector

$$\rho_{AB} := |\Psi\rangle\langle\Psi|$$

and the reduced state on A

$$\rho_A := \mathrm{tr}_B(\rho_{AB}) \in \mathcal{S}(\mathcal{H}_A).$$

Then ρ_A is Hermitian, positive semidefinite, and satisfies $\mathrm{tr}(\rho_A) = 1$. By the spectral theorem there exist an orthonormal set $\{|k\rangle_A\}_{k=1}^r$ and numbers $\lambda_k \geq 0$ with $\sum_{k=1}^r \lambda_k = 1$ such that

$$\rho_A = \sum_{k=1}^r \lambda_k\, |k\rangle_A\langle k|\,,$$

where $r = \mathrm{rank}(\rho_A) \leq N_A$.

For each k with $\lambda_k > 0$ define a vector in $\mathcal{H}_B$ by

$$|\tilde{k}\rangle_B := \frac{1}{\sqrt{\lambda_k}} (\langle k|_A \otimes \mathbb{1}_B)\, |\Psi\rangle\,.$$

We first check orthonormality. For k, ℓ with $\lambda_k, \lambda_\ell > 0$ we compute

$$\begin{aligned}\langle\tilde{k}|\tilde{\ell}\rangle &= \frac{1}{\sqrt{\lambda_k\lambda_\ell}} \langle\Psi|\big(|k\rangle\langle\ell|_A \otimes \mathbb{1}_B\big)|\Psi\rangle \\ &= \frac{1}{\sqrt{\lambda_k\lambda_\ell}}\, \langle k|\, \rho_A\, |\ell\rangle = \frac{1}{\sqrt{\lambda_k\lambda_\ell}}\, \lambda_\ell\, \delta_{k\ell} = \delta_{k\ell}\,,\end{aligned}$$

so $\{|\tilde{k}\rangle_B\}_{k=1}^r$ is an orthonormal set in $\mathcal{H}_B$. Hence $r \leq N_B$ as well.

Next we claim that $|\Psi\rangle = \sum_{k=1}^r \sqrt{\lambda_k}\, |k\rangle_A \otimes |\tilde{k}\rangle_B$. Let us define

$$|\Phi\rangle := \sum_{k=1}^r \sqrt{\lambda_k}\, |k\rangle_A \otimes |\tilde{k}\rangle_B\,,$$

and compare the two vectors by projecting onto A. For any m in an orthonormal basis of $\mathcal{H}_A$ that extends $\{|k\rangle_A\}_{k=1}^r$ we have

$$(\langle m|_A \otimes \mathbb{1}_B)\, |\Psi\rangle = \begin{cases} \sqrt{\lambda_m}\, |\tilde{m}\rangle_B & \text{if } \lambda_m > 0 \\ 0 & \text{if } \lambda_m = 0 \end{cases}$$

by construction. The same identities hold with $|\Psi\rangle$ replaced by $|\Phi\rangle$. Therefore

$$(\langle m|_A \otimes \langle \phi|_B)\left(|\Psi\rangle - |\Phi\rangle\right) = 0$$

for every m and every $|\phi\rangle \in \mathcal{H}_B$. Since such product bras span $(\mathcal{H}_A \otimes \mathcal{H}_B)^*$, it follows that $|\Psi\rangle = |\Phi\rangle$.

Finally observe the reduced state on B,

$$\rho_B := \mathrm{tr}_A(\rho_{AB}) = \sum_{k=1}^{r} \lambda_k \, |\tilde{k}\rangle_B \langle \tilde{k}| \,,$$

so the nonzero spectra of ρ_A and ρ_B agree and equal $\{\lambda_k\}$. The number r is therefore the common rank of ρ_A and ρ_B, which gives $r \leq \min\{N_A, N_B\}$.

We have produced orthonormal sets $\{|k\rangle_A\}$ and $\{|\tilde{k}\rangle_B\}$ and nonnegative numbers $\{\lambda_k\}$ that sum to one such that

$$|\Psi\rangle = \sum_{k=1}^{r} \sqrt{\lambda_k} \, |k\rangle_A \otimes |\tilde{k}\rangle_B \,,$$

which is the desired form. □

Remark 34 (Uniqueness and degeneracies)**.** *The multiset of nonzero coefficients $\{\lambda_k\}$ is uniquely determined by $|\Psi\rangle$ since it is the spectrum of ρ_A and also of ρ_B. The orthonormal families $\{|k\rangle_A\}$ and $\{|\tilde{k}\rangle_B\}$ are unique up to phases when the λ_k are distinct. Within a degenerate eigenspace one may apply a unitary rotation on A and the same conjugate rotation on the corresponding span on B without changing the state $|\Psi\rangle$.*

Now we turn to some examples.

Example 11 (Embedding classical probability into quantum states). Fix the computational basis $\{|i\rangle\}_{i=1}^N$ of $\mathbb{C}^N$. A classical distribution $\vec{p} = (p_1, \ldots, p_N) \in \Delta_N$ is encoded as the diagonal density matrix

$$\rho_{\mathrm{cl}}(\vec{p}) = \sum_{i=1}^{N} p_i \, |i\rangle\langle i|.$$

A measurement in this basis with projectors $P_i = |i\rangle\langle i|$ returns outcome i with probability $\mathrm{tr}(P_i \rho_{\mathrm{cl}}) = p_i$, matching the classical rule.

Example 12 (Bell state, reduced states, and entanglement). Consider two qubits with computational basis $|0\rangle, |1\rangle$. We will write $|00\rangle$ as a shorthand for $|0\rangle \otimes |0\rangle$, and similarly for $|11\rangle$. The maximally entangled vector

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right) \,, \quad \rho_{AB} = |\Phi^+\rangle\langle\Phi^+| \,,$$

has reduced states

$$\rho_A = \mathrm{tr}_B(\rho_{AB}) = \frac{1}{2}\,\mathbb{1}, \qquad \rho_B = \mathrm{tr}_A(\rho_{AB}) = \frac{1}{2}\,\mathbb{1} \,.$$

Each qubit by itself looks completely random, yet the pair together sits in a definite pure state. Local mixedness together with global purity is a signature of entanglement and has no classical analogue.

In summary, tensor products allow us to assemble composite systems, while density matrices enable us to represent both quantum superposition and classical randomization within a single calculus. The partial trace serves as the quantum marginalization operator, mirroring our earlier $\vec{1}^T$ trick. Together, these tools provide a unified linear-algebraic framework for handling open systems, correlations, and measurements on subsystems.

2.3.2. *POVMs and channels*

We now broaden the two pillars introduced so far, namely unitary time evolution and projective (yes/no) measurements, into the general language of **quantum channels** and **POVMs** (positive operator-valued measures). This framework cleanly captures **open-system** dynamics (interaction with an environment) and the most general measurement statistics allowed by quantum mechanics. The picture to keep in mind is simple: attach an ancilla (the "apparatus" or "environment"), evolve unitarily on the larger space, and then either (i) forget the ancilla (a channel), or (ii) read the ancilla (a measurement). Everything that happens to a system can be modeled this way.

First we consider dynamics in the form of quantum channels. Fix a system Hilbert space $\mathcal{H}_S \simeq \mathbb{C}^d$ (here the subscript 'S' stands for 'system'). In practice a system rarely evolves in isolation; it can interact with an external register $\mathcal{H}_E \simeq \mathbb{C}^{d'}$ prepared in some state ρ_E (here the subscript 'E' stands for 'environment'). If the joint closed dynamics is unitary U_{SE}, then any initial system state ρ_S evolves as

$$\rho_S \longmapsto \mathcal{E}[\rho_S] := \mathrm{tr}_E\big(U_{SE}(\rho_S \otimes \rho_E)U_{SE}^\dagger\big).$$

From the cyclicity of trace and $\mathrm{tr}(\rho_E) = 1$, we immediately get $\mathrm{tr}(\mathcal{E}[\rho_S]) = \mathrm{tr}(\rho_S)$, i.e. *trace preservation*. Moreover, tensoring with an arbitrary ancilla and applying the above form shows *complete positivity*: $(\mathrm{Id}_A \otimes \mathcal{E})[X] \succeq 0$ for every positive X on $\mathcal{H}_A \otimes \mathcal{H}_S$.[9]

Definition 35 (Quantum channel)**.** *A* ***quantum channel*** *(or* ***quantum process****) on $\mathcal{H}_S$ is a linear map $\mathcal{E} : \mathcal{S}(\mathcal{H}_S) \to \mathcal{S}(\mathcal{H}_S)$ that is completely positive and trace-preserving (CPTP).*

The dilation form above is not just an example; it is universal:

Theorem 36 (Stinespring dilation)**.** *Every CPTP map $\mathcal{E}$ on $\mathcal{H}_S \simeq \mathbb{C}^d$ admits a representation of the above form for some environment dimension d', environment state ρ_E, and unitary U_{SE} that are fixed independently of the input ρ_S.*

We defer the proof of this since we need an additional structural result about quantum channels.

A convenient "matrix-element" form drops out when ρ_E is pure, say $\rho_E = |0\rangle\langle 0|$. Expanding U_{SE} in an orthonormal basis $\{|i\rangle_E\}$ and defining the **Kraus operators**

$$K_i := \langle i|U_{SE}|0\rangle \in \mathbb{C}^{d\times d},$$

[9]Positivity alone would require $\mathcal{E}[X] \succeq 0$ whenever $X \succeq 0$ on $\mathcal{H}_S$; *complete* positivity demands the same after adjoining *any* spectator system A. Physically, this guarantees the map never creates negative probabilities even on half of an entangled state.

we obtain the **operator-sum** (Kraus) representation

$$\mathcal{E}[\rho] = \sum_i K_i \, \rho \, K_i^\dagger, \qquad \sum_i K_i^\dagger K_i = \mathbb{1}.$$

Conversely, any family $\{K_i\}$ obeying the completeness relation defines a CPTP map. The Kraus representation is nonunique: $\{K_i\}$ and $\{\sum_j u_{ij} K_j\}$ (with u unitary) describe the same channel. These facts are formalized and proved in the following theorem:

Theorem 37 (Kraus decomposition)**.** *Let $\mathcal{E} : \mathcal{S}(\mathcal{H}_S) \to \mathcal{S}(\mathcal{H}_S)$ be CPTP on a d–dimensional Hilbert space $\mathcal{H}_S \simeq \mathbb{C}^d$. Then there exist operators $K_1, \dots, K_r$ on $\mathcal{H}_S$ with*

$$\mathcal{E}[X] = \sum_{i=1}^{r} K_i \, X \, K_i^\dagger \quad \textit{for all } X, \quad \sum_{i=1}^{r} K_i^\dagger K_i = \mathbb{1},$$

where $r \le d^2$. Conversely, any finite family $\{K_i\}$ obeying $\sum_i K_i^\dagger K_i = \mathbb{1}$ defines a CPTP map by the same formula. The representation is nonunique: if U is any unitary and $K_i' := \sum_j U_{ij} K_j$, then $\{K_i'\}$ yields the same channel.

Proof. To begin, recall the Choi-Jamiołkowski isomorphism. Fix an orthonormal basis $\{|j\rangle\}_{j=1}^d$ of $\mathcal{H}_S$ and define the (unnormalized) maximally entangled vector

$$|\Omega\rangle := \sum_{j=1}^{d} |j\rangle \otimes |j\rangle \;\in\; \mathcal{H}_S \otimes \mathcal{H}_S.$$

The **Choi matrix** of $\mathcal{E}$ is

$$J_{\mathcal{E}} := (\mathrm{Id} \otimes \mathcal{E})(|\Omega\rangle\langle\Omega|) = \sum_{j,k=1}^{d} |j\rangle\langle k| \otimes \mathcal{E}\big(|j\rangle\langle k|\big).$$

By complete positivity we know that $J_{\mathcal{E}} \succeq 0$. Moreover, one can check that for any X on $\mathcal{H}_S$ we have

$$\mathcal{E}[X] = \mathrm{tr}_1\Big[(X^T \otimes \mathbb{1})\, J_{\mathcal{E}}\Big], \tag{14}$$

where tr_1 is the partial trace over the first tensor factor. This "reconstruction identity" follows by expanding X in the basis $\{|j\rangle\langle k|\}$.

Next observe that since $J_{\mathcal{E}} \succeq 0$ it admits a decomposition into rank–one projectors,

$$J_{\mathcal{E}} = \sum_{i=1}^{r} |v_i\rangle\langle v_i|$$

where $|v_i\rangle \in \mathcal{H}_S \otimes \mathcal{H}_S$, and $r = \mathrm{rank}(J_{\mathcal{E}}) \le d^2$. Each vector $|v_i\rangle$ can be viewed as defining an operator $K_i : \mathcal{H}_S \to \mathcal{H}_S$ via the canonical "vectorization" correspondence: if $|v_i\rangle = \sum_{a,b} v_{ab}^{(i)} |a\rangle \otimes |b\rangle$, then

$$K_i = \sum_{a,b} v_{ab}^{(i)} \, |b\rangle\langle a|.$$

One can verify directly that for every X,

$$\mathrm{tr}_1\Big[(X^T \otimes \mathbb{1})\, |v_i\rangle\langle v_i|\Big] = K_i X K_i^\dagger.$$

Combining this with (14), we find

$$\mathcal{E}[X] = \sum_{i=1}^{r} K_i X K_i^\dagger,$$

which is precisely the operator–sum form.

It remains to check the normalization. Since $\mathcal{E}$ is trace–preserving, for all ρ we have

$$\mathrm{tr}(\rho) = \mathrm{tr}(\mathcal{E}[\rho]) = \sum_{i=1}^{r} \mathrm{tr}(K_i \rho K_i^\dagger) = \mathrm{tr}\Big(\rho \sum_{i=1}^{r} K_i^\dagger K_i\Big).$$

Because this holds for all density operators ρ, it follows that $\sum_i K_i^\dagger K_i = \mathbb{1}$.

Conversely, suppose we start with any collection of operators $\{K_i\}$ satisfying $\sum_i K_i^\dagger K_i = \mathbb{1}$. The map

$$\mathcal{E}[X] = \sum_i K_i X K_i^\dagger$$

is clearly linear. Trace preservation follows from the same computation above, and complete positivity is immediate: for any ancilla system A and any positive operator Z on $\mathcal{H}_A \otimes \mathcal{H}_S$, we have

$$(\mathrm{Id}_A \otimes \mathcal{E})[Z] = \sum_i (\mathbb{1}_A \otimes K_i)\, Z\, (\mathbb{1}_A \otimes K_i)^\dagger \;\succeq\; 0.$$

Finally, note that the Kraus representation is not unique. If $u = (u_{ij})$ is any unitary matrix and we define $K_i' = \sum_j u_{ij} K_j$, then

$$\sum_i K_i' X K_i'^\dagger = \sum_j K_j X K_j^\dagger, \qquad \sum_i K_i'^\dagger K_i' = \sum_j K_j^\dagger K_j = \mathbb{1},$$

so $\{K_i\}$ and $\{K_i'\}$ describe the same channel. □

Remark 38 (Minimal Kraus number)**.** *The number r of Kraus operators can always be chosen as $r = \mathrm{rank}(J_\mathcal{E}) \le d^2$. This number is minimal; any other representation can be obtained by enlarging the list with zero operators and applying a unitary rotation among them.*

Having established the Kraus decomposition, we can now establish Stinespring dilation:

Proof of Theorem 36. By the Kraus decomposition, choose operators $K_1, \dots, K_r$ on $\mathcal{H}_S$ with $r \le d^2$ such that

$$\mathcal{E}[\rho] = \sum_{i=1}^{r} K_i\, \rho\, K_i^\dagger \quad \text{and} \quad \sum_{i=1}^{r} K_i^\dagger K_i = \mathbb{1}.$$

Let us introduce an environment Hilbert space $\mathcal{H}_E \simeq \mathbb{C}^r$ with orthonormal basis $\{|i\rangle_E\}_{i=1}^r$ and define an isometry

$$V : \mathcal{H}_S \longrightarrow \mathcal{H}_S \otimes \mathcal{H}_E, \quad V|\psi\rangle \;:=\; \sum_{i=1}^{r} K_i|\psi\rangle \otimes |i\rangle_E.$$

Because $\sum_i K_i^\dagger K_i = \mathbb{1}$, we have $V^\dagger V = \mathbb{1}$; indeed, for all $|\phi\rangle, |\psi\rangle \in \mathcal{H}_S$,

$$\langle\phi|V^\dagger V|\psi\rangle = \sum_{i=1}^{r} \langle\phi|K_i^\dagger K_i|\psi\rangle = \langle\phi|\psi\rangle.$$

Taking the partial trace over E then recovers the channel:

$$\mathrm{tr}_E\big(V\rho V^\dagger\big) = \mathrm{tr}_E\left(\sum_{i,j} K_i \rho K_j^\dagger \otimes |i\rangle\langle j|\right) = \sum_i K_i \rho K_i^\dagger = \mathcal{E}[\rho].$$

To express V using a unitary on system plus environment with a fixed environment state, fix a distinguished vector $|0\rangle_E \in \mathcal{H}_E$ and identify $\mathcal{H}_S$ with the d–dimensional subspace $\mathcal{H}_S \otimes |0\rangle_E \subset \mathcal{H}_S \otimes \mathcal{H}_E$. Define U_{SE} on this subspace by

$$U_{SE}\big(|\psi\rangle \otimes |0\rangle_E\big) := V|\psi\rangle$$

for all $|\psi\rangle$ in $\mathcal{H}_S$. Since V is an isometry, this prescription maps an orthonormal basis of $\mathcal{H}_S \otimes |0\rangle_E$ to an orthonormal set in $\mathcal{H}_S \otimes \mathcal{H}_E$. Extend that partial isometry to a unitary U_{SE} on all of $\mathcal{H}_S \otimes \mathcal{H}_E$ by completing orthonormal bases on the domain and codomain and defining U_{SE} to map one basis to the other. Consequently,

$$\mathcal{E}[\rho] = \mathrm{tr}_E\big(V\rho V^\dagger\big) = \mathrm{tr}_E\Big(U_{SE}\,(\rho \otimes |0\rangle\langle 0|)\,U_{SE}^\dagger\Big),$$

which is precisely the stated dilation with environment state $\rho_E = |0\rangle\langle 0|$ and environment dimension $d' = r$. The unitary U_{SE} and the state ρ_E are determined by the chosen Kraus family for $\mathcal{E}$ and therefore are fixed independently of the input ρ. This completes the proof. □

Remark 39 (Minimal and nonunique dilations)**.** *If the Kraus family is chosen to be minimal (with $r = \mathrm{rank}(J_\mathcal{E})$), then $d' = r$ is the minimal environment dimension. Any two Kraus representations $\{K_i\}$ and $\{K_i'\}$ related by a unitary mixing $K_i' = \sum_j u_{ij} K_j$ yield dilations whose isometries differ by a unitary on the environment: $V' = (\mathbb{1} \otimes u)\,V$. Allowing a mixed ρ_E entails no extra generality, since any mixed state can be purified by enlarging the environment.*

Next we make some additional remarks about quantum channels.

Remark 40 (Composition and randomized control)**.** *Channels are closed under composition and convex combination. If $\mathcal{E}$ and $\mathcal{F}$ are channels, then so is $\mathcal{F} \circ \mathcal{E}$. And if with classical probabilities r_j you apply $\mathcal{E}_j$, the average map $\sum_j r_j\,\mathcal{E}_j$ is again a channel. Thus the set of channels is a convex monoid under composition.*

Remark 41 (Heisenberg picture)**.** *The adjoint map $\mathcal{E}^*$ acts on observables and satisfies*

$$\mathrm{tr}\big(\mathcal{E}[\rho]\,A\big) = \mathrm{tr}\big(\rho\,\mathcal{E}^*[A]\big), \quad \mathcal{E}^*[\mathbb{1}] = \mathbb{1}\,.$$

In Kraus form, $\mathcal{E}^*[A] = \sum_i K_i^\dagger A K_i$. We will use this duality to shuttle between "state evolution" and "observable evolution."

Having discussed general dynamics, we now turn out attension to general measurements. Projective measurements are special cases of more general procedures obtained by attaching an apparatus, evolving unitarily, and reading an outcome on the apparatus. Let $\{|i\rangle_A\}_{i=1}^N$ be an orthonormal basis for the apparatus and let U

act on system+apparatus. If the apparatus is initialized in $|0\rangle_A$ and we measure it in the $\{|i\rangle_A\}$ basis, the probability of outcome i on input ρ is

$$p(i) = \mathrm{tr}(F_i\,\rho)\,, \qquad F_i := M_i^\dagger M_i, \qquad M_i := \langle i|U|0\rangle,$$

with $\sum_i F_i = \mathbb{1}$ by unitarity.

Definition 42 (POVM)**.** *A **positive operator-valued measure** (POVM) on $\mathcal{H}_S$ is a finite collection of positive semidefinite operators $\{F_i\}_{i=1}^N$ obeying $\sum_i F_i = \mathbb{1}$. Given a state ρ, the Born rule assigns outcome probabilities $p(i) = tr(F_i\rho)$.*

The operators F_i are sometimes called **effects**. When $F_i = P_i$ are orthogonal projectors that sum to $\mathbb{1}$ we recover the projective measurements from the axioms. In general, many distinct physical procedures can realize the same POVM statistics. One convenient realization chooses **measurement operators** (one set among many)

$$M_i \quad \text{with} \quad M_i^\dagger M_i = F_i,$$

and then the post-measurement state conditioned on outcome i is

$$\rho \;\longmapsto\; \frac{M_i\,\rho\,M_i^\dagger}{\mathrm{tr}(F_i\rho)}.$$

The family $\{\mathcal{I}_i\}_i$ with $\mathcal{I}_i[\rho] := M_i\rho M_i^\dagger$ is called a **quantum instrument**; it records both the probabilities and the (normalized) output states. Forgetting the outcome yields the average channel $\sum_i \mathcal{I}_i$.

As with channels, there is a universal dilation theorem for POVMs:

Theorem 43 (Naimark dilation)**.** *Every POVM $\{F_i\}$ on $\mathcal{H}_S$ can be realized as a projective measurement on a larger space: there exist an auxiliary Hilbert space $\mathcal{H}_A$, an isometry $V : \mathcal{H}_S \to \mathcal{H}_S \otimes \mathcal{H}_A$, and orthogonal projections $\{\Pi_i\}$ on $\mathcal{H}_A$ such that*

$$F_i = V^\dagger(\mathbb{1}\otimes\Pi_i)V \quad \textit{and} \quad p(i) = \mathrm{tr}\big(F_i\rho\big) = \mathrm{tr}\big[(\mathbb{1}\otimes\Pi_i)\,V\rho V^\dagger\big].$$

Remark 44 (Rank-one refinement)**.** *Every POVM admits a refinement to rank-one effects. Diagonalize each $F_i = \sum_j \lambda_{ij}\,|v_{ij}\rangle\langle v_{ij}|$ and regard the collection $\{F_{i,j} := \lambda_{ij}|v_{ij}\rangle\langle v_{ij}|\}_{i,j}$ as a new POVM. Coarse-graining its outcomes by summing over j reproduces the original statistics:*

$$\sum_j \mathrm{tr}(F_{i,j}\rho) = \mathrm{tr}(F_i\rho).$$

Thus, without loss of generality, one may work with rank-one POVMs when convenient.

To concretize the formalism, we record two examples.

Example 13 (Unsharp qubit measurement). For a qubit with Pauli vector $\vec{\sigma} = (X, Y, Z)$ and a unit vector $\hat{n} \in \mathbb{R}^3$, the two-outcome effects

$$F_\pm^{(\eta,\hat{n})} = \frac{\mathbb{1} \pm \eta\,\hat{n}\cdot\vec{\sigma}}{2}, \qquad 0 \le \eta \le 1,$$

form a POVM. The parameter η is a *sharpness*: $\eta = 1$ gives the projective measurement along $\hat{n}$, while smaller η yields noisy readout with probabilities

$$p(\pm) = \mathrm{tr}\big(F_\pm^{(\eta,\hat{n})}\rho\big) = \tfrac{1}{2}\big(1 \pm \eta\,\hat{n}\cdot\vec{r}\big),$$

where $\vec{r} = (\langle X\rangle, \langle Y\rangle, \langle Z\rangle)$ is the Bloch vector of ρ.

Example 14 (Embedding classical dynamics into a channel). Classical column-stochastic matrices are naturally realized as quantum channels that act classically on the computational basis and erase coherence. Fix an orthonormal basis $\{|i\rangle\}_{i=1}^{N}$ and let $M = (M_{ij})$ be column-stochastic ($M_{ij} \geq 0$ and $\sum_i M_{ij} = 1$ for each j). Define Kraus operators

$$K_{i|j} = \sqrt{M_{ij}}\, |i\rangle\langle j|.$$

Then

$$\mathcal{E}_M[\rho] = \sum_{i,j} K_{i|j}\, \rho\, K_{i|j}^\dagger, \qquad \sum_{i,j} K_{i|j}^\dagger K_{i|j} = \sum_j \Big(\sum_i M_{ij}\Big) |j\rangle\langle j| = \mathbb{1},$$

so $\mathcal{E}_M$ is CPTP. On diagonal inputs $\rho_{\mathrm{cl}}(\vec{p}) = \sum_j p_j |j\rangle\langle j|$ we recover the classical update

$$\mathcal{E}_M\big[\rho_{\mathrm{cl}}(\vec{p})\big] = \sum_{i,j} M_{ij} p_j\, |i\rangle\langle i| = \rho_{\mathrm{cl}}(M \cdot \vec{p}),$$

while for $j \neq k$ the coherence $|j\rangle\langle k|$ is sent to 0 because each Kraus term carries the same input label on both sides. Thus $\mathcal{E}_M$ is a "classicalizing" channel: it dephases in the computational basis and then applies the Markov update to the resulting distribution.

We have seen that the familiar tools of unitary evolution and projective measurements represent only the simplest quantum operations. Real quantum systems demand a richer framework: we enlarge the Hilbert space with ancillary systems, apply unitary evolution to the combined system, then either trace out the ancilla (yielding quantum channels) or measure it (yielding POVMs). This procedure generates the most general dynamics and measurement statistics that quantum mechanics allows. We have explained that quantum channels are completely positive trace-preserving (CPTP) linear maps, characterized by the Kraus representation or Stinespring dilation. POVMs are sets of positive operators that sum to the identity, understood through Naimark's theorem. But the conceptual heart is simple: we compose systems, evolve them unitarily, and then selectively forget or record information.

This unified framework will prove essential for understanding real quantum devices; indeed, in the real world, noise is inevitable, information is incomplete, and systems interact with environments beyond our control. Rather than limitations to work around, these general operations become the natural language for describing quantum processes in practice.

3. A taste of quantum many-body physics

We now turn to many–body systems built from n qubits. The ambient Hilbert space is the n–fold tensor product

$$\mathcal{H} := (\mathbb{C}^2)^{\otimes n} \simeq \mathbb{C}^{2^n}.$$

It is convenient to fix the computational basis $\{|0\rangle, |1\rangle\}$ on each site and to use the Pauli operators X, Y, Z discussed above. To streamline notation, we introduce a

shorthand: for $1 \le i \le n$ we write

$$X_i := \mathbb{1}^{\otimes(i-1)} \otimes X \otimes \mathbb{1}^{\otimes(n-i)},$$

and similarly for Y_i and Z_i. Products such as Z_iZ_j are understood to mean $Z_i \otimes Z_j$ with identities on all other sites, which we will not display explicitly.

More generally, a **Pauli string** on n qubits is a tensor product

$$P = \sigma_{a_1} \otimes \cdots \otimes \sigma_{a_n}, \qquad \sigma_{a_k} \in \{\, \mathbb{1}, X, Y, Z \,\},$$

and its **weight** is the number of non-identity factors,

$$w(P) := |\{\, k : \sigma_{a_k} \neq \mathbb{1} \,\}|,$$

while its **support** is the set $\mathrm{supp}(P)$ of sites where $\sigma_{a_k} \neq \mathbb{1}$. Two elementary commutation facts will be used repeatedly: Pauli matrices on different sites commute, while distinct Pauli matrices on the same site anticommute. Equivalently, Pauli strings P and Q either commute or anticommute, with

$$PQ = (-1)^{N_{\mathrm{anti}}(P,Q)}\, QP,$$

where $N_{\mathrm{anti}}(P, Q)$ counts the number of sites where both act nontrivially with different Pauli matrices.

With this notation in hand, we can define Hamiltonians. A **Hamiltonian** on $\mathcal{H}$ is a Hermitian operator $H = H^\dagger$. In units $\hbar \equiv 1$, the closed–system time evolution is

$$U(t) = e^{-\,iHt}, \qquad |\Psi(t)\rangle = U(t)\,|\Psi(0)\rangle.$$

Since H is Hermitian, its spectrum is real. We denote its smallest eigenvalue by E_0 (the **ground energy**) and the corresponding eigenspace by the **ground space**. A Hamiltonian is called k–**local** if it decomposes as

$$H = \sum_a H_a\,, \quad w(H_a) \le k \;\text{ for every term } H_a,$$

i.e. each interaction acts nontrivially on at most k sites. In the qubit setting one often expands H in the Pauli–string basis,

$$H = \sum_\alpha h_\alpha\, P_\alpha\,, \quad w(P_\alpha) \le k,$$

with real coefficients h_α. To express **geometric locality**, we can place the n qubits on the vertices V of a graph $G = (V, E)$. A geometrically k–local Hamiltonian has each H_a supported on a connected region of at most k vertices (for $k = 2$, typically on edges $(i, j) \in E$). For example, on a line $G = \{1, \ldots, n\}$ with edges $(i, i+1)$, a nearest–neighbor two–local Hamiltonian has the form

$$H = \sum_{i=1}^{n-1} H_{i,i+1} + \sum_{i=1}^{n} H_i,$$

with $H_{i,i+1}$ acting only on sites $i, i+1$ and H_i acting on site i.

The canonical playground for these ideas is the (ferromagnetic) **transverse–field Ising model** (TFIM) on a graph $G = (V, E)$:

$$H_{\mathrm{TFIM}}(J, h) = -\,J \sum_{(i,j)\in E} Z_iZ_j \;-\; h \sum_{i\in V} X_i, \quad J \ge 0,\, h \ge 0.$$

The first term lowers the energy when neighboring Z–spins align, while the second term lowers the energy for qubits pointing in the x–direction (the $|+\rangle$ eigenstate of

X). Thus the two terms compete, and since Z and X do not commute, the model is genuinely quantum. The model is 2–local and geometrically local on G.

Two limiting regimes are exactly solvable and already illustrative. In the classical limit $h = 0$, all terms commute. Ground states maximize each Z_iZ_j, so for $J > 0$ they are the two fully aligned product states $|0\cdots0\rangle$ and $|1\cdots1\rangle$, with two–fold degeneracy. Excitations are domain walls: a bond with anti–aligned neighbors costs energy $2J$ (on an open chain; with periodic boundary conditions, domain walls come in pairs costing $4J$ total). In the opposite paramagnetic limit $J = 0$, each site independently minimizes $-hX_i$, with a unique ground state $|+\rangle^{\otimes n}$ where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. A single spin flip to $|-\rangle$ costs energy $2h$.

Between these limits, the terms fail to commute, which is the source of genuinely quantum behavior. The model enjoys a $\mathbb{Z}_2$ symmetry generated by the global "spin–flip" operator

$$\mathcal{P} := \prod_{i\in V} X_i,$$

under which $Z_i \mapsto -Z_i$ while $X_i \mapsto X_i$. Since $[\mathcal{P}, H_{\mathrm{TFIM}}] = 0$, the Hamiltonian preserves this symmetry. For small h/J the ground space on large graphs approximately breaks the symmetry, exhibiting long–range Z–order. For large h/J the unique ground state is the symmetric paramagnet. On a one–dimensional chain the model is exactly solvable (via Jordan–Wigner fermionization), and at zero temperature there is a quantum phase transition in the thermodynamic limit ($n \to \infty$) at $h = J$ where the energy gap between the lowest and second lowest eigenvalues of H go to zero. While we will not derive this here, a two–site analysis already captures the competition of the two terms.

Example 15 (Two–site TFIM). On two qubits,

$$H_2(J, h) = -J\, Z_1Z_2 - h\,(X_1 + X_2).$$

Diagonalizing (for instance in the joint eigenbasis of the parity X_1X_2) yields four eigenvalues

$$E \in \left\{-\sqrt{J^2 + 4h^2},\ -J,\ +J,\ +\sqrt{J^2 + 4h^2}\right\}.$$

For $J \geq 0$ the ground energy is $E_0 = -\sqrt{J^2 + 4h^2}$, and the gap to the first excited level is

$$\Delta(J, h) = \sqrt{J^2 + 4h^2} - J.$$

We recover the limits discussed above: $\Delta(0, h) = 2h$ and $\Delta(J, 0) = 0$ (reflecting the two–fold degeneracy at $h = 0$). Already at two sites we see how the transverse field h lifts the classical degeneracy and stabilizes a unique paramagnet, while the interaction J favors ferromagnetic order.

On longer chains, the low–energy excitations can be understood in terms of order and disorder. In the $h = 0$ limit, excitations are domain walls that can move freely; turning on a small h allows them to hop and to be created or annihilated in pairs. In the opposite $J = 0$ limit, the excitations are independent spin flips. The $\mathbb{Z}_2$ symmetry generated by $\mathcal{P}$ forbids a nonzero $\langle Z_i\rangle$ expectation value in any exact eigenstate on a finite chain; nevertheless, in the ferromagnetic phase ($h/J \ll 1$) the ground space is nearly two–fold degenerate and exhibits robust long–range correlations $\langle Z_iZ_j\rangle \approx 1$ for distant i, j.