Categorical Quantum Mechanics
An Introduction

Lectured by David Reutter and Jamie Vicary
Notes by Chris Heunen and Jamie Vicary

Department of Computer Science, University of Oxford
16 Lectures, Hilary Term 2019

The idea for this book came from a mini-course at a spring school in 2010, aimed at beginning graduate students from various fields. We first developed the notes in 2012, when they formed the basis for a graduate course at the Department of Computer Science in Oxford, which has run every year since. As of 2016 a version of this course has also run in the School of Informatics in Edinburgh. The text formed the basis for postgraduate summer and winter schools in Dalhousie, Pisa, and Palmse as well, and has improved with feedback from all these students.

In selecting the material, we have strived to strike a balance between theory and application. Applications are interspersed throughout the main text and exercises, but at the same time, the theory aims at maximum reasonable generality. The emphasis is slightly on the theory, because there are so many applications that we can only hint at them. Proofs are written out in full, excepting a handful that are beyond the scope of this book, and a couple of chores that are left as exercises. We have tried to assign appropriate credit, including references, in historical notes at the end of each chapter. Of course the responsibility for mistakes remains entirely ours, and we hope that readers will point them out to us. To make this book as self-contained as possible, there is a zeroth chapter that briefly defines all prerequisites and fixes notation.

This text would not exist were it not for the motivation of Bob Coecke. Between inception and publication of this book, he and Aleks Kissinger wrote another one, that targets a different audience but covers similar material [44]. Thanks are also due to the students who let us use them as guinea pigs for testing out this material. Finally, we are enormously grateful to John-Mark Allen, Pablo Andres Martinez, Miriam Backens, Bruce Bartlett, Oscar Cunningham, Brendan Fong, Pau Enrique Moliner, Tobias Fritz, Peter Hines, Martti Karvonen, Alex Kavvos, Aleks Kissinger, Bert Lindenhovius, Daniel Marsden, Alex Merry, Vaia Patta, David Reutter, Francisco Rios, Peter Selinger, Sean Tull, Dominic Verdon, Linde Wester and Vladimir Zamdzhiev for careful reading and useful feedback on early versions.

Chris Heunen and Jamie Vicary
Edinburgh and Oxford, December 2018

Introduction

Physical systems cannot be studied in isolation. After all, we can only observe their behaviour with respect to other systems, such as a measurement device. The central premise of this book is that the ability to group individual systems into compound systems should be taken seriously. We adopt the action of grouping systems together as a primitive notion, and investigate models of quantum theory from there.

The judicious language for this story is that of categories. Category theory teaches that a lot can be learned about a given type of mathematical species by studying how specimens of the species interact with each other, and it provides a potent instrument to discover patterns in these interactions. No knowledge of specimens' insides is needed; in fact, this often only leads to tunnel vision.

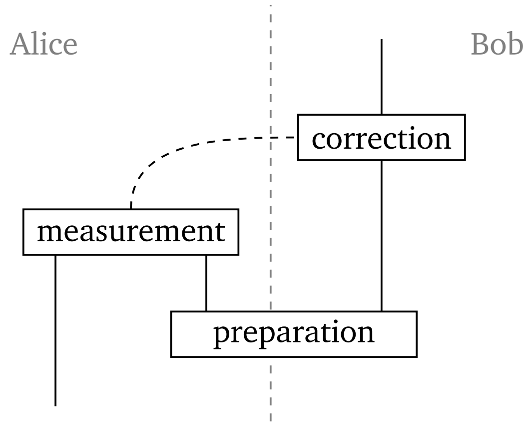
The methods of categories might look nothing like what you would expect from a treatise on quantum theory. But a crucial theme of quantum theory naturally fits with our guiding principle of compositionality: entanglement says that complete knowledge of the parts is not enough to determine the whole.

In providing an understanding of the way physical systems interact, category theory draws closely on mathematics and computer science as well as physics. The unifying language of categories accentuates connections between its subjects. In particular, all physical systems are really quantum systems, including those in computer science. This book applies its foundations to describe protocols and algorithms that leverage quantum theory.

Operational foundations An operational scientist tries to describe the world in terms of operations she can perform. The only things one is allowed to talk about are such operations – preparing a physical system in some state, manipulating a physical system via some experimental setup, or measuring a physical quantity – and their outcomes, or what can be derived from those outcomes by mathematical reasoning.

This is a very constructive way of doing science. After all, these operations and outcomes are what really matter when you build a machine, design a protocol, or otherwise put your knowledge of nature to practical use. But traditional quantum theory contains many ingredients for which we have no operational explanation, even though many people have tried to find one. For example, if states are unit vectors in a Hilbert space, what are the other vectors? If a measurement is a hermitian operator on a Hilbert space, what do other operators signify? Why do we work with complex numbers, when at the end of the day all probabilities are real numbers? Categories offer a way out of these details, while maintaining powerful conclusions from basic assumptions. They let us focus on what is going on conceptually, showcasing the forest rather than the trees.

Graphical calculus When thinking operationally, one cannot help but draw schematic pictures similar to flowcharts to represent what is going on. For example, the *quantum teleportation protocol*, which we will meet many times in this book, has the following schematic representation:



We read time upwards, and space extends left-to-right. We say "time" and "space", but we mean this in a very loose sense. Space is only important in so far as Alice and Bob's operations influence their part of the system. Time is only important in that there is a notion of start and finish. All that matters in such a diagram is its connectivity.

Such operational diagrams seem like informal, non-mathematical devices, useful for illustration and intuitive understanding, but not for precise deduction. In fact, we will see that they can literally be taken as pieces of formal category theory. The "time-like" lines become identity morphisms, and "spatial" separation is modeled by tensor products of objects, leading to monoidal categories.

Monoidal categories form a branch that does not play a starring role, or even any role at all, in most standard courses on category theory. Nevertheless, they put working with operational diagrams on a completely rigorous footing. Conversely, the graphical calculus is an effective tool for calculation in monoidal categories. This graphical language is perhaps one of the most compelling features that monoidal categories have to offer. By the end of the book we hope to have convinced you that this is the appropriate language for describing and understanding many phenomena in quantum theory.

Nonstandard models Once we have made the jump from operational diagrams to monoidal categories, many options open up. In particular, rather than interpreting diagrams in the category of Hilbert spaces, where quantum theory traditionally takes place, we can instead interpret diagrams in a different category, and thereby explore alternatives to quantum theory. Any calculation that was performed purely using the graphical calculus will also hold without additional work in these novel settings. For example, when we present quantum teleportation in the graphical calculus, and represent it in the category of sets and relations, we obtain a description of classical one-time-pad encryption. Thus we can investigate exactly what it is that makes quantum theory 'tick', and what features set it apart from other compositional theories.

Thus monoidal categories provide a unifying language for a wide variety of phenomena, drawn from areas including quantum theory, quantum information, logic, topology, representation theory, quantum algebra, quantum field theory, and even linguistics.

Within quantum theory, categories highlight different aspects than other approaches. Instruments like tensor products and dual spaces are of course available in the traditional Hilbert space setting, but their relevance is heightened here, as they become the central focus. How we represent mathematical ideas affects how we think about them.

Outline After this somewhat roundabout discussion of the subject, it is time to stop beating about the bush, and describe the contents of each chapter.

Chapter 0 covers the background material. It fixes notations and conventions while very briefly recalling the basic notions from category theory, linear algebra and quantum theory that we will be using. Our running example categories are introduced: functions between sets, relations between sets, and bounded linear maps between Hilbert spaces.

Chapter 1 introduces our main object of study: monoidal categories. These are categories that have a good notion of tensor product, which groups multiple objects together into a single compound object. We also introduce the graphical calculus, the visual notation for monoidal categories. This gives a notion of compositionality for an abstract physical theory. The next few chapters will add more structure, so that the resulting categories exhibit more features of quantum theory. Section 1.3 investigates coherence, a technical topic which is essential to the correctness of the graphical calculus, but which is not needed to understand later chapters.

To someone who equates quantum theory with Hilbert space geometry – and this will probably include most readers – the obvious next structure to consider is linear algebra. Chapter 2 shows that important notions such as scalars, superposition, adjoints, and the Born rule can all be represented in the categorical setting.

Chapter 3 investigates entanglement in terms of monoidal categories, using the notion of dual object, building up to the important notion of compact category. This structure is quite simple and powerful: it gives rise to abstract notions of trace and dimension, and is already enough to talk about the quantum teleportation protocol.

Up to this point we considered arbitrary tensor products. But there is an obvious way to build compound objects usually studied in category theory, namely Cartesian products (which already made their appearance in Chapter 2.) In Chapter 4 we consider what happens if the tensor product is in fact a Cartesian product. The result is an abstract version of the no-cloning theorem: if a category with Cartesian products is compact, then it must degenerate.

Chapter 5 then turns this no-cloning theorem on its head. Instead of saying that quantum data cannot be copied, rather, classical data is viewed as quantum data with a copying map, satisfying certain axioms. This leads us to define Frobenius structures, and the derived notion of classical structure. In finite-dimensional Hilbert spaces, classical structures turn out to correspond to a choice of basis. We establish a normal form theorem for Frobenius structures that greatly simplifies computations. Classical structures also allow the description of quantum measurements, and we use this in several application protocols such as state transfer and quantum teleportation.

One of the defining features of quantum mechanics is that systems can be measured in incompatible – or complementary – ways. (The famous example is that of position and momentum.) Chapter 6 defines complementary Frobenius structures. There are strong links to Hopf algebras and quantum groups. With complementarity in hand, we discuss several applications to quantum computing, including the Deutsch-Jozsa algorithm, and some qubit gates which are important to measurement-based quantum computing. We also briefly discuss the ZX calculus: a sound, complete, and universal way to handle any quantum computation graphically, which is eminently amenable to automation.

All discussions so far have focused on pure-state quantum theory. Chapter 7 lifts everything to mixed quantum theory, where we can take probabilistic combinations of states and processes. This is done by analyzing the categorical structure of completely positive maps. The result is axiomatized in terms of environment structures and decoherence structures, and we use it to give another model of quantum teleportation. The chapter ends with a discussion of the difference between classical and quantum information in these terms.

The book finishes with Chapter 8, which sketches higher categories. While an ordinary category has objects, and morphisms going between the objects, a 2-category also has 2-morphisms going between the morphisms. We show how these structures, along with the techniques of higher representation theory, allow us to give a fully geometrical description of quantum teleportation, as a single graphical equation in higher dimension.

That concludes the main development of the material, at which point you will have met the basic ideas of using categories for quantum theory. The book ends there, being an introduction, after all. But this is really just the beginning! After that, it is up to you to expedite the expiration date of this book by studying this exciting topic further.

Contents

Chapter 0

Basics

Traditional first courses in category theory and quantum computing would prepare the reader with solid foundations for this book. However, not much of that material is truly essential to get the most out of this book. This chapter gives a very brief introduction to category theory, linear algebra and quantum computing, enough to get you going with this book if you have not taken a course in any of these areas before, or perhaps to remind you of some details if you have forgotten them. Everything in this chapter can be found in more detail in many other standard texts (see the Notes at the end of the chapter for references). You could skip this chapter for now, and refer back to it whenever some background is missing.

The material is divided into three sections. Section 0.1 gives an introduction to category theory, and in particular the categories $\mathbf{Set}$ of sets and functions, and $\mathbf{Rel}$ of sets and relations. Section 0.2 introduces the mathematical formalism of Hilbert spaces that underlies quantum mechanics, and defines the categories $\mathbf{Vect}$ of vector spaces and linear maps, and $\mathbf{Hilb}$ of Hilbert spaces and bounded linear maps. Section 0.3 recalls the basics of quantum theory, including the standard interpretation of states, dynamics and measurement, and the quantum teleportation procedure.

0.1 Category theory

This section gives a brief introduction to category theory. We focus in particular on the category $\mathbf{Set}$ of sets and functions, and the category $\mathbf{Rel}$ of sets and relations, and present a matrix calculus for relations. We introduce the idea of commuting diagrams, and define isomorphisms, groupoids, skeletal categories, opposite categories and product categories. We then define functors, equivalences and natural transformations, and also products, equalizers and idempotents.

0.1.1 Categories

Categories are formed from two basic structures: *objects* $A, B, C, \ldots$, and *morphisms* $A \xrightarrow{f} B$ going between objects. In this book, we will often think of an object as a *system*, and a morphism $A \xrightarrow{f} B$ as a *process* under which the system A becomes the system B. Categories can be constructed from almost any reasonable notion of system and process. Here are a few examples:

- physical systems, and physical processes governing them;
- data types in computer science, and algorithms manipulating them;
- algebraic or geometric structures in mathematics, and structure-preserving functions;
- logical propositions, and implications between them.

Category theory is quite different from other areas of mathematics. While a category is itself just an algebraic structure — much like a group, ring, or field — we can use categories to organize and understand other mathematical objects. This happens in a surprising way: by neglecting all information about the structure of the objects, and focusing entirely on relationships *between* the objects. Category theory is the study of the patterns formed by these relationships. While at first this may seem limiting, it is in fact empowering, as it becomes a general language for the description of many diverse structures.

Here is the definition of a category.

Definition 0.1. A *category* $\mathbf{C}$ consists of the following data:

- a collection $\mathrm{Ob}(\mathbf{C})$ of *objects*;
- for every pair of objects A and B, a collection $\mathbf{C}(A, B)$ of *morphisms*, with $f \in \mathbf{C}(A, B)$ written $A \xrightarrow{f} B$;
- for every pair of morphisms $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$ with common intermediate object, a *composite* $A \xrightarrow{g \circ f} C$;
- for every object A an *identity morphism* $A \xrightarrow{\mathrm{id}_A} A$.

These must satisfy the following properties, for all objects A, B, C, D, and all morphisms $A \xrightarrow{f} B$, $B \xrightarrow{g} C$, $C \xrightarrow{h} D$:

- *associativity*:

$$h \circ (g \circ f) = (h \circ g) \circ f; \tag{0.1}$$

- *identity*:

$$\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A. \tag{0.2}$$

We will also sometimes use the notation $f \colon A \to B$ for a morphism $f \in \mathbf{C}(A, B)$.

From this definition we see quite clearly that the morphisms are 'more important' than the objects; after all, every object A is canonically represented by its identity morphism id_A. This seems like a simple point, but it is a significant departure from much of classical mathematics, in which particular structures (like groups) play a more important role than the structure-preserving maps between them (like group homomorphisms.)

Our definition of a category refers to collections of objects and morphisms, rather than sets, because sets are too small in general. The category $\mathbf{Set}$ defined below illustrates this well, since Russell's paradox prevents the collection of all sets from being a set. However, such size issues will not play a role in this book, and we will use set theory naively throughout. (See the Notes and further reading at the end of this chapter for more sophisticated references on category theory.)

0.1.2 The category Set

The most basic relationships between sets are given by functions.

Definition 0.2. For sets A and B, a *function* $A \xrightarrow{f} B$ comprises, for each $a \in A$, a choice of element $f(a) \in B$. We write $f \colon a \mapsto f(a)$ to denote this choice.

Writing $\emptyset$ for the empty set, the data for a function $\emptyset \to A$ can be provided trivially; there is nothing for the 'for each' part of the definition to do. So there is exactly one function of this type for every set A. However, functions of type $A \to \emptyset$ cannot be constructed unless $A = \emptyset$. In general there are $|B|^{|A|}$ functions of type $A \to B$, where $|-|$ indicates the cardinality of a set.

We can now use this to define the category of sets and functions.

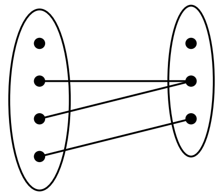
Definition 0.3 ($\mathbf{Set}$, $\mathbf{FSet}$)**.** In the category $\mathbf{Set}$ of sets and functions:

- **objects** are sets $A, B, C, \ldots$;
- **morphisms** are functions $f, g, h, \ldots$;
- **composition** of $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$ is the function $g \circ f \colon a \mapsto g(f(a))$; this is the reason the standard notation $g \circ f$ is not in the other order, even though that would be more natural in some equations such as (0.5) below;
- **the identity morphism** on A is the function $\mathrm{id}_A \colon a \mapsto a$.

Write $\mathbf{FSet}$ for the restriction of $\mathbf{Set}$ to finite sets.

Think of a function $A \xrightarrow{f} B$ in a dynamical way, as indicating how elements of A can evolve into elements of B. This suggests the following sort of picture:

$$A \xrightarrow{f} B$$



(0.3)

0.1.3 The category $\mathbf{Rel}$

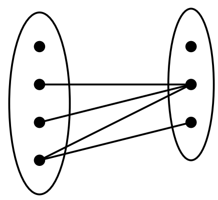
Relations give a more general notion of process between sets.

Definition 0.4. Given sets A and B, a *relation* $A \xrightarrow{R} B$ is a subset $R \subseteq A \times B$.

If elements $a \in A$ and $b \in B$ satisfy $(a, b) \in R$, we often indicate this by writing $a\,R\,b$, or even $a \sim b$ when R is clear. Since a subset can be defined by giving its elements, we can define our relations by listing the related elements, in the form $a_1\,R\,b_1$, $a_2\,R\,b_2$, $a_3\,R\,b_3$, and so on.

We can think of a relation $A \xrightarrow{R} B$ in a dynamical way, generalizing (0.3):

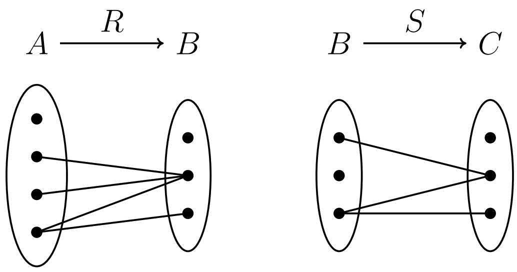
$$A \xrightarrow{R} B$$



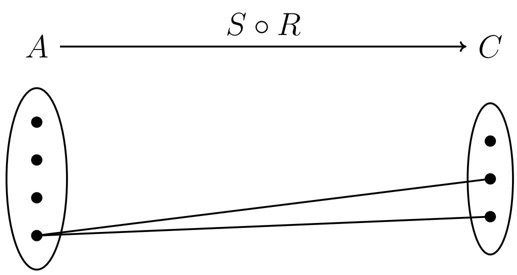
(0.4)

The difference with functions is that this picture indicates interpreting a relation as a kind of nondeterministic classical process: each element of A can evolve into any element of B to which it is related. Nondeterminism enters here because an element of A can relate to more than one element of B, so under this interpretation, we cannot predict perfectly how it will evolve. An element of A could also be related to no elements of B: we interpret this to mean that, for these elements of A, the dynamical process halts. Because of this interpretation, the category of relations is important in the study of nondeterministic classical computing.

Suppose we have a pair of relations, with the codomain of the first equal to the domain of the second:



Our interpretation of relations as dynamical processes then suggests a natural notion of composition: an element $a \in A$ is related to $c \in C$ if there is some $b \in B$ with $a\,R\,b$ and $b\,S\,c$. For the example above, this gives rise to the following composite relation:



This definition of relational composition has the following algebraic form:

$$S \circ R = \{(a, c) \mid \exists b \in B \colon aRb \text{ and } bSc\} \subseteq A \times C \tag{0.5}$$

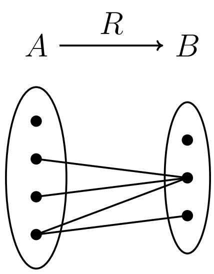
We can write this differently as

$$a\,(S \circ R)\,c \;\Leftrightarrow\; \bigvee_b (bSc \wedge aRb), \tag{0.6}$$

where $\vee$ represents *logical disjunction* (`or`), and $\wedge$ represents *logical conjunction* (`and`). Comparing this with the definition of matrix multiplication, we see a strong similarity:

$$(g \circ f)_{ik} = \sum_k g_{ij} f_{jk} \tag{0.7}$$

This suggests another way to interpret a relation: as a matrix of truth values. For the example relation (0.4), this gives the following matrix, where we write 0 for false and 1 for true:



$$\rightsquigarrow \quad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{0.8}$$

Composition of relations is then just given by ordinary matrix multiplication, with logical disjunction and conjunction replacing $+$ and $\times$, respectively (so that $1+1=1$).

There is an interesting analogy between quantum dynamics and the theory of relations. Firstly, a relation $A \xrightarrow{R} B$ tells us, for each $a \in A$ and $b \in B$, whether it is *possible* for a to produce b, whereas a complex-valued matrix $H \xrightarrow{f} K$ gives us the *amplitude* for a to evolve to b. Secondly, relational composition tells us the *possibility* of evolving via an intermediate point through a sum-of-paths formula, whereas matrix composition tells us the *amplitude* for this to happen.

The intuition we have developed leads to the following category.

Definition 0.5 ($\mathbf{Rel}$, $\mathbf{FRel}$)**.** In the category $\mathbf{Rel}$ of sets and relations:

- **objects** are sets $A, B, C, \ldots$;
- **morphisms** are relations $R \subseteq A \times B$;
- **composition** of $A \xrightarrow{R} B$ and $B \xrightarrow{S} C$ is the relation

$$\{(a,c) \in A \times C \mid \exists b \in B\colon (a,b) \in R, (b,c) \in S\};$$

- **the identity morphism** on A is the relation $\{(a,a) \in A \times A \mid a \in A\}$.

Write $\mathbf{FRel}$ for the restriction of $\mathbf{Rel}$ to finite sets.

While $\mathbf{Set}$ is a setting for classical physics, and $\mathbf{Hilb}$ (to be introduced in Section 0.2) is a setting for quantum physics, $\mathbf{Rel}$ is somewhere in the middle. It seems like it should be a lot like $\mathbf{Set}$, but in fact, its properties are much more like those of $\mathbf{Hilb}$. This makes it an excellent test-bed for investigating different aspects of quantum mechanics from a categorical perspective.

0.1.4 Morphisms

It often helps to draw diagrams of morphisms, indicating how they compose. Here is an example:

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "h"'] & B \arrow[r, "g"] \arrow[d, "i"'] & C \\
D \arrow[r, "k"'] & E \arrow[ur, "j"'] &
\end{tikzcd} \tag{0.9}$$

We say a diagram *commutes* when every possible path from one object in it to another is the same. In the above example, this means $i \circ f = k \circ h$ and $g = j \circ i$. It then follows that $g \circ f = j \circ k \circ h$, where we do not need to write parentheses thanks to associativity. Thus we have two ways to speak about equality of composite morphisms: by algebraic equations, or by commuting diagrams.

The following terms are very useful when discussing morphisms. The term 'operator' below comes from physics.

Definition 0.6 (Domain, codomain, endomorphism, operator)**.** For a morphism $A \xrightarrow{f} B$, its *domain* is the object A, and its *codomain* is the object B. If $A = B$ then we call f an *endomorphism* or *operator*. We sometimes write $\mathrm{dom}(f) = A$ and $\mathrm{cod}(f) = B$.

Definition 0.7 (Isomorphism, retraction)**.** A morphism $A \xrightarrow{f} B$ is an *isomorphism* when it has an *inverse* morphism $B \xrightarrow{f^{-1}} A$ satisfying:

$$f^{-1} \circ f = \mathrm{id}_A \qquad\qquad f \circ f^{-1} = \mathrm{id}_B \tag{0.10}$$

We then say that A and B are *isomorphic*, and write $A \simeq B$. If only the left or right equation of (0.10) holds, then f is called *left-* or *right-invertible*, respectively. A left-invertible morphism is also called a *retraction*.

Lemma 0.8. *If a morphism has an inverse, then this inverse is unique.*

Proof. If g and g' are inverses for f, then:

$$g \overset{(0.2)}{=} g \circ \mathrm{id} \overset{(0.10)}{=} g \circ (f \circ g') \overset{(0.1)}{=} (g \circ f) \circ g' \overset{(0.10)}{=} \mathrm{id} \circ g' \overset{(0.2)}{=} g' \qquad \square$$

Example 0.9. Let's see what isomorphisms are like in our example categories:

- in $\mathbf{Set}$, the isomorphisms are exactly the bijections of sets;
- in $\mathbf{Rel}$, the isomorphisms are the graphs of bijections: a relation $A \xrightarrow{R} B$ is an isomorphism when there is some bijection $A \xrightarrow{f} B$ such that $aRb \Leftrightarrow f(a) = b$.

The notion of isomorphism leads to some important types of category.

Definition 0.10 (Skeletal category)**.** A category is *skeletal* when any two isomorphic objects are equal.

We will show below that every category is *equivalent* to a skeletal category, which means they encode essentially the same algebraic data.

Definition 0.11 (Groupoid, group)**.** A *groupoid* is a category in which every morphism is an isomorphism. A *group* is a groupoid with one object.

Of course, this definition of group agrees with the ordinary one.

Many constructions with and properties of categories can be easily described in terms of morphisms.

Definition 0.12 (Opposite category)**.** Given a category $\mathbf{C}$, its *opposite* $\mathbf{C}^{\mathrm{op}}$ is a category with the same objects, but with $\mathbf{C}^{\mathrm{op}}(A, B)$ given by $\mathbf{C}(B, A)$. That is, the morphisms $A \to B$ in $\mathbf{C}^{\mathrm{op}}$ are morphisms $B \to A$ in $\mathbf{C}$.

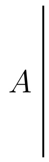
Definition 0.13 (Product category)**.** For categories $\mathbf{C}$ and $\mathbf{D}$, their *product* is a category $\mathbf{C} \times \mathbf{D}$, whose objects are pairs (A, B) of objects $A \in \mathrm{Ob}(\mathbf{C})$ and $B \in \mathrm{Ob}(\mathbf{D})$, and whose morphisms are pairs $(A, B) \xrightarrow{(f,g)} (C, D)$ with $A \xrightarrow{f} C$ and $B \xrightarrow{g} D$.

Definition 0.14 (Discrete category)**.** A category is *discrete* when all the morphisms are identities.

Definition 0.15 (Indiscrete category)**.** A category is *indiscrete* when there is a unique morphism $A \to B$ for each two objects A and B.

0.1.5 Graphical notation

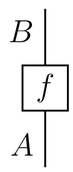
There is a graphical notation for morphisms and their composites. Draw an object A as follows:



(0.11)

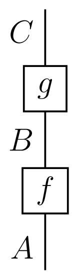
It's just a line. In fact, you should think of it as a picture of the identity morphism $A \xrightarrow{\mathrm{id}_A} A$. Remember: in category theory, the morphisms are more important than the objects.

A morphism $A \xrightarrow{f} B$ is drawn as a box with one 'input' at the bottom, and one 'output' at the top:



(0.12)

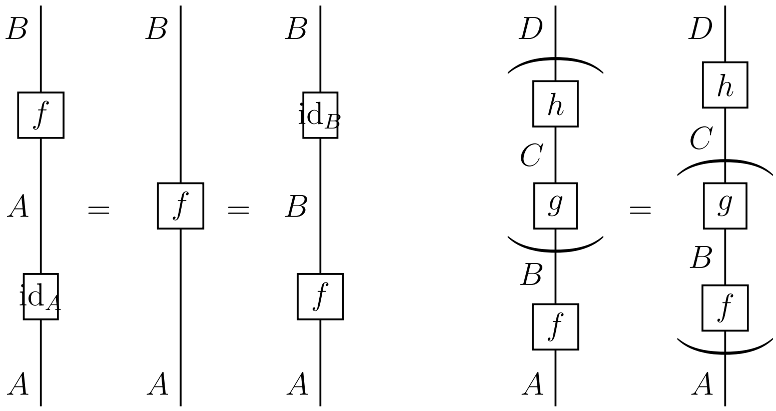
Composition of $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$ is then drawn by connecting the output of the first box to the input of the second box:



(0.13)

The identity law $f \circ \mathrm{id}_A = f = \mathrm{id}_B \circ f$ and the associativity law $(h \circ g) \circ f = h \circ (g \circ f)$

then look like:



(0.14)

To make these laws immediately obvious, we choose to not depict the identity morphisms id_A at all, and not indicate the bracketing of composites.

The graphical calculus is useful because it 'absorbs' the axioms of a category, making them a consequence of the notation. This is because the axioms of a category are about stringing things together in sequence. At a fundamental level, this connects to the geometry of the line, which is also *one-dimensional*. Of course, this graphical representation is quite familiar: you usually draw it horizontally, and call it algebra.

0.1.6 Functors

Remember the motto that in category theory, morphisms are more important than objects. Category theory takes its own medicine here: there is an interesting notion of 'morphism between categories', as given by the following definition.

Definition 0.16 (Functor, covariance, contravariance)**.** Given categories $\mathbf{C}$ and $\mathbf{D}$, a *functor* $F\colon \mathbf{C} \to \mathbf{D}$ is defined by the following data:

- for each object $A \in \mathrm{Ob}(\mathbf{C})$, an object $F(A) \in \mathrm{Ob}(\mathbf{D})$;
- for each morphism $A \xrightarrow{f} B$ in $\mathbf{C}$, a morphism $F(A) \xrightarrow{F(f)} F(B)$ in $\mathbf{D}$.

This data must satisfy the following properties:

- $F(g \circ f) = F(g) \circ F(f)$ for all morphisms $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$ in $\mathbf{C}$;
- $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$ for every object A in $\mathbf{C}$.

Functors are implicitly *covariant*. There are also *contravariant* versions reversing the direction of morphisms: $F(g \circ f) = F(f) \circ F(g)$. We will only use the above definition, and model the contravariant version $\mathbf{C} \to \mathbf{D}$ as (covariant) functors $\mathbf{C}^{\mathrm{op}} \to \mathbf{D}$. A functor between groups is also called a *group homomorphism*; of course this coincides with the usual notion.

We can use functors to give a notion of equivalence for categories.

Definition 0.17 (Equivalence)**.** A functor $F\colon \mathbf{C} \to \mathbf{D}$ is an *equivalence* when it is:

- *full*, meaning that the functions $\mathbf{C}(A,B) \to \mathbf{D}\big(F(A), F(B)\big)$ given by $f \mapsto F(f)$ are surjective for all $A, B \in \mathrm{Ob}(\mathbf{C})$;
- *faithful*, meaning that the functions $\mathbf{C}(A,B) \to \mathbf{D}\big(F(A), F(B)\big)$ given by $f \mapsto F(f)$ are injective for all $A, B \in \mathrm{Ob}(\mathbf{C})$;
- *essentially surjective on objects*, meaning that for each object $B \in \mathrm{Ob}(\mathbf{D})$ there is an object $A \in \mathrm{Ob}(\mathbf{C})$ such that $B \simeq F(A)$.

If two categories are equivalent, then one is just as good as the other for the purposes of doing category theory, even thought they might be defined in quite a different way. Nonetheless, one might be much easier to work with than the other, and that's one reason why the notion of equivalence is so useful.

A category $\mathbf{C}$ is a *subcategory* of a category $\mathbf{D}$ when every object of $\mathbf{C}$ is an object of $\mathbf{D}$, every morphism of $\mathbf{C}$ is a morphism of $\mathbf{D}$, and composition and identities in $\mathbf{C}$ are the same as in $\mathbf{D}$. In other words, the inclusion $\mathbf{C} \to \mathbf{D}$ is a faithful functor.

Every category has a skeleton, a smaller category with the same algebraic structure, that is equivalent to it.

Definition 0.18 (Skeleton)**.** A *skeleton* of a category $\mathbf{C}$ is a subcategory $\mathbf{S}$ such that every object in $\mathbf{C}$ is isomorphic (in $\mathbf{C}$) to exactly one object in $\mathbf{S}$.

Intuitively, a skeleton is built by restricting the category $\mathbf{C}$ to contain just one object from each isomorphism class. The definition says, in other words, that the inclusion functor $\mathbf{S} \to \mathbf{C}$ is an equivalence and that $\mathbf{S}$ is skeletal.

0.1.7 Natural transformations

Just as a functor is a map between categories, so there is a notion of a map between functors, called a *natural transformation*.

Definition 0.19 (Natural transformation, natural isomorphism)**.** Given functors $F\colon \mathbf{C} \to \mathbf{D}$ and $G\colon \mathbf{C} \to \mathbf{D}$, a *natural transformation* $\zeta\colon F \Rightarrow G$ is an assignment to every object A in $\mathbf{C}$ of a morphism $F(A) \xrightarrow{\zeta_A} G(A)$ in $\mathbf{D}$, such that the following diagram commutes for every morphism $A \xrightarrow{f} B$ in $\mathbf{C}$.

$$\begin{tikzcd} F(A) \arrow[r, "\zeta_A"] \arrow[d, "F(f)"'] & G(A) \arrow[d, "G(f)"] \\ F(B) \arrow[r, "\zeta_B"'] & G(B) \end{tikzcd} \tag{0.15}$$

If every component ζ_A is an isomorphism then ζ is called a *natural isomorphism*, and F and G are called *naturally isomorphic*.

Many important concepts in mathematics can be defined in a simple way using functors and natural transformations, such as the following.

Example 0.20. A *group representation* is a functor $\mathbf{G} \to \mathbf{Vect}$, where $\mathbf{G}$ is a group regarded as a category with one object (see Definition 0.11.) An *intertwiner* is a natural transformation between such functors.

The notion of natural isomorphism leads to another characterization of equivalence of categories.

Definition 0.21 (Equivalence by natural isomorphism)**.** A functor $F\colon \mathbf{C} \to \mathbf{D}$ is an *equivalence* if and only if there exists a functor $G\colon \mathbf{D} \to \mathbf{C}$ and natural isomorphisms $G \circ F \simeq \mathrm{id}_{\mathbf{C}}$ and $\mathrm{id}_D \simeq F \circ G$.

A functor is an equivalence by Definition 0.21 just when it is an equivalence by Definition 0.17, and so we abuse terminology mildly, using the word "equivalence" for both concepts. It is interesting to consider the difference between these definitions: while Definition 0.17 is written in terms of the internal structure of the categories involved, in the form of their objects and morphisms, Definition 0.21 is written in terms of their external context, given by the functors and natural transformations between them. This is a common dichotomy in category theory, with "internal" concepts often being more elementary and direct, while the associated "external" perspective, although making use of more sophisticated notions, is often more powerful and elegant. We revisit this external notion of equivalence in Chapter 8, from the perspective of higher category theory.

0.1.8 Limits

Limits are recipes for finding objects and morphisms with *universal properties*, with great practical use in category theory. We won't describe the general case here, but just the important special cases of products, equalizers, terminal objects, and their dual notions.

To get the idea, it is useful to think about the disjoint union $S + T$ of sets S and T. It is not just a bare set; it comes equipped with functions $S \xrightarrow{i_S} S + T$ and $T \xrightarrow{i_T} S + T$ that show how the individual sets embed into the disjoint union. And furthermore, these functions have a special property: a function $S + T \xrightarrow{f} U$ corresponds exactly to a pair of functions of types $S \xrightarrow{f_S} U$ and $T \xrightarrow{f_T} U$, such that $f \circ i_S = f_S$ and $f \circ i_T = f_T$. The concepts of limit and colimit generalize this observation.

We now define product and coproduct, and also terminal and initial object.

Definition 0.22 (Product, coproduct)**.** Given objects A and B, a *product* is an object $A \times B$ together with morphisms $A \times B \xrightarrow{p_A} A$ and $A \times B \xrightarrow{p_B} B$, such that any two morphisms $X \xrightarrow{f} A$ and $X \xrightarrow{g} B$ allow a unique morphism $\left(\begin{smallmatrix} f \\ g \end{smallmatrix}\right)\colon X \to A \times B$ with $p_A \circ \left(\begin{smallmatrix} f \\ g \end{smallmatrix}\right) = f$ and $p_B \circ \left(\begin{smallmatrix} f \\ g \end{smallmatrix}\right) = g$. The following diagram summarizes these relationships:

$$\begin{tikzcd} & X \arrow[dl, "f"'] \arrow[dr, "g"] \arrow[d, dashed, "\left(\begin{smallmatrix} f \\ g \end{smallmatrix}\right)"] & \\ A & A \times B \arrow[l, "p_A"] \arrow[r, "p_B"'] & B \end{tikzcd}$$

A *coproduct* is the dual notion, that reverses the directions of all the arrows in this diagram. Given objects A and B, a coproduct is an object $A + B$ equipped with morphisms $A \xrightarrow{i_A} A+B$ and $B \xrightarrow{i_B} A+B$, such that for any morphisms $A \xrightarrow{f} X$ and $B \xrightarrow{g} X$, there is a unique morphism $(\,f\ g\,)\colon A+B \to X$ such that $(\,f\ g\,) \circ i_A = f$ and $(\,f\ g\,) \circ i_B = g$.

Definition 0.23 (Terminal object, initial object)**.** An object A is *terminal* if for every object X, there is exactly one morphism $X \to A$. It is *initial* if for every object X, there is exactly one morphism $A \to X$.

A category may not have any of these structures, but if they exist, they are unique up to isomorphism.

Definition 0.24 (Cartesian category)**.** A category is *Cartesian* when it has a terminal object and products of any pair of objects.

These structures do exist in our main example categories.

Example 0.25. Products, coproducts, terminal objects and initial objects take the following forms in our main example categories:

- in $\mathbf{Set}$, products are given by the Cartesian product, and coproducts by the disjoint union, any 1-element set is a terminal object, and the empty set is the initial object;
- in $\mathbf{Rel}$, products and coproducts are both given by the disjoint union, and the empty set is both the terminal and initial object;

Given a pair of functions $S \xrightarrow{f,g} T$, it is interesting to ask on which elements of S they take the same value. Category theory dictates that we shouldn't ask about elements, but use morphisms to get the same information using a universal property. This leads to the notion of equalizer, a structure that may or may not exist in any particular category.

Definition 0.26. For morphisms $A \xrightarrow{f,g} B$, their *equalizer* is a morphism $E \xrightarrow{e} A$ satisfying $f \circ e = g \circ e$, such that any morphism $E' \xrightarrow{e'} A$ satisfying $f \circ e' = g \circ e'$ allows a unique $E' \xrightarrow{m} E$ with $e' = e \circ m$:

$$\begin{tikzcd} E \arrow[r, "e"] & A \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & B \\ E' \arrow[u, dashed, "m"] \arrow[ur, "e'"'] & & \end{tikzcd}$$

The *coequalizer* of f and g is their equalizer in the opposite category.

Example 0.27. Let's see what equalizers look like in our example categories.

- The categories **Set**, **Vect** and **Hilb** (see Section 0.2) have equalizers for all pairs of parallel morphisms. An equalizer for $A \xrightarrow{f,g} B$ is the set $E = \{a \in A \mid f(a) = g(a)\}$, equipped with its embedding $E \xrightarrow{e} A$; that is, it's the largest subset of A on which f and g agree.

- The category **Rel** does not have all equalizers. For example, consider the relation $R = \{(y,z) \in \mathbb{R}^2 \mid y < z \in \mathbb{R}\} \colon \mathbb{R} \to \mathbb{R}$. Suppose $E \colon X \to \mathbb{R}$ were an equalizer of R and $\mathrm{id}_{\mathbb{R}}$. Then $R \circ R = \mathrm{id}_{\mathbb{R}} \circ R$, so there is a relation $M \colon \mathbb{R} \to X$ with $R = E \circ M$. Now $E \circ (M \circ E) = (E \circ M) \circ E = R \circ E = \mathrm{id}_{\mathbb{R}} \circ E = E$, and since $S = \mathrm{id}_X$ is the unique morphism satisfying $E \circ S = E$, we must have $M \circ E = \mathrm{id}_X$. But then xEy and yMx for some $x \in X$ and $y \in \mathbb{R}$. It follows that $y(E \circ M)y$, that is, $y < y$, which is a contradiction.

A kernel is a special kind of equalizer.

Definition 0.28. A *kernel* of a morphism $A \xrightarrow{f} B$ is an equalizer of f and the *zero* morphism $A \xrightarrow{0} B$ (see Section 2.2.)

A last instance of universal properties is the idea of split idempotents.

Definition 0.29 (Idempotent, splitting)**.** An endomorphism $A \xrightarrow{f} A$ is called *idempotent* when $f \circ f = f$. An idempotent $A \xrightarrow{f} A$ *splits* when there exist an object $\widehat{f}$ and morphisms $A \xrightarrow{p_f} \widehat{f}$ and $\widehat{f} \xrightarrow{i_f} A$ such that the following hold:

$$i_f \circ p_f = f \tag{0.16}$$

$$p_f \circ i_f = \mathrm{id}_{\widehat{f}} \tag{0.17}$$

Given such a split idempotent, the injection $\widehat{f} \xrightarrow{i_f} A$ gives an equalizer of f and id_A, and the projection $A \xrightarrow{p_f} \widehat{f}$ gives a coequalizer of f and id_A.

0.2 Hilbert spaces

This section introduces the mathematical formalism that underlies quantum theory: (complex) vector spaces, inner products, and Hilbert spaces. We define the categories **Vect** and **Hilb**, and define basic concepts such as orthonormal bases, linear maps, matrices, dimensions and duals of Hilbert spaces. We then introduce the adjoint of a linear map between Hilbert spaces, and define the terms unitary, isometry, partial isometry, and positive. We also define the tensor product of Hilbert spaces, and introduce the Kronecker product of matrices.

0.2.1 Vector spaces

A vector space is a collection of elements that can be added to one another, and scaled.

Definition 0.30 (Vector space)**.** A *vector space* is a set V with a chosen element $0 \in V$, an addition operation $+\colon V \times V \to V$, and a scalar multiplication operation $\cdot\colon \mathbb{C} \times V \to V$, satisfying the following properties for all $a, b, c \in V$ and $s, t \in \mathbb{C}$:

- *additive associativity*: $a + (b + c) = (a + b) + c$;
- *additive commutativity*: $a + b = b + a$;
- *additive unit*: $a + 0 = a$;
- *additive inverses*: there exists a $-a \in V$ such that $a + (-a) = 0$;
- *additive distributivity*: $s \cdot (a + b) = (s \cdot a) + (s \cdot b)$
- *scalar unit*: $1 \cdot a = a$;
- *scalar distributivity*: $(s + t) \cdot a = (s \cdot a) + (t \cdot a)$;
- *scalar compatibility*: $s \cdot (t \cdot a) = (st) \cdot a$.

The prototypical example of a vector space is $\mathbb{C}^n$, the cartesian product of n copies of the complex numbers.

Definition 0.31 (Linear map, anti-linear map)**.** A *linear map* is a function $f\colon V \to W$ between vector spaces, with the following properties, for all $a, b \in V$ and $s \in \mathbb{C}$:

$$f(a + b) = f(a) + f(b) \tag{0.18}$$
$$f(s \cdot a) = s \cdot f(a) \tag{0.19}$$

An *anti-linear map* is a function that satisfies (0.18), but instead of (0.19), satisfies

$$f(s \cdot a) = s^* \cdot f(a), \tag{0.20}$$

where the star denotes complex conjugation.

Vector spaces and linear maps form a category.

Definition 0.32 (**Vect**, **FVect**)**.** In the category **Vect** of vector spaces and linear maps:

- **objects** are complex vector spaces;
- **morphisms** are linear functions;
- **composition** is composition of functions;
- **identity morphisms** are identity functions.

Write **FVect** for the restriction of **Vect** to those vector spaces that are isomorphic to $\mathbb{C}^n$ for some natural number n; these are also called *finite-dimensional*, see Definition 0.34 below.

Any morphism $f\colon V \to W$ in $\mathbf{Vect}$ has a kernel, namely the inclusion of $\ker(f) = \{v \in V \mid f(v) = 0\}$ into V. Hence kernels in the categorical sense coincide precisely with kernels in the sense of linear algebra.

Definition 0.33. The *direct sum* of vector spaces V and W is the vector space $V \oplus W$, whose elements are pairs (a, b) of elements $a \in V$ and $b \in W$, with entrywise addition and scalar multiplication.

Direct sums are both products and coproducts in the category $\mathbf{Vect}$. Similarly, the 0-dimensional space is both terminal and initial in $\mathbf{Vect}$.

0.2.2 Bases and matrices

One of the most important structures a vector space can have is a *basis*. A basis give rise to the notion of dimension of a vector space, and lets us represent linear maps using matrices.

Definition 0.34 (Basis). For a vector space V, a family of elements $\{e_i\}$ is *linearly independent* when every element $a \in V$ can be expressed as a finite linear combination $a = \sum_i a_i e_i$ with *coefficients* $a_i \in \mathbb{C}$ in at most one way. It is a *basis* if additionally any $a \in V$ can be expressed as such a finite linear combination.

Every vector space admits a basis, and any two bases for the same vector space have the same cardinality. This is not quite trivial to see.

Definition 0.35 (Dimension, finite-dimensionality). The *dimension* of a vector space V, written $\dim(V)$, is the cardinality of any basis. A vector space is *finite-dimensional* when it has a finite basis.

If vector spaces V and W have bases $\{d_i\}$ and $\{e_j\}$, and we fix some order on the bases, we can represent a linear map $V \xrightarrow{f} W$ as the matrix with $\dim(W)$ rows and $\dim(V)$ columns, whose entry at row i and column j is the coefficient $f(d_j)_i$. Composition of linear maps then corresponds to matrix multiplication (0.7). This directly leads to a category.

Definition 0.36 ($\mathbf{Mat}_{\mathbb{C}}$). In the skeletal category $\mathbf{Mat}_{\mathbb{C}}$:

- **objects** are natural numbers $0, 1, 2, \ldots$;
- **morphisms** $n \to m$ are complex matrices with m rows and n columns;
- **composition** is given by matrix multiplication;
- **identities** $n \xrightarrow{\mathrm{id}_n} n$ are given by n-by-n matrices with entries 1 on the main diagonal, and 0 elsewhere.

This theory of matrices is 'just as good' as the theory of finite-dimensional vector spaces, made precise by the category theory developed in Section 0.1.

Proposition 0.37. *There is an equivalence of categories* $\mathbf{Mat}_{\mathbb{C}} \to \mathbf{FVect}$ *that sends* n *to* $\mathbb{C}^n$ *and a matrix to its associated linear map.*

Proof. Because every finite-dimensional complex vector space H is isomorphic to $\mathbb{C}^{\dim(H)}$, the functor R is essentially surjective on objects. It is full and faithful since there is an exact correspondence between matrices and linear maps for finite-dimensional vector spaces. □

For square matrices, the trace is an important operation.

Definition 0.38 (Trace)**.** For a square matrix with entries m_{ij}, its *trace* is the sum $\sum_i m_{ii}$ of its diagonal entries.

0.2.3 Hilbert spaces

Hilbert spaces are structures that are built on vector spaces. The extra structure lets us define angles and distances between vectors, and is used in quantum theory to calculate probabilities of measurement outcomes.

Definition 0.39 (Inner product)**.** An *inner product* on a complex vector space V is a function $\langle - | - \rangle \colon V \times V \to \mathbb{C}$ that is:

- *conjugate-symmetric*: for all $a, b \in V$,

$$\langle a|b\rangle = \langle b|a\rangle^*; \tag{0.21}$$

- *linear* in the second argument: for all $a, b, c \in V$ and $s \in \mathbb{C}$,

$$\langle a|s \cdot b\rangle = s \cdot \langle a|b\rangle, \tag{0.22}$$

$$\langle a|b + c\rangle = \langle a|b\rangle + \langle a|c\rangle; \tag{0.23}$$

- *positive definite*: for all $a \in V$,

$$\langle a|a\rangle \geq 0, \tag{0.24}$$

$$\langle a|a\rangle = 0 \Rightarrow v = 0. \tag{0.25}$$

Definition 0.40 (Norm)**.** For a vector space with inner product, the *norm* of an element v is $\|v\| = \sqrt{\langle v|v\rangle}$, a nonnegative real number.

The complex numbers carry a canonical inner product:

$$\langle s|t\rangle = s^* t \tag{0.26}$$

The induced norm satisfies the triangle inequality $\|a + b\| \leq \|a\| + \|b\|$ by virtue of the Cauchy-Schwarz inequality $|\langle a|b\rangle|^2 \leq \langle a|a\rangle \cdot \langle b|b\rangle$, that holds in any vector space with an inner product. Thanks to these properties, it makes sense to think of $\|a - b\|$ as the distance between vectors a and b.

A Hilbert space is an inner product space in which it makes sense to add infinitely many vectors in certain cases.

Definition 0.41 (Hilbert space)**.** A *Hilbert space* is a vector space H with an inner product that is *complete* in the following sense: if a sequence $v_1, v_2, \ldots$ of vectors satisfies $\sum_{i=1}^{\infty} \|v_i\| < \infty$, then there is a vector v such that $\|v - \sum_{i=1}^{n} v_i\|$ tends to zero as n goes to infinity.

Every finite-dimensional vector space with inner product is necessarily complete. Any vector space with an inner product can be completed to a Hilbert space by formally adding the appropriate limit vectors.

There is a notion of bounded map between Hilbert spaces that makes use of the inner product structure. The idea is that for each map there is some maximum amount by which the norm of a vector can increase.

Definition 0.42 (Bounded linear map)**.** A linear map $f\colon H \to K$ between Hilbert spaces is *bounded* when there exists a number $r \in \mathbb{R}$ such that $\|f(a)\| \le r \cdot \|a\|$ for all $a \in H$.

Every linear map between finite-dimensional Hilbert spaces is bounded.

Hilbert spaces and bounded linear maps form a category. This category will be the main example throughout the book to model phenomena in quantum theory.

Definition 0.43 (**Hilb**, **FHilb**)**.** In the category **Hilb** of Hilbert spaces and bounded linear maps:

- **objects** are Hilbert spaces;
- **morphisms** are bounded linear maps;
- **composition** is composition of linear maps as ordinary functions;
- **identity morphisms** are given by the identity linear maps.

Write **FHilb** for the restriction of **Hilb** to finite-dimensional Hilbert spaces.

This definition is perhaps surprising, especially in finite dimensions: since every linear map between Hilbert spaces is bounded, **FHilb** is an equivalent category to **FVect**. In particular, the inner products play no essential role. We will see in Section 2.3 how to model inner products categorically, using the idea of *daggers*.

Hilbert spaces have a more discerning notion of basis.

Definition 0.44 (Basis, orthogonal basis, orthonormal basis)**.** For a Hilbert space H, an *orthogonal basis* is a family of elements $\{e_i\}$ with the following properties:

- they are *pairwise orthogonal*, *i.e.* $\langle e_i | e_j \rangle = 0$ for all $i \neq j$;
- every element $a \in H$ can be written as an infinite linear combination of e_i; *i.e.* there are *coefficients* $a_i \in \mathbb{C}$ for which $\|a - \sum_{i=1}^{n} a_i e_i\|$ tends to zero as n goes to infinity.

It is *orthonormal* when additionally $\langle e_i | e_i \rangle = 1$ for all i.

Any orthogonal family of elements is linearly independent. For finite-dimensional Hilbert spaces, the ordinary notion of basis as a vector space, as given by Definition 0.34, is still useful. Hence once we fix (ordered) bases on finite-dimensional Hilbert spaces, linear maps between them correspond to matrices, just as with vector spaces. For infinite-dimensional Hilbert spaces, however, having a basis for the underlying vector space is rarely mathematically useful.

If two vector spaces carry inner products, we can give an inner product to their direct sum, leading to the direct sum of Hilbert spaces.

Definition 0.45 (Direct sum)**.** The *direct sum* of Hilbert spaces H and K is the vector space $H \oplus K$, made into a Hilbert space by the inner product $\langle (a_1, b_1) | (a_2, b_2) \rangle = \langle a_1 | a_2 \rangle + \langle b_1 | b_2 \rangle$.

Direct sums provide both products and coproducts for the category **Hilb**. Hilbert spaces have the good property that any closed subspace can be complemented. That is, if the inclusion $U \hookrightarrow V$ is a morphism of **Hilb** satisfying $\|u\|_U = \|u\|_H$, then there exists another inclusion morphism $U^\perp \hookrightarrow V$ of **Hilb** with $V = U \oplus U^\perp$. Explicitly, $U^\perp$ is the *orthogonal subspace* $\{a \in V \mid \forall b \in U \colon \langle a|b \rangle = 0\}$.

0.2.4 Adjoint linear maps

The inner product gives rise to the *adjoint* of a bounded linear map.

Definition 0.46. For a bounded linear map $f \colon H \to K$, its *adjoint* $f^\dagger \colon K \to H$ is the unique linear map with the following property, for all $a \in H$ and $b \in K$:

$$\langle f(a) | b \rangle = \langle a | f^\dagger(b) \rangle. \tag{0.27}$$

The existence of the adjoint follows from the Riesz representation theorem for Hilbert spaces, which we do not cover here. It follows immediately from (0.27) by uniqueness of adjoints that they also satisfy the following properties:

$$(f^\dagger)^\dagger = f, \tag{0.28}$$
$$(g \circ f)^\dagger = f^\dagger \circ g^\dagger, \tag{0.29}$$
$$\mathrm{id}_H{}^\dagger = \mathrm{id}_H. \tag{0.30}$$

Taking adjoints is an anti-linear operation.

Adjoints give rise to various specialized classes of linear maps.

Definition 0.47. A bounded linear map $H \xrightarrow{f} K$ between Hilbert spaces is:

- *self-adjoint* when $f = f^\dagger$;
- a *projection* when $f = f^\dagger$ and $f \circ f = f$;
- *unitary* when both $f^\dagger \circ f = \mathrm{id}_H$ and $f \circ f^\dagger = \mathrm{id}_K$;

- an *isometry* when $f^\dagger \circ f = \mathrm{id}_H$;
- a *partial isometry* when $f^\dagger \circ f$ is a projection;
- and *positive* when $f = g^\dagger \circ g$ for some bounded linear map $H \xrightarrow{g} K$.

The following notation is standard in the physics literature.

Definition 0.48 (Bra, ket)**.** Given an element $a \in H$ of a Hilbert space, its *ket* $\mathbb{C} \xrightarrow{|a\rangle} H$ is the linear map $s \mapsto sa$. Its *bra* $H \xrightarrow{\langle a|} \mathbb{C}$ is the linear map $b \mapsto \langle a|b\rangle$.

You can check that $|a\rangle^\dagger = \langle a|$:

$$\left(\mathbb{C} \xrightarrow{|a\rangle} H \xrightarrow{\langle b|} \mathbb{C}\right) = \left(\mathbb{C} \xrightarrow{\langle b|\circ|a\rangle} \mathbb{C}\right) = \left(\mathbb{C} \xrightarrow{\langle b|a\rangle} \mathbb{C}\right) \tag{0.31}$$

The final expression identifies the number $\langle b|a\rangle$ with the linear map $1 \mapsto \langle b|a\rangle$. Thus the inner product (or 'bra-ket') $\langle b|a\rangle$ decomposes into a $\langle b|$ and a ket $|a\rangle$. Originally due to Paul Dirac, this is traditionally called *Dirac notation*.

The correspondence between $|a\rangle$ and $\langle a|$ leads to the notion of a dual space.

Definition 0.49. For a Hilbert space H, its *dual Hilbert space* H^* is the vector space $\mathbf{Hilb}(H, \mathbb{C})$.

A Hilbert space is isomorphic to its dual in an anti-linear way: the map $H \to H^*$ given by $|a\rangle \mapsto \varphi_a = \langle a|$ is an invertible anti-linear function. The inner product on H^* is given by $\langle \varphi_a|\varphi_b\rangle_{H^*} = \langle a|b\rangle_H$, and makes the function $|a\rangle \mapsto \langle a|$ bounded.

Some bounded linear maps support a notion of trace.

Definition 0.50 (Trace, trace class)**.** When it converges, the *trace* of a positive linear map $f\colon H \to H$ is given by $\mathrm{Tr}(f) = \sum \langle e_i|f(e_i)\rangle$ for any orthonormal basis $\{e_i\}$, in which case the map is called *trace class*.

If the sum converges for one orthonormal basis, then with effort you can prove that it converges for all orthonormal bases, and that the trace is independent of the chosen basis. In the finite-dimensional case, the trace defined in this way agrees with the matrix trace of Definition 0.38.

0.2.5 Tensor products

The tensor product is a way to make a new vector space out of two given ones. With some work the tensor product can be constructed explicitly, but it is only important for us that it exists, and is defined up to isomorphism by a universal property. If U, V and W are vector spaces, a function $f\colon U \times V \to W$ is called *bilinear* when it is linear in each variable; that is, when the function $u \mapsto f(u, v)$ is linear for each $v \in V$, and the function $v \mapsto f(u, v)$ is linear for each $u \in U$.

Definition 0.51. The *tensor product of vector spaces* U and V is a vector space $U \otimes V$ together with a bilinear function $f\colon U \times V \to U \otimes V$ such that for every bilinear function $g\colon U \times V \to W$ there exists a unique linear function $h\colon U \otimes V \to W$ such that $g = h \circ f$.

$$\begin{tikzcd}
U \times V \arrow[r, "\text{(bilinear) } f"] \arrow[dr, "\text{(bilinear) } g"'] & U \otimes V \arrow[d, dashed, "h \text{ (linear)}"] \\
& W
\end{tikzcd}$$

Note that $U \times V$ is not itself a vector space, so it doesn't make sense to ask if f or g are linear. The function f usually stays anonymous and is written as $(a, b) \mapsto a \otimes b$. It follows that arbitrary elements of $U \otimes V$ take the form $\sum_{i=1}^{n} s_i a_i \otimes b_i$ for $s_i \in \mathbb{C}$, $a_i \in U$, and $b_i \in V$. The tensor product also extends to linear maps. If $f_1\colon U_1 \to V_1$ and $f_2\colon U_2 \to V_2$ are linear maps, there is a unique linear map $f_1 \otimes f_2\colon U_1 \otimes U_2 \to V_1 \otimes V_2$ that satisfies $(f_1 \otimes f_2)(a_1 \otimes a_2) = f_1(a_1) \otimes f_2(a_2)$ for $a_1 \in U_1$ and $a_2 \in U_2$. In this way, the tensor product becomes a functor $\otimes\colon \mathbf{Vect} \times \mathbf{Vect} \to \mathbf{Vect}$.

Definition 0.52. The *tensor product of Hilbert spaces* H and K is the Hilbert space $H \otimes K$ built by taking tensor product of the underlying vector spaces, giving it the inner product $\langle a_1 \otimes b_1 | a_2 \otimes b_2 \rangle = \langle a_1 | a_2 \rangle_H \cdot \langle b_1 | b_2 \rangle_K$, then completing it. If $H \xrightarrow{f} H'$ and $K \xrightarrow{g} K'$ are bounded linear maps, then so is the continuous extension of the tensor product of linear maps to a function that we again call $f \otimes g\colon H \otimes K \to H' \otimes K'$. This gives a functor $\otimes\colon \mathbf{Hilb} \times \mathbf{Hilb} \to \mathbf{Hilb}$.

If $\{e_i\}$ is an orthonormal basis for Hilbert space H, and $\{f_j\}$ is an orthonormal basis for K, then $\{e_i \otimes f_j\}$ is an orthonormal basis for $H \otimes K$. So when H and K are finite-dimensional, there is no difference between their tensor products as vector spaces and as Hilbert spaces.

Definition 0.53 (Kronecker product)**.** When finite-dimensional Hilbert spaces H_1, H_2, K_1, K_2 are equipped with fixed ordered orthonormal bases, linear maps $H_1 \xrightarrow{f} K_1$ and $H_2 \xrightarrow{g} K_2$ can be written as matrices. Their tensor product $H_1 \otimes H_2 \xrightarrow{f \otimes g} K_1 \otimes K_2$ corresponds to the following block matrix, called their *Kronecker product*:

$$(f \otimes g) := \begin{pmatrix} (f_{11}g) & (f_{12}g) & \cdots & (f_{1n}g) \\ (f_{21}g) & (f_{22}g) & \ldots & (f_{2n}g) \\ \vdots & \vdots & \ddots & \vdots \\ (f_{m1}g) & (f_{m2}g) & \ldots & (f_{mn}g) \end{pmatrix}. \tag{0.32}$$

0.3 Quantum information

Quantum information theory studies the information processing capabilities of quantum systems, using the mathematical abstractions of Hilbert spaces and linear maps.

0.3.1 State spaces

Classical computer science often considers systems to have a finite set of states. An important simple system is the *bit*, with state space given by the set $\{0, 1\}$. Quantum information theory instead assumes that systems have state spaces given by finite-dimensional Hilbert spaces. The quantum version of the bit is the qubit.

Definition 0.54. A *qubit* is a quantum system with state space $\mathbb{C}^2$.

A *pure state* of a quantum system is given by a vector $v \in H$ in its associated Hilbert space. Such a state is *normalized* when the vector in the Hilbert space has norm 1:

$$\langle a|a\rangle = 1 \tag{0.33}$$

In particular, a complex number of norm 1 is called a phase. A pure state of a qubit is therefore a vector of the form

$$a = \begin{pmatrix} s \\ t \end{pmatrix}$$

with $s, t \in \mathbb{C}$, which is normalized when $|s|^2 + |t|^2 = 1$. In Section 0.3.4 we will encounter a more general notion of state, called a mixed state. However, when our meaning is clear, we'll often just say *state* instead of pure state.

When performing computations in quantum information, we often use the following privileged basis.

Definition 0.55 (Computational basis, Z basis)**.** For the Hilbert space $\mathbb{C}^n$, the *computational basis*, or *Z basis* is the orthonormal basis given by the following vectors:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \qquad \cdots \qquad |n-1\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \tag{0.34}$$

This orthonormal basis is no better than any other, but it is useful to fix a standard choice. Every state $a \in \mathbb{C}^n$ can be written in terms of the computational basis; for a qubit, we can write $a = s|0\rangle + t|1\rangle$ for some $s, t \in \mathbb{C}$. The following alternative qubit basis also plays an important role.

Definition 0.56. The *X basis* for a qubit $\mathbb{C}^2$ is given by the following states:

$$|+\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|-\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Processing quantum information takes place by applying unitary maps $H \xrightarrow{f} H$ to the Hilbert space of states. Such a map will take a normalized state $a \in H$ to a normalized state $f(a) \in H$. An example of a unitary map is the *X gate* represented by the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, which acts as $|0\rangle \mapsto |1\rangle$ and $|1\rangle \mapsto |0\rangle$ on the computational basis states of a qubit.

0.3.2 Compound systems and entanglement

Given two quantum systems with state spaces given independently by Hilbert spaces H and K, as a joint system their overall state space is $H \otimes K$, the tensor product of the two Hilbert spaces (see Section 0.2.5). This is a postulate of quantum theory. As a result, state spaces of quantum systems grow large very rapidly: a collection of n qubits will have a state space isomorphic to $\mathbb{C}^{2^n}$, requiring 2^n complex numbers to specify its state vector exactly. In contrast, a classical system consisting of n bits can have its state specified by a single binary number of length n.

In quantum theory, (pure) product states and (pure) entangled states are defined as follows.

Definition 0.57 (Product state, entangled state)**.** For a compound system with state space $H \otimes K$, a *product state* is a state of the form $a \otimes b$ with $a \in H$ and $b \in K$. An *entangled state* is a state not of this form.

The definition of product and entangled state also generalizes to systems with more than two components. When using Dirac notation, if $|a\rangle \in H$ and $|b\rangle \in K$ are chosen states, we will often write $|ab\rangle$ for their product state $|a\rangle \otimes |b\rangle$.

The following family of entangled states plays an important role in quantum information theory.

Definition 0.58 (Bell state)**.** The *Bell basis* for a pair of qubits with state space $\mathbb{C}^2 \otimes \mathbb{C}^2$ is the orthonormal basis given by the following states:

$$\begin{aligned}
|\text{Bell}_0\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\\
|\text{Bell}_1\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle)\\
|\text{Bell}_2\rangle &= \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle)\\
|\text{Bell}_3\rangle &= \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
\end{aligned}$$

The state $|\text{Bell}_0\rangle$ is often called 'the Bell state', and is very prominent in quantum information. The Bell states are *maximally entangled*, meaning that they induce an extremely strong correlation between the two systems involved (see Definition 0.72 below).

0.3.3 Pure states and measurements

For a quantum system in a pure state, the most basic notion of measurement is a *projection-valued measure*. Quantum theory is a set of rules that says what happens to the quantum state when a projection-valued measurement takes place, and the probabilities of the different outcomes. Recall from Definition 0.47 that projections are maps satisfying $p = p^\dagger = p \circ p$.

Definition 0.59. A finite family of linear maps $H \xrightarrow{f_i} H$ is *complete* when the following holds:

$$\sum_i f_i = \text{id}_H \tag{0.35}$$

Definition 0.60. A family of linear maps $H \xrightarrow{f_i} H$ is *orthogonal* when for any $i \neq j$, the following holds:

$$f_i \circ f_j = 0 \tag{0.36}$$

Definition 0.61 (Projection-valued measure, nondegenerate)**.** A *projection-valued measure (PVM)* on a Hilbert space H is a finite family of projections $H \xrightarrow{p_i} H$ which are complete and orthogonal. A PVM is *nondegenerate* when $\mathrm{Tr}(p_i) = 1$ for all i.

In this definition of PVM, the orthogonality property is actually redundant; that is, a complete family of projections is necessarily also orthogonal. For simplicity, however, we include the orthogonality requirement here directly. Also note that while our PVMs are finite, in general infinite PVMs are possible; for simplicity, we focus on the finite case.

Lemma 0.62. *For a finite-dimensional Hilbert space, nondegenerate projection-valued measures correspond to orthonormal bases, up to phase.*

Proof. For an orthonormal basis $|i\rangle$, define a nondegenerate PVM by $p_i = |i\rangle\langle i|$. Conversely, since projections p have eigenvalues 1, if $\mathrm{Tr}(p) = 1$ then p must have rank one, too. That is, there is a ket $|i\rangle$ such that $p = |i\rangle\langle i|$, unique up to multiplication by a complex phase $e^{i\theta}$. $\square$

A projection-valued measure, when applied to a Hilbert space, will have a unique outcome, given by one of the projections. This outcome will be probabilistic, with distribution described by the Born rule, defined below. Dirac notation is often extended to self-adjoint bounded linear functions $H \xrightarrow{f} K$ between Hilbert spaces, writing $\langle a|f|b\rangle$ for $\langle a|f(b)\rangle = \langle f(a)|b\rangle$.

Definition 0.63 (Born rule)**.** For a projection-valued measure $\{p_i\}$ on a system in a normalized state $a \in H$, the *probability of outcome* i is $\langle a|p_i|a\rangle$.

The definition of a projection-valued measure guarantees that the total probability across all outcomes is 1:

$$\textstyle\sum_i \langle a|p_i|a\rangle \overset{(0.18)}{=} \langle a|(\sum_i p_i)|a\rangle \overset{(0.35)}{=} \langle a|a\rangle \overset{(0.33)}{=} 1 \tag{0.37}$$

After a measurement, the new state of the system is $p_i(a)$, where p_i is the projection corresponding to the outcome that occured. This part of the standard interpretation is called the *projection postulate*. Note that this new state is not necessarily normalized. If the new state is not zero, it can be normalized in a canonical way, giving $p_i(a)/\|p_i(a)\|$.

Given some classical information and some quantum information, it is often the case that we want to apply a unitary operator to the quantum information, in a way that depends on the classical information.

Definition 0.64 (Controlled operation)**.** Given a Hilbert space H and a set S, a *controlled operation* is a choice for all $s \in S$ of a unitary $U_s \colon H \to H$.

0.3.4 Mixed states and measurements

Suppose there is a machine that produces a quantum system with Hilbert space H. The machine has two buttons: one that will produce the system in state $a \in H$, and another that will produce it in state $b \in H$. You receive the system that the machine produces, but you cannot see it operating; all you know is that the operator of the machine flips a fair coin to decide which button to press. Taking into account this uncertainty, the state of the system that you receive cannot be described by an element of H; the system is in a more general type of state, called a *mixed state*.

Definition 0.65 (Density matrix, normalized)**.** A *density matrix* on a Hilbert space H is a positive map $H \xrightarrow{m} H$. A density matrix is *normalized* when $\mathrm{Tr}(m) = 1$. (Warning: a density matrix is not a matrix in the sense of Definition 0.36.)

Recall from Definition 0.47 that m is positive when there exists some g with $m = g^\dagger \circ g$. Density matrices are more general than pure states, since every pure state $a \in H$ gives rise to a density matrix $m = |a\rangle\langle a|$ in a canonical way. This last piece of Dirac notation is the projection onto the line spanned by the vector a.

Definition 0.66 (Pure state, mixed state)**.** A density matrix $m \colon H \to H$ is *pure* when $m = |a\rangle\langle a|$ for some $a \in H$; generally, it is *mixed*.

Definition 0.67 (Maximally mixed state)**.** For a finite-dimensional Hilbert space H, the *maximally mixed state* is the density matrix $\frac{1}{\dim(H)} \cdot \mathrm{id}_H$.

There is a notion of convex combination of density matrices, which corresponds physically to the idea of probabilistic choice between alternative states.

Definition 0.68 (Convex combination)**.** For nonnegative real numbers s, t with $s + t = 1$, the *convex combination* of matrices $H \xrightarrow{m,n} H$ is the matrix $H \xrightarrow{s \cdot m + t \cdot n} H$.

It can be shown that the convex combination of two density matrices is again a density matrix. The density matrix $s \cdot m + t \cdot n$ describes the state of a system produced by a machine that promises to output state m with probability s, and state n with probability t. In finite dimension, it turns out that every mixed state can be produced as a convex combination of some number of pure states, which are not unique, and that the convex combination of distinct density matrices is always a mixed state.

There is a standard notion of measurement that generalizes the projection-valued measure in the same way that mixed states generalize pure states.

Definition 0.69. A *positive operator-valued measure (POVM)* on a Hilbert space H is a family of positive maps $H \xrightarrow{f_i} H$ satisfying

$$\sum_i f_i = \mathrm{id}_H. \tag{0.38}$$

Every projection-valued measure $\{p_i\}$ gives rise to a positive operator–valued measure in a canonical way, by choosing $f_i = p_i$.

The outcome of a positive operator-valued measurement is governed by a generalization of the Born rule.

Definition 0.70 (Born rule for POVMs)**.** For a positive operator-valued measure $\{f_i\}$ on a system with normalized density matrix $H \xrightarrow{m} H$, the *probability of outcome* i is $\mathrm{Tr}(f_i\, m)$.

A density matrix on a Hilbert space $H \otimes K$ can be modified to obtain a density matrix on H alone.

Proposition 0.71 (Partial trace)**.** *For Hilbert spaces H and K, there is a unique linear map* $\mathrm{Tr}_K \colon \mathbf{Hilb}(H \otimes K, H \otimes K) \to \mathbf{Hilb}(H, H)$ *satisfying* $\mathrm{Tr}_K(m \otimes n) = \mathrm{Tr}(n) \cdot m$*. It is called the* partial trace over K.

Explicitly, the partial trace of $H \otimes K \xrightarrow{f} H \otimes K$ is computed as follows, using any orthonormal basis $\{|i\rangle\}$ for K:

$$\mathrm{Tr}_K(f) = \textstyle\sum_i (\mathrm{id}_H \otimes \langle i|) \circ f \circ (\mathrm{id}_H \otimes |i\rangle). \tag{0.39}$$

Physically, this corresponds to discarding the subsystem K and retaining only the part with Hilbert space H.

Partial traces give rise to a definition of maximally entangled state.

Definition 0.72. A pure state $a \in H \otimes K$ is *maximally entangled* when tracing out either H or K from $|a\rangle\langle a|$ gives a maximally mixed state; explicitly this means the following, for some $s, t \in \mathbb{C}$:

$$\mathrm{Tr}_H(|a\rangle\langle a|) = s \cdot \mathrm{id}_K \qquad\qquad \mathrm{Tr}_K(|a\rangle\langle a|) = t \cdot \mathrm{id}_H \tag{0.40}$$

When $|a\rangle$ is normalized, its trace will be a normalized density matrix, so $s = 1/\dim(H)$ and $t = 1/\dim(K)$.

Up to unitary equivalence there is only one maximally entangled state for each system, as the following lemma shows; its proof will follow from Theorem 3.50.

Lemma 0.73. *Any two maximally entangled states $a, b \in H \otimes K$ are related by* $(f \otimes \mathrm{id}_K)(a) = b$ *for a unique unitary* $H \xrightarrow{f} H$. □

0.3.5 Decoherence

By Lemma 0.62, every nondegenerate projection-valued measure $\{p_1, \ldots, p_n\}$ on a Hilbert space H corresponds (up to a phase) to an orthonormal basis $\{|1\rangle, \ldots, |n\rangle\}$ for H via $p_i = |i\rangle\langle i|$, and hence induces n pure states of H. We may regard this as a *controlled preparation*: depending on some classical data $i = 1, \ldots, n$, we prepare state $|i\rangle$. Consider how this controlled preparation composes with a measurement in the same basis.

If we start with some classical information, use it to prepare a quantum system, and then immediately measure, we should end up with the same classical information we started with. Indeed, according to the Born rule of Definition 0.63, the probability of getting outcome j after preparing state i is:

$$\langle j|p_i|j\rangle = \langle j|i\rangle\langle i|j\rangle = |\langle i|j\rangle|^2, \tag{0.41}$$

which is 1 for $i = j$ but 0 for $i \neq j$.

The other way around is conceptually less straightforward: if you measure a quantum system, yielding a piece of classical data, and then immediately use that to prepare a state of a quantum system, what do you get? Well, supposing that the quantum system starts in a mixed state given by a density matrix $H \xrightarrow{m} H$ with $m = \sum_{ij} c_{ij}|i\rangle\langle j|$, the measurement results in outcome $|i\rangle$ with probability $\mathrm{Tr}(p_i m) = \langle i|m|i\rangle$, so the state eventually prepared is

$$\sum_i c_{ii}|i\rangle\langle i|. \tag{0.42}$$

The nondiagonal elements of the density matrix m have vanished, and the mixed state has become a convex combination of pure states that no longer cohere. This process is called *decoherence*. Any quantum state undergoes decoherence constantly as it interacts with its environment. It takes extremely good experimental control to keep a quantum state from decohering rapidly.

0.3.6 Quantum teleportation

Quantum teleportation is a beautiful and simple procedure, which demonstrates some of the counterintuitive properties of quantum information. It involves two agents, Alice and Bob. Alice has a qubit, which she would like to give to Bob without changing its quantum state, but she is limited to sending classical information only. Assume that Alice and Bob share a maximally entangled state, say the Bell state.

Definition 0.74 (Teleportation of a qubit)**.** The procedure is as follows.

1. Alice prepares her initial qubit I which she would like to teleport to Bob.

2. Alice and Bob share a pair of maximally entangled qubits, in the Bell state $|\mathrm{Bell}_0\rangle$. We write A for Alice's qubit and B for Bob's qubit.

3. Alice measures the system $I \otimes A$ in the Bell basis (see Definition 0.58.)

4. Alice communicates the result of the measurement to Bob as classical information.

5. Bob applies one of the following unitaries f_i to his qubit B, depending on which Bell state $|\mathrm{Bell}_i\rangle$ was measured by Alice:

$$f_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad f_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad f_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad f_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{0.43}$$

At the end of the procedure, Bob's qubit B is guaranteed to be in the same state in which I was at the beginning. Furthermore, the measurement result that Alice obtains by itself gives no information about the state that Alice is trying to teleport; each possible value has an equal probability.

At first quantum teleportation seems counterintuitive – impossible, even – given basic knowledge of the principles of quantum information: the state of a qubit is a vector in $\mathbb{C}^2$, requiring an infinite amount of classical information to specify, yet in quantum teleportation only 2 classical bits are transferred from Alice to Bob. Nonetheless, the procedure is correct.

As high-level categorical techniques are introduced throughout the book, we will revisit quantum teleportation time and again, seeing it in a new light each time, and gaining further insight into 'why it works'.

Notes and further reading

Categories arose in algebraic topology and homological algebra in the 1940s. They were first defined by Eilenberg and Mac Lane in 1945. Early uses of categories were mostly as a convenient language. With applications by Grothendieck in algebraic geometry in the 1950s, and by Lawvere in logic in the 1960s, category theory became an autonomous field of research. It has developed rapidly since then, with applications in computer science, physics, linguistics, cognitive science, philosophy, and many other areas. Good first textbooks are [9, 101, 103, 124]; excellent advanced textbooks are [107, 27]. The counterexample in Example 0.27 is due to Koslowski [109, 8.16].

Abstract vector spaces as generalizations of Euclidean space had been gaining traction for a while by 1900. Two parallel developments in mathematics in the 1900s led to the introduction of Hilbert spaces: the work of Hilbert and Schmidt on integral equations, and the development of the Lebesgue integral. The following two decades saw the realization that Hilbert spaces offer one of the best mathematical formulations of quantum mechanics. The first axiomatic treatment was given by von Neumann in 1929, who also coined the name Hilbert space. Although they have many deep uses in mathematics, Hilbert spaces have always had close ties to physics. For a rigorous textbook with a physical motivation, see [123].

Quantum information theory is a special branch of quantum mechanics that became popular around 1980 with the realization that entanglement can be used as a resource rather than a paradox. It has grown into a large area of study since. For a good introduction, read [91]. The quantum teleportation protocol was discovered in 1993 by Bennett, Brassard, Crépeau, Jozsa, Peres, and Wootters [24], and has been performed experimentally many times since, on land, overseas, and in space [28]. As described above, this fundamental procedure is quite elementary and only uses simple techniques, but it took decades to regard the counterintuitive nature of entanglement as a feature to be exploited.

Chapter 1

Monoidal categories

A monoidal category is a category equipped with extra data, describing how objects and morphisms can be combined 'in parallel'. This chapter introduces the theory of monoidal categories, and shows how our example categories $\mathbf{Hilb}$, $\mathbf{Set}$ and $\mathbf{Rel}$ can be given a monoidal structure, in Section 1.1. We also introduce a visual notation called the graphical calculus, which provides an intuitive and powerful way to work with them. The barest graphical calculus is two-dimensional, but this dimension goes up if we allow symmetry, which we discuss in Section 1.2. The correctness of the graphical calculus is based on coherence theorems, which we prove in Section 1.3.

1.1 Monoidal structure

Throughout this book, we interpret objects of categories as systems, and morphisms as processes. A monoidal category has additional structure allowing us to consider processes occurring *in parallel*, as well as sequentially. In terms of the example categories given in Section 0.1, one could interpret this in the following ways:

- letting independent physical systems evolve simultaneously;
- running computer algorithms in parallel;
- taking products or sums of algebraic or geometric structures;
- using separate proofs of P and Q to construct a proof of the conjunction (P and Q).

It is perhaps surprising that a nontrivial theory can be developed at all from such simple intuition. But in fact, some interesting general issues quickly arise. For example, let A, B and C be processes, and write $\otimes$ for the parallel composition. Then what relationship should there be between the processes $(A \otimes B) \otimes C$ and $A \otimes (B \otimes C)$? You might say they should be equal, as they are different ways of expressing the same arrangement of systems. But for many applications this is simply too strong: for example, if A, B and C are Hilbert spaces and $\otimes$ is the usual tensor product of Hilbert spaces, these two composite Hilbert spaces are *not* exactly equal; they are only isomorphic. But we then have a new problem: what equations should these isomorphisms satisfy? The theory of monoidal categories is formulated to deal with these issues.

Definition 1.1. A *monoidal category* is a category $\mathbf{C}$ equipped with the following data:

- a *tensor product* functor $\otimes \colon \mathbf{C} \times \mathbf{C} \to \mathbf{C}$;
- a *unit object* $I \in \mathrm{Ob}(\mathbf{C})$;
- an *associator* natural isomorphism $(A \otimes B) \otimes C \xrightarrow{\alpha_{A,B,C}} A \otimes (B \otimes C)$;
- a *left unitor* natural isomorphism $I \otimes A \xrightarrow{\lambda_A} A$;
- a *right unitor* natural isomorphism $A \otimes I \xrightarrow{\rho_A} A$.

This data must satisfy the *triangle* and *pentagon* equations, for all objects A, B, C and D:

$$\begin{tikzcd}
(A \otimes I) \otimes B \arrow[rr, "\alpha_{A,I,B}"] \arrow[dr, "\rho_A \otimes \mathrm{id}_B"'] & & A \otimes (I \otimes B) \arrow[dl, "\mathrm{id}_A \otimes \lambda_B"] \\
& A \otimes B &
\end{tikzcd} \tag{1.1}$$

$$\begin{tikzcd}
& \big(A \otimes (B \otimes C)\big) \otimes D \arrow[r, "\alpha_{A,B\otimes C,D}"] & A \otimes \big((B \otimes C) \otimes D\big) \arrow[dr, "\mathrm{id}_A \otimes \alpha_{B,C,D}"] & \\
\big((A \otimes B) \otimes C\big) \otimes D \arrow[ur, "\alpha_{A,B,C} \otimes \mathrm{id}_D"] \arrow[drr, "\alpha_{A\otimes B,C,D}"'] & & & A \otimes \big(B \otimes (C \otimes D)\big) \\
& & (A \otimes B) \otimes (C \otimes D) \arrow[ur, "\alpha_{A,B,C\otimes D}"'] &
\end{tikzcd} \tag{1.2}$$

The naturality conditions for α, λ and ρ correspond to the following equations:

$$\begin{tikzcd}
(A \otimes B) \otimes C \arrow[r, "\alpha_{A,B,C}"] \arrow[d, "(f \otimes g) \otimes h"] & A \otimes (B \otimes C) \arrow[d, "f \otimes (g \otimes h)"'] \\
(A' \otimes B') \otimes C' \arrow[r, "\alpha_{A',B',C'}"] & A' \otimes (B' \otimes C')
\end{tikzcd}
\qquad
\begin{tikzcd}
I \otimes A \arrow[r, "\lambda_A"] \arrow[d, "I \otimes f"] & A \arrow[d, "f"] & A \otimes I \arrow[l, "\rho_A"'] \arrow[d, "f \otimes I"] \\
I \otimes B \arrow[r, "\lambda_B"'] & B & B \otimes I \arrow[l, "\rho_B"]
\end{tikzcd} \tag{1.3}$$

The tensor unit object I represents the 'trivial' or 'empty' system. This interpretation comes from the unitors λ_A and ρ_A, which witness the fact that the object A is 'just as good as', or isomorphic to, the objects $A \otimes I$ and $I \otimes A$.

Each of the triangle and pentagon equations says that two particular ways of 'reorganizing' a system are equal. Surprisingly, this implies that *any* two 'reorganizations' are equal; this is the content of the Coherence Theorem, which we prove in in Section 1.3.

Theorem 1.2 (Coherence for monoidal categories)**.** *Given the data of a monoidal category, if the pentagon and triangle equations hold, then any well-typed equation built from α, λ, ρ and their inverses holds.* □

In particular, the triangle and pentagon equation together imply $\rho_I = \lambda_I$. To appreciate the power of the coherence theorem, try to show this yourself (this is Exercise 1.4.13).

Coherence is the fundamental motivating idea of a monoidal category, and gives an answer to the question we posed earlier in the chapter: the isomorphisms should satisfy *all* possible well-typed equations. So while these morphisms are not trivial – for example, they are not necessarily identity morphisms – it doesn't matter how we apply them in any particular case.

Our first example of a monoidal structure is on the category **Hilb**, whose structure as a category was given in Definition 0.43.

Definition 1.3. In the monoidal category **Hilb**, and by restriction in **FHilb**,:

- **the tensor product** $\otimes$: $\mathbf{Hilb}\times\mathbf{Hilb}\to\mathbf{Hilb}$ is the tensor product of Hilbert spaces, as defined in Section 0.2.5;
- **the unit object** I is the one-dimensional Hilbert space $\mathbb{C}$;
- **associators** $(H\otimes J)\otimes K \xrightarrow{\alpha_{H,J,K}} H\otimes(J\otimes K)$ are the unique linear maps satisfying $(a\otimes b)\otimes c \mapsto a\otimes(b\otimes c)$ for all $a \in H$, $b \in J$ and $c \in K$;
- **left unitors** $\mathbb{C}\otimes H \xrightarrow{\lambda_H} H$ are the unique linear maps satisfying $1\otimes a \mapsto a$ for all $a \in H$;
- **right unitors** $H\otimes\mathbb{C} \xrightarrow{\rho_H} H$ are the unique linear maps satisfying $a\otimes 1 \mapsto a$ for all $a \in H$.

Although we call the functor $\otimes$ of a monoidal category the 'tensor product', that does not mean that we have to choose the *actual* tensor product of Hilbert spaces for our monoidal structure. There are other monoidal structures on the category that we could choose; a good example is the direct sum of Hilbert spaces. However, the tensor product we have defined above has a special status, since it describes the state space of a composite system in quantum theory.

While **Hilb** is relevant for quantum computation, the monoidal category **Set** is an important setting for classical computation. The category **Set** was described in Definition 0.3; we now add the monoidal structure.

Definition 1.4. In the monoidal category **Set**, and by restriction on **FSet**:

- **the tensor product** is Cartesian product of sets, written $\times$, acting on functions $A \xrightarrow{f} B$ and $C \xrightarrow{g} D$ as $(f\times g)(a,c) = \big(f(a), g(c)\big)$;
- **the unit object** is a chosen singleton set $\{\bullet\}$;
- **associators** $(A\times B)\times C \xrightarrow{\alpha_{A,B,C}} A\times(B\times C)$ are the functions $\big((a,b),c\big) \mapsto \big(a,(b,c)\big)$;
- **left unitors** $I\times A \xrightarrow{\lambda_A} A$ are the functions $(\bullet, a) \mapsto a$;
- **right unitors** $A\times I \xrightarrow{\rho_A} A$ are the functions $(a,\bullet) \mapsto a$.

The Cartesian product in **Set** is a categorical product. This is an example of a general phenomenon (see Exercise 1.4.9): if a category has products and a terminal object, then these furnish the category with a monoidal structure. The same is true for coproducts and an initial object, which in **Set** are given by disjoint union.

This highlights an important difference between the standard tensor products on $\mathbf{Hilb}$ and $\mathbf{Set}$: while the tensor product on $\mathbf{Set}$ comes from a categorical product, the tensor product on $\mathbf{Hilb}$ does not. (See also Chapter 4 and Exercise 2.5.2.) Over the course of this book, we will discover many more differences between $\mathbf{Hilb}$ and $\mathbf{Set}$, which provide insight into the differences between quantum and classical information.

There is also a canonical monoidal structure on the category $\mathbf{Rel}$ introduced in Definition 0.5.

Definition 1.5. In the monoidal category $\mathbf{Rel}$:

- **the tensor product** is Cartesian product of sets, written $\times$, acting on relations $A \xrightarrow{R} B$ and $C \xrightarrow{S} D$ by setting $(a,c)(R \times S)(b,d)$ if and only if aRb and cSd;
- **the unit object** is a chosen singleton set $= \{\bullet\}$;
- **associators** $(A \times B) \times C \xrightarrow{\alpha_{A,B,C}} A \times (B \times C)$ are the relations defined by $\big((a,b),c\big) \sim \big(a,(b,c)\big)$ for all $a \in A$, $b \in B$, and $c \in C$;
- **left unitors** $I \times A \xrightarrow{\lambda_A} A$ are the relations defined by $(\bullet, a) \sim a$ for all $a \in A$;
- **right unitors** $A \times I \xrightarrow{\rho_A} A$ are the relations defined by $(a, \bullet) \sim a$ for all $a \in A$.

The Cartesian product is *not* a categorical product in $\mathbf{Rel}$, so although this monoidal structure looks like that of $\mathbf{Set}$, it is in fact more similar to that of $\mathbf{Hilb}$.

Example 1.6. If $\mathbf{C}$ is a monoidal category, then so is its opposite $\mathbf{C}^{\mathrm{op}}$. The tensor unit I in $\mathbf{C}^{\mathrm{op}}$ is the same as that in $\mathbf{C}$, whereas the tensor product $A \otimes B$ in $\mathbf{C}^{\mathrm{op}}$ is given by $B \otimes A$ in $\mathbf{C}$, the associators in $\mathbf{C}^{\mathrm{op}}$ are the inverses of those morphisms in $\mathbf{C}$, and the left and right unitors of $\mathbf{C}$ swap roles in $\mathbf{C}^{\mathrm{op}}$.

Monoidal categories have an important property called the *interchange law*, which governs the interaction between the categorical composition and tensor product.

Theorem 1.7 (Interchange). *Any morphisms $A \xrightarrow{f} B$, $B \xrightarrow{g} C$, $D \xrightarrow{h} E$ and $E \xrightarrow{j} F$ in a monoidal category satisfy the interchange law:*

$$(g \circ f) \otimes (j \circ h) = (g \otimes j) \circ (f \otimes h) \tag{1.4}$$

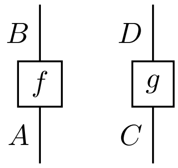
Proof. Use properties of the category $\mathbf{C} \times \mathbf{C}$ and the fact that $\otimes \colon \mathbf{C} \times \mathbf{C} \to \mathbf{C}$ is a functor:

$$\begin{aligned}
(g \circ f) \otimes (j \circ h) &\equiv \otimes(g \circ f, j \circ h) \\
&= \otimes\big((g,j) \circ (f,h)\big) && \text{(composition in } \mathbf{C} \times \mathbf{C}) \\
&= \big(\otimes(g,j)\big) \circ \big(\otimes(f,h)\big) && \text{(functoriality of } \otimes) \\
&= (g \otimes j) \circ (f \otimes h)
\end{aligned}$$

Recall that functoriality of F says that $F(g \circ f) = F(g) \circ F(f)$. □

1.1.1 Graphical calculus

A monoidal structure allows us to interpret multiple processes in our category taking place at the same time. For morphisms $A \xrightarrow{f} B$ and $C \xrightarrow{g} D$, it therefore seems reasonable, at least informally, to draw their tensor product $A \otimes C \xrightarrow{f \otimes g} B \otimes D$ like this:



(1.5)

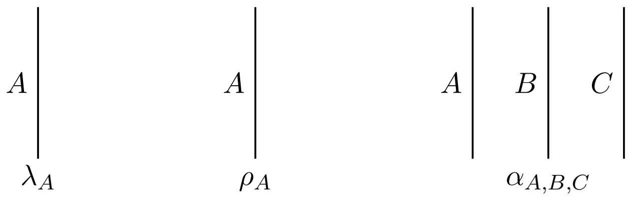
The idea is that f and g represent processes taking place at the same time on distinct systems. Inputs are drawn at the bottom, and outputs are drawn at the top; in this sense, "time" runs upwards. This extends the one-dimensional notation for categories outlined in Section 0.1.5. Whereas the graphical calculus for ordinary categories was one-dimensional, or *linear*, the graphical calculus for monoidal categories is two-dimensional or *planar*. The two dimensions correspond to the two ways to combine morphisms: by categorical composition (vertically) or by tensor product (horizontally).

One could imagine this notation being a useful short-hand when working with monoidal categories. This is true, but in fact a lot more can be said, as we will examine shortly. Namely, the graphical calculus gives a sound and complete language for monoidal categories.

The (identity on the) monoidal unit object I is drawn as the empty diagram:

(1.6)

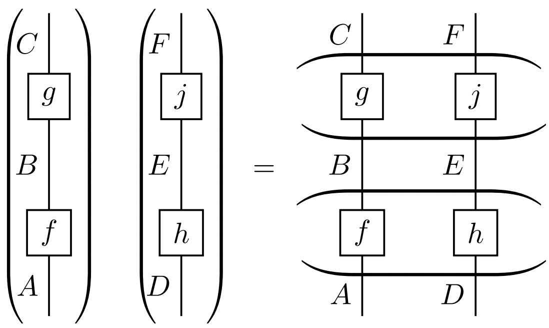
The left unitor $I \otimes A \xrightarrow{\lambda_A} A$, the right unitor $A \otimes I \xrightarrow{\rho_A} A$ and the associator $(A \otimes B) \otimes C \xrightarrow{\alpha_{A,B,C}} A \otimes (B \otimes C)$ are also simply not depicted:



(1.7)

The coherence of α, λ and ρ is therefore important for the graphical calculus to function: since there can only be a single morphism built from their components of any given type by Theorem 1.2, it doesn't matter that their graphical calculus encodes no information.

Now consider the graphical representation of the interchange law (1.4):



(1.8)

We used brackets to indicate how we are forming the diagrams on each side. They merely record in which order we drew the picture; the two pictures are exactly the same. Dropping the brackets showcases that the interchange law is very natural; what seemed to be a mysterious algebraic identity becomes clear from the graphical perspective.

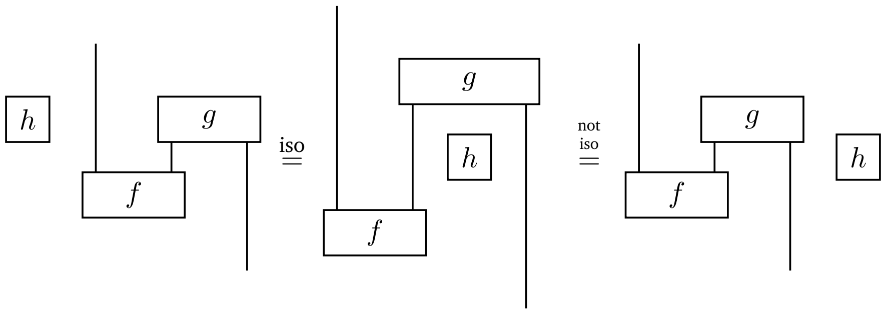
The point of the graphical calculus is that all the superficially complex aspects of the algebraic definition of monoidal categories – the unit law, the associativity law, associators, left unitors, right unitors, the triangle equation, the pentagon equation, the interchange law – melt away, allowing us to use the theory of monoidal categories in a direct way. The algebraic features are still there, but they are absorbed into the geometry of the plane, of which you happen to have an excellent intuitive understanding.

The following theorem is the formal statement that connects the graphical calculus to the theory of monoidal categories.

Theorem 1.8 (Correctness of the graphical calculus for monoidal categories)**.** *A well-typed equation between morphisms in a monoidal category follows from the axioms if and only if it holds in the graphical language up to planar isotopy.*

Two diagrams are *planar isotopic* when one can be deformed continuously into the other within some rectangular region of the plane, with the input and output wires terminating at the lower and upper boundaries of the rectangle, without introducing any intersections of the components. For this purpose, assume that wires have zero width, and morphism boxes have zero size.

Example 1.9. Here are examples of isotopic and non-isotopic diagrams:



As above, we will often allow the heights of the diagrams to change, and allow input and output wires to slide horizontally along their respective boundaries, although they must never change order. The third diagram is not isotopic to the first two, since for the box h to move to the right-hand side, it would have to 'pass through' one of the wires, which is not allowed. The box cannot pass 'in front of' or 'behind' the wire, since the diagrams are confined to the plane – that is what is meant by *planar* isotopy. Imagine that the components of the diagram are trapped between two pieces of glass. Also, the box h cannot move over the top end of the wire, or under the bottom end, since that would mean leaving the rectangular region of the plane in which the diagram is defined.

The correctness theorem is really saying two distinct things: that the graphical calculus is *sound*, and that it is *Complete*. To understand these concepts, let f and g be morphisms such that the equation $f = g$ is well-typed, and consider the following statements:

- $P(f, g)$: "under the axioms of a monoidal category, $f = g$";

- $Q(f, g)$: "the graphical representations of f and g are planar isotopic".

Soundness is the assertion that $P(f, g) \Rightarrow Q(f, g)$ for all such f and g: that is, if the morphisms are equal, then the pictures are isotopic. *Completeness* is the reverse assertion, that $Q(f, g) \Rightarrow P(f, g)$ for all such f and g: that is, if the pictures are isotopic, then the morphisms are equal.

Proving soundness is straightforward: there are only a finite number of axioms for a monoidal category, and you just have to check that they are all valid in terms of planar isotopy of diagrams. Completeness is harder: one must analyze the definition of planar isotopy, and show that any planar isotopy can be built from a small set of moves, each of which independently leave the underlying morphism in the monoidal category unchanged.

Let's take a closer look at the condition that the equation $f = g$ be well-typed. Firstly, f and g must have the same domain and the same codomain. For example, let $f = \mathrm{id}_{A \otimes B}$, and $g = \rho_A \otimes \mathrm{id}_B$. Then their types are $A \otimes B \xrightarrow{f} A \otimes B$ and $(A \otimes I) \otimes B \xrightarrow{g} A \otimes B$. These have different domains, and so the equation is not well-typed, even though their graphical representations are planar isotopic. Also, suppose that our category happened to satisfy $A \otimes B = (A \otimes I) \otimes B$; then although f and g would have the same type, the equation $f = g$ would still not be well-typed, since it would be making use of this 'accidental' equality. For a careful examination of the well-typed property, see Section 1.3.4.

Throughout the book we apply the correctness property of the graphical calculus by writing $\overset{\text{iso}}{=}$ to denote isotopic diagrams, whose interpretations as morphisms in a monoidal category are therefore equal.

1.1.2 States and effects

If a mathematical structure lives as an object in a category, and we want to learn something about its internal structure, we must find a way to do it using the morphisms of the category only. For example, consider a set $A \in \mathrm{Ob}(\mathbf{Set})$ with a chosen element $a \in A$: we can represent this with the function $\{\bullet\} \to A$ defined by $\bullet \mapsto a$. This inspires the following definition, which generalizes the notion of set-theoretical state.

Definition 1.10 (State)**.** In a monoidal category, a *state* of an object A is a morphism $I \to A$.

Since the monoidal unit object represents the trivial system, a state $I \to A$ of a system can be thought of as a way for the system A to be brought into being.

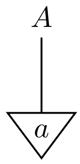
Example 1.11. Let's examine what the states are in our example categories:

- in $\mathbf{Hilb}$, states of a Hilbert space H are linear functions $\mathbb{C} \to H$, which correspond to elements of H by considering the image of $1 \in \mathbb{C}$;
- in $\mathbf{Set}$, states of a set A are functions $\{\bullet\} \to A$, which correspond to elements of A by considering the image of $\bullet$;
- in $\mathbf{Rel}$, states of a set A are relations $\{\bullet\} \xrightarrow{R} A$, which correspond to subsets of A by considering all elements related to $\bullet$.

Definition 1.12. A monoidal category is *well-pointed* if for all parallel pairs of morphisms $A \xrightarrow{f,g} B$, we have $f = g$ when $f \circ a = g \circ a$ for all states $I \xrightarrow{a} A$. A monoidal category is *monoidally well-pointed* if for all parallel pairs of morphisms $A_1 \otimes \cdots \otimes A_n \xrightarrow{f,g} B$, we have $f = g$ when $f \circ (a_1 \otimes \cdots \otimes a_n) = g \circ (a_1 \otimes \cdots \otimes a_n)$ for all states $I \xrightarrow{a_1} A_1, \ldots, I \xrightarrow{a_n} A_n$.

The idea is that in a well-pointed category, we can tell whether or not morphisms are equal just by seeing how they affect states of their domains. In a monoidally well-pointed category, it is even enough to consider product states to verify equality of morphisms out of a compound object. The categories $\mathbf{Set}$, $\mathbf{Rel}$, $\mathbf{Vect}$, and $\mathbf{Hilb}$ are all monoidally well-pointed. For the latter two, this comes down to the fact that if $\{d_i\}$ is a basis for H and $\{e_j\}$ is a basis for K, then $\{d_i \otimes e_j\}$ is a basis for $H \otimes K$.

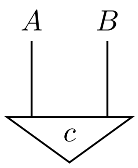
To emphasize that states $I \xrightarrow{a} A$ have the empty picture (1.6) as their domain, we will draw them as triangles instead of boxes.



(1.9)

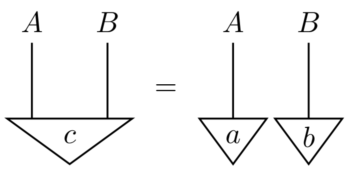
1.1.3 Product states and entangled states

For objects A and B of a monoidal category, a morphism $I \xrightarrow{c} A \otimes B$ is a *joint state* of A and B. It is depicted graphically as follows:



(1.10)

Definition 1.13 (Product state, entangled state)**.** A joint state $I \xrightarrow{c} A \otimes B$ is a *product state* when it is of the form $I \xrightarrow{\lambda_I^{-1}} I \otimes I \xrightarrow{a \otimes b} A \otimes B$ for $I \xrightarrow{a} A$ and $I \xrightarrow{b} B$:



(1.11)

A joint state is *entangled* when it is not a product state.

Entangled states represent preparations of $A \otimes B$ which cannot be decomposed as a preparation of A alongside a preparation of B. In this case, there is some essential connection between A and B which means that they cannot have been prepared independently.

Example 1.14. Joint states, product states, and entangled states look as follows in our example categories:

- in $\mathbf{Hilb}$:
  - **joint states** of H and K are elements of $H \otimes K$;

  - **product states** are factorizable states;
  - **entangled states** are elements of $H \otimes K$ which cannot be factorized;
- in **Set**:
  - **joint states** of A and B are elements of $A \times B$;
  - **product states** are elements $(a, b) \in A \times B$ coming from $a \in A$ and $b \in B$;
  - **entangled states** don't exist;
- in $\mathbf{Rel}$:
  - **joint states** of A and B are subsets of $A \times B$;
  - **product states** are 'square' subsets $U \subseteq A \times B$: for some $V \subseteq A$ and $W \subseteq B$, $(a, b) \in U$ if and only if $a \in V$ and $b \in W$;
  - **entangled states** are subsets of $A \times B$ that are not of this form.

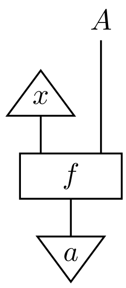
This hints at why entanglement can be difficult to understand intuitively: it cannot occur classically, in the processes encoded by the category $\mathbf{Set}$. However, if we allow nondeterministic behaviour as encoded by $\mathbf{Rel}$, an analogue of entanglement does appear.

1.1.4 Effects

An *effect* represents a process by which a system is destroyed, or consumed.

Definition 1.15 (Effect)**.** In a monoidal category, an *effect* or *costate* for an object A is a morphism $A \to I$.

Given a diagram constructed using the graphical calculus, we can interpret it as a history of events that have taken place. If the diagram contains an effect, this is interpreted as the assertion that a measurement was performed, with the given effect as the result. For example, the diagram



(1.12)

describes a history in which a state a is prepared, and then a process f is performed producing two systems, the first of which is measured giving outcome x. This does not imply that the effect x was the *only* possible outcome for the measurement; just that by drawing this diagram, we are only interested in the cases when the outcome x does occur. An effect can be thought of as a *postselection*: keep repeating the entire experiment until the measurement has the specified outcome.

The overall history is a morphism of type $I \to A$, which is a state of A. The postselection interpretation dictates how to prepare this state, given the ability to perform its components.

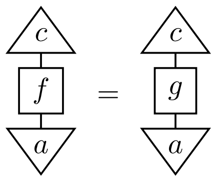
Example 1.16. These statements are at a very general level. To say more, we must take account of the particular theory of processes described by the monoidal category in which we are working.

- In quantum theory, as encoded by $\mathbf{Hilb}$, the morphisms a, f and x must be partial isometries. The Born rule of quantum mechanics dictate that the probability for this history to take place is given by the square norm of the resulting state. So in particular, the history described by this composite morphism is impossible exactly when the overall state is zero.

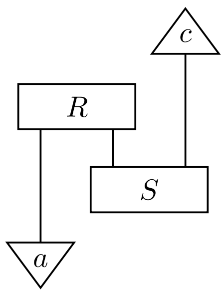
- In nondeterministic classical physics, as described by $\mathbf{Rel}$, there are no particular requirements on a, f and x, which may be arbitrary relations of the correct types. The overall composite relation then describes the possible ways in which A can be prepared as a result of this history. If the overall composite is empty, then this particular sequence of a state preparation, a dynamics step, and a measurement result cannot occur.

- Things are very different in $\mathbf{Set}$. The monoidal unit object is *terminal* in that category, meaning $\mathbf{Set}(A, I)$ has only a single element for any object A. So every object has a *unique* effect, and there is no nontrivial notion of 'measurement'.

We may think of the wires in the graphical calculus carrying information flow as follows. If the monoidal dagger category is monoidally well-pointed, two morphisms $A \xrightarrow{f,g} C$ are equal if and only if for all states $I \xrightarrow{a} A$ and $I \xrightarrow{c} C$ the following two scalars are equal:



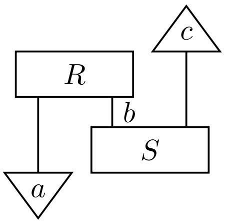
So we could verify an equation by computing these 'matrix entries' of both sides. In the category $\mathbf{Rel}$ it is convenient to do this by decorating the wires with elements. For example, the relation $I \to I$ given by



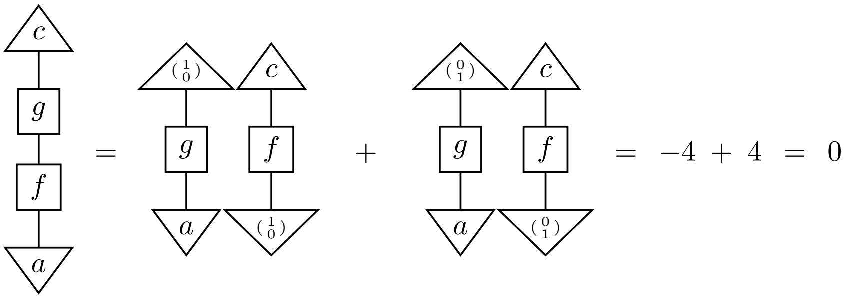
is nonempty if and only if there exists an element b such that both the relations

(1.13)

are nonempty. Thus we can decorate



to signify that if element a is connected to c by the composite morphism, then it must ‘flow’ through some element b in the middle. In the category **FHilb**, however, this technique doesn’t work because of (destructive) interference. For example, if $g = \left(\begin{smallmatrix} -1 & -1 \\ 1 & 1 \end{smallmatrix}\right)$, $f = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, and $a = c = \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)$, the scalar



vanishes, but nevertheless both histories in the sum are possible.

1.2 Braiding and symmetry

In many theories of processes, if A and B are systems, the systems $A \otimes B$ and $B \otimes A$ can be considered essentially equivalent. While we would not expect them to be equal, we might at least expect there to be some special process of type $A \otimes B \to B \otimes A$ that ‘switches’ the systems, and does nothing more. Developing these ideas gives rise to *braided* and *symmetric* monoidal categories, which we now investigate.

1.2.1 Braided monoidal categories

We first consider braided monoidal categories.

Definition 1.17. A *braided monoidal category* is a monoidal category equipped with a natural isomorphism

$$A \otimes B \xrightarrow{\sigma_{A,B}} B \otimes A \tag{1.14}$$

satisfying the following *hexagon equations*:

$$\begin{tikzcd}
& A \otimes (B \otimes C) \arrow[r, "\sigma_{A,B\otimes C}"] \arrow[dl, "\alpha^{-1}_{A,B,C}"'] & (B \otimes C) \otimes A & \\
(A \otimes B) \otimes C \arrow[dr, "\sigma_{A,B} \otimes \mathrm{id}_C"'] & & & B \otimes (C \otimes A) \arrow[ul, "\alpha^{-1}_{B,C,A}"'] \\
& (B \otimes A) \otimes C \arrow[r, "\alpha_{B,A,C}"'] & B \otimes (A \otimes C) \arrow[ur, "\mathrm{id}_B \otimes \sigma_{A,C}"'] &
\end{tikzcd} \tag{1.15}$$

$$
\begin{tikzcd}
 & (A \otimes B) \otimes C \arrow[r, "\sigma_{A \otimes B, C}"] \arrow[dl, "\alpha_{A,B,C}"'] & C \otimes (A \otimes B) & \\
A \otimes (B \otimes C) \arrow[dr, "\mathrm{id}_A \otimes \sigma_{B,C}"'] & & & (C \otimes A) \otimes B \arrow[ul, "\alpha_{C,A,B}"'] \\
 & A \otimes (C \otimes B) \arrow[r, "\alpha^{-1}_{A,C,B}"'] & (A \otimes C) \otimes B \arrow[ur, "\sigma_{A,C} \otimes \mathrm{id}_B"'] &
\end{tikzcd}
\tag{1.16}
$$

We include the braiding in the graphical notation like this:

$$A \otimes B \xrightarrow{\sigma_{A,B}} B \otimes A \qquad\qquad B \otimes A \xrightarrow{\sigma^{-1}_{A,B}} A \otimes B \tag{1.17}$$

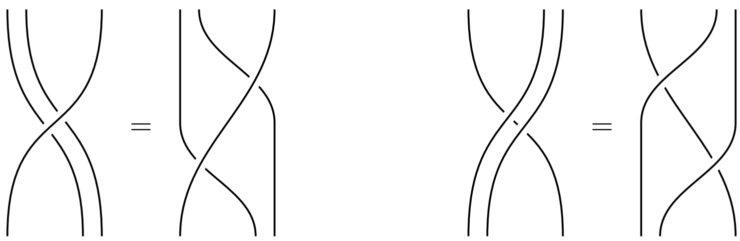
Invertibility then takes the following graphical form:

(1.18)

This captures part of the geometric behaviour of strings. Naturality of the braiding and the inverse braiding have the following graphical representations:

(1.19)

The hexagon equations have the following graphical representations:



(1.20)

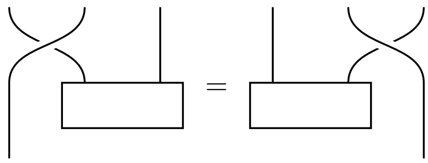
Each of these equations has two strands close to each other on the left-hand side, to indicate that thay are treated as a single composite object for the purposes of the braiding. We see that the hexagon equations express something quite straightforward: to braid with a tensor product of two strands is the same as braiding separately with one and then with the other.

Since the strands of a braiding cross over each other, they are not lying on the plane; they live in three-dimensional space. So while categories have a one-dimensional or linear notation, and monoidal categories have a two-dimensional or planar graphical notation, braided monoidal categories have a three-dimensional notation. Because of this, braided monoidal categories have an important connection to three-dimensional quantum field theory.

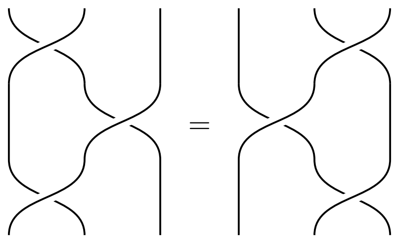
Braided monoidal categories have a sound and complete graphical calculus, as established by the following theorem. The notion of isotopy it uses is now three-dimensional; that is, the diagrams are assumed to lie in a cube, with input wires terminating at the lower face and output wires terminating at the upper face. This is also called *spatial isotopy*.

Theorem 1.18 (Correctness of graphical calculus for braided monoidal categories)**.** *A well-typed equation between morphisms in a braided monoidal category follows from the axioms if and only if it holds in the graphical language up to spatial isotopy.*

Given two isotopic diagrams, it can be quite nontrivial to show they are equal using the axioms of braided monoidal categories directly. So as with ordinary monoidal categories, the coherence theorem is quite powerful. For example, try to show that the following two equations hold directly using the axioms of a braided monoidal category:



(1.21)



(1.22)

(This is Exercise 1.4.4.) Equation (1.22) is called the *Yang-Baxter equation*, which plays an important role in the mathematical theory of knots.

For each of our main example categories there is a naive notion of a ‘swap’ process, which in each case gives a braided monoidal structure.

Definition 1.19. The monoidal categories $\mathbf{Hilb}$, $\mathbf{Set}$ and $\mathbf{Rel}$ can all be equipped with a canonical braiding:

- in $\mathbf{Hilb}$, $H \otimes K \xrightarrow{\sigma_{H,K}} K \otimes H$ is the unique linear map extending $a \otimes b \mapsto b \otimes a$ for all $a \in H$ and $b \in K$;
- in $\mathbf{Set}$, $A \times B \xrightarrow{\sigma_{A,B}} B \times A$ is defined by $(a, b) \mapsto (b, a)$ for all $a \in A$ and $b \in B$;
- in $\mathbf{Rel}$, $A \times B \xrightarrow{\sigma_{A,B}} B \times A$ is defined by $(a, b) \sim (b, a)$ for all $a \in A$ and $b \in B$.

Each of these in fact has the stronger structure of being *symmetric monoidal*, which we explore in the next section. We will see an example of a braided monoidal category that is not symmetric later in the book, in Definition 2.43.

1.2.2 Symmetric monoidal categories

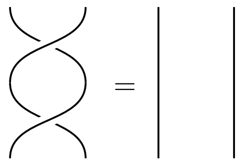
In our example categories $\mathbf{Hilb}$, $\mathbf{Rel}$ and $\mathbf{Set}$, the braidings satisfy an extra property that makes them very easy to work with.

Definition 1.20. A braided monoidal category is *symmetric* when

$$\sigma_{B,A} \circ \sigma_{A,B} = \mathrm{id}_{A \otimes B} \tag{1.23}$$

for all objects A and B, in which case we call σ the *symmetry*.

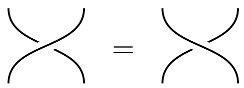
Graphically, condition (1.23) has the following representation:



(1.24)

Intuitively, the strings can pass through each other, and nontrivial knots cannot be formed.

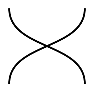
Lemma 1.21. *In a symmetric monoidal category, $\sigma_{A,B} = \sigma^{-1}_{B,A}$:*



(1.25)

Proof. Combine (1.18) and (1.24). □

A symmetric monoidal category therefore makes no distinction between over- and under-crossings, and we may simplify our graphical notation, drawing



(1.26)

for the single type of crossing.

The graphical calculus with the extension of braiding or symmetry is still sound: if the two diagrams of morphisms can be deformed into one another, then the two morphisms are equal.

Suppose our diagrams depict curves embedded in four-dimensional space. For example, imagine a colour or temperature that continuously varies over a wire, in addition to the wire occupying three-dimensional space. Then we can smoothly deform one crossing into the other, in the manner of equation (1.25), by making use of the extra dimension. In this sense, symmetric monoidal categories have a four-dimensional graphical notation.

Theorem 1.22 (Correctness of the graphical calculus for symmetric monoidal categories)**.** *A well-typed equation between morphisms in a symmetric monoidal category follows from the axioms if and only if it holds in the graphical language up to graphical equivalence.*

By "graphical equivalence", we mean three-dimensional isotopy with the addition of equation (1.25). While a stronger statement involving true four-dimensional isotopy is almost certainly correct, it is not currently supported by the literature.

The following gives an important family of examples of symmetric monoidal categories, with a mathematical flavour, but also with important applications in physics. Understanding this example requires a little bit of knowledge of group representation theory.

Definition 1.23. For a finite group $\mathbf{G}$, there is a symmetric monoidal category $\mathbf{Rep}(\mathbf{G})$ of finite-dimensional representations of $\mathbf{G}$, in which:

- **objects** are finite-dimensional representations of $\mathbf{G}$;
- **morphisms** are intertwiners for the group action;
- the **tensor product** is tensor product of representations;
- the **unit object** is the trivial action of G on the 1-dimensional vector space;
- the **symmetry** is inherited from $\mathbf{Vect}$.

Another interesting symmetric monoidal category is inspired by the physics of bosons and fermions. These are quantum particles with the property that when two fermions exchange places, a phase of -1 is obtained. When two bosons exchange places, or when a boson and a fermion exchange places, there is no extra phase. The categorical structure can be described as follows.

Definition 1.24. In the symmetric monoidal category $\mathbf{SuperHilb}$:

- **objects** are pairs (H, K) of Hilbert spaces;
- **morphisms** $(H, K) \to (H', K')$ are pairs of linear maps $H \to H'$ and $K \to K'$;
- the **tensor product** is given on objects by $(H, K) \otimes (L, M) = \big((H \otimes L) \oplus (K \otimes M), (H \otimes M) \oplus (K \otimes L)\big)$, and similarly on morphisms;
- the **unit object** is $(\mathbb{C}, 0)$;
- the **associator**s and **unitor**s are defined similarly to those of $\mathbf{Hilb}$;
- the **symmetry** is given by

$$\sigma_{(H,K),(L,M)} = \left(\begin{pmatrix} \mathrm{id}_{H\otimes L} & 0 \\ 0 & -\mathrm{id}_{K\otimes M} \end{pmatrix}, \begin{pmatrix} \mathrm{id}_{H\otimes M} & 0 \\ 0 & \mathrm{id}_{K\otimes L} \end{pmatrix} \right).$$

Interpret an object (H, K) as a composite quantum system whose state space splits as a direct sum of a bosonic part H and a fermionic part K.

1.3 Coherence

In this section we prove the coherence theorem for monoidal categories. To do so, we first discuss *strict* monoidal categories, which are easier to work with. Then we rigorously introduce the notion of monoidal equivalence, which encodes when two monoidal categories 'behave the same'. This puts us in a position to prove the Strictification Theorem 1.38, which says that any monoidal category is monoidally equivalent to a strict one. From there we prove the Coherence Theorem. It is not necessary to absorb these proofs to understand the rest of the book, but these theorems play such a crucial role in establishing the soundness of the graphical language that we cover them here for the sake of completeness; we recommend skipping this section on a first reading.

1.3.1 Strictness

Some types of monoidal category have no data encoded in their unit and associativity morphisms. In this section we prove that in fact, every monoidal category can be made into a such a *strict* one.

Definition 1.25. A monoidal category is *strict* if the natural isomorphisms $\alpha_{A,B,C}$, λ_A and ρ_A are all identities.

The category $\mathbf{Mat}_{\mathbb{C}}$ of Definition 0.36 can be given strict monoidal structure.

Definition 1.26. The following structure makes $\mathbf{Mat}_{\mathbb{C}}$ strict monoidal:

- **tensor product** $\otimes\colon \mathbf{Mat}_{\mathbb{C}} \times \mathbf{Mat}_{\mathbb{C}} \to \mathbf{Mat}_{\mathbb{C}}$ is given on objects by multiplication of numbers $n \otimes m = nm$, and on morphisms by Kronecker product of matrices (0.32);
- **the monoidal unit** is the natural number 1;
- **associators, left unitors and right unitors** are the identity matrices.

The Strictification Theorem 1.38 below will show that any monoidal category is monoidally equivalent to a strict one. Sometimes this is not as useful as it sounds. For example, you often have some idea of what you want the objects of your category to be, but you might have to abandon this to construct a strict version of your category. In particular, it's often useful for categories to be *skeletal* (see Definition 0.10). Every monoidal category is equivalent to a skeletal monoidal category, and skeletal categories are often particularly easy to work with. Some monoidal categories are both strict and skeletal, such as $\mathbf{Mat}_{\mathbb{C}}$. But one cannot always have these properties together, as Proposition 1.35 below will show. First we have to discuss what exactly it means to be monoidally equivalent.

1.3.2 Monoidal functors

Monoidal functors are functors that preserve monoidal structure; they have to satisfy some coherence properties of their own.

Definition 1.27. A *monoidal functor* $F\colon \mathbf{C} \to \mathbf{C}'$ between monoidal categories is a functor equipped with natural isomorphisms

$$(F_2)_{A,B}\colon F(A) \otimes' F(B) \to F(A \otimes B) \tag{1.27}$$
$$F_0\colon I' \to F(I) \tag{1.28}$$

making the following diagrams commute:

$$\begin{tikzcd}
\big(F(A) \otimes' F(B)\big) \otimes' F(C) \arrow[rr, "\alpha'_{F(A),F(B),F(C)}"] \arrow[d, "(F_2)_{A,B} \otimes' \mathrm{id}_{F(C)}"] & & F(A) \otimes' \big(F(B) \otimes' F(C)\big) \arrow[d, "\mathrm{id}_{F(A)} \otimes' (F_2)_{B,C}"'] \\
F(A \otimes B) \otimes' F(C) \arrow[d, "(F_2)_{A\otimes B,C}"] & & F(A) \otimes' F(B \otimes C) \arrow[d, "(F_2)_{A,B\otimes C}"'] \\
F\big((A \otimes B) \otimes C\big) \arrow[rr, "F(\alpha_{A,B,C})"'] & & F\big(A \otimes (B \otimes C)\big)
\end{tikzcd} \tag{1.29}$$

$$\begin{tikzcd}
F(A) \otimes' I' \arrow[r, "\rho'_{F(A)}"] \arrow[d, "\mathrm{id}_{F(A)} \otimes' F_0"] & F(A) \arrow[d, "F(\rho_A^{-1})"] \\
F(A) \otimes' F(I) \arrow[r, "(F_2)_{A,I}"'] & F(A \otimes I)
\end{tikzcd}
\qquad
\begin{tikzcd}
I' \otimes' F(A) \arrow[r, "\lambda'_{F(A)}"] \arrow[d, "F_0 \otimes' \mathrm{id}_{F(A)}"'] & F(A) \arrow[d, "F(\lambda_A^{-1})"'] \\
F(I) \otimes' F(A) \arrow[r, "(F_2)_{I,A}"'] & F(I \otimes A)
\end{tikzcd} \tag{1.30}$$

Monoidal functors may also be compatible with a braiding if one is available.

Definition 1.28. A *braided monoidal functor* is a monoidal functor $F\colon \mathbf{C} \to \mathbf{C}'$ between braided monoidal categories making the following diagram commute:

$$\begin{tikzcd}
F(A) \otimes' F(B) \arrow[r, "\gamma'_{F(A),F(B)}"] \arrow[d, "(F_2)_{A,B}"'] & F(B) \otimes' F(A) \arrow[d, "(F_2)_{B,A}"] \\
F(A \otimes B) \arrow[r, "F(\gamma_{A,B})"'] & F(B \otimes A)
\end{tikzcd} \tag{1.31}$$

One might additionally ask for a braided monoidal functor to be compatible with a symmetry, but this does not lead to any further algebraic conditions.

Definition 1.29. A *symmetric monoidal functor* is a braided monoidal functor $F\colon \mathbf{C} \to \mathbf{C}'$ between symmetric monoidal categories.

The only reason to introduce this definition is that it sounds a bit strange to talk about braided monoidal functors between symmetric monoidal categories.

Let's look at some examples.

Example 1.30. There are monoidal functors between our example categories in the finite-dimensional case, as follows:

$$\mathbf{FRel} \xleftarrow{F} \mathbf{FSet} \xrightarrow{G} \mathbf{FHilb} \tag{1.32}$$

The functor F is the identity on objects, and sends a morphism $A \xrightarrow{f} B$ to its graph $F(f) = \{(a, f(a)) | a \in A\}$. The functor G takes a set A to the Hilbert space $G(A) = \{g \colon A \to \mathbb{C}\}$, and a morphism $A \xrightarrow{f} B$ to $G(A) \xrightarrow{G(f)} G(B)$ defined by $G(f)(g)(b) = \sum_{f(a)=b} g(a)$.

Example 1.31. There are full and faithful monoidal functors embedding the finite-dimensional example categories into the infinite-dimensional ones:

$$\mathbf{FRel} \to \mathbf{Rel} \qquad \mathbf{FSet} \to \mathbf{Set} \qquad \mathbf{FHilb} \to \mathbf{Hilb} \tag{1.33}$$

These take the objects and morphisms to themselves in the larger context. They are examples of *monoidal subcategories*.

Example 1.32. For any finite group G, the forgetful functor $F \colon \mathbf{Rep}(G) \to \mathbf{Hilb}$ is a symmetric monoidal functor. It takes a representation of G to its underlying Hilbert space, and an intertwiner of representations to its underlying linear map. The natural isomorphisms F_2 and F_0 are the identity.

Monoidal functors between two monoidal categories witness the two monoidal structures are essentially the same.

Definition 1.33. A *monoidal equivalence* is a monoidal functor that is an equivalence as a functor.

Example 1.34. The equivalence $R \colon \mathbf{Mat}_{\mathbb{C}} \to \mathbf{FHilb}$ of Proposition 0.37 is a monoidal equivalence.

Proof. Set $R_0 = \mathrm{id}_{\mathbb{C}} \colon \mathbb{C} \to \mathbb{C}$, and define $(R_2)_{m,n} \colon \mathbb{C}^m \otimes \mathbb{C}^n \to \mathbb{C}^{mn}$ by $|i\rangle \otimes |j\rangle \mapsto |ni + j\rangle$ for the computational basis. Then $(R_2)_{m,1} = \rho_{\mathbb{C}^m}$ and $(R_2)_{1,n} = \lambda_{\mathbb{C}^n}$, satisfying (1.30). Equation (1.29) is also satisfied by this definition. Thus R is a monoidal functor. □

As promised, we can now make rigorous that not every monoidal is monoidally equivalent to a strict skeletal one.

Proposition 1.35. *The monoidal category* $\mathbf{Set}$ *is not monoidally equivalent to a strict, skeletal monoidal category.*

Proof. By contradiction. Write $\mathbf{Set}'$ for a strict, skeletal monoidal category monoidally equivalent to $\mathbf{Set}$. The monoidal structure of $\mathbf{Set}$ arises from its Cartesian product structure, and since Cartesian products are preserved by equivalences, the monoidal structure on $\mathbf{Set}'$ must also be Cartesian. Write $\mathbb{N} \in \mathbf{Set}'$ for the image of the natural numbers under the equivalence, and $p_1 \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ for the projection onto the first factor in $\mathbf{Set}'$ arising from the Cartesian structure. Then build the following commutative diagram, where the first and last squares commute due to naturality of the projection maps (see Exercise 1.4.9), and the middle square commutes due to naturality of the associator:

$$\begin{tikzcd}
\mathbb{N} & \mathbb{N} \times (\mathbb{N} \times \mathbb{N}) \arrow[l, "p_1"'] & (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} \arrow[l, "\alpha_{\mathbb{N},\mathbb{N},\mathbb{N}} = \mathrm{id}"'] \arrow[r, "p_1"] & \mathbb{N} \times \mathbb{N} \\
\mathbb{N} \arrow[u, "f"] & \mathbb{N} \times (\mathbb{N} \times \mathbb{N}) \arrow[l, "p_1"] \arrow[u, "f \times (g \times h)"'] & (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} \arrow[l, "\alpha_{\mathbb{N},\mathbb{N},\mathbb{N}} = \mathrm{id}"] \arrow[r, "p_1"'] \arrow[u, "(f \times g) \times h"'] & \mathbb{N} \times \mathbb{N} \arrow[u, "f \times g"']
\end{tikzcd}$$

Note that in this diagram, the morphism p_1 is used with a number of apparently different domains and codomains, none of which agree with its definition as $p_1 \colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ above. However, by skeletality $\mathbb{N} = \mathbb{N} \times \mathbb{N}$, so there is no inconsistency.

Now use the diagram above to compute:

$$f \circ p_1 = p_1 \circ (f \times (g \times h)) = p_1 \circ ((f \times g) \times h) = (f \times g) \circ p_1$$

Hence $f \circ p_1 = (f \times g) \circ p_1$, and because p_1 is surjective, $f = f \times g$. By a similar argument $g = f \times g$, and so $f = g$ for all $f, g \colon \mathbb{N} \to \mathbb{N}$. But this is clearly false, completing the proof. □

As a final preparation for the Strictification Theorem, it is natural to ask for natural transformations between monoidal functors to satisfy some equations.

Definition 1.36 (Monoidal natural transformation)**.** Let $F, G \colon \mathbf{C} \to \mathbf{C}'$ be monoidal functors between monoidal categories. A *monoidal natural transformation* is a natural transformation $\mu \colon F \Rightarrow G$ making the following diagrams commute:

$$\begin{tikzcd}
F(A) \otimes' F(B) \arrow[r, "(F_2)_{A,B}"] \arrow[d, "\mu_A \otimes' \mu_B"'] & F(A \otimes B) \arrow[d, "\mu_{A\otimes B}"] \\
G(A) \otimes' G(B) \arrow[r, "(G_2)_{A,B}"'] & G(A \otimes B)
\end{tikzcd}
\qquad
\begin{tikzcd}
 & F(I) \arrow[dd, "\mu_I"'] \\
I' \arrow[ur, "F_0"] \arrow[dr, "G_0"'] & \\
 & G(I)
\end{tikzcd}
\tag{1.34}$$

The further notions of braided or symmetric monoidal natural transformation do not give any further algebraic conditions, as with the definition of symmetric monoidal functor, but for similar reasons they give useful terminology.

Definition 1.37. A *braided monoidal natural transformation* is a monoidal natural transformation $\mu : F \Rightarrow G$ between braided monoidal functors. A *symmetric monoidal natural transformation* is a monoidal natural transformation between symmetric monoidal functors.

Another way to define a monoidal equivalence between monoidal categories $\mathbf{C}$ and $\mathbf{D}$ is as a pair of monoidal functors $F \colon \mathbf{C} \to \mathbf{D}$ and $G \colon \mathbf{D} \to \mathbf{C}$ for which both $F \circ G$ and $G \circ F$ are naturally monoidally isomorphic to the identity functors. This turns out to be equivalent to Definition 1.33.

1.3.3 Strictification

We are ready to prove the Strictification Theorem, which says that any monoidal category can be replaced by a strict one with the same expressivity.

Theorem 1.38 (Strictification)**.** *Every monoidal category is monoidally equivalent to a strict monoidal category.*

Proof. We will emulate Cayley's theorem, which states that any group G is isomorphic to the group of all permutations $G \to G$ that commute with right multiplication, by sending g to left-multiplication with g.

Let $\mathbf{C}$ be a monoidal category, and define $\mathbf{D}$ as follows. Objects are pairs (F, γ) consisting of a functor $F \colon \mathbf{C} \to \mathbf{C}$ and a natural isomorphism

$$F(A) \otimes B \xrightarrow{\gamma_{A,B}} F(A \otimes B).$$

Think of γ as witnessing that F commutes with right multiplication. A morphism $(F, \gamma) \to (F', \gamma')$ is a natural transformation $\theta \colon F \Rightarrow F'$ making the following square commute for all objects A, B of $\mathbf{C}$:

$$\begin{tikzcd}
F(A) \otimes B \arrow[r, "\gamma_{A,B}"] \arrow[d, "\theta_A \otimes \mathrm{id}_B"'] & F(A \otimes B) \arrow[d, "\theta_{A \otimes B}"] \\
F'(A) \otimes B \arrow[r, "\gamma'_{A,B}"'] & F'(A \otimes B)
\end{tikzcd} \tag{1.35}$$

Composition is given by $(\theta' \circ \theta)_A = \theta'_A \circ \theta_A$. The tensor product of objects in $\mathbf{D}$ is given by $(F, \gamma) \otimes (F', \gamma') = (F \circ F', \delta)$, where δ is the composition

$$F(F'(A)) \otimes B \xrightarrow{\gamma_{F'(A),B}} F(F'(A) \otimes B) \xrightarrow{F(\gamma'_{A,B})} F(F'(A \otimes B));$$

the tensor product of morphisms $\theta \colon F \to F'$ and $\theta' \colon G \to G'$ is the composite

$$F(G(A)) \xrightarrow{\theta_{G(A)}} F'(G(A)) \xrightarrow{F'(\theta'_A)} F'(G'(A)),$$

which again satisfies (1.35). You can check that $((F, \gamma) \otimes (F', \gamma')) \otimes (F'', \gamma'') = (F, \gamma) \otimes ((F', \gamma') \otimes (F'', \gamma''))$, and that the category accepts a strict monoidal structure, with unit object given by the identity functor on $\mathbf{C}$.

Now consider the following functor $L \colon \mathbf{C} \to \mathbf{D}$:

$$L(A) = (A \otimes -, \alpha_{A,-,-}) \qquad\qquad L(f) = f \otimes -$$

Think of this functor as 'multiplying on the left'. We will show that L is a full and faithful monoidal functor. For faithfulness, if $L(f) = L(g)$ for morphisms f, g in $\mathbf{C}$, that means $f \otimes \mathrm{id}_I = g \otimes \mathrm{id}_I$, and so $f = g$ by naturality of ρ.For fullness, let $\theta \colon L(A) \to L(B)$ be a morphism in $\mathbf{D}$, and define $f \colon A \to B$ as the composite

$$A \xrightarrow{\rho_A^{-1}} A \otimes I \xrightarrow{\theta_I} B \otimes I \xrightarrow{\rho_B} B.$$

Then the following diagram commutes:

$$\begin{tikzcd}
A \otimes C \arrow[r, "\rho_A^{-1} \otimes \mathrm{id}_C"] \arrow[d, "f \otimes \mathrm{id}_C"] & (A \otimes I) \otimes C \arrow[r, "\alpha_{A,I,C}"] \arrow[d, "\theta_I \otimes \mathrm{id}_C"] & A \otimes (I \otimes C) \arrow[r, "\mathrm{id}_A \otimes \lambda_C"] \arrow[d, "\theta_{I \otimes C}"] & A \otimes C \arrow[d, "\theta_C"'] \\
B \otimes C \arrow[r, "\rho_B^{-1} \otimes \mathrm{id}_C"'] & (B \otimes I) \otimes C \arrow[r, "\alpha_{B,I,C}"'] & B \otimes (I \otimes C) \arrow[r, "\mathrm{id}_B \otimes \lambda_C"'] & B \otimes C
\end{tikzcd}$$

The left square commutes by definition of f, the middle square by (1.35), and the right square by naturality of θ. Moreover, the rows both equal the identity by the triangle identity (1.1). Hence $\theta_C = f \otimes \mathrm{id}_C$, and so $\theta = L(f)$.

Next we show that L is a monoidal functor.Define the isomorphism $L_0 \colon I \to L(I)$ to be λ^{-1}, and define $(L_2)_{A,B} \colon L(A) \otimes L(B) \to L(A \otimes B)$ by

$$\alpha^{-1}_{A,B,-} \colon \big(A \otimes (B \otimes -), (A \otimes \alpha_{B,-,-}) \circ \alpha_{A,B\otimes -,-}\big) \to \big((A \otimes B) \otimes -, \alpha_{A\otimes B,-,-}\big).$$

These form a well-defined morphism in $\mathbf{D}$, because equation (1.35) is just the pentagon equation (1.2) of $\mathbf{C}$.Verifying equations (1.30) comes down to the fact that $\lambda_I = \rho_I$ (see Exercise 1.4.13) and the triangle equation (1.1). Because $\mathbf{D}$ is strict, equation (1.29) comes down to the pentagon identity (1.2) of $\mathbf{C}$.

Finally, let $\mathbf{C_s}$ be the subcategory of $\mathbf{D}$ containing all objects that are isomorphic to those of the form $L(A)$, and all morphisms between them. Then $\mathbf{C_s}$ is still a strict monoidal category, and L restricts to a functor $L \colon \mathbf{C} \to \mathbf{C_s}$ that is still monoidal, full, and faithful, but is additionally essentially surjective on objects by construction. Thus $L \colon \mathbf{C} \to \mathbf{C_s}$ is a monoidal equivalence. □

1.3.4 The coherence theorem

The Coherence Theorem derives from the Strictification Theorem. To state the former, we have to be more precise about the equations that we coyly called 'well-typed' earlier in Theorem 1.2.

To do so, we will talk about different ways to parenthesize a finite list of things. More precisely, define *bracketings* in $\mathbf{C}$ inductively: $()$ is the empty bracketing; for any object A in $\mathbf{C}$ there is a bracketing A; and if v and w are bracketings, then so is $(v \otimes w)$. For example, $v = (A \otimes B) \otimes (C \otimes D)$ and $w = ((A \otimes B) \otimes C) \otimes D$ are different bracketings, even though they could denote the same object of $\mathbf{C}$.

Actually, a bracketing is independent of the objects and even of the category. So for example, we may use the notation $v(W, X, Y, Z) = (W \otimes X) \otimes (Y \otimes Z)$ to define a procedure v that operates on any quartet of objects. Thus it also makes sense to talk about transformations $\theta \colon v \Rightarrow w$ built from coherence isomorphisms.

Theorem 1.39 (Coherence for monoidal categories)**.** *Let $v(A, \dots, Z)$ and $w(A, \dots, Z)$ be bracketings in a monoidal category $\mathbf{C}$. Any two transformations $\theta, \theta' \colon v \Rightarrow w$ built from α, α^{-1}, λ, λ^{-1}, ρ, ρ^{-1}, id, $\otimes$, and $\circ$ are equal.*

Proof. Let $L \colon \mathbf{C} \to \mathbf{C_s}$ be the monoidal equivalence from Theorem 1.38. Inductively define a morphism $L_v \colon v(L(A), \dots, L(Z)) \to L(v(A, \dots, Z))$ in $\mathbf{C_s}$ by setting $L_{()} = L_0$, $L_A = \mathrm{id}_{L(A)}$, and $L_{(x \otimes y)} = L_2 \circ (L_x \otimes L_y)$. Define L_w similarly. Then the following diagram in $\mathbf{C_s}$ commutes:

$$\begin{tikzcd}
v(L(A), \dots, L(Z)) \arrow[r, "\theta_{(L(A),\dots,L(Z))}"] \arrow[d, "L_v"'] & w(L(A), \dots, L(Z)) \arrow[d, "L_w"] \\
L(v(A, \dots, Z)) \arrow[r, "L(\theta_{(A,\dots,Z)})"'] & L(w(A, \dots, Z))
\end{tikzcd}$$

The same diagram for θ' commutes similarly. But as $\mathbf{C_s}$ is a strict monoidal category, and θ and θ' are built from coherence isomorphisms, we must have $\theta_{(L(A),\dots,L(Z))} = \theta'_{(L(A),\dots,L(Z))} = \mathrm{id}$. Since L_v and L_w are by construction isomorphisms, it follows from the diagram above that $L(\theta_{(A,\dots,Z)}) = L(\theta'_{(A,\dots,Z)})$. Finally, L is an equivalence and hence faithful, so $\theta_{(A,\dots,Z)} = \theta'_{(A,\dots,Z)}$. □

Notice that the transformations θ, θ' in the previous theorem have to go from a single bracketing v to a single bracketing w. Suppose we have an object A for which $A \otimes A = A$. Then $A \xrightarrow{\mathrm{id}_A} A$ and $A \xrightarrow{\alpha_{A,A,A}} A$ are both well-defined morphisms. But equating them does not give a well-formed equation, as they do not give rise to transformations from the same bracketing to the same bracketing.

1.3.5 Braided monoidal functors

Versions of the Strictification Theorem 1.38 and the Coherence Theorem 1.2 still hold for braided monoidal categories and symmetric monoidal categories. In fact, they link nicely with the Correctness Theorems for the graphical calculus, Theorem 1.18 and Theorem 1.22. We will not detail the proofs, and just discuss the statements here.

We call a braided monoidal category *strict* when the underlying monoidal category is strict. This does not mean that the braiding should be the identity.

Theorem 1.40 (Strictification for braided monoidal categories)**.** *Every braided monoidal category has a braided monoidal equivalence to a braided strict monoidal category. Every symmetric monoidal category has a symmetric monoidal equivalence to a symmetric strict monoidal category.* □

To state the coherence theorem in the braided and symmetric case, we again have to be precise about what 'well-formed' equations are. Consider a morphism f in a braided monoidal category that is built from the coherence isomorphisms and the braiding, and their inverses, using identities and tensor products. Using the graphical calculus of braided monoidal categories, we can always draw it as a *braid*, such as the pictures in equations (1.19) and (1.22). By the correctness of the graphical calculus for braided monoidal categories, Theorem 1.18, this picture defines a morphism g built from coherence isomorphisms and the braiding in a canonical bracketing, say with all brackets to the left. Moreover, up to isotopy of the picture this is the unique such morphism g. We call that morphism g, or equivalently the isotopy class of its picture, the *underlying braid* of the original morphism f. Since the underlying braid is merely about the connectivity, and not about the actual objects, it lifts from morphisms to bracketings.

Corollary 1.41 (Coherence for braided monoidal categories)**.** *Let* $v(A, \ldots, Z)$ *and* $w(A, \ldots, Z)$ *be bracketings in a braided monoidal category* $\mathbf{C}$*. Any two transformations* $\theta, \theta' \colon v \Rightarrow w$ *built from* α*,* α^{-1}*,* λ*,* λ^{-1}*,* ρ*,* ρ^{-1}*,* σ*,* σ^{-1}*,* id*,* $\otimes$*, and* $\circ$*, are equal if and only if they have the same underlying braid.*

Proof. By definition of the underlying braid, this follows immediately from the Coherence Theorem 1.39 for monoidal categories and the Correctness Theorem 1.18 of the graphical calculus for braided monoidal categories. □

For symmetric monoidal categories, we can simplify the underlying braid to an *underlying permutation*. It is a bijection between the set $\{1, \ldots, n\}$ and itself, where n is the number of objects in the bracketing, namely precisely the bijection that is indicated by the graphical calculus when we draw the bracketing.

Corollary 1.42 (Coherence for symmetric monoidal categories)**.** *Let* $v(A, \ldots, Z)$ *and* $w(A, \ldots, Z)$ *be bracketings in a symmetric monoidal category* $\mathbf{C}$*. Any two transformations* $\theta, \theta' \colon v \Rightarrow w$ *built from* α*,* α^{-1}*,* λ*,* λ^{-1}*,* ρ*,* ρ^{-1}*,* σ*,* σ^{-1}*,* id*,* $\otimes$*, and* $\circ$*, are equal if and only if they have the same underlying permutation.*

Proof. By definition of the underlying permutation, this follows immediately from Corollary 1.41, and the correctness of the graphical calculus for symmetric monoidal categories, Theorem 1.22. □

1.4 Exercises

Exercise 1.4.1. Let A, B, C, D be objects in a monoidal category. Construct a morphism

$$(((A \otimes I) \otimes B) \otimes C) \otimes D \to A \otimes (B \otimes (C \otimes (I \otimes D))).$$

Can you find another?

Exercise 1.4.2. Convert the following algebraic equations into graphical language. Which would you expect to be true in any symmetric monoidal category?

(a) $(g \otimes \mathrm{id}) \circ \sigma \circ (f \otimes \mathrm{id}) = (f \otimes \mathrm{id}) \circ \sigma \circ (g \otimes \mathrm{id})$ for $A \xrightarrow{f,g} A$.

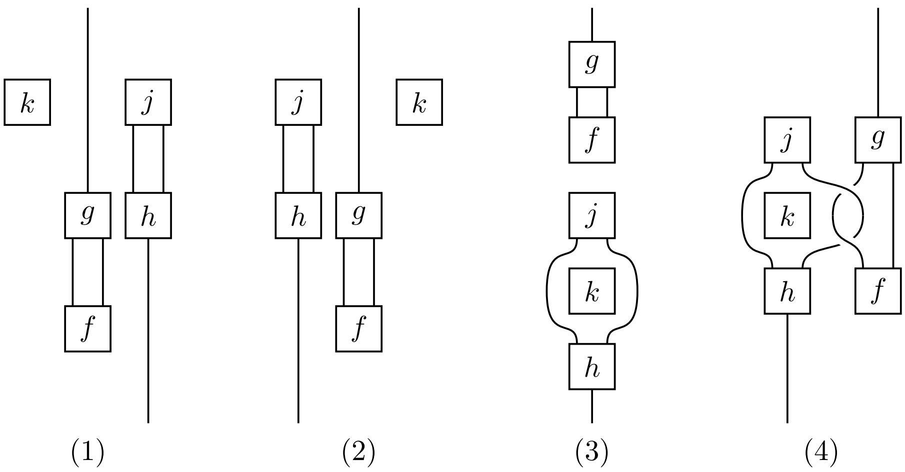
(b) $(f \otimes (g \circ h)) \circ k = (\mathrm{id} \otimes f) \circ ((g \otimes h) \circ k)$, for $A \xrightarrow{k} B \otimes C$, $C \xrightarrow{h} B$ and $B \xrightarrow{f,g} B$.

(c) $(\mathrm{id} \otimes h) \circ g \circ (f \otimes \mathrm{id}) = (\mathrm{id} \otimes f) \circ g \circ (h \otimes \mathrm{id})$, for $A \xrightarrow{f,h} A$ and $A \otimes A \xrightarrow{g} A \otimes A$.

(d) $h \circ (\mathrm{id} \otimes \lambda) \circ (\mathrm{id} \otimes (f \otimes \mathrm{id})) \circ (\mathrm{id} \otimes \lambda^{-1}) \circ g = h \circ g \circ \lambda \circ (f \otimes \mathrm{id}) \circ \lambda^{-1}$, for $A \xrightarrow{g} B \otimes C$, $I \xrightarrow{f} I$ and $B \otimes C \xrightarrow{h} D$.

(e) $\rho_C \circ (\mathrm{id} \otimes f) \circ \alpha_{C,A,B} \circ (\sigma_{A,C} \otimes \mathrm{id}_B) = \lambda_C \circ (f \otimes \mathrm{id}) \circ \alpha^{-1}_{A,B,C} \circ (\mathrm{id} \otimes \sigma_{C,B}) \circ \alpha_{A,C,B}$ for $A \otimes B \xrightarrow{f} I$.

Exercise 1.4.3. Consider the following diagrams in the graphical calculus:

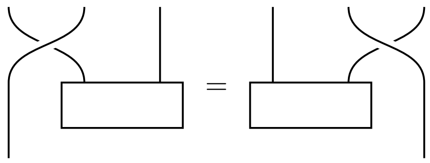


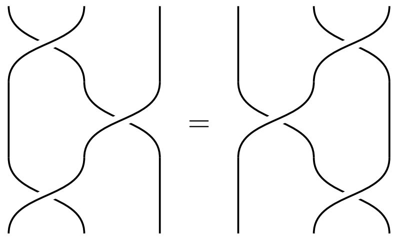
(a) Which of the diagrams (1), (2) and (3) are equal as morphisms in a monoidal category?

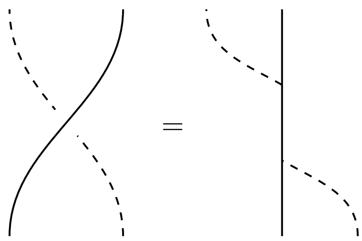
(b) Which of the diagrams (1), (2), (3) and (4) are equal as morphisms in a braided monoidal category?

(c) Which of the diagrams (1), (2), (3) and (4) are equal as morphisms in a symmetric monoidal category?

Exercise 1.4.4. Prove the following graphical equations using the basic axioms of a braided monoidal category, without relying on the coherence theorem.

(a) 

(b) 

(c)  $(\sigma_{A,I} = \lambda_A^{-1} \circ \rho_A)$

Exercise 1.4.5. Look at Definition 0.53 of the Kronecker product.

(a) Show explicitly that the Kronecker product of three 2-by-2 matrices is strictly associative.

(b) We could consider infinite matrices to have rows and columns indexed by cardinal numbers, that is, totally ordered sets, rather than natural numbers as in Definition 0.36. What might go wrong if you try to include infinite-dimensional Hilbert spaces in a strict, skeletal category as in Definition 1.26?

Exercise 1.4.6. Recall that an entangled state of objects A and B is a state of $A \otimes B$ that is not a product state.

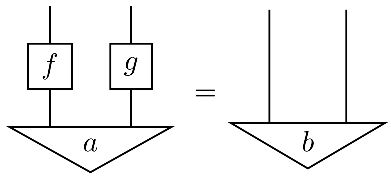
(a) Which of these states of $\mathbb{C}^2 \otimes \mathbb{C}^2$ in $\mathbf{Hilb}$ are entangled?

$$\begin{gathered}
\tfrac{1}{2}\big(|00\rangle + |01\rangle + |10\rangle + |11\rangle\big) \\
\tfrac{1}{2}\big(|00\rangle + |01\rangle + |10\rangle - |11\rangle\big) \\
\tfrac{1}{2}\big(|00\rangle + |01\rangle - |10\rangle + |11\rangle\big) \\
\tfrac{1}{2}\big(|00\rangle - |01\rangle - |10\rangle + |11\rangle\big)
\end{gathered}$$

(b) Which of these states of $\{0,1\} \otimes \{0,1\}$ in $\mathbf{Rel}$ are entangled?

$$\begin{gathered}
\{(0,0),(0,1)\} \\
\{(0,0),(0,1),(1,0)\} \\
\{(0,1),(1,0)\} \\
\{(0,0),(0,1),(1,0),(1,1)\}
\end{gathered}$$

Exercise 1.4.7. We say that two joint states $I \xrightarrow{a,b} A \otimes B$ are *locally equivalent*, written $a \sim b$, if there exist invertible maps $A \xrightarrow{f} A$, $B \xrightarrow{g} B$ such that



(a) Show that $\sim$ is an equivalence relation.

(b) Find all isomorphisms $\{0,1\} \to \{0,1\}$ in $\mathbf{Rel}$.

(c) Write out all 16 states of the object $\{0,1\} \times \{0,1\}$ in $\mathbf{Rel}$.

(d) Use your answer to (b) to group the states of (c) into locally equivalent families. How many families are there? Which of these are entangled?

Exercise 1.4.8. Recall equation (1.12) and its interpretation.

(a) In $\mathbf{FHilb}$, take $A = I$. Let f be the Hadamard gate $\frac{1}{\sqrt{2}}\left(\begin{smallmatrix}1 & 1\\ 1 & -1\end{smallmatrix}\right)$, let a be the $|0\rangle$ state $\left(\begin{smallmatrix}1\\ 0\end{smallmatrix}\right)$, let x be the $\langle 0|$ effect $\left(\begin{smallmatrix}1 & 0\end{smallmatrix}\right)$, and let y be the $\langle 1|$ effect $\left(\begin{smallmatrix}0 & 1\end{smallmatrix}\right)$. Can the history $x \circ f \circ a$ occur? How about $y \circ f \circ a$?

(b) In $\mathbf{Rel}$, take $A = I$. Let R be the relation $\{0,1\} \to \{0,1\}$ given by $\{(0,0),(0,1),(1,0)\}$, let a be the state $\{0\}$, let x be the effect $\{0\}$, and let y be the effect $\{1\}$. Can the history $x \circ R \circ a$ occur? How about $y \circ R \circ a$?

Exercise 1.4.9. This question is about the symmetric monoidal structure on a Cartesian category.

(a) Show that if a category has products and a terminal object, these can be used to construct a monoidal structure.

(b) Show that this monoidal structure can be equipped with a canonical symmetry.

(c) Show that the projection maps of the products are natural for this monoidal structure, meaning that for any two morphisms f, g we have $p_1 \circ (f \otimes g) = f \circ p_1$ and $p_2 \circ (f \otimes g) = g \circ p_2$.

Exercise 1.4.10. Show that $\mathbf{Set}$ is:

(a) a strict monoidal category under $I = \emptyset$ and $A \otimes B = A \cup B$;

(b) a symmetric monoidal category under $I = \emptyset$ and $A \otimes B = A + B + (A \times B)$, where we write $\times$ for Cartesian product of sets, and $+$ for disjoint union of sets.

Exercise 1.4.11. Let $\mathbf{C}$ be an arbitrary category.

(a) Show that functors $F \colon \mathbf{C} \to \mathbf{C}$ and natural transformation between them form a category $[\mathbf{C}, \mathbf{C}]$.

(b) Show that $[\mathbf{C}, \mathbf{C}]$ is a strict monoidal category with tensor product $F \otimes G = G \circ F$, and tensor unit the identity functor.

(c) Find a category $\mathbf{C}$ and functors $F, G \colon \mathbf{C} \to \mathbf{C}$ satisfying $G \circ F \neq F \circ G$. Conclude that the monoidal category $[\mathbf{C}, \mathbf{C}]$ cannot be braided.

Exercise 1.4.12. Let $\mathbf{C}$ and $\mathbf{D}$ be monoidal categories. Suppose that $F\colon \mathbf{C} \to \mathbf{D}$ is a functor, that $(F_2)_{A,B}\colon F(A) \otimes F(B) \to F(A \otimes B)$ is a natural isomorphism satisfying (1.29), and that there exists some isomorphism $\psi\colon I \to F(I)$. Define $F_0\colon I \to F(I)$ as the composite

$$I \xrightarrow{\psi} F(I) \xrightarrow{F(\lambda^{-1})} F(I \otimes I) \xrightarrow{(F_2)^{-1}_{I,I}} F(I) \otimes F(I) \xrightarrow{\psi^{-1} \otimes \mathrm{id}_{F(I)}} I \otimes F(I) \xrightarrow{\lambda_{F(I)}} F(I).$$

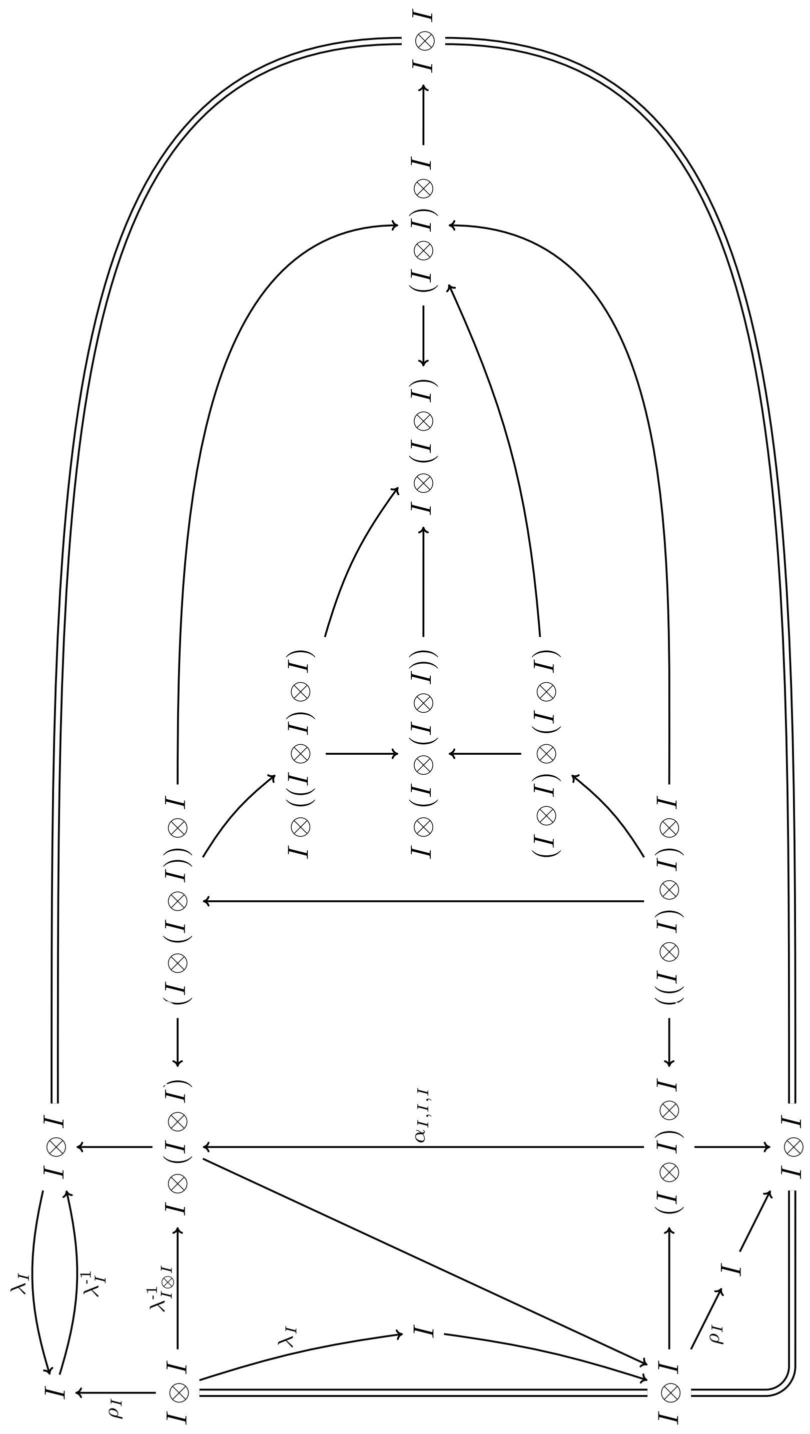
(a) Show that the following composite equals $\mathrm{id}_{F(I) \otimes F(I)}$.

$$\begin{aligned} F(I) \otimes F(I) &\xrightarrow{F(\lambda_I^{-1}) \otimes \mathrm{id}_{F(I)}} F(I \otimes I) \otimes F(I) \\ &\xrightarrow{(F_2)^{-1}_{I,I} \otimes \mathrm{id}_{F(I)}} (F(I) \otimes F(I)) \otimes F(I) \\ &\xrightarrow{\alpha_{F(I),F(I),F(I)}} F(I) \otimes (F(I) \otimes F(I)) \\ &\xrightarrow{\mathrm{id}_{F(I)} \otimes (F_2)_{I,I}} F(I) \otimes F(I \otimes I) \\ &\xrightarrow{\mathrm{id}_{F(I)} \otimes F(\lambda_I)} F(I) \otimes F(I). \end{aligned}$$

(Hint: Insert $\mathrm{id}_{F(I \otimes I)} = (F_2) \circ (F_2)^{-1}_{I,I}$, use naturality of F_2, and the Coherence Theorem 1.2.)

(b) Show that φ_I satisfies (1.30), making F into a monoidal functor.

Exercise 1.4.13. Complete the following proof that $\rho_I = \lambda_I$ in a monoidal category, by labelling every arrow, and indicating for each region whether it follows from the triangle equations, the pentagon equations, naturality, or invertibility.


$I \otimes I$
$(I \otimes I) \otimes I$
$I \otimes (I \otimes I)$
$I \otimes ((I \otimes I) \otimes I)$
$I \otimes (I \otimes (I \otimes I))$
$(I \otimes I) \otimes (I \otimes I)$
$(I \otimes (I \otimes I)) \otimes I$
$((I \otimes I) \otimes I) \otimes I$
$I \otimes I$
$I \otimes (I \otimes I)$
$\alpha_{I,I,I}$
$(I \otimes I) \otimes I$
$I \otimes I$
λ_I
λ_I^{-1}
$\lambda^{-1}_{I \otimes I}$
I
I
ρ_I
I
ρ_I
I
$I \otimes I$
λ_I
$I \otimes I$

Notes and further reading

Symmetric monoidal categories were introduced independently by Bénabou and Mac Lane in 1963 [23, 106]. Early developments revolved around the problem of coherence, and were resolved by Mac Lane's Coherence Theorem 1.2. For a comprehensive treatment, see the textbooks [107, 27]. There are some caveats to our formulation of the Coherence Theorem 1.2 – that all "well-formed" equations are satisfied; see Section 1.3. But for all (our) intents and purposes, we may interpret "well-formed" to mean that both sides of the equation are well-defined compositions with the same domain and codomain. The argument in Proposition 1.35 that skeletality and strictness do not go together is due to Isbell.

The graphical language had probably been an open secret among various researchers, that was mostly used calculations but not in publications. It surfaced in 1971, when Penrose used it to abbreviate tensor contraction calculations [118]; Penrose reported using it already as an undergraduate student. Kelly used it to investigate coherence in 1972 [92]. The graphical calculus was formalized for monoidal categories by Joyal and Street in 1991 [83], who later also generalized it to braided monoidal categories [85]. The latter paper is also the source of the streamlined proof of the Strictification Theorem 1.38. For a modern survey, focusing on soundness and completeness of the graphical calculus, see [133].

The relevance of monoidal categories for quantum theory was emphasized originally by Abramsky and Coecke [4, 35], and was also popularized by Baez [13] in the context of quantum field theory and quantum gravity. Our remarks about the dimensionality of the graphical calculus are a shadow of higher category theory, and are further discussed in Chapter 8.

Chapter 2

Linear structure

Many aspects of linear algebra can be described using categorical structures. This chapter examines abstractions of the base field (in Section 2.1), zero-dimensional spaces, addition of linear operators, direct sums, matrices (in Section 2.2) and inner products (in Section 2.3). We will see how to use these to model important features of quantum mechanics such as classical data, superposition, and measurement, in Section 2.4.

2.1 Scalars

If we begin with the monoidal category **Hilb**, we can extract from it much of the structure of the complex numbers. The monoidal unit object I is given by the complex numbers $\mathbb{C}$, and so morphisms $I \to I$ are linear maps $\mathbb{C} \xrightarrow{f} \mathbb{C}$. Such a map is determined by $f(1)$, since by linearity we have $f(s) = s \cdot f(1)$. So, we have a correspondence between morphisms of type $I \to I$ and the complex numbers. Also, it's easy to check that multiplication of complex numbers corresponds to composition of their corresponding linear maps.

In general, it is often useful to think of the morphisms of type $I \to I$ in a monoidal category as behaving like a field in linear algebra. For this reason, we give them a special name.

Definition 2.1. In a monoidal category, the *scalars* are the morphisms $I \to I$.

A *monoid* is a set A equipped with a multiplication operation, which we write as juxtaposition of elements of A, and a chosen unit element $1 \in A$, satisfying for all $r, s, t \in A$ an associativity law $r(st) = (rs)t$ and a unit law $1s = s = s1$. We will study monoids closely from a categorical perspective in Chapter 4, but for now we note that it is easy to show from the axioms of a category that the scalars form a monoid under composition.

Example 2.2. The monoid of scalars is very different in each of our running example categories.

- In **Hilb**, scalars $\mathbb{C} \xrightarrow{f} \mathbb{C}$ correspond to complex numbers $f(1) \in \mathbb{C}$ as discussed above. Composition of scalars $\mathbb{C} \xrightarrow{f,g} \mathbb{C}$ corresponds to multiplication of complex numbers, as $(g \circ f)(1) = g(f(1)) = f(1) \cdot g(1)$. Hence the scalars in **Hilb** are the complex numbers under multiplication.

- In **Set**, scalars are functions $\{\bullet\} \xrightarrow{f} \{\bullet\}$. There is only one unique such function, namely $\mathrm{id}_{\{\bullet\}} \colon \bullet \mapsto \bullet$, which we will also simply write as 1. Hence the scalars in **Set** form the trivial one-element monoid.

- In **Rel**, scalars are relations $\{\bullet\} \xrightarrow{R} \{\bullet\}$. There are two such relations: $F = \emptyset$ and $T = \{(\bullet, \bullet)\}$. Working out the composition in **Rel** gives the following multiplication table:

	F	T
F	F	F
T	F	T

  Hence we recognize the scalars in **Rel** as the Boolean truth values $\{\texttt{true}, \texttt{false}\}$ under conjunction.

2.1.1 Commutativity

Multiplication of complex numbers is commutative: $st = ts$. It turns out that this holds for scalars in any monoidal category.

Lemma 2.3. *In a monoidal category, the scalars are commutative.*

Proof. Consider the following diagram, for any two scalars $I \xrightarrow{s,t} I$:

$$
\begin{tikzcd}
I \arrow[rr, "s"] \arrow[dr, "t"] \arrow[dd, "\lambda_I^{-1}"', "\rho_I^{-1}"] & & I \arrow[dr, "t"] \arrow[dd, "\lambda_I^{-1}"', "\rho_I^{-1}"] & \\
& I \arrow[rr, "s"] & & I \\
I \otimes I \arrow[rr, "s \otimes \mathrm{id}_I"'] \arrow[dr, "\mathrm{id}_I \otimes t"'] & & I \otimes I \arrow[dr, "\mathrm{id}_I \otimes t"'] & \\
& I \otimes I \arrow[rr, "s \otimes \mathrm{id}_I"'] \arrow[uu, "\lambda_I", "\rho_I"'] & & I \otimes I \arrow[uu, "\lambda_I", "\rho_I"']
\end{tikzcd}
\qquad (2.1)
$$

The four side cells of the cube commute by naturality of λ_I and ρ_I, and the bottom cell commutes by an application of the interchange law of Theorem 1.7. Hence $st = ts$. Note the importance of coherence here, as we rely on the fact that $\rho_I = \lambda_I$. □

Example 2.4. The scalars in our example categories are indeed commutative.

- In **Hilb**: multiplication of complex numbers is commutative.

- In **Set**: $1 \circ 1 = 1 \circ 1$ is trivially commutative.

- In **Rel**: let s, t be Boolean values; then (s and t) is true precisely when (t and s) is true.

2.1.2 Graphical calculus

We draw scalars as circles:

$$s \tag{2.2}$$

Commutativity of scalars then has the following graphical representation:

$$\begin{array}{c} t \\ \\ s \end{array} \quad = \quad \begin{array}{c} s \\ \\ t \end{array} \tag{2.3}$$

The diagrams are isotopic, so it follows from correctness of the graphical calculus that scalars are commutative. Once again, a nontrivial property of monoidal categories follows straightforwardly from the graphical calculus.

2.1.3 Scalar multiplication

Objects in an arbitrary monoidal category do not have to be anything particularly like vector spaces, at least at first glance. Nevertheless, many of the features of the mathematics of vector spaces can be mimicked. For example, if $s \in \mathbb{C}$ is a scalar and f a linear map, then sf is again a linear map, and we can mimic this in general monoidal categories as follows.

Definition 2.5 (Left scalar multiplication)**.** In a monoidal category, for a scalar $I \xrightarrow{s} I$ and a morphism $A \xrightarrow{f} B$, the *left scalar multiplication* $A \xrightarrow{s \bullet f} B$ is the following composite:

$$\begin{tikzcd} A \arrow[r, "s \bullet f"] \arrow[d, "\lambda_A^{-1}"'] & B \\ I \otimes A \arrow[r, "s \otimes f"] & I \otimes B \arrow[u, "\lambda_B"'] \end{tikzcd} \tag{2.4}$$

This abstract scalar multiplication satisfies many properties we are familiar with from scalar multiplication of vector spaces.

Lemma 2.6 (Scalar multiplication)**.** *In a monoidal category, let $I \xrightarrow{s,t} I$ be scalars, and $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$ be arbitrary morphisms. Then the following properties hold:*

(a) $\mathrm{id}_I \bullet f = f$;

(b) $s \bullet t = s \circ t$;

(c) $s \bullet (t \bullet f) = (s \bullet t) \bullet f$;

(d) $(t \bullet g) \circ (s \bullet f) = (t \circ s) \bullet (g \circ f)$.

Proof. These statements all follow straightforwardly from the graphical calculus, thanks to Theorem 1.8. We also give the direct algebraic proofs. Part (a) follows directly from naturality of λ. For part (b), diagram (2.1) shows that $s \circ t = \lambda_I \circ (s \otimes t) \circ \lambda_I^{-1} = s \bullet t$. Part (c) follows from the following diagram that commutes by coherence:

$$\begin{tikzcd}
A \arrow[r, "\mathrm{id}_A"] \arrow[d, "\lambda_A^{-1}"] & A \arrow[r, "s \bullet (t \bullet f)"] \arrow[d, "\lambda_A^{-1}"] & B \arrow[r, "\mathrm{id}_B"] & B \\
I \otimes A \arrow[r, "\mathrm{id}_{I \otimes A}"] \arrow[ddr, "\lambda_I^{-1} \otimes \mathrm{id}_A"'] & I \otimes A \arrow[r, "s \otimes (t \bullet f)"] \arrow[d, "\mathrm{id}_I \otimes \lambda_A^{-1}"] & I \otimes B \arrow[r, "\mathrm{id}_{I \otimes B}"] \arrow[u, "\lambda_B"'] & I \otimes B \arrow[u, "\lambda_B"'] \\
 & I \otimes (I \otimes A) \arrow[r, "s \otimes (t \otimes f)"] \arrow[d, "\alpha_{I,I,A}^{-1}"] & I \otimes (I \otimes B) \arrow[u, "\mathrm{id}_I \otimes \lambda_B"'] & \\
 & (I \otimes I) \otimes A \arrow[r, "(s \otimes t) \otimes f"] & (I \otimes I) \otimes B \arrow[u, "\alpha_{I,I,B}"'] \arrow[uur, "\lambda_I \otimes \mathrm{id}_B"'] &
\end{tikzcd}$$

Part (d) follows from the interchange law of Theorem 1.7. $\square$

Example 2.7. Scalar multiplication looks as follows in our example categories.

- In **Hilb**: if $s \in \mathbb{C}$ is a scalar and $H \xrightarrow{f} K$ a morphism, then $H \xrightarrow{s \bullet f} K$ is the morphism $a \mapsto sf(a)$.
- In **Set**, scalar multiplication is trivial: if $A \xrightarrow{f} B$ is a function, and 1 is the unique scalar, then $\mathrm{id}_1 \bullet f = f$ is again the same function.
- In **Rel**: for any relation $A \xrightarrow{R} B$, we find that $\texttt{true} \bullet R = R$, and $\texttt{false} \bullet R = \emptyset$.

2.2 Superposition

A superposition of qubits $a, b \in \mathbb{C}^2$ is a linear combination $sa + tb$ of them for scalars $s, t \in \mathbb{C}$. The previous section dealt with the scalar multiplication; this section focuses on the addition of vectors. We analyze this abstractly with the help of various categorical structures, just as we did with scalar multiplication.

2.2.1 Zero morphisms

Addition of matrices has a unit, namely the matrix whose entries are all zeroes: adding the zero matrix to any other matrix just results in that other matrix. More generally, between any two vector spaces V, W there is always the zero linear map $V \to W$ given by $a \mapsto 0$, sending every element to the zero element of W (see Definition 0.30 for the definition of the zero element of a vector space.) This linear map is characterized by saying that it factors uniquely through the zero-dimensional vector space $V \to \{0\} \to W$. Specifically, there is a unique linear map $\{0\} \to W$, namely $0 \mapsto 0$, and a unique linear map $V \to \{0\}$, namely $a \mapsto 0$. This characterization makes sense in arbitrary categories.

Definition 2.8 (Zero object, zero morphism)**.** An object 0 is a *zero object* when it is both initial and terminal, that is, when there are unique morphisms $A \to 0$ and $0 \to A$ for any object A. In a category with a zero object, a *zero morphism* $A \xrightarrow{0_{A,B}} B$ is the unique morphism $A \to 0 \to B$ factoring through the zero object.

Lemma 2.9. *Initial, terminal and zero objects are unique up to unique isomorphism.*

Proof. If A and B are initial objects, then there are unique morphisms of type $A \to B$, $B \to A$, $A \to A$ and $B \to B$. So the morphisms $A \to B$ and $B \to A$ must be inverses. A similar argument holds for terminal objects. This immediately implies that zero objects are also unique up to unique isomorphism. □

Lemma 2.10. *Composition with a zero morphism always gives a zero morphism, that is, for any objects A, B and C, and any morphism $A \xrightarrow{f} B$:*

$$f \circ 0_{C,A} = 0_{C,B} \qquad\qquad 0_{B,C} \circ f = 0_{A,C} \tag{2.5}$$

Proof. The composition of $C \xrightarrow{0_{C,A}} A$ and $A \xrightarrow{f} B$ is of type $C \to B$ and factors through the zero object, so by definition must equal $0_{C,A}$. □

Example 2.11. Of our example categories, **Hilb** and **Rel** have zero objects, whereas **Set** does not.

- In **Hilb**, the 0-dimensional vector space is a zero object, and the zero morphisms are the linear maps sending all vectors to the zero vector.
- In **Rel**, the empty set is a zero object, and the zero morphisms are the empty relations.
- In **Set**, the empty set is an initial object, and the one-element set is a terminal object. As they are not isomorphic, **Set** cannot have a zero object.

2.2.2 Superposition rules

In quantum computing, superposing qubit states needs vector addition. More generally, given linear maps $V \xrightarrow{f,g} W$ between vector spaces, their sum $V \xrightarrow{f+g} W$ is another linear map. Such a *superposition rule* can be phrased in terms of categorical structure alone.

Definition 2.12 (Superposition rule)**.** An operation $(f, g) \mapsto f + g$, that is defined for morphisms $A \xrightarrow{f,g} B$ between any objects A and B, is a *superposition rule* if it has the following properties:

- **Commutativity:**

$$f + g = g + f \tag{2.6}$$

- **Associativity:**

$$(f + g) + h = f + (g + h) \tag{2.7}$$

- **Units:** for all A, B there is a unit morphism $A \xrightarrow{u_{A,B}} B$ such that for all $A \xrightarrow{f} B$:

$$f + u_{A,B} = f \tag{2.8}$$

- **Addition is compatible with composition:**

$$(g + g') \circ f = (g \circ f) + (g' \circ f) \tag{2.9}$$

$$g \circ (f + f') = (g \circ f) + (g \circ f') \tag{2.10}$$

- **Units are compatible with composition:** for all $f\colon A \to B$:

$$f \circ u_{A,A} = u_{A,B} = u_{B,B} \circ f \tag{2.11}$$

A superposition rule is sometimes called an *enrichment in commutative monoids* in the category theory literature.

Example 2.13. Both **Hilb** and **Rel** have a superposition rule; **Set** does not.

- In **Hilb** the superposition rule is addition of linear maps: $(f+g)(a) = f(a)+g(a)$.
- In **Rel** the superposition rule is union of subsets: $R + S = R \cup S$. In the matrix representation of relations (0.8), this corresponds to entrywise disjunction.
- In **Set** there cannot be a superposition rule. If there were one, there would be a unit morphism $A \xrightarrow{u_{A,\emptyset}} \emptyset$, but there are no such functions for nonempty sets A.

Superposition rules are intimately connected with zero morphisms.

Lemma 2.14. *In a category with a zero object and a superposition rule, $u_{A,B} = 0_{A,B}$ for any objects A and B.*

Proof. Because units are compatible with composition, $u_{A,B} = u_{0,B} \circ u_{A,0}$. But by definition of zero morphisms, this equals $0_{A,B}$. □

Because of the previous lemma we write $0_{A,B}$ instead of $u_{A,B}$ whenever we are working in such a category. We can see this in action in both **Hilb** and **Rel**: the zero linear map is the unit for addition, and the empty relation is the unit for taking unions.

Lemma 2.15. *If a monoidal category has a zero object and a superposition rule, its scalars form a* commutative semiring with an absorbing zero*, that is, a set equipped with commutative, associative multiplication and addition operations with the following properties:*

$$\begin{aligned}(r+s)t &= rt + st\\ r(s+t) &= rs + rt\\ s + t &= t + s\\ s + 0 &= s\\ s0 = 0 &= 0s\end{aligned}$$

Proof. The first four properties follow directly from Definition 2.12: the first two from (2.9) and (2.10); the third from (2.6); and the fourth from (2.11). The fifth property follows from Lemma 2.14. □

Example 2.16. The previous lemma extends Example 2.7 with addition.

- In **Hilb**, the scalar semiring is the field $\mathbb{C}$ with its usual multiplication and addition.
- In **Rel**, it is the Boolean semiring $\{$`true`, `false`$\}$, with multiplication given by logical conjunction (`and`) and addition given by logical disjunction (`or`).

Finally, given two categories with superposition rules, there is a natural compatibility condition on a functor that goes between them.

Definition 2.17 (Linear functor)**.** Given categories $\mathbf{C}, \mathbf{D}$ with superposition rules, a functor $F : \mathbf{C} \to \mathbf{D}$ is *linear* when $F(f + g) = F(f) + F(g)$ for all morphisms f, g in $\mathbf{C}$ with the same domain and codomain.

2.2.3 Biproducts

Direct sums $V \oplus W$ provide a way to "glue together" the vector spaces V and W. The constituent vector spaces form part of the direct sum via the injection maps $V \to V \oplus W$ and $W \to V \oplus W$ given by $a \mapsto (a, 0)$ and $b \mapsto (0, b)$. At the same time, the direct sum is completely determined by its parts via the projection maps $V \oplus W \to V$ and $V \oplus W \to W$ given by $(a, b) \mapsto a$ and $(a, b) \mapsto b$. Moreover, the latter reconstruction operation can undo the former deconstruction operation because $(a, b) = (a, 0) + (0, b)$. Superposition rules help phrase this structure in any category.

Definition 2.18 (Biproducts)**.** In a category with a zero object and a superposition rule, the *biproduct* of two objects A_1 and A_2 is an object $A_1 \oplus A_2$ equipped with injection morphisms $A_n \xrightarrow{i_n} A_1 \oplus A_2$ and projection morphisms $A_1 \oplus A_2 \xrightarrow{p_n} A_n$ for $n = 1, 2$, satisfying

$$\mathrm{id}_{A_n} = p_n \circ i_n \tag{2.12}$$

$$0_{A_n, A_m} = p_m \circ i_n \tag{2.13}$$

$$\mathrm{id}_{A_1 \oplus A_2} = i_1 \circ p_1 + i_2 \circ p_2 \tag{2.14}$$

for all $m \neq n$. This generalizes to an arbitrary finite number of objects; the nullary case, the biproduct of no objects, is the zero object.

Biproducts, if they exist, allow us to 'glue' objects together to form a larger compound object. The injections i_n show how the original objects form parts of the biproduct; the projections p_n show how we can transform the biproduct into either of the original objects; and the equation (2.14) indicates that these original objects together form the whole of the biproduct. A biproduct $A_1 \oplus A_2$ acts simultaneously as a product with projections p_n, and a coproduct with injections i_n.

Lemma 2.19. *If $A_1 \oplus A_2$ is a biproduct in a category with a zero object and a superposition rule, with injections $A_1 \xrightarrow{i_1} A_1 \oplus A_2 \xleftarrow{i_2} A_2$ and projections $A_1 \xleftarrow{p_1} A_1 \oplus A_2 \xrightarrow{p_2} A_2$, then it is also a product with projections p_1, p_2, and a coproduct with injections i_1, i_2.*

Proof. We have to verify the universal property of Definition 0.22 of products. Let $B \xrightarrow{f_n} A_n$ be arbitrary morphisms. Define $\begin{pmatrix} f_1 \\ f_2 \end{pmatrix}$ to be $B \xrightarrow{i_1 \circ f_1 + i_2 \circ f_2} A_1 \oplus A_2$. Then:

$$p_1 \circ \begin{pmatrix} f_1 \\ f_2 \end{pmatrix} \overset{(2.10)}{=} p_1 \circ i_1 \circ f_1 + p_1 \circ i_2 \circ f_2 \overset{\substack{(2.12)\\(2.13)}}{=} f_1 + 0 \overset{(2.8)}{=} f_1,$$

and similarly $p_2 \circ \begin{pmatrix} f_1 \\ f_2 \end{pmatrix} = f_2$. Suppose $B \xrightarrow{g} A_1 \oplus A_2$ satisfies $p_n \circ g = f_n$. Then

$$g \overset{(2.14)}{=} (i_1 \circ p_1 + i_2 \circ p_2) \circ g \overset{(2.9)}{=} i_1 \circ p_1 \circ g + i_2 \circ p_2 \circ g = i_1 \circ f_1 + i_2 \circ f_2,$$

so this is the unique morphisms satisfying those constraints. The argument for coproducts is the same, just with all the arrows reversed. □

Since they are given by categorical product, biproducts *aren't* a good choice of monoidal product if we want to model quantum mechanics: all joint states are product states (see also Exercise 2.5.2), and there can be no correlations between different factors. However, this means that biproducts are suitable to model classical information, by 'carving an object into different classical brances'; and Chapter 4 will discuss this in more depth. The biproduct of a pair of objects is unique up to a unique isomorphism, by a similar reasoning to Lemma 2.9.

Example 2.20. Both **Hilb** and **Rel** have biproducts of finitely many objects, while **Set** has no superposition rule so cannot have any biproducts.

- In **Hilb**, the direct sum of Hilbert spaces provides biproducts. Projections $p_H \colon H \oplus K \to H$ and $p_K \colon H \oplus K \to K$ are given by $(a, b) \mapsto a$ and $(a, b) \mapsto b$. Injections $i_H \colon H \to H \oplus K$ and $i_K \colon K \to H \oplus K$ are given by $a \mapsto (a, 0)$ and $b \mapsto (0, b)$.
- In **Rel**, the disjoint union $A+B$ of sets provides biproducts. Projections $A+B \to A$ and $A+B \to B$ are given by $a \sim a$ and $b \sim b$. Injections $A \to A+B$ and $B \to A+B$ are given by $a \sim a$ and $b \sim b$.

The definition of biproducts above seemed to rely on a chosen superposition rule, but this is only superficial: the presence of biproducts renders superposition rules unique.

Lemma 2.21 (Unique superposition)**.** *If a category has biproducts, then it has a unique superposition rule.*

Proof. Write $+$ and $\boxplus$ for any two superposition rules. Then we do the following computation for any $A \xrightarrow{f,g} B$, where $A \xrightarrow{i_1,i_2} A \oplus A \xrightarrow{p_1,p_2} A$ are the injections and projections for a biproduct:

$$\begin{aligned}
f + g &= (f \boxplus 0_{A,B}) + (0_{A,B} \boxplus g) \\
&= \big((f \circ p_1 \circ i_1) \boxplus (f \circ p_1 \circ i_2)\big) + \big((g \circ p_2 \circ i_1) \boxplus (g \circ p_2 \circ i_2)\big) \\
&= \big((f \circ p_1) \circ (i_1 \boxplus i_2)\big) + \big((g \circ p_2) \circ (i_1 \boxplus i_2)\big) \\
&= \big((f \circ p_1) + (g \circ p_2)\big) \circ (i_1 \boxplus i_2) \\
&= \big(((f \circ p_1) + (g \circ p_2)) \circ i_1\big) \boxplus \big(((f \circ p_1) + (g \circ p_2)) \circ i_2\big) \\
&= \big((f \circ p_1 \circ i_1) + (g \circ p_2 \circ i_1)\big) \boxplus \big((f \circ p_1 \circ i_2) + (g \circ p_2 \circ i_2)\big) \\
&= (f + 0_{A,B}) \boxplus (0_{A,B} + g) \\
&= f \boxplus g
\end{aligned}$$

Note that the full biproduct structure is not needed here, so the hypothesis could be weakened. □

In **Hilb** this means that addition of linear maps is determined by the structure of direct sums of Hilbert spaces, and in **Rel** it means that disjoint union of relations is determined by the structure of disjoint unions of sets.

Since biproducts are defined by equations involving composition and addition, they are preserved by any functor which is linear in the sense of Definition 2.17.

Definition 2.22 (Biproduct preservation)**.** A functor $F\colon \mathbf{C} \to \mathbf{D}$ between categories with zero objects and superposition rules *preserves biproducts* if $F(A \oplus B)$ is a biproduct with injections $F(i_A)$ and $F(i_B)$ and projections $F(p_A)$ and $F(p_B)$ in $\mathbf{D}$ whenever $A \oplus B$ is a biproduct with injections i_A and i_B and projections p_A and p_B in $\mathbf{C}$.

Proposition 2.23. *Let $\mathbf{C}$ be a category with biproducts and a zero object, and suppose that a functor $F\colon \mathbf{C} \to \mathbf{D}$ preserves zero objects. Then F preserves biproducts if and only if it is linear.*

Proof. Suppose the functor preserves biproducts. Then for a biproduct $(A \oplus A, i_1, i_2, p_1, p_2)$ in $\mathbf{C}$, considering equation (2.14) for both this biproduct and its image in F gives $F((i_1 \circ p_1) + (i_2 \circ p_2) = F(i_1 \circ p_1) + F(i_2 \circ p_2)$, which we refer to as $(*)$. Then F is linear, because for any morphisms $A \xrightarrow{f,g} B$:

$$\begin{aligned}
&F(f+g) \\
&\overset{(2.8)}{=} F(f + 0_{A,A} + 0_{A,A} + g) \\
&\overset{(2.13)}{=} F((f \circ p_1 \circ i_1) + (g \circ p_2 \circ i_1) + (f \circ p_1 \circ i_2) + (g \circ p_2 \circ i_2)) \\
&\overset{\substack{(2.9)\\(2.10)}}{=} F\big(((f \circ p_1) + (g \circ p_2)) \circ (i_1 + i_2)\big) \\
&\overset{(2.14)}{=} F\big(((f \circ p_1) + (g \circ p_2)) \circ ((i_1 \circ p_1) + (i_2 \circ p_2)) \circ (i_1 + i_2)\big) \\
&= F((f \circ p_1) + (g \circ p_2)) \circ F((i_1 \circ p_1) + (i_2 \circ p_2)) \circ F(i_1 + i_2) \\
&\overset{(*)}{=} F((f \circ p_1) + (g \circ p_2)) \circ (F(i_1 \circ p_1) + F(i_2 \circ p_2)) \circ F(i_1 + i_2) \\
&\overset{\substack{(2.9)\\(2.10)}}{=} F((f \circ p_1) + (g \circ p_2)) \circ F(i_1 \circ p_1) \circ F(i_1 + i_2) \\
&\qquad\quad + F((f \circ p_1) + (g \circ p_2)) \circ F(i_2 \circ p_2) \circ F(i_1 + i_2) \\
&= F\big(((f \circ p_1) + (g \circ p_2)) \circ i_1 \circ p_1 \circ (i_1 + i_2)\big) \\
&\qquad\quad + F\big(((f \circ p_1) + (g \circ p_2)) \circ i_2 \circ p_2 \circ (i_1 + i_2)\big) \\
&\overset{\substack{(2.9)\\(2.10)}}{=} F\big((f \circ p_1 \circ i_1 \circ p_1 \circ i_1) + (g \circ p_2 \circ i_1 \circ p_1 \circ i_1) \\
&\qquad\quad + (f \circ p_1 \circ i_1 \circ p_1 \circ i_2) + (g \circ p_2 \circ i_1 \circ p_1 \circ i_2)\big) \\
&\quad + F\big((f \circ p_1 \circ i_2 \circ p_2 \circ i_1) + (g \circ p_2 \circ i_2 \circ p_2 \circ i_1) \\
&\qquad\quad + (f \circ p_1 \circ i_2 \circ p_2 \circ i_2) + (g \circ p_2 \circ i_2 \circ p_2 \circ i_2)\big) \\
&\overset{(2.13)}{=} F(f + 0_{A,B} + 0_{A,B} + 0_{A,B}) + F(0_{A,B} + 0_{A,B} + 0_{A,B} + g) \\
&\overset{(2.8)}{=} F(f) + F(g)
\end{aligned}$$

Conversely, note that biproducts are defined in terms of a finite number of equalities involving composition, zero objects, and the superposition rule. Since all these are preserved by linear functors F, it follows that F will preserve biproducts. □

Natural transformations between linear functors are valued on biproduct objects in terms of their value on the summands.

Proposition 2.24. *Let $\mathbf{C}$ and $\mathbf{D}$ be categories with a zero object and a superposition rule. For linear functors $F, G\colon \mathbf{C} \to \mathbf{D}$ preserving zero, and a natural transformation $\mu\colon F \Longrightarrow G$, then for all objects A and B, $\mu_{A \oplus B}$ is determined by μ_A and μ_B:*

$$\mu_{A \oplus B} = \big(G(i_A) \circ \mu_A \circ F(p_A)\big) + \big(G(i_B) \circ \mu_B \circ F(p_B)\big) \tag{2.15}$$

Proof. Compute:

$$\begin{aligned}
\mu_{A\oplus B} &= \big(G(i_B) \circ (G(i_A) + G(p_B)) \circ G(p_A)\big) \circ \mu_{A\oplus B} \\
&\overset{(2.10)}{=} \big(G(i_A) \circ G(p_A) \circ \mu_{A\oplus B}\big) + \big(G(i_B) \circ G(p_B) \circ \mu_{A\oplus B}\big) \\
&\overset{(0.15)}{=} \big(G(i_A) \circ \mu_A \circ F(p_A)\big) + \big(G(i_B) \circ \mu_B \circ F(p_B)\big)
\end{aligned}$$

This completes the proof. □

2.2.4 Matrix notation

Writing linear maps as matrices is an extremely useful technique, and any category with biproducts allows a generalized matrix notation. For example, for morphisms $A \xrightarrow{f} C$, $A \xrightarrow{g} D$, $B \xrightarrow{h} C$ and $B \xrightarrow{j} D$, write

$$A \oplus B \xrightarrow{\begin{pmatrix} f & h \\ g & j \end{pmatrix}} C \oplus D \tag{2.16}$$

as shorthand for the following map:

$$A \oplus B \xrightarrow{(i_C \circ f \circ p_A) + (i_D \circ g \circ p_A) + (i_C \circ h \circ p_B) + (i_D \circ j \circ p_B)} C \oplus D \tag{2.17}$$

Matrices with any finite number of rows and columns are defined similarly.

Definition 2.25 (Matrix). For a collection of maps $A_m \xrightarrow{f_{m,n}} B_n$, where $A_1, \ldots A_M$ and $B_1, \ldots, B_N$ are finite lists of objects, we define their *matrix* as follows:

$$\big(f_{m,n}\big) \equiv \begin{pmatrix} f_{11} & f_{21} & \cdots & f_{M1} \\ f_{12} & f_{22} & \cdots & f_{M1} \\ \vdots & \vdots & \ddots & \vdots \\ f_{1N} & f_{2N} & \cdots & f_{MN} \end{pmatrix} := \sum_{m,n} (i_n \circ f_{m,n} \circ p_m) \tag{2.18}$$

Lemma 2.26 (Matrix representation). *In a category with biproducts, every morphism* $\bigoplus_{m=1}^M A_m \xrightarrow{f} \bigoplus_{n=1}^N B_n$ *has a matrix representation.*

Proof. We construct a matrix representation explicitly, for clarity just in the case when the source and target are biproducts of two objects:

$$\begin{aligned}
f &\overset{(0.2)}{=} \mathrm{id}_{C\oplus D} \circ f \circ \mathrm{id}_{A\oplus B} \\
&\overset{(2.14)}{=} \big((i_C \circ p_C) + (i_D \circ p_D)\big) \circ f \circ \big((i_A \circ p_A) + (i_B \circ p_B)\big) \\
&\overset{\substack{(2.9)\\(2.10)}}{=} i_C \circ (p_C \circ f \circ i_A) \circ p_A + i_C \circ (p_C \circ f \circ i_B) \circ p_B \\
&\qquad + i_D \circ (p_D \circ f \circ i_A) \circ p_A + i_D \circ (p_D \circ f \circ i_B) \circ p_B \\
&\overset{(2.18)}{=} \begin{pmatrix} p_C \circ f \circ i_A & p_C \circ f \circ i_B \\ p_D \circ f \circ i_A & p_D \circ f \circ i_B \end{pmatrix}
\end{aligned}$$

This gives an explicit matrix representation for f. The general case is similar. □

Corollary 2.27 (Entries determine matrices)**.** *In a category with biproducts, morphisms between biproduct objects are equal if and only if their matrix entries are equal.*

Proof. If the matrix entries (2.18) are equal, by definition the morphisms (2.17) are equal. Conversely, if the morphisms are equal, so are the entries, since they are given explicitly in terms of the morphisms in the proof of Lemma 2.26. □

We can use this result to demonstrate that identity morphisms have a familiar matrix representation:

$$\mathrm{id}_{A\oplus B} = \begin{pmatrix} \mathrm{id}_A & 0_{B,A} \\ 0_{A,B} & \mathrm{id}_B \end{pmatrix} \tag{2.19}$$

Matrices compose in the ordinary way familiar from linear algebra, except that morphism composition replaces multiplication, and the superposition rule replaces addition.

Proposition 2.28. *Matrices compose in the following way:*

$$\big(g_{kn}\big) \circ \big(f_{mk}\big) = \big(\textstyle\sum_k g_{kn} \circ f_{mk}\big) \tag{2.20}$$

Proof. Calculate

$$\begin{aligned} \big(g_{kn}\big) \circ \big(f_{mk}\big) &= \left(\sum_{k,n} (i_n \circ g_{kn} \circ p_k)\right) \circ \left(\sum_{m,l} (i_l \circ f_{ml} \circ p_m)\right) \\ &= \sum_{k,l,m,n} (i_n \circ g_{kn} \circ p_k \circ i_l \circ f_{ml} \circ p_m) \\ &= \sum_{k,m,n} (i_n \circ g_{kn} \circ f_{mk} \circ p_m)\,, \end{aligned}$$

which completes the proof. □

Notice that composition of morphisms is non-commutative in general, as is familiar from ordinary matrix composition. For example, it follows from the previous lemma that 2-by-2 matrices compose as follows:

$$\begin{pmatrix} s & p \\ q & r \end{pmatrix} \circ \begin{pmatrix} f & g \\ h & j \end{pmatrix} = \begin{pmatrix} (s\circ f) + (p \circ h) & (s \circ g) + (p \circ j) \\ (q \circ f) + (r \circ h) & (q \circ g) + (r \circ j) \end{pmatrix} \tag{2.21}$$

Example 2.29. Consider this matrix notation in our example categories.

- In **Hilb**, the matrix notation gives block matrices between direct sums of Hilbert spaces, and ordinary matrix multiplication.
- In **Rel**, we can think of relations as matrices with entries in $\{\texttt{false}, \texttt{true}\}$, as explored in Section 0.1.3.

2.2.5 Interaction with monoidal structure

Just like scalar multiplication distributes over a superposition rule, as in Lemma 2.15, you might expect that tensor products distribute in a similar way over biproducts. For vector spaces, this is indeed the case: $U \otimes (V \oplus W)$ and $(U \otimes V) \oplus (U \otimes W)$ are isomorphic. But for general monoidal categories, it isn't true that $f \otimes (g + h) = (f \otimes g) + (f \otimes h)$, or even that $f \otimes 0 = 0$; for counterexamples to both of these, consider the category of Hilbert spaces with direct sum as the tensor product operation. To get this sort of good interaction we require *duals for objects*, which we will encounter in Chapter 3.

However, the following result does hold in general.

Lemma 2.30. *In a monoidal category with a zero object,* $0 \otimes 0 \simeq 0$.

Proof. First note that $I \otimes 0$, being isomorphic to 0, is a zero object. Consider the following composites:

$$0 \xrightarrow{\lambda_0^{-1}} I \otimes 0 \xrightarrow{0_{I,0} \otimes \mathrm{id}_0} 0 \otimes 0$$
$$0 \otimes 0 \xrightarrow{0_{0,I} \otimes \mathrm{id}_0} I \otimes 0 \xrightarrow{\lambda_0} 0$$

Composing them in one direction we obtain a morphism of type $0 \to 0$, which is necessarily id_0 as 0 is a zero object. Composing in the other direction also gives the identity:

$$\begin{tikzcd}
0 \otimes 0 \arrow[rr, "0_{0,I} \otimes \mathrm{id}_0"] \arrow[d, "{\begin{array}{l} 0_{0,0} \otimes \mathrm{id}_0 \\ = \mathrm{id}_0 \otimes \mathrm{id}_0 \\ = \mathrm{id}_{0 \otimes 0} \end{array}}"'] & & I \otimes 0 \arrow[d, "\mathrm{id}_{I \otimes 0}"'] \arrow[dr, "\lambda_0"] & \\
& & & 0 \arrow[dl, "\lambda_0^{-1}"] \\
0 \otimes 0 & & I \otimes 0 \arrow[ll, "0_{I,0} \otimes \mathrm{id}_0"] &
\end{tikzcd}$$

Hence $0 \otimes 0$ is isomorphic to a zero object, and so is itself a zero object. □

2.3 Daggers

In Definition 0.43 of the category of Hilbert spaces, one aspect seems strange: inner products are not used in a central way. This leaves a gap in our categorical model, since inner products play a central role in quantum theory. In this section we will see how inner products can be described abstractly using a *dagger*, a contravariant involutive endofunctor on the category that is compatible with the monoidal structure. The motivation is the construction of the adjoint of a linear map between Hilbert spaces, which as we will see encodes all the information about the inner products.

2.3.1 Dagger categories

To describe inner products abstractly, begin by thinking about *adjoints*. As explored in Section 0.2.4, any bounded linear map $H \xrightarrow{f} K$ between Hilbert spaces has a unique adjoint, which is another bounded linear map $K \xrightarrow{f^\dagger} H$. The assignment $f \mapsto f^\dagger$ is functorial.

Definition 2.31. On **Hilb**, the functor *taking adjoints* $\dagger\colon \mathbf{Hilb} \to \mathbf{Hilb}$ is the contravariant functor that takes objects to themselves, and morphisms to their adjoints as bounded linear maps.

For $\dagger$ to be a contravariant functor it must satisfy the equation $(g \circ f)^\dagger = f^\dagger \circ g^\dagger$and send identities to identities, which is indeed the case for this operation. Furthermore it must be the identity on objects, meaning that $\mathrm{id}_H{}^\dagger = \mathrm{id}_H$ for all objects H, and it must be involutive, meaning that $(f^\dagger)^\dagger = f$ for all morphisms f.

Knowing all adjoints suffices to reconstruct the inner products on Hilbert spaces. To see how this works, let $\mathbb{C} \xrightarrow{a,b} H$ be states of some Hilbert space H. The following calculation shows that the scalar $\mathbb{C} \xrightarrow{b} H \xrightarrow{a^\dagger} \mathbb{C}$ is equal to the inner product $\langle a|b\rangle$:

$$(\mathbb{C} \xrightarrow{b} H \xrightarrow{a^\dagger} \mathbb{C}) = a^\dagger(b(1)) \overset{(0.26)}{=} \langle 1|a^\dagger(b(1))\rangle \overset{(0.27)}{=} \langle a|b\rangle \tag{2.22}$$

So the functor construction adjoints contains all the information required to reconstruct the inner products on our Hilbert spaces. Since the functor is defined in terms of inner products in the first place, knowing the functor taking adjoints is equivalent to knowing the inner products. This correspondence suggests how to generalize the idea of inner products to arbitrary categories.

Definition 2.32 (Dagger, dagger category)**.** A *dagger* on a category $\mathbf{C}$ is an involutive contravariant functor $\dagger\colon \mathbf{C} \to \mathbf{C}$ that is the identity on objects. A *dagger category* is a category equipped with a dagger.

A contravariant functor is therefore a dagger exactly when it has the following properties:

$$(g \circ f)^\dagger = f^\dagger \circ g^\dagger \tag{2.23}$$

$$\mathrm{id}_H{}^\dagger = \mathrm{id}_H \tag{2.24}$$

$$(f^\dagger)^\dagger = f \tag{2.25}$$

The identity-on-objects and contravariant properties mean that if f has type $A \to B$, then $f^\dagger$ has type $B \to A$. The involutive property says that $(f^\dagger)^\dagger = f$.

The canonical dagger on **Hilb** is the functor taking adjoints. **Rel** also has a canonical dagger.

Definition 2.33. The dagger structure on **Rel** is given by relational converse: for $S \xrightarrow{R} T$, define $T \xrightarrow{R^\dagger} S$ by setting $t\,R^\dagger\,s$ if and only if $s\,R\,t$.

The category **Set** cannot be made into a dagger category: writing $|A|$ for the cardinality of a set A, the set of functions $\mathbf{Set}(A, B)$ contains $|B|^{|A|}$ elements, whereas $\mathbf{Set}(B, A)$ contains $|A|^{|B|}$ elements. A dagger would give an bijection between these sets for all A and B, which is impossible.

Another important non-example is **Vect**, the category of complex vector spaces and linear maps. For an infinite-dimensional complex vector space V, the set $\mathbf{Vect}(\mathbb{C}, V)$ has a strictly smaller cardinality than the set $\mathbf{Vect}(V, \mathbb{C})$, so no dagger is possible. The category **FVect** containing only finite-dimensional objects *can* be equipped with a dagger: one way to do this is by choosing an inner product on every object, and then constructing the associated adjoints. However, there is no *canonical* dagger.

A one-object dagger category is also called an *involutive monoid*. It consists of a set M together with an element $1 \in M$ and functions $M \times M \xrightarrow{\cdot} M$ and $M \xrightarrow{\dagger} M$ satisfying $1a = a = a1$, $a(bc) = (ab)c$, $(ab)^\dagger = b^\dagger a^\dagger$, and $(a^\dagger)^\dagger = a$ for all $a, b, c \in M$.

In a dagger category we give special names to some basic properties of morphisms. These generalize the terms in Definition 0.47 usually reserved for bounded linear maps between Hilbert spaces.

Definition 2.34. A morphism $A \xrightarrow{f} B$ in a dagger category is:

- the *adjoint* of $B \xrightarrow{g} A$ when $g = f^\dagger$;
- *self-adjoint* when $f = f^\dagger$ (and $A = B$);
- *idempotent* when $f = f \circ f$ (and $A = B$);
- a *projection* when it is idempotent and self-adjoint;
- *unitary* when both $f^\dagger \circ f = \mathrm{id}_A$ and $f \circ f^\dagger = \mathrm{id}_B$;
- an *isometry* when $f^\dagger \circ f = \mathrm{id}_A$;
- a *partial isometry* when $f^\dagger \circ f$ is a projection;
- *positive* when $f = g^\dagger \circ g$ for some morphism $A \xrightarrow{g} C$ (and $A = B$).

If a category carries an important structure, it is often fruitful to require that the constructions one makes are compatible with that structure. The dagger is an important structure for us, and for most of this book we will require compatibility with it. This principle guides the search for good definitions, and we summarize it as the *way of the dagger*. Sometimes this compatibility comes for free.

Lemma 2.35. *In a dagger category with a zero object,* $0^\dagger_{A,B} = 0_{B,A}$.

Proof. Immediately from functoriality:

$$0^\dagger_{A,B} = (A \to 0 \to B)^\dagger = (B \to 0 \to A) = 0_{B,A} \qquad \square$$

The following result also has an easy proof.

Lemma 2.36. *In a dagger category, if an object is initial or terminal, then it is a zero object.*

Proof. If A is an initial object, then that means $\mathrm{Hom}(A, B)$ has cardinality 1 for every object B. The dagger functor gives an isomorphism $\mathrm{Hom}(A, B) \simeq \mathrm{Hom}(B, A)$, and so it follows that $\mathrm{Hom}(B, A)$ also has cardinality 1 for every object B, and we conclude that A is in fact a zero object. A similar argument holds for the hypothesis that A is a terminal object. $\square$

2.3.2 Monoidal dagger categories

We start by looking at cooperation between dagger structure and monoidal structure. For matrices $H_1 \xrightarrow{f_1} K_1$ and $H_2 \xrightarrow{f_2} K_2$, their tensor product $f_1 \otimes f_2$ is given by the Kronecker product, and their adjoints $f_1^\dagger, f_2^\dagger$ are given by conjugate transpose. The order of these two operations is irrelevant: $(f_1 \otimes f_2)^\dagger = f_1^\dagger \otimes f_2^\dagger$. We abstract this behaviour of linear maps to arbitrary monoidal categories.

Definition 2.37 (Monoidal dagger category, braided, symmetric)**.** A *monoidal dagger category* is a dagger category that is also monoidal, such that $(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger$ for all morphisms f and g, and such that all components of associator α and unitors λ and ρ are unitary. A *braided monoidal dagger category* is a monoidal dagger category equipped with a unitary braiding. A *symmetric monoidal dagger category* is a braided monoidal dagger category for which the braiding is a symmetry.

Example 2.38. Both $\mathbf{Hilb}$ and $\mathbf{Rel}$ are symmetric monoidal dagger categories.

- In $\mathbf{Hilb}$, we have $(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger$, since the former is the unique map satisfying

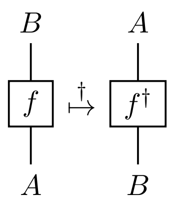
$$\begin{aligned}
&\langle (f \otimes g)^\dagger (a_1 \otimes b_1) | a_2 \otimes b_2 \rangle \\
&\quad = \langle a_1 \otimes b_1 | (f \otimes g)(a_2 \otimes b_2) \rangle \\
&\quad = \langle a_1 \otimes b_1 | f(a_2) \otimes g(b_2) \rangle \\
&\quad = \langle a_1 | f(a_2) \rangle \langle b_1 | g(b_2) \rangle \\
&\quad = \langle f^\dagger(a_1) | a_2 \rangle \langle g^\dagger(b_1) | b_2 \rangle \\
&\quad = \langle (f^\dagger \otimes g^\dagger)(a_1 \otimes b_1) | a_2 \otimes b_2 \rangle.
\end{aligned}$$

- In $\mathbf{Rel}$, a simple calculation for $A \xrightarrow{R} B$ and $C \xrightarrow{S} D$ shows that

$$(R \times S)^\dagger = \{\big((b,d),(a,c)\big) \mid aRb,\ cSd\} = R^\dagger \times S^\dagger.$$

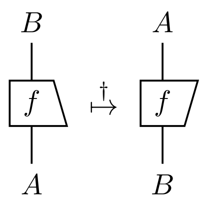
In each case the coherence isomorphisms $\lambda, \rho, \alpha, \sigma$ are also clearly unitary.

We depict taking daggers in the graphical calculus by flipping the graphical representation about a horizontal axis:



(2.26)

To help differentiate between these morphisms, we will draw morphisms in a way that breaks their symmetry. Taking daggers then has the following representation:



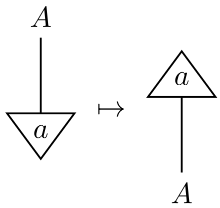
(2.27)

We no longer write the † symbol within the label, as this is already indicated by the orientation of the wedge.

For example, the graphical representation unitarity (see Definition 2.34) is:

(2.28)

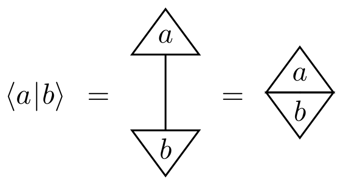
In particular, in a monoidal dagger category, we can use this notation for morphisms $I \xrightarrow{a} A$ representing a state. This represents the adjoint morphism $A \xrightarrow{a^\dagger} I$ as follows:



(2.29)

A state of an object $I \xrightarrow{a} A$ can be thought of as a *preparation* of A by the process a. Dually, a costate $A \xrightarrow{a^\dagger} I$ models the *effect* of eliminating A by the process $a^\dagger$. A dagger gives a correspondence between states and effects.

Equation (2.22) demonstrated how to recover inner products from the ability to take daggers of states. Applying this argument graphically yields the following expression for the inner product $\langle a|b\rangle$ of two states $I \xrightarrow{a,b} H$.



(2.30)

The right-hand side picture is defined by this equation. Notice that it is a rotated form of Dirac's bra-ket notation given on the left-hand side. For this reason, we can think of the graphical calculus for monoidal dagger categories as a generalized Dirac notation.

2.3.3 Dagger biproducts

The adjoint of a block matrix of linear maps is just the conjugate transpose matrix, where all the blocks themselves are also transposed and conjugated. In particular, we get the following adjoints of row and column vectors: $\begin{pmatrix} 1 \\ 0 \end{pmatrix}^\dagger = \begin{pmatrix} 1 & 0 \end{pmatrix}$, and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}^\dagger = \begin{pmatrix} 0 & 1 \end{pmatrix}$. This property of direct sums of Hilbert spaces transfers to biproducts as follows.

Definition 2.39 (Dagger biproducts)**.** In a dagger category with a zero object and a superposition rule, a *dagger biproduct* of objects A and B is a biproduct $A \oplus B$ whose injections and projections satisfy $i_A^\dagger = p_A$ and $i_B^\dagger = p_B$.

Example 2.40. While ordinary biproducts are unique up to isomorphism, dagger biproducts are unique up to *unitary* isomorphism.

- In **Rel**, every biproduct is a dagger biproduct.
- In **Hilb**, dagger biproducts are *orthogonal* direct sums. The notion of orthogonality relies on the inner product, so it makes sense that it can only be described categorically in the presence of a dagger.

You might expect a property like $(f \oplus g)^\dagger = f^\dagger \oplus g^\dagger$ to be needed for good cooperation between biproducts and taking daggers. Dagger biproducts guarantee this good interaction of daggers and the superposition rule; the following two results show that this already follows from Definition 2.39.

Lemma 2.41 (Adjoint of a matrix)**.** *In a dagger category with dagger biproducts, the adjoint of a matrix is its conjugate transpose:*

$$\begin{pmatrix} f_{11} & f_{21} & \cdots & f_{m1} \\ f_{12} & f_{22} & \cdots & f_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ f_{1n} & f_{2n} & \cdots & f_{mn} \end{pmatrix}^\dagger = \begin{pmatrix} f_{11}^\dagger & f_{12}^\dagger & \cdots & f_{1n}^\dagger \\ f_{21}^\dagger & f_{22}^\dagger & \cdots & f_{2n}^\dagger \\ \vdots & \vdots & \ddots & \vdots \\ f_{m1}^\dagger & f_{m2}^\dagger & \cdots & f_{mn}^\dagger \end{pmatrix} \tag{2.31}$$

Proof. Just expand, using the superposition rule and dagger biproduct properties.

$$\begin{aligned}
\begin{pmatrix} f_{11} & f_{21} & \cdots & f_{m1} \\ f_{12} & f_{22} & \cdots & f_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ f_{1n} & f_{2n} & \cdots & f_{mn} \end{pmatrix}^\dagger
&\overset{(2.18)}{=} \left(\sum_{n,m} i_n \circ f_{n,m} \circ i_m^\dagger \right)^\dagger \\
&\overset{(2.14)}{=} \left(\sum_p i_p \circ i_p^\dagger \right) \circ \left(\sum_{n,m} i_n \circ f_{n,m} \circ i_m^\dagger \right)^\dagger \circ \left(\sum_q i_q \circ i_q^\dagger \right) \\
&\overset{\substack{(2.9)\\(2.10)}}{=} \sum_{p,q} i_p \circ i_p^\dagger \circ \left(\sum_{n,m} i_n \circ f_{n,m} \circ i_m^\dagger \right)^\dagger \circ i_q \circ i_q^\dagger \\
&\overset{(2.23)}{=} \sum_{p,q} i_p \circ \left(i_q^\dagger \circ \left(\sum_{n,m} i_n \circ f_{n,m} \circ i_m^\dagger \right) \circ i_p \right)^\dagger \circ i_q^\dagger \\
&\overset{\substack{(2.9)\\(2.10)}}{=} \sum_{p,q} i_p \circ \left(\sum_{n,m} i_q^\dagger \circ i_n \circ f_{n,m} \circ i_m^\dagger \circ i_p \right)^\dagger \circ i_q^\dagger \\
&\overset{(2.12)}{=} \sum_{p,q} i_q \circ (f_{p,q})^\dagger \circ i_p^\dagger
\end{aligned}$$

The last morphism is precisely the right-hand side of the statement. □

It follows that daggers interact well with superposition.

Corollary 2.42. *In a dagger category with dagger biproducts, daggers distribute over addition. For $A \xrightarrow{f,g} B$,*

$$(f+g)^\dagger = f^\dagger + g^\dagger \tag{2.32}$$

Proof. We perform the following calculation:

$$
\begin{aligned}
(f+g)^\dagger &\overset{(2.20)}{=} \left(\begin{pmatrix} f & g \end{pmatrix} \circ \begin{pmatrix} \mathrm{id}_A \\ \mathrm{id}_A \end{pmatrix}\right)^\dagger \overset{(2.23)}{=} \begin{pmatrix} \mathrm{id}_A \\ \mathrm{id}_A \end{pmatrix}^\dagger \circ \begin{pmatrix} f & g \end{pmatrix}^\dagger \\
&\overset{(2.31)}{=} \begin{pmatrix} \mathrm{id}_A & \mathrm{id}_A \end{pmatrix} \circ \begin{pmatrix} f^\dagger \\ g^\dagger \end{pmatrix} \overset{(2.20)}{=} f^\dagger + g^\dagger
\end{aligned}
$$

This completes the proof. □

2.3.4 Anyons

The linear structure of biproducts lets us gives more advanced examples of braided monoidal dagger categories that are our running examples. For example, there is category **Fib** of *Fibonacci anyons*. An *anyon* is a hypothetical particle confined to live in a 2-dimensional plane. Its dynamics over time will yield worldlines in 3 dimensions, and therefore appropriate they form a braided monoidal category. Anyons behave *topologically*, meaning that if two anyon histories are (spatially) isotopic in the braided monoidal graphical calculus, then they have the same effect on the state of the particle.

The following definition of **Fib** gives the monoidal structure only on a restricted family of objects. These *simple objects* generate all objects by taking biproducts, and by Propositions 2.23 and 2.24 this suffices to define the monoidal structure on the entire category up to natural isomorphism.

Definition 2.43. In the dagger category **Fib**:

- **objects** are pairs of natural numbers (n, m);
- **morphisms** $(n, m) \xrightarrow{(f_1, f_2)} (n', m')$ are pairs of matrices $\mathbb{C}^n \xrightarrow{f_1} \mathbb{C}^{n'}$, $\mathbb{C}^m \xrightarrow{f_2} \mathbb{C}^{m'}$, with the obvious componentwise composition and dagger.

The dagger category **Fib** is therefore a product category $\mathbf{Mat}_\mathbb{C} \times \mathbf{Mat}_\mathbb{C}$. Since $\mathbf{Mat}_\mathbb{C}$ has a superposition rule and biproducts, so too does **Fib**, with $(f, g)+(f', g') = (f+f', g+g')$ and $(n, m) \oplus (n', m') = (n+n', m+m')$. Define the *simple objects* of **Fib** to be $I = (1, 0)$ and $\tau = (0, 1)$, and write $nI \oplus m\tau$ for the object (n, m).

The monoidal structure on the simple objects as now defined as follows:

- the **tensor product** is given by the following *fusion rules*:

$$
I \otimes I = I \qquad I \otimes \tau = \tau \qquad \tau \otimes I = \tau \qquad \tau \otimes \tau = I \oplus \tau \tag{2.33}
$$

- the **unit object** is I.

Name the biproduct injections and projections for $\tau \otimes \tau$ as follows:

$$
I \xrightarrow{i_I} \tau \otimes \tau \qquad \tau \xrightarrow{i_\tau} \tau \otimes \tau \qquad \tau \otimes \tau \xrightarrow{p_I} I \qquad \tau \otimes \tau \xrightarrow{p_\tau} \tau \tag{2.34}
$$

The coherence isomorphisms are:

- the **associator** is defined as the sum of the following composites at stage $\alpha_{\tau,\tau,\tau}$, where $\phi = (1+\sqrt{5})/2$ is the *golden ratio*:

$$
(\tau \otimes \tau) \otimes \tau \xrightarrow{p_I \otimes \mathrm{id}_\tau} I \otimes \tau = \tau \xrightarrow{(0, \phi^{-1})} \tau = \tau \otimes I \xrightarrow{\mathrm{id}_\tau \otimes i_I} \tau \otimes (\tau \otimes \tau) \tag{2.35}
$$

$$(\tau\otimes\tau)\otimes\tau \xrightarrow{p_\tau\otimes\mathrm{id}_\tau} \tau\otimes\tau \xrightarrow{p_\tau} \tau \xrightarrow{(0,\phi^{-1/2})} \tau = \tau\otimes I \xrightarrow{\mathrm{id}_\tau\otimes i_I} \tau\otimes(\tau\otimes\tau) \tag{2.36}$$
$$(\tau\otimes\tau)\otimes\tau \xrightarrow{p_I\otimes\mathrm{id}_\tau} I\otimes\tau = \tau \xrightarrow{(0,\phi^{-1/2})} \tau \xrightarrow{i_\tau} \tau\otimes\tau \xrightarrow{\mathrm{id}_\tau\otimes i_\tau} \tau\otimes(\tau\otimes\tau) \tag{2.37}$$
$$(\tau\otimes\tau)\otimes\tau \xrightarrow{p_\tau\otimes\mathrm{id}_\tau} \tau\otimes\tau \xrightarrow{p_\tau} \tau \xrightarrow{(0,-\phi^{-1})} \tau \xrightarrow{i_\tau} \tau\otimes\tau \xrightarrow{\mathrm{id}_\tau\otimes i_\tau} \tau\otimes(\tau\otimes\tau) \tag{2.38}$$
$$(\tau\otimes\tau)\otimes\tau \xrightarrow{p_\tau\otimes\mathrm{id}_\tau} \tau\otimes\tau \xrightarrow{p_I} I \xrightarrow{(1,0)} I \xrightarrow{i_I} \tau\otimes\tau \xrightarrow{\mathrm{id}_\tau\otimes i_\tau} \tau\otimes(\tau\otimes\tau) \tag{2.39}$$

and at other combinations of simple objects, the associator is the identity;

- the **unitor**s are also identities;
- the **braiding** is defined as the following composite at stage $\sigma_{\tau,\tau}$:

$$\tau\otimes\tau \xrightarrow{\begin{pmatrix} p_I \\ p_\tau \end{pmatrix}} I\oplus\tau \xrightarrow{\begin{pmatrix} e^{-\frac{4\pi i}{5}} & 0 \\ 0 & e^{\frac{3\pi i}{5}} \end{pmatrix}} I\oplus\tau \xrightarrow{\begin{pmatrix} i_I & i_\tau \end{pmatrix}} \tau\otimes\tau \tag{2.40}$$

at other pairs of simple objects the braiding is simply the identity. Note that **Fib** is not symmetric monoidal: $\sigma_{\tau,\tau}\circ\sigma_{\tau,\tau}\neq\mathrm{id}$.

Since morphisms are pairs of linear maps $(f_1,f_2)\colon(n,m)\to(n',m')$ for any complex number s we can define the scalar multiple $s(f_1,f_2)=(sf_1,sf_2)$, where sf_1 and sf_2 is the ordinary product of a scalar with a matrix. Our final requirement is that the tensor product is *bilinear*, which means that for morphisms f,f',g,g' and complex numbers s,s',t,t', we have the following:

$$(sf+s'f')\otimes(tg+t'g') = st(f\otimes g)+st'(f\otimes g')+s't(f'\otimes g)+s't'(f'\otimes g') \tag{2.41}$$

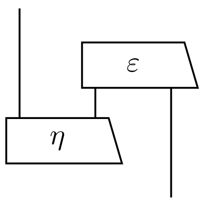
It can be shown that the data above satisfies the pentagon, triangle and hexagon equations. (This is Exercise 2.5.11.) This finishes the definition of the braided monoidal dagger category **Fib**.

Repeated application of the fusion rules (2.33) gives the following n-fold tensor products of τ:

$$\tau^0=I \qquad \tau^1=\tau \qquad \tau^2=I\oplus\tau \qquad \tau^3=I\oplus2\tau \qquad \tau^4=2I\oplus3\tau \qquad \tau^5=3I\oplus5\tau \tag{2.42}$$

The coefficients of τ give the Fibonacci sequence $0,1,1,2,3,5,\ldots$, explaining the terminology.

Let's use this data to evaluate a string diagram in **Fib**. For example, define $\eta=c\,i_I\colon I\to\tau\otimes\tau$, and $\varepsilon=c'p_I\colon\tau\otimes\tau\to\tau$, where c,c' are complex numbers. Then the string diagram



yields the following composite:

$$\tau \xrightarrow{\lambda_\tau^{-1}} I\otimes\tau \xrightarrow{\eta\otimes\mathrm{id}_\tau} (\tau\otimes\tau)\otimes\tau \xrightarrow{\alpha_{\tau,\tau,\tau}} \tau\otimes(\tau\otimes\tau) \xrightarrow{\mathrm{id}_\tau\otimes\varepsilon} \tau\otimes I \xrightarrow{\rho_\tau} \tau \tag{2.43}$$

Expanding the definition of $\alpha_{\tau,\tau,\tau}$, and using the properties of biproducts together with bilinearity, we see that only one of the five composed morphisms contributes, and the composite equals:

$$\tau \xrightarrow{(0,cc'\phi^{-1})} \tau \tag{2.44}$$

This illustrates a general technique for working with **Fib**, and the way that the bilinearity and biproduct structure interact to allow calculations.

2.4 Measurement

The fundamental Born rule of quantum mechanics ties measurements to probabilities. Namely, if a qubit is in state $a \in \mathbb{C}^2$ and is measured in the orthonormal basis $\{b, b^\perp\}$ for $b \in \mathbb{C}^2$, the outcome will be b with probability $|\langle a|b\rangle|^2$. This rules makes sense in general monoidal dagger categories with dagger biproducts.

2.4.1 Probabilities

If $I \xrightarrow{a} A$ is a state and $A \xrightarrow{x} I$ an effect, recall that we interpret the scalar $I \xrightarrow{a} A \xrightarrow{x} I$ as the *amplitude* of measuring outcome $x^\dagger$ immediately after preparing state a; in bra-ket notation this would be $\langle x^\dagger|a\rangle$. The *probability* that this history occurred is the square of its absolute value, which is $|\langle x^\dagger|a\rangle|^2 = \langle a|x^\dagger\rangle \cdot \langle x^\dagger|a\rangle = \langle a|x^\dagger\rangle \circ x(a)$ in bra-ket notation. This makes sense for scalars in any monoidal dagger category.

Definition 2.44 (Probability). If $I \xrightarrow{a} A$ is a state, and $A \xrightarrow{x} I$ an effect, in a monoidal dagger category, set

$$\mathrm{Prob}(x, a) = a^\dagger \circ x^\dagger \circ x \circ a \colon I \to I. \tag{2.45}$$

Example 2.45. In example categories, probabilities match our interpretation.

- In $\mathbf{Hilb}$, probabilities are non-negative real numbers $|\langle x^\dagger|a\rangle|^2$.
- In $\mathbf{Rel}$, the probability of observing an effect $X \subseteq A$ after preparing the state $B \subseteq A$ is the scalar `true` when $X \cap B \neq \emptyset$, and the scalar `false` when X and B are disjoint. This matches the interpretation that the state B consists of all those elements of A that the initial state $\bullet$ before preparation can possibly evolve into.

2.4.2 Dagger kernels

The probabilistic story above is quantitative. When talking about protocols later on, we will often mostly be interested in qualitative or *possibilistic* aspects. In our interpretation, a particular composite morphism equals zero precisely when it describes a sequence of events that cannot physically occur. There is another concept from linear algebra that makes sense in general monoidal dagger categories that is useful here, namely orthogonal subspaces given by *kernels*. A kernel of a morphism $A \xrightarrow{f} B$ can be understood as picking out the largest set of events that cannot be followed by f.

Definition 2.46 (Dagger kernel). In a dagger category with a zero object, an isometry $K \xrightarrow{k} A$ is a *dagger kernel* of $A \xrightarrow{f} B$ when $f \circ k = 0_{K,B}$, and every morphism $X \xrightarrow{x} A$ satisfying $f \circ x = 0_{X,B}$ factors through k.

$$\begin{tikzcd}
K \arrow[r, "k"] & A \arrow[r, shift left, "f"] \arrow[r, shift right, "0"'] & B \\
X \arrow[u, dashed] \arrow[ur, "x"'] & &
\end{tikzcd}$$

The morphism $m \colon X \to K$ is unique: it must be $k^\dagger \circ x$, since k is an isometry and therefore $m = k^\dagger \circ k \circ m = k^\dagger \circ x$. This makes dagger kernels unique up to a unique unitary isomorphism.

Example 2.47. Both $\mathbf{Hilb}$ and $\mathbf{Rel}$ have dagger kernels.

- In $\mathbf{Hilb}$, the dagger kernel of a bounded linear map $H \xrightarrow{f} K$ is the closed subspace $\ker(f) = \{a \in H \mid f(a) = 0\}$, or rather, the inclusion of this subspace into H. This is a dagger kernel rather than just a kernel because $\ker(f)$ carries the inner product induced by H, rather than just any inner product.

- In $\mathbf{Rel}$, the dagger kernel of a given relation $A \xrightarrow{R} B$ is the subset $\ker(R) = \{a \in A \mid \neg\exists b \in B \colon aRb\}$, or rather, the inclusion of this subset into A. (See also Exercise 2.5.7.)

In a dagger categories with a zero object, not all morphisms need have a dagger kernel. But the morphisms that are interesting from the perspective of the Born rule do always have dagger kernels.

Lemma 2.48 (Isometries have zero kernels)**.** *In a dagger category with a zero object, isometries always have a dagger kernel, and a dagger kernel of an isometry is zero.*

Proof. If $A \xrightarrow{f} B$ is an isometry, $0_{0,A}$ certainly satisfies $f \circ 0_{0,A} = 0_{0,B}$. When $X \xrightarrow{x} A$ also satisfies $f \circ x = 0_{X,B}$, then $x = f^\dagger \circ f \circ x = f^\dagger \circ 0_{X,B} = 0_{X,A}$, so x factors through $0_{0,A}$. Conversely, if $K \xrightarrow{k} A$ is a dagger kernel of $A \xrightarrow{f} B$ and $f^\dagger \circ f = \mathrm{id}_A$, then

$$k = f^\dagger \circ f \circ k = f^\dagger \circ 0_{K,B} = 0_{K,A}$$

must be the zero morphism. □

Dagger kernels also have a good influence on abstract inner products.

Lemma 2.49 (Nondegeneracy)**.** *In a dagger category with a zero object and dagger kernels of arbitrary morphisms, $f^\dagger \circ f = 0_{A,A}$ implies $f = 0_{A,B}$ for any morphism $A \xrightarrow{f} B$.*

Proof. Consider the isometry $k = \ker(f^\dagger) \colon K \to B$. If $f^\dagger \circ f = 0_{A,A}$, there is unique $A \xrightarrow{m} K$ with $f = k \circ m$. But then

$$f = k \circ m = k \circ k^\dagger \circ k \circ m = k \circ k^\dagger \circ f = k \circ 0^\dagger_{K,A} = 0_{A,B}.$$ □

If $I \xrightarrow{a} A$ is a state, nondegeneracy implies that $(I \xrightarrow{a} A \xrightarrow{a^\dagger} I) = 0$ if and only if $a = 0$. Interpreting $I \xrightarrow{a} A \xrightarrow{a^\dagger} I$ as the result of measuring the system A in state a immediately after preparing it in state a, the outcome is zero precisely when this history cannot possibly have occurred, so a must have been an impossible state to begin with.

2.4.3 Complete and disjoint sets of effects

When does a set of effects $A \xrightarrow{x_i} I$ tell us as much as possible about a system?

Definition 2.50. A set of effects $A \xrightarrow{x_i} I$ is *complete* if every nonzero process yields a nonzero effect; that is, for all morphisms $B \xrightarrow{f} A$ with $f \neq 0_{B,A}$, there is some x_i such that $x_i \circ f \neq 0_{B,I}$.

A complete set of effects might cover all you possibly want to know about a system, but it may be huge. A set of effects $A \xrightarrow{x_i} I$ is as efficient as possible when the effects are perfectly disjoint: preparing the system in state $x_i^\dagger$ and observing it with our set of effects, only outcome x_i can occur.

Definition 2.51. A set of effects $A \xrightarrow{x_i} I$ is *disjoint* if for all $i \neq j$ it satisfies:

$$x_i \circ x_i^\dagger = \mathrm{id}_I \qquad\qquad x_i \circ x_j^\dagger = 0_{I,I} \tag{2.46}$$

Complete disjoint sets of effects are characterized by biproducts. For example, zero is a dagger kernel of the matrix $\begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix}$ for any complete set of effects $\{A \xrightarrow{x_n} I\}$ in a monoidal dagger category with a zero object and dagger biproducts. This means that if $I \xrightarrow{a} A$ is any state, then at least one of the histories $I \xrightarrow{a} A \xrightarrow{x_n} I$ must occur.

Lemma 2.52. *Finite complete disjoint sets of effects $A \xrightarrow{x_n} I$ correspond exactly to morphisms $A \xrightarrow{x} \bigoplus_n I$ for which $x^\dagger$ is an isometry and that have zero kernel.*

Proof. A set of effects $A \xrightarrow{x_n} I$ corresponds exactly to a column matrix $A \xrightarrow{x} \bigoplus_{n=1}^N I$. For this to have zero kernel is exactly the completeness condition. For $x^\dagger$ to be an isometry corresponds to the disjointness condition:

$$\begin{aligned} x \circ x^\dagger &= \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_N \end{pmatrix} \circ \begin{pmatrix} x_1^\dagger & x_2^\dagger & \cdots & x_N^\dagger \end{pmatrix} = \begin{pmatrix} x_1 \circ x_1^\dagger & x_1 \circ x_2^\dagger & \cdots & x_1 \circ x_N^\dagger \\ x_2 \circ x_1^\dagger & x_2 \circ x_2^\dagger & \cdots & x_2 \circ x_N^\dagger \\ \vdots & \vdots & \ddots & \vdots \\ x_N \circ x_1^\dagger & x_N \circ x_2^\dagger & \cdots & x_N \circ x_N^\dagger \end{pmatrix} \\ &= \begin{pmatrix} \mathrm{id}_I & 0_{I,I} & \cdots & 0_{I,I}nn \\ 0_{I,I} & \mathrm{id}_I & \cdots & 0_{I,I} \\ \vdots & \vdots & \ddots & \vdots \\ 0_{I,I} & 0_{I,I} & \cdots & \mathrm{id}_I \end{pmatrix} \end{aligned}$$

This completes the proof. □

Let's call a superposition rule *invertible* when for each $A \xrightarrow{f} B$ there exists $A \xrightarrow{-f} B$ such that $f + (-f) = 0_{A,B}$. Notice that it follows automatically that such a morphism $-f$ is unique: for if $f + g = 0 = f + g'$, then $g = g + (f + g') = (g + f) + g' = g'$.

Lemma 2.53. *Given a finite complete disjoint set of effects $A \xrightarrow{x_i} I$ in a category with equalizers and invertible superposition rule, the biproduct $A \xrightarrow{x} \bigoplus_n I$ is unitary.*

Proof. Consider the following diagram:

$$\begin{tikzcd} E = 0 \arrow[r, "e"] & A \arrow[r, shift left, "x"] \arrow[r, shift right, "0"'] & \bigoplus_{n=1}^N I \\ A \arrow[u, dashed, "m"] \arrow[ur, "y = x^\dagger \circ x - \mathrm{id}_A"'] & & \end{tikzcd}$$

The morphism $A \xrightarrow{y} A$ satisfies $x \circ y = 0 \circ y$, since $x \circ y = x \circ x^\dagger \circ x - x = x - x = 0$. Hence y must factor through the equalizer E of x and 0. But by assumption $E = 0$, and so y is a zero morphism. Hence $x^\dagger \circ x - \mathrm{id}_A = 0$, which gives $x^\dagger \circ x = \mathrm{id}_A$. Together with the disjointness condition $x \circ x^\dagger = \mathrm{id}_{\bigoplus_{n=1}^N I}$, this demonstrates that x is unitary. □

Example 2.54. Let us examine complete disjoint sets of effects in our example categories.

- **Hilb** has equalizers and an invertible superposition rule, so by Lemma 2.53 complete disjoint sets of effects correspond to unitary morphisms $H \simeq \mathbb{C}^n$. Thus choosing a complete disjoint set of effects is just the same as choosing an orthonormal basis for H.

- In **Rel**, a complete disjoint set effects for a set A is a partition of the set into subsets.

Before we prove that the probabilities add up to one, observe that this only makes sense if the state of the system is specified well enough. In a monoidal dagger category there is a duality between states $I \xrightarrow{a} A$ and effects $A \xrightarrow{a^\dagger} I$. We interpret $I \xrightarrow{a} A \xrightarrow{a^\dagger} I$ as the result of measuring the system A in state a immediately after preparing it in state a. This had better be the identity. That is, if we want to say something about probabilities, we should only consider isometric states. In **Hilb**, these correspond to unit vectors; in **Rel**, these correspond to nonempty subsets.

Proposition 2.55 (Born rule)**.** *Let $A \xrightarrow{x_n} I$ be a finite complete set of effects in a monoidal dagger category with dagger biproducts, and let $I \xrightarrow{a} A$ be an isometric state. Then* $\sum_n \mathrm{Prob}(x_n, a) = 1$.

Proof. By the superposition rule,

$$\sum_{n=1}^{N} \mathrm{Prob}(x_n, a) = \sum_{n=1}^{N} a^\dagger \circ x_n^\dagger \circ x_n \circ a = a^\dagger \circ \left(\sum_{i=n}^{N} x_n^\dagger \circ x_n \right) \circ a.$$

But Lemma 2.52 guarantees that $x^\dagger \circ x = \mathrm{id}$, so this equals $a^\dagger \circ a$. Finally, because a is an isometry, this equals $\mathrm{id}_I = 1$. □

2.5 Exercises

Exercise 2.5.1. Recall Definition 2.18.

(a) Show that the biproduct of a pair of objects is unique up to a unique isomorphism.

(b) Suppose that a category has biproducts of pairs of objects, and a zero object. Show that this gives rise to a monoidal structure.

Exercise 2.5.2. Show that all joint states are product states when $A \otimes B$ is a product of A and B, and I is terminal. Conclude that monoidal categories modeling nonlocal correlation such as entanglement must have a tensor product that is not a (categorical) product.

Exercise 2.5.3. Show that any category with products, a zero object, and a superposition rule, automatically has biproducts.

Exercise 2.5.4. Show that the following diagram commutes in any monoidal category with biproducts.

$$
\begin{tikzcd}
 & A \otimes B \arrow[dl, "\mathrm{id}_A \otimes \begin{pmatrix} \mathrm{id}_B \\ \mathrm{id}_B \end{pmatrix}"'] \arrow[dr, "\begin{pmatrix} \mathrm{id}_{A\otimes B} \\ \mathrm{id}_{A\otimes B} \end{pmatrix}"] & \\
A \otimes (B \oplus B) \arrow[rr, "\begin{pmatrix} \mathrm{id}_A \otimes (\,\mathrm{id}_B \;\; 0_{B,B}\,) \\ \mathrm{id}_A \otimes (\,0_{B,B} \;\; \mathrm{id}_B\,) \end{pmatrix}"'] & & (A \otimes B) \oplus (A \otimes B)
\end{tikzcd}
$$

Exercise 2.5.5. Daggers can model *Bayesian inference* in classical probability theory. Show that the following is a well-defined dagger category:

- *objects* (A, p) are finite sets A equipped with *prior probability distributions*, functions $p\colon A \to (0, \infty)$ such that $\sum_{a \in A} p(a) = 1$;
- *morphisms* $(A, p) \xrightarrow{f} (B, q)$ are *conditional probability distributions*, functions $f\colon A \times B \to [0, \infty)$ such that for all $a \in A$ we have $\sum_{b \in B} f(a, b) = 1$, and for all $b \in B$ we have $q(b) = \sum_{a \in A} p(a) f(a, b)$;
- *composition* is composition of probability distributions as matrices of real numbers;
- the *dagger* acts on $f\colon A \times B \to [0, \infty)$ to give $f^\dagger\colon B \times A \to [0, \infty)$, defined as $f^\dagger(b, a) = f(a, b)p(a)/q(b)$.

Exercise 2.5.6. Let A and B be objects in a dagger category. Show that if $A \oplus B$ is a dagger biproduct, then i_A is a dagger kernel of p_B.

Exercise 2.5.7. Let $A \xrightarrow{R} B$ be a morphism in the dagger category $\mathbf{Rel}$.

(a) Show that R is unitary if and only if it is (the graph of) a bijection;

(b) Show that R is self-adjoint if and only if it is symmetric;

(c) Show that R is positive if and only if R is symmetric and $a\,R\,b \;\Rightarrow\; a\,R\,a$.

(d) Show that R is a dagger kernel if and only if it is (the graph of a) subset inclusion.

(e) Is every isometry in $\mathbf{Rel}$ a dagger kernel?

(f) Is every isometry $A \to A$ in $\mathbf{Rel}$ unitary?

(g) Show that every biproduct in $\mathbf{Rel}$ is a dagger biproduct.

Exercise 2.5.8. Recall the monoidal category $\mathbf{Mat}_{\mathbb{C}}$ from Definition 1.26.

(a) Show that transposition of matrices makes the monoidal category $\mathbf{Mat}_{\mathbb{C}}$ into a monoidal dagger category.

(b) Show that $\mathbf{Mat}_{\mathbb{C}}$ does not have dagger kernels under this dagger functor.

Exercise 2.5.9. Given morphisms $A \xrightarrow{f, g} B$ in a dagger category, a *dagger equalizer* is an isometry $E \xrightarrow{e} A$ satisfying $f \circ e = g \circ e$, with the property that every morphism $X \xrightarrow{x} A$ satisfying $f \circ x = g \circ x$ factors through e.

$$
\begin{tikzcd}
E \arrow[r, "e"] & A \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & B \\
X \arrow[u, dashed] \arrow[ur, "x"'] & &
\end{tikzcd}
$$

Prove the following properties for $A \xrightarrow{f,g,h} B$ in a dagger category with dagger biproducts and dagger equalizers:

(a) $f = g$ if and only if $f + h = g + h$;
(Hint: consider the dagger equalizer of $\begin{pmatrix} f & h \end{pmatrix}$ and $\begin{pmatrix} g & h \end{pmatrix} : A \oplus A \to B$);

(b) $f = g$ if and only if $f + f = g + g$;
(Hint: consider the dagger equalizer of $\begin{pmatrix} f & f \end{pmatrix}$ and $\begin{pmatrix} g & g \end{pmatrix} : A \oplus A \to A$);

(c) $f = g$ if and only if $f^\dagger \circ g + g^\dagger \circ f = f^\dagger \circ f + g^\dagger \circ g$.
(Hint: consider the dagger equalizer of $\begin{pmatrix} f & g \end{pmatrix}$ and $\begin{pmatrix} g & f \end{pmatrix} : A \oplus A \to B$);

Exercise 2.5.10. Fuglede's theorem is the following statement for morphisms $f, g \colon A \to A$ in $\mathbf{Hilb}$: if $f \circ f^\dagger = f^\dagger \circ f$ and $f \circ g = g \circ f$, then also $f^\dagger \circ g = g \circ f^\dagger$. Show that this does not hold in $\mathbf{Rel}$.

Exercise 2.5.11. Show that $\mathbf{Fib}$, given in Definition 2.43, satisfies the triangle and pentagon equations for a monoidal category, and the hexagon equations for a braided monoidal category. By Proposition 2.24, it is sufficient to verify this for simple objects only.

Notes and further reading

The early uses of category theory were in algebraic topology. Therefore early developments mostly considered categories like $\mathbf{Vect}$. The most general class of categories for which known methods worked are so-called Abelian categories, for which biproducts and what we called superposition rules are important axioms; see Freyd's book [62]. By Mitchell's embedding theorem, any Abelian category embeds into $\mathbf{Mod}_R$, the category of R-modules for some ring R, preserving all the important structure [110]. Superposition rules are more formally known as enrichment in commutative monoids, and play an important role in such embedding theorems. See also [27] for an overview.

Self-duality in the form of involutive endofunctors on categories has been considered as early as 1950 [104, 105]. A link between adjoint functors and adjoints in Hilbert spaces was made precise in 1974 [114]. The systematic exploitation of daggers in the way we have been using them started with Selinger in 2007 [132].

Using different terminology, Lemma 2.3 was proved in 1980 by Kelly and Laplaza [94]. The realization that endomorphisms of the tensor unit behave as scalars was made explicit by Abramsky and Coecke in 2004 [4, 2]. Heunen proved an analogue of Mitchell's embedding theorem for $\mathbf{Hilb}$ in 2009 [71]. Conditions under which the scalars embed into the complex numbers are due to Vicary [138].

Anyons are important for topological quantum field theory [139], and for topological quantum computation [113].

Chapter 3

Dual objects

This chapter studies the key property of dualizability. In terms of linear algebra, it means that maximally entangled states exist. In operational terms, it means that protocols resembling quantum teleportation are possible. In terms of the graphical calculus, it means that wires can bend 'back in time'. After introducing the basic definition and proving some basic properties in Section 3.1, we will treat the quantum teleportation protocol in Section 3.2. We say teleportation, but in $\mathbf{Rel}$ it models classical one-time pad encryption. Next we prove that the presence of dual objects ensures that tensor products interact well with any linear structure available, in Section 3.3. In particular, dual objects capture linear-algebraic properties such as traces and dimension. To see this we will make a fairly thorough study of various ways dual objects on different objects cooperate, in Section 3.4.

3.1 Dual objects

Let's start right away with the definition, which is perhaps the most important one in this book.

Definition 3.1 (Dual object)**.** In a monoidal category, an object L is *left-dual* to an object R, and R is *right-dual* to L, written $L \dashv R$, when there exist a unit morphism $I \xrightarrow{\eta} R \otimes L$ and a counit morphism $L \otimes R \xrightarrow{\varepsilon} I$ making the following diagrams commute:

$$\begin{tikzcd}
L \arrow[r, "\rho_L^{-1}"] \arrow[d, "\mathrm{id}_L"'] & L \otimes I \arrow[r, "\mathrm{id}_L \otimes \eta"] & L \otimes (R \otimes L) \arrow[d, "\alpha^{-1}_{L,R,L}"] \\
L & I \otimes L \arrow[l, "\lambda_L"] & (L \otimes R) \otimes L \arrow[l, "\varepsilon \otimes \mathrm{id}_L"]
\end{tikzcd} \tag{3.1}$$

$$\begin{tikzcd}
R \arrow[r, "\lambda_R^{-1}"] \arrow[d, "\mathrm{id}_R"'] & I \otimes R \arrow[r, "\eta \otimes \mathrm{id}_R"] & (R \otimes L) \otimes R \arrow[d, "\alpha_{R,L,R}"] \\
R & R \otimes I \arrow[l, "\rho_R"] & R \otimes (L \otimes R) \arrow[l, "\mathrm{id}_R \otimes \varepsilon"]
\end{tikzcd} \tag{3.2}$$

When L is both left and right dual to R, we simply call L a *dual* of R.

In the graphical calculus, to keep track of which object is left dual and which is right dual, draw an object L as a wire with an upward-pointing arrow, and a right dual R as a wire with a downward-pointing arrow:

Similarly, the unit $I \xrightarrow{\eta} R \otimes L$ and counit $L \otimes R \xrightarrow{\varepsilon} I$ are such important morphisms that they deserve a special depiction. Instead of generic morphism boxes, they will be drawn as bent wires, called the *cup* and the *cap*:

(3.3)

This notation renders the duality equations (3.1) and (3.2) in an attractive form:

(3.4)

Because of their graphical form, they are also called the *snake equations*.

These equations add *orientation* to the graphical calculus. Physically, η represents a state of $R \otimes L$; a way for these two systems to be brought into being. We will see later that it represents a full-rank entangled state of $R \otimes L$. The fact that entanglement is modelled so naturally using monoidal categories is a key reason for interest in the categorical approach to quantum information.

Example 3.2. Let's see what dual objects look like in our example categories.

- The monoidal category **FHilb** has all duals. Every finite-dimensional Hilbert space H is both right dual and left dual to its dual Hilbert space H^* (see Definition 0.49), in a canonical way. The counit $H \otimes H^* \xrightarrow{\varepsilon} \mathbb{C}$ of the duality $H \dashv H^*$ is given by the following map:

$$\varepsilon : |\phi\rangle \otimes \langle\psi| \mapsto \langle\psi|\phi\rangle \tag{3.5}$$

  The unit $\mathbb{C} \xrightarrow{\eta} H^* \otimes H$ is defined as follows, for any orthonormal basis $|i\rangle$:

$$\eta : 1 \mapsto \sum_i \langle i| \otimes |i\rangle \tag{3.6}$$

  These definitions sit together oddly, since η seems basis-dependent, while ε is not. In fact the same value of η is obtained whatever orthonormal basis is used, as Lemma 3.5 below makes clear.

- Infinite-dimensional Hilbert spaces do not have duals. For an infinite-dimensional Hilbert space, the definitions of η and ε given above are no good, as they do not give bounded linear maps. In Corollary 3.65, we will see that a Hilbert space has a dual if and only if it is finite-dimensional.

- In $\mathbf{Rel}$, every object is its own dual, even sets of infinite cardinality. For a set A, the relations $1 \xrightarrow{\eta} A \times A$ and $A \times A \xrightarrow{\varepsilon} 1$ are defined in the following way, where we write $\bullet$ for the unique element of the 1-element set:

$$\begin{aligned} \bullet \sim_\eta (a,a) &\text{ for all } a \in A \\ (a,a) \sim_\varepsilon \bullet &\text{ for all } a \in A \end{aligned}$$

- In $\mathbf{Mat}_{\mathbb{C}}$, every object n is its own dual, with a canonical choice of η and ε given as follows:

$$\eta : 1 \mapsto \sum_i |i\rangle \otimes |i\rangle \qquad\qquad \varepsilon : |i\rangle \otimes |j\rangle \mapsto \delta_{ij} 1$$

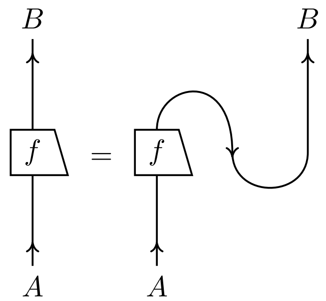
- In $\mathbf{Fib}$, every object is its own dual. Consider the simple case $\tau \dashv \tau$; then $\eta = i_I$ and $\varepsilon = \phi\, p_I$ satisfy the snake equation, using the calculation at the end of Section 2.3.4. This extends to biproduct objects by a similar method to the proof of Lemma 3.23, invoking bilinearity in place of (3.17) and (3.18).

The category $\mathbf{Set}$ only has duals for singleton sets. To understand why, it helps to introduce the *name* and *coname* of a morphism.

Definition 3.3 (Name, coname)**.** In a monoidal category with dualities $A \dashv A^*$ and $B \dashv B^*$, given a morphism $A \xrightarrow{f} B$, define its *name* $I \xrightarrow{\ulcorner f \urcorner} A^* \otimes B$ and *coname* $A \otimes B^* \xrightarrow{\llcorner f \lrcorner} I$ as the following morphisms:

(3.7)

Morphisms can be recovered from their names or conames via the snake equations:



This correspondence is sometimes called *map-state* duality, or the *Choi-Jamiołkowski* correspondence.

In $\mathbf{Set}$, the monoidal unit object 1 is terminal, and so all conames $A \otimes B^* \xrightarrow{\llcorner f \lrcorner} 1$ must be equal. If the set B had a dual, this would imply that for all sets A, all functions $A \xrightarrow{f} B$ are equal, which is only the case for $B = \emptyset$ or $B = 1$. It is easy to see that $\emptyset$ does not have a dual, because there is no function $1 \to \emptyset \times \emptyset^*$ for any set $\emptyset^*$. A 1-element set does have a dual since it is isomorphic to the monoidal unit; see Lemmas 3.4 and 3.7 below.

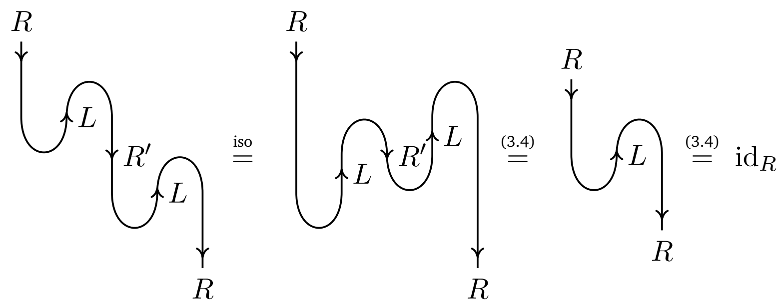
3.1.1 Basic properties

The first thing to establish is that duals are well-defined up to canonical isomorphism.

Lemma 3.4 (Duals are unique up to isomorphism)**.** *In a monoidal category with $L \dashv R$, then $L \dashv R'$ if and only if $R \simeq R'$. Similarly, if $L \dashv R$, then $L' \dashv R$ if and only if $L \simeq L'$.*

Proof. If $L \dashv R$ and $L \dashv R'$, define maps $R \to R'$ and $R' \to R$ as follows:

It follows from the snake equations that these are inverse to each other. There are two equations to check, and one of them can be verified as follows, with the other being similar:



(3.8)

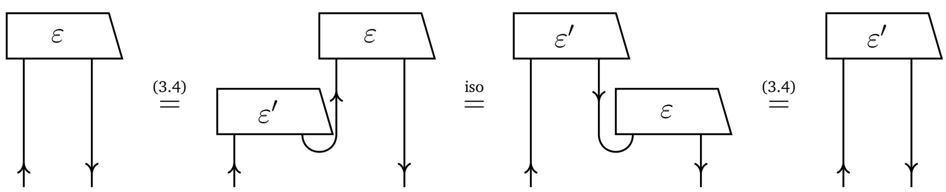
Conversely, if $L \dashv R$ and $R \xrightarrow{f} R'$ is an isomorphism, then we can construct a duality $L \dashv R'$ as follows:

An isomorphism $L \simeq L'$ allows us to produce a duality $L' \dashv R$ in a similar way. □

In a duality, the unit determines the counit, and vice versa.

Lemma 3.5 (Cup determines cap)**.** *In a monoidal category, if $(L, R, \eta, \varepsilon)$ and $(L, R, \eta, \varepsilon')$ both exhibit a duality, then $\varepsilon = \varepsilon'$. Similarly, if $(L, R, \eta, \varepsilon)$ and $(L, R, \eta', \varepsilon)$ both exhibit a duality, then $\eta = \eta'$.*

Proof. The first case is proven by the following graphical argument:



The second case is similar. □

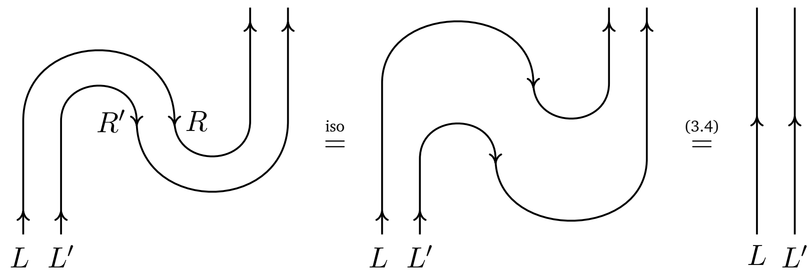
The following two lemmas show that dual objects interact well with the monoidal structure.

Lemma 3.6. *In a monoidal category, $I \dashv I$.*

Proof. Take $\eta = \lambda_I^{-1} \colon I \to I \otimes I$ and $\varepsilon = \lambda_I \colon I \otimes I \to I$ shows that $I \dashv I$. The snake equations follow directly from the Coherence Theorem 1.2. Alternatively we can prove this using the graphical calculus; all the geometrical images are empty, and the result follows trivially. □

Lemma 3.7. *In a monoidal category, $L \dashv R$ and $L' \dashv R'$ implies $L \otimes L' \dashv R' \otimes R$.*

Proof. Suppose that $L \dashv R$ and $L' \dashv R'$. We make the new unit and counit maps from the old ones, and prove one of the snake equations graphically:



The other snake equation follows similarly. □

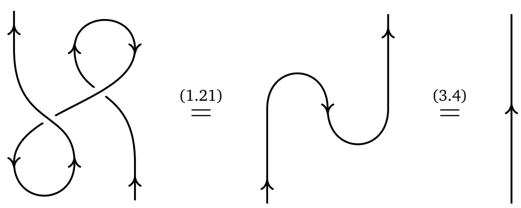
If the monoidal category has a braiding then a duality $L \dashv R$ gives rise to a duality $R \dashv L$, as the next lemma investigates.

Lemma 3.8. *In a braided monoidal category, $L \dashv R \Rightarrow R \dashv L$.*

Proof. Suppose $(L, R, \eta, \varepsilon)$ witnesses the duality $L \dashv R$. Construct a duality $(R, L, \eta', \varepsilon')$ as follows, using the ordinary graphical calculus for the duality $(L, R, \eta, \varepsilon)$:

$I \xrightarrow{\eta'} L \otimes R$ $\qquad$ $R \otimes L \xrightarrow{\varepsilon'} I$

Writing out one of the snake equations for these new duality morphisms shows that they are satisfied by properties of the swap map and the snake equations for the original duality morphisms η and ε:

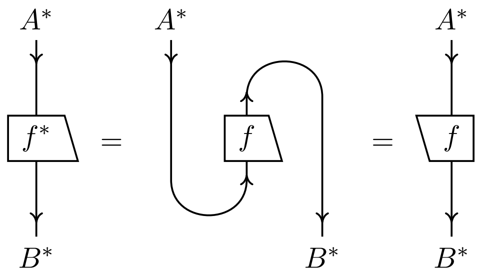


The other snake equation can be proved in a similar way. □

3.1.2 The right-duals functor

Choosing duals for objects gives a strong structure that extends functorially to morphisms.

Definition 3.9 (Transpose)**.** In a monoidal category, for a morphism $A \xrightarrow{f} B$ and chosen dualities $A \dashv A^*$, $B \dashv B^*$, the *right dual* or *transpose* $B^* \xrightarrow{f^*} A^*$ is defined as follows:



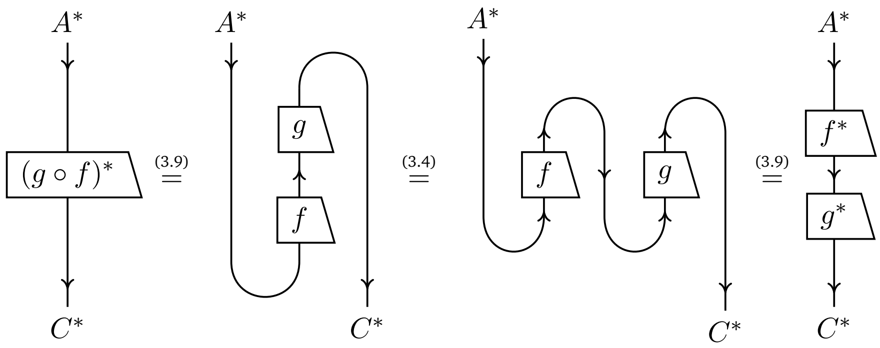
(3.9)

As the third image above shows, the right dual is drawn by rotating the box representing f.

Definition 3.10 (Right dual functor)**.** In a monoidal category $\mathbf{C}$ in which every object X has a chosen right dual X^*, the *right dual functor* $(-)^* \colon \mathbf{C} \to \mathbf{C}^{\mathrm{op}}$ is defined on objects as $(X)^* = X^*$ and on morphisms as $(f)^* = f^*$.

Proposition 3.11. *The right-duals functor satisfies the functor axioms.*

Proof. Let $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$. Then:



Similarly, $(\mathrm{id}_A)^* = \mathrm{id}_{A^*}$ follows from the snake equations. □

The dual of a morphism can 'slide' along the cups and the caps.

Lemma 3.12 (Sliding)**.** *In a monoidal category with chosen dualities $A \dashv A^*$ and $B \dashv B^*$, the following equations hold for all morphisms $A \xrightarrow{f} B$:*

(3.10)

Proof. Direct from writing out the definitions of the components involved. □

Example 3.13. Let's see how the right duals functor acts in example categories, with right duals chosen as in Example 3.2.

- In $\mathbf{FVect}$ and $\mathbf{FHilb}$, the right dual of a morphism $V \xrightarrow{f} W$ is $W^* \xrightarrow{f^*} V^*$, acting as $f^*(e) = e \circ f$, where $W \xrightarrow{e} \mathbb{C}$ is an arbitrary element of W^*.
- In $\mathbf{Mat}_{\mathbb{C}}$, the dual of a matrix is its transpose.
- In $\mathbf{Rel}$, the dual of a relation is its converse. So the right duals functor and the dagger functor acts the same way: $R^* = R^\dagger$ for all relations R.

3.1.3 Interaction with monoidal functors

Dual objects interact well monoidal structure. For example, they are automatically preserved by monoidal functors.

Theorem 3.14. *Monoidal functors preserve duals.*

Proof. Suppose that $F : \mathbf{C} \to \mathbf{C}'$ is a monoidal functor (see Definition 1.27) with $I \xrightarrow{\eta} A^* \otimes A$ and $A \otimes A^* \xrightarrow{\varepsilon} I$ witnessing a duality $A \dashv A^*$ in $\mathbf{C}$. Then we will show that $F(A) \dashv F(A^*)$ in $\mathbf{C}'$. Define η' and ε' as follows:

$$\eta' = I' \xrightarrow{F_0} F(I) \xrightarrow{F(\eta)} F(A^* \otimes A) \xrightarrow{(F_2)^{-1}_{A^*,A}} F(A^*) \otimes F(A)$$
$$\varepsilon' = F(A) \otimes F(A^*) \xrightarrow{(F_2)_{A,A^*}} F(A \otimes A^*) \xrightarrow{F(\varepsilon)} F(I) \xrightarrow{(F_0)^{-1}} I'$$

Now consider the following commutative diagram, where each cell commutes either due to naturality, or due to one of the monoidal functor axioms. The left-hand side is the snake equation (3.1) in $\mathbf{C}'$ in terms of η' and ε'. The right-hand side is the snake equation in $\mathbf{C}$ in terms of η and ε, under the image of F.

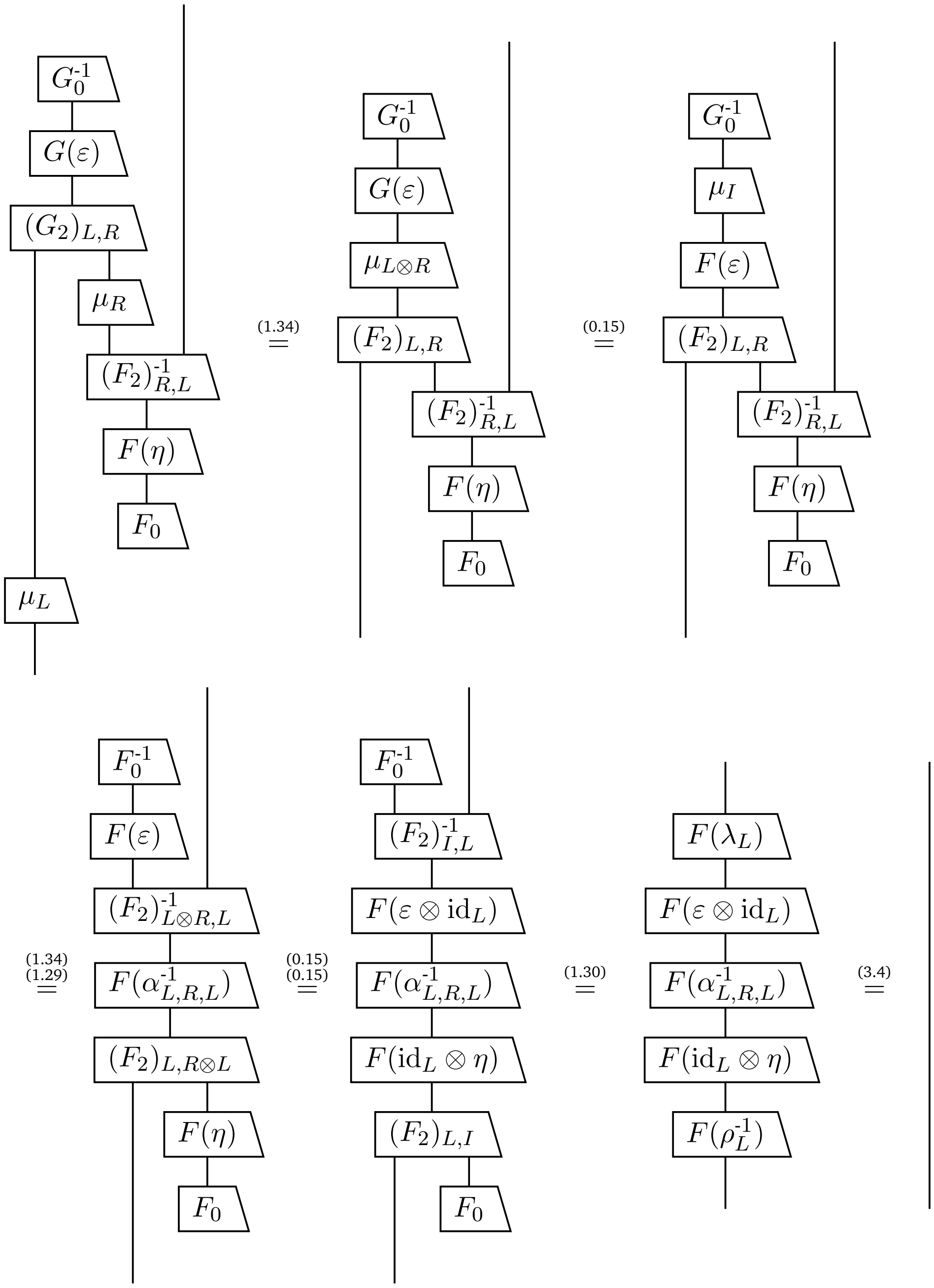
$$
\begin{tikzcd}
F(A) \arrow[d, "\rho^{-1}_{F(A)}"'] \arrow[ddr, "F(\rho^{-1}_A)"] & \\
F(A) \otimes' I' \arrow[d, "\mathrm{id}_{F(A)} \otimes' F_0"'] \arrow[r, phantom, "(1.30)"] & \\
F(A) \otimes' F(I) \arrow[r, "(F_2)_{A,I}"] \arrow[d, "\mathrm{id}_{F(A)} \otimes' F(\eta)"'] \arrow[dr, phantom, "(NAT)"] & F(A \otimes I) \arrow[d, "F(\mathrm{id}_A \otimes \eta)"] \\
F(A) \otimes' F(A^* \otimes A) \arrow[r, "(F_2)_{A,A^* \otimes A}"] \arrow[d, "\mathrm{id}_{F(A)} \otimes' (F_2)^{-1}_{A^*,A}"'] & F\big(A \otimes (A^* \otimes A)\big) \arrow[ddd, "F(\alpha^{-1}_{A,A^*,A})"] \\
F(A) \otimes' \big(F(A^*) \otimes' F(A)\big) \arrow[d, "\alpha'^{-1}_{F(A),F(A^*),F(A)}"'] \arrow[r, phantom, "(1.29)"] & \\
\big(F(A) \otimes' F(A^*)\big) \otimes' F(A) \arrow[d, "(F_2)_{A,A^*} \otimes' \mathrm{id}_{F(A)}"'] & \\
F(A \otimes A^*) \otimes' F(A) \arrow[r, "(F_2)_{A \otimes A^*,A}"] \arrow[d, "F(\varepsilon) \otimes' \mathrm{id}_{F(A)}"'] \arrow[dr, phantom, "(NAT)"] & F\big((A \otimes A^*) \otimes A\big) \arrow[d, "F(\varepsilon \otimes A)"] \\
F(I) \otimes' F(A) \arrow[r, "(F_2)_{I,A}"] \arrow[d, "F_0^{-1} \otimes' \mathrm{id}_{F(A)}"'] & F\big(I \otimes A\big) \arrow[ddl, "F(\lambda_A)"] \\
I' \otimes' F(A) \arrow[d, "\lambda'_{F(A)}"'] \arrow[r, phantom, "(1.30)"] & \\
F(A) &
\end{tikzcd}
$$

Since functors preserve identities, the right-hand side is the identity, which establishes the first snake equation. The second one is proven similarly. □

In fact, having a dual object is a surprisingly strong property: components of natural transformations between monoidal functors (see Definition 1.36) at dual objects must be invertible.

Theorem 3.15. *Let $\mu \colon F \Longrightarrow G$ be a monoidal natural transformation between monoidal functors $F, G \colon \mathbf{C} \to \mathbf{D}$, where $\mathbf{C}$ and $\mathbf{D}$ are monoidal categories, and where $A \in \mathrm{Ob}(\mathbf{C})$ has a right or left dual. Then $F(A) \xrightarrow{\mu_A} G(A)$ is invertible.*

Proof. First suppose that $A = L$, with $L \dashv R$. Then μ_L has a left inverse:

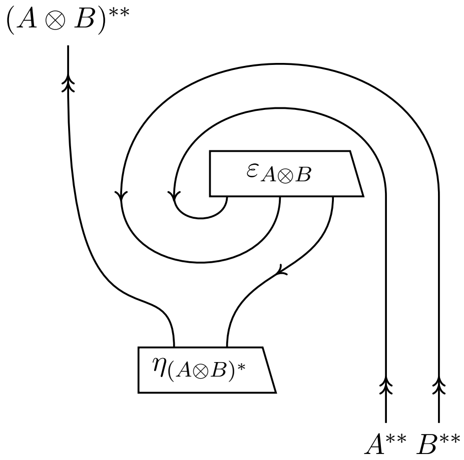


The inverse μ_L^{-1} is everything in the first diagram shown, above the μ_L node; this calculation then shows that $\mu_L^{-1} \circ \mu_L = \mathrm{id}_L$. The proofs that $\mu_L \circ \mu_L^{-1} = \mathrm{id}_L$, and that μ_R has an inverse, are similar. □

Iterating the right-duals functor twice is a monoidal functor.

Lemma 3.16. *For a monoidal category with chosen right duals for objects, the double duals functor* $(-)^{**} : \mathbf{C} \to \mathbf{C}$ *is monoidal.*

Proof. The isomorphism $\phi_{A,B} \colon A^{**} \otimes B^{**} \to (A \otimes B)^{**}$ looks like this, where we decorate a wire with $\Lsh$ to denote the double dual:



(3.11)

Similarly, the isomorphism $\psi\colon I \to I^{**}$ is given by $\psi = \rho_{I^{**}} \circ (\mathrm{id}_{I^{**}} \otimes \varepsilon_I) \circ (\mathrm{id}_{I^{**}} \otimes \lambda_{I^*}^{-1}) \circ \eta_{I^*}$. Showing this satisfies the monoidal functor axioms takes a big diagram, which we won't write out here. □

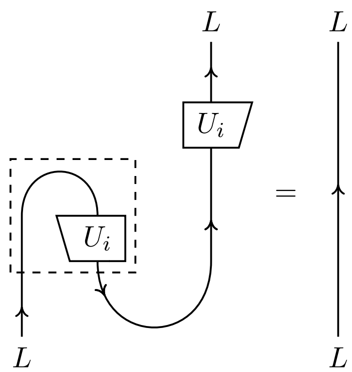
The $\Lsh$ notation is a bit unpleasant, but we will be able to dispense with it after introducing the notion of pivotal structure in Section 3.4.

3.2 Teleportation

Having seen some category-theoretical properties of dual objects, we now turn to an operational explanation, by discussing how quantum teleportation can be understood abstractly in terms of dual objects. We will see that in **Hilb** this models quantum teleportation, and in **Rel** this models classical encrypted communication.

3.2.1 Abstract description

Consider the following diagram:

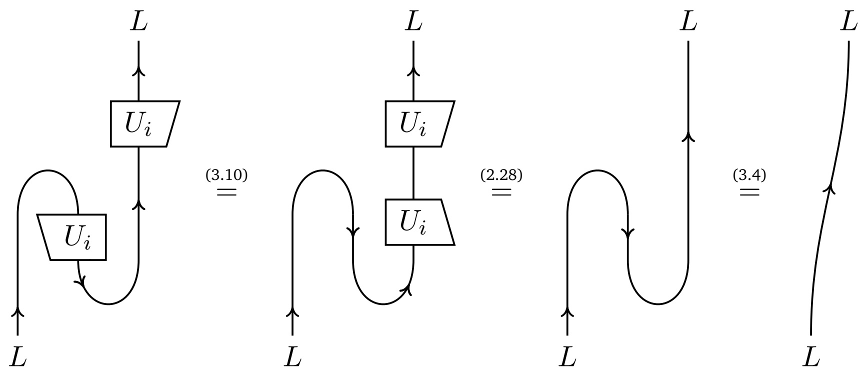


(3.12)

It makes use of a duality $L \dashv R$ witnessed by morphisms $I \xrightarrow{\eta} R \otimes L$ and $L \otimes R \xrightarrow{\varepsilon} I$, and a unitary morphism $L \xrightarrow{U} L$. The dashed box around part of the diagram indicates that we will treat it as a single effect. Let's describe this history in words:

1. Begin with a single system L.
2. Independently, prepare a joint system $R \otimes L$ in the state η, resulting in a total system $L \otimes (R \otimes L)$.
3. Perform a joint measurement on the first two systems, with a result given by the effect $\varepsilon \circ (\mathrm{id}_L \otimes U_i^*)$.
4. Perform a unitary operation U_i on the remaining system.

Ignoring the dashed box, the graphical calculus simplifies the history:



Rotating the box U along the path of the wire, using unitarity of U, and then using a snake equation to straighten out the wire, results in the identity. So if the events described in (3.12) come to pass, then the original system is transmitted unaltered.

For this procedure to be guaranteed to succeed, some history of this form has to occur; that is, the components in the dashed box in (3.12) must form a complete, disjoint set of effects, as discussed in Section 2.4.3.

This presentation gives some additional insight into the nature of quantum teleportation, compared to the traditional presentation in Section 0.3.6. The state is transferred because of the topological properties of the cup and cap, allowing us to 'straighten out' the flow of information. And the reason for the different choices of correction U_i are to account for the fact that we might obtain different effects $\varepsilon \circ (\mathrm{id}_L \otimes U_i^*)$. However, some aspects still remain unclear. What is the formal mathematical status of the dotted box around the effect? And how can we formally understand the classical communication step, where information about Alice's measurement result is passed to Bob? Further categorical machinery later in the book will answer these questions.

3.2.2 Interpretation

Now let's instantiate the abstract teleportation procedure in our example categories. The interpretation in **Hilb** matches conventional quantum teleportation, as intended.

Example 3.17. In **Hilb**, choose $L = R = \mathbb{C}^2$ and $\eta^\dagger = \varepsilon = \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}$, and choose the following family of unitaries U_i:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{3.13}$$

This gives rise to the following family of effects:

$$\begin{pmatrix}1 & 0 & 0 & 1\end{pmatrix} \qquad \begin{pmatrix}1 & 0 & 0 & -1\end{pmatrix} \qquad \begin{pmatrix}0 & 1 & 1 & 0\end{pmatrix} \qquad \begin{pmatrix}0 & 1 & -1 & 0\end{pmatrix}$$

This is a complete set of effects, since it forms a basis for the vector space $\mathbf{Hilb}(\mathbb{C}^2 \otimes \mathbb{C}^2, \mathbb{C})$. As a result, thanks to the categorical argument, we can implement a teleportation scheme which is guaranteed to be successful whatever measurement result is obtained. This scheme is precisely conventional qubit teleportation.

In the category $\mathbf{Rel}$, abstract teleportation instead can be interpreted in terms of encrypted communication.

Example 3.18. In $\mathbf{Rel}$, choose $L = R = 2 = \{0,1\}$, and $\eta^\dagger = \begin{pmatrix}1 & 0 & 0 & 1\end{pmatrix}$. There are two unitaries of type $2 \to 2$, as the unitaries are exactly the permutations (see Exercise 2.5.7):

$$U_0 = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \qquad\qquad U_1 = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

Choosing these as the family of unitaries U_i gives rise to the following effects:

$$e_0 = \begin{pmatrix}1 & 0 & 0 & 1\end{pmatrix} \qquad\qquad e_1 = \begin{pmatrix}0 & 1 & 1 & 0\end{pmatrix}$$

These form a complete set of effects, since they partition the set.

Perhaps surprisingly, we can interpret this as *classical encrypted communication* using a one-time pad. Let's step through the protocol to see how it works.

- Firstly, the relation $\eta\colon (0,0) \cup (1,1) \subset 2 \times 2$ describes the preparation of two systems in a correlated state, either both 0, or both 1. This creates a secret key. It is a nondeterministic process, which is obviously important for security, since if we always used the same key our messages would be easy to crack.

- Secondly, Alice takes her original message bit and her secret key bit, and verifies the effects $e_0\colon (0,0) \cup (1,1) \subset 2 \times 2$ and $e_1\colon (0,1) \cup (1,0) \cup 2 \times 2$. If she obtains result e_0, this means that her bits sum to 0 modulo 2, and if she obtains result e_1, this means that her bits sum to 1 modulo 2. So by testing these effects and recording which one is successful, she is essentially performing addition of her bits modulo 2. The value she obtains is the ciphertext. Note that for a given message bit, either value of the ciphertext is possible, since the secret key bit could have been 0 or 1. So as desired, knowledge of the ciphertext alone does not reveal any information about the original message.

- Finally, Alice communicates her measurement outcome to Bob. If it equals 0, he leaves his secret key bit alone; if it equals 1, he flips the value of his secret key bit using U_1. As a result, Bob's bit will now have the same value as Alice's original plaintext.

In this way, we see an interesting parallel between quantum and classical information processing. Identifying such structural similarities between disciplines is one of the main strengths of abstract approaches like category theory.

3.3 Interaction with linear structure

In the presence of dual objects, the tensor structure interacts well with the linear structure, such as superposition rule, biproducts and zero objects. This interaction indicates a fundamental relationship between the graphical calculus and linear structure.

3.3.1 Interaction with zero objects

We start by analyzing tensor products with zero objects and morphisms.

Lemma 3.19. *In a monoidal category with a zero object* 0*:*

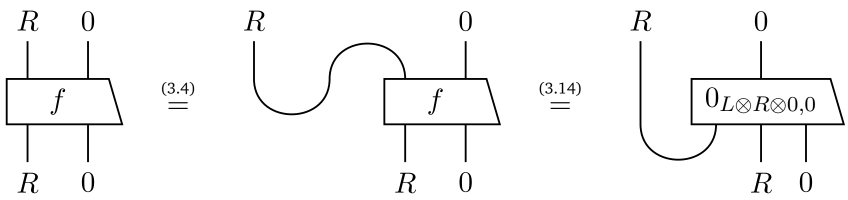
(a) $0 \dashv 0$*;*

(b) if $L \dashv R$*, then*

$$L \otimes 0 \simeq R \otimes 0 \simeq 0 \simeq 0 \otimes L \simeq 0 \otimes R. \tag{3.14}$$

Proof. Because $0 \otimes 0 \simeq 0$ by Lemma 2.30, there are unique morphisms $I \xrightarrow{\eta} 0 \otimes 0$ and $0 \otimes 0 \xrightarrow{\varepsilon} I$. It also follows that $0 \otimes (0 \otimes 0) \simeq 0$, so that both sides of the snake equation must equal the unique morphism $0 \to 0$. This establishes (a).

For (b), let $R \otimes 0 \xrightarrow{f} R \otimes 0$ be an arbitrary morphism. Then:



So there really is only one morphism $R \otimes 0 \to R \otimes 0$, namely the identity. Similarly, the only morphism of type $0 \to 0$ is the identity. Therefore the unique morphisms $R \otimes 0 \to 0$ and $0 \to R \otimes 0$ must be each other's inverse, showing that $R \otimes 0 \simeq 0$. The other claims follow similarly. □

Corollary 3.20 (Tensor with zero)**.** *In a monoidal category, let* A, B, C, D *be objects, and* $A \xrightarrow{f} B$ *a morphism. If one of* A *or* B *has either a left or a right dual, then:*

$$f \otimes 0_{C,D} = 0_{A \otimes C, B \otimes D}, \tag{3.15}$$

$$0_{C,D} \otimes f = 0_{C \otimes A, D \otimes B}. \tag{3.16}$$

Proof. Suppose A has a left or a right dual. The morphism $A \otimes C \xrightarrow{f \otimes 0_{C,D}} B \otimes D$ factors through $A \otimes 0$. But this object is isomorphic to 0 by Lemma 3.19(b). Hence $f \otimes 0_{C,D}$ must have been the zero morphism. Similarly, $0_{C,D} \otimes f$ is the zero morphism. A similar argument applies if B has a left or a right dual, since the objects $B \otimes 0$ and $0 \otimes B$ must then be zero objects. □

3.3.2 Interaction with biproducts

The next result shows that tensor products distribute over biproducts on the level of objects, provided the necessary dual objects exist.

Lemma 3.21 (Tensor distributes over biproduct)**.** *In a monoidal category with biproducts, let A, B, C be objects. If A has either a left or right dual, then the following morphisms are inverse to each other:*

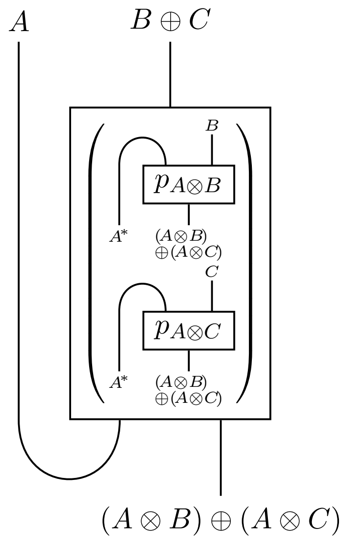
$$\begin{tikzcd}
A \otimes (B \oplus C) \arrow[rr, bend left, "{f = \begin{pmatrix} \mathrm{id}_A \otimes \begin{pmatrix}\mathrm{id}_B & 0_{C,B}\end{pmatrix} \\ \mathrm{id}_A \otimes \begin{pmatrix}0_{B,C} & \mathrm{id}_C\end{pmatrix} \end{pmatrix}}"] & & (A \otimes B) \oplus (A \otimes C) \arrow[ll, bend left, "{g = \begin{pmatrix} \mathrm{id}_A \otimes \begin{pmatrix}\mathrm{id}_B \\ 0_{B,C}\end{pmatrix} & \mathrm{id}_A \otimes \begin{pmatrix}0_{C,B} \\ \mathrm{id}_C\end{pmatrix} \end{pmatrix}}"]
\end{tikzcd}$$

Proof. Use Corollary 3.20 to see:

$$\begin{aligned}
f \circ g &= \begin{pmatrix} \mathrm{id}_A \otimes (\mathrm{id}_B + 0_{B,B}) & \mathrm{id}_A \otimes (0_{C,B} + 0_{C,B}) \\ \mathrm{id}_A \otimes (0_{B,C} + 0_{B,C}) & \mathrm{id}_A \otimes (0_{C,C} + \mathrm{id}_C) \end{pmatrix} \\
&= \begin{pmatrix} \mathrm{id}_{A\otimes B} & 0_{A\otimes C, A\otimes B} \\ 0_{A\otimes B, A\otimes C} & \mathrm{id}_{A\otimes C} \end{pmatrix} = \mathrm{id}_{(A\otimes B)\oplus(A\otimes C)}.
\end{aligned}$$

Hence f has a right inverse g. To show that it is invertible, and hence that g is a full inverse, we must find a left inverse to f. Suppose that $^*A \dashv A$, and consider the following morphism:

$g' =$



This diagram combines matrix calculus and graphical calculus. The central box is a column matrix representing a morphism $A^* \otimes ((A \otimes B) \oplus (A \otimes C)) \to B \oplus C$, and involves the biproduct projection morphisms $(A \otimes B) \oplus (A \otimes C) \xrightarrow{p_{A\otimes B}} A \otimes B$ and $(A\otimes B)\oplus(A\otimes C) \xrightarrow{p_{A\otimes C}} A\otimes C$. With this definition of g', it follows that $g' \circ f = \mathrm{id}_{A\otimes(B\oplus C)}$. Hence $g = (g' \circ f) \circ g = g' \circ (f \circ g) = g'$, and f and g are inverse to each other. The proof of the case where A has a right dual is similar. □

The presence of dual objects also guarantees that tensor products interact well with superpositions of morphisms, as the following lemma shows.

Lemma 3.22 (Tensor distributes over superposition)**.** *In a monoidal category with biproducts, let A, B, C, D be objects, and let $A \xrightarrow{f} B$ and $C \xrightarrow{g,h} D$ be morphisms. If A has either a left or a right dual, we have the following:*

$$(f \otimes g) + (f \otimes h) = f \otimes (g + h) \tag{3.17}$$
$$(g \otimes f) + (h \otimes f) = (g + h) \otimes f \tag{3.18}$$

Proof. Compose the morphisms of Lemma 3.21 for $B = C$ to obtain the identity on $A \otimes (C \oplus C)$. Applying the interchange law shows that this identity equals

$$A \otimes (C \oplus C) \xrightarrow{\mathrm{id}_A \otimes \begin{pmatrix} \mathrm{id}_C & 0_{C,C} \\ 0_{C,C} & 0_{C,C} \end{pmatrix} + \mathrm{id}_A \otimes \begin{pmatrix} 0_{C,C} & 0_{C,C} \\ 0_{C,C} & \mathrm{id}_C \end{pmatrix}} A \otimes (C \oplus C). \tag{3.19}$$

Now, by further applications of the matrix calculus and the interchange law:

$$f \otimes (g + h) = \big(\mathrm{id}_B \otimes \begin{pmatrix} \mathrm{id}_D & \mathrm{id}_D \end{pmatrix}\big) \circ \left(f \otimes \begin{pmatrix} g & 0 \\ 0 & h \end{pmatrix}\right) \circ \left(\mathrm{id}_A \otimes \begin{pmatrix} \mathrm{id}_C \\ \mathrm{id}_C \end{pmatrix}\right) \tag{3.20}$$

Inserting the identity in the form of morphism (3.19), and using the interchange law and distributivity of composition over superposition (2.9), gives

$$\begin{aligned} f \otimes \begin{pmatrix} g & 0 \\ 0 & h \end{pmatrix} &= \left(f \otimes \begin{pmatrix} g & 0 \\ 0 & h \end{pmatrix}\right) \circ \left(\mathrm{id}_A \otimes \begin{pmatrix} \mathrm{id}_C & 0_{C,C} \\ 0_{C,C} & 0_{C,C} \end{pmatrix} + \mathrm{id}_A \otimes \begin{pmatrix} 0_{C,C} & 0_{C,C} \\ 0_{C,C} & \mathrm{id}_C \end{pmatrix}\right) \\ &= \left(f \otimes \begin{pmatrix} g & 0 \\ 0 & 0 \end{pmatrix}\right) + \left(f \otimes \begin{pmatrix} 0 & 0 \\ 0 & h \end{pmatrix}\right). \end{aligned}$$

Substituting this into equation (3.20):

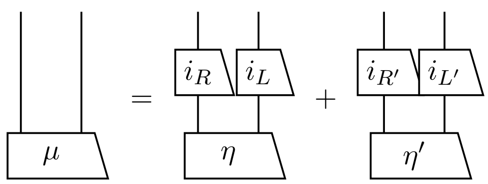
$$\begin{aligned} f \otimes (g + h) &= \big(\mathrm{id}_B \otimes \begin{pmatrix} \mathrm{id}_D & \mathrm{id}_D \end{pmatrix}\big) \circ \left(f \otimes \begin{pmatrix} g & 0 \\ 0 & 0 \end{pmatrix} + f \otimes \begin{pmatrix} 0 & 0 \\ 0 & h \end{pmatrix}\right) \circ \left(\mathrm{id}_A \otimes \begin{pmatrix} \mathrm{id}_C \\ \mathrm{id}_C \end{pmatrix}\right) \\ &= f \otimes \left(\begin{pmatrix} \mathrm{id}_D & \mathrm{id}_D \end{pmatrix} \circ \begin{pmatrix} g & 0 \\ 0 & 0 \end{pmatrix} \circ \begin{pmatrix} \mathrm{id}_C \\ \mathrm{id}_C \end{pmatrix}\right) + f \otimes \left(\begin{pmatrix} \mathrm{id}_D & \mathrm{id}_D \end{pmatrix} \circ \begin{pmatrix} 0 & 0 \\ 0 & h \end{pmatrix} \circ \begin{pmatrix} \mathrm{id}_C \\ \mathrm{id}_C \end{pmatrix}\right) \\ &= (f \otimes g) + (f \otimes h) \end{aligned}$$

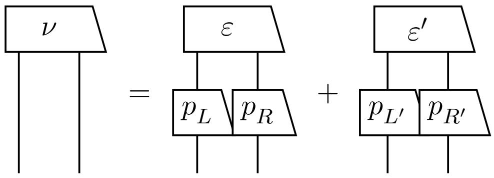
The equation $(g + h) \otimes f = (g \otimes f) + (h \otimes f)$ can be proved similarly. □

Finally, taking biproducts preserves dual objects.

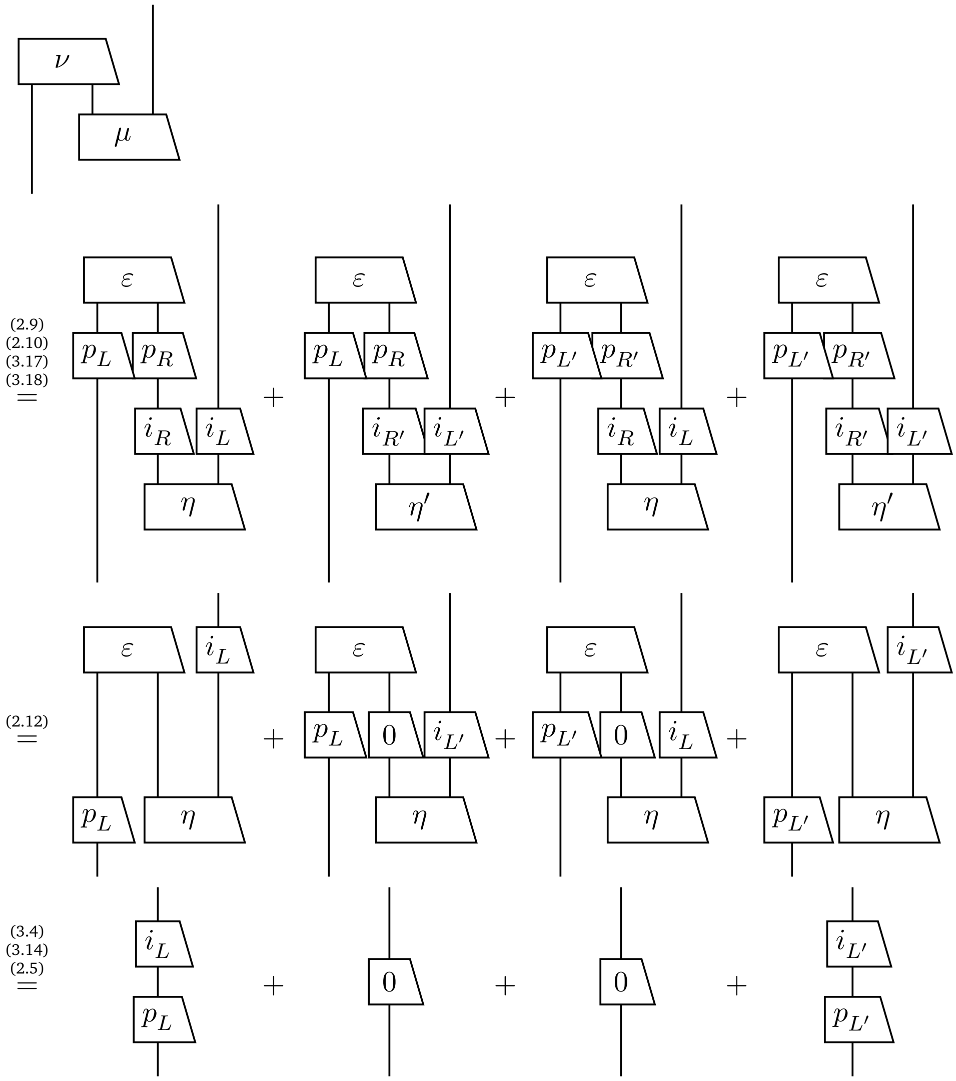
Lemma 3.23 (Biproducts preserve duals)**.** *In a monoidal category with duals and biproducts, $L \dashv R$ and $L' \dashv R'$ imply $L \oplus L' \dashv R \oplus R'$.*

Proof. Let $I \xrightarrow{\eta} R \otimes L$, $L \otimes R \xrightarrow{\varepsilon} I$, $I \xrightarrow{\eta'} R' \otimes L'$ and $L' \otimes R' \xrightarrow{\varepsilon'} I$ be maps witnessing the dualities, and write $L \xrightarrow{i_L} L \oplus L'$, $L' \xrightarrow{i_{L'}} L \oplus L'$, $R \xrightarrow{i_R} R \oplus R'$ and $R' \xrightarrow{i_{R'}} R \oplus R'$ for the biproduct injections, and $p_{[-]}$ for the corresponding projections. Then define the following candidate morphisms $I \xrightarrow{\mu} (R \oplus R') \otimes (L \oplus L')$ and $(L \oplus L') \otimes (R \oplus R') \xrightarrow{\nu} I$ for the duality $L \oplus L' \dashv R \oplus R'$:





The first snake equation (3.4) can then be established as follows:



$$\stackrel{(2.14)}{=} \mathrm{id}_{L\oplus L'}$$

The second snake equation can be established with a similar argument. □

3.4 Pivotality

For a finite-dimensional vector space, there is an isomorphism $V^{**} \simeq V$. This section will show categorically why this map exists and is invertible, and investigate the strong extra properties it endows the graphical calculus with.

Definition 3.24 (Pivotal category)**.** A monoidal category with right duals is *pivotal* when it is equipped with a monoidal natural transformation $A \xrightarrow{\pi_A} A^{**}$.

Concretely, this means π_A must satisfy the following equations, where the canonical isomorphisms arising from Lemma 3.16 are denoted $A^{**} \otimes B^{**} \xrightarrow{\phi_{A,B}} (A \otimes B)^{**}$ and $I \xrightarrow{\psi} I^{**}$:

$$\begin{tikzcd} & A \otimes B \arrow[dl, "\pi_A \otimes \pi_B"'] \arrow[dr, "\pi_{A\otimes B}"] & \\ A^{**} \otimes B^{**} \arrow[rr, "\phi_{A,B}"'] & & (A \otimes B)^{**} \end{tikzcd} \qquad \pi_I = \psi \tag{3.21}$$

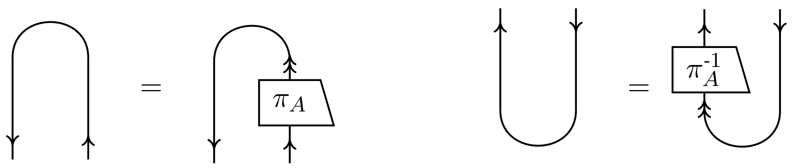
3.4.1 Basic properties

Like with dual objects, let's build some intuition for pivotal structure by exploring their mathematical properties.

Corollary 3.25. *In a pivotal category, the morphisms $A \xrightarrow{\pi_A} A^{**}$ are invertible.*

Proof. Follows from Theorem 3.15. □

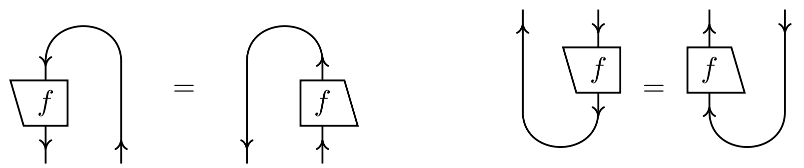
In the graphical calculus for a pivotal category we define the following abbreviations, where again $\Uparrow$ indicates the double right dual:



(3.22)

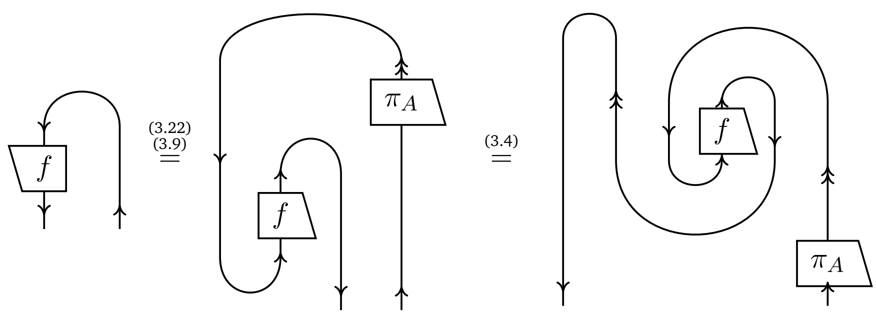
Note that the above makes use of Corollary 3.25. With these extra cups and caps, Lemma 3.12 extends to arbitrary sliding of morphisms.

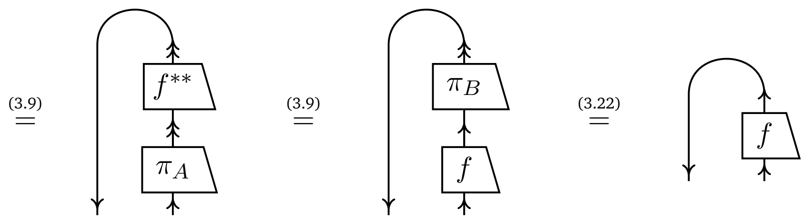
Lemma 3.26 (Sliding)**.** *In a pivotal category, for all morphisms $A \xrightarrow{f} B$:*



(3.23)

Proof. The first equality is proven as follows:



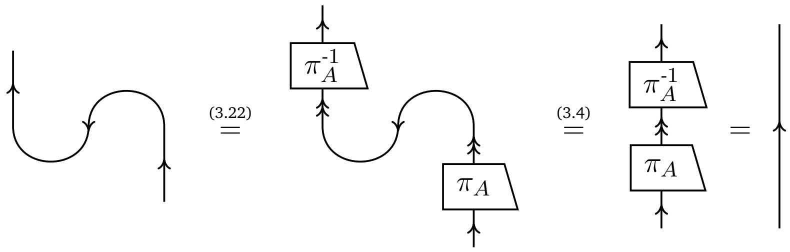


The second equality is derived similarly. □

The pivotal structure says that taking right duals twice is equivalent to doing nothing. But since taking the left dual and taking the right dual are inverse processes, a pivotal structure can also be presented as an equivalence between left duals and right duals.

Theorem 3.27. *In a pivotal category, every object has a left dual.*

Proof. One of the left duality equations is established as follows:

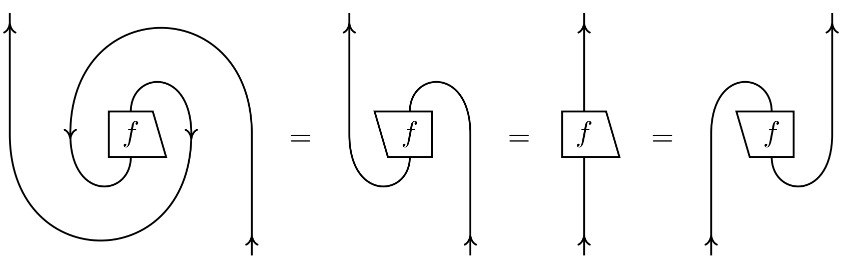


The other equation is proved similarly. □

In general, a pivotal structure allows arbitrary oriented isotopies of the plane as legal graphical transformations.

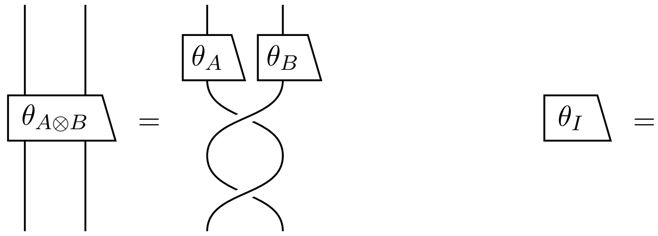
Theorem 3.28 (Correctness of the graphical calculus for pivotal categories)**.** *In a pivotal category, a well-formed equation between morphisms follows from the axioms if and only if it holds in the graphical language up to planar oriented isotopy.*

The new feature of this correctness theorem is the word *oriented*. The wires of our diagram now have arrows, and a valid isotopy must preserve them. For example, the following are valid isotopies:



In the presence of a braiding, pivotal structure can be expressed in terms of a twist.

Definition 3.29 (Balanced, twist)**.** A braided monoidal category is *balanced* when it is equipped with a natural isomorphism $\theta_A \colon A \to A$ called a *twist*, satisfying the following equations:



(3.24)

The second equation here says $\theta_I = \mathrm{id}_I$.

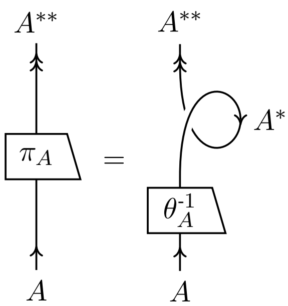
Example 3.30. Every symmetric monoidal category admits the trivial twist $\theta_A = \mathrm{id}_A$.

Example 3.31. The symmetric monoidal dagger category **SuperHilb** admits a nontrivial twist $\theta_{(H,K)} = (\mathrm{id}_H, -\mathrm{id}_K)$, as well as the trivial twist of Example 3.30.

Example 3.32. The braided monoidal dagger category **Fib** admits a nontrivial balanced structure, with $\theta_I = \mathrm{id}_I$ and $\theta_\tau = e^{4\pi i/5}\,\mathrm{id}_\tau$. The methods of Section 2.3.4 allow us to verify $\theta_{\tau\otimes\tau} = (\theta_\tau \otimes \theta_\tau) \cdot \sigma^2_{\tau,\tau}$ (see Exercise 3.5.19).

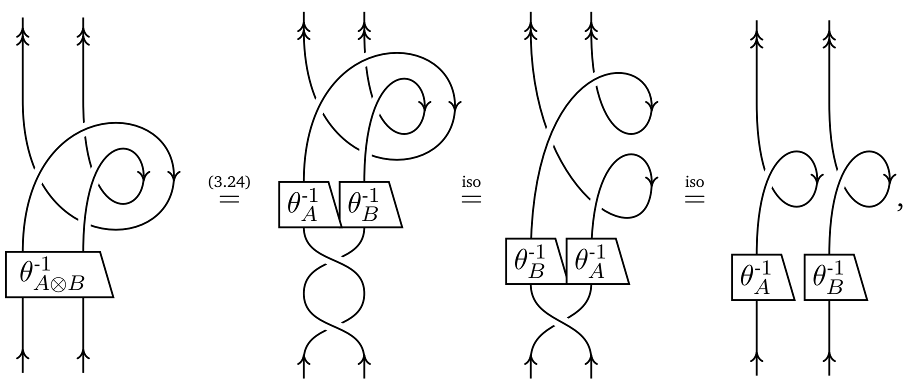
Theorem 3.33. *In a braided monoidal category with right duals, a pivotal structure uniquely induces a twist structure, and vice versa.*

Proof. Suppose given a twist structure $\theta_A \colon A \to A$. Define a pivotal structure as follows:

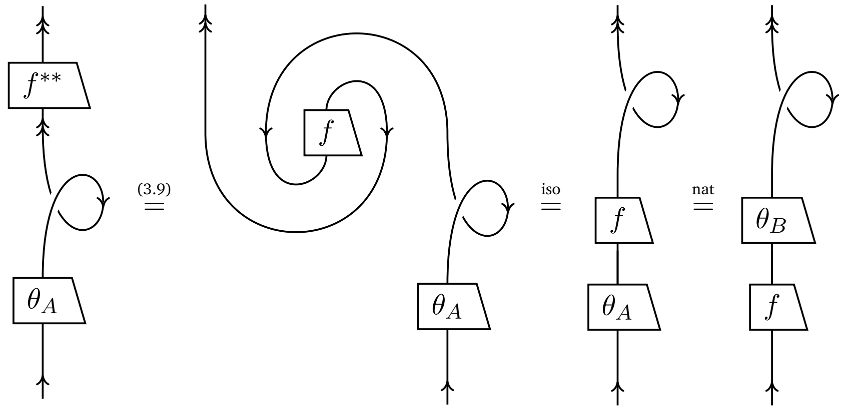


(3.25)

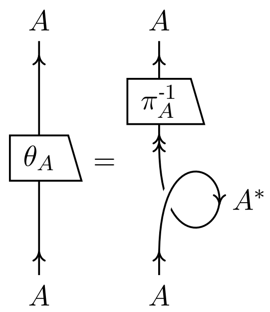
We must verify that the transformation π_A is natural and monoidal. For the latter, observe that $\pi_{A\otimes B}$ equals



which is $\pi_A \otimes \pi_B$. For simplicity the above computation suppressed the canonical isomorphism $(A \otimes B)^{**} \simeq A^{**} \otimes B^{**}$. To see naturality, let $A \xrightarrow{f} B$, and compute:



Conversely, given a pivotal structure, define a balanced structure as follows:



(3.26)

The balanced equations (3.24) follows from the pivotality equations (3.21) by a calculation similar to the one above. The constructions (3.25) and (3.26) are clearly inverse to each other. □

3.4.2 Compact categories

When a braided monoidal category with duals is symmetric, there is a canonical choice of balancing.

Definition 3.34. A *compact category* is a pivotal symmetric monoidal category where the canonical twist of Theorem 3.33 is the identity; that is, $\theta_A = \mathrm{id}_A$.

Remark 3.35. Any symmetric monoidal category in which every object has a right dual is compact in a canonical way: combining Lemmas 3.4 and 3.8 provides a canonical choice of the pivotal structure that automatically satisfies the requirements of the previous definition. But note that in general, as illustrated by Example 3.31, other balancings may exist; that is, it is possible for a balanced symmetric monoidal category with duals *not* to be compact.

Example 3.36. Since they are symmetric monoidal categories with duals, our main example categories $\mathbf{FHilb}$, $\mathbf{FVect}$, $\mathbf{Mat}_{\mathbb{C}}$, $\mathbf{Rel}$ can all be given the structure of a compact category, as can $\mathbf{SuperHilb}$. Of course, $\mathbf{Fib}$ does not admit a compact structure, since it is not symmetric monoidal.

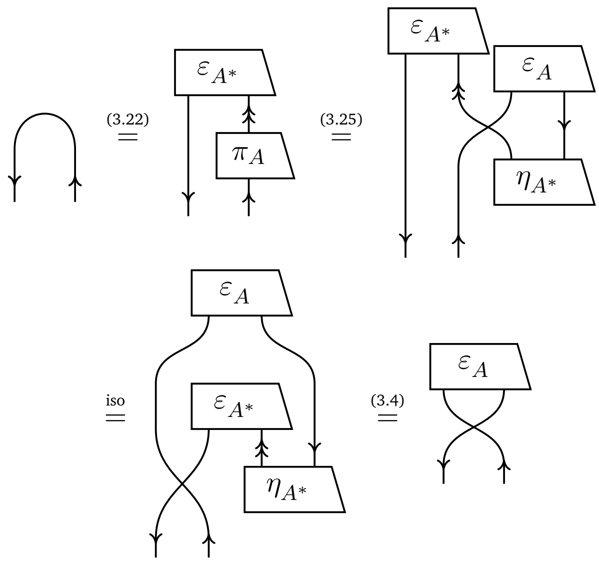
Compact categories have a particularly simple graphical calculus.

Lemma 3.37. *In a compact category, the following equations hold:*

(3.27)

(3.28)

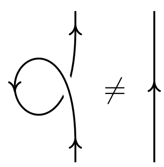
Proof. Let's prove the second equation of (3.27):



The others are proved in a similar way. □

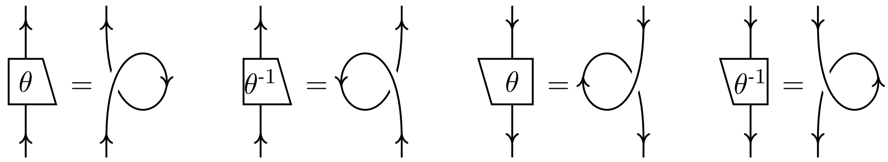
3.4.3 Ribbon categories

When using the graphical calculus for braided pivotal categories, we need to be careful with loops on a single strand. You might think that correctness of the graphical calculus for pivotal categories (see Theorem 3.28 above) implies that a loop equals the identity. But this isn't true, because the correctness theorem only allows *planar* oriented isotopy, not spatial oriented isotopy:



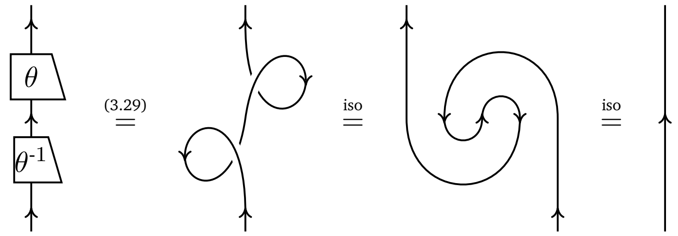
In fact, a loop on a single strand is directly related to the twist.

Lemma 3.38. *In a braided pivotal category, the following equations hold:*



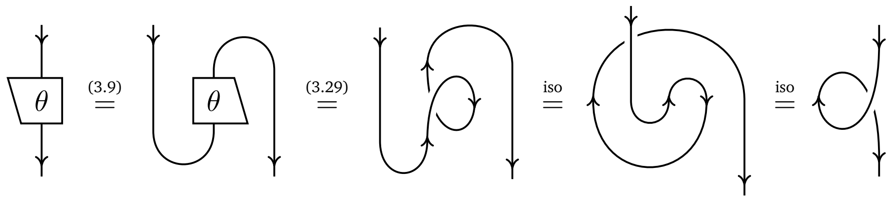
(3.29)

Proof. The first of these comes directly from equation (3.26) giving the twist in terms of the pivotal structure, using equations (3.22) defining the graphical calculus for a pivotal category. To verify the expression for θ^{-1}:



The equation $\theta \circ \theta^{-1} = \mathrm{id}$ follows similarly. Since inverses in a category are unique (see Lemma 0.8), the expression for θ^{-1} above is correct.

As for the graphical form of θ^*:



The graphical form for $(\theta^{-1})^*$ is proven in a similar way. □

In a balanced braided monoidal category with duals, it is natural to ask the twist to be compatible with the duals.

Definition 3.39. A *ribbon* or *tortile* category is a balanced monoidal category with duals, such that $(\theta_A)^* = \theta_{A^*}$.

The ribbon property has a satisfactory graphical characterization.

Corollary 3.40. *A balanced monoidal category with duals is a ribbon category if and only if either of these equivalent equations are satisfied:*

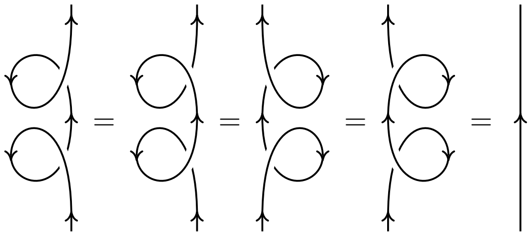
(3.30)

Proof. Follows from Lemma 3.38. □

Corollary 3.41. *A compact category is a ribbon category.*

Proof. Equations (3.30) follow from 3.28. □

Corollary 3.42. *In a ribbon category, the following equations hold:*



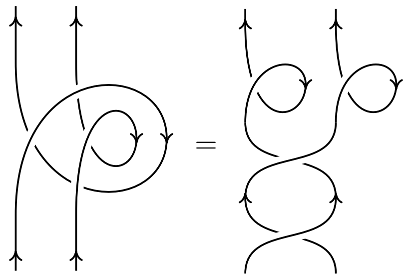
(3.31)

Proof. Apply Lemma 3.38. □

These are exactly the equations we would expect to be satisfied by *ribbons* in an ambient three-dimensional space. The correctness theorem for the ribbon category graphical calculus makes this precise.

Theorem 3.43 (Correctness of the graphical calculus for ribbon categories)**.** *A well-formed equation between morphisms in a ribbon category follows from the axioms if and only if it holds in the graphical language up to framed isotopy in three dimensions.*

Framed isotopy is the name for the version of isotopy where the strands are thought of as ribbons, rather than just wires. To get a feeling for framed isotopy, find some ribbons, or make some from strips of of paper. Use them to verify equations (3.30) and (3.31), and also the balancing equation (3.24) specialized to ribbon categories:

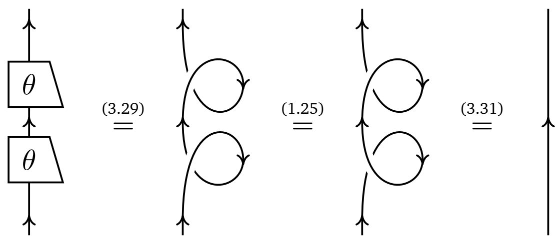


(3.32)

A symmetric ribbon category puts a strong constraint on the twist θ. Remember that a symmetric ribbon category is not necessarily a compact category, which would have $\theta = \mathrm{id}$.

Lemma 3.44. *In a symmetric ribbon category,* $\theta \circ \theta = \mathrm{id}$.

Proof. Graphically:



Intuitively, if a ribbon can pass through itself, a double twist can be removed. □

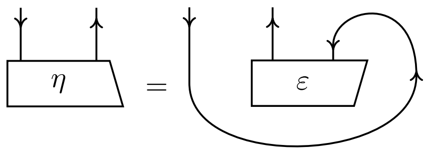
3.4.4 Dagger duality

We now consider the interaction of pivotal structure with dagger structure, building up to Theorem 3.50 which proves that maximally-entangled states are unique up to unique unitary isomorphism, and Definition 3.51 of a dagger pivotal category.

Lemma 3.45. *In a monoidal dagger category, $L \dashv R \Leftrightarrow R \dashv L$.*

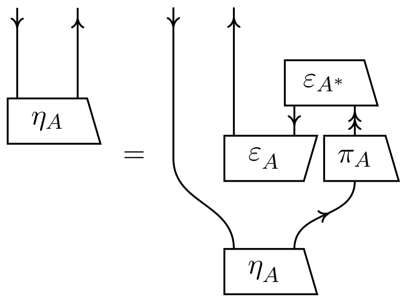
Proof. Follows directly from the axiom $(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger$ of a monoidal dagger category. $\square$

Definition 3.46. In a dagger category with a pivotal structure, a *dagger dual* is a duality $A \dashv A^*$ witnessed by morphisms $I \xrightarrow{\eta} A^* \otimes A$ and $A \otimes A^* \xrightarrow{\varepsilon} I$ that satisfy the following equation:



(3.33)

Unpacking the pivotal structure, the previous equation takes the following form:

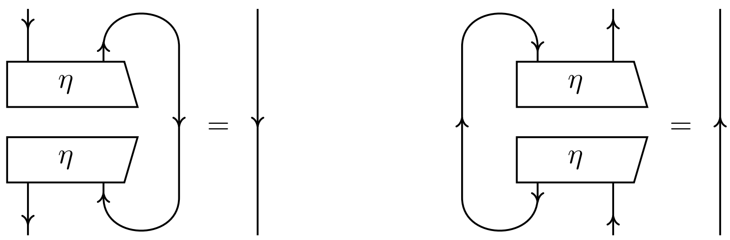


(3.34)

Rearranging this expression gives an explicit formula for π_A, which Proposition 3.52 below explores.

Dagger duality is equivalent to the notion of maximally entangled state from quantum theory (see Definition 0.72).

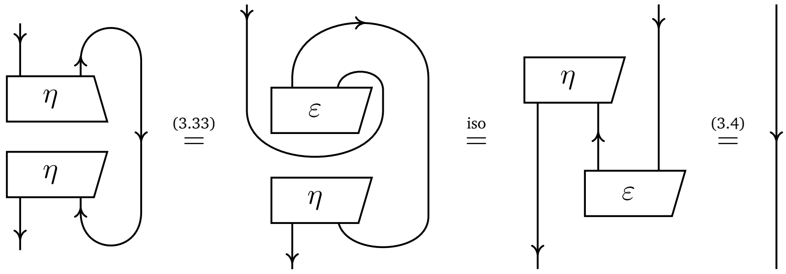
Definition 3.47. In a dagger category with a pivotal structure, a *maximally entangled state* $I \xrightarrow{\eta} A^* \otimes A$ is a bipartite state satisfying:



(3.35)

Lemma 3.48. *In a dagger category with a pivotal structure, a bipartite state is maximally entangled if and only if it is part of a dagger duality.*

Proof. Use the dagger dual condition (3.33) to verify the first equation of (3.35):

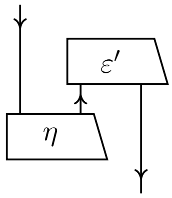


The central isotopy here is a bit hard to see; the box ε makes a full rotation. The other equation, and the reverse implication, can be proved in a similar way. □

Dagger dualities have strong uniqueness properties.

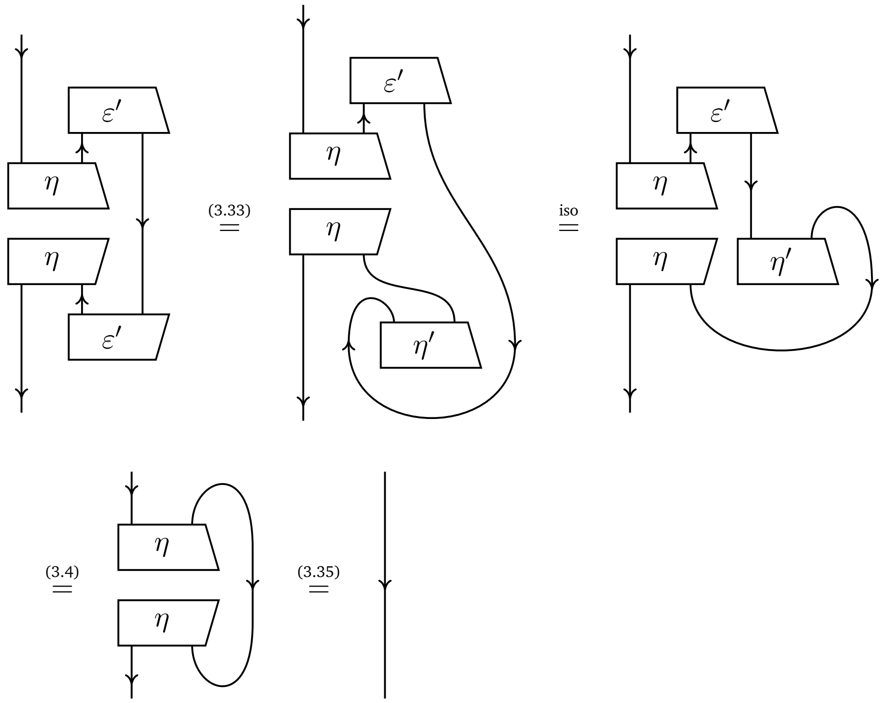
Lemma 3.49. *In a dagger category with a pivotal structure, dagger duals are unique up to unique unitary isomorphism.*

Proof. Given dagger duals $(L \dashv R, \eta, \varepsilon)$ and $(L \dashv R', \eta', \varepsilon')$, construct an isomorphism $R \simeq R'$ as for Lemma 3.4 as follows:



(3.36)

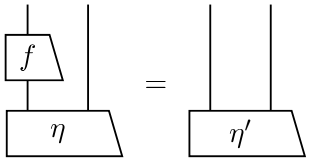
The following calculation establishes that this is a co-isometry:



As with the previous proof, the central isotopy here is a bit tricky to see; the η' morphism performs a full anticlockwise rotation. Similarly, it can be shown that equation (3.36) is also an isometry, and hence unitary. Uniqueness is straightforward. □

Putting the previous results together proves the following theorem about maximally-entangled states.

Theorem 3.50. *In a dagger category with a pivotal structure, for any two maximally entangled states $I \xrightarrow{\eta,\eta'} A \otimes B$ there is a unique unitary $A \xrightarrow{f} A$ satisfying:*



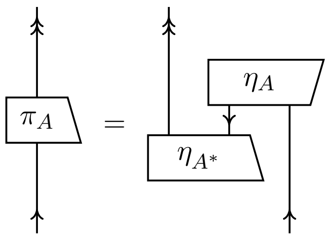
(3.37)

Proof. Follows from Lemmas 3.48 and 3.49. □

We can now give the appropriate compatibility condition between the pivotal structure and dagger dualities on the same category.

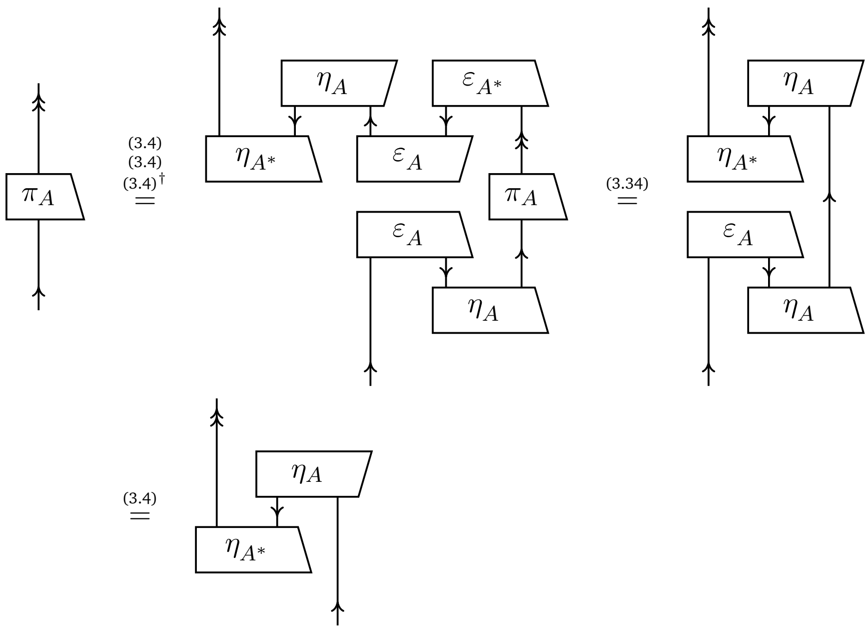
Definition 3.51. A *dagger pivotal category* is a monoidal dagger category with a pivotal structure, such that the chosen right duals are all dagger duals.

Proposition 3.52. *In a dagger pivotal category, the pivotal structure is given by the following composite:*



(3.38)

Proof. Use expression (3.34):

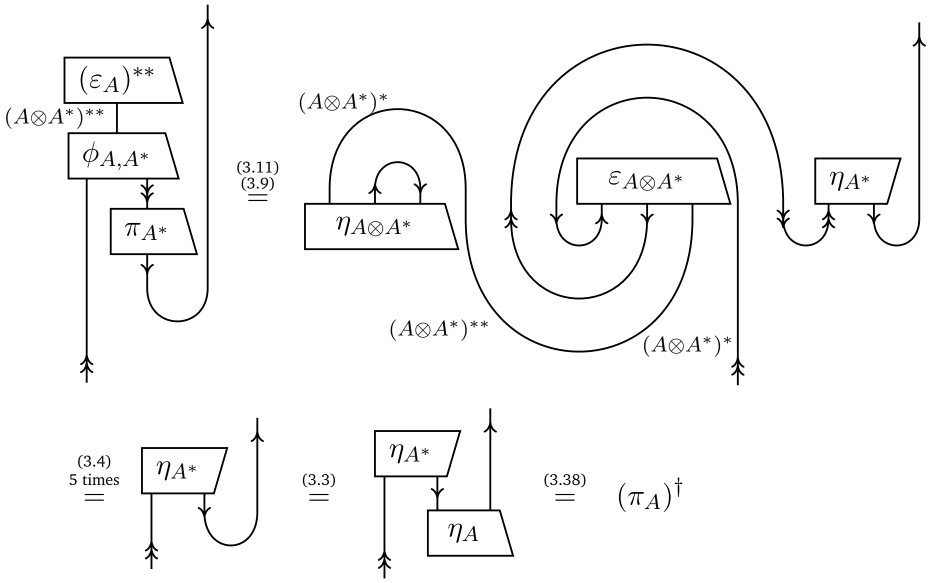


This completes the proof. □

The following result is simple to state, but its proof requires the full power of the technology built up in this chapter.

Proposition 3.53. *In a dagger pivotal category, the pivotal structure is unitary.*

Proof. By the proof of Theorem 3.15, π_A^{-1} equals



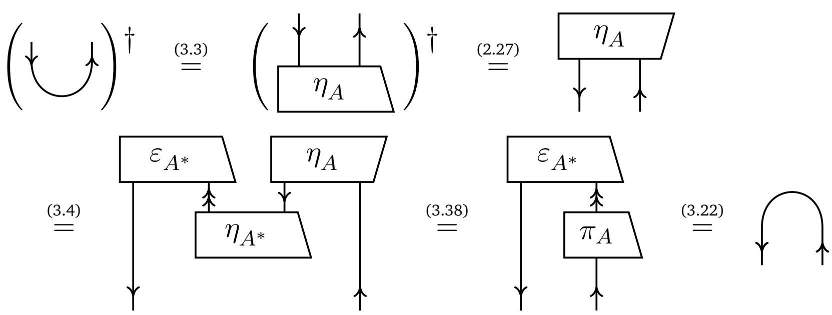
This completes the proof. □

Dagger pivotal categories have a good graphical calculus, where the dagger acts as reflection along a horizontal axis.

Lemma 3.54. *In a dagger pivotal category, the following equations hold:*

(3.39)

Proof. First consider the first equation:



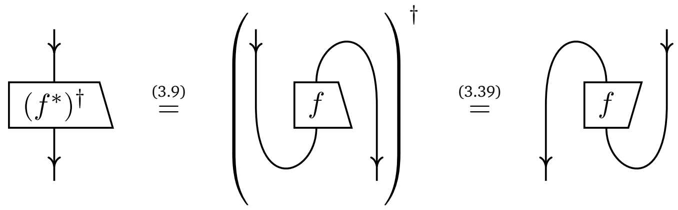
The second equation then follows by Lemma 3.5. □

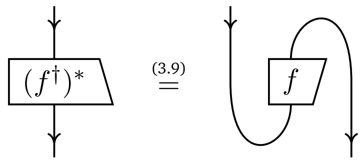
Furthermore, the dagger functor and right-duals functor commute.

Lemma 3.55. *In a dagger pivotal category, every morphism f satisfies:*

$$(f^*)^\dagger = (f^\dagger)^* \tag{3.40}$$

Proof. Compute both sides:





These are isotopic, and hence equal by Theorem 3.28. □

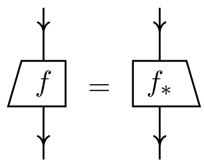
It is useful to give the composite of the dagger functor and right-duals functor a special name.

Definition 3.56 (Conjugation)**.** On a dagger pivotal category, *conjugation* $(-)_*$ is the composite of the dagger functor and the right-duals functor:

$$(-)_* = (-)^{*\dagger} = (-)^{\dagger *}$$

Since the dagger is the identity on objects $A_* = A^*$. Also, since $(-)^*$ and taking daggers are both contravariant, the conjugation functor is covariant.

We denote conjugation graphically by reflecting about a vertical axis:



According to the way of the dagger, the dagger should interact with ribbon or compact structure when present.

Definition 3.57. A *ribbon dagger category* is a braided dagger pivotal category with unitary braiding and twist. A *compact dagger category* is a symmetric dagger pivotal category with unitary symmetry, and $\theta = \mathrm{id}$.

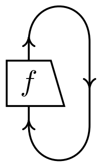
Example 3.58. Our examples $\mathbf{FHilb}$, $\mathbf{Mat}_{\mathbb{C}}$ and $\mathbf{Rel}$ are all dagger compact categories.

- On $\mathbf{FHilb}$, the conjugation functor gives the conjugate of a linear map.
- On $\mathbf{Mat}_{\mathbb{C}}$, the conjugation functor gives the conjugate of a matrix, with each matrix entry replaced by its conjugate as a complex number.
- On $\mathbf{Rel}$, the conjugation functor is the identity.

3.4.5 Traces and dimensions

Just like monoidal categories abstract scalars and scalar multiplication, dagger categories abstract inner products, and biproducts abstract a matrix calculus (see Chapter 2), pivotal categories have good notions of trace and dimension.

Definition 3.59 (Trace)**.** In a pivotal category, the *trace* of a morphism $A \xrightarrow{f} A$ is the following scalar:



(3.41)

It is denoted by $\mathrm{Tr}(f)$, or sometimes $\mathrm{Tr}_A(f)$ to emphasize A (not to be confused with the partial trace of Proposition 0.71).

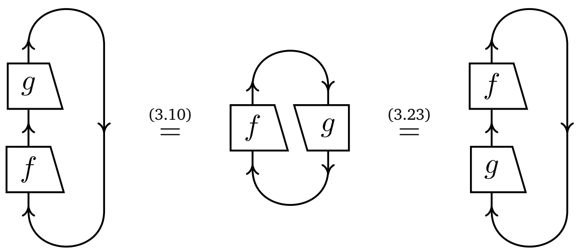
A trace $\mathrm{Tr}^\beta(f)$ can also be defined for a braided monoidal category with duals, but without necessarily having a pivotal structure; see Exercise 3.5.7 to investigate this. We focus on the pivotal notion here.

Definition 3.60 (Dimension)**.** In a pivotal category, the *dimension* of an object A is the scalar $\dim(A) = \mathrm{Tr}(\mathrm{id}_A)$.

This abstract trace operation, like its concrete cousin from linear algebra, enjoys the familiar cyclic property.

Lemma 3.61. *In a pivotal category,* $\mathrm{Tr}_A(g \circ f) = \mathrm{Tr}_B(f \circ g)$ *for* $A \xrightarrow{f} B$ *and* $B \xrightarrow{g} A$*.*

Proof. Graphically:



The morphism g slides around the circle, and ends up underneath the morphism f. □

Example 3.62. To determine $\mathrm{Tr}(f)$ for a morphism $H \xrightarrow{f} H$ in **FHilb**, substitute equations (3.6) and (3.5) into the definition of the abstract trace (3.41). This gives $\mathrm{Tr}(f) = \sum_i \langle i|f|i\rangle$, so the abstract trace of f is in fact the usual trace of f from linear algebra. Therefore, for an object H of **FHilb**, also $\dim(H) = \mathrm{Tr}(\mathrm{id}_H)$ equals the usual dimension of H.

Abstract traces satisfy many properties familiar from linear algebra.

Lemma 3.63. *In a pivotal category, the trace has the following properties:*

(a) $\mathrm{Tr}_A(f + g) = \mathrm{Tr}_A(f) + \mathrm{Tr}_A(g)$ *for any superposition rule;*

(b) $\mathrm{Tr}_{A\oplus B}\begin{pmatrix} f & g \\ h & j \end{pmatrix} = \mathrm{Tr}_A(f) + \mathrm{Tr}_B(j)$ *if there are biproducts;*

(c) $\mathrm{Tr}_I(s) = s$ *for any scalar* $I \xrightarrow{s} I$*;*

(d) $\mathrm{Tr}_A(0_{A,A}) = 0_{I,I}$ *if there is a zero object;*

(e) $\mathrm{Tr}_{A\otimes B}(f \otimes g) = \mathrm{Tr}_A(f) \circ \mathrm{Tr}_B(g)$ *in a braided pivotal category;*

(f) $\big(\mathrm{Tr}_A(f)\big)^\dagger = \mathrm{Tr}_A(f^\dagger)$ *in a dagger pivotal category.*

Proof. Property (a) follows directly from Lemma 3.22 and compatibility of addition with composition as in equation (2.9). For property (b), use the cyclic property of Lemma 3.61:

$$\begin{aligned}
&\mathrm{Tr}_{A\oplus B}\begin{pmatrix} f & g \\ h & j \end{pmatrix} \\
&= \mathrm{Tr}_{A\oplus B}(i_A \circ f \circ p_A) + \mathrm{Tr}_{A\oplus B}(i_A \circ g \circ p_B) + \mathrm{Tr}_{A\oplus B}(i_B \circ h \circ p_A) + \mathrm{Tr}_{A\oplus B}(i_B \circ j \circ p_B) \\
&= \mathrm{Tr}_A(f \circ p_A \circ i_A) + \mathrm{Tr}_A(g \circ p_B \circ i_A) + \mathrm{Tr}_B(h \circ p_A \circ i_B) + \mathrm{Tr}_B(j \circ p_B \circ i_B) \\
&= \mathrm{Tr}_A(f) + \mathrm{Tr}_B(j).
\end{aligned}$$

Property (c) follows from $\mathrm{Tr}_I(s) = s \bullet \mathrm{id}_I = s$, which trivializes graphically. For property (d): because $0_{A,A} \otimes \mathrm{id}_{A^*} = 0_{A\otimes A^*, A\otimes A^*}$ by Corollary 3.20, also $\mathrm{Tr}_A(0_{A,A}) = \varepsilon \circ (0_{A,A} \otimes \mathrm{id}_{A^*}) \circ \sigma \circ \eta = 0_{I,I}$. Property (e) follows because the traces over A and B can separate in a braided monoidal category; the inner one is not trapped by the outer one. Finally, property (f) follows from correctness of the graphical language for dagger pivotal categories. □

This immediately yields some properties of dimensions of objects.

Lemma 3.64. *In a braided pivotal category, the following properties hold:*

(a) $\dim(A \oplus B) = \dim(A) + \dim(B)$ *if there are biproducts;*

(b) $\dim(I) = \mathrm{id}_I$*;*

(c) $\dim(0) = 0_{I,I}$ *if there is a zero object;*

(d) $A \simeq B \Rightarrow \dim(A) = \dim(B)$*;*

(e) $\dim(A \otimes B) = \dim(A) \circ \dim(B)$ *in a braided pivotal category.*

Proof. Properties (a)–(c) and (e) are straightforward consequences of Lemma 3.63. Property (d) follows from the cyclic property of the trace demonstrated in Lemma 3.61: if $A \xrightarrow{k} B$ is an isomorphism, then $\dim(A) = \mathrm{Tr}_A(k^{-1} \circ k) = \mathrm{Tr}_B(k \circ k^{-1}) = \dim(B)$. □

Using these results, we can give a simple argument that infinite-dimensional Hilbert spaces cannot have duals.

Corollary 3.65. *In* **Hilb***, infinite-dimensional Hilbert spaces do not have duals.*

Proof. Suppose H is an infinite-dimensional Hilbert space. Then there is an isomorphism $H \oplus \mathbb{C} \simeq H$. If H had a dual, then by properties (a) and (d) of Lemma 3.64 this would imply $\dim(H) + 1 = \dim(H)$, which has no solutions for $\dim(H) \in \mathbb{C}$. □

As a consequence of the existence of an 'infinite' object A satisfying $A \oplus I \simeq A$, in any monoidal category where scalar addition is invertible (or at least *cancellative*, i.e. satisfying $a+b = a+c \Leftrightarrow b = c$ for all scalars a, b, c) we conclude that $\mathrm{id}_I = 0_{I,I}$, which can only be satisfied in a trivial category.

This argument would not apply in $\mathbf{Rel}$, because there $\mathtt{true}\,\mathtt{or}\,\mathtt{true} = \mathtt{true}$, that is, $\mathrm{id}_1 + \mathrm{id}_1 = \mathrm{id}_1$. And indeed, as we have seen at the beginning of this chapter, both finite and infinite sets are self-dual in this category, despite the fact that sets S of infinite cardinality can be equipped with isomorphisms $S \simeq S + 1$.

3.5 Exercises

Exercise 3.5.1. Suppose that $L \dashv R$ are dual objects in a monoidal category, and that the cup $I \xrightarrow{\eta} R \otimes L$ is a product state. Show that id_L and id_R must factor through I. Conclude that, in our interpretation of graphical diagrams as observable histories, η is always an entangled state, except in degenerate situations.

Exercise 3.5.2. Recall the notion of local equivalence from Exercise 1.4.7. In $\mathbf{Hilb}$, we can write a state $\mathbb{C} \xrightarrow{\phi} \mathbb{C}^2 \otimes \mathbb{C}^2$ as a column vector

$$\phi = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix},$$

or as a matrix

$$M_\phi = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

(a) Show that ϕ is an entangled state if and only if M_ϕ is invertible. (Hint: a matrix is invertible if and only if it has nonzero determinant.)

(b) Show that $M_{(\mathrm{id}_{\mathbb{C}^2} \otimes f) \circ \phi} = M_\phi \circ f^{\mathrm{T}}$, where $\mathbb{C}^2 \xrightarrow{f} \mathbb{C}^2$ is any linear map and f^{T} is the transpose of f in the canonical basis of $\mathbb{C}^2$.

(c) Use this to show that there are three families of locally equivalent joint states of $\mathbb{C}^2 \otimes \mathbb{C}^2$.

Exercise 3.5.3. Pick a basis $\{e_i\}$ for a finite-dimensional vector space V, and define $\mathbb{C} \xrightarrow{\eta} V \otimes V$ and $V \otimes V \xrightarrow{\varepsilon} \mathbb{C}$ by $\eta(1) = \sum_i e_i \otimes e_i$ and $\varepsilon(e_i \otimes e_i) = 1$, and $\varepsilon(e_i \otimes e_j) = 0$ when $i \neq j$.

(a) Show that this satisfies the snake equations, and hence that V is dual to itself in the category $\mathbf{FVect}$.

(b) Show that f^* is given by the transpose of the matrix of the morphism $V \xrightarrow{f} V$ (where the matrix is written with respect to the basis $\{e_i\}$).

(c) Suppose that $\{e_i\}$ and $\{e_i'\}$ are both bases for V, giving rise to two units η, η' and two counits $\varepsilon, \varepsilon'$. Let $V \xrightarrow{f} V$ be the 'change-of-base' isomorphism $e_i \mapsto e_i'$. Show that $\eta = \eta'$ and $\varepsilon = \varepsilon'$ if and only if f is *(complex) orthogonal*, i.e. $f^{-1} = f^*$.

Exercise 3.5.4. In $\mathbf{FVect}$, suppose that $L \dashv R$ with unit η and counit ε. Pick a basis $\{r_i\}$ for R.

(a) Show that there are unique $l_i \in L$ satisfying $\eta(1) = \sum_i r_i \otimes l_i$.

(b) Show that every $l \in L$ can be written as a linear combination of the l_i, and hence that the map $R \xrightarrow{f} L$, defined by $f(r_i) = l_i$, is surjective.

(c) Show that f is an isomorphism, and hence that $\{l_i\}$ must be a basis for L.

(d) Conclude that any duality $L \dashv R$ in $\mathbf{FVect}$ is of the following *standard form* for a basis $\{l_i\}$ of L and a basis $\{r_i\}$ of R:

$$\eta(1) = \sum_i r_i \otimes l_i, \qquad \varepsilon(l_i \otimes r_j) = \delta_{ij}. \tag{3.42}$$

Exercise 3.5.5. In $\mathbf{FHilb}$, let $L \dashv R$ be dagger dual objects with unit η and counit ε.

(a) Use the previous exercise to show that there are an orthonormal basis $\{r_i\}$ of R and a basis $\{l_i\}$ of L such that $\eta(1) = \sum_i r_i \otimes l_i$ and $\varepsilon(l_i \otimes r_j) = \delta_{ij}$.

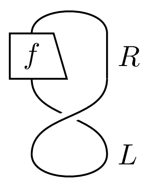
(b) Show that $\varepsilon(l_i \otimes r_j) = \langle l_j | l_i \rangle$. Conclude that $\{l_i\}$ is also an orthonormal basis, and hence that every dagger duality $L \dashv R$ in $\mathbf{FHilb}$ has the standard form (3.42) for *orthonormal* bases $\{l_i\}$ of L and $\{r_i\}$ of R.

Exercise 3.5.6. In $\mathbf{Rel}$, show that any duality $L \dashv R$ is of the following *standard form* for an isomorphism $R \xrightarrow{f} L$:

$$\eta = \{(\bullet, (r, f(r))) \mid r \in R\}, \qquad \varepsilon = \{((l, f^{-1}(l)), \bullet) \mid l \in L\}.$$

Conclude that specifying a duality $L \dashv R$ in $\mathbf{Rel}$ is the same as choosing an isomorphism $R \to L$, and that dual objects in $\mathbf{Rel}$ are automatically dagger dual objects.

Exercise 3.5.7. In a braided monoidal category with $L \dashv R$, we can define a *braided trace* for any morphism $L \xrightarrow{f} L$ in the following way:

$\mathrm{Tr}^\beta(f) =$  (3.43)

Show that this has the following properties:

(a) The scalar $\mathrm{Tr}^\beta(f)$ is independent of the chosen duality $L \dashv R$.

(b) For $L \xrightarrow{f} L$ and $L \xrightarrow{g} L$ we have $\mathrm{Tr}^\beta(g \circ f) = \mathrm{Tr}^\beta(f \circ g)$.

(c) For scalars $I \xrightarrow{s} I$ we have $\mathrm{Tr}^\beta(s) = s$.

(d) If the category is symmetric, $L \dashv R$, $L' \dashv R'$, $L \xrightarrow{f} L$, and $L' \xrightarrow{g} L'$, then $\mathrm{Tr}^\beta(f \otimes g) = \mathrm{Tr}^\beta(f) \circ \mathrm{Tr}^\beta(g)$.

(e) If the category is compact, $\mathrm{Tr}^\beta(f) = \mathrm{Tr}(f)$.

Exercise 3.5.8. Find some ribbons, or make some by cutting long, thin strips from a piece of paper. Use them to verify equations (3.30), (3.31) and (3.32).

Exercise 3.5.9. In a monoidal category, show that:

(a) if an initial object 0 exists and $L \dashv R$, then $L \otimes 0 \simeq 0 \simeq 0 \otimes R$;

(b) if a terminal object 1 exists and $L \dashv R$, then $R \otimes 1 \simeq 1 \simeq 1 \otimes L$.

Exercise 3.5.10. In a monoidal category, suppose that all idempotents split. Show:

(a) If there are morphisms $I \xrightarrow{\eta} R \otimes L$ and $L \otimes R \xrightarrow{\varepsilon} I$ satisfying the first snake equation (3.4), then L has a right dual.

(b) If $L \dashv R$, and $L \xrightarrow{f} M \xrightarrow{g} L$ satisfy $f \circ g = \mathrm{id}_M$, then M has a right dual.

Exercise 3.5.11. In $\mathbf{Rel}$, show that the trace of an endomorphism can be used to identify whether a relation has a fixed point.

Exercise 3.5.12. Working in a dagger compact category, solve the following problems.

(a) Show that $\mathrm{Tr}(f)$ is positive when $A \xrightarrow{f} A$ is a positive morphism.

(b) Show that f^* is positive when $A \xrightarrow{f} A$ is a positive morphism.

(c) Show that $\mathrm{Tr}_{A^*}(f^*) = \mathrm{Tr}_A(f)$ for any morphism $A \xrightarrow{f} A$.

(d) Show that $\mathrm{Tr}_{A\otimes B}(\sigma_{B,A} \circ (f \otimes g)) = \mathrm{Tr}_A(g \circ f)$ for morphisms $A \xrightarrow{f} B$ and $B \xrightarrow{g} A$.

(e) Show that $\mathrm{Tr}(g \circ f)$ is positive when $A \xrightarrow{f,g} A$ are positive morphisms.

Exercise 3.5.13. In a braided monoidal category, with morphisms $A \xrightarrow{f} A$ and $B \xrightarrow{g} B$, assume that A and B have duals and that the scalars $\dim(A)$ and $\dim(B)$ are invertible. Show that $f \otimes g$ is an isomorphism if and only if both f and g are isomorphisms. What assumption do you need for this to hold in an arbitrary monoidal category?

Exercise 3.5.14. In a monoidal dagger category, show that if $L \dashv R$ are dagger dual objects, then $\dim(L)^\dagger = \dim(R)$.

Exercise 3.5.15. In the category $\mathbf{Hilb}$, define

$$H \odot K = \begin{cases} H & \text{if } \dim(K) = 0, \\ K & \text{if } \dim(H) = 0, \\ 0 & \text{otherwise.} \end{cases} \qquad f \odot g = \begin{cases} f & \text{if } \dim(K) = 0 = \dim(K'), \\ g & \text{if } \dim(H) = 0 = \dim(H'), \\ 0 & \text{otherwise.} \end{cases}$$

for $H \xrightarrow{f} H'$ and $K \xrightarrow{g} K'$. Show that $(\mathbf{Hilb}, \odot, 0)$ is a monoidal category, in which any object is its own dual. Conclude that Corollary 3.65 ("infinite-dimensional spaces cannot have duals") crucially depends on the monoidal structure.

Exercise 3.5.16. Consider vector spaces as objects, and the following *linear relations* as morphisms $V \to W$: vector subspaces $R \subseteq V \oplus W$.

(a) Show that this is a well-defined subcategory of $\mathbf{Rel}$.

(b) Show that this is a compact dagger category under direct sum of vector spaces.

(c) Show that the scalars are the Boolean semiring.

Exercise 3.5.17. Let $\mathbf{C}$ be any dagger compact category, and let $\mathbf{D}$ be a dagger category whose every morphism is an isometry.

(a) Consider the category $[\mathbf{D}, \mathbf{C}]$, whose objects are functors $F\colon \mathbf{D} \to \mathbf{C}$ that satisfy $F(f^\dagger) = F(f)^\dagger$ for any morphism f, and whose morphisms are natural transformations. Show that $[\mathbf{D}, \mathbf{C}]$ is a dagger compact category.

(b) Show that $\mathbf{D}$ is a groupoid, where $f^{-1} = f^{\dagger}$.

Exercise 3.5.18. Complete the proof of Lemma 3.16, which states that the square of the double duals functor is a monoidal functor.

Exercise 3.5.19. Show that the balanced structure on $\mathbf{Fib}$, given in Example 3.32, satisfies the twist equation.

Notes and further reading

Compact categories were first introduced by Kelly in 1972 as a class of examples in the context of the coherence problem [92]. They were subsequently studied first from the perspective of categorical algebra [53, 94], and later in relation to linear logic [130, 19]. Categories with duals and their graphical calculi were surveyed exhaustively by Selinger [133].

The terminology 'compact category' is historically explained as follows. If G is a Lie group, then its finite-dimensional representations form a compact category. The group G can be reconstructed from the category when it is compact [84]. Thus the name 'compact' transferred from the group to categories resembling those of finite-dimensional representations. Compact categories and their closely related nonsymmetric variants are known under an abundance of different names in the literature not mentioned here: rigid, autonomous, sovereign, spherical, and category with conjugates [133]. Compact categories are also sometimes called compact closed categories, see Exercise 4.4.4. Dual objects form an important ingredient in so-called modular tensor categories [16], which form the mathematical foundation for topological quantum computing using anyons [113]. There are also intimate links to knot theory [144, 89, 63].

Abstract traces in monoidal categories were introduced by Joyal, Street and Verity in 1996 [86]. Definition 3.59 is one instance: any compact category is a so-called traced monoidal category. In fact, Hasegawa proved in 2008 that abstract traces in a compact category are unique [70]. Conversely, any traced monoidal category gives rise to a compact category via the so-called Int–construction. This gives rise to many more examples of compact categories not treated in this book. Theorem 3.15 is due to Saavedra Rivano [125]. The link between abstract traces and traces of matrices was made explicit by Abramsky and Coecke in 2005 [5]. The use of compact categories in foundations of quantum mechanics was initiated in 2004 by Abramsky and Coecke [4]. This was the article that initiated the study of categorical quantum mechanics. Independently, Kaufmann approached teleportation in a similar way in 2005 [90]. All of this builds on work on coherence for compact categories by Kelly and Laplaza [94].

Jamiołkowski [81] and Choi [34] independently discovered map-state duality in 1975 and 1972, respectively. The former used a basis-independent framework, whereas the latter used a basis-dependent one.

Chapter 4

Monoids and comonoids

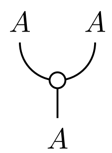
The tensor product of a monoidal category allows us to consider multiplications on its objects, leading to the notion of a monoid. In fact, this notion is so important, that one can almost say the entire reason for defining monoidal categories is that one can define monoids in them. We investigate such structures in Section 4.1, and their relation to dual objects. We also consider comonoids, whose operation is something like copying. Classical information can be copied and deleted, whereas quantum information cannot. This leads to big differences between classical and quantum information; we think of a classical system as a quantum one equipped with special morphisms that copy and delete the information it carries. We prove categorical no-deleting and no-cloning theorems in Section 4.2, showing that if these structures are able to copy and delete every state of the system, then the category collapses. Finally, we characterize when a tensor product is a categorical product in Section 4.3.

4.1 Monoids and comonoids

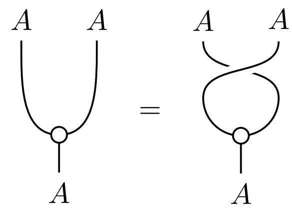
Let's start by making the notions of copying and deleting more precise in our setting of monoidal categories.

4.1.1 Comonoids

It makes sense to model copying as an operation of type $A \xrightarrow{d} A \otimes A$. As we will be using this morphism a lot, we will draw it as follows rather than with a generic box:



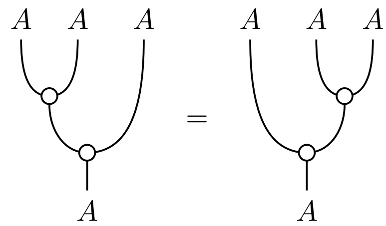
What does it mean that d copies information? First, it shouldn't matter if we switch both output copies, corresponding to the requirement that $d = \sigma_{A,A} \circ d$:



(4.1)

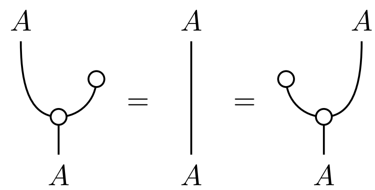
Note that it doesn't matter which braiding we choose here, because this equation is equivalent to the one in which we choose the other braiding.

Secondly, if we make a third copy, if shouldn't matter if we start from the first or the second copy. We can formulate this as $\alpha_{A,A,A} \circ (d \otimes \mathrm{id}_A) \circ d = (\mathrm{id}_A \otimes d) \circ d$:



(4.2)

Finally, remember that we think of I as the empty system. So deletion should be an operation of type $A \xrightarrow{e} I$. With this in hand, we can formulate what it means that both output copies should equal the input: that $\rho_A \circ (\mathrm{id}_A \otimes e) \circ d = \mathrm{id}_A$ and $\mathrm{id}_A = \lambda_A \circ (e \otimes \mathrm{id}_A) \circ d$. Graphically:



(4.3)

These three properties together constitute the structure of a *cocommutative comonoid* on A.

Definition 4.1 (Comonoid)**.** In a monoidal category, a *comonoid* is a triple $(A, ⋎, ⫯)$ of an object A and morphisms $⋎\colon A \to A \otimes A$ and $⫯\colon A \to I$ satisfying equations (4.2) and (4.3). If the monoidal category is braided and equation (4.1) holds, the comonoid is called *cocommutative*.

The morphism $⋎$ is called the *comultiplication*, and $⫯$ is called the *counit*. Properties (4.2) and (4.3) are *coassociativity* and *counitality*.

Example 4.2. Here are some comonoids in our example monoidal categories.

- In **Set**, the tensor product is in fact a Cartesian product. It therefore follows from counitality (4.3) that any object A carries a unique cocommutative comonoid structure with comultiplication $A \xrightarrow{d} A \times A$ given by $d(a) = (a, a)$, and the unique function $A \to I$ as counit.

- In $\mathbf{Rel}$, any group G forms a comonoid with comultiplication $g \sim (h, h^{-1}g)$ for all $g, h \in G$, and counit $1 \sim \bullet$. To see counitality, for example, notice that the left-hand side of (4.3) is the relation $g \sim h$ where $h^{-1}g = 1$, and the right-hand side is $g \sim 1^{-1}g$; that is, both equal the identity $g \sim g$.

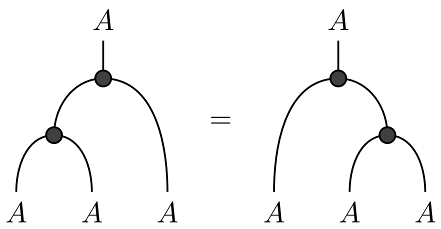
  The comonoid is cocommutative when the group is abelian. The left-hand side of (4.1) is $g \sim (h, h^{-1}g)$ for all $h \in G$, whereas the right-hand side is $g \sim (k, k^{-1}g)$ for all $k \in G$. But if $k = h^{-1}g$, then $k^{-1}g = g^{-1}hg = h$ when G is abelian, so that left and right-hand sides are equal.

- In **FHilb**, any choice of basis $\{e_i\}$ for a Hilbert space H provides it with cocommutative comonoid structure, with comultiplication $A \xrightarrow{d} A \otimes A$ defined by $e_i \mapsto e_i \otimes e_i$ and counit $A \xrightarrow{e} I$ defined by $e_i \mapsto 1$.

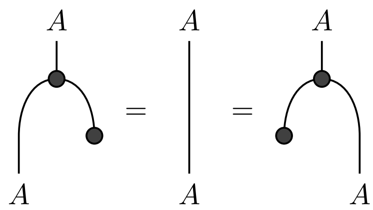
4.1.2 Monoids

Dualizing everything gives the better-known notion of a *monoid*.

Definition 4.3 (Monoid)**.** In a monoidal category, a *monoid* is a triple $(A, \ , \ )$ of an object A, a morphism : $A \otimes A \to A$, and a state : $I \to A$, satisfying the following two equations called *associativity* and *unitality*:

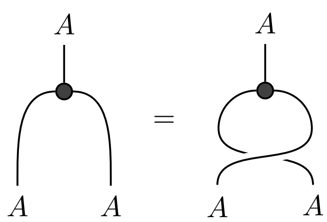


(4.4)



(4.5)

In a braided monoidal category, a monoid is *commutative* when the following equation holds:



(4.6)

As above, the choice of braid is arbitrary here; this condition is equivalent to the one using the other choice of braiding.

Example 4.4. There are many examples of monoids:

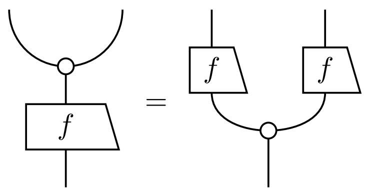
- In any monoidal category, the tensor unit I can be equipped with the structure of a monoid, with $m = \rho_I$ $(= \lambda_I)$ and $u = \mathrm{id}_I$.
- In $\mathbf{Set}$, a monoid is simply the ordinary mathematical notion of a monoid. Any group is an example.
- In $\mathbf{Vect}$, a monoid is what is usually called a (unital) *algebra*. The multiplication is a linear function $A \otimes A \xrightarrow{m} A$, corresponding to a bilinear function $A \times A \to A$. Hence an algebra is a set where we can not only add vectors and multiply vectors with scalars, but also multiply vectors with each other in a bilinear way. For example, $\mathbb{C}^n$ forms an algebra under coordinatewise multiplication, where the unit is the vector $(1, 1, \ldots, 1)$. For another example, the vector space of complex n-by-n matrices $\mathbb{M}_n$ forms an algebra under matrix multiplication.

We have used a black dot for the comonoid structures and a white dot for the monoid structures, but that is not essential; we will just make sure to use different colours to differentiate structures as the need arises. Later on we will use monoids and comonoids for which the multiplication is the adjoint of the comultiplication, and the unit is the adjoint of the counit, and in that case we will use the same colour dots for all of these structures.

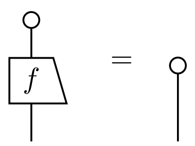
4.1.3 Combining monoids

The comonoids in a monoidal category form a category of their own, with the following morphisms.

Definition 4.5. In a monoidal category, a *comonoid homomorphism* from a comonoid (A, d, e) to a comonoid (A', d', e') is a morphism $A \xrightarrow{f} A'$ such that $(f \otimes f) \circ d = d' \circ f$ and $e' \circ f = e$:



(4.7)



(4.8)

The visual impression is that the morphism f is copied by d', and deleted by e'. Comonoid homomorphisms compose associatively, and the identity morphism is always a comonoid homomorphism, so comonoids and comonoid homomorphisms form a category.

Example 4.6. Consider again the comonoids of Example 4.2.

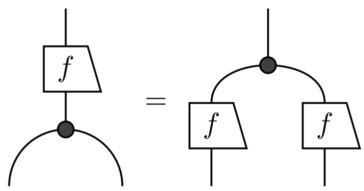
- In $\mathbf{Set}$, any function $f \colon A \to B$ is a comonoid homomorphism: by definition $(f \times f)(a, a) = \big(f(a), f(a)\big)$, and $A \xrightarrow{f} B \to I$ equals the unique function $A \to I$.

- In **Rel**, any surjective homomorphism $f\colon G \to H$ of groups is a comonoid homomorphism. The left-hand side of (4.7) is the relation $g \sim (h, h^{-1}f(g))$ for $h \in H$, and the right-hand side is $g \sim (f(g'), f(g')^{-1}f(g))$. Since f is surjective, any $h \in H$ is of the form $f(g')$ for some $g' \in G$, making both sides equal. Similarly, both sides of (4.8) come down to the relation $1 \sim f(1) = 1$.

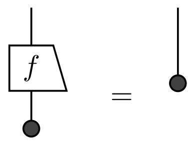
- In **FHilb**, any function $f\colon \{d_i\} \to \{e_j\}$ between bases extends linearly to a comonoid homomorphism between the Hilbert spaces they span. Almost by definition $d'(f(d_i)) = f(d_i) \otimes f(d_i)$ and $e'(f(d_j)) = 1 = e(d_j)$.

Morphisms of monoids are dual to morphisms of comonoids.

Definition 4.7 (Monoid homomorphism)**.** In a monoidal category, a *monoid homomorphism* from a monoid (A, m, u) to a monoid (A', m', u') is a morphism $A \xrightarrow{f} A'$ such that $f \circ m = m' \circ (f \otimes f)$ and $u' = f \circ u$:



(4.9)



(4.10)

Again, there is a category whose objects are monoids and whose morphisms are monoid homomorphisms.

In a braided monoidal category we can combine two comonoids to give a single comonoid on the tensor product object.

Lemma 4.8 (Product comonoid)**.** *In a braided monoidal category, given a pair of comonoids, we can produce a new comonoid with the following comultiplication and counit:*

(4.11)

Proof. The two comonoid structures are just sitting on top of each other, and the coassociativity and counitality properties of the original comonoids are inherited by the new composite structure. □

In the case that the braiding is a symmetry, this gives the actual categorical product of comonoids in the category of cocommutative comonoids and comonoid homomorphisms.

The product of two monoids is formed in a similar way.

Example 4.9. Products of the comonoids of Example 4.2 are as follows.

- In $\mathbf{Set}$, the product of the unique comonoids on sets A and B is, of course, the unique comonoid on $A \times B$.
- In $\mathbf{Rel}$, the product of groups G and H in is the comonoid of the product group $G \times H$ with multiplication $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$.
- In $\mathbf{FHilb}$, the product of comonoids on Hilbert spaces H and K that copy orthonormal bases $\{d_i\}$ and $\{e_j\}$ is the comonoid that copies the orthonormal basis $\{d_i \otimes e_j\}$ of $H \otimes K$.

In a monoidal dagger category, there is a duality between monoids and comonoids.

Lemma 4.10. *In a monoidal dagger category, if (A, d, e) is a comonoid, then $(A, d^\dagger, e^\dagger)$ is a monoid.*

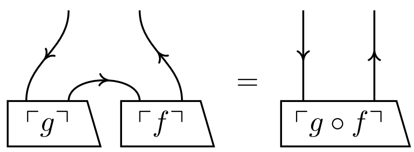
Proof. Equations (4.4) and (4.5) are just (4.2) and (4.3) vertically reflected. □

The previous lemma shows that Examples 4.2 and 4.4 are related by taking daggers in $\mathbf{Rel}$. Taking daggers in $\mathbf{Rel}$ constructs converse relations, and applying this to Example 4.2 turns the comultiplication $G \xrightarrow{d} G \times G$ given by $g \sim (h, h^{-1}g)$ for a group G into the multiplication $G \times G \xrightarrow{m} G$ given by $(g, h) \sim gh$.

4.1.4 Monoids of operators

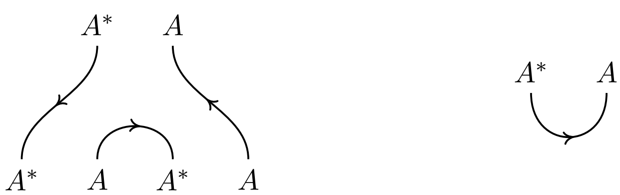
One of the most important features of matrices is that they can be multiplied. In other words, linear maps $\mathbb{C}^n \to \mathbb{C}^n$ can be composed. Using the dual objects of the previous chapter we can *internalize* this, to see that the vector space $\mathbb{M}_n$ of Example 4.4 is actually a monoid that lives in the same category as $\mathbb{C}^n$.

More generally, if an object A in a monoidal category has a right dual A^*, then operators $A \xrightarrow{f} A$ correspond bijectively to states $I \xrightarrow{\ulcorner f \urcorner} A^* \otimes A$. Composition $A \xrightarrow{g \circ f} A$ of operators transfers to states $I \xrightarrow{\ulcorner g \circ f \urcorner} A^* \otimes A$:



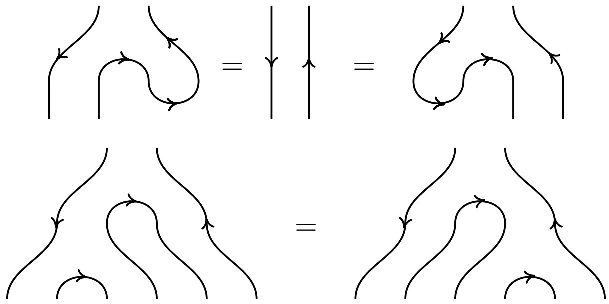
Thus the object $A^* \otimes A$ canonically becomes a monoid. We will call it the *pair of pants* monoid.

Lemma 4.11 (Pair of pants)**.** *If a monoidal category has a chosen duality $A \dashv A^*$, then $A^* \otimes A$ has a canonical monoid structure, with multiplication and unit:*



(4.12)

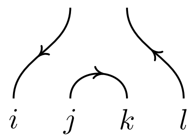
Proof. Straightforward graphical manipulation:



Hence this definition satisfies unitality and associativity. □

Example 4.12. In **FHilb**, the pair of pants monoid on the object $\mathbb{C}^n$ is the algebra $\mathbb{M}_n$ of n-by-n matrices under matrix multiplication.

Proof. Fix an orthonormal basis $\{|i\rangle\}$ for $A = \mathbb{C}^n$, so that an orthonormal basis of $A^* \otimes A$ is given by $\{\langle j| \otimes |i\rangle\}$. Define a linear function $A^* \otimes A \to \mathbb{M}_n$ by mapping $\langle j| \otimes |i\rangle$ to the matrix e_{ij}, which has a single entry 1 on row i and column j and zeroes elsewhere. This is clearly a bijection. Furthermore, it respects multiplication; using the decorated notation from Section 1.1.4:

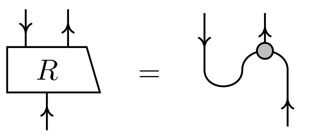


$$= \begin{bmatrix} \langle i| \otimes |l\rangle & \text{if } j = k, \\ 0 & \text{if } j \neq k \end{bmatrix} \longmapsto \begin{bmatrix} e_{il} & \text{if } j = k, \\ 0 & \text{if } j \neq k \end{bmatrix} = e_{ij}e_{kl}$$

Similarly, it respects units, and is therefore a monoid homomorphism. □

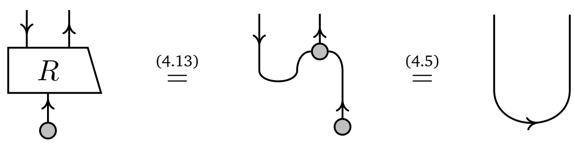
Pair of pants monoids are universal, in the sense that any monoid embeds into a pair of pants monoid.

Proposition 4.13 (Everybody wears pants)**.** *In a monoidal category, for a monoid* $(A, \ , \ )$ *and a duality* $A \dashv A^*$*, there is a monoid homomorphism* $R : (A, \ , \ ) \to (A^* \otimes A, \ , \ )$ *that has a retraction.*

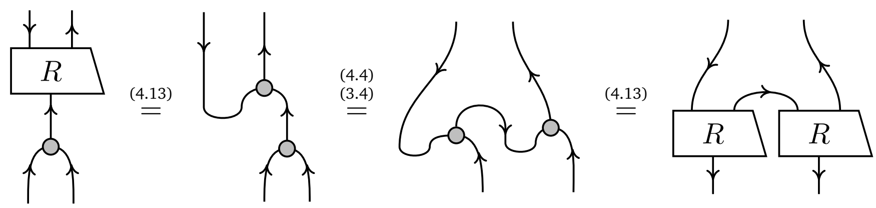


(4.13)

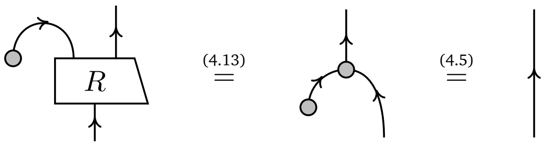
Proof. The morphism R preserves units:



It also preserves multiplication:



Finally, R has a left inverse:



This finishes the proof. $\square$

4.2 Uniform copying and deleting

We now set out to prove categorical no-cloning and no-deleting theorems. Such theorems say that it is physically impossible to build a machine that inputs an unknown quantum system and outputs two perfect copies of it, nor to build a machine that simply forgets the input and outputs nothing. Categorically, this statement takes the form: if the monoidal category has duals (so that it 'has entanglement'), and it has a morphism behaving as such a perfect copying machine, then the category must degenerate in some way.

4.2.1 Uniform deleting

The counit $A \xrightarrow{e} I$ of a comonoid A tells us we can 'forget' about A if we want to. In other words, we can delete the information contained in A. It is perfectly possible to delete individual systems like this. The no-deleting theorem only prohibits a systematic way of deleting arbitrary systems.

What happens when *every* object in our category can be deleted *systematically*? In our setting, deleting systematically means that the deleting operations respect the categorical structure. This means that deleting is *uniform*, in the sense that it doesn't matter if we delete something right away, or first process it for a while and then delete the result. In that case, we can say something quite dramatic. Let us first make uniform deleting precise.

Definition 4.14 (Uniform deleting)**.** A category has *uniform deleting* if there is a natural transformation $A \xrightarrow{e_A} I$ with $e_I = \mathrm{id}_I$.

Naturality of e_A here means that $e_B \circ f = e_A$ for any morphism $A \xrightarrow{f} B$. This is already strong enough to imply that any monoidal category whose tensor unit I is terminal, such as $\mathbf{Set}$, has uniform deleting.

Proposition 4.15. *A category* $\mathbf{C}$ *has uniform deleting if and only if* I *is terminal.*

Proof. Uniform deleting gives a morphism $A \xrightarrow{e_A} I$ for each object A. Naturality and $e_I = \mathrm{id}_I$ then imply that any morphism $A \xrightarrow{f} I$ must equal e_A:

$$\begin{tikzcd} A \arrow[r, "e_A"] \arrow[d, "f"'] & I \arrow[d, "\mathrm{id}_I"] \\ I \arrow[r, "e_I = \mathrm{id}_I"'] & I \end{tikzcd}$$

Conversely, if I is terminal, we can define $A \xrightarrow{e_A} I$ as the unique morphism of that type. This will automatically satisfy naturality as well as $e_I = \mathrm{id}_I$. $\square$

We can now show that biproducts are not as independent a development as they may have seemed so far: a superposition rule automatically makes coproducts into biproducts, and, dually, products into biproducts.

Proposition 4.16. *If a category has a superposition rule and an initial object, then any finite coproduct is a biproduct, and in particular the initial object is a zero object.*

Proof. Write 0 for the initial object. The units $A \xrightarrow{u_{A,0}} 0$ of the superposition rule (2.8) are natural for any $A \xrightarrow{f} B$:

$$u_{B,0} \circ f \overset{(2.11)}{=} u_{B,0} \circ u_{B,B} \circ f \overset{(2.11)}{=} u_{B,0} \circ u_{A,B} \overset{(2.11)}{=} u_{A,0} \overset{(2.11)}{=} u_{0,0} \circ u_{A,0}$$

Furthermore, $u_{0,0}$ is the unique morphism $0 \to 0$ because 0 is initial. Therefore 0 is also a terminal object, and hence a zero object, by Proposition 4.15.

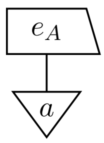
Define $p_A = \begin{pmatrix} \mathrm{id}_A & 0_{B,A} \end{pmatrix} : A+B \to A$ and $p_B = \begin{pmatrix} 0_{A,B} & \mathrm{id}_B \end{pmatrix}$. We will show that this makes $A+B$ into a biproduct. Equations (2.12) and (2.13) are satisfied by construction, and we have to show (2.14). That is, we have to show that $m = i_A \circ p_A + i_B \circ p_B = \mathrm{id}_{A+B}$. By the universal property of the coproduct of Definition 0.22 it suffices to show that $m \circ i_A = i_A$ and $m \circ i_B = i_B$. We establish the first as follows:

$$m \circ i_A \overset{(2.9)}{=} i_A \circ p_A \circ i_A + i_B \circ p_B \circ i_B \overset{\substack{(2.12)\\(2.13)}}{=} i_A + i_B \circ 0_{A,B} \overset{\substack{(2.8)\\(2.11)}}{=} i_A$$

The second can be demonstrated in a similar way, completing the proof. □

To further justify the name "uniform deleting" of Definition 4.14, we now observe that it indeed "deletes" states.

Definition 4.17 (Deleting)**.** In a monoidal category, a morphism $A \xrightarrow{e_A} I$ *deletes* a state $I \xrightarrow{a} A$ when:



$$= \tag{4.14}$$

Corollary 4.18. *Consider a monoidal category with maps $A \xrightarrow{e_A} I$ for each object A. If the maps e_A provide uniform deleting, they delete any state. The converse holds when the category is well-pointed.*

Proof. If there is uniform deleting, then $e_A \circ u = \mathrm{id}_I$ for each state $I \xrightarrow{a} A$ by Proposition 4.15.

Now suppose that the category is well-pointed, and let $A \xrightarrow{f} I$ and $A \xrightarrow{g} I$ be morphisms. By Proposition 4.15 it suffices to show that $f \circ a = g \circ a$ for any state $I \xrightarrow{a} A$. Both are states of I, so $e_I \circ f \circ a = \mathrm{id}_I = e_I \circ g \circ a$. That is, both scalars $f \circ a$ and $g \circ a$ are inverse to the scalar e_I, and hence must be equal: $f \circ a = g \circ a \circ e_I \circ f \circ a = g \circ a$. □

The no-deleting theorem below will show that uniform deleting has significant effects in a compact category. Namely, the category must collapse, in the following sense.

Definition 4.19 (Preorder)**.** A *preorder* is a category that has at most one morphism $A \to B$ for any pair of objects A, B.

Preorders are clearly quite uninteresting from a dynamical perspective, as there is at most one way to transition between any two systems.

Theorem 4.20 (No deleting). *If a compact category has uniform deleting, then it is a preorder.*

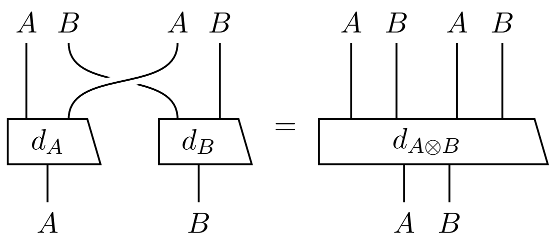
Proof. By Proposition 4.15, the tensor unit I is terminal. So any two parallel morphisms $A \xrightarrow{f,g} B$ must have the same coname $\llcorner f \lrcorner = \llcorner g \lrcorner$, whence $f = g$. $\square$

4.2.2 Uniform copying

We now move to uniform copying. The comultiplication $A \xrightarrow{d} A \otimes A$ of a comonoid lets us copy the information contained in one object A. What happens if we have this ability for all objects, systematically? In this section we will prove a categorical no-cloning theorem, showing that compact categories with uniform copying must degenerate.

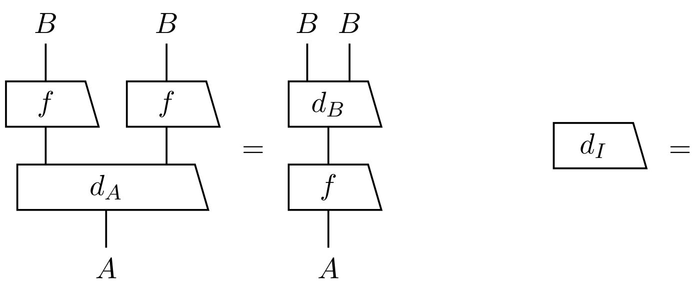
Uniform deleting meant deleting something straight away is the same as processing it for a while first and then deleting the result. We want a similar definition to say that a copying procedure is uniform. It shouldn't matter whether we copy something first and then process both copies, or process the original first and then copy the result. This amounts to naturality of the comultiplication: it must respect composition. Moreover, we want these copying maps to respect the tensor product: copying a compound object should be the same as copying both constituents. The following definition makes this precise, using Lemma 4.8 for compound objects.

Definition 4.21 (Uniform copying). A braided monoidal category has *uniform copying* if there is a natural transformation $A \xrightarrow{d_A} A \otimes A$ with $d_I = \rho_I^{-1}$, satisfying equations (4.1) and (4.2), and making the following diagram commute for all objects A, B.



(4.15)

Naturality and $d_I = \rho_I^{-1}$ graphically look like this for arbitrary $A \xrightarrow{f} B$:



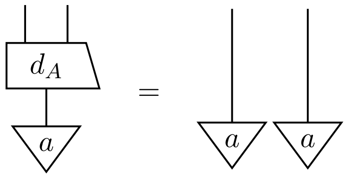
(4.16)

Example 4.22. The monoidal category **Set** has uniform copying. The copying maps $A \xrightarrow{d_A} A \times A$ given by $a \mapsto (a, a)$ fit the bill: $d_1(\bullet) = (\bullet, \bullet) = \rho_1(\bullet)$, and both sides of (4.15) are the function $A \times B \to A \times B \times A \times B$ given by $(a, b) \mapsto (a, b, a, b)$.

We study more examples of uniform copying in Exercises 4.4.7, 4.4.9, and 4.4.10.

To justify calling the notion of Definition 4.21 copying, we now observe that it actually copies states.

Definition 4.23 (Copyable state). In a braided monoidal category, given an object A equipped with a morphism $A \xrightarrow{d} A \otimes A$, a state $I \xrightarrow{a} A$ is *copyable* when the following holds:

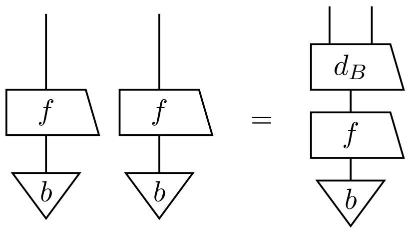


(4.17)

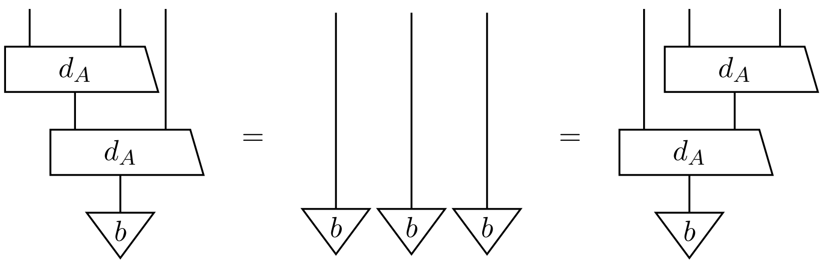
Proposition 4.24. *In a braided monoidal category, let $A \xrightarrow{d_A} A \otimes A$ be a family of morphisms. If this family exhibits uniform copying, any state is copyable. When the category is monoidally well-pointed, then the converse also holds.*

Proof. If there is uniform copying, then, by naturality of the copying maps, we have $d_A \circ a = (a \otimes a) \circ \rho_I^{-1}$ for each state $I \xrightarrow{a} A$.

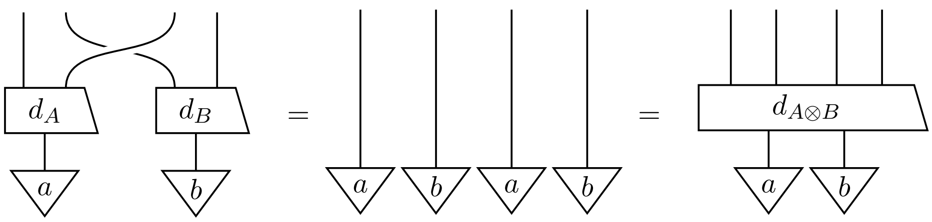
Now suppose the category is monoidally well-pointed and every state is copyable. In particular, the state $I \xrightarrow{\mathrm{id}_I} I$ is then copyable, which means $d_I = \rho_I^{-1}$. To see that d_A is natural, let $A \xrightarrow{f} B$ be any morphism. By monoidal well-pointedness, it suffices to show for any state $I \xrightarrow{b} A$ that



But that is just copyability of the state $I \xrightarrow{f \circ b} B$. Associativity (4.4) and commutativity (4.6) similarly follow from well-pointedness. For example:



because any state $I \xrightarrow{b} A$ is copyable. Finally, we have to verify equation (4.15). This is where we need monoidal well-pointedness, rather than mere well-pointedness:



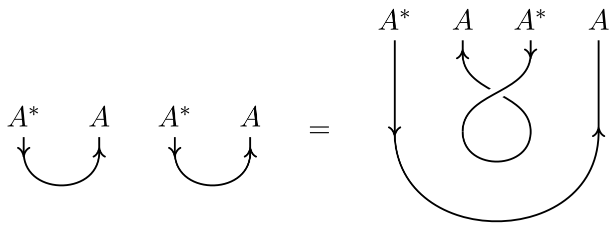
for all states $I \xrightarrow{a} A$ and $I \xrightarrow{b} B$. □

Hence our definition of uniform copying coincides with the naive one in monoidally well-pointed categories such as **Set**, **Rel**, and **Hilb**. Definition 4.21 makes sense for non-well-pointed categories, too.

4.2.3 No-cloning

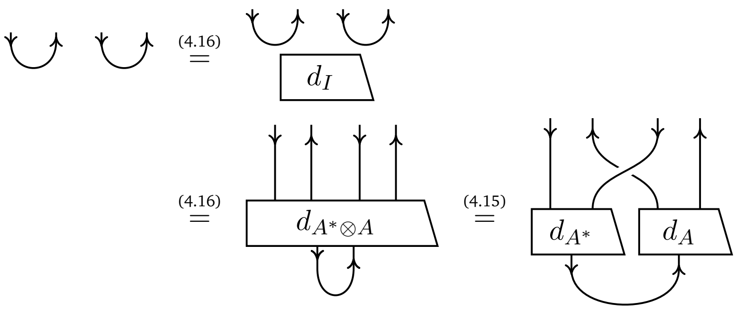
You might have expected Example 4.22: in classical physics, as modeled in **Set**, you *can* uniformly copy states. The no-cloning theorem says something about quantum physics, which we have modeled by compact categories, which **Set** is not. Uniform copying on a compact category turns out to be a drastic restriction. It means that the category degenerates: it must have trivial dynamics, in the sense that all endomorphisms are scalar multiples of the identity. To prove this categorical no-cloning theorem, we start with a preparatory lemma.

Lemma 4.25. *If a braided monoidal category with duals has uniform copying, then:*



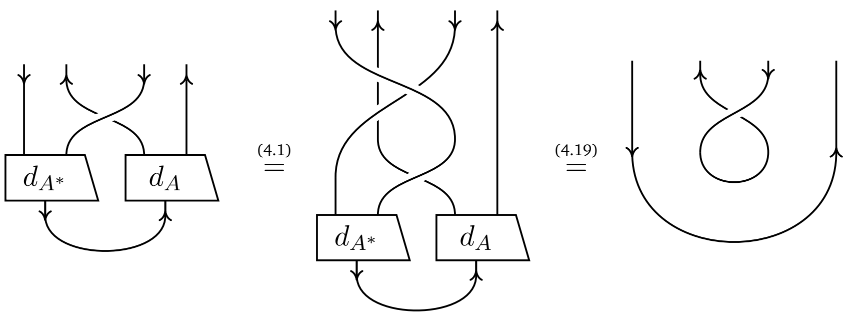
(4.18)

Proof. First, consider the following equalities:



(4.19)

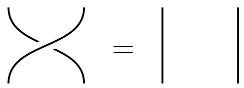
Then use this equality again as follows:



The first equality applies the cocommutativity equation above the morphism d_{A^*} followed by an isotopy. $\square$

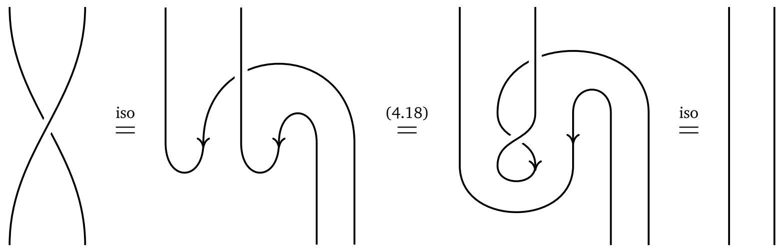
The previous lemma already shows the core of the degeneracy, as it equates two morphisms with different connectivity. We can now prove the no-cloning theorem.

Proposition 4.26. *In a braided monoidal category with duals and uniform copying, the braiding is the identity:*



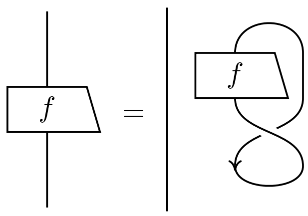
(4.20)

Proof. Graphically:



This completes the proof. □

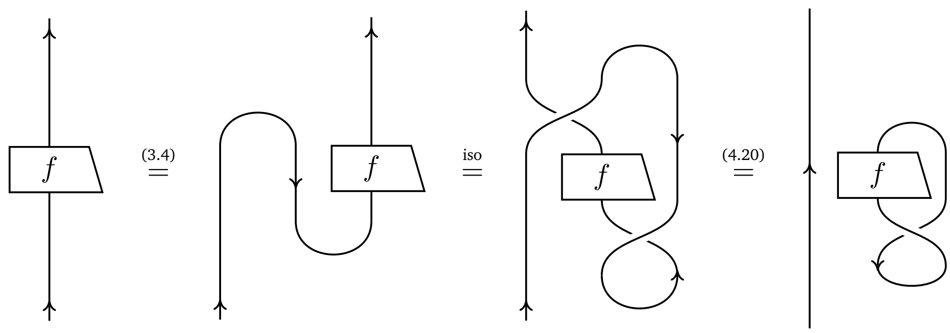
Theorem 4.27 (No cloning)**.** *If a braided monoidal category with duals has uniform copying, then every endomorphism is a scalar multiple of the identity:*



(4.21)

Notice that the scalar is the trace of f as defined for braided monoidal categories in Exercise 3.5.7.

Proof. Graphically:



This completes the proof. □

While highly degenerate, such categories are not necessarily trivial; Exercises 4.4.9 and 4.4.10 characterize them.

4.3 Products

Let's forget about duals for this section. If a category has products and a terminal object – that is, if it's Cartesian – then it has a symmetric monoidal structure (see Exercise 1.4.9). It turns out that such a symmetric monoidal structure has uniform copying and deleting. Moreover, adding an extra property exactly characterizes the monoidal structures that arise in this way.

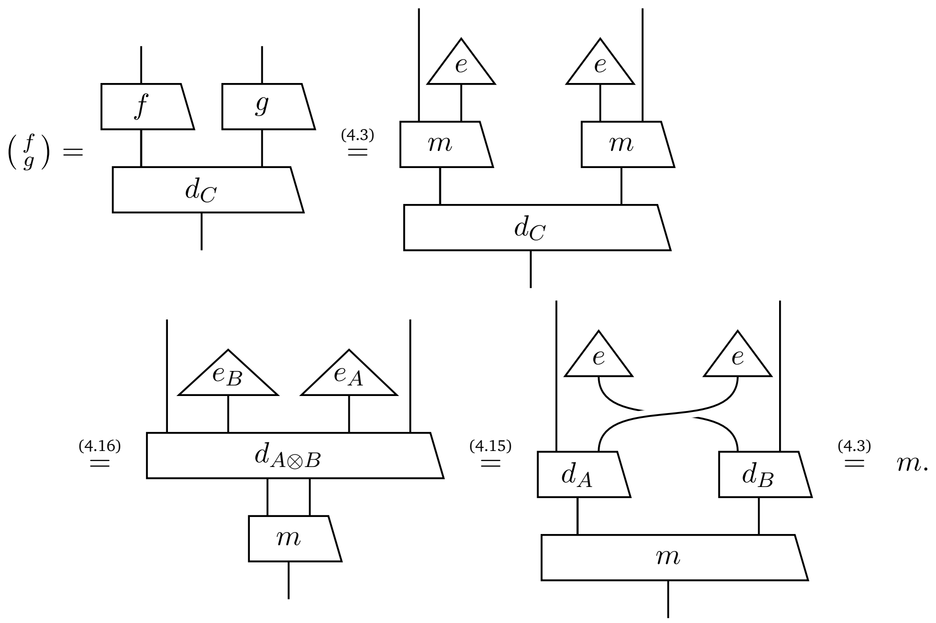
Theorem 4.28. *The following are equivalent for a symmetric monoidal category:*

(a) it is Cartesian, with tensor product given by the categorical product and the tensor unit given by the terminal object;

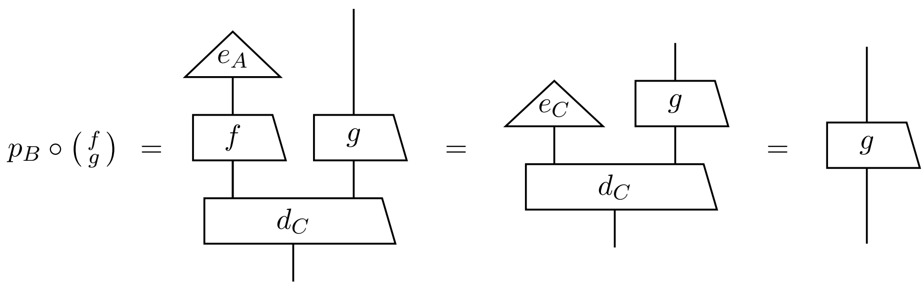
(b) it has uniform copying and deleting, and equation (4.3) *holds.*

Proof. For $(a) \Rightarrow (b)$, choose $d_A = \begin{pmatrix} \mathrm{id}_A \\ \mathrm{id}_A \end{pmatrix}$ for uniform copying, and the terminal morphism $A \xrightarrow{e_A} I$ for uniform deleting. It is easy to show that these satisfy (4.3).

For $(b) \Rightarrow (a)$, we need to prove that $A \otimes B$ is a product of A and B. Define $p_A = \rho_A \circ (\mathrm{id}_A \otimes e_B) \colon A \otimes B \to A$ and $p_B = \lambda_B \circ (e_A \otimes \mathrm{id}_B) \colon A \otimes B \to B$. For given $C \xrightarrow{f} A$ and $C \xrightarrow{g} B$, define $\begin{pmatrix} f \\ g \end{pmatrix} = (f \otimes g) \circ d$. First, suppose $C \xrightarrow{m} A \otimes B$ satisfies $p_A \circ m = f$ and $p_B \circ m = g$. Then:



The second equality is our assumption, the third equality is naturality of d, the fourth equality follows from the definition of uniform copying, and the last equality uses counitality. Hence mediating morphisms, if they exist, are unique: they all equal $\begin{pmatrix} f \\ g \end{pmatrix}$. Finally, we show that $\begin{pmatrix} f \\ g \end{pmatrix}$ indeed satisfies $p_B \circ \begin{pmatrix} f \\ g \end{pmatrix} = g$:



The first equality holds by definition, the second equality is naturality of e, and the last equality is equation (4.3). Similarly $p_A \circ \left(\begin{smallmatrix} f \\ g \end{smallmatrix}\right) = f$. □

4.4 Exercises

Exercise 4.4.1. In a monoidal category, show that a comonoid homomorphism $(I, \lambda_I^{-1}, \mathrm{id}_I) \xrightarrow{a} (A, d, e)$ gives a copyable state. Conversely, show that if a state $I \xrightarrow{a} A$ is copyable and satisfies $e \circ a = \mathrm{id}_I$, then it gives a comonoid homomorphism.

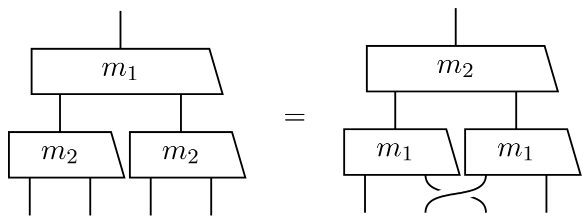
Exercise 4.4.2. This exercise is about *property* versus *structure*; the latter is something you have to choose, the former is something that exists uniquely (if at all).

(a) Show that in a monoidal category, if a monoid (A, m, u) has a map $I \xrightarrow{u'} A$ satisfying $m \circ (\mathrm{id}_A \otimes u') = \rho_A$ and $\lambda_A = m \circ (u' \otimes \mathrm{id}_A)$, then $u' = u$. Conclude that unitality is a property.

(b) Show that in categories with binary products and a terminal object, every object has a unique comonoid structure under the monoidal structure induced by the categorical product.

(c) For a symmetric monoidal category $(\mathbf{C}, \otimes, I)$, denote by $\mathbf{cMon}(\mathbf{C})$ the category of commutative monoids in $\mathbf{C}$ with monoid homomorphisms as morphisms. Show that the forgetful functor $\mathbf{cMon}(\mathbf{C}) \to \mathbf{C}$ is an isomorphism of categories if and only if $\otimes$ is a coproduct and I is an initial object.

Exercise 4.4.3. This exercise is about the *Eckmann-Hilton argument*, concerning interacting monoid structures in a braided monoidal category. Suppose you have morphisms $A \otimes A \xrightarrow{m_1, m_2} A$ and $I \xrightarrow{u_1, u_2} A$, such that (A, m_1, u_1) and (A, m_2, u_2) are both monoids, and the following diagram commutes:



(a) Show that $u_1 = u_2$.

(b) Show that $m_1 = m_2$.

(c) Show that m_1 is commutative.

Exercise 4.4.4. Let A and B be objects in a monoidal category. Their *exponential* is an object B^A together with a map $B^A \otimes A \xrightarrow{\mathrm{ev}} B$ such that every morphism $X \otimes A \xrightarrow{f} B$ allows a unique morphism $X \xrightarrow{g} B^A$ with $f = \mathrm{ev} \circ (g \otimes \mathrm{id}_A)$.

$$\begin{tikzcd}
X \otimes A \arrow[r, "f"] \arrow[dr, dashed, "g \otimes \mathrm{id}_A"'] & B \\
& B^A \otimes A \arrow[u, "\mathrm{ev}"']
\end{tikzcd}$$

The category is called *left closed* when every pair of objects has an exponential. Show that any monoidal category in which every object has a left dual is left closed.

Exercise 4.4.5. Let $(A, \cdot, 1)$ be a monoid in $(\mathbf{Set}, \times, 1)$ that is partially ordered in such a way that $ac \leq bc$ and $ca \leq cb$ when $a \leq b$. Consider it as a monoidal category, whose objects are $a \in A$, where there is a unique morphism $a \to b$ when $a \leq b$, and whose monoidal structure is given by $a \otimes b = ab$. Show that an object has a dual if and only if it is invertible in A. Conclude that every ordered abelian group induces a compact category. When is it a compact dagger category?

Exercise 4.4.6. In a monoidal category, a *semigroup* is an object A together with a morphism $A \otimes A \xrightarrow{m} A$ that satisfies the associative law (4.4). Recall from Exercise 1.4.10 that $\mathbf{Set}$ is a symmetric monoidal category under $I = \emptyset$ and $A \otimes B = A + B + (A \times B)$. Show that monoids in $(\mathbf{Set}, \otimes, I)$ correspond bijectively with semigroups in $(\mathbf{Set}, \times, 1)$.

Exercise 4.4.7. Let $(G, \cdot, 1)$ be a group.

(a) Show that the following defines a strict monoidal discrete category: objects are $g \in G$; morphisms are $g \xrightarrow{\mathrm{id}_g} g$ for $g \in G$; the tensor unit is $1 \in G$; the tensor product of objects is $g \otimes h = gh$; the tensor product of morphisms is $\mathrm{id}_g \otimes \mathrm{id}_h = \mathrm{id}_{gh}$.

(b) Show that every object g in this category has a dual g^{-1}, and that this category is symmetric precisely when the group G is abelian.

Exercise 4.4.8. A monoid is *idempotent* when all its elements are idempotent, *i.e.* satisfy $a^2 = a$. A *semilattice* is a partially ordered set L that has a greatest element 1, and greatest lower bounds; that is, for each $a, b \in L$, there exists $a \wedge b \in L$ such that $c \leq a$ and $c \leq b$ if and only if $c \leq a \wedge b$.

(a) If $(L, \leq, 1)$ is a semilattice, show that $(L, \wedge, 1)$ is a commutative idempotent monoid.

(b) Conversely, if $(M, \cdot, 1)$ is a commutative idempotent monoid, show that $(M, \leq, 1)$ is a semilattice, where $a \leq b$ if and only if $a = ab$.

Exercise 4.4.9. Let $(M, \cdot, 1)$ be a monoid, and $D \subseteq M$ a subset of idempotents.

(a) Show that the following defines a category $\mathbf{Split}_D(M)$: objects are $d \in D$; morphisms $d \to e$ are $a \in M$ such that $ea = a = ad$; composition is given by the monoid multiplication; identity on d is d itself.

(b) Show that if M is commutative and D is a submonoid, then $\mathbf{Split}_D(M)$ is a compact category that is in fact strict symmetric monoidal, where: the tensor unit I is $1 \in D$; the tensor product is monoid multiplication on both objects and morphisms; the symmetry $d \otimes e \to e \otimes d$ is the identity map de; dual objects are $d^* = d$, with cup $d \colon 1 \to d^* \otimes d$ and cap $d \colon d \otimes d^* \to 1$.

(c) Show that if M is idempotent and commutative, then $\mathbf{Split}_D(M)$ has uniform copying, with copying map $d \to d \otimes d$ on d the identity d.

(d) Conversely, show that if M is commutative and $\mathbf{Split}_D(M)$ has uniform copying, then M is idempotent.

(e) Conclude that any commutative monoid arises as the scalars of a monoidal category, and show that the dimension of d in $\mathbf{Split}_D(M)$ is d itself.

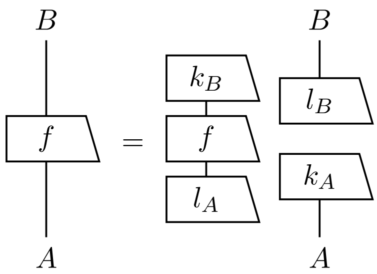
Exercise 4.4.10. Let $\mathbf{C}$ be a compact category with uniform copying. Write $M = \mathbf{C}(I, I)$ for the monoid of scalars.

(a) Show that M is idempotent, and that $D = \{\dim^\beta(A) \mid A \in \mathrm{Ob}(\mathbf{C})\}$ is a submonoid of M, where $\dim^\beta(A) = \mathrm{Tr}^\beta(\mathrm{id}_A)$ is the braided dimension of Exercise 3.5.7.

(b) For each object A, define morphisms:

Show that $k_A \circ l_A = \dim^\beta(A)$ and $l_A \circ k_A = \mathrm{id}_A$.

(c) Derive that Theorem 4.27 generalizes to morphisms that are not endomorphisms as:



(d) Define $F \colon \mathbf{C} \to \mathbf{Split}_D(M)$ by $F(A) = \dim^\beta(A)$ on objects, and $F(A \xrightarrow{f} B) = k_B \circ f \circ l_A$ on morphisms. Show that F is a symmetric monoidal equivalence.

Exercise 4.4.11. Let $F \colon \mathbf{C} \to \mathbf{D}$ be a monoidal functor between monoidal categories. If (M, m, u) is a monoid in $\mathbf{C}$, show that $\big(F(M), F(m) \circ (F_2)_{M,M}, F(u) \circ F_0\big)$ is a monoid in $\mathbf{D}$.

Notes and further reading

Cayley's theorem is due to Cayley in 1854 in what could be said to be the first article in group theory, although a gap was filled by Jordan in 1870 [112].

The no-cloning theorem was proved in 1982 independently by Wootters and Zurek, and Dieks [143, 54]. The categorical version we presented here is due to Abramsky in 2010 [3], in a simplified form due to Kirst. The no-deleting theorem we presented is due to Coecke and was also published in that paper. The extension of the no-cloning theorem to arbitrary morphisms in Exercise 4.4.10 is due to Tull in 2015. The category of Exercise 4.4.9 is well-known in category theory as the split idempotent completion, Karoubi envelope, or Cauchy completion [132, 75].

Theorem 4.28 was given by Zoran Petrić in 2000 [120]. Jacobs also gave a logically-oriented account in 1994 [80]. Terminal objects figure prominently in a categorical quantum mechanics approach to relativity [45]. In compact categories, products are automatically biproducts, which was proved by Houston in 2008 [79, 65].

The notion of closure of monoidal categories from Exercise 4.4.4 is the starting point for a large area called *enriched* category theory [93]. It also plays an important role in categorical logic, where it encodes implications between logical formulae.

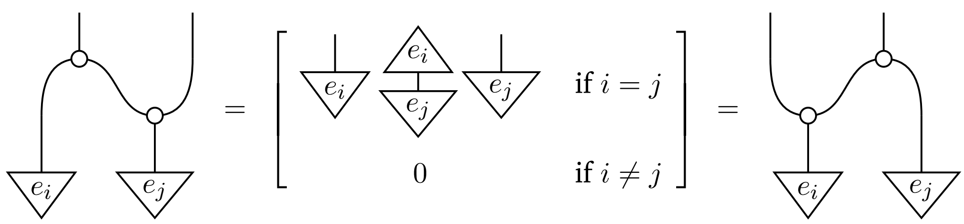
Chapter 5

Frobenius structures

In this chapter we deal with Frobenius structures: a monoid and a comonoid that interact according to the so-called Frobenius law. Section 5.1 studies its basic consequences. It turns out that the graphical calculus is very satisfying for Frobenius structures, and we prove in Section 5.2 that any diagram built up from the components of a Frobenius structure is equal to one in a simple normal form. The Frobenius law itself is justified as a coherence property between daggers and closure of a category in Section 5.3. We classify all Frobenius structures of a certain class in **FHilb** and **Rel** in Section 5.4, in terms of operator algebras and groupoids respectively. Of special interest is the commutative case, as in **FHilb** this corresponds to a choice of orthonormal basis. This gives us a way to copy and delete classical information without resorting to biproducts. Frobenius structures also allow us to discuss phase gates and the state transfer protocol in Section 5.5. Finally, we discuss modules for Frobenius structures to model measurement, controlled operations, and the pure quantum teleportation protocol in Section 5.6.

5.1 Frobenius structures

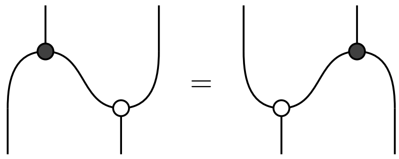
If $\{e_i\}$ is an orthogonal basis for a finite-dimensional Hilbert space H, then the copying map : $e_i \mapsto e_i \otimes e_i$ is the comultiplication of a comonoid; see Example 4.2. The adjoint is the comparison map given by $e_i \otimes e_i \mapsto \langle e_i | e_i \rangle e_i$ and $e_i \otimes e_j \mapsto 0$ for $i \neq j$. These copying and comparison maps cooperate in the following way:



This relationship between a multiplication and comultiplication is called the Frobenius law.

This property motivates the following general definition, which we justify further Section 5.3.

Definition 5.1 (Frobenius structure via diagrams)**.** In a monoidal category, a *Frobenius structure* is a pair of a comonoid $(A, \ , \ )$ and a monoid $(A, \ , \ )$ satisfying the following equation, called the *Frobenius law*:


(5.1)

The definition of Frobenius structure is sometimes taken to include the additional equality (5.4) below, but in Lemma 5.4 we show that this is redundant.

We already saw that any choice of orthogonal basis induces a Frobenius structure in **FHilb**, but there are many other examples.

Example 5.2 (Group algebra)**.** Any finite group G induces a Frobenius structure in **FHilb**. Let A be the Hilbert space of linear combinations of elements of G with its standard inner product. In other words, A has G as an orthonormal basis. Define : $A \otimes A \to A$ by linearly extending $g \otimes h \mapsto gh$, and define : $\mathbb{C} \to A$ by $s \mapsto s \cdot 1_G$. This monoid is called the *group algebra*. Its adjoint is given by

$$: A \to A \otimes A \qquad g \mapsto \sum_{h \in G} gh^{-1} \otimes h = \sum_{h \in G} h \otimes h^{-1} g$$

$$: A \to I \qquad g \mapsto \begin{bmatrix} 1 & \text{if } g = 1_G \\ 0 & \text{if } g \neq 1_G \end{bmatrix}$$

This gives a Frobenius structure, because both sides of the Frobenius law (5.1) compute to $\sum_{k \in G} gk^{-1} \otimes kh$ on input $g \otimes h$.

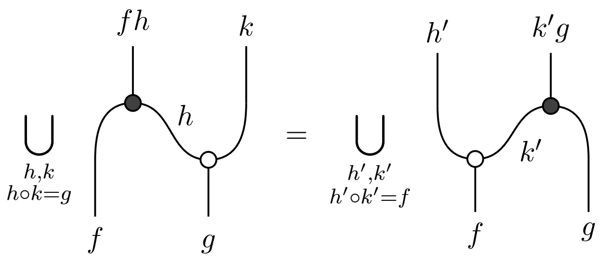
Example 5.3 (Groupoid Frobenius structure)**.** Any group G also induces a Frobenius structure in **Rel**:

$$\begin{aligned} &= \{((g,h), gh) \mid g, h \in G\} : G \times G \to G, \\ &= \{(\bullet, 1_G)\} : 1 \to G, \end{aligned} \tag{5.2}$$

where is the converse relation of , and that of . More generally, any groupoid **G** induces a Frobenius structure in **Rel** on the set G of all morphisms of **G**:

$$\begin{aligned} &= \{((g,f), g \circ f) \mid \mathrm{dom}(g) = \mathrm{cod}(f)\}, \\ &= \{(\bullet, \mathrm{id}_x) \mid x \in \mathrm{Ob}(\mathbf{G})\}. \end{aligned} \tag{5.3}$$

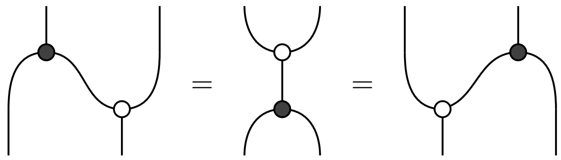
where again is the converse relation of , and that of . To see that this satisfies the Frobenius law (5.1), evaluate it on arbitrary input (f, g) in the decorated notation of Section 1.1.4:



On the left we obtain output $\cup_{h,k|h \circ k = g}(f \circ h, k)$, on the right $\cup_{h',k'|h' \circ k' = f}(h', k' \circ g)$. Making the change of variables $h' = f \circ h$ and $k' = k \circ g^{-1}$, the condition $h' \circ k' = f$ becomes $f \circ h \circ k \circ g^{-1} = f$, which is equivalent to $h \circ k = g$. So the two composites above are indeed equal, establishing the Frobenius law.

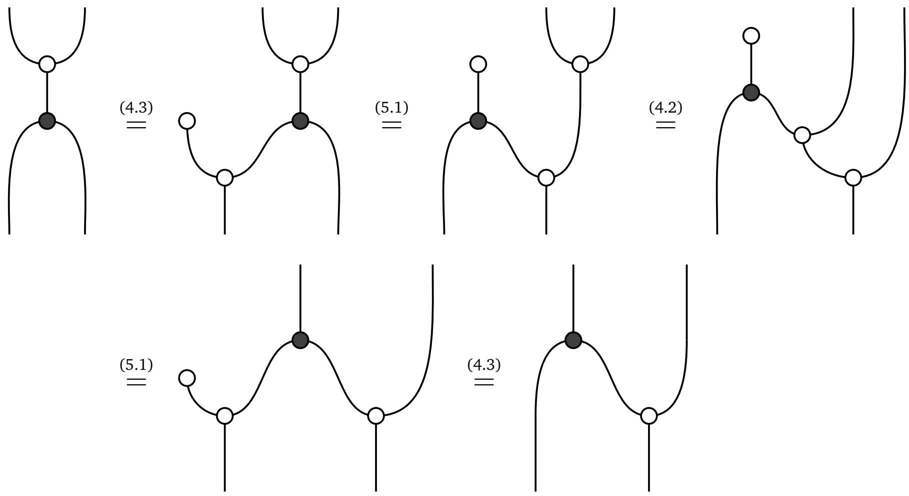
Frobenius structures automatically satisfy a further equality.

Lemma 5.4 (Extended Frobenius law). *In a monoidal category, a Frobenius structure satisfies the following equalities:*



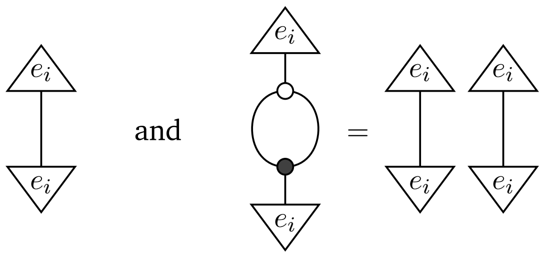
(5.4)

Proof. We prove one half graphically; the other then follows from the Frobenius law.

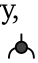


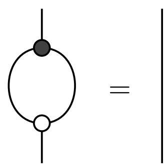
These equations use, respectively: counitality, the Frobenius law, coassociativity, the Frobenius law, and counitality. □

Consider again the Frobenius structure in **FHilb** induced by copying an orthogonal basis $\{e_i\}$. As we saw in Section 2.3, we can measure the squared norm of e_i and its square as:



Thus we can characterize when the orthogonal basis is orthonormal in terms of the Frobenius structure as follows.

Definition 5.5 (Special). In a monoidal category, a pair consisting of a monoid $(A,$ , $)$ and a comonoid $(A,$ , $)$ is *special* when  is a left inverse of :



(5.5)

Notice that speciality (5.5) and the Frobenius law (5.1), are the only two canonical ways in which a single multiplication and comultiplication can interact.

Example 5.6. The group algebra of Example 5.2 is only special for the trivial group. The groupoid Frobenius structure of Example 5.3 is always special.

5.1.1 Symmetry and commutativity

In all the examples of Frobenius structures we have seen so far, the multiplication is the dagger of the comultiplication, and the unit is the dagger of the counit. This compatibility condition has the following name.

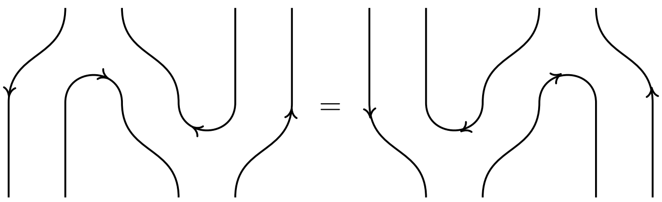
Definition 5.7 (Dagger Frobenius structure)**.** In a monoidal dagger category, a Frobenius structure $(A, \tinymult, \tinyunit, \tinycomult, \tinycounit)$ is a *dagger Frobenius structure* when $\tinymult = (\tinycomult)^\dagger$ and $\tinyunit = (\tinycounit)^\dagger$.

We call a Frobenius structure *commutative* when its monoid is commutative and its comonoid is cocommutative. For dagger Frobenius structures, this is equivalent to commutativity of the monoid.

Example 5.8. The Frobenius structure in **FHilb** induced by a choice of orthogonal basis is a dagger Frobenius structure. So are the Frobenius structures from Examples 5.2 and 5.3.

Lemma 5.9. *In a monoidal dagger category, given a dagger duality $A \dashv A^*$, the pair of pants monoid of Lemma 4.11 is a dagger Frobenius structure.*

Proof. The comultiplication and counit are chosen as the dagger of the multiplication and unit. The Frobenius law is readily verified:



This completes the proof. □

By Example 4.12, the algebra $\mathbb{M}_n$ of n-by-n complex matrices is therefore a dagger Frobenius structure in **FHilb**. We will also specifically be interested in commutative Frobenius structures. For example, the Frobenius structure induced by copying an orthonormal basis is commutative. As it allows us to copy and delete information, we think of this as *classical structure*. Rather than a negative statement about *quantum* objects like in Chapter 4 ("you *cannot* copy them uniformly"), think of this as a positive statement about *classical* objects ("you *can* copy their classical states").

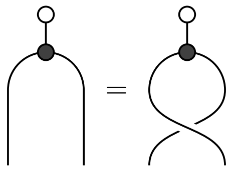
Definition 5.10 (Classical structure)**.** In a braided monoidal category, a *classical structure* is a dagger Frobenius structure that is special and commutative.

Example 5.11. The groupoid Frobenius structure of Example 5.3 is a classical structure when the groupoid is *abelian*, in the sense that all morphisms are endomorphisms and $f \circ g = g \circ f$ for all endomorphisms f, g of the same object. An abelian groupoid is essentially a list of abelian groups. Notice that abelian groupoids are skeletal.

There is some redundancy in the axioms of a classical structure, which we explore in Exercise 5.7.2.

A weakening of commutativity, called *symmetry*, is often studied.

Definition 5.12 (Symmetric Frobenius structure)**.** In a braided monoidal category, a Frobenius structure is *symmetric* when:



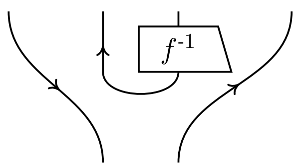
(5.6)

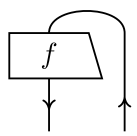
Clearly every commutative Frobenius structure is symmetric. The word "symmetric" is a bit unfortunate, as it could be confused with the terminology of symmetric monoidal categories, but it has now stuck.

Example 5.13. Some of our previous examples of Frobenius structures are symmetric.

- In a compact category, pair of pants structures are symmetric.
- The group algebra of Example 5.2 is always symmetric. The left-hand side of equation (5.6) sends $g \otimes h$ to 1 if $gh = 1$ and to 0 otherwise. The right-hand side sends $g \otimes h$ to 1 if $hg = 1$ and to 0 otherwise. So this comes down to the fact that inverses in groups are two-sided inverses.
- The groupoid Frobenius structure of Example 5.3 is always symmetric for a similar reason. The left-hand side of (5.6) contains $(g, h) \sim \bullet$ precisely when $g \circ h = \mathrm{id}_B$ for some object B. The right-hand side contains $(g, h) \sim \bullet$ when $h \circ g = \mathrm{id}_A$ for some object A. Both mean that $h = g^{-1}$.

Example 5.14. Here is a general way to construct nonsymmetric Frobenius structures. In a braided monoidal category, let $A \dashv A^*$ be dual objects, and let $A^* \xrightarrow{f} A^*$ be an isomorphism. Then build a Frobenius structure by taking the multiplication and unit to be the same as the pair of pants monoid of Lemma 4.11, and the comultiplication and counit to be as follows:





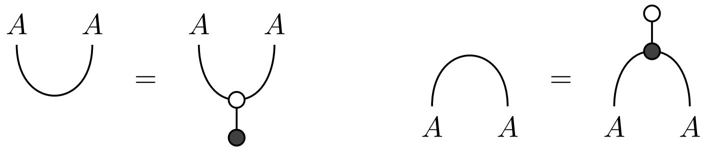
It is easy to see that this data is coassociative and counital, and that the Frobenius law holds. However, the symmetry condition (5.6) is not then satisfied in general, and it is easy to find choices of f that violate it in **Hilb** or **Rel**.

5.1.2 Self-duality and nondegenerate forms

Let's now consider some properties of general Frobenius structures. First of all, they are closely related to dual objects.

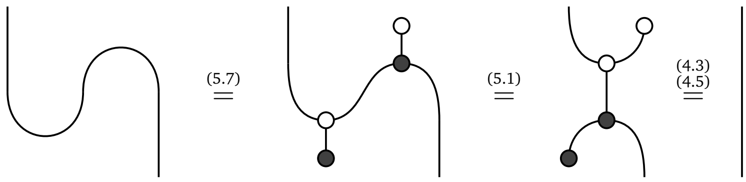
Theorem 5.15 (Frobenius structures have duals)**.** *In a monoidal category, if* $(A, \ , \ , \ , \ )$ *is a Frobenius structure, then* $A \dashv A$.

Proof. Choose the following unit and counit:



(5.7)

The first snake equation (3.4) follows from this choice of the cups and caps, the Frobenius law, and unitality and counitality:



(5.8)

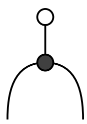
The other snake equation is proved similarly. □

It follows from the previous theorem that, if we chose a Frobenius structure on every object in a given monoidal category, then that category would have duals. By the collapse theorems of Chapter 4, it would be too much to ask for this Frobenius structure to support uniform copying. But we can use this obstruction contrapositively to motivate Definition 5.10 once more: classical structures are objects that *do* support copying and deleting, not uniformly but for some subset of their states.

The converse to the previous theorem can be used to characterize Frobenius structures.

Proposition 5.16 (Frobenius structures by nondegenerate form)**.** *In a monoidal category, for a monoid* $(A, \ , \ )$ *there is a bijective correspondence between:*

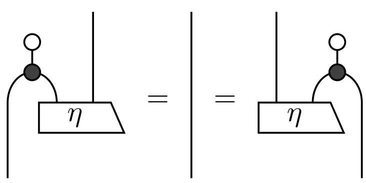
1. *comonoids* $(A, \ , \ )$ *making the pair into a Frobenius structure;*
2. *morphisms* $\colon A \to I$*, called* nondegenerate forms*, making the composite*



(5.9)

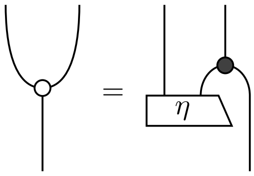
the cap of a self-duality $A \dashv A$*.*

Proof. The implication $1 \Rightarrow 2$ follows immediately from Theorem 5.15, by choosing the nondegenerate form to be the counit. For the other direction, suppose we have a monoid $(A, \ , \ )$ and a nondegenerate form $\colon A \to I$. That is, there exists a morphism $I \xrightarrow{\eta} A \otimes A$ satisfying the following equations:



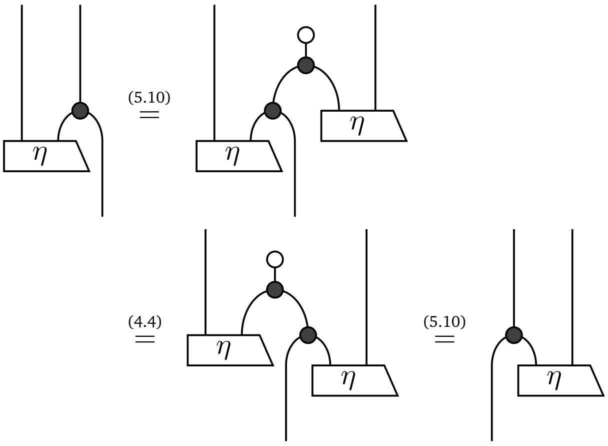
(5.10)

Use the map η to define a comultiplication in the following way:



(5.11)

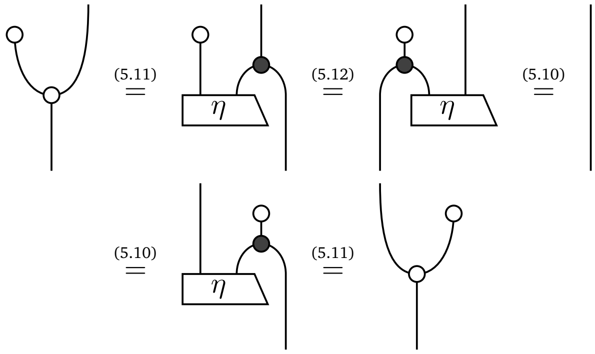
The following computation shows that we could have defined the comultiplication with the η on the left or the right, using the nondegeneracy property, associativity, and the nondegeneracy property again:



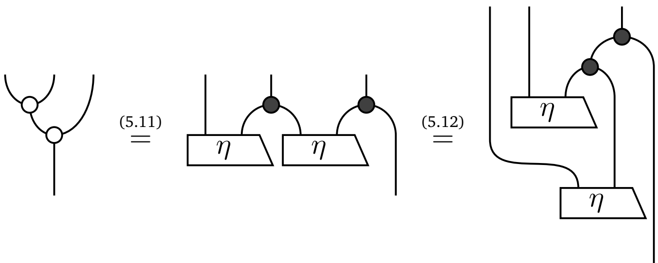
(5.12)

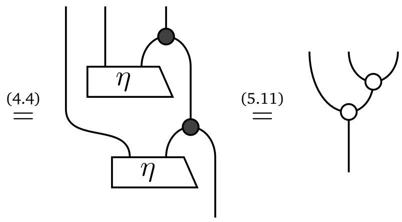
We must show that our new comultiplication satisfies coassociativity and counitality, and the Frobenius law (5.1). For the counit, choose the nondegenerate form.

Counitality is the easiest property to demonstrate, using the definition of the comultiplication, symmetry of the comultiplication, nondegeneracy twice, and definition of the comultiplication:

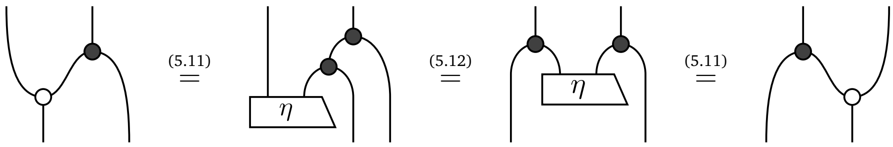


To see coassociativity, use the definition of the comultiplication, symmetry of the comultiplication, associativity, and the definition of the comultiplication:





Finally, the Frobenius law. Use the definition of the comultiplication, symmetry of the comultiplication, and the definition of the comultiplication again:



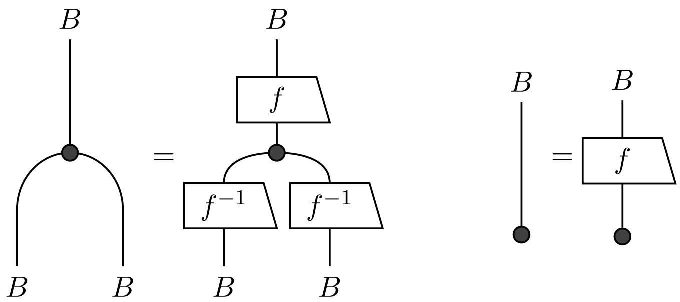
This completes the description of the correspondence.

Finally, this correspondence is bijective. Starting with a nondegenerate form, turning it into a comonoid, and then taking the counit, ends with the same nondegenerate form. Starting with a comonoid ends with the same counit but with comultiplication (5.11). However, Lemma 3.5 guarantees that η must be as in Theorem 5.15, and then the Frobenius law guarantees that this comultiplication in fact equals the original one. □

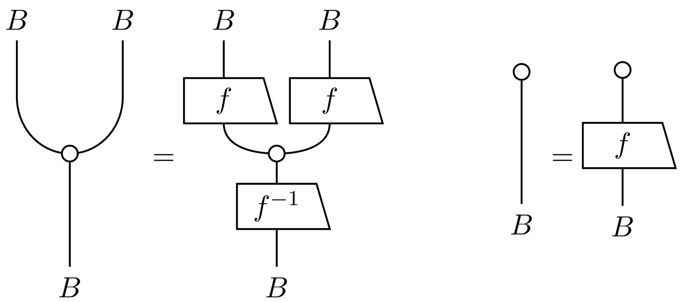
5.1.3 Homomorphisms

We now investigate properties of maps that preserves Frobenius structure.

Definition 5.17 (Frobenius structure transport)**.** In a monoidal category, the *transport* of a Frobenius structure $(A, \curlywedge, \bullet, \curlyvee, \circ)$ across an isomorphism $A \xrightarrow{f} B$ is the Frobenius structure defined by the following data:



(5.13)



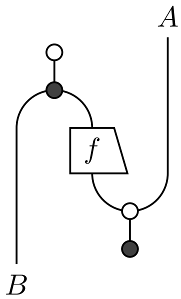
(5.14)

Proof. Straightforward graphical manipulation. □

Definition 5.18. In a monoidal category, a *homomorphism of Frobenius structures* is a morphism that is simultaneously a monoid homomorphism and a comonoid homomorphism.

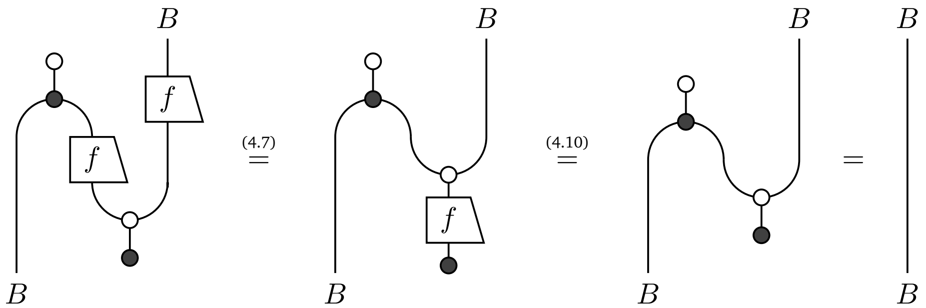
Lemma 5.19. *In a monoidal category, a homomorphism of Frobenius structures is invertible, and the inverse is again a homomorphism of Frobenius structures.*

Proof. Given Frobenius structures on objects A and B and a Frobenius structure homomorphism $A \xrightarrow{f} B$, construct an inverse to f as follows:

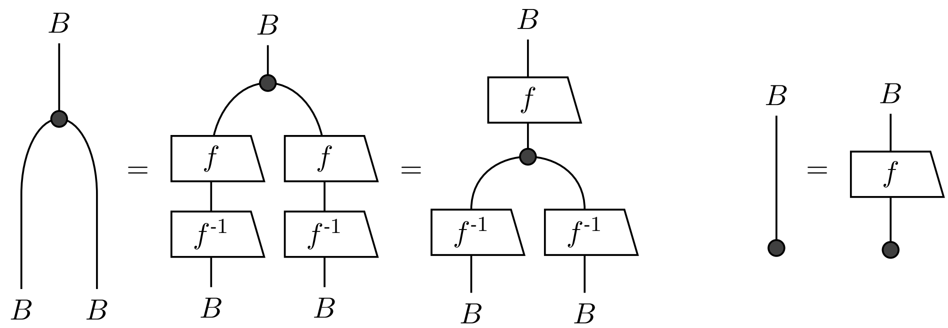


(5.15)

The composite with f gives the identity in one direction:



Here, the first equality uses the comonoid homomorphism property, the second equality uses the monoid homomorphism property, and the third equality follows from Theorem 5.15. By a similar argument, the other composite equals the identity. Finally, because f is a monoid homomorphism, we have:



Postcomposing with f^{-1} shows that f^{-1} is again a monoid homomorphism. Similarly, it is again a comonoid homomorphism. □

5.2 Normal forms

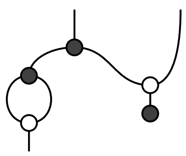
In general there are two ways to think about the graphical calculus:

- a diagram represents a morphism, since it is just a shorthand to express a composition in a monoidal category;
- a diagram is an entity in its own right, which can be manipulated directly by isotopy, and by replacing a subdiagram by one equal to it.

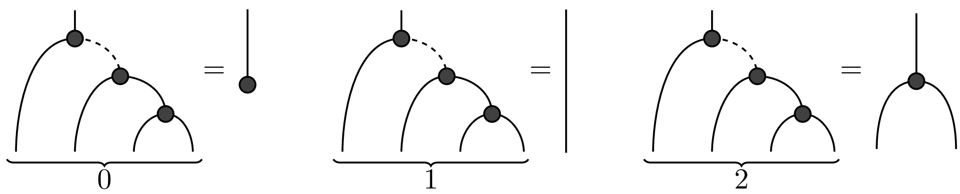
From the first of these perspectives, we may check if two diagrams are equal by evaluating the corresponding morphism of the monoidal category. From the second perspective, determining equality can be harder. However, in some cases, diagrams have a *normal forms*: a unique representation that lets us decide whether or not two diagrams are equal.

5.2.1 Normal forms for Frobenius structures

Consider a morphism $A^{\otimes m} \to A^{\otimes n}$ built out of the ingredients of a Frobenius structure $(A, , , ,)$ in a monoidal category. For example, in the graphical calculus:

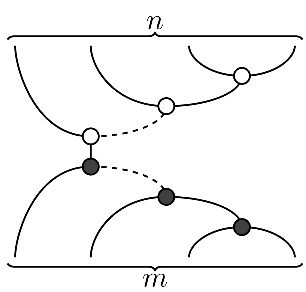


Think of it as a graph: the wires are edges, and each dot $\circ$ or $\bullet$ is a vertex, as is the end of each input or output wire. Such a morphism is *connected* when it has a graphical representation which has a path between any two vertices. When these graphs are large we will use ellipses in graphical notation, as in the following examples:



We will use this kind of representation to prove normal form theorems for different sorts of Frobenius structures.

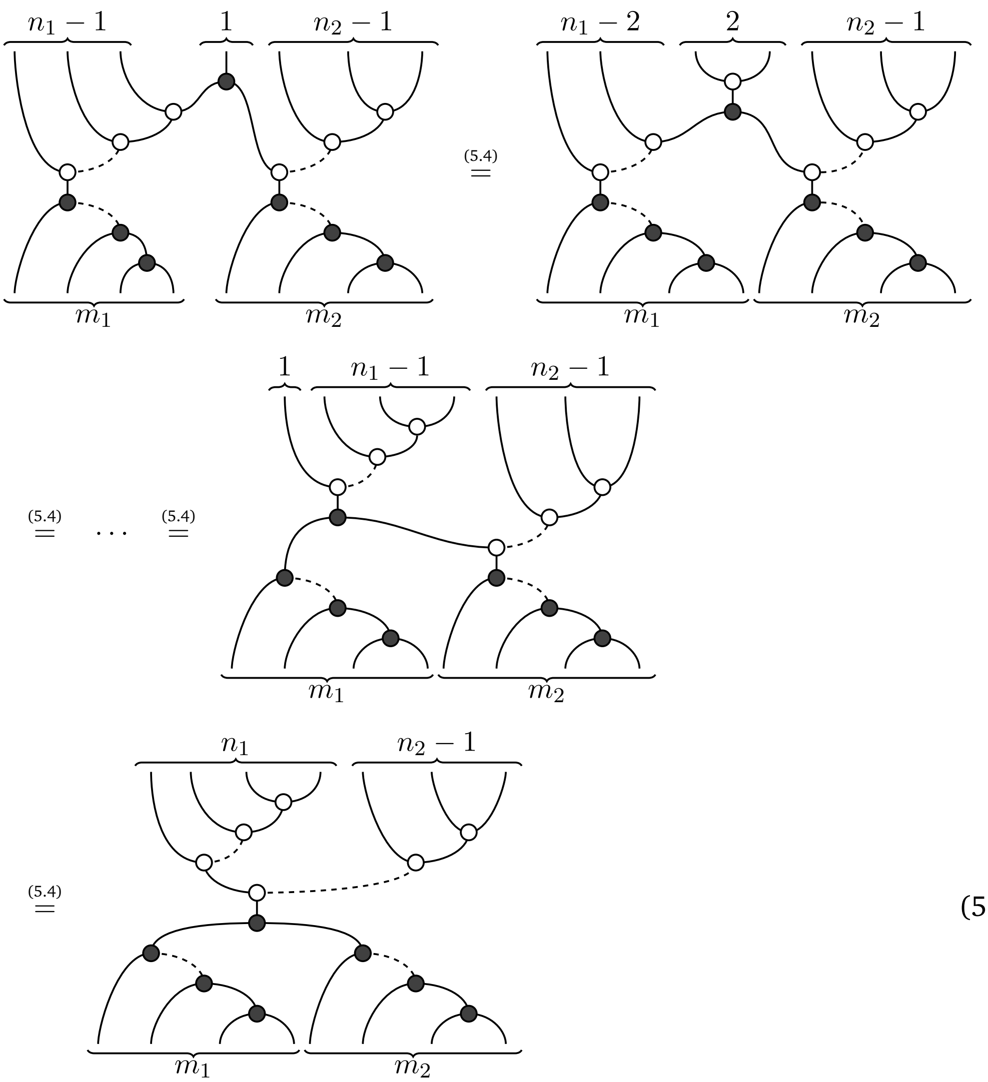
Lemma 5.20 (Special noncommutative spider theorem)**.** *In a monoidal category, let* $(A, , , ,)$ *be a special Frobenius structure. Any connected morphism* $A^{\otimes m} \to A^{\otimes n}$ *built out of finitely many pieces , , , , and* id*, using* $\circ$ *and* $\otimes$*, is equal to the following normal form:*



(5.16)

Proof. We argue by induction on the number of dots. The base case is trivial: there are no dots and the morphism is an identity. The case of a single dot is still trivial, as the diagram must be one of , , , . For the induction step, assume that all diagrams with at most n dots can be brought in normal form (5.16), and consider a diagram with $n+1$ dots. Use naturality to write the diagram in a form where there is a topmost dot. If the topmost dot is a , use the induction hypothesis to bring the rest of the diagram in normal form (5.16), and use unitality (4.5) to finish the proof. If it is a , associativity (4.4) finishes the proof. It cannot be a because the diagram was assumed connected. That leaves the case of a . We distinguish whether the part of the diagram below the is connected or not.

If the subdiagram is disconnected, use the induction hypothesis on the two connected components to bring them in normal form (5.16). The diagram is then of the form below, where we can use the Frobenius identity (5.4) repeatedly to push the topmost down and left:



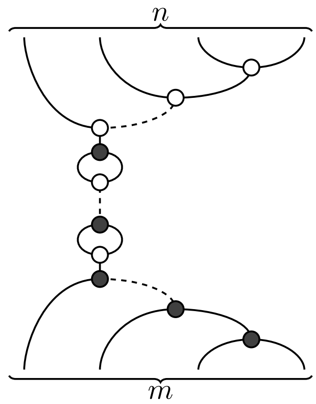
(5.17)

By (co)associativity (4.4) this is a normal form (5.16).

Finally, we are left with the case where the extra dot is on top of a connected subdiagram. Use the induction hypothesis to bring the subdiagram in normal form (5.16). By (co)associativity (4.4) the diagram rewrites to a normal form (5.16) with a $\tinyspecial$ on top, which vanishes by speciality (5.5). This completes the proof. □

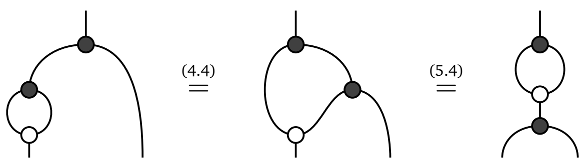
Normal form results for Frobenius structures such as the previous lemma are called Spider Theorems because (5.16) looks a bit like an $(m+n)$–legged spider. It extends to the non-special case as well.

Theorem 5.21 (Noncommutative spider theorem). *In a monoidal category, let* $(A, \tinymult, \tinyunit, \tinycomult, \tinycounit)$ *be a Frobenius structure. Any connected morphism* $A^{\otimes m} \to A^{\otimes n}$ *built out of finitely many pieces* $\tinymult$*,* $\tinyunit$*,* $\tinycomult$*,* $\tinycounit$*, and* id*, using* $\circ$ *and* $\otimes$*, is equal to the following normal form:*



(5.18)

Proof. Use the same strategy as in Lemma 5.20 to reduce to a $\tinymult$ on top of a subdiagram that is connected or not. First assume the subdiagram is disconnected. By the following argument, we may push arbitrarily many $\tinyspecial$ past a $\tinymult$:



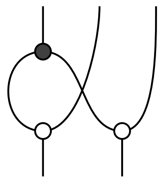
(5.19)

If the two subdiagrams in the first diagram of (5.17) did have $\tinyspecial$ in the middle, these would carry over to the last diagram of (5.17) just below the topmost $\tinymult$. Then (5.19) lets us push them above the $\tinymult$, after which (co)associativity (4.4) finishes the proof as before, but now without assuming speciality.

Finally, assume the extra dot $\tinymult$ is on top of a connected subdiagram. As in Lemma 5.20 the diagram rewrites into a normal form (5.18) with a $\tinyspecial$ on top. A similar argument to (5.19) lets us push the $\tinyspecial$ down past $\tinycomult$ dots, and by (co)associativity (4.4) we end up with a normal form (5.18) again. □

5.2.2 Normal forms for classical structures

Next we consider the commutative case of classical structures. We can allow symmetries as building blocks and still expect the same normal form. This introduces a subtlety in the induction step of a $\tinymult$ on top of a disconnected subdiagram, because the subdiagram need not be a monoidal product of two connected morphisms; think for example of the following situation:

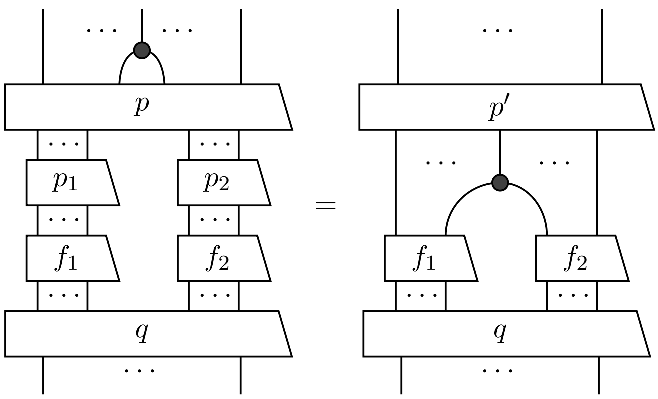


We will call a morphism $A^{\otimes n} \xrightarrow{p} A^{\otimes n}$ built from pieces id and using $\circ$ and $\otimes$ *permutations*. They correspond to bijections $\{1,\ldots,n\} \to \{1,\ldots,n\}$, and we may write things like $p^{-1}(2)$ for the (unique) input wire that p connects to the 2nd output wire.

Theorem 5.22 (Commutative spider theorem)**.** *In a symmetric monoidal category, let* $(A, \;, \;, \;, \;)$ *be a commutative Frobenius structure. Any connected morphism* $A^{\otimes m} \to A^{\otimes n}$ *built out of finitely many pieces , , , ,* id*, and , using* $\circ$ *and* $\otimes$*, is equal to the normal form* (5.18).

Proof. Again use the same strategy as in Lemma 5.20. Without loss of generality we may assume there are no above the topmost dot, because they will vanish by coassociativity (4.2) and cocommutativity (4.1) once we have rewritten the lower subdiagram in a normal form (5.18). So again the proof reduces to a on top of a subdiagram that is either connected or not. In the connected case, the very same strategy as in Theorem 5.21 finishes the proof.

The disconnected case is more subtle. Because the whole diagram is connected, the subdiagram without the has exactly two connected components, and every input wire and every output wire belongs to one of the two. Therefore the subdiagram is of the form $p \circ (f_1 \otimes f_2) \circ q$ for permutations p, q and connected morphisms f_i. Use the induction hypothesis to bring f_i in a normal form (5.18). By cocommutativity (4.1) and coassociativity (4.2) we may freely postcompose both f_i with any permutations p_i, and precompose the with a . For example, if $f_i \colon A^{\otimes m_i} \to A^{\otimes n_i}$, we may choose any permutations p_i with $p_1(n_1) = p^{-1}(k_1)$ and $p_2(1) = p^{-1}(k_2) - n_1$, where k_i is the position of the leg of the connecting to f_i. So by naturality we can write the whole diagram as follows for some permutation p':



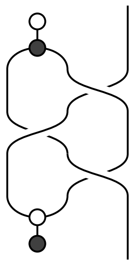
Now the subdiagram consisting of f_i and the topmost is of the form (5.17), and the same strategy used in the proof of Theorem 5.21 brings it in normal form (5.18), after which p' and q vanish by (co)associativity (4.4) and (co)commutativity (4.6). $\square$

For a (co)commutative Frobenius structure in a symmetric monoidal category, any morphism built from the basic ingredients by finite means, connected or not, equals

$p \circ (f_1 \otimes \cdots \otimes f_n) \circ q$ for some permutations p, q and morphisms $f_1, \ldots, f_n$ of the form (5.18). In braided monoidal categories, however, this breaks down.

Proposition 5.23 (No braided spider theorem)**.** *In a braided monoidal category that is not symmetric, the analogous statement to Theorem 5.22 does not hold.*

Proof. Regard the following diagram as a piece of string on which an overhand knot is tied:



The Frobenius structure axioms can all be interpreted as homotopies of the string – (co)associativity (4.4), (co)unitality (4.5), (co)commutativity (4.6), and the Frobenius law (5.4) – which respect the embedding in 3-dimensional space. But clearly, such a homotopy cannot untie the string. □

5.3 Justifying the Frobenius law

Morphisms $A \to A$ in a category can be composed, and by map-state duality, this endows $A^* \otimes A$ with the pair of pants monoid structure, as discussed in Section 4.1.4. In the presence of daggers, this monoid picks up the additional structure of an involution. This section proves that the Frobenius law holds precisely when the Cayley embedding of Proposition 4.13 preserves this additional structure. Thus Frobenius structures are motivated by the 'way of the dagger'.

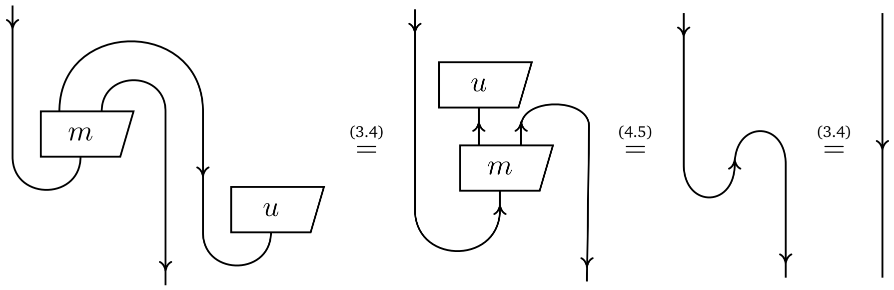
5.3.1 Involutive monoids

Any morphism $H \xrightarrow{f} K$ in a monoidal dagger category gives rise to another morphism $K \xrightarrow{f^\dagger} H$. The name $\ulcorner f \urcorner \colon I \to H^* \otimes K$ of f lands in $A = H^* \otimes K$, whereas the name $\ulcorner f^\dagger \urcorner$ of $f^\dagger$ lives in $A^* = K^* \otimes H$. Indeed, in the category **FHilb**, taking daggers $f \mapsto f^\dagger$ is anti-linear (see Section 0.2), and so is a morphism $A \to A^*$.We will use this in particular when $H = K$. Then $A = H^* \otimes H$ becomes a pair of pants monoid under (names of) composition of morphisms $H \to H$, which also has an involution $A \to A^*$ induced by taking (names of) daggers.

The involution $f \mapsto f^\dagger$ additionally satisfies $(g \circ f)^\dagger = f^\dagger \circ g^\dagger$. Hence it is a homomorphism of monoids if we take the codomain to be the monoid with the opposite multiplication. This comes down to the following lemma and definition when we internalize the involution along map-state duality.

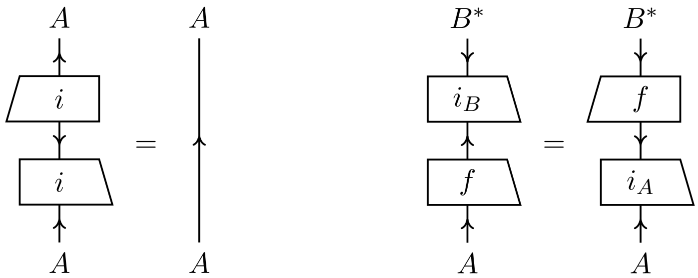
Lemma 5.24 (The opposite monoid)**.** *In a dagger pivotal category, if (A, m, u) is a monoid, then (A^*, m_*, u_*) is also a monoid.*

Proof. Unitality of m_* and u_* follows directly from unitality of m and u:



Associativity of m_* follows in a similar way from associativity of m. □

Definition 5.25 (Involutive monoid). In a dagger pivotal category, a monoid $(A, \tinymult, \tinyunit)$ is *involutive* when it comes equipped with an *involution*, a morphism of monoids $A \xrightarrow{i} A^*$ satisfying $i_* \circ i = \mathrm{id}_A$. A *morphism of involutive monoids* is a monoid homomorphism $A \xrightarrow{f} B$ satisfying $i_B \circ f = f_* \circ i_A$.



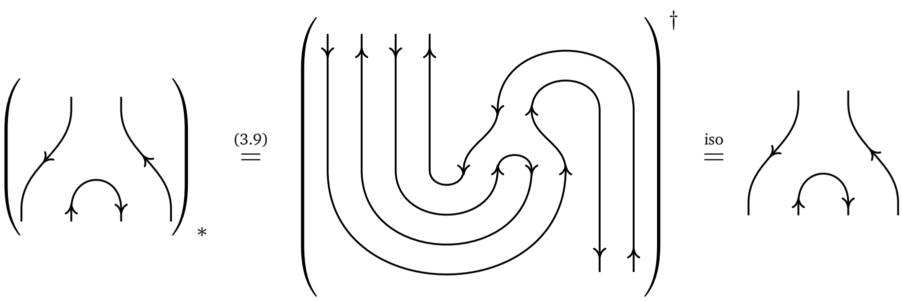
(5.20)

Note that the involution i is necessarily an isomorphism: by definition of an involution we have $i_* \circ i = \mathrm{id}_A$, and the opposite identity $i \circ i_* = \mathrm{id}_{A^*}$ then follows by applying the functor $(-)_*$.

We now consider some examples.

Example 5.26. In $\mathbf{Rel}$, the Frobenius structure $(G, \tinymult, \tinyunit)$ induced by a groupoid $\mathbf{G}$ in the manner of Example 5.3 has a canonical involutive structure. The opposite monoid arises from the opposite groupoid, and the involution can be chosen as sending a morphism $f \in \mathbf{C}$ to its inverse $f^{-1} \in \mathbf{C}^{\mathrm{op}}$.

Example 5.27. In a dagger pivotal category, a pair of pants monoid on $A^* \otimes A$ (see Lemma 4.11) has a canonical involutive structure, with the involution given by the identity. The opposite monoid is the pair of pants monoid itself. We can verify this as follows:



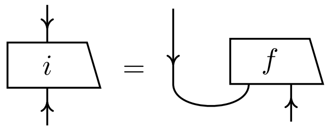
Two abstract identifications hide the concrete algebra here. Consider $A = \mathbb{C}^n$ in $\mathbf{FHilb}$, so the pair of pants monoid $A^* \otimes A$ becomes the matrix algebra $\mathbb{M}_n$ (see

Example 4.12). Firstly, since the dual space A^* in **FHilb** consists of functions $A \to I$, the convention $B^* \otimes A^* \simeq (A \otimes B)^*$ identifies $\langle j| \otimes \langle i| \in B^* \otimes A^*$ with $|ij\rangle \in (A \otimes B)^*$. Thus, if we want to think of $\mathbb{M}_n^*$ as being the complex n-by-n matrices again, it has to carry the opposite multiplication: ab in $\mathbb{M}_n^*$ is the ordinary matrix multiplication ba in $\mathbb{M}_n$. Secondly, the canonical isomorphism $A^* \simeq A$ given by $\langle i| \mapsto |i\rangle$ is anti-linear (see Chapter 0). Hence the canonical involution $\mathbb{M}_n \to \mathbb{M}_n^*$ becomes the complex conjugate transpose $f \mapsto f^\dagger$, and scalar multiplication in $\mathbb{M}_n^*$ is the complex conjugate of scalar multiplication in $\mathbb{M}_n$.

5.3.2 Dagger closure

Proposition 4.13 showed that any monoid on a dual object is a submonoid of a pair of pants monoid. Example 5.27 showed that pair of pants monoids in monoidal dagger categories are involutive monoids. It therefore makes sense to ask when a monoid on a dagger dual object is an involutive submonoid of a pair of pants monoid. The following theorem characterizes when this is the case.

We can also phrase when a monoid $(A, \ , \ )$ on an object A has an involution i in terms of a map $A \otimes A \xrightarrow{f} I$:



A canonical choice for such a map f would be : $A \otimes A \to I$. For a pair of pants monoid as in Example 5.27, this would give $i = \mathrm{id}_{H^* \otimes H}$. Compare also Proposition 5.16.

We now give a powerful theorem showing two alternative ways to understand a dagger Frobenius structure.

Theorem 5.28. *In a dagger pivotal category, given a monoid* $(A, \ , \ )$*, define* $R : A \to A^* \otimes A$ *and* $i : A \to A^*$ *as follows:*

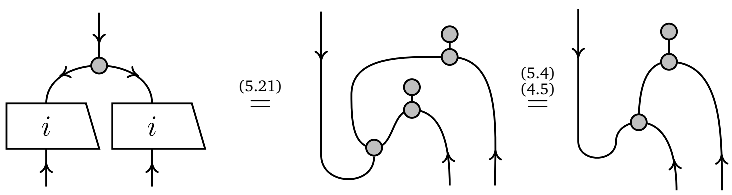
(5.21)

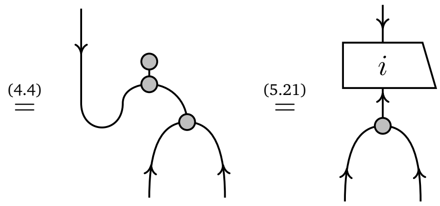
Then the following are equivalent:

- *(a)* $(A, \ , \ , \ , \ )$ *is a dagger Frobenius structure;*
- *(b)* $(A, \ , \ )$ *is an involutive monoid when equipped with* i*;*
- *(c)* $R_* \circ i = R$.

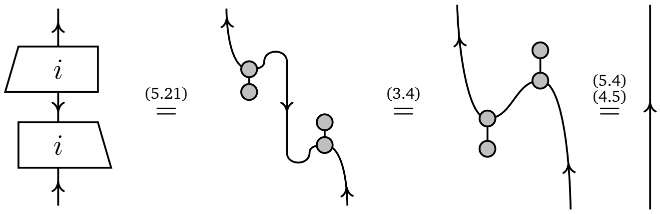
Proof. In this proof we show that (a) and (b) are equivalent. We leave their equivalence to property (c) to Exercise 5.7.9.

Assuming (a), we prove that i respects multiplication as in equation (4.9):



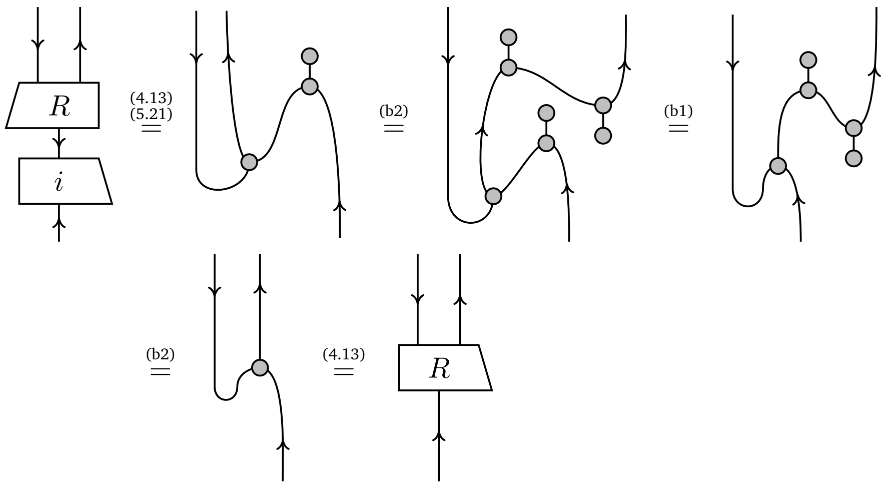


The second equation uses Lemma 5.4 and unitality, the third associativity. That i preserves units is trivial. Finally, i is indeed involutive:

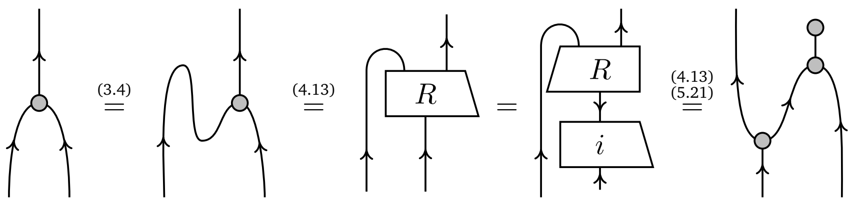


The second equation is the snake identity, and last equation uses the Frobenius law and unitality. Thus the monoid is involutive, and (b) holds.

Next assume (b), and split the assumption into two as in the previous step; write (b1) for $i \circ {} = ({})_* \circ (i \otimes i)$, and (b2) for $i_* \circ i = \mathrm{id}_A$. Then:

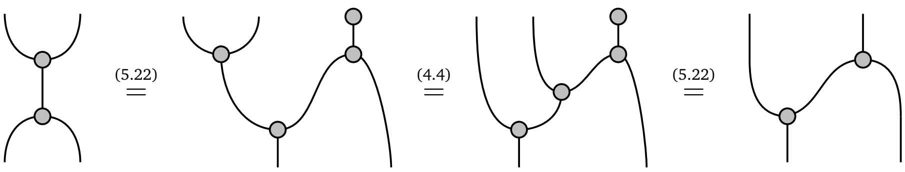


So:



(5.22)

Hence:



Combining this equation with its adjoint establishes the Frobenius law. □

Thus, if we want to think of endomorphisms as forming monoids via map-state duality, cooperation with daggers forces the Frobenius law on us. We may regard the Frobenius law as a coherence property between daggers and dual objects.

5.4 Classification

This section classifies the special dagger Frobenius structures in our two running examples, the category of Hilbert spaces, and the category of sets and relations. It turns out that dagger Frobenius structures in **FHilb** must be direct sums of the matrix algebras of Example 4.12; hence classical structures in **FHilb** must copy an orthonormal basis as in Section 5.1; and special dagger Frobenius structures in **Rel** must be induced by a groupoid as in Example 5.3.

5.4.1 H*-algebras

This subsection combines standard results with Theorem 5.28 to give the exact form of special dagger Frobenius structures in **FHilb**, by relating them to finite-dimensional H*-algebras. These structures have been studied thoroughly in functional analysis, and we will use some of these deep results without proof.

Definition 5.29. An *H*-algebra* is an algebra (see Example 4.4) A, that is also a Hilbert space, equipped with an anti-linear involution $\dagger \colon A \to A$ satisfying

$$\langle ab|c\rangle = \langle b|a^\dagger c\rangle = \langle a|cb^\dagger\rangle \tag{5.23}$$

for all $a, b, c \in A$.

Sometimes the definition also includes the normalization requirement $\|ab\| \leq \|a\|\|b\|$, but we do not include this here.

Example 5.30. Any finite-dimensional Hilbert space H and positive real number k induces an H*-algebra with elements given by $B(H, k)$, the space of linear maps from H to itself, with the dagger given by the adjoint, and with inner product given by the following condition:

$$\langle a, b\rangle = k\,\mathrm{Tr}(a^\dagger b) \tag{5.24}$$

Up to the normalisation factor k, these are subsets $A \subseteq \mathbb{M}_n$ of matrix algebras that are closed under addition, scalar multiplication, matrix multiplication, matrix adjoint, and that contain the identity matrix.

If $A \subseteq \mathbb{M}_m$ and $B \subseteq \mathbb{M}_n$ are finite-dimensional H*-algebras, then so is their direct sum $A \oplus B \subseteq \mathbb{M}_{m+n}$. Indeed, if (A, μ_A) and (B, μ_B) are dagger Frobenius structures in a compact dagger category with dagger biproducts, then so is $A \oplus B$. Using the matrix calculus of Lemma 2.26 and the distributivity of Lemma 3.21, the multiplication and unit are given as follows:

$$\begin{pmatrix} \mu_A & 0 & 0 & 0 \\ 0 & 0 & 0 & \mu_B \end{pmatrix} : (A \oplus B) \otimes (A \oplus B) \to A \oplus B \qquad \begin{pmatrix} \mu_A \\ \mu_B \end{pmatrix} : I \to A \oplus B \tag{5.25}$$

See also Exercise 5.7.8 and Lemma 7.47. But taking direct sums of weighted matrix algebras is the only freedom there is in finite-dimensional H*-algebras, as a result of the following structure theorem.

Theorem 5.31 (Ambrose)**.** *Any finite-dimensional H*-algebra is an orthogonal direct sum of the form* $A \simeq B(H_1, k_1) \oplus \cdots \oplus B(H_n, k_n)$ *for a natural number* n*, finite-dimensional Hilbert spaces* $H_1, \ldots, H_n$*, and positive real numbers* $k_1, \ldots, k_n$*.* □

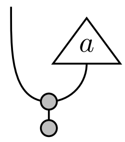
Therefore, via the Cayley embedding, we may think of H*-algebras in **FHilb** as algebras of matrices, with a scaling factor attached to each factor.

The classification of symmetric dagger Frobenius structures in **FHilb** is now completed by relating them to finite-dimensional H*-algebras.

Theorem 5.32. *In* **FHilb***, for a monoid* (A, μ, η)*, the following are equivalent:*

(a) it is a symmetric dagger Frobenius structure;

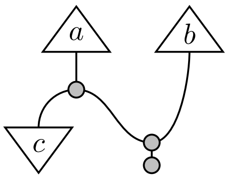
(b) it is a finite-dimensional H-algebra under the involution mapping* $a \in A$ *to:*



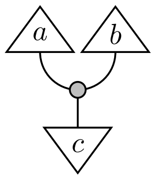
(5.26)

Proof. Assuming (a), the H*-axiom (5.23) is established graphically using the fact that **FHilb** is monoidally well-pointed:

$\langle a|cb^\dagger\rangle \;=$

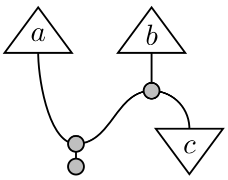


$\overset{(5.1)}{\underset{(4.5)}{=}}$

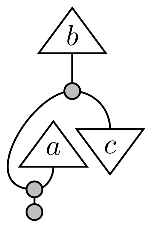


$= \;\langle ab|c\rangle$

$\overset{(5.1)}{\underset{(4.5)}{=}}$



$\overset{(5.6)}{=}$



$= \;\langle b|a^\dagger c\rangle$

The converse follows from Theorem 5.31 and implication (b) ⇒ (a) of Theorem 5.28, by observing that any matrix algebras $B(H, k)$ is symmetric, as in Example 5.13, as are direct sums of them. □

Notice that (5.26) is an anti-linear representation of (5.21). Also, note that this does not apply to all dagger Frobenius structures, but only the symmetric ones.

Given Theorem 5.32, an obvious question is how to construct the canonical H*-algebras $B(\mathbb{C}^n, k)$ as symmetric dagger Frobenius structures. We do this by scaling the canonical pair of pants algebras of Example 4.12, as follows.

Proposition 5.33. *For a Hilbert space* $\mathbb{C}^n$ *and* $p \in \mathbb{C}$*, the symmetric dagger Frobenius structure* $(\mathbb{C}^n \otimes \mathbb{C}^n, p\diagup\!\frown\!\diagdown, p^{-1}\cup)$ *yields the H*-algebra* $B(\mathbb{C}^n, 1/pp^*)$*.*

Proof. It is clear by Example 4.12 that this Frobenius structure is isomorphic as an algebra to $B(\mathbb{C}^n)$, which has simply been rescaled, with the unit $p^{-1}\cup$ corresponding to the identity matrix id_n. To fix the H*-algebra parameter k, we consider equation (5.24) for the case that $a = b = \mathrm{id}_n$; since $\mathrm{Tr}(\mathrm{id}_n) = n$, we have $\langle \mathrm{id}_n, \mathrm{id}_n\rangle = kn$. The left-hand side is $\langle p^{-1}\cup, p^{-1}\cup\rangle = \langle \cup, \cup\rangle/pp^* = n/pp^*$, yielding $k = 1/pp^*$. □

Hence, we can build any basic H*-algebra $B(\mathbb{C}^n, k)$ as the dagger Frobenius structure $(\mathbb{C}^n \otimes \mathbb{C}^n, k^{-1/2}/\!\!\cap\!\!\backslash, k^{1/2}\cup)$. As a corollary, we can identify the special symmetric dagger Frobenius algebras, as follows.

Corollary 5.34. *Special symmetric dagger Frobenius structures are direct sums of monoids of the form $(\mathbb{C}^n \otimes \mathbb{C}^n, n^{-1/2}/\!\!\cap\!\!\backslash, n^{1/2}\cup)$, corresponding to H*-algebras of the form $B(\mathbb{C}^n, n)$.*

Proof. The specialness condition (5.5) holds for an algebra $(\mathbb{C}^n \otimes \mathbb{C}^n, p/\!\!\cap\!\!\backslash, p^{-1}\cup)$ just when $pp^* = 1/n$, since we have $\cap \circ (\cap)^\dagger = \cap \circ \cup = \bigcirc = n$. The result then follows from Proposition 5.33. □

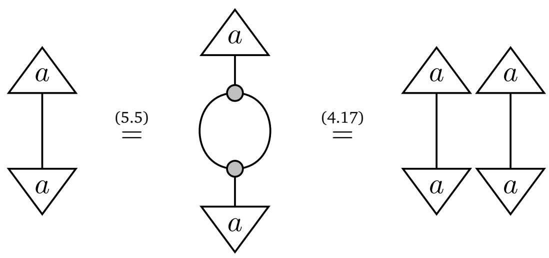
5.4.2 Orthogonal and orthonormal bases

Since the only commutative matrix algebra is the algebra of 1-by-1 matrices, we can conclude from Theorem 5.31 that commutative finite-dimensional H*-algebras are all of the form $A \simeq \sum_i B(\mathbb{C}, k_i)$. But $B(\mathbb{C}) \simeq \mathbb{C}$, and so this gives us a basis for A; writing $|i\rangle$ for the ith element of this basis, the inner product structure then tells us that $\langle i|j\rangle = \delta_{i,j} k_i$. We can use this to characterize orthogonal and orthonormal bases in terms of commutative Frobenius algebras.

We start with the following lemma.

Lemma 5.35. *In* **FHilb**, *nonzero copyable states of a dagger special monoid-comonoid pair in* **FHilb** *have unit length.*

Proof. It follows from speciality that any nonzero copyable state a has a norm that squares to itself:

$\langle a|a\rangle =$ 

$= \langle a|a\rangle^2.$

If a is nonzero then $\langle a|a\rangle$ must be nonzero by (0.25), hence $\|a\| = 1$. □

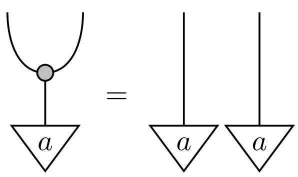
The main basis classification theorem is the following.

Theorem 5.36. *For a fixed finite-dimensional Hilbert space in* **FHilb**, *there are bijective correspondences between:*

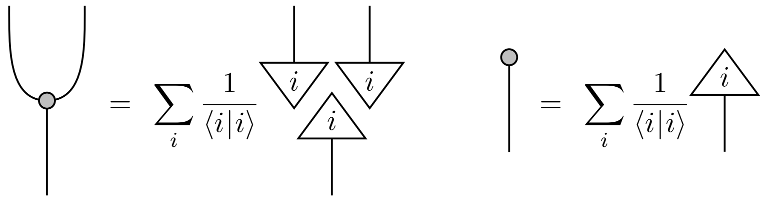
- *orthogonal bases and commutative dagger Frobenius structures;*
- *orthonormal bases and classical structures;*

as follows:

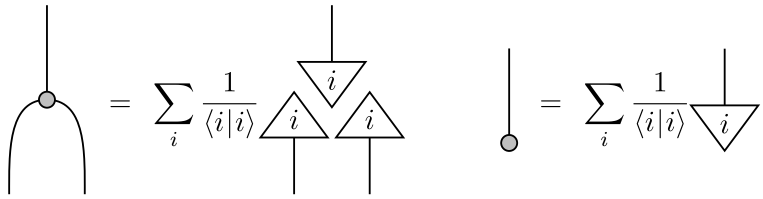
- *given a commutative dagger Frobenius structure $(A, ,)$, the corresponding basis comprises those vectors $a \in A$ satisfying:*



- *given a basis $\{a_1, \ldots, a_n\}$ of A, a commutative dagger Frobenius structure on A is given by:*



(5.27)

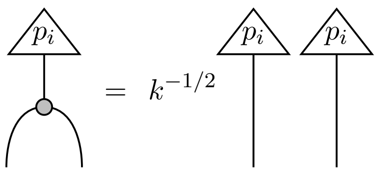


(5.28)

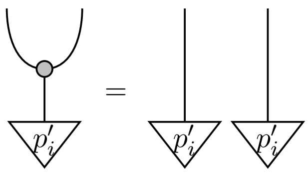
Proof. Given an orthogonal basis, (5.27) gives a comonoid, its adjoint (5.28) gives a monoid, and these are commutative and satisfy the Frobenius law.

Conversely, a commutative dagger Frobenius structure is symmetric, so by Theorem 5.32 gives finite-dimensional commutative H*-algebra, which by Theorem 5.31 is of the form $A = B(H_1, k_1) \oplus \cdots \oplus B(H_n, k_n)$ for finite-dimensional Hilbert spaces H_i and positive real numbers k_i. But such an algebra is commutative exactly when each H_i is isomorphic to $\mathbb{C}$.

Now consider the projection $p_i : A \to B(\mathbb{C}, k_i)$. This is an algebra homomorphism, since $p_i\big((a_1, \ldots, a_n) \cdot (a'_1, \ldots, a'_n)\big) = p_i(a_1 \cdot a'_1, \ldots, a_n \cdot a'_n) = a_i \cdot a'_i$ and $p_i(a_1, \ldots, a_n) \cdot p_i(a'_1, \ldots, a'_n) = a_i \cdot a'_i$. Writing this out graphically gives the following condition:



Note that the space $B(\mathbb{C}, k_i)$ is not depicted, since it is isomorphic to $\mathbb{C}$, and that by Proposition 5.33, we write the scalar $k^{-1/2}$ for its multiplication operation. Redefining $p'_i = k^{-1/2} p_i$, and taking the adjoint, we obtain the following:



This exhibits p'_i as a copyable state. Therefore the nonzero copyable states are precisely the projections $p_i : B(\mathbb{C}, k_1) \oplus \cdots \oplus B(\mathbb{C}, k_n) \to B(\mathbb{C}, k_i)$, and they form a basis. Moreover, because the direct sums in Theorem 5.31 are orthogonal, the copyable states are orthogonal, and hence form an orthogonal basis.

Finally, these procedures are inverse to each other. Given an orthogonal basis, the associated commutative dagger Frobenius structure clearly has the basis elements as the copyable states. Conversely, given a commutative dagger Frobenius algebra, if we extract its copyable states and use that to build a new commutative dagger

Frobenius algebra, it will clearly have the same family of copyable states. But then, if two comultiplications copy the same basis of states, they must be equal, as we have determined their action on a family of states which span the space, and **FHilb** is well-pointed.

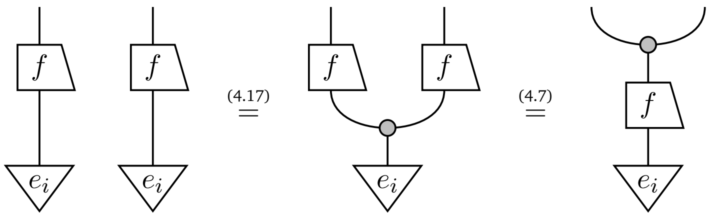
Lemma 5.35 shows that the commutative dagger Frobenius structure is special, and hence a classical structure, just when all of the copyable states are of unit length. □

We can now recognize Definition 5.17 of transport of a Frobenius structure as saying that the image of an orthonormal basis under a unitary map is again an orthonormal basis. Note that the map has to be unitary; if it is merely invertible then the transport is merely a Frobenius structure, and not necessarily a dagger Frobenius structure, so that the previous theorem does not apply.

Theorem 5.36 gives a converse to Example 4.6: every comonoid homomorphism between classical structures in **FHilb** is a function between the corresponding orthonormal bases.

Corollary 5.37. *In* **FHilb***, a morphism between two commutative dagger Frobenius structures preserves comultiplication if and only if it sends copyable states to copyable states. It is a comonoid homomorphism if and only if it sends nonzero copyable states to nonzero copyable states.*

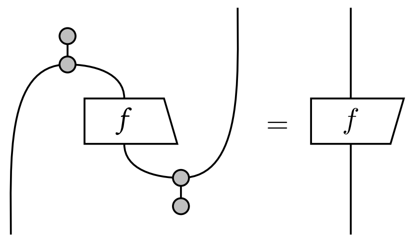
Proof. By linear extension, the comonoid homomorphism condition (4.7) will hold if and only if it holds on a basis of copyable states $\{e_i\}$ of the first classical structure, which must exist by Theorem 5.36. This gives the following equation:



Here the first equality expresses the fact that the state e_i is copyable, and the second equality is the comonoid homomorphism condition. Hence $f(e_i)$ is itself a copyable state. Thus (4.7) holds if and only if f sends copyable states to copyable states. The counit preservation condition (4.8) follows if and only if f sends nonzero copyable states to nonzero copyable states, because the unit of a classical structure is just the sum of its copyable states. □

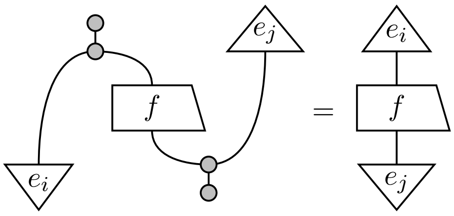
Because comonoid homomorphisms between classical structures in **FHilb** behave like functions, if we write them in matrix form using the bases of the associated classical structures, the result will be a matrix of zeroes and ones, with a single entry one in each column. These matrices are of course self-conjugate, since all the entries are real numbers. This gives a further property of comonoid homomorphisms.

Lemma 5.38. *In* **FHilb***, comonoid homomorphisms between classical structures are self-conjugate:*



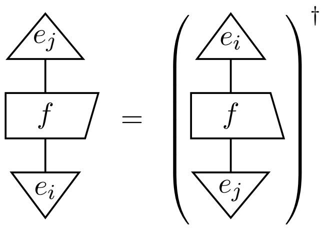
(5.29)

Proof. These linear maps will be the same if their matrix entries are the same. On the left-hand side, this gives:



$$= \begin{bmatrix} 1 & \text{if } e_i = f(e_j) \\ 0 & \text{if } e_i \neq f(e_j) \end{bmatrix}$$

On the right-hand side:

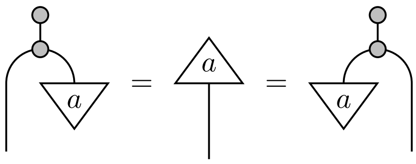


$$= \begin{bmatrix} 1 & \text{if } e_i = f(e_j) \\ 0 & \text{if } e_i \neq f(e_j) \end{bmatrix}^\dagger = \begin{bmatrix} 1 & \text{if } e_i = f(e_j) \\ 0 & \text{if } e_i \neq f(e_j) \end{bmatrix}$$

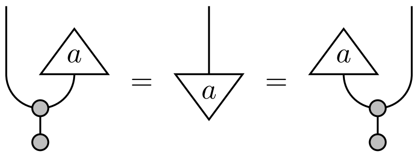
Thus (5.29) holds. □

Some further results about classical structures follow.

Lemma 5.39. *In* **FHilb***, for a commutative dagger Frobenius structure, the following equations hold for any copyable state* a*:*



(5.30)

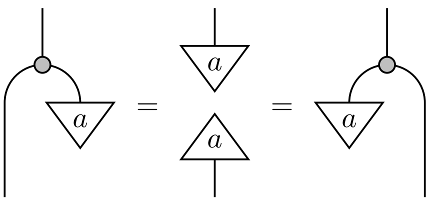


(5.31)

Proof. A copyable state $I \xrightarrow{a} A$ can be thought of as a function from the unique copyable state on the trivial classical structure on I, to the chosen copyable state, and therefore gives a comonoid homomorphism. The result now follows from Lemma 5.38. □

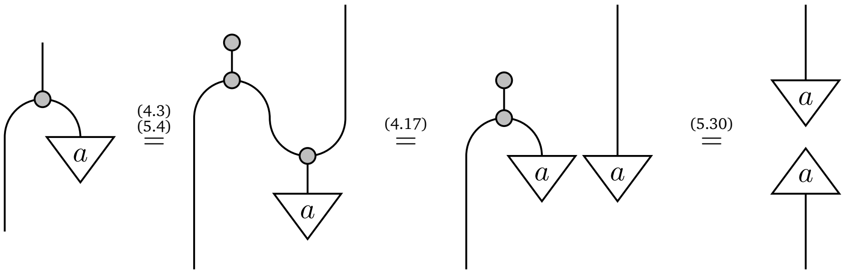
States are also copied 'on the side' of the multiplication of a commutative dagger Frobenius structure.

Lemma 5.40. *In* **FHilb***, for a commutative dagger Frobenius structure, the following equations hold for any copyable state* a*:*



(5.32)

Proof. A simple graphical argument establishes the first equality:



(5.33)

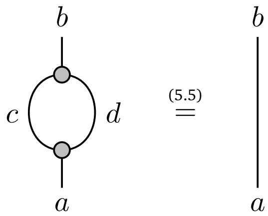
The second equality follows similarly. □

5.4.3 Groupoids

We now investigate what special dagger Frobenius structures look like in $\mathbf{Rel}$. Recall that a groupoid is a category in which every morphism has an inverse, and that any groupoid induces a dagger Frobenius structure in $\mathbf{Rel}$ by Example 5.3 and Example 5.11. It turns out that these examples are the only ones.

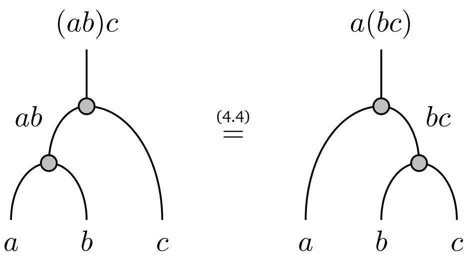
Theorem 5.41. *In* $\mathbf{Rel}$*, special dagger Frobenius structures correspond exactly to groupoids.*

Proof. Examples 5.3 and 5.6 already showed that groupoids give rise to special dagger Frobenius structures by writing A for its set of arrows, U for its subset of identities, and M for the composition relation. Conversely, let A be a special dagger monoid-comonoid pair in $\mathbf{Rel}$ with multiplication $M\colon A \times A \to A$ and unit $U \subseteq A$. Suppose that $b\,(M \circ M^\dagger)\,a$ for $a, b \in A$. Then by the definition of relational composition, there must be some $c, d \in A$ such that $b\,M\,(c,d)$ and $(c,d)\,M^\dagger\,a$. To understand the consequence of the dagger speciality condition (5.5), we use the decorated notation of Section 1.1.4:



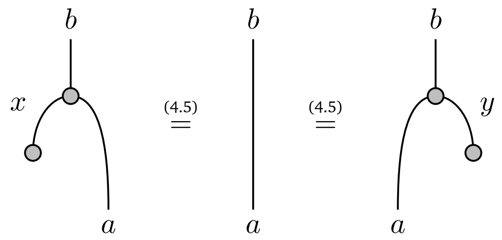
On the right-hand side, two elements $a, b \in A$ are only related by the identity relation if they are equal. So the same must be true on the left-hand side. Thus: if two elements $c, d \in A$ multiply to both $a \in A$ and $b \in A$ – that is, both $b\,M\,(c,d)$ and $a\,M\,(c,d)$ hold – then necessarily $a = b$. Hence the multiplication of two elements is unique, if it exists. We may simply write cd for the multiplication of c and d, remembering that this only makes sense if it is defined.

Next, consider associativity:



So ab and $(ab)c$ are both defined exactly when bc and $a(bc)$ are both defined, and then $(ab)c = a(bc)$. So when a triple product is defined under one bracketing, it is also defined under the other bracketing, and the products are equal.

Finally, unitality:

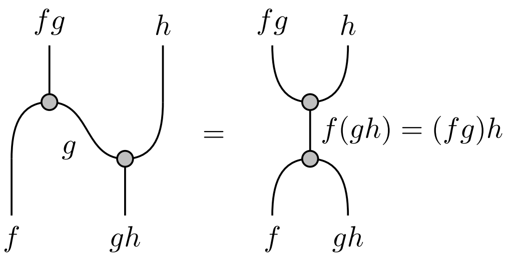


Here $x, y \in U \subseteq A$ are units, determined by the unit $1 \xrightarrow{U} A$ of the monoid. The first equality says that all a, b allow some $x \in U$ with $xa = b$ if and only if $a = b$. The second equality says that $ay = b$ for some $y \in U$ if and only $a = b$. Put differently: multiplying on the left or the right by a element of U is either undefined, or gives back the original element.

What happens when you multiply elements from U together? If $z \in U$ then certainly $z \in A$, and so $xz = x$ for some $x \in U$. But then we can multiply $z \in U \subseteq A$ on the left with x to produce x, and so $x = z$ by the previous paragraph! So elements of U are idempotent, and if we multiply two different elements, the result is undefined.

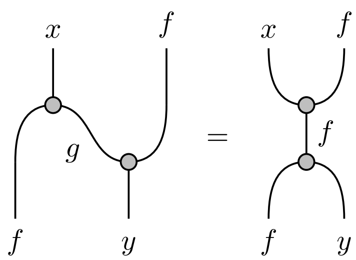
Lastly, suppose that an element $a \in A$ has two left identities; that is, suppose that distinct $x, x' \in U$ satisfy $xa = a = x'a$. This would imply $a = xa = x(x'a) = (xx')a$, which is undefined, as we have seen. So every element has a unique left identity, and similarly every element has a unique right identity.

Altogether, this gives exactly the data to define a category. Let U be the set of objects, and A the set of morphisms. Suppose $f, g, h \in A$ are morphisms such that fg is defined and gh is defined. To establish that $(fg)h = f(gh)$ is also defined, decorate the Frobenius law with the following elements:



If fg and gh are defined then the left-hand side is defined, and hence the right hand side must also be defined.

To show that every morphism has an inverse, consider the following different decoration of the Frobenius law, for any $f \in A$ with left unit x and right unit y:



The properties of left and right units make the right-hand side decoration valid. Hence there must be $g \in A$ with which to decorate the left-hand side. But such a g is precisely an arrow with $fg = y$ and $gf = x$, which is an inverse for f. □

Note also that the nondegenerate form of Proposition 5.16 is the coname of the function $g \mapsto g^{-1}$; see also Example 5.26.

Classifying the pair of pants Frobenius structures of Lemma 4.11 and Lemma 5.9 leads to the indiscrete categories of Definition 0.15.

Corollary 5.42. *In* $\mathbf{Rel}$*, pair of pants structures correspond precisely to indiscrete groupoids.*

Proof. Let A be a set. By definition, $(A^* \otimes A, ,)$ corresponds to a groupoid $\mathbf{G}$ whose set of morphisms is $A \times A$, and whose composition is given by

$$(b_2, b_1) \circ (a_2, a_1) = \begin{cases} (b_2, a_1) & \text{if } b_1 = a_2, \\ \text{undefined} & \text{otherwise.} \end{cases}$$

We deduce that the identity morphisms of $\mathbf{G}$ are the pairs (a_2, a_1) with $a_2 = a_1$. So objects of $\mathbf{G}$ just correspond to elements of A. Similarly, we find that the morphism (a_2, a_1) has domain a_1 and codomain a_2. Hence (a_2, a_1) is the unique morphism $a_1 \to a_2$ in $\mathbf{G}$. □

Classifying classical structures in $\mathbf{Rel}$ is now easy. Recall from Example 5.11 that a groupoid is abelian when $g \circ h = h \circ g$ whenever one of the two sides is defined.

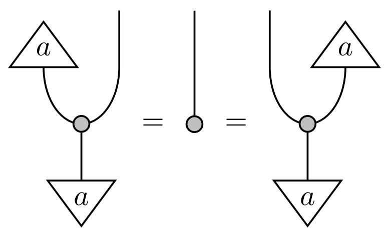
Corollary 5.43. *In* $\mathbf{Rel}$*, classical structures exactly correspond to abelian groupoids.*

Proof. An immediate consequence of Theorem 5.41. □

5.5 Phases

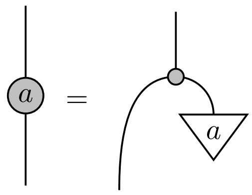
In quantum information theory, an interesting family of maps are *phase gates*: diagonal matrices whose diagonal entries are complex numbers of norm 1. For a particular Hilbert space equipped with a basis, these form a group under composition, which we will call the *phase group*. This turns out to work fully abstractly: any dagger Frobenius structure in any monoidal dagger category gives rise to a phase group.

Definition 5.44 (Phase)**.** In a monoidal dagger category, given a dagger Frobenius structure $(A, ,)$, a state $I \xrightarrow{a} A$ is called a *phase* when:



(5.34)

Its *(right) phase shift* is the following morphism $A \to A$:



(5.35)

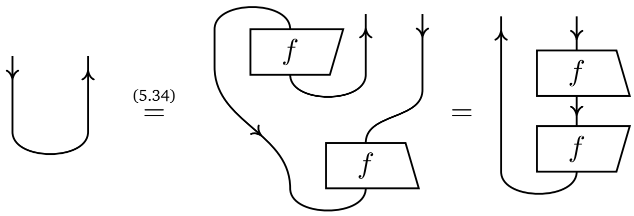
Example 5.45. For the classical structure copying an orthonormal basis $\{e_i\}$ in **FHilb**, a vector $a = a_1 e_1 + \cdots + a_n e_n$ is a phase precisely when each scalar a_i lies on the unit circle: $|a_i|^2 = 1$.

In any monoidal category, the unit of a Frobenius structure is always a phase. Also, a phase of the tensor unit (which is a Frobenius structure by Exercise 5.7.1) is a scalar $I \xrightarrow{s} I$ satisfying $s^\dagger \bullet s = \mathrm{id}_I$.

The following lemma gives more examples.

Lemma 5.46. *In a dagger pivotal category, the phases of a pair of pants structure* $(A^* \otimes A, \ldots)$ *are exactly the names of unitary operators* $A \to A$.

Proof. The name of an operator $A \xrightarrow{f} A$ is a phase when:



But using the snake equations (3.4), we see that this is equivalent to $f \circ f^\dagger = \mathrm{id}_A$. The other similar equation defining phases comes down to $f^\dagger \circ f = \mathrm{id}_A$. □

Example 5.47 (Phases in **FHilb**)**.** The set of phases of the Frobenius structure $\mathbb{M}_n$ in **FHilb** is the set $U(n)$ of n-by-n unitary matrices. Hence the phases of the Frobenius structure $\mathbb{M}_{k_1} \oplus \cdots \oplus \mathbb{M}_{k_n}$ range over $U(k_1) \times \cdots \times U(k_n)$.

Now consider the special case of a classical structure on $\mathbb{C}^n$ that copies an orthonormal basis $\{e_1, \ldots, e_n\}$. The phases are elements of $U(1) \times \cdots \times U(1)$; that is, phases a are vectors of the form $e^{i\phi_1} e_1 + \cdots + e^{i\phi_n} e_n$ for real numbers $\phi_1, \ldots, \phi_n$. The accompanying phase shift $\mathbb{C}^n \to \mathbb{C}^n$ is the unitary matrix

$$\begin{pmatrix} e^{i\phi_1} & 0 & \cdots & 0 \\ 0 & e^{i\phi_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & e^{i\phi_n} \end{pmatrix}.$$

Example 5.48 (Phases in **Rel**)**.** The phases of a Frobenius structure in **Rel** induced by a group G are elements of that group G itself.

Proof. For a subset $a \subseteq G$, the equation (5.34) defining phases reads

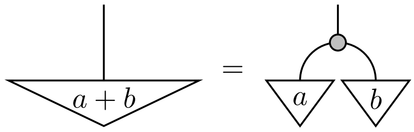
$$\{g^{-1}h \mid g, h \in a\} = \{1_G\} = \{hg^{-1} \mid g, h \in a\}.$$

So if $g \in G$, then $a = \{g\}$ is a phase. But if a contains two distinct elements $g \neq h$ of G, then it cannot be a phase. Similarly, $a = \emptyset$ is not a phase. Hence a is a phase precisely when it is a singleton $\{g\}$. □

5.5.1 Phase groups

The phases in all of the previous examples can be composed: unitary matrices under matrix multiplication, group elements under group multiplication. In general, phase shifts can be composed, and hence we expect phases to form a monoid. The following proposition shows that they in fact always form a group.

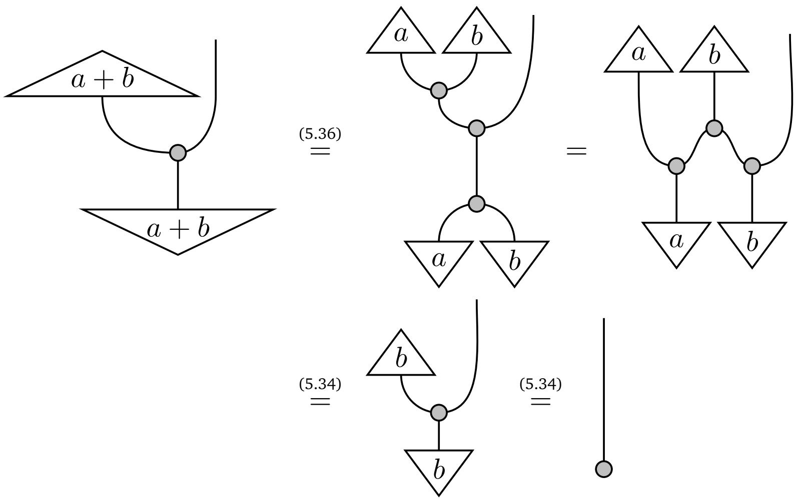
Proposition 5.49 (Phase group)**.** *In a monoidal dagger category, given a dagger Frobenius structure* $(A, ,)$*, its phases form a group with unit under the following addition:*



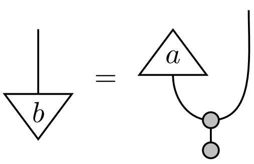
(5.36)

Equivalently, the phase shifts form a group under composition. In a braided monoidal dagger category, the phases of a classical structure form an abelian group.

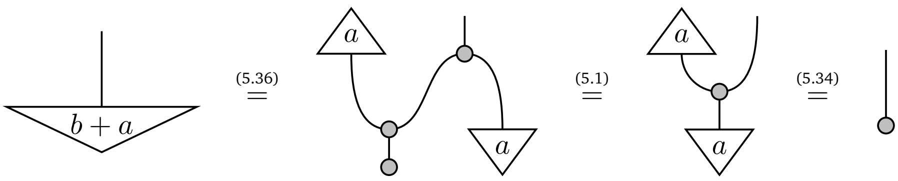
Proof. First we show that (5.36) is again a well-defined phase:



The second equality follows from the noncommutative Spider Theorem 5.21. As the other equation of (5.34) follows similarly, the set of phases form a monoid by associativity (4.4). Fix a phase a, and define b as follows:

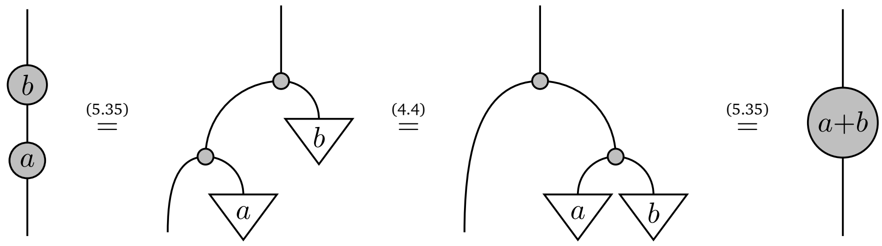


Then b is a left-inverse of a:



The reflection of b similarly gives a right-inverse c. But then actually $b = b + 0 = b + (a + c) = (b + a) + c = 0 + c = c$, so a has a unique (two-sided) inverse $-a = b = c$ making the phase monoid into a group. (See also Exercise 4.4.2.)

Notice that (5.36) corresponds to composition when we turn phases into phase shifts:



Clearly this group is abelian when the Frobenius structure is commutative. □

The group of the previous proposition is called the *phase group*.

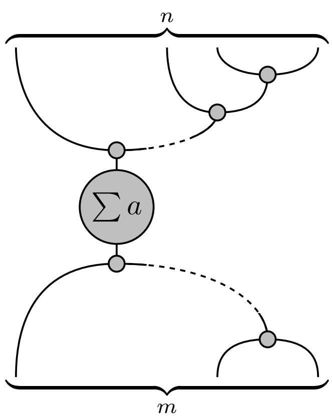
Example 5.50. Here are examples of phase groups for some of our standard dagger Frobenius structures:

- The group operation on the phases of the pair of pants Frobenius structure of Lemma 5.46, which are names of unitary morphisms $A \xrightarrow{f} A$, is simply taking the name of composition of operators.
- The group operation on the phases $U(k_1) \times \cdots \times U(k_n)$ of a Frobenius structure $\mathbb{M}_{k_1} \oplus \cdots \oplus \mathbb{M}_{k_n}$ in **FHilb** of Example 5.47 is simply entrywise multiplication. In particular, the group operation on a classical structure is multiplication of diagonal matrices.
- The group operation on the phases G of a Frobenius structure in $\mathbf{Rel}$ induced by a group G as in Example 5.48 is by construction (5.36) the multiplication of G itself. Hence the phase group of the Frobenius structure G in $\mathbf{Rel}$ is G itself. (See also Exercise 5.7.4 for the phase group of a groupoid.)

5.5.2 Phased normal forms

The next theorem generalizes the spider theorem to take phases into account, which can be done as long as the Frobenius structure is a classical structure.

Corollary 5.51 (Phased spider theorem)**.** *In a symmetric monoidal dagger category, for a classical structure* $(A, \,, \,)$*, any connected morphism* $A^{\otimes m} \to A^{\otimes n}$ *built out of finitely many* $\,, \,, \mathrm{id}, \,$ *and phases using* $\circ$*,* $\otimes$*, and* $\dagger$*, is equal to the following, where* a *ranges over all phases of the diagram:*



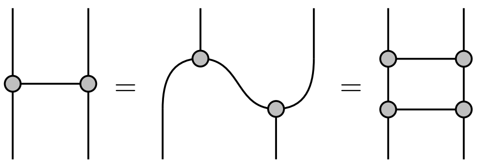
(5.37)

Proof. First use symmetries to ensure all the phases dangle at the bottom right of the diagram. Next apply Theorem 5.22. By definition (5.36) of the phase group, the phases on the bottom right, together with the multiplications above them, reduce to a single phase $\sum a$ on the bottom right. Finally, another application of Theorem 5.22 turns the diagram into the desired form (5.37). $\square$

5.5.3 State transfer

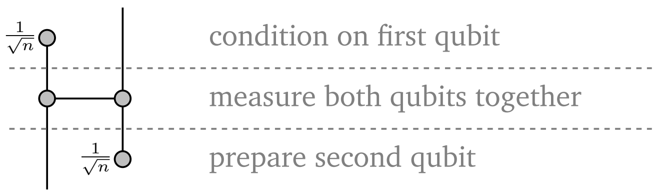
We're now going to apply our knowledge of classical structures to analyze the quantum state transfer protocol, which transfers the quantum state of an n-dimensional Hilbert space H from one system to another. Interest in state transfer lies in the fact that all the procedures involved are state preparations or measurements; no unitary dynamics takes place. However, unlike quantum teleportation, the state transfer protocol is not always successful, with a success probability of $1/\dim(H)^2$.

By virtue of the spider theorem, we can be quite free with the graphical notation when building diagrams from the components of a classical structure, even allowing wires to enter nodes horizontally. For example, the following morphisms all define the same projection $H \otimes H \to H \otimes H$:



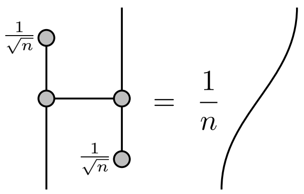
(5.38)

Define the procedure for state transfer graphically by the following diagram:



(5.39)

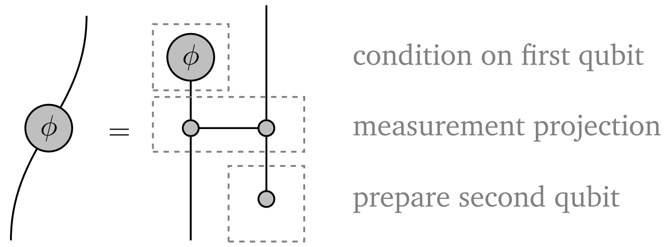
The spider theorem easily simplifies this diagram:



(5.40)

Hence this protocol indeed achieves the goal of transferring the first qubit to the second. To appreciate the power of the graphical calculus, one only needs to compute the same protocol using matrices.

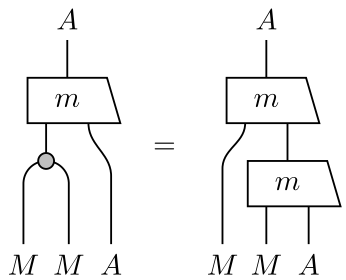
By using the phased spider theorem, Corollary 5.51, we can also easily achieve the extra challenge of applying a phase gate in the process of transferring the state, by the following adaptation:



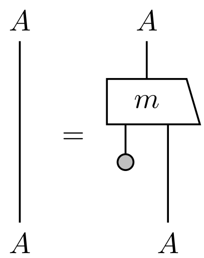
5.6 Modules

This section gives mathematical structure to the notion of quantum measurement using classical structures. The idea is as follows. As we saw in Section 5.3.1, operators $A \to A$ correspond to states of pair of pants structures $A^* \otimes A$. In particular, observables, as modeled by self-adjoint operators $A \to A$, correspond to states of $A^* \otimes A$. In fact, a monoid A always embeds into $A^* \otimes A$ by Proposition 4.13; we can think of this as a set of observables indexed by A. If the system we care about is modeled by A, so that its observables live in $A^* \otimes A$, it makes sense to consider observables indexed by any monoid M as a map $M \to A^* \otimes A$. Via map-state duality, this comes down to the theory of *modules*.

Definition 5.52 (Module)**.** In a monoidal category, given a monoid $(M, \ , \ )$, a *module* is an object A equipped with a morphism $M \otimes A \xrightarrow{m} A$, called the *action*, satisfying the following equations:



(5.41)



(5.42)

More precisely this is a *left module*, with *right modules* similarly defined with action $A \otimes M \to A$. We will mostly consider left modules in this book, and so we'll just refer to them as modules.

Think of a module as follows: the morphism $M \otimes A \xrightarrow{m} A$ is a way to 'update' A, based on the 'instructions' in M. This perspective explains the module equations:

equation (5.41) says "if you combine the instructions and then update, that's the same as updating twice", and equation (5.42) says "if you update with trivial instructions, that's the same as not updating at all".

The following are important instances of modules.

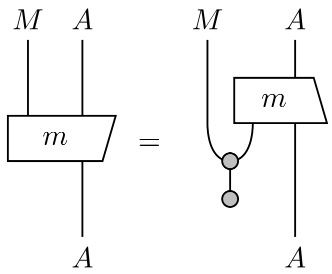
Definition 5.53 (Free module)**.** In a monoidal category, given a monoid (M, m, u), a *free module* is an object $M \otimes A$, equipped with the action $M \otimes M \otimes A \xrightarrow{m \otimes \mathrm{id}_A} M \otimes A$.

In particular, this last definition makes it clear that monoids can act on themselves as a module, by choosing $A = I$.

Example 5.54. A representation of a finite group G in $\mathbb{C}^n$ is a group homomorphism from G to the group of invertible n-by-n matrices. The group G induces the group algebra A in **FHilb** as in Example 5.2. Representations f of G correspond exactly to modules $A \otimes \mathbb{C}^n \xrightarrow{m} \mathbb{C}^n$ given by $g \otimes a \mapsto f(g)(a)$. The action of G on itself is the regular representation.

In the presence of a dagger, there is an additional compatibility to consider.

Definition 5.55 (Dagger module)**.** In a monoidal dagger category, a *dagger module* for a dagger Frobenius structure $(M, \tinymult, \tinyunit)$ is a module action $M \otimes A \xrightarrow{m} A$ satisfying the following additional equation:



(5.43)

For group algebras, this captures the notion of unitary representation.

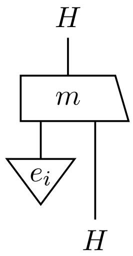
Example 5.56. A unitary representation of a group G is a group homomorphism $G \xrightarrow{f} U(n)$. These correspond precisely to the dagger modules of the group algebra A of G: if we put the effect $A \xrightarrow{g^\dagger} I$ for $g \in G$ on the top left in equation (5.43), the left-hand side becomes $f(g)^\dagger$, whereas the right-hand side becomes $f(g^{-1}) = f(g)^{-1}$; but this means precisely that $f(g) \in \mathbb{M}_n$ is unitary.

5.6.1 Measurement

In **Hilb**, dagger modules are important because they correspond exactly to *projection-valued measures* (PVMs, see Definition 0.61). This is a powerful abstraction, since we can now prove theorems about PVMs using graphical diagrams built from the module structure, rather than having to reason algebraically about the individual projections in the PVM. We can also generalize PVMs to other categorical settings, where the conventional approach of Definition 0.61 may not extend in any obvious way.

Lemma 5.57. *In* **Hilb***, a dagger module for a classical structure* $(M, \tinymult, \tinyunit)$ *acting on* H *corresponds to a PVM on* H *with* $\dim(M)$ *outcomes.*

Proof. The module $M \otimes H \xrightarrow{m} H$ is determined by the following morphisms p_i, for copyable states $e_i \in M$:



(5.44)

First, by associativity (5.41) and copyability (4.17) of e_i, we see that $p_i \circ p_i = p_i$ and $p_i \circ p_j = 0$ for $i \neq j$. Second, the dagger module axiom (5.43) gives $p_i = p_i^\dagger$. Third, since $\phi = \sum_i e_i$, also $\sum_i p_i = \mathrm{id}_H$. Hence $\{p_i\}$ form a PVM. Finally, it is clear that this argument works in reverse: if $\{p_I\}$ is a PVM on H, we get a module action $M \otimes H \to H$ by asserting that each composite of the form (5.44) corresponds to one p_i. $\square$

Example 5.58. In **Hilb**, for a classical structure $(M, \curlywedge, \phi)$, the action of M on itself gives a PVM, which describes measuring M in the basis of copyable states of the classical structure. Such a PVM will always be nondegenerate.

For a classical structure $(M, \curlywedge, \phi)$, given a dagger module $M \otimes A \to A$, we may think of its adjoint $A \to M \otimes A$ as an abstraction of the measurement process itself: it starts with only the system A to be measured, and finishes with some classical information stored in M, along with the (possibly altered) system A.

We can consider such measurements in other categories, such as $\mathbf{Rel}$. In that case, a measurement $A \to \mathbf{G} \times A$ for an abelian groupoid $\mathbf{G}$ can be interpreted as in the following lemma: measuring A in state $a \in A$ results in outcome g and final state $g^{-1}a$. Recall that $\mathbf{Rel}(A, A)$ may be regarded as a one-object dagger category, namely the full subcategory of $\mathbf{Rel}$ containing only the object A. Similarly, a groupoid has a dagger given by inverses.

Lemma 5.59. *Consider a dagger Frobenius structure in* $\mathbf{Rel}$ *induced by a groupoid* $\mathbf{G}$*. A dagger module acting on a set A corresponds to a functor $R\colon \mathbf{G} \to \mathbf{Rel}(A, A)$ that preserves daggers. In fact $R(g)$ is a partial bijection.*

Such functors are called $\mathbf{G}$-*actions*, sometimes written as $a \mapsto ga$ instead of $R(g)$.

Proof. Conditions (5.41), (5.42), and (5.43) correspond to the following:

$$(g \circ h, a) \sim c \iff \exists b\colon (h, a) \sim b, (g, b) \sim c \tag{5.45}$$

$$(\mathrm{id}_x, a) \sim b \iff a = b \tag{5.46}$$

$$(g, a) \sim b \iff (g^{-1}, b) \sim a \tag{5.47}$$

For a morphism g in $\mathbf{G}$, define $R(g) = \{(a, b) \in A \times A \mid (g, a) \sim b\}$. The above conditions then become the following:

$$R(g \circ h) = R(g) \circ R(h)$$
$$R(\mathrm{id}_x) = \mathrm{id}_A$$
$$R(g^\dagger) = R(g)^\dagger$$

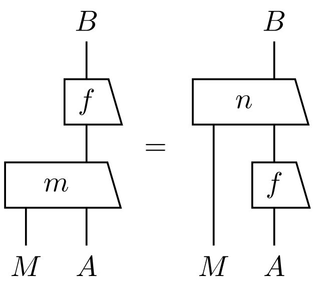
This means precisely that R is a functor $\mathbf{G} \to \mathbf{Rel}(A, A)$ that preserves daggers.

That $R(g)$ is a partial bijection means: if $a \sim b$ and $a \sim b'$ then $b = b'$, and similarly, if $a \sim b$ and $a' \sim b$, then $a = a'$. To see this, apply (5.47) to $a \sim b$ and $a \sim b'$ to get $(g^{-1}, b) \sim a$. Next $(\mathrm{id}_{\mathrm{cod}(g)}, b) \sim b'$ by (5.45). But then $b = b'$ by (5.46). The second statement now follows from (5.47). $\square$

5.6.2 Module morphisms

Given a pair of modules for the same monoid, the maps between them are given by the *module homomorphisms*.

Definition 5.60 (Module homomorphism). In a monoidal category, given a monoid $(M, \tinymult, \tinyunit)$ and module actions $M \otimes A \xrightarrow{m} A$ and $M \otimes B \xrightarrow{n} B$, a *module homomorphism* $m \xrightarrow{f} n$ is a morphism $A \xrightarrow{f} B$ satisfying the following condition:



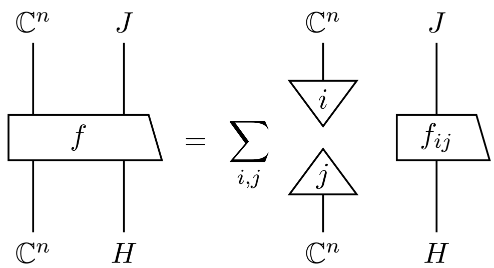
(5.48)

Comodule homomorphisms are defined by reversing all morphisms.

Module homomorphisms give an abstract description of controlled operations (see Definition 0.64). As for PVMs, the advantage of this characterization is that it is entirely geometrical: rather than making reference to the individual unitary operations, one need only work directly with a single structure, the module homomorphism.

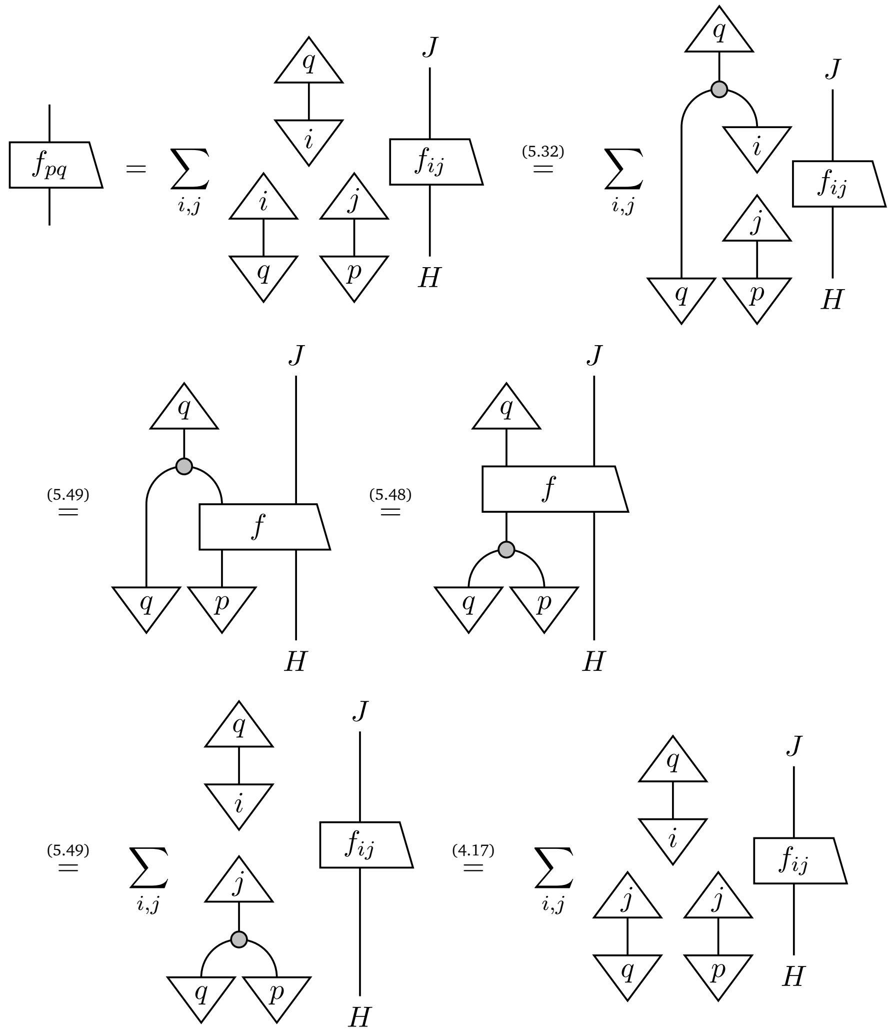
Lemma 5.61. *In* **Hilb***, for a classical structure* $(\mathbb{C}^n, \tinymult, \tinyunit)$*, unitary module morphisms between free modules correspond exactly to controlled operations.*

Proof. Consider a homomorphism $\mathbb{C}^n \otimes H \xrightarrow{f} \mathbb{C}^n \otimes J$ between free modules. We can write any such map as follows, using the canonical orthonormal basis associated to the classical structure, where $f_{ij} : H \to J$ is an indexed family of linear maps, and where each index of the sum goes from 1 to n:



(5.49)

We first show that $f_{pq} = \delta_{p,q} \cdot f_{pq}$:



$$= \sum_{i,j} \delta_{q,j}\delta_{p,j}\delta_{i,q} f_{ij} \;=\; \delta_{p,q} f_{pq}$$

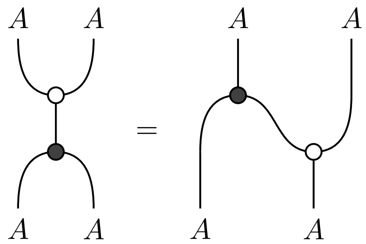
It follows that $i \neq j \Rightarrow f_{ij} = 0$. Using this to simplify the decomposition of f, it is simple to show that f is unitary exactly when f_{ii} is unitary for all i. $\square$

The module homomorphism condition (5.48) also gives another characterization of Frobenius structures.

Lemma 5.62 (Frobenius structure via modules)**.** *In a monoidal category, a monoid and comonoid on the same object* $(A, \,, \,, \,, \,)$ *form a Frobenius structure if and only if* *is a left-module homomorphism going from the action of* A *on itself to the action* $\otimes \mathrm{id}_A$*, and a right-module homomorphism going from the action of* A *on itself to the action* $\mathrm{id}_A \otimes$.

Proof. Employing Definition 5.60 of a left-module homomorphism for $m =$, $n =$

$\otimes \mathrm{id}_A$ and $f =$ gives the following:

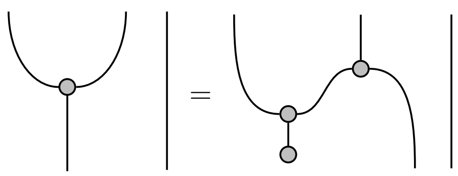


That is also a right-module homomorphism corresponds to the other equation in Lemma 5.4. Thus, together they correspond to the Frobenius law. □

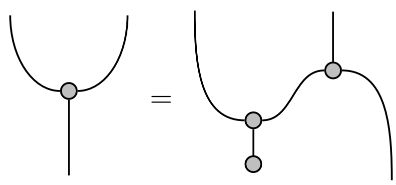
According to the way of the dagger, there is also a way to characterize dagger Frobenius structures in terms of dagger modules.

Lemma 5.63. *A monoid* $(A, ,)$ *in a dagger monoidal category is a dagger Frobenius structure if and only if* $A \otimes A$ *is a dagger module under both the actions* $\otimes \mathrm{id}_A$ *and* $\mathrm{id}_A \otimes$.

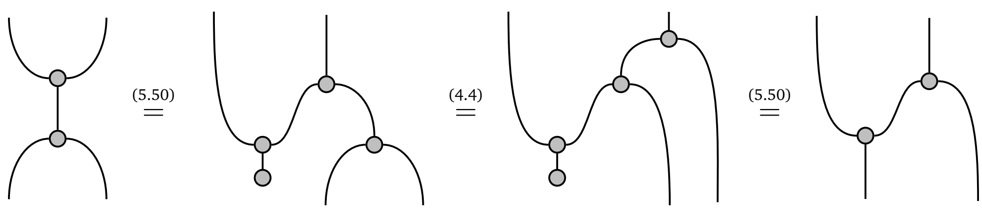
Proof. First consider the action $\otimes \mathrm{id}_A$. Writing out the dagger module condition (5.43) gives:



Postcomposing with $\mathrm{id}_A \otimes$ and precomposing with $\mathrm{id}_A \otimes$ shows that this is equivalent to:


(5.50)

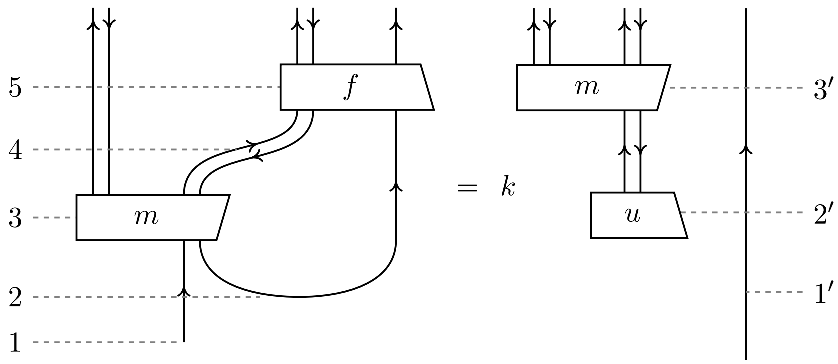
It follows that:



The other action $\otimes \mathrm{id}_A$ similarly implies the other half of the extended Frobenius law (5.4). Conversely, the Frobenius law and unitality (4.5) immediately imply (5.50). □

5.6.3 Pure quantum teleportation

We now use the results above to give a new characterization of quantum teleportation (see Definition 0.74). In contrast to Section 3.2, this time we will avoid any indices or direct sums. The teleportation procedure involves a nondegenerate measurement on a joint system $A \otimes A^*$. According to Example 5.58, we model this using a classical structure on $A \otimes A^*$, which acts on itself. The entire quantum teleportation procedure is now described as follows, where f is a unitary comodule homomorphism, and where k is some invertible scalar factor:

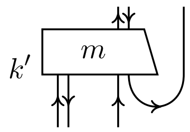


(5.51)

Here, horizontal dotted lines label the parts of the diagrams. The labels for the left-hand side matches individual steps of Definition 0.74; the morphism f is a controlled operation (that is, a unitary comodule homomorphism) describing Bob's correction. On the right-hand side, $1'$ indicates that the state of the initial qubit is perfectly preserved, $2'$ creates a uniform superposition over all the possible measurement states, and $3'$ measures this, so that at the end of the protocol, Alice and Bob hold the same classical information. The scalar factor k allows us to correct for the fact that some components of these diagrams may not give exactly the desired operation, but only something proportional to it.

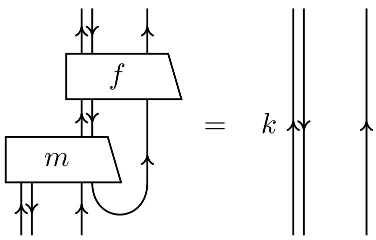
Given a classical structure on $(A \otimes A^*, m, u)$, one can ask whether a module homomorphism f can be found yielding a quantum teleportation procedure. The following theorem gives a precise answer to this question.

Proposition 5.64. *In a dagger pivotal category, a dagger Frobenius structure* $(A \otimes A^*, m, u)$ *gives a solution to the quantum teleportation equation* (5.51) *if and only if there is some invertible scalar* k' *making the following composite unitary:*



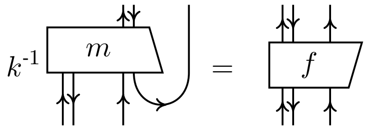
(5.52)

Proof. To begin, assume that $(A \otimes A^*, m, u)$ satisfies equation (5.51) along with some unitary comodule homomorphism f. Our goal is to demonstrate that expression (5.52) is unitary, for some invertible scalar k. First, use Theorem 5.15 to bend down the top-left pair of wires on both sides of equation (5.51):



(5.53)

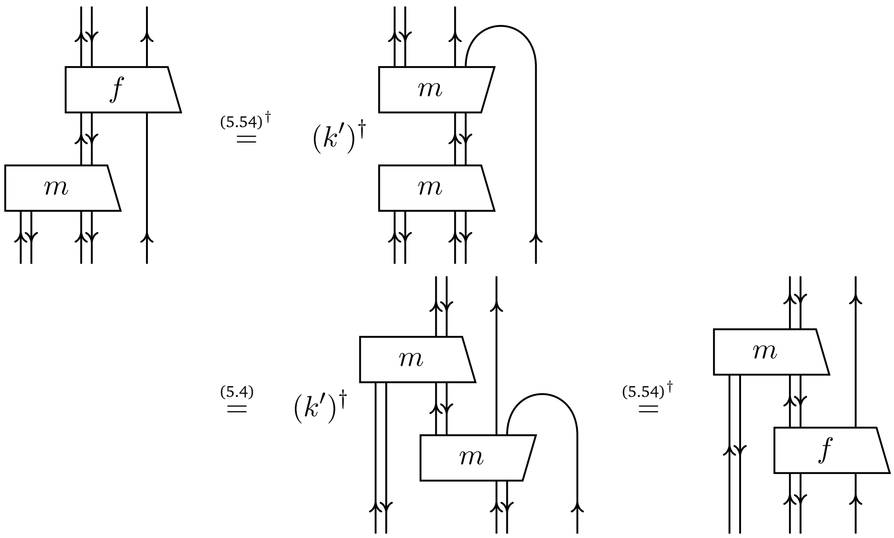
Postcomposing both sides with $f^\dagger$, and multiplying with k^{-1}, then yields an explicit expression for $f^\dagger$ in terms of m:



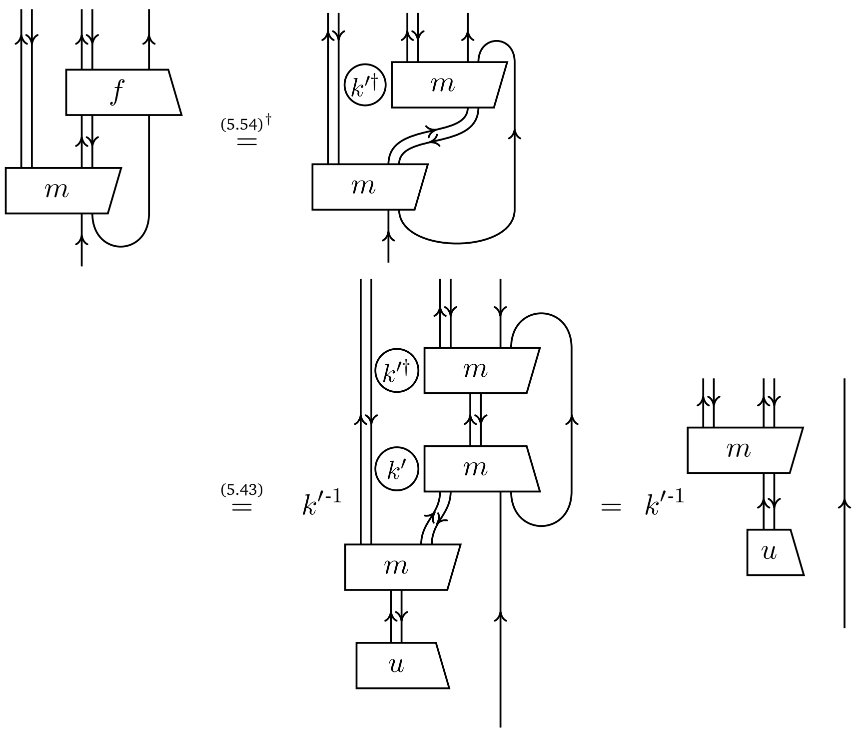
(5.54)

But since f is unitary, we see that (5.52) is unitary up to a scalar factor $k' = k^{-1}$.

For the converse, suppose that a classical structure $(A \otimes A^*, m, u)$ makes (5.52) unitary for some invertible scalar factor k. Define a morphism f as the adjoint of (5.52), which will by definition be unitary. To see that f is a comodule homomorphism, evaluate equation (5.48) as follows:



All that remains is to show that it correctly implements the main quantum teleportation equation (5.51). To verify this, plug in the definition of f:



Equation (5.51) is therefore validated by choosing $k = k'^{-1}$. In the final step here we use the fact that (5.52) is unitary. □

5.7 Exercises

Exercise 5.7.1. Recall that in a braided monoidal category, the tensor product of monoids is again a monoid (see Lemma 4.8).

(a) Show that, in any monoidal category, the tensor unit is a Frobenius structure (see also Example 4.4).

(b) Show that, in a braided monoidal category, the tensor product of Frobenius structures is again a Frobenius structure.

(c) Show that, in a symmetric monoidal category, the tensor product of symmetric Frobenius structures is again a symmetric Frobenius structure.

(d) Show that, in a symmetric monoidal dagger category, the tensor product of classical structures is again a classical structure.

Exercise 5.7.2. This exercise is about the interdependencies of the defining properties of Frobenius structures in a braided monoidal dagger category. Recall the Frobenius law (5.1).

(a) Show that for any maps $A \xrightarrow{d} A \otimes A$ and $A \otimes A \xrightarrow{m} A$, speciality ($m \circ d = \mathrm{id}$) and equation (5.4) together imply associativity for m.

(b) Suppose $A \xrightarrow{d} A \otimes A$ and $A \otimes A \xrightarrow{m} A$ satisfy equation (5.4), speciality, and commutativity (4.6). Given a dual object $A \dashv A^*$, construct a map $I \xrightarrow{u} A$ such that unitality (4.5) holds.

Exercise 5.7.3. Recall that a set $\{x_0, \ldots, x_n\}$ of vectors in a vector space is *linearly independent* when $\sum_{i=0}^{n} z_i x_i = 0$ for $z_i \in \mathbb{C}$ implies $z_0 = \ldots = z_n = 0$.Show that the nonzero copyable states of a comonoid in **FHilb** are linearly independent. (Hint: consider a minimal linearly dependent set.)

Exercise 5.7.4. This exercise is about the phase group of a Frobenius structure in **Rel** induced by a groupoid **G**.

(a) Show that a phase of **G** corresponds to a subset of the arrows of **G** that contains exactly one arrow out of each object and exactly one arrow into each object.

(b) A *cycle* in a category is a series of morphisms $A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} A_3 \cdots A_n \xrightarrow{f_n} A_1$. For finite **G**, show that a phase corresponds to a union of cycles that cover all objects of **G**. Find a phase on the indiscrete category on $\mathbb{Z}$ that is not a union of cycles.

(c) Show that for skeletal groupoids **G**, the phase group is **G** itself, regarded as a group: $\prod_{x \in \mathrm{Ob}(\mathbf{G})} \mathbf{G}(x, x)$. Conclude that this holds in particular for classical structures.

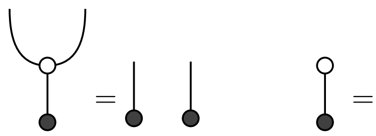
(d) Show that taking the phase group is a monoidal functor from the category of groupoids and functors that are bijective on objects, to the category of groups and group homomorphisms.

Exercise 5.7.5. Show that, if $F\colon \mathbf{C} \to \mathbf{D}$ is a monoidal functor, and (A, m, u, d, e) is a Frobenius structure in **C**, then $(F(A), F(m) \circ (F_2)_{A,A}, F(u) \circ F_0, (F_2)^{-1}_{A,A} \circ F(d), F_0^{-1} \circ$

$F(e))$ is a Frobenius structure in $\mathbf{D}$. (See also Theorem 3.14 and Exercise 4.4.11.)

Exercise 5.7.6. Let $A \dashv A^*$ be dagger dual objects in a symmetric monoidal dagger category. Show that if the pair of pants Frobenius structure $(A, ,)$ is commutative, then $\dim(A)^3 = \dim(A)$.

Exercise 5.7.7. Let $(A, , , ,)$ be a symmetric Frobenius structure in symmetric monoidal category. Suppose it is *disconnected*, in the sense that:



Define $\dim^\beta(A) = \mathrm{Tr}^\beta(\mathrm{id}_A)$, where Tr^β is defined as in Exercise 3.5.7.

(a) Prove that $\dim^\beta(A) = 1$.

(b) Which objects in $\mathbf{Hilb}$ can carry disconnected Frobenius structures?

(c) Which objects in $\mathbf{Rel}$ can carry disconnected Frobenius structures?

(d) Which objects in $\mathbf{Rel}$ can carry disconnected special dagger Frobenius structures?

Exercise 5.7.8. Prove that the biproduct of dagger Frobenius structures in a monoidal dagger category with dagger biproducts, with multiplication as in (5.25), is again a dagger Frobenius structure.

Exercise 5.7.9. Let R be as defined in equation (4.13), and let i be as defined in equation 5.21. Show that the equivalent conditions of Theorem 5.28 are equivalent to the following third condition:

$$R_* \circ i = R.$$

Recall from Example 5.27 that the identity is an involution on $A^* \otimes A$, and so this third condition says that the embedding preserves the canonical maps, $R_* \circ i_A = i_{A^* \otimes A} \circ R$, as in Definition 5.25.

Notes and further reading

The Frobenius law (5.1) is named after F. Georg Frobenius, who first studied the requirement that $A \simeq A^*$ as right A-modules for a ring A in the context of group representations in 1903 [64]. They were studied further by Brauer and Nesbitt in 1937 [29], and great advances were made by Nakayama in 1941, who coined the name [111]. The formulation with multiplication and comultiplication we use is due to Lawvere in 1967 [99], and was rediscovered by Quinn in 1995 [121] and Abrams in 1997 [1]. Carboni and Walters used this formulation to axiomatize (bi)categories of relations in 1987 [31]. Dijkgraaf realized in 1989 that the category of commutative Frobenius structures is equivalent to that of 2-dimensional topological quantum field theories [55]. For a comprehensive treatment, see the monograph by Kock [96].

The commutative spider theorem 5.21 was proved using the homotopy theory of 2-dimensional surfaces with boundary by Abrams [1]. A category-theoretic proof was given by Lack in 2004 [98].

Coecke and Pavlović first realized in 2007 that commutative Frobenius structures could be used to model the flow of classical information [47]. That paper also describes quantum measurement in terms of modules for the first time. Theorem 5.36, that classical structures in **FHilb** correspond to orthonormal bases, was proved in 2009 by Coecke, Pavlović and Vicary [48]. In 2011, Abramsky and Heunen adapted Definition 5.10 to generalize this correspondence to infinite dimensions in **Hilb** [6], and Vicary generalized it to the noncommutative case [137].

Operator algebra is a venerable field of study in functional analysis, with breakthroughs by Gelfand in 1939 and von Neumann in 1936 [66, 141]. For a first introduction see [52, 60]. It usually concerns C*-algebras, which have a very rich theory. We haven't mentioned C*-algebras at all because they disregard the Hilbert space structure of the carrier space. True to the way of the dagger, this chapter considered H*-algebras instead. These were defined and studied by Ambrose in 1945 [7]. Terminology warning: the involution of a C*-algebra or H*-algebra is typically denoted $*$, which matches our $\dagger$ rather than our $*$.

Theorem 5.41, that classical structures in **Rel** are groupoids, was proven by Pavlović in 2009 [116], and generalized to the noncommutative case by Heunen, Contreras and Cattaneo in 2012 [73].

The involutive generalization of Cayley's theorem in Theorem 5.28 was proven in the commutative case by Pavlović in 2010 [117], and in the general case by Heunen and Karvonen in 2015 [74].

The phase group was made explicit by Coecke and Duncan in 2008 [37], and later Edwards in 2009 [59, 39], in the commutative case. The state transfer protocol is important in efficient measurement-based quantum computation. It is due to Perdrix in 2005 [119].

Chapter 6

Complementarity

This chapter studies what happens when we have *two* interacting Frobenius structures. Specifically, we are interested in when they are "maximally incompatible", or *complementary*, and give a definition that makes sense in arbitrary monoidal dagger categories in Section 6.1. We will see that it comes down to the standard notion of mutually unbiased bases from quantum information theory in the category of Hilbert spaces, and classify the complementary groupoids in the category of sets and relations. We will also characterize complementarity in terms of a canonical morphism being unitary. This is exemplified by discussing the Deutsch-Jozsa algorithm in Section 6.2, where the canonical morphism plays the role of an oracle. Section 6.3 links complementarity to the subject of Hopf algebra. It turns out that this well-studied notion gives rise to a stronger form of complementarity that we characterize. We then turn to quantum computation: Section 6.4 discusses how many-qubit gates can be modeled in categorical quantum mechanics using only complementary Frobenius structures, such as controlled negation, controlled phase gates, and arbitrary single qubit gates. Finally, Section 6.5 discusses the ZX calculus, a sound and complete way to handle quantum computations using only equations in the graphical calculus.

We have been using colours to distinguish between monoid multiplication and comonoid comultiplication. We have also been indicating that one is the dagger of the other by abbreviating = to just a single colour. From this chapter on, we will deal with *two* Frobenius structures, each carrying both a multiplication and a comultiplication. When this is the case we will specialize to dagger Frobenius structures, so we can distinguish them. By drawing the operations of a single Frobenius structure in a single colour, we can speak about two dagger Frobenius structures $(A, \ , \ , \ , \ )$ and $(A, \ , \ , \ , \ )$, in a way perfectly consistent with our conventions. Nevertheless, many results hold more generally without daggers.

6.1 Complementary structures

Consider two measurements of a qubit: one in the basis $\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\}$, and one in the basis $\{\begin{pmatrix}1\\1\end{pmatrix}/\sqrt{2}, \begin{pmatrix}1\\-1\end{pmatrix}/\sqrt{2}\}$. If we measure in the first basis, the qubit will collapse to either $\begin{pmatrix}1\\0\end{pmatrix}$ or $\begin{pmatrix}0\\1\end{pmatrix}$; a repeated measurement in the first basis is guaranteed to repeat the same outcome. However, a measurement in the second basis could yield either outcome with equal probability, yielding no information at all. Two bases with this property are said to be unbiased; this is a simple form of Heisenberg's uncertainty principle.

Definition 6.1 (Complementary bases)**.** For a finite-dimensional Hilbert space H, two orthogonal bases $\{a_i\}$ and $\{b_j\}$ are *complementary*, or *unbiased*, when there is some constant $s \in \mathbb{C}$ such that the following holds for all i, j:

$$\langle a_i | b_j \rangle \langle b_j | a_i \rangle = s \tag{6.1}$$

In other words, the inner products have constant absolute value.

We can prove the following simple lemma about complementary bases.

Lemma 6.2. *For a pair of complementary bases $\{a_i\}$ and $\{b_j\}$, within each basis, the elements have constant norm.*

Proof. Calculate:

$$\langle b_j | b_j \rangle = \sum_i \frac{\langle b_j | a_i \rangle \langle a_i | b_j \rangle}{\langle a_i | a_i \rangle} \stackrel{(6.1)}{=} \sum_i \frac{s}{\langle a_i | a_i \rangle} \tag{6.2}$$

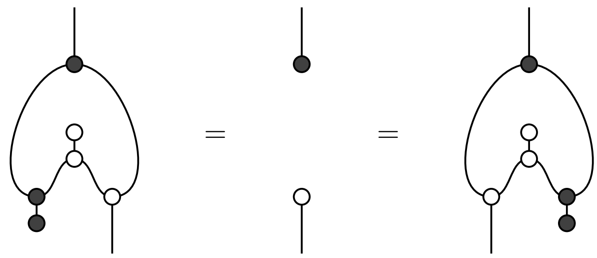
For the first equality, insert the identity as a sum over the complete family of projections $|a_i\rangle\langle a_i| / \langle a_i | a_i \rangle$. The final expression is independent of j as required. A similar argument holds for the $\{a_i\}$ basis. □

Combining expressions (6.1) and (6.2) shows that s can be cancelled, leading to the following general equation for all i, j:

$$\langle a_i | b_j \rangle \langle b_j | a_i \rangle \dim(H) = \langle a_i | a_i \rangle \langle b_j | b_j \rangle \tag{6.3}$$

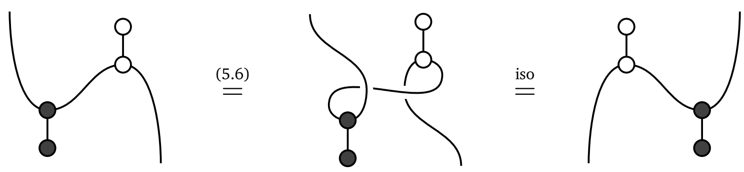
An orthogonal basis can be represented as a commutative dagger Frobenius structure by Theorem 5.36, so a natural goal is to characterize complementarity as an interaction law between two commutative dagger Frobenius structures. We achieve this with the following definition.

Definition 6.3 (Complementary Frobenius structures)**.** In a braided monoidal dagger category, two symmetric dagger Frobenius structures and on the same object are *complementary* when the following equations hold:



(6.4)

The roles of the black and white dots in the previous definition are not obviously interchangeable. However, since the Frobenius structures are symmetric, the following rearrangement is possible:



(6.5)

Using these equations and the dagger, we see that 'black is complementary to white' is equivalent to 'white is complementary to black'.

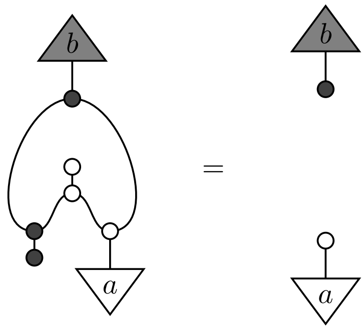
6.1.1 Examples

Let's first establish that Definition 6.3 indeed captures the correct notion in **FHilb**.

Proposition 6.4 (Complementarity in **FHilb**). *In* **FHilb***, the following are equivalent for two commutative dagger Frobenius structures on the same object:*

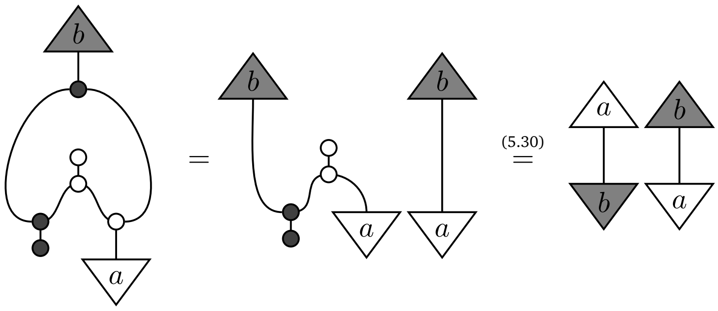
- *as Frobenius structures, they are complementary;*
- *as bases, they are complementary with constant $s = 1$.*

Proof. The complementarity equation (6.4) holds if and only if the following equation holds for all a in the white basis, and b in the black basis:



(6.6)

The left-hand side can be simplified as follows:



(6.7)

The right-hand side expands to 1, and so we recover equation (6.1). □

Example 6.5 (Pauli bases). Here are three bases of the Hilbert space $\mathbb{C}^2$:

$$
\begin{aligned}
X \text{ basis:} \quad & \left\{ \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} \right\} \\
Y \text{ basis:} \quad & \left\{ \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix} \right\} \\
Z \text{ basis:} \quad & \left\{ \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix} \right\}
\end{aligned}
$$

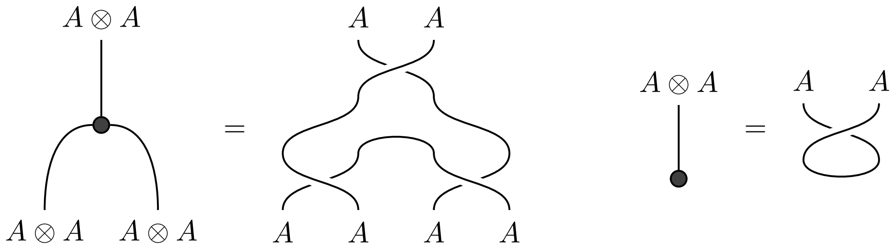
These are all mutually complementary. The terminology is explained by the fact that these bases consist of eigenvectors of the three Pauli matrices that measure spin in the X, Y and Z coordinates of a spin-$\frac{1}{2}$ particle in 3-dimensional space.

It is known that this is the largest family of complementary bases that can exist in $\mathbb{C}^2$, in the sense that it is not possible to find four bases for this Hilbert space which are all mutually complementary. Establishing the maximum possible number of mutually complementary bases in a Hilbert space of a given dimension is a difficult problem, which has not been solved in general for Hilbert spaces of dimensions which are not a prime power.

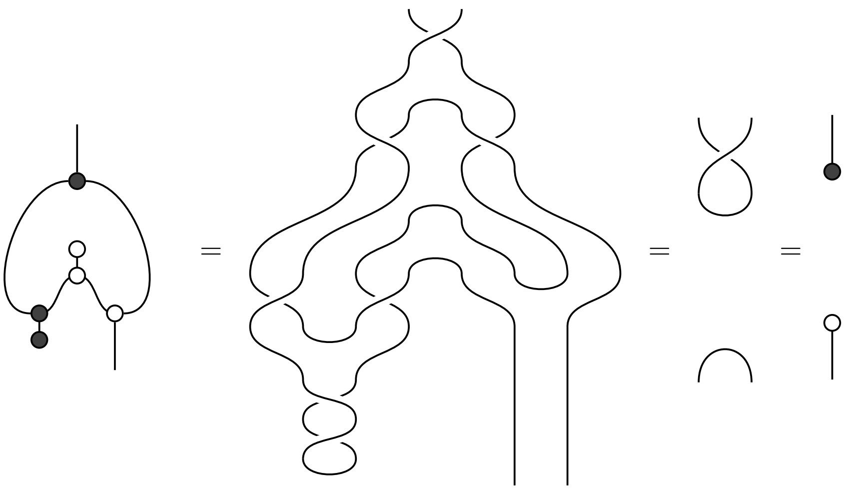
Here is a large stock of examples of complementary Frobenius structures.

Lemma 6.6 (Twisted knickers). *In a braided monoidal dagger category with a self-dual object A, the pair of pants structure from Lemma 5.9 is complementary to its transport across the braiding $\sigma_{A,A}$ as in Definition 5.17.*

Proof. Denote the pair of pants Frobenius structure from Lemma 5.9 by white dots, and its transport across the braiding by black dots:



Then a straightforward graphical calculation shows the following:



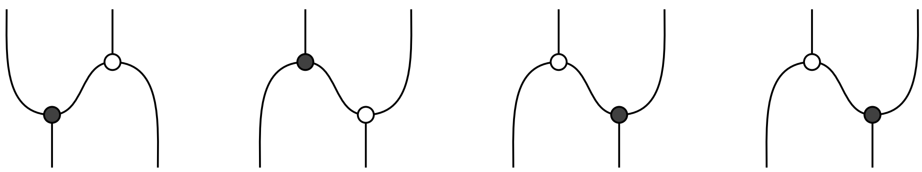
The other identity in (6.4) follows similarly. □

Combined with Theorem 5.15, the previous lemma says that any dagger Frobenius structure on A gives rise to a complementary pair of Frobenius structures on $A \otimes A$ in any braided monoidal dagger category.

6.1.2 Dagger complementarity

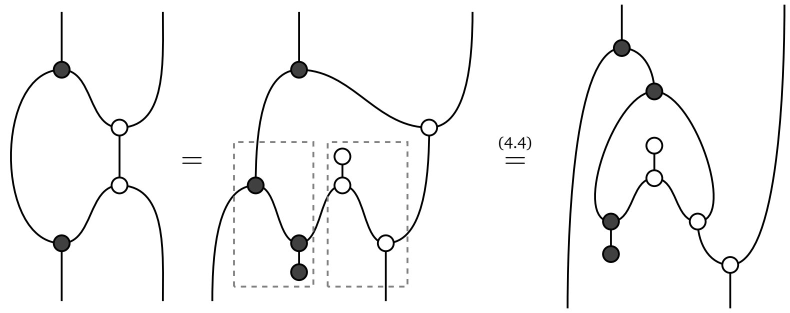
Complementarity is an equality of morphisms built from the (co)multiplication and (co)unit of a Frobenius structure. We can also characterize complementarity in terms of daggers, namely as some canonical morphism being unitary.

Proposition 6.7. *In a braided monoidal dagger category, two symmetric dagger Frobenius structures are complementary if and only if any, and hence all, of the following endomorphisms are unitary:*



(6.8)

Proof. Unitarity of the first endomorphism means that, in particular, composing the first two endomorphisms in the manner shown below results in the identity:



(6.9)

Here, the first equality follows from two applications of the noncommutative spider Theorem 5.21 to the dashed areas. Now, if complementarity (6.4) holds, then clearly (6.9) equals the identity. Conversely, if the right-hand side of (6.9) equals the identity, then composing with the white counit on the top right and the black unit on the bottom left gives back the left-hand equality of complementarity (6.4). Therefore the left identity in (6.4) holds if and only if (6.8) is an isometry. By a similar argument, composing the first two composites in (6.8) in the other order corresponds to the right-hand equality of complementarity (6.4).

It follows that unitarity of each of the first two composites (6.8) is equivalent to complementarity. A similar argument can be given for the second two composites. □

6.1.3 Complementary groupoids

Now we investigate what complementarity means in $\mathbf{Rel}$. It turns out to be a phenomenon similar to mutual unbiasedness. The construction in the following example is a lot like that of Lemma 6.6.

Example 6.8. Let G and H be nontrivial groups. Set $A = G \times H$. Let $\mathbf{G}$ be the groupoid with objects G and homsets $\mathbf{G}(g,g) = H$ and no morphisms between distinct objects, and let $\mathbf{H}$ be the groupoid with objects H and homsets $\mathbf{H}(h,h) = G$ and no morphisms between distinct objects. Then in a natural way, $\mathbf{G}$ and $\mathbf{H}$ have the same set A of morphisms, and they are complementary as Frobenius structures.

Proof. Consider the left-hand side of (6.4). It expands to

$$\{(a,b) \mid \exists x \in A \colon x \bullet a = x \circ b\},$$

where we write $\bullet$ for the composition in $\mathbf{G}$, and $\circ$ for the composition in $\mathbf{H}$. This set clearly contains the right-hand side of (6.4), which is

$$\{(\mathrm{id}_g, \mathrm{id}_h) \mid g \in \mathrm{Ob}(\mathbf{G}), h \in \mathrm{Ob}(\mathbf{H}))\}.$$

Remember that we cannot compose any two morphisms in a groupoid; they have to have matching domain and codomain. Suppose $x \bullet a = x \circ b$. Then the $\circ$-inverse of x is $\circ$-composable with $x \bullet a$. That is, $\mathrm{cod}_\circ(x) = \mathrm{cod}_\circ(x \bullet a)$. But by construction, that means a must be a $\bullet$-identity. Similarly, b must be a $\circ$-identity. So the left and right-hand sides of (6.4) are equal, and $\mathbf{G}$ and $\mathbf{H}$ are complementary. □

The previous example suggests a certain balance between two complementary groupoids. The following proposition makes this precise: the fewer objects one groupoid has, the more a complementary one must have.

Proposition 6.9 (Complementarity in $\mathbf{Rel}$)**.** *The following are equivalent for groupoids* $\mathbf{G}$ *and* $\mathbf{H}$ *with the same set* A *of morphisms:*

- *their Frobenius structures are complementary;*
- *the map* $A \to \mathrm{Ob}(\mathbf{G}) \times \mathrm{Ob}(\mathbf{H})$ *given by* $a \mapsto \big(\mathrm{cod}_{\mathbf{G}}(a), \mathrm{cod}_{\mathbf{H}}(a)\big)$ *is bijective.*

Proof. Write $\bullet$ for the multiplication in $\mathbf{G}$, and $\circ$ for that in $\mathbf{H}$. By Proposition 6.7, complementarity is equivalent to unitarity of the morphism (6.8). Unitaries in $\mathbf{Rel}$ are exactly the bijective functions (see Exercise 2.5.7). Unfolding this, we see that complementarity is equivalent to:

$$\forall a, b \in A\ \exists! c, d \in A\ \exists e \in A \colon b = e \bullet d,\ c = a \circ e.$$

Because we're in a groupoid, when a, b, c, d are fixed, there is only one possible e fitting the bill, so we can reformulate this as:

$$\forall a, b \in A\ \exists! c, d, e \in A \colon d = e^{-1} \bullet b,\ c = a \circ e,$$

where the inverse is taken in $\mathbf{G}$. This just means that all $a, b \in A$ allow a unique $e \in A$ making $e^{-1} \bullet b$ and $a \circ e$ well-defined. But this happens precisely when e and b have the same codomain in $\mathbf{G}$, and $\mathrm{cod}(e) = \mathrm{dom}(a)$ in $\mathbf{H}$. Thus complementarity holds if and only if all objects g of $\mathbf{G}$ and h of $\mathbf{H}$ allow unique $e \in A$ with $\mathbf{G}$-codomain g and $\mathbf{H}$-codomain h. □

In particular: if two classical structures in $\mathbf{Rel}$ corresponding to abelian groupoids $\mathbf{G}$ and $\mathbf{H}$ are complementary, then $\mathbf{G}(g,g) \simeq \mathrm{Ob}(\mathbf{H})$ and $\mathbf{H}(h,h) \simeq \mathrm{Ob}(\mathbf{G})$ for each object g of $\mathbf{G}$ and h of $\mathbf{H}$.

In $\mathbf{FHilb}$, it so happens any classical structure allows a complementary one. That is, every orthonormal basis has a mutually unbiased one. This is not always the case in $\mathbf{Rel}$, where dagger Frobenius structures need to be 'homogeneous' in the sense that the groupoid looks the same under any 'translation' from one object to another.

Proposition 6.10. *A Frobenius structure in* $\mathbf{Rel}$ *corresponding to a groupoid* $\mathbf{G}$ *allows a complementary one exactly when the cardinality of the set of all morphisms into an object* g *is independent of* g*.*

Proof. One direction is obvious after the previous proposition. We will prove the other, by constructing a complementary groupoid $\mathbf{H}$. We may assume that $\mathbf{G}$ is not empty without loss of generality. Pick some object g_0. Observe that the set of A morphisms of $\mathbf{G}$ decomposes as $\bigcup_{g' \in \mathrm{Ob}(\mathbf{G})} \Big(\bigcup_{g \in \mathrm{Ob}(\mathbf{G})} \mathbf{G}(g, g')\Big)$. We will define $\mathbf{H}$ by carving up the set of morphisms of $\mathbf{G}$ the other way around. Set $\mathrm{Ob}(\mathbf{H}) = \bigcup_{g \in \mathrm{Ob}(\mathbf{G})} \mathbf{G}(g, g_0)$. By assumption, there are bijections $\varphi_{g'} \colon \mathrm{Ob}(\mathbf{H}) \to \bigcup_{g \in \mathrm{Ob}(\mathbf{G})} \mathbf{G}(g, g')$. Define $\mathbf{H}(h, h') = \emptyset$ for distinct h, h', and set $\mathbf{H}(h, h) = \{\varphi_g(h) \mid g \in \mathrm{Ob}(\mathbf{G})\}$. Then $\mathbf{H}$ has the same set of morphisms as $\mathbf{G}$, and if $a \in \mathbf{G}(g, g')$, then $a = \varphi'_g(h)$ for a unique $h \in \mathrm{Ob}(\mathbf{H})$, namely $h = \mathrm{cod}_{\mathbf{H}}(a)$. This construction makes the map $A \to \mathrm{Ob}(\mathbf{G}) \times \mathrm{Ob}(\mathbf{H})$ given by $a \mapsto (\mathrm{cod}_{\mathbf{G}}(a), \mathrm{cod}_{\mathbf{H}}(a))$ into a bijection.

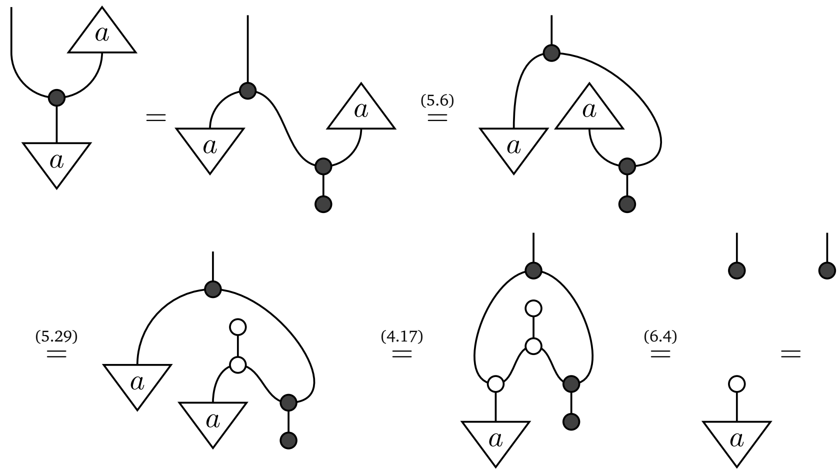
By the previous proposition, all that is left to do is to make $\mathbf{H}$ a well-defined groupoid in some way. For this it suffices to make $\mathrm{Ob}(\mathbf{G})$ into a group. If $\mathrm{Ob}(\mathbf{G})$ is finite, you can use the multiplication of $\mathbb{Z}_n$. If $\mathrm{Ob}(\mathbf{G})$ is infinite, then it is isomorphic to the set of its finite subsets, which form a group under the symmetric difference $U \cdot V = (U \cup V) \setminus (U \cap V)$. $\square$

6.1.4 Unbiased states

One way to understand complementary bases is to recognize that copyable states for one basis will be *unbiased* for a complementary basis. In other words, if you write out one basis element as a column vector in the coordinate system of the other basis, then each entry will be unitary up to an overall scalar factor. We captured this abstractly with the notion of a *phase* for a Frobenius structure in Definition 5.44. In other words, a state is unbiased for a dagger Frobenius structure when its phase shift is unitary.

Proposition 6.11. *In a braided monoidal dagger category, given complementary symmetric dagger Frobenius structures* $(A, \mu_{\circ}, \eta_{\circ})$ *and* $(A, \mu_{\bullet}, \eta_{\bullet})$*, if a state of A is self-conjugate, copyable and deletable for* $(\mu_{\circ}, \eta_{\circ})$*, then it is a phase for* $(\mu_{\bullet}, \eta_{\bullet})$*.*

Proof. Using the graphical calculus:



The third equality uses the self-conjugate property, the fourth equality uses the copyable property, and the last equality uses the deletable property. The symmetric requirement of (5.34) is analogous. $\square$

6.2 The Deutsch-Jozsa algorithm

The Deutsch-Jozsa algorithm solves a certain problem faster in the quantum case than is possible in the classical case. It is a typical example of a quantum algorithm that decides on a solution without relying on approximation. The Deutsch-Jozsa algorithm solves a slightly artificial problem, but other algorithms in this family include Shor's factoring algorithm, Grover's search algorithm, and the more general hidden subgroup problem. The 'all or nothing' nature of these algorithms make them amenable to categorical models, where we can see the structural difference between no information flow and maximum information flow. This section discusses the algorithm and proves its correctness categorically.

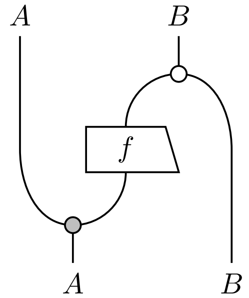
The Deutsch-Jozsa algorithm addresses the following problem. Suppose we have a 2-valued function $A \xrightarrow{f} \{0,1\}$ on a finite set A. If the function f takes just a single value on every element of A, it is called *constant*. Another possibility is that the function takes the value 0 on exactly half the elements of A, and takes the value 1 on the other half; in this case it is called *balanced*. Most functions are neither balanced or constant, but we will restrict to those that are. The Deutsch-Jozsa problem, given a function $A \xrightarrow{f} \{0,1\}$ promised to be either balanced or constant, is to determine which of the two is the case.

The best classical strategy is rather simple. We have no knowledge of the structure of the function f in general, so we must proceed to sample the function on elements of A. If we find two elements which have different values, then f cannot be constant, so we conclude that f is balanced and we are done. However, in the worst case, if f is balanced we might have to sample $\frac{1}{2}|A|+1$ elements until we find two elements with different values. If we sample this many elements and we find that f returns the same value for each one, then we can conclude that f is constant.

6.2.1 Oracles

The quantum Deutsch-Jozsa algorithm decides between the constant and balanced cases with just a *single* use of the function f. However, we have to be more precise about how to access the function f. A quantum computation only allows unitary gates; so we have to linearize the function $A \xrightarrow{f} \{0,1\}$ to a unitary map, called an *oracle*.

Definition 6.12. In a monoidal dagger category, given dagger Frobenius structures $(A, \bullet, \bullet)$ and $(B, \circ, \circ)$, an *oracle* is a morphism $A \xrightarrow{f} B$ that makes following morphism unitary:



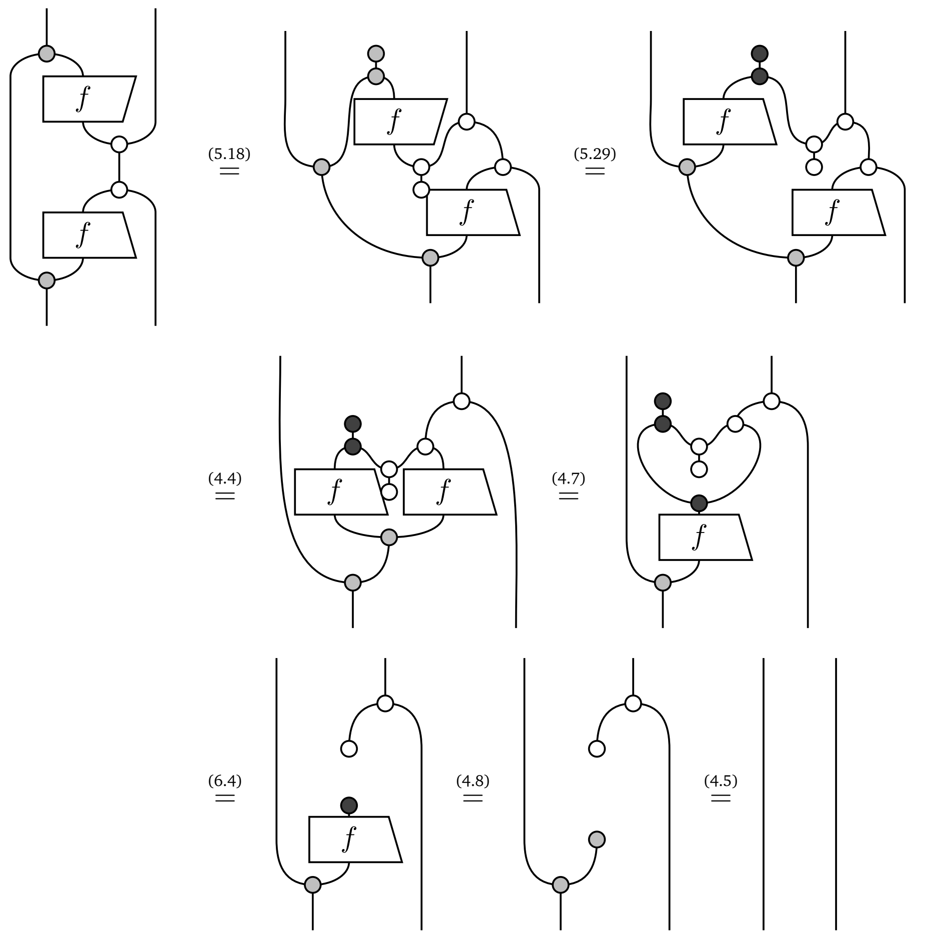
(6.10)

Example 6.13. Let $S \xrightarrow{f} T$ be a morphism of $\mathbf{FSet}$. Write A and B for the free Hilbert spaces with orthonormal bases S and T respectively. The function f induces a unique morphism $A \to B$ in $\mathbf{FHilb}$ that linearly extends the function $a \mapsto f(a)$. Now choose an orthogonal basis $\{e_i\}$ for B that is mutually unbiased to the elements of T, with squared norms $\|e_i\|^2 = \dim(B)$. With this basis as the white Frobenius structure, the map (6.10) sends $a \otimes e_i$ to $\langle e_i | f(a) \rangle a \otimes e_i$. We can use equation (6.3) to see that $|\langle e_i | f(a) \rangle|^2 = \|e_i\|^2 \|f(a)\|^2 / \dim(B) = 1$. Hence (6.10) is unitary, and the morphism $A \to B$ is an oracle. Because it extends the function f, we say it is an *oracle for f*.

The previous example is typical: we now prove that any oracle extends a function between bases. Recall from Corollary 5.37 that functions between bases are comonoid homomorphisms between classical structures, and from Lemma 5.38 that the latter are always self-conjugate.

Proposition 6.14. *In a braided monoidal dagger category, let $(A, \odot)$, $(B, \bullet)$, and $(B, \circ)$ be symmetric dagger Frobenius structures. If $\bullet$ and $\circ$ are complementary, then a self-conjugate comonoid homomorphism $(A, \odot) \xrightarrow{f} (B, \bullet)$ is an oracle.*

Proof. Compose (6.10) with its adjoint:

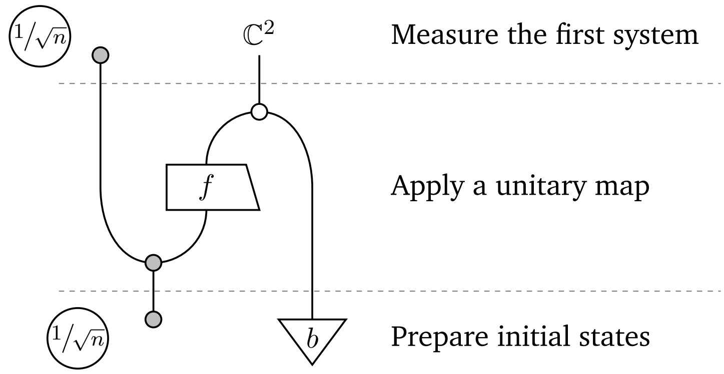


These equalities used the noncommutative spider theorem, self-conjugacy of f, (co)associativity, the fact that f preserves comultiplication, complementarity, the fact that f preserves the counit, and the unit and counit laws. The composition of (6.10) and its adjoint in the other order similarly gives the identity. Thus f is an oracle. □

6.2.2 The algorithm

We are now ready to state the procedure of the Deutsch-Jozsa algorithm itself.

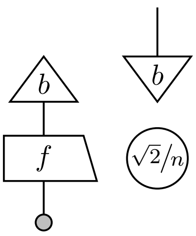
Definition 6.15 (The Deutsch-Jozsa algorithm)**.** Say that the set A has n elements, and let $A \xrightarrow{f} \{0, 1\}$ be the given function. Extend it to an oracle $H \to \mathbb{C}^2$ as in Example 6.13; the two complementary bases on $\mathbb{C}^2$ are the computational basis and the X basis from Example 6.5 scaled by $\sqrt{2}$. Write b for the state $\begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix}$ of $\mathbb{C}^2$. The *Deutsch-Jozsa* *algorithm* is the following morphism in **FHilb**:



(6.11)

The dashed horizontal lines separate the different stages of the procedure. In the language of states and effects of Sections 1.1.2 and 2.4: first prepare two systems in initial states, one in the maximally mixed state according to the gray classical structure, the other in state b; then apply a unitary gate; finally postselect on the first system being measured in the maximally mixed effect for the gray classical structure. Notice that either the computational basis or the X basis gives rise to a complete and disjoint set of effects on the qubit as in Section 2.4.3.The diagram (6.11) describes a particular quantum history, and taking the square of the norm of the state it represents gives the probability this history will occur.

Lemma 6.16. *The Deutsch-Jozsa algorithm* (6.11) *simplifies to:*



(6.12)

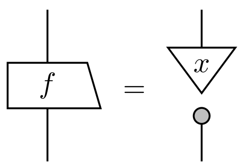
Proof. Duplicate the copyable state $\sqrt{2}b$ through the white dot in (6.11), and apply the noncommutative Spider Theorem 5.21 to the cluster of gray dots. □

6.2.3 Correctness

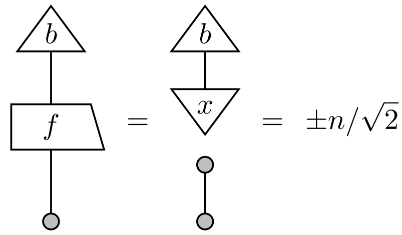
To prove correctness of the Deutsch-Jozsa algorithm, we distinguish the constant and balanced cases.

Lemma 6.17 (The constant case)**.** *If the function* $A \xrightarrow{f} \{0,1\}$ *is constant, then the history described in diagram* (6.11) *is certain.*

Proof. Suppose $f(a) = x$ for all $a \in A$. Then the oracle $H \xrightarrow{f} \mathbb{C}^2$ decomposes as:



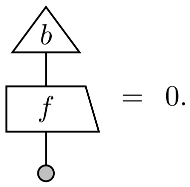
Thus the amplitude of the main component of the quantum history (6.12) is:



Hence the norm of (6.12) is 1. □

Lemma 6.18 (The balanced case)**.** *If the function* $A \xrightarrow{f} \{0,1\}$ *is balanced, then the history described in diagram* (6.11) *is impossible.*

Proof. Suppose f takes each value of the set $\{0,1\}$ on an equal number of elements of A. To test whether a particular f is balanced, we could perform a sum indexed by $a \in A$, with summand given by $+1$ if $f(a) = 0$, and by -1 if $f(a) = 1$; the function f would be balanced exactly when this sum gives 0. Given the definition of the state b, we could equivalently test the equality $\sum_{a \in A} b^\dagger(f(a)) = 0$, with the following graphical representation:



Hence the norm of (6.12) is 0. □

Theorem 6.19 (Deutsch-Jozsa is correct)**.** *The Deutsch-Jozsa algorithm* (6.11) *correctly identifies constant functions* $A \xrightarrow{f} \{0,1\}$.

Proof. The squared norm of the state (6.12) is the probability of the history occurring. The previous two lemmas show that the history (6.11) is a perfect test for discriminating constant and balanced functions. □

6.3 Bialgebras

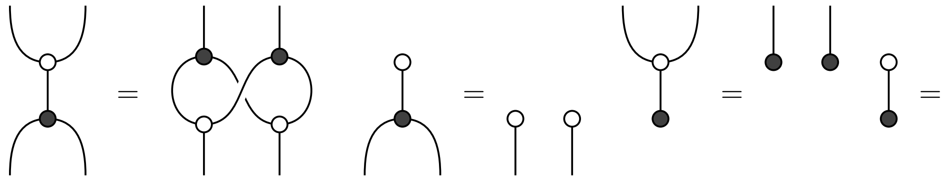
As we saw in Proposition 6.4, complementary classical structures **FHilb** are mutually unbiased bases. One common way to construct mutually unbiased bases is the following. Let G be a finite group, and consider the Hilbert space for which $\{g \in G\}$ is an orthonormal basis. Defining

$$: g \mapsto g \otimes g \qquad : g \mapsto 1 \tag{6.13}$$

$$: g \otimes h \mapsto gh \qquad : 1 \mapsto 1_G \tag{6.14}$$

gives complementary dagger Frobenius structures; see Examples 4.2 and 5.2. This construction additionally satisfies $\circ$: $g \otimes h \mapsto gh \otimes gh$, which is captured abstractly as follows.

Definition 6.20 (Bialgebra, dagger bialgebra)**.** In a braided monoidal category, a *bialgebra* comprises a monoid (,) and comonoid (,) on the same object, satisfying the following *bialgebra laws*:



(6.15)

In the first equation here we make a choice of using the over-crossing; using the under-crossing would yield an inequivalent definition, yielding inequivalent versions of some of the results in this chapter. In practice, these structures are often studied in symmetric monoidal categories, where of course this distinction does not arise. The last equation is not missing a picture, because we are drawing id_I as the empty picture (1.6). A bialgebra is *commutative* when the underlying monoid and comonoid are commutative. In a braided monoidal dagger category, a *dagger bialgebra* is a bialgebra for which = .

Example 6.21. There are many interesting examples of bialgebras.

- In any category with biproducts, any object A has a bialgebra structure given by its copying and deleting maps:

$$A \xrightarrow{\left(\begin{smallmatrix}\mathrm{id}_A\\ \mathrm{id}_A\end{smallmatrix}\right)} A \oplus A \qquad 0 \xrightarrow{0_{0,A}} A \qquad A \oplus A \xrightarrow{\left(\mathrm{id}_A\ \mathrm{id}_A\right)} A \qquad A \xrightarrow{0_{A,0}} 0$$

- Any monoid M is a bialgebra in $\mathbf{Set}$, as follows:

$$: m \mapsto (m, m) \qquad : m \mapsto \bullet \qquad : (m, n) \mapsto mn \qquad : \bullet \mapsto 1_M$$

- Any monoid M in $\mathbf{FSet}$ induces a bialgebra in $\mathbf{FHilb}$. Let $(A,$, $)$ be the group algebra; see Example 5.2, and define comultiplication and counit as follows:

$$: m \mapsto m \otimes m \qquad\qquad : m \mapsto 1$$

  When M is a group, $(A,$, $)$ can also be made into a Frobenius structure as in Example 5.2, but with different and . In Section 6.3.2 we will see a converse: bialgebras in $\mathbf{FSet}$ satisfying some additional properties always arise from groups like this.

  Any monoid in $\mathbf{Set}$ induces a bialgebra in $\mathbf{Rel}$ in a similar way.

The following concise formulation is a good way to remember the bialgebra laws; compare Lemma 5.62.

Lemma 6.22 (Bialgebras via homomorphisms)**.** *In a braided monoidal category, the following are equivalent:*

- *a comonoid* $(A,$, $)$ *and monoid* $(A,$, $)$ *form a bialgebra;*
- *and* *are comonoid homomorphisms, where* $A \otimes A$ *is a comonoid as in Lemma 4.8;*

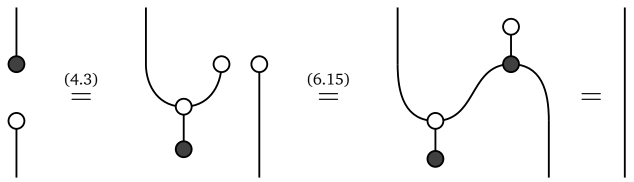
- *and are monoid homomorphisms, where $A \otimes A$ is a monoid as in Lemma 4.8.*

Proof. Unfolding what it means for to be a comonoid homomorphism: comultiplication preservation gives the first of the bialgebra laws (6.15); counit preservation gives the second; and the last two come from requiring that is a comonoid homomorphism. The case of monoid homomorphisms is analogous. □

As far as interaction between monoids and comonoids is concerned, Frobenius structures and bialgebras are in some sense opposite extremes. The following theorem shows that both sets of axioms cannot hold simultaneously, except in the trivial case. What leads to the degeneracy is that the Frobenius law (5.1) equates only *connected* diagrams, whereas the bialgebra laws (6.15) equate connected diagrams with *disconnected* ones.

Theorem 6.23 (Frobenius bialgebras are trivial)**.** *In a braided monoidal category, if a monoid $(A, \,,\,)$ and comonoid $(A, \,,\,)$ form both a Frobenius structure and a bialgebra, then $A \simeq I$.*

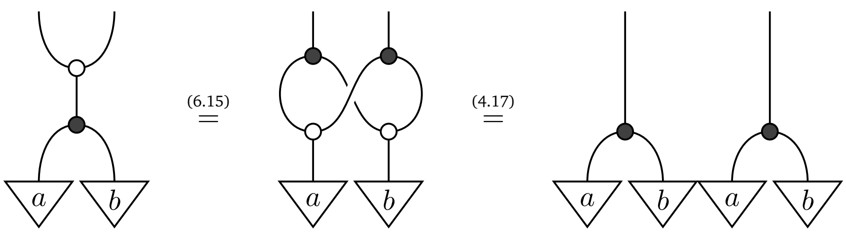
Proof. We will show that and are inverse morphisms. The bialgebra laws (6.15) already require $\circ = \mathrm{id}_I$. For the other composite:



The first equality is counitality, the second equality is the second bialgebra law, and the last equality follows from Theorem 5.15. □

Lemma 6.24 (Monoid of copyable states)**.** *In a braided monoidal category, given a bialgebra $(A, \,,\,,\,,\,)$, the states that are copyable by and deletable by form a monoid under with unit .*

Proof. Associativity (4.4) is immediate. Unitality (4.5) comes down to the third and fourth bialgebra laws (6.15): is copyable by and deletable by . What has to be proven is that if we multiply two -copyable states using , we get another -copyable state:



Similarly using the second bialgebra law (6.15) shows that multiplying two -deletable states with gives another -deletable state. □

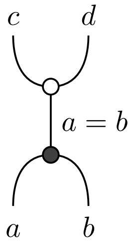
6.3.1 Strong complementarity

We now investigate the relationship between complementarity and bialgebras.

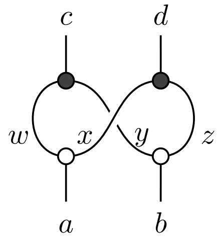
Lemma 6.25. *In* $\mathbf{Rel}$*, the special dagger Frobenius structures induced by a group and a discrete groupoid on the same set of morphisms form a bialgebra.*

The bialgebra structure is between the monoid part of one structure and the comonoid part of the other. This must be the case, since Frobenius bialgebras must be trivial by Theorem 6.23.

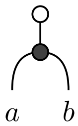
Proof. Let $(G, \circ, 1)$ be a group and $(G, \bullet)$ a discrete groupoid. Then:



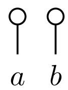
$$\iff \exists w,x,y,z \in G\colon \begin{bmatrix} a = w \circ x \\ b = y \circ z \\ c = w \bullet y \\ d = x \bullet z \end{bmatrix} \iff$$



because for $c = w \bullet y$ to make sense we must have $c = w = y$. Similarly:



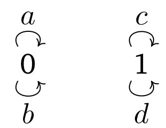
$$\iff a \bullet b = 1 \iff a = b = 1 \iff$$



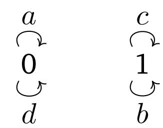
The final two bialgebra laws hold similarly by Proposition 6.9. □

It is not true that any two complementary groupoids form a bialgebra in $\mathbf{Rel}$.

Example 6.26. The following two groupoids are complementary, but do not form a bialgebra in $\mathbf{Rel}$.



$$b^2 = a = \mathrm{id}_0 \qquad d^2 = c = \mathrm{id}_1$$



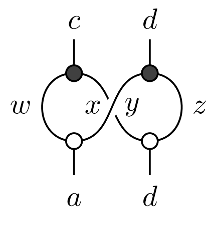
$$d^2 = a = \mathrm{id}_0 \qquad b^2 = c = \mathrm{id}_1$$

Proof. Both groupoids have $G = \{a, b, c, d\}$ as set of morphisms, and $\{a, c\}$ as set of identities. Write $\circ$ for the composition in the left groupoid, and $\bullet$ for the right one. The function $G \to \{0,1\}^2$ given by $g \mapsto (\mathrm{cod}_\circ(g), \mathrm{cod}_\bullet(g))$ is bijective:

$$a \mapsto (0,0) \qquad b \mapsto (0,1) \qquad c \mapsto (1,1) \qquad d \mapsto (1,0)$$

Hence the two groupoids are complementary by Proposition 6.9.

Notice that $a \bullet d = d = c \circ d$. Hence $(a, d) \sim (c, d)$ in the left-hand side of the first bialgebra law (6.15). Suppose it held in the right-hand side too:

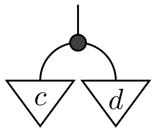


Then $w \bullet y = c$, so either $w = y = c$, or $w = y = b$. But also $y \circ z = d$, so either $y = c$ and $z = d$, or $y = d$ and $z = c$. Therefore $w = y = c$ and $z = d$. But that contradicts $w \circ x = a$, so the two groupoids do not form a bialgebra. $\square$

The same situation occurs in **FHilb**: complementary Frobenius structures often do not form a bialgebra.

Example 6.27. Consider the object $\mathbb{C}^2$ in **FHilb**. The computational basis $\{\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right), \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)\}$ gives it a dagger Frobenius structure. For any angles $\varphi, \theta \in \mathbb{R}$, the orthogonal basis $\{\left(\begin{smallmatrix}e^{i\varphi}\\e^{i\theta}\end{smallmatrix}\right), \left(\begin{smallmatrix}e^{i\varphi}\\-e^{i\theta}\end{smallmatrix}\right)\}$ gives it a dagger Frobenius structure. These two Frobenius structures are complementary, but they only form a bialgebra when the angles φ and θ are integer multiples of 2π.

Proof. Write $\{a, b\}$ for the computational basis, and $\{c, d\}$ for the other one. The two bases are complementary because $\langle a|c\rangle\langle c|a\rangle = \langle a|d\rangle\langle d|a\rangle = \langle b|c\rangle\langle c|b\rangle = \langle b|d\rangle\langle d|b\rangle = 1$. Plugging in $c \otimes d$, the first bialgebra law (6.15) holds if and only if the state



$$= \begin{pmatrix} e^{2i\varphi} \\ -e^{2i\theta} \end{pmatrix}$$

is copyable for; that is, when φ and θ are zero modulo 2π. $\square$

We give the following name to pairs of symmetric dagger Frobenius structures that simultaneously are complementary and form a bialgebra.

Definition 6.28 (Strong complementarity)**.** In a braided monoidal dagger category, two symmetric dagger Frobenius structures are *strongly complementary* when they are complementary, and also form a bialgebra.

Example 6.26 and Example 6.27 showed that strong complementarity is strictly stronger than complementarity. Strongly complementary pairs of Frobenius structures enjoy extra properties. Note the resemblance of the following theorem to the phase group (5.36).

Theorem 6.29. *In a braided monoidal dagger category, let* $(A, \;,\;)$ *and* $(A, \;,\;)$ *be strongly complementary symmetric dagger Frobenius structures. The states that are self-conjugate, copyable and deletable for* $(\;,\;)$ *form a group under* .

Proof. By Lemma 6.24 these states form a monoid, and by Proposition 6.11 every element of this monoid has a left and right inverse. $\square$

When one of the Frobenius structures is commutative, strong complementarity lets us classify strongly complementary pairs in **FHilb**. The following theorem shows that the group algebra of Example 5.2, and (6.13) and (6.14), are in fact the only way to generate strongly complementary pairs in **FHilb**.

Theorem 6.30. *In* **FHilb***, pairs of strongly complementary symmetric dagger Frobenius structures, one of which is commutative, correspond to finite groups via* (6.13) *and* (6.14).

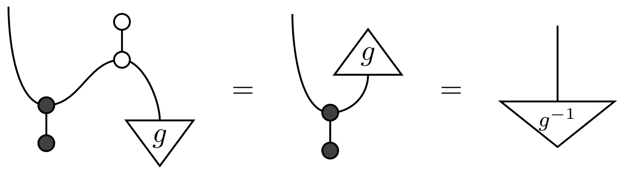
Proof. Equations (6.13) and (6.14) give symmetric dagger Frobenius structures that form a strongly complementary pair, and one of them is commutative.

Conversely, suppose symmetric dagger Frobenius structures and form a strongly complementary pair on H in **FHilb**, and that is commutative. By Theorem 6.29 the states which are self-conjugate, copyable and deletable for (,) form a group for . But by the classification of commutative dagger Frobenius structures in **FHilb** of Theorem 5.36, there is an entire basis of such states for . So must be the group algebra of Example 5.2. □

Contrast the previous theorem with the open problem of classifying (non-strongly) complementary pairs of commutative Frobenius structures – mutually unbiased bases – on Hilbert spaces whose dimension is not a prime power.

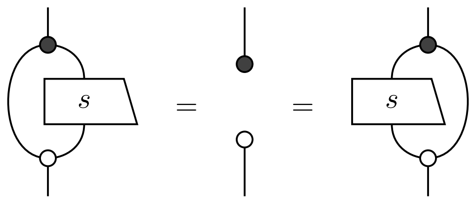
6.3.2 Hopf algebras

By Theorem 6.30, for strongly complementary symmetric dagger Frobenius structures in **FHilb**, one of which is commutative, the map (6.5) is the linear extension of the inverse operation $g \mapsto g^{-1}$ of a group:



The same calculation holds for complementary Frobenius structures in **Rel**, because we may assume that is a group and is a skeletal groupoid thanks to Proposition 6.9. It is therefore natural to ask what abstract property this map (6.5) satisfies. This motivates the following definition.

Definition 6.31 (Antipode, Hopf algebra)**.** In a monoidal category, an *antipode* for a monoid $(A, \,)$ and comonoid $(A, \,)$ is a morphism $A \xrightarrow{s} A$ satisfying the following equations:

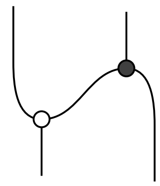


(6.16)

In a braided monoidal category, a *Hopf algebra* is a bialgebra equipped with an antipode; equation (6.16) is then called the *Hopf law*.

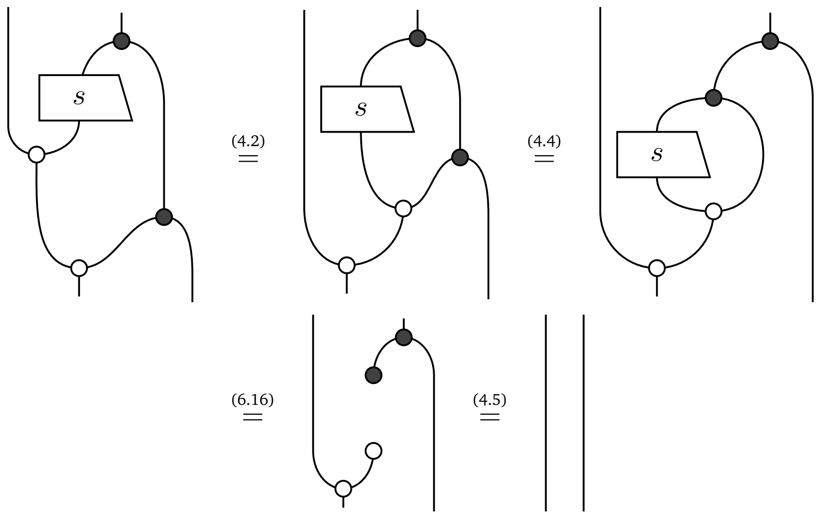
Strongly complementary symmetric dagger Frobenius structures are by definition Hopf algebras, with (6.5) as antipode. There are many Hopf algebras that do not arise in this way. The following theorem illustrates this; compare it to Proposition 6.7 by way of the dagger.

Theorem 6.32. *A monoid-comonoid pair in a monoidal category allows an antipode satisfying the Hopf law* (6.16) *if and only if the following morphism is invertible:*



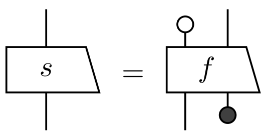
(6.17)

Proof. First suppose that the Hopf law (6.16) is satisfied with antipode s. Then (6.17) has a left inverse:



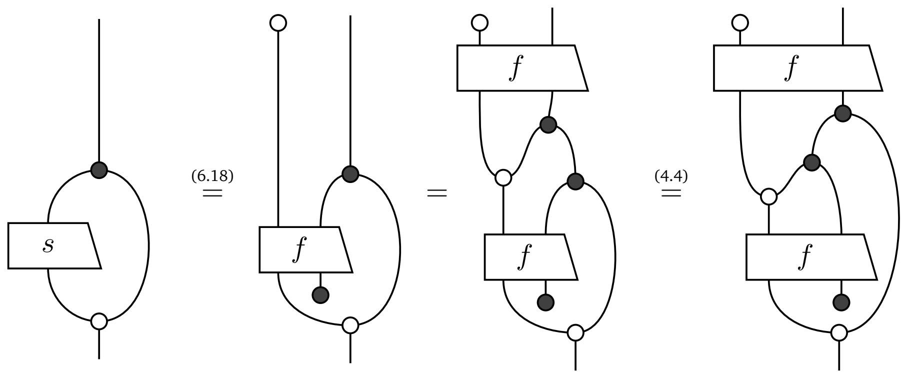
The composition the other way around similarly equals the identity. Thus (6.17) is invertible.

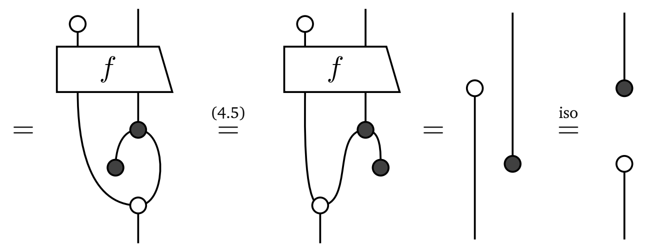
For the converse, suppose that (6.17) has an inverse f. Define:



(6.18)

Then:



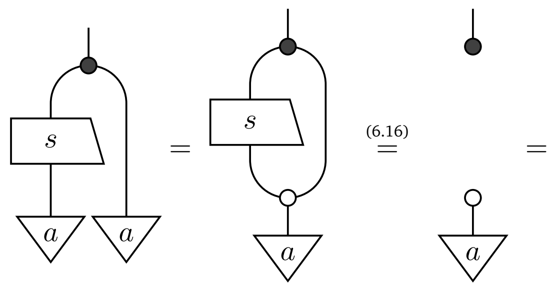


The other equation of the Hopf law (6.16) follows similarly. □

Hopf algebras are related to so-called *quantum groups*; the following proposition shows that they indeed generalize groups.

Proposition 6.33. *In a braided monoidal category, given a Hopf algebra, the states which are copied by the comultiplication and deleted by the counit form a group under the multiplication.*

Proof. By Lemma 6.24, the states which are copied by the comultiplication form a monoid. Acting on a state with the antipode gives a left inverse:



(6.19)

Similarly, acting by the antipode also gives a right inverse. □

Corollary 6.34. *In* **Set***, Hopf algebras are exactly groups.*

Proof. This follows immediately from Example 4.2, since the only comonoids in **Set** are built from the diagonal and terminal morphisms, which copy and delete every element of the underlying set. □

If Frobenius structures are all about involutions (as in Section 5.3.2), then Hopf algebras are all about inverses. This intuitively explains Theorem 6.23: the only idempotent of a group is the unit.

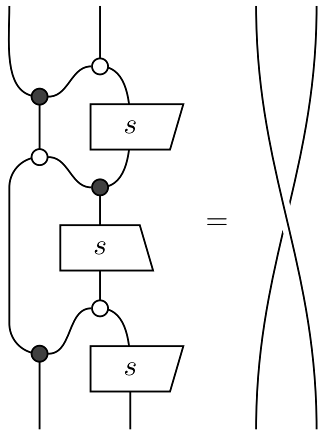
6.4 Qubit gates

The graphical calculus can be used to describe various quantum computing gates, and to prove that they have good properties. Before specializing to qubits in Hilbert spaces, we first exemplify how basic properties of quantum computation really hold more generally, and only depends on (strong) complementarity: a swap gate can be built from three controlled NOT gates.

6.4.1 Controlled negation

The following theorem proves that the first bialgebra law is equivalent to the property that the swap map can be built from three CNOT gates.

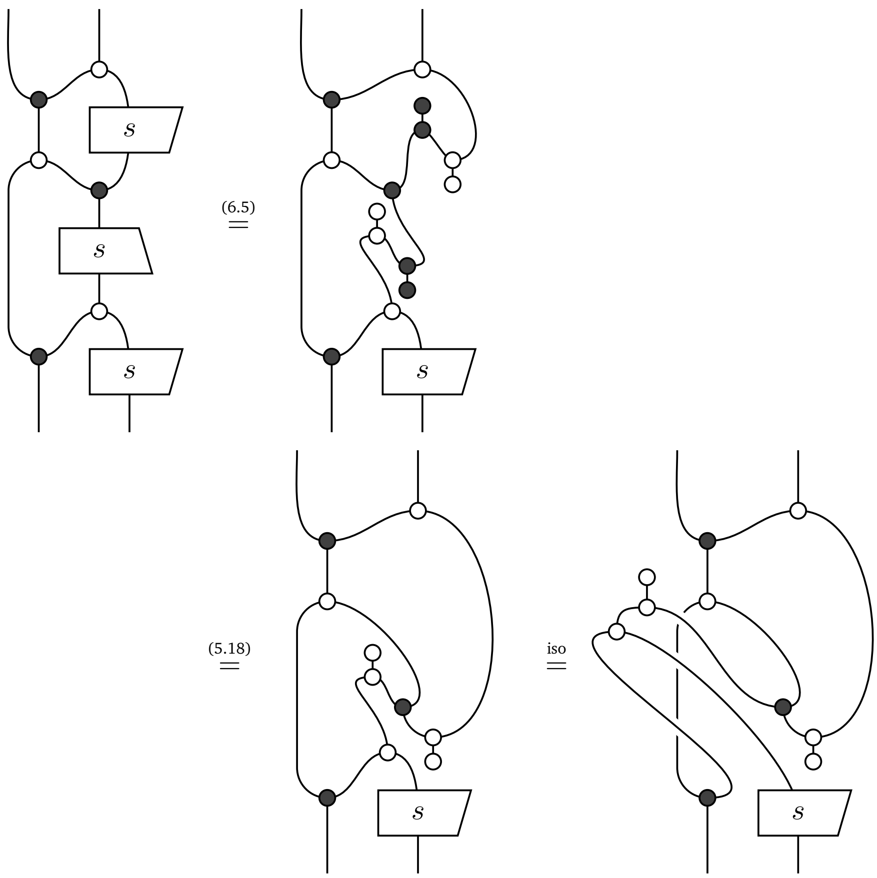
Theorem 6.35 (Swap via three CNOTs)**.** *In a braided monoidal dagger category, let* (,) *and* (,) *be complementary classical structures. If they are strongly complementary, then the following equation holds, where* s *is the morphism* (6.5)*:*

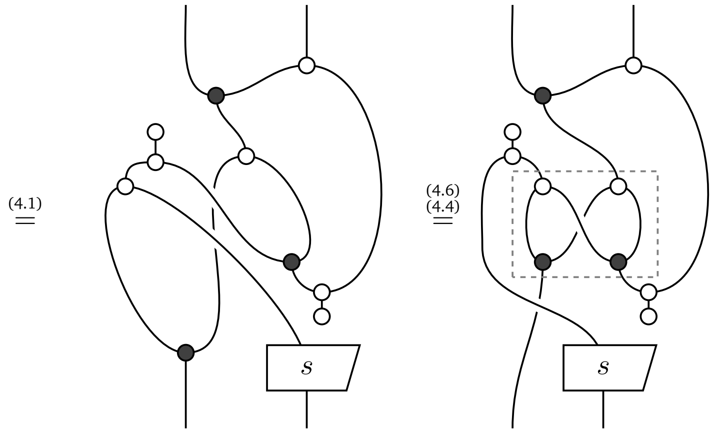


(6.20)

In fact, equation (6.20) *holds if and only if the first equation of* (6.15) *does.*

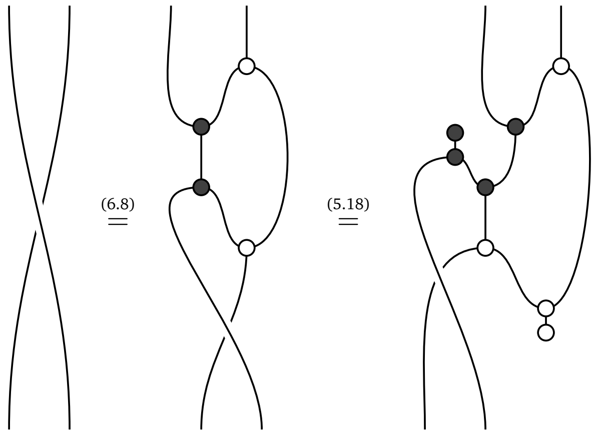
Proof. First, rewrite the left-hand side of (6.20):

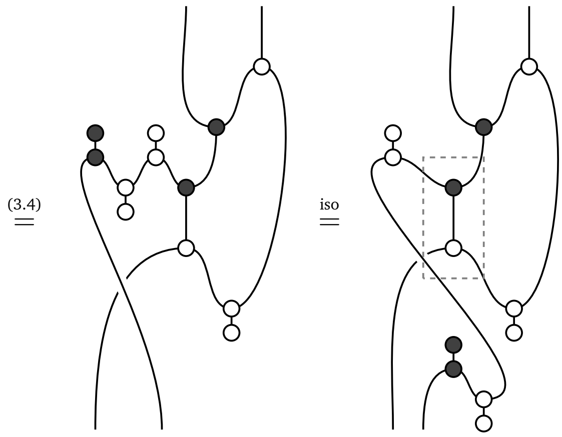




The second equality uses the (noncommutative) black spider Theorem 5.21, the fourth uses cocommmutativity of , and the fifth uses associativity and commutativity of the white structure.

Rewrite the right-hand side similarly:





The first equality comes from Proposition 6.7.

Now, using strong complementarity on the marked parts turns the left-hand side into the right-hand side. Conversely, if the left-hand side equals the right-hand side, we can use snake equations to 'undo' everything but the marked parts to see that the bialgebra law must hold. □

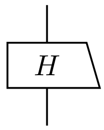
Why may we think of the left-hand side of (6.20) as a generalization of 'three CNOT gates'? It is clearly a composition of six unitary maps, namely three unitaries of the form (6.8), and three of the form (6.5).

Example 6.36. In **FHilb**, fix A to be the qubit $\mathbb{C}^2$. Let (,) be defined by the computational basis $\{|0\rangle, |1\rangle\}$, and (,) by the X basis from Example 6.5. Then the three antipodes (6.5) become identities. Furthermore, each unitary of the form (6.8) reduces to a CNOT gate.This gate performs a NOT operation on the second qubit if the first (control) qubit is $|1\rangle$, and does nothing if the first qubit is $|0\rangle$:

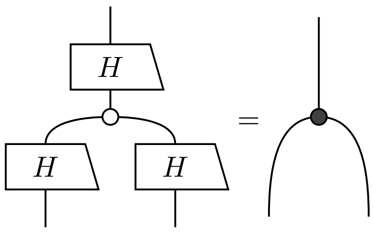
$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{6.21}$$

We will fix these two classical structures for the rest of this chapter. The relationship between them is $|+\rangle = |0\rangle + |1\rangle$, and $|-\rangle = |0\rangle - |1\rangle$. Hence they are transported into each other by the *Hadamard gate* (see also Definition 5.17).

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \tag{6.22}$$



Thus the exact relationship between H, , and is as follows:



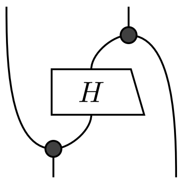
(6.23)

6.4.2 Controlled phases

In addition to the CNOT gate, we can now also define the CZ gate abstractly. This gate performs a Z phase shift on the second qubit when the first (control) qubit is $|1\rangle$, and leaves it alone when the first qubit is $|0\rangle$.

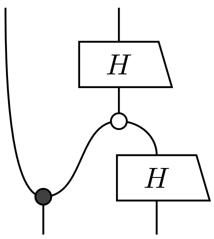
Lemma 6.37. *In* **FHilb***, the* CZ *gate can be defined as follows:*

$$\mathrm{CZ} = \tag{6.24}$$



Proof. Rewrite equation (6.24) as follows:

$$\mathrm{CZ} \overset{(5.13)}{=}$$



Hence, by Example 6.36:

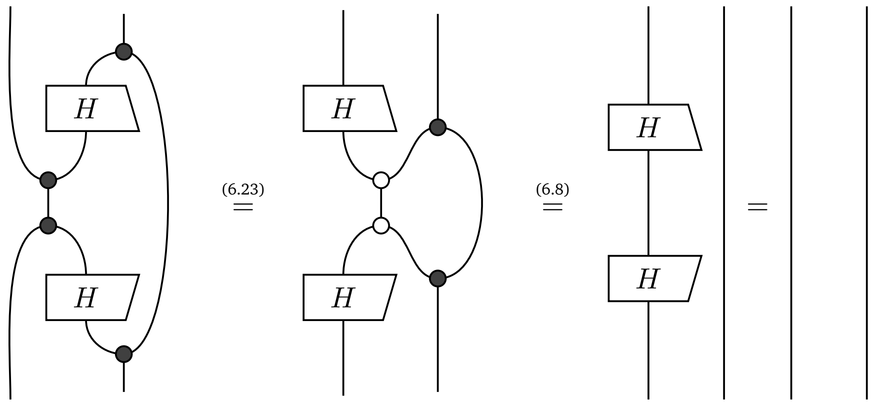
$$\mathrm{CZ} = (\mathrm{id} \otimes H) \circ \mathrm{CNOT} \circ (\mathrm{id} \otimes H) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

This is indeed the controlled Z gate. □

We may take (6.24) as a definition of CZ in any braided monoidal dagger category in which the Hadamard gate makes sense. First we prove that this abstract CZ gate is always unitary.

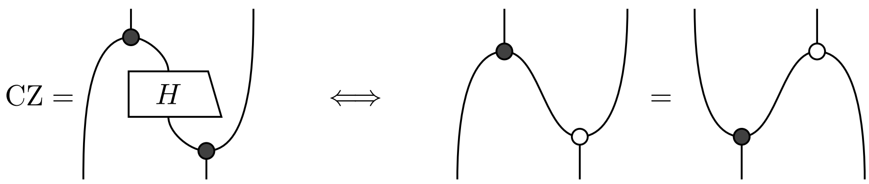
Lemma 6.38 (CZ is unitary). *In a braided monoidal dagger category, let* $(A, \whitedot)$ *be a commutative Frobenius structure, and let* $A \xrightarrow{H} A$ *be unitary. Define* $\blackdot$ *by* (6.23). *If* $\whitedot$ *and* $\blackdot$ *are complementary, then* (6.24) *is unitary.*

Proof. First, $\mathrm{CZ} \circ \mathrm{CZ}^\dagger$ equals the identity:



A similar argument shows that $\mathrm{CZ}^\dagger \circ \mathrm{CZ}$ equals the identity. Hence CZ is unitary. □

Note that there was a choice to be made in our definition (6.24) of the abstract CZ gate. We could also have defined it as on the left below. The two choices are equal if and only if the right-hand property below is satisfied.

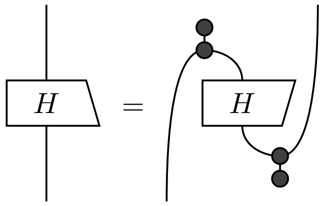


The following proposition shows that the abstract CZ gate is of order two, *i.e.* an involution, precisely when the Hadamard gate is a symmetric matrix.

Proposition 6.39 (CZ has order two). *In a braided monoidal dagger category, let* $(A, \blackdot)$ *be a classical structure, assume that* $A \xrightarrow{H} A$ *is a unitary, and that it transports* $(A, \blackdot)$ *to a complementary structure* $(A, \whitedot)$. *The following are equivalent:*

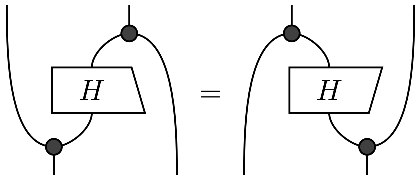
- $\mathrm{CZ} \circ \mathrm{CZ} = \mathrm{id}$;
- $\mathrm{CZ}^\dagger = \mathrm{CZ}$;

- *H is self-conjugate:*



(6.25)

Proof. Equivalence of the first two parts follows from Lemma 6.38. Expanding $\mathrm{CZ} = \mathrm{CZ}^\dagger$ gives:

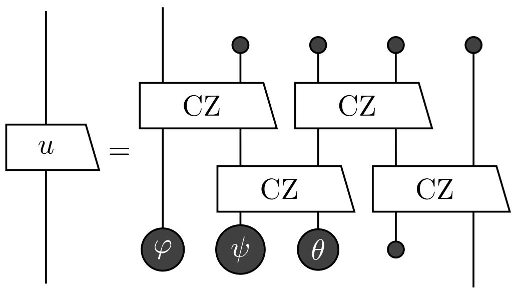


Composing this with black (co)units on the top left and bottom right wire gives (6.25). Conversely, composing (6.25) with black (co)multiplications on the bottom left and top right wire gives the equation above. □

6.4.3 Single qubit gates

Finally, qubits have the nice property that any unitary on them can be implemented via its *Euler angles*. More precisely: for any unitary $\mathbb{C}^2 \xrightarrow{u} \mathbb{C}^2$, there exist phases $\varphi, \psi, \theta \in \mathbb{C}$ such that $u = Z_\theta \circ X_\psi \circ Z_\varphi$, where Z_θ is the unitary rotation in the Z basis over angle θ, and X_φ in the X basis over angle φ. Therefore we can implement such unitaries abstractly using only CZ-gates.

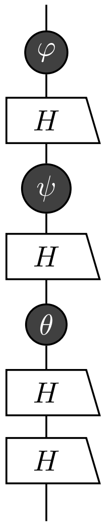
Theorem 6.40. *Any unitary $\mathbb{C}^2 \xrightarrow{u} \mathbb{C}^2$ in* $\mathbf{FHilb}$ *can be written as:*



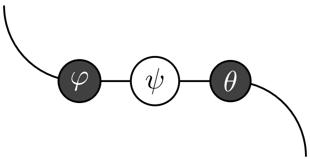
(6.26)

for some angles φ, ψ, θ. The phased spider notation here is that of Corollary 5.51.

Proof. Let φ, ψ, θ be the Euler angles for u. Substituting (6.24) and using Corollary 5.51, equation (6.26) reduces to:



But by Proposition 6.39 and Definition 5.17, this is just:

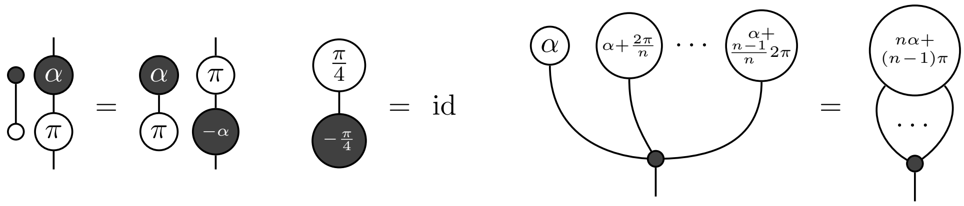


which equals u by definition. □

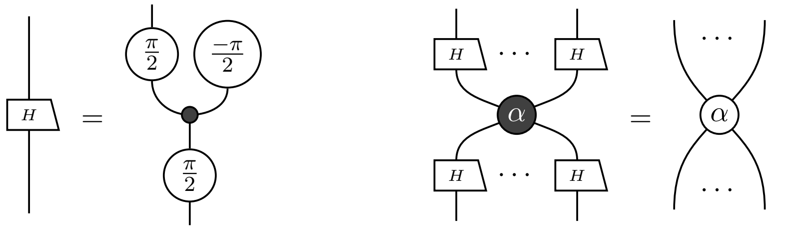
6.5 ZX calculus

This chapter has studied the behaviour of complementary observables in the abstract. So far, in this section, we have seen that this leads to a useful practical language for quantum circuits: the Pauli Z and X observables on qubits are complementary, and can be used to formulate quantum gates. In this last section, we will briefly discuss the *ZX calculus*. It turns out that not only can we break many-qubit gates into more primitive components as above, but adding a couple of rules to the ones we already have for complementary observables, this graphical language can describe any possible quantum computation, manipulating diagrams graphically doesn't change their computational meaning, and any proof of showing that two circuits are equal can be done graphically.

Let us pose the axioms without ado. The ZX calculus concerns two strongly complementary classical structures  and  in a compact dagger category, on an underlying object A. The calculus is built from *generators*, meaning the morphisms that are composed, and *equations*, which specify how they must behave; any family of generators satisfying the indicated equations yields a *model* of the ZX calculus. Complex phases α are allowed as generators. They will be restricted to integer multiples of $\pi/4$ or $\pi/2$ in the discussion below. At any rate, they must satisfy the following equations for all $n = 1, 2, 3, \ldots$, as well as their colour-swapped versions:



Moreover, the *Hadamard gate* $A \xrightarrow{H} A$ is a generator, and is required to satisfy the following equations, as well as their colour-swapped versions:



(6.27)

These generators and relations define a compact dagger subcategory of **FHilb**. Indeed, the formal symbols above have a standard interpretation, which we'll write as $[\![-]\!]$. For example, $[\![A]\!] = \mathbb{C}^2$, $[\![\,\text{copy}\,]\!] \colon \mathbb{C}^2 \to \mathbb{C}^2 \otimes \mathbb{C}^2$ copies the Z basis, and $[\![H]\!] = \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right) / \sqrt{2} \colon \mathbb{C}^2 \to \mathbb{C}^2$ is the usual Hadamard matrix.

Firstly, this interpretation is *sound*. In other words, any graphical manipulations done with ZX diagrams yield valid equalities between matrices under the standard interpretation.

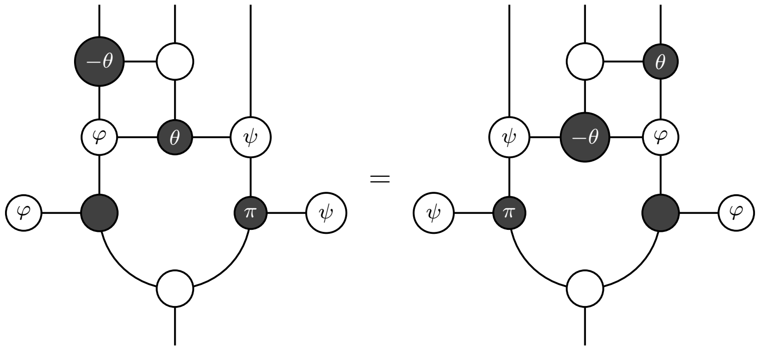
Theorem 6.41 (ZX calculus is sound)**.** *Let D_1, D_2 be diagrams in the ZX calculus. If D_1 equals D_2 under the axioms of the ZX calculus, then $[\![D_1]\!] = [\![D_2]\!]$.*

Proof. This comes down to checking that the axioms of the ZX calculus remain true under the standard interpretation $[\![-]\!]$. □

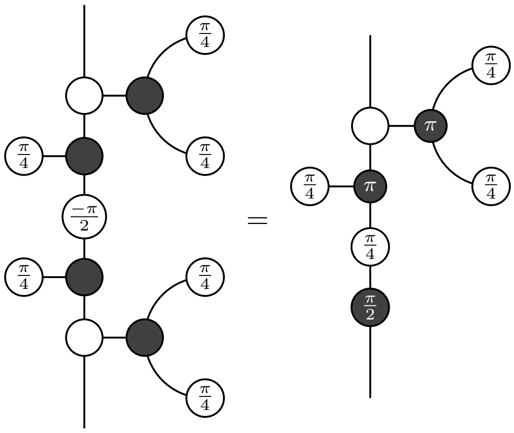
Secondly, any possible linear transformation from m qubits to n qubits can be approximated up to arbitrary precision with ZX diagrams. In other words, the ZX calculus is *approximately universal*. The proof of this is beyond the scope of this book.

Theorem 6.42 (ZX calculus is approximately universal)**.** *For any morphism $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 \xrightarrow{f} \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$ in* **FHilb**, *and any error margin $\varepsilon > 0$, there exists a diagram D in the ZX calculus, that only includes phases that are integer multiples of $\frac{\pi}{4}$, such that $\|[\![D]\!] - f\| < \varepsilon$.*

Finally, is the ZX calculus *complete*? That is, if two linear transformations are equal, and are both given by some ZX calculus diagrams, is there always a graphical proof of this using only the axioms of the ZX calculus? The answer is no when we allow arbitrary phases ϕ. But if we restrict the phases, then the answer is yes! We can restrict to integer multiples of π, or to integer multiples of $\frac{\pi}{2}$. However, for these restrictions, Theorem 6.42 no longer guarantees universality, as it might use phases that do not meet the restriction. To get completeness for phases that are multiples of $\frac{\pi}{4}$, we need to add the following further two axioms for any phases φ, ψ, θ that are multiples of $\frac{\pi}{4}$:



(6.28)



(6.29)

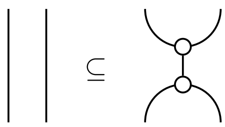
Theorem 6.43 (ZX calculus is complete)**.** *Let D_1, D_2 be diagrams in the ZX calculus that only includes phases that are integer multiples of $\pi/4$. If $[\![D_1]\!] = [\![D_2]\!]$, then $D_1 = D_2$ under the axioms of the ZX calculus together with* (6.28) *and* (6.29).

The proof of this completeness theorem is beyond the scope of this book, but the statement alone illustrates the power of graphical methods. All in all, the ZX calculus reduces reasoning about and constructing quantum computations from infinitely many possibilities to finitely many equations between finitely many generators, which computers can handle.

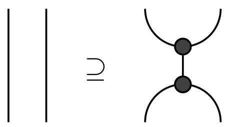
6.6 Exercises

Exercise 6.6.1. Let $(G, \circ)$ and $(G, \bullet)$ be two complementary groupoids (see Proposition 6.9).

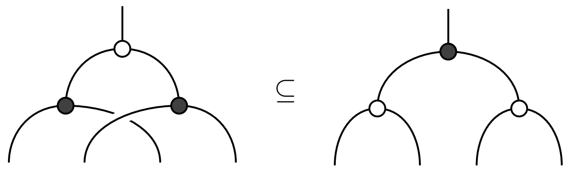
(a) Assume that $(G, \circ)$ is a group. Show that:



(b) Assume that $(G, \circ)$ is a group. Show that:



(c) Assume that $(G, \circ)$ is a group and that the corresponding Frobenius structures in $\mathbf{Rel}$ form a bialgebra. Show that:



Compare this to the Eckmann-Hilton property of Exercise 4.4.3.

Exercise 6.6.2. Let A be a set with a prime number of elements. Show that pairs of complementary special dagger Frobenius structures on A in $\mathbf{Rel}$ correspond to groups whose underlying set is A.

Exercise 6.6.3. Consider a special dagger Frobenius structure in $\mathbf{Rel}$ corresponding to a groupoid $\mathbf{G}$.

(a) Show that nonzero copyable states correspond to endohomsets $\mathbf{G}(A, A)$ of $\mathbf{G}$ that are isolated in the sense that $\mathbf{G}(A, B) = \emptyset$ for each object B in $\mathbf{G}$ different from A.

(b) Show that unbiased states of $\mathbf{G}$ correspond to sets containing exactly one morphism into each object of $\mathbf{G}$ and exactly one morphism out of each object of $\mathbf{G}$.

(c) Consider the following two groupoids on the morphism set $\{a, b, c, d\}$.

Show that copyable states for one are unbiased for the other, but that they are not complementary. Conclude that the converse of Proposition 6.11 is false.

Exercise 6.6.4. Consider a monoid in a monoidal category $\mathbf{C}$. The category of modules and module homomorphisms over the monoid (see Section 5.6) has nice properties when the monoid does. Show that:

(a) if the monoid is a bialgebra, then the category of modules is a monoidal category under the tensor product inherited from $\mathbf{C}$;

(b) if the monoid is a Hopf algebra and $\mathbf{C}$ is compact, then the category of modules is compact;

(c) if the monoid is a Hopf algebra and $\mathbf{C}$ is left-closed (see Exercise 4.4.4), then the category of modules is left-closed.

Exercise 6.6.5. A *Latin square* is an n-by-n matrix L with entries from $\{1, \ldots, n\}$, with each $i = 1, \ldots, n$ appearing exactly once in each row and each column. Choose an orthonormal basis $\{e_1, \ldots, e_n\}$ for $\mathbb{C}^n$. Define : $\mathbb{C}^n \to \mathbb{C}^n \otimes \mathbb{C}^n$ by $e_i \mapsto e_i \otimes e_i$, and : $\mathbb{C}^n \otimes \mathbb{C}^n \to \mathbb{C}^n$ by $e_i \otimes e_j \mapsto e_{L_{ij}}$. Show that the composite (6.17) is unitary. Note that need not be associative or unital.

Exercise 6.6.6. This exercise is about *property* versus *structure*. (See also Exercise 4.4.2.)

(a) Suppose that a category $\mathbf{C}$ has products and terminal objects. Show that any monoid in $\mathbf{C}$ has a unique bialgebra structure with respect to the monoidal structure given by the categorical product.

(b) It follows from Theorem 6.32 that being a Hopf algebra is a property of, rather than a structure on, a bialgebra. Prove directly that a bialgebra can have at most one antipode.

Exercise 6.6.7. Let $F\colon \mathbf{C} \to \mathbf{D}$ be a monoidal dagger functor between monoidal dagger categories. Suppose that $(A, \ , \ , \ , \ )$ and $(A, \ , \ , \ , \ )$ are complementary symmetric dagger Frobenius structures in $\mathbf{C}$. Show that the two induced Frobenius structures on $F(A)$ are also complementary. (See also Exercise 5.7.5.)

Notes and further reading

Complementarity has been a basic principle of quantum theory from very early on. It was proposed by Niels Bohr in the 1920s, and is closely identified with the Copenhagen interpretation [126]. Its mathematical formulation in terms of mutually unbiased bases is due to Schwinger in 1960 [129]. The abstract formulation in terms of classical structures we used was first given by Coecke and Duncan in 2008 [37]. (Terminology warning: some authors require complementary Frobenius structures to be special, leading to an extra scalar factor in Definition 6.3.) Strong complementarity was first discussed in that article, too, and the ensuing Theorem 6.30 is due to Coecke, Duncan, Kissinger and Wang in 2012 [38]. The relationship between Latin squares and complementary structures explored in Exercise 6.6.5 is due to Musto in 2014. Example 6.26 is due to Tull in 2015.

The abstract description of the Deutsch-Jozsa algorithm is due to Vicary in 2013 [140]. That paper includes the observation of Proposition 6.7, which is due to Zeng. The Grover and hidden-subgroup algorithms can be treated similarly. The applications in Section 6.4 are basic properties in quantum computation, and are especially important to measurement based quantum computing [122]. See also work by Duncan and Perdrix from 2009 for more abstract results on Euler angles [57].

Our proofs that oracles behave like functions (Lemma 5.19, Corollary 5.37, Lemma 5.38, and Proposition 6.14) is an echo of a more general theory: special Frobenius structures and morphisms that preserve multiplication and comultiplication (but not necessarily unit and counit) form a so-called discrete inverse category [68].

Bialgebras and Hopf algebras are the starting point for the theory of quantum groups [88, 136, 108]. They have been around in algebraic form since the 1960s, when Heinz Hopf first studied them [78]. Graphical notation for them is becoming more standard now, with so-called Sweedler notation as a middle ground [33]. Various results in this chapter are well-known in the quantum group literature, although not often in graphical form, such as Theorem 6.32 in [22].

Research on the ZX calculus was started by Coecke and Duncan in 2008 [37]. Completeness was established first for various fragments by Duncan and Perdrix in 2013 [58], and Backens in 2013 [10] and 2014 [11]. Full completeness was shown to be impossible in 2014 by De Witt and Zamdzhiev [128]. The approximately complete axiomatisation we discussed is due to Jeandel, Perdrix, and Vilmart in 2017 [82]. There exist other other axiomatisations too [61].

Chapter 7

Complete positivity

Up to now, we have only considered categorical models of *pure* states. But if we really want to take grouping systems together seriously as a primitive notion, we should also care about *mixed* states: if a compound system is in a pure state, but we only care about one constituent system and want to forget about the rest, the resulting state may be mixed. This means we have to add another layer of structure to our categories. This chapter studies a beautiful construction with which we don't have to step outside the realm of compact dagger categories after all, and brings together all the material from previous chapters. It revolves around *completely positive maps*.

Section 7.1 first abstracts this notion from standard quantum theory to the categorical setting. In Section 7.2, we then reformulate such morphisms into a convenient condition, and present the *CP construction*, which is central to this chapter. In the resulting categories, classical and quantum systems live on equal footing. We also prove an abstract version of Stinespring's theorem, characterizing completely positive maps in operational terms.

Subsequently we consider the two subcategories containing only classical systems and only quantum systems. Section 7.3 considers the former subcategory, and considers no-broadcasting theorems as mixed versions of the no-cloning theorem of Section 4.2.2. Section 7.4 axiomatizes the latter subcategory. Section 7.5 then axiomatizes the full CP construction. This lets us treat full-blown quantum teleportation categorically, complete with mixed states and classical communication. Finally, Section 7.6 shows that the CP construction respects linear structure.

7.1 Completely positive maps

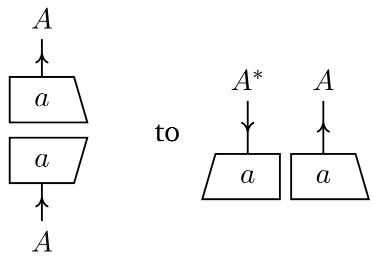
In this section we investigate evolution of mixed states of systems, by which we mean procedures that send mixed states to mixed states. First, we define mixed states themselves, as in Section 0.3.4, and then extrapolate. It turns out that the evolutions we are after correspond to completely positive maps, and mixed states are simply completely positive maps from the tensor unit I to a system.

7.1.1 Mixed states

So far we have defined a *pure state* as a morphism $I \xrightarrow{a} A$. To eventually arrive at a definition of mixed state that makes sense in arbitrary compact dagger categories, we proceed in four steps, analogous to Section 0.3.4.

The first step is to consider the induced morphism $p = a \circ a^\dagger \colon A \to A$ instead of $I \xrightarrow{a} A$. This is really just a switch of perspective, as we can recover a from p up to a physically unimportant phase. (We will make this precise later, in Lemma 7.38).

The second step is to switch from



(7.1)

Instead of a morphism $A \to A$ in a compact dagger category, we may equivalently work with matrices $I \to A^* \otimes A$ by taking names (see Definition 3.3). That is, a *matrix* is a state on $A^* \otimes A$. So no information is lost in this step; morphisms of the form $A \xrightarrow{a \circ a^\dagger} A$ turn out to correspond to certain so-called *positive matrices* $I \xrightarrow{m} A^* \otimes A$.

Definition 7.1 (Positive matrix, pure state)**.** In a monoidal dagger category, a *positive matrix* is a morphism $I \xrightarrow{m} A^* \otimes A$ that is the name $\ulcorner f^\dagger \circ f \urcorner$ of a positive morphism for some $A \xrightarrow{f} B$. If we can choose $B = I$, we call m a *pure state*.

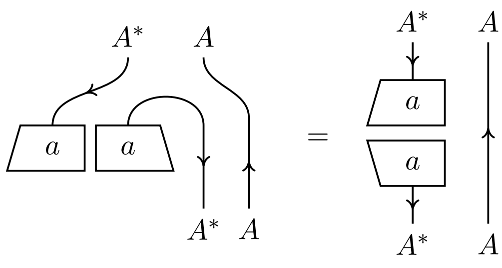
We will sometimes write $\sqrt{m}$ for f to indicate that m has a 'square root' and is hence positive. However, notice that such a morphism $\sqrt{m}$ is by no means unique.

Example 7.2. We examine positive matrices in our example categories.

- In **FHilb**, positive matrices correspond to linear maps $\mathbb{C} \to \mathbb{M}_n$ that send 1 to a positive matrix $f \in \mathbb{M}_n$; use Example 4.12. Pure states correspond to positive matrices of rank at most 1, that is, those of the form $|a\rangle\langle a|$ for a vector $a \in \mathbb{C}^n$. This is precisely what we called a *pure state* in Definition 0.66.
- In $\mathbf{Rel}$, positive matrices $I \to A \times A$ correspond to subsets $R \subseteq A \times A$ that are symmetric and satisfy aRa when aRb; see Exercise 2.5.7. The pure states are of the form $R = X \times X \subseteq A \times A$ for subsets $X \subseteq A$.

So far we have merely reformulated pure states. We now generalize from pure states to mixed states. The final two steps of our process reformulate and generalize this further.

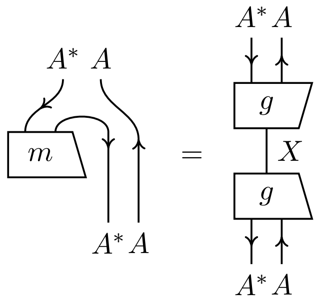
The third step is a conceptual leap, that moves from the positive matrix $I \xrightarrow{m} A^* \otimes A$ to the map $A^* \otimes A \to A^* \otimes A$ that multiplies on the left with the matrix m; compare also the Cayley embedding of Proposition 4.13:



(7.2)

This morphism is clearly positive. The following lemma shows the converse, so that this reformulation again loses no information.

Lemma 7.3. *In* **FHilb***, if a morphism* $I \xrightarrow{m} A^* \otimes A$ *satisfies*

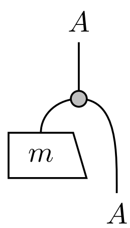


(7.3)

then it is a positive matrix.

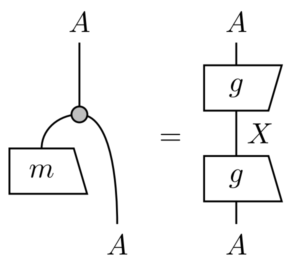
Proof. For any morphism $H \xrightarrow{f} H$ in **FHilb**, it follows from the Kronecker product (0.32) that $f \otimes \mathrm{id}_K$ is a block diagonal matrix; the $\dim(K)$ many diagonal blocks are simply the matrix of f. Hence $f \otimes \mathrm{id}_K$ is diagonalizable precisely when f is (and $\dim(K) > 0$), and the eigenvalues of $f \otimes \mathrm{id}_K$ are simply ($\dim(K)$ many copies of) the eigenvalues of f. In particular, if $\dim(K) > 0$ then $f \otimes \mathrm{id}_K$ is positive precisely when f is. Thus if (7.3) holds, then $m = \ulcorner f \urcorner$ for some positive morphism f, making m a positive matrix. $\square$

In the fourth and final step, we recognize in the left-hand sides of (7.2) and (7.3) the multiplication of the pair of pants monoid (see Lemma 5.9). Upgrade the pair of pants to an arbitrary Frobenius structure multiplication to obtain the generalization:



We have arrived at our definition of a mixed state.

Definition 7.4 (Mixed state)**.** In a monoidal dagger category, a *mixed state* of a dagger Frobenius structure $(A, \;, \;)$ is a morphism $I \xrightarrow{m} A$ satisfying the following equation, for some object X and some morphism $A \xrightarrow{g} X$:



(7.4)

We will sometimes write $\sqrt[\circ]{m}$ for such a morphism g, remembering that it is not necessarily unique.

Example 7.5. Let's examine this idea in our example categories.

- In **FHilb**, recall from Example 4.12 that the pair of pants monoid on $A = \mathbb{C}^n$ is precisely the algebra of n-by-n matrices. The mixed states come down to n-by-n matrices m satisfying $m = \sqrt{m}^\dagger \circ \sqrt{m}$ for some n-by-m matrix $\sqrt{m}$. Those are precisely the *mixed states*, or *density matrices*, of Definition 0.66.

  In general, recall from Theorem 5.32 that dagger Frobenius structures in **FHilb** correspond to finite-dimensional H*-algebras A. The mixed states $I \to A$ come down to those elements $a \in A$ satisfying $a = b^*b$ for some $b \in A$; these are usually called the *positive* elements.

- In $\mathbf{Rel}$, recall from Theorem 5.41 that special dagger Frobenius structures correspond to groupoids $\mathbf{G}$. Mixed states come down to subsets R of the morphisms of $\mathbf{G}$ such that the relation, defined by $g \sim h$ if and only if $h = r \circ g$ for some $r \in R$, is positive. Using Exercise 2.5.7, this boils down to: R is closed under inverses, and if $g \in R$, then also $\mathrm{id}_{\mathrm{dom}(g)} \in R$.

7.1.2 Completely positive maps

We may think of Frobenius structures as comprising *observables*, *i.e.* self-adjoint operators $A \to A$, as in Sections 5.3.2 and 5.4.1. This section develops the accompanying notion of morphism. Individual morphisms are regarded as physical processes, such as free or controlled time evolution, preparation, or measurement. They should therefore take (mixed) states to (mixed) states, and should be completely determined by their behaviour on (mixed) states. Such morphisms are abbreviated to *positive maps*, because they preserve positive elements; just as a linear map is one that preserves linear combinations.

Definition 7.6 (Positive map). In a monoidal dagger category, given dagger Frobenius structures $(A, ,)$ and $(B, ,)$, a *positive map* is a morphism $A \xrightarrow{f} B$ such that $I \xrightarrow{f \circ m} B$ is a mixed state whenever $I \xrightarrow{m} A$ is a mixed state.

Warning: note the difference with *positive-semidefinite* morphisms $f = g^\dagger \circ g$, that we have abbreviated to *positive morphisms* in Chapter 0 and Definition 2.34; luckily contexts will hardly arise where it's difficult to differentiate between these.

Instead of mixed states $I \xrightarrow{m} A$ and morphisms $A \xrightarrow{f} B$, we could dualize to effects $A \to I$ and morphisms $B \xrightarrow{f^\dagger} A$. Rather than f mapping states to states, $f^\dagger$ will map effects to effects in the other direction. This is the difference between the *Schrödinger picture* and the *Heisenberg picture*. In the former, observables stay fixed, while states evolve over time. In the latter, states stay fixed, while observables (effects) evolve over time. Although both pictures are equivalent, we will mostly adhere to the Schrödinger one.

However, positive maps are not yet the 'right' morphisms, precisely because they forget about the main premise of this book: always take compound systems into account! If f and g are physical channels, then we would like $f \otimes g$ to be a physical channel, too. Specifically, we would like $f \otimes \mathrm{id}_E$ to be a positive map for any Frobenius structure E and any positive map $A \xrightarrow{f} B$. We might only be interested in the system A, but we can never be completely sure that we have isolated it from the environment E. To account for the dynamics of such *open systems* we have to use *completely positive* maps.

Definition 7.7 (Completely positive map)**.** In a symmetric monoidal dagger category, given dagger Frobenius structures $(A, ,)$ and $(B, ,)$, a *completely positive map* is a morphism $A \xrightarrow{f} B$ such that $f \otimes \mathrm{id}_E$ is a positive map for any dagger Frobenius structure $(E, ,)$.

The next two subsections investigate the completely positive maps in our example categories $\mathbf{FHilb}$ and $\mathbf{Rel}$.

This definition perhaps seems not particularly useful, since it involves a quantification over all dagger Frobenius structures $(E, ,)$. But Theorem 7.18 below shows that it is equivalent to a property of f which can be checked directly.

7.1.3 Evolution and measurement

In the category $\mathbf{FHilb}$, Definition 7.7 is precisely the traditional definition of completely positive maps; that's how we engineered it. They bring evolution, measurement, and preparation on an equal footing.

Example 7.8. The following are completely positive maps in $\mathbf{FHilb}$:

- *Unitary evolution*: letting an n-by-n matrix m evolve freely along a unitary u to $u^\dagger \circ m \circ u$ is a completely positive map. With Example 4.12 we can phrase it as the map $A^* \otimes A \xrightarrow{u_* \otimes u} A^* \otimes A$, from a pair of pants Frobenius structure to itself, where $A = \mathbb{C}^n$.

- Let $A \xrightarrow{p_1, \ldots, p_n} A$ form a projection-valued measure with n outcomes (see Definition 0.61). Then the function $\mathbb{C}^n \to A^* \otimes A$ that sends the computational basis vector $|i\rangle$ to p_i is a completely positive map, from the classical structure $\mathbb{C}^n$ to the pair of pants Frobenius structure $A^* \otimes A$.

  Note the direction: that of the Heisenberg picture. In Proposition 7.25 below, we will see that the choice of direction is arbitrary.

- More generally, if $A \xrightarrow{p_1, \ldots, p_n} A$ is a positive operator-valued measure (see Definition 0.69), $|i\rangle \mapsto p_i$ is still a completely positive map $\mathbb{C}^n \to A^* \otimes A$.

  In fact, the converse holds, too: if $\mathbb{C}^n \xrightarrow{p} A^* \otimes A$ is a completely positive map that preserves units, then $\{p(|1\rangle), \ldots, p(|n\rangle)\}$ is a positive operator-valued measure. Hence a completely positive map from a classical structure to a pair of pants Frobenius structure corresponds to a *measurement*, generalizing Lemma 5.57.

- A completely positive map $\mathbb{C} \to A^* \otimes A$ is precisely (the *preparation* of) a mixed state. This example generalizes to arbitrary braided monoidal dagger categories.

- More generally, suppose we would like to prepare one of n mixed states $A \xrightarrow{m_i} A$, depending on some input parameter $i = 1, \ldots, n$. We can phrase this as the map $\mathbb{C}^n \to A^* \otimes A$ given by $|i\rangle \mapsto m_i$, which is completely positive. We can therefore regard a completely positive map from a classical structure to a pair of pants Frobenius structure, as a *controlled preparation*.

7.1.4 Inverse-respecting relations

In our other running example, the category $\mathbf{Rel}$ of sets and relations, special dagger Frobenius structures correspond to groupoids by Theorem 5.41. Just like completely positive maps in **FHilb** only care about positivity, but not the full structure of multiplication of the involved Frobenius structure in terms of which positivity is defined, completely positive maps in $\mathbf{Rel}$ only care about inverses, but not the full structure of multiplication of the groupoid in terms of which inverses are defined.

Definition 7.9 (Inverse-respecting relation)**.** Let G and H be the sets of morphisms of groupoids $\mathbf{G}$ and $\mathbf{H}$. A relation $G \xrightarrow{R} H$ is said to *respect inverses* when gRh implies $g^{-1}Rh^{-1}$ and $\mathrm{id}_{\mathrm{dom}(g)}R\mathrm{id}_{\mathrm{dom}(h)}$.

Proposition 7.10. *In* $\mathbf{Rel}$*, a morphism* $\mathbf{G} \xrightarrow{R} \mathbf{H}$ *is completely positive if and only if it respects inverses.*

Proof. First assume R respects inverses. Let $\mathbf{K}$ be any groupoid; write G, H, K for the sets of morphisms of $\mathbf{G}, \mathbf{H}, \mathbf{K}$. Suppose $S \subseteq G \times K$ that is a mixed state, that is, by Example 7.5, that S is closed under inverses and identities. Then $(R \times \mathrm{id}) \circ S$ is $\{(h, k) \in H \times K \mid \exists g \in G\colon (g, k) \in S, (g, k) \in R\}$. This is clearly closed under inverses and identities again, so R is completely positive.

Conversely, suppose R is completely positive. Take $\mathbf{K} = \mathbf{G}$, and let $a \xrightarrow{g} b$ be a morphism in $\mathbf{G}$. Define $S = \{(g, g), (g^{-1}, g^{-1}), (\mathrm{id}_a, \mathrm{id}_a), (\mathrm{id}_b, \mathrm{id}_b)\}$. This is a mixed state, hence so is $(R \times \mathrm{id}) \circ S$, which equals

$$\{(h, g) \mid gRh\} \cup \{(h, g^{-1}) \mid g^{-1}Rh\} \cup \{(h, \mathrm{id}_a) \mid \mathrm{id}_a Rh\} \cup \{(h, \mathrm{id}_b) \mid \mathrm{id}_b Rh\}.$$

If gRh, it follows that $g^{-1}Rh^{-1}$, and $\mathrm{id}_a R\mathrm{id}_{\mathrm{dom}(h)}$, so R respects inverses. $\square$

The characterization of completely positive maps in $\mathbf{Rel}$ of the previous proposition is the source of many ways in which $\mathbf{Rel}$ differs from **FHilb**. In other words, even though we have sketched $\mathbf{Rel}$ as a model of 'possibilistic quantum mechanics', it is a *nonstandard model* of quantum mechanics. It provides counterexamples to many features that are sometimes thought to have a quantum nature but turn out to be 'accidentally' true in **FHilb**. See for example Section 7.3.2 later. For another example: a positive map between Frobenius structures in **FHilb**, at least one of which is commutative, is automatically completely positive. The same is not true in $\mathbf{Rel}$.

Example 7.11 (The need for complete positivity)**.** The following relation $(\mathbb{Z}, +, 0) \xrightarrow{R} (\mathbb{Z}, +, 0)$ is positive but not completely positive:

$$R = \{(n, n) \mid n \geq 0\} \cup \{(n, -n) \mid n \geq 0\} = \{(|n|, n) \mid n \in \mathbb{Z}\}.$$

Hence complete positivity is strictly stronger than positivity.

Proof. Let $I \xrightarrow{m} \mathbb{Z}$ be a nonzero mixed state. We may equivalently consider the subset $S = \{n \in \mathbb{Z} \mid (*, n) \in m\} \subseteq \mathbb{Z}$ satisfying $0 \in S$ and $S^{-1} \subseteq S$ by Proposition 7.10. Now $(*, n) \in R \circ m$ if and only if $|n| \in S$, if and only if $-n, n \in S$, if and only if $(*, -n) \in R \circ m$. Trivially also $(*, 0) \in R \circ m$. Thus $R \circ m$ is a mixed state, and R is a positive map.

However, R is not completely positive because it clearly does not respect inverses: $(1, 1) \in R$ but not $(-1, -1) \in R$. $\square$

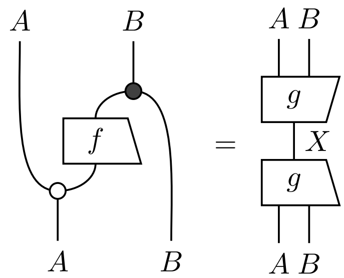
7.2 Categories of completely positive maps

This section describes the main construction of the chapter: starting with a category of pure states, it constructs the corresponding category of mixed states. We start by characterizing Definition 7.7 of completely positive maps from an operational form into a more convenient structural form.

7.2.1 The CP condition

A mixed state of a Frobenius structure $(A, \curlywedge_{\circ}, \circ)$ is the special case of a completely positive map $I \to A$, as illustrated in Example 7.5. The condition characterizing when a map is completely positive that we will use generalizes equation (7.4).

Definition 7.12 (CP condition)**.** In a monoidal dagger category, given dagger Frobenius structures $(A, \curlywedge_{\circ}, \circ)$ and $(B, \curlywedge_{\bullet}, \bullet)$, a morphism $A \xrightarrow{f} B$ satisfies the *CP condition* when



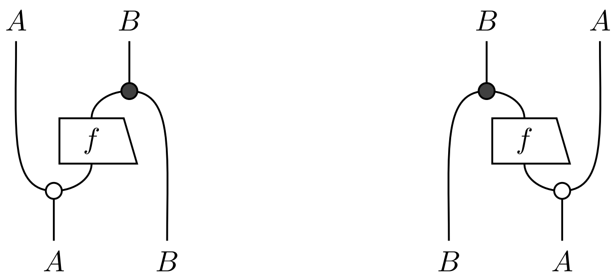
(7.5)

for some object X and some morphism $A \otimes B \xrightarrow{g} X$. In other words, the left-hand composite is a positive morphism.

Notice the similarity of the CP condition (7.5) to the Frobenius identity (5.4), and also to the oracles of Definition 6.12; the latter required the left-hand side to be unitary, whereas the CP condition requires it to be positive. The object X is called the *ancilla system*. The map g is called a *Kraus morphism*, and is also written $\sqrt[\circ]{f}$, although it is not unique.

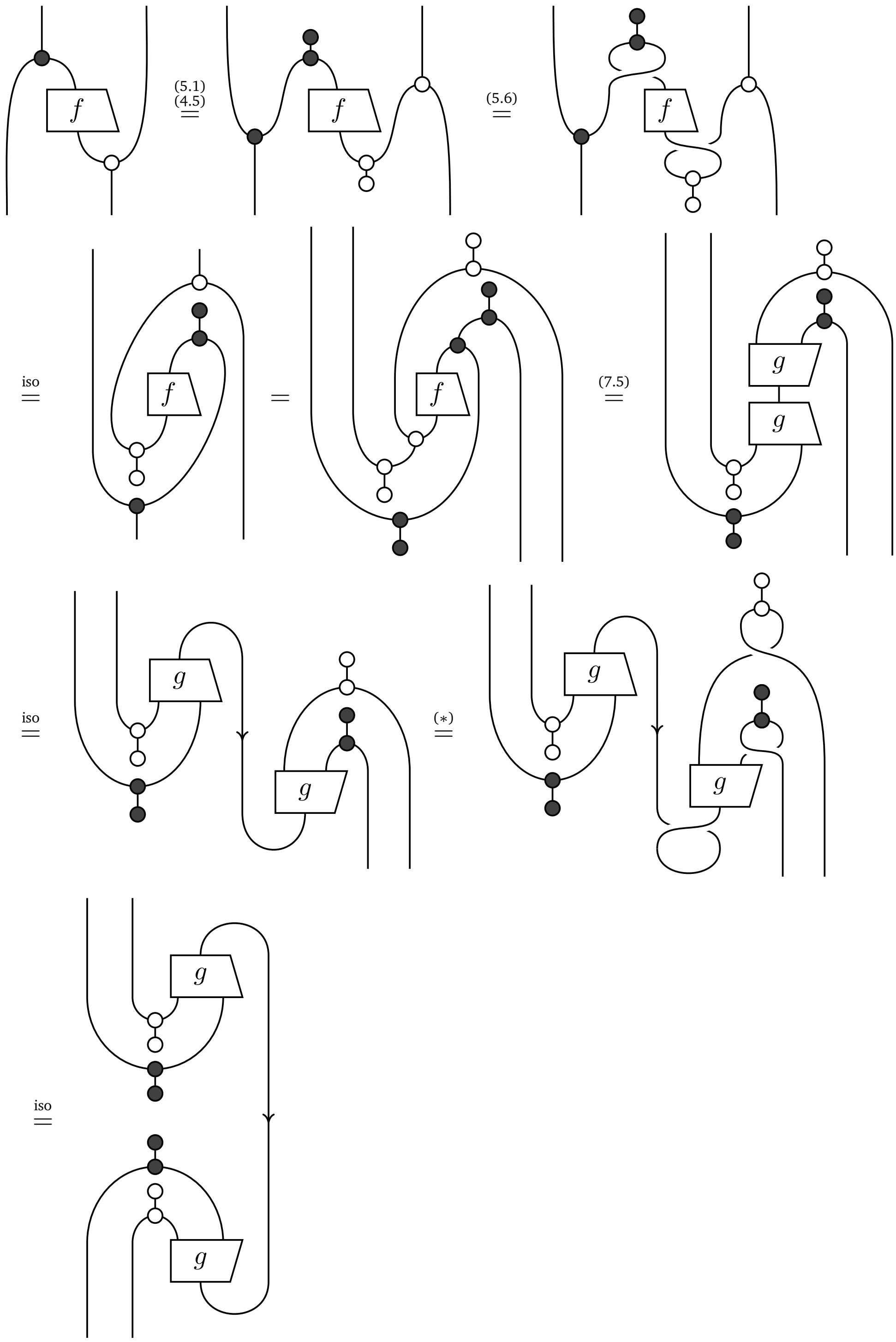
The CP condition is asymmetrical, in the sense that we could instead have had the white comultiplication to the right, and the black multiplication to the left. While these two conditions are different in general, for our example categories $\mathbf{Hilb}$ and $\mathbf{Rel}$ they are equivalent for symmetric dagger Frobenius structures.

Proposition 7.13. *In a dagger ribbon category with trivial twist, let* $(A, \curlywedge_{\circ}, \circ)$ *and* $(B, \curlywedge_{\bullet}, \bullet)$ *be symmetric dagger Frobenius structures. If one of the following composites is positive, then both are:*



(7.6)

Proof. We show that if the first composite above is positive, then so is the second:



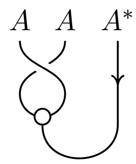
The step marked (∗) applies symmetry (5.6) of the Frobenius structures, and also triviality of the twist. The final composite is positive by construction. The reverse implication holds similarly. □

To prove that completely positive maps indeed satisfy the CP condition, we will need the same mild assumption as we did in the third step of Section 7.1.1. Namely that if $(A, \;, \;)$ is a dagger Frobenius structure, B is not a zero object, and $f \otimes \mathrm{id}_B$ for

$A \otimes B \xrightarrow{f} A \otimes B$ is a positive morphism (*i.e.* is of the form $g^\dagger \circ g$ for some g), then f itself is already positive. Let's call a category with this property *positively monoidal*. This requirement is satisfied when is an invertible scalar, for example; it is also satisfied when A is a zero object. Intuitively, this requirement demands that the dimension of a Frobenius structure is zero or invertible, which is the case in both of our running example categories **FHilb** and **Rel**.

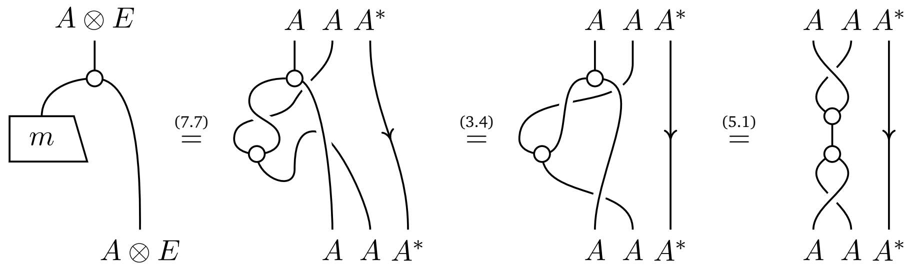
Lemma 7.14 (Complete positivity implies CP)**.** *In a braided monoidal dagger category which is positively monoidal, given dagger Frobenius structures $(A, ,)$ and $(B, ,)$, if $A \xrightarrow{f} B$ is completely positive then it satisfies the CP condition.*

Proof. Notice that A supports a dagger Frobenius structure and hence has a dual object A^* (which can be taken to be A itself) by Theorem 5.15. Let E be the pair of pants monoid $A \otimes A^*$, and define $I \xrightarrow{m} A \otimes E$ as:

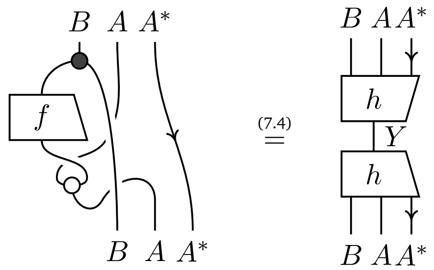


(7.7)

Then m is a mixed state:

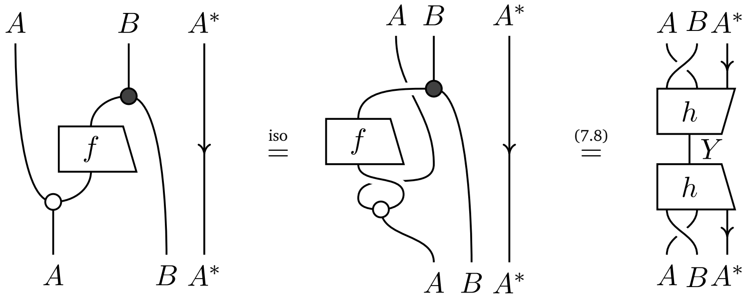


The first equality just unfolds the definition of m and the composite Frobenius structure on $A \otimes E$, the second equality uses a snake equation 3.4, whereas the third equality uses the Frobenius law. Now $(f \otimes \mathrm{id}_E) \circ m$ is a mixed state:



(7.8)

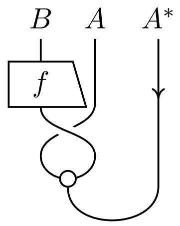
for some object Y and morphism h. Hence:



Because the category is positively monoidal, equation (7.5) now follows. □

Let us highlight an element of the proof of the previous lemma that we will use again.

Definition 7.15 (Choi matrix)**.** In a braided monoidal dagger category, given symmetric dagger Frobenius structures $(A, \curlywedge_{\circ}, \circ)$ and $(B, \curlywedge_{\bullet}, \bullet)$, the *Choi matrix* of a completely positive map $A \xrightarrow{f} B$ is the mixed state $(f \otimes \mathrm{id}) \circ m \colon I \to B \otimes (A \otimes A^*)$:

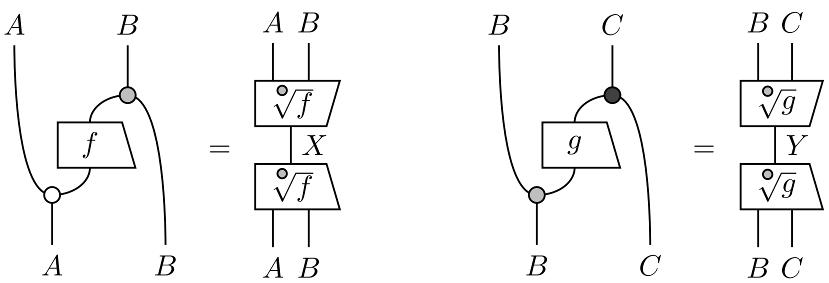


It is the transform under the Choi-Jamiołkowski isomorphism of the completely positive map.

We will shortly prove the converse of the previous lemma, but to prepare first show that the CP condition is well-behaved with respect to composition and tensor products.

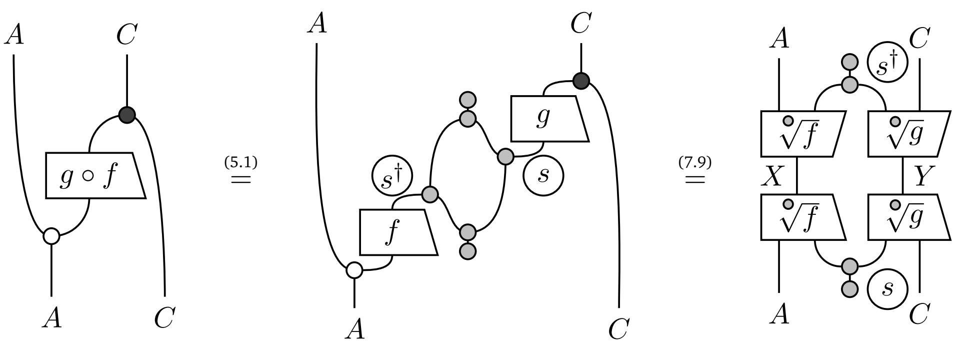
Lemma 7.16 (CP maps compose)**.** *In a monoidal dagger category, let* $(A, \curlywedge_{\circ}, \circ)$, $(B, \curlywedge_{\circ}, \circ)$*, and* $(C, \curlywedge_{\bullet}, \bullet)$ *be dagger Frobenius structures, such that there exists a scalar* s *with* $s^\dagger \bullet\!\!\oslash\!\!\bullet\, s = \mathrm{id}_B$*. If* $A \xrightarrow{f} B$ *and* $B \xrightarrow{g} C$ *satisfy the CP condition, then so does* $A \xrightarrow{g \circ f} C$*.*

Proof. Suppose that objects X, Y and morphisms $\sqrt[\circ]{f}$, $\sqrt[\circ]{g}$ satisfy the following:



(7.9)

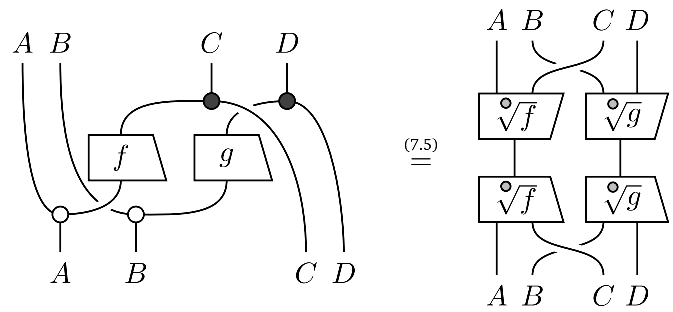
Then $g \circ f$ satisfies the CP condition:



This uses the Frobenius law to insert a 'handle' $s^\dagger \bullet\!\!\oslash\!\!\bullet\, s$. □

Lemma 7.17 (Product CP maps)**.** *In a braided monoidal dagger category, let* $(A, \whitemult, \whiteunit)$*,* $(B, \blackmult, \blackunit)$*,* $(C, \whitemult, \whiteunit)$*, and* $(D, \blackmult, \blackunit)$ *be dagger Frobenius structures. If* $(A, \whitemult, \whiteunit) \xrightarrow{f} (B, \blackmult, \blackunit)$ *and* $(C, \whitemult, \whiteunit) \xrightarrow{g} (D, \blackmult, \blackunit)$ *satisfy the CP condition, then so does* $(A, \whitemult, \whiteunit) \otimes (C, \whitemult, \whiteunit) \xrightarrow{f \otimes g} (B, \whitemult, \whiteunit) \otimes (D, \whitemult, \whiteunit)$*. Here,* $A \otimes C$ *and* $B \otimes D$ *carry the product Frobenius structure of Lemma 4.8 (see also Exercise 5.7.1).*

Proof. Suppose $\sqrt[\circ]{f}$ and $\sqrt[\circ]{g}$ are Kraus morphisms for f and g. Then:



This proves the lemma. $\square$

7.2.2 Stinespring's theorem

We now prove that the CP condition characterizes completely positive maps. Notice that the proof of Lemma 7.14 did not need arbitrary ancilla systems E, and pair of pants monoids sufficed. The following theorem will also record that.

Theorem 7.18 (Stinespring)**.** *Consider a symmetric monoidal dagger category which is positively monoidal, where each symmetric Frobenius structure has a scalar* d *such* $d^\dagger \bullet \phi \bullet d = \mathrm{id}$*. For symmetric dagger Frobenius structures* $(A, \whitemult, \whiteunit)$ *and* $(B, \whitemult, \whiteunit)$ *and a morphism* $A \xrightarrow{f} B$*, the following are equivalent:*

(a) f *is completely positive;*

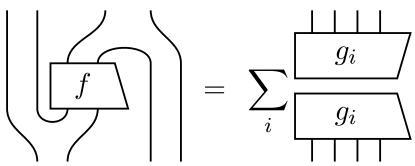
(b) $f \otimes \mathrm{id}_E$ *is a positive map for all objects* X*, where* $E = (X^* \otimes X, \pantsmult, \cup)$*;*

(c) f *satisfies the CP condition* (7.5).

Proof. Clearly (a) implies (b). Lemma 7.14 shows that (b) implies (c). Finally, to show that (c) implies (a), let $I \xrightarrow{m} (A, \whitemult, \whiteunit) \otimes (E, \whitemult, \whiteunit)$ be a mixed state. Then m is a completely positive map and so satisfies the CP condition. Hence, by Lemmas 7.16 and 7.17, also $(f \otimes \mathrm{id}_E) \circ m$ satisfies the CP condition and is thus a mixed state. $\square$

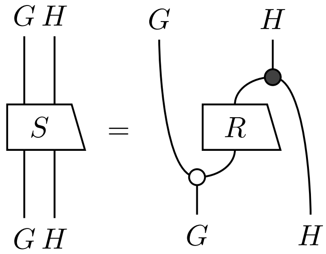
Example 7.19. Let's unpack what the previous theorem says in our example categories **FHilb** and **Rel**.

- For a completely positive map $A^* \otimes A \xrightarrow{f} A^* \otimes A$ in **FHilb**, for $A = \mathbb{C}^n$, so on n-by-n matrices, the CP condition (7.5) becomes



by choosing a basis $|i\rangle$ for the ancilla system and indexing the Kraus morphisms g_i accordingly. Putting a cap on the top left and a cup on the bottom right we see that this is equivalent to $f(m) = \sum_i f_i^\dagger \circ m \circ f_i$ for matrices m. This generalizes Example 7.8, and we recognize the previous theorem as Stinespring's theorem, or rather Choi's finite-dimensional version of it.

- In $\mathbf{Rel}$, a relation $\mathbf{G} \xrightarrow{R} \mathbf{H}$ between groupoids satisfies the CP condition when the relation



$$= \{\big((g_1,h_1),(g_2,h_2)\big) \mid (g_2^{-1} \circ g_1) R (h_2 \circ h_1^{-1})\}$$

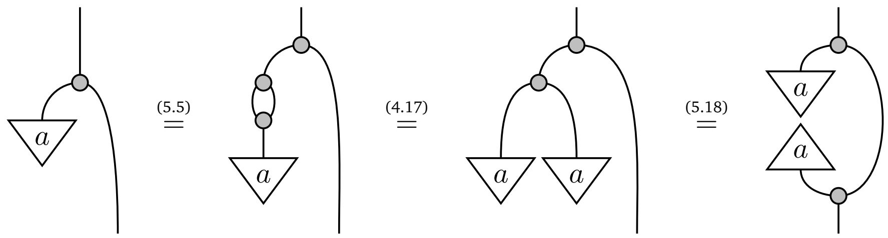
is positive. This is the case when it is symmetric and satisfies $(g,h)S(g,h)$ when $(g,h)S(g',h')$ (see Exercise 2.5.7), matching Proposition 7.10 as follows.

First, S is symmetric when $(g_2^{-1} \circ g_1)R(h_2 \circ h_1^{-1}) \Leftrightarrow (g_1^{-1} \circ g_2)R(h_1 \circ h_2^{-1})$. Taking g_2 and h_1 to be identities shows that this means $gRh \Leftrightarrow g^{-1}Rh^{-1}$ for all $g \in G$ and $h \in H$. Similarly, S satisfies the other property when $(g_2^{-1} \circ g_1)R(h_2 \circ h_1^{-1})$ implies $\mathrm{id}_{\mathrm{dom}(g_1)} R \,\mathrm{id}_{\mathrm{dom}(h_1^{-1})}$. But this means precisely that gRh implies $\mathrm{id}_{\mathrm{dom}(g)} R \,\mathrm{id}_{\mathrm{dom}(h)}$.

For another example, we can now prove that copyable states are always completely positive maps, generalizing Example 7.8.

Corollary 7.20. *In a symmetric monoidal dagger category, given a classical structure* $(A, \ , \ )$*, any self-conjugate copyable state* $I \xrightarrow{a} A$ *is a completely positive map.*

Proof. Graphical manipulation:



This used specialness, copyability, self-conjugateness and the Spider Theorem 5.22. □

7.2.3 The CP construction

We are now ready to define the main construction of this chapter. It takes a compact dagger category $\mathbf{C}$ modelling systems and pure processes, and lifts it to a new compact dagger category $\mathrm{CP}[\mathbf{C}]$ of systems and mixed processes. We build it up in stages, seeing how extra structure on $\mathbf{C}$ endows $\mathrm{CP}[\mathbf{C}]$ with extra structure.

Proposition 7.21 (CP as a category)**.** *Given a monoidal dagger category* $\mathbf{C}$*, there is a category* $\mathrm{CP}[\mathbf{C}]$ *in which:*

- *objects are special symmetric dagger Frobenius structures in* **C***;*
- *morphisms are morphisms of* **C** *that satisfy the CP condition.*

Proof. Identities in **C** satisfy the CP condition precisely because of the Frobenius law, and Lemma 7.16 shows that composition preserves the CP condition. □

A braiding on **C** gives monoidal structure to $\mathrm{CP}[\mathbf{C}]$.

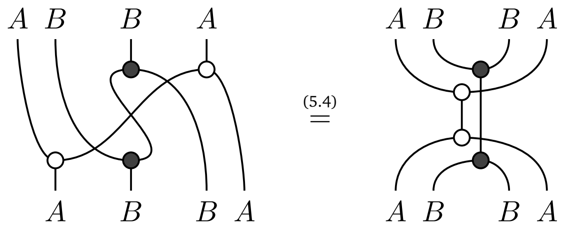
Proposition 7.22 (CP monoidal structure)**.** *If* **C** *is braided monoidal dagger category, then* $\mathrm{CP}[\mathbf{C}]$ *is a monoidal category in which:*

- *the tensor product of objects is that of Lemma 4.8;*
- *the tensor product of morphisms is well-defined by Lemma 7.17;*
- *the tensor unit is* I *with multiplication* $I \otimes I \xrightarrow{\rho_I} I$ *and unit* $I \xrightarrow{\mathrm{id}_I} I$*;*
- *the coherence isomorphisms* α*,* λ*, and* ρ*, are inherited from* **C***.*

Proof. The tensor unit I is a well-defined special dagger Frobenius structure by the coherence theorem. (For the tensor product of objects, see also Exercise 5.7.1.) Using these definitions of $\otimes$ and I, the unitary coherence isomorphisms α, λ, and ρ, from **C** trivially satisfy the CP condition. Thus $\mathrm{CP}[\mathbf{C}]$ is a well-defined monoidal category. □

Proposition 7.23 (CP preserves symmetric monoidal structure)**.** *If* **C** *is a symmetric monoidal dagger category, then the monoidal category* $\mathrm{CP}[\mathbf{C}]$ *is symmetric.*

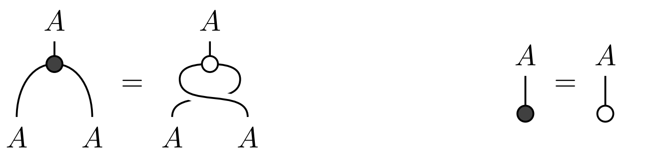
Proof. We must check that the symmetry morphisms satisfy the CP condition:



This is valid by the Frobenius law. □

It might look like the following result shows that the CP construction fabricates dual objects out of thin air. But note that they were already present in **C**, since by Theorem 5.15, any object admitting a Frobenius structure must be self-dual.

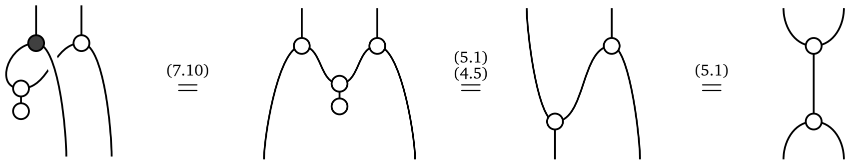
Proposition 7.24 (CP constructs duals)**.** *In a braided monoidal dagger category* **C***, given a special dagger Frobenius structure* $(A, \circ, \circ)$*, define a new such structure as follows:*



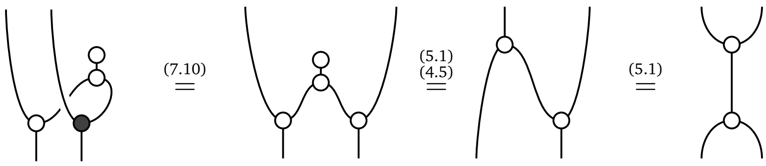
(7.10)

Then $(A, \circ, \circ) \dashv (A, \bullet, \bullet)$ *in* $\mathrm{CP}[\mathbf{C}]$.

Proof. Easy graphical manipulations show that $(A, ,)$ again satisfies associativity, unitality, the Frobenius law, and specialness. Hence we have two well-defined objects $L = (A, ,)$ and $R = (A, ,)$ of $\mathrm{CP}[\mathbf{C}]$. Next, define $=$: $I \to R \otimes L$. We show that this is a well-defined morphism in $\mathrm{CP}[\mathbf{C}]$ by checking the CP condition:



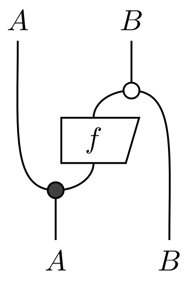
The first equality unfolds definitions and uses naturality of braiding, and the last two apply the Frobenius law and unitality. Similarly, $=$: $L \otimes R \to I$ is completely positive:



Because composition in $\mathrm{CP}[\mathbf{C}]$ is as in $\mathbf{C}$, the snake equations come down precisely to the Frobenius law. Thus and witness $L \dashv R$ in $\mathrm{CP}[\mathbf{C}]$. □

Proposition 7.25 (CP preserves daggers)**.** *If* $\mathbf{C}$ *is a ribbon dagger category with trivial twist, then* $\mathrm{CP}[\mathbf{C}]$ *is a dagger category.*

Proof. Let $(A, ,)$ and $(B, ,)$ be symmetric dagger Frobenius structures in $\mathbf{C}$, and suppose that $A \xrightarrow{f} B$ satisfies the CP condition (7.5). Then the CP condition for $f^\dagger$ comes down to the following composite being positive:



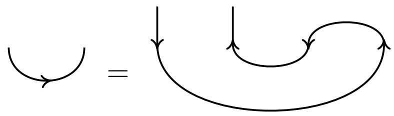
Apply Proposition 7.13 to f, and observe that the composite denoted above is the dagger of the second condition (7.6). □

Finally, the CP construction preserves dagger compact structure.

Proposition 7.26 (CP preserves dagger compactness)**.** *If* $\mathbf{C}$ *is a dagger compact category, then so is* $\mathrm{CP}[\mathbf{C}]$.

Proof. Combining Proposition 7.23, Proposition 7.24 and Proposition 7.25, we see that $\mathrm{CP}[\mathbf{C}]$ is a symmetric monoidal category with duals, and with a dagger structure. We must show that the dualities in $\mathrm{CP}[\mathbf{C}]$ are dagger dualities. Using the notation $L \dashv R$ of Proposition 7.24,

satisfy the CP condition, as both are the composition of the swap map and the dagger of a map we have already shown to satisfy the CP condition. The snake equations come down to the Frobenius law. By definition:



So in this case L and R are dagger dual objects in $\mathrm{CP}[\mathbf{C}]$. □

Example 7.27. Consider these structures on CP for our example categories.

- It follows immediately from Theorem 5.32 and Theorem 7.18 that $\mathrm{CP}[\mathbf{FHilb}]$ is the category of finite-dimensional H*-algebras and completely positive maps, and that this is a compact dagger category. This was the original motivation for the CP construction. By Corollary 3.65 and Theorem 5.15, we see that $\mathrm{CP}[\mathbf{Hilb}] = \mathrm{CP}[\mathbf{FHilb}]$ is the same category of finite-dimensional H*-algebras and completely positive maps.

- Similarly, Theorem 5.41 and Proposition 7.10 say that $\mathrm{CP}[\mathbf{Rel}]$ is the category of groupoids and inverse-respecting relations, which is a compact dagger category.

7.3 Classical structures

This section considers completely positive maps to and from classical structures. We will see that the subcategory of classical structures and completely positive maps models statistical mechanics, as expected when taking mixed states of classical systems.

Definition 7.28 (The $\mathrm{CP_c}$ construction)**.** Given a braided monoidal dagger category $\mathbf{C}$, we define the category $\mathrm{CP_c}[\mathbf{C}]$ as follows: objects are classical structures, and morphisms are completely positive maps.

As before, if $\mathbf{C}$ is compact, then so is $\mathrm{CP_c}[\mathbf{C}]$. In fact, according to Proposition 7.24, any object in $\mathrm{CP_c}[\mathbf{C}]$ is self-dual.

As for examples: the next subsection investigates $\mathrm{CP_c}[\mathbf{FHilb}]$. In the case of $\mathbf{Rel}$, completely positive maps between classical structures have no well-known simplification. All we can say is that $\mathrm{CP_c}[\mathbf{Rel}]$ consists of abelian groupoids and inverse-respecting relations.

7.3.1 Stochastic matrices

If $\mathbf{C}$ models pure state quantum mechanics, and $\mathrm{CP}[\mathbf{C}]$ mixed state quantum mechanics, then $\mathrm{CP_c}[\mathbf{C}]$ models *statistical mechanics*.

Example 7.29. The category $\mathrm{CP_c}[\mathbf{FHilb}]$ is monoidally equivalent to the following category: objects are natural numbers, and morphisms $m \to n$ are m-by-n matrices whose entries are nonnegative real numbers. The maps that preserve counits correspond to those matrices whose rows sum up to one, *i.e. stochastic matrices*.

Proof. In **FHilb**, classical structures $(H, \curlywedge, \bullet)$ correspond to a choice of orthonormal basis on H by Theorem 5.36. Hence we may identify linear maps between them with matrices. The positive elements of the classical structure corresponding to the standard basis on $\mathbb{C}^n$ are by definition precisely the vectors whose coordinates are nonnegative real numbers. By Theorem 7.18, a completely positive map $\mathbb{C}^m \xrightarrow{f} \mathbb{C}^n$ must make $f(|i\rangle)$ a positive element of $\mathbb{C}^n$. Combining the last two facts shows that f's matrix has nonnegative real entries $\langle j|f|i\rangle$.

Conversely, any special dagger Frobenius structure H in **FHilb** has an orthonormal basis $|k\rangle$ of positive elements by Theorem 5.32. To verify that $f \otimes \mathrm{id}_H \colon \mathbb{C}^m \otimes H \to \mathbb{C}^n \otimes H$ is a positive morphism, it suffices to observe that it sends $|i\rangle \otimes |k\rangle$ to the positive element $f(|i\rangle) \otimes |k\rangle$.

The counit of the classical structure $\mathbb{C}^n$ is $(x_1, \ldots, x_n) \mapsto x_1 + \cdots + x_n$. So $\mathbb{C}^m \xrightarrow{f} \mathbb{C}^n$ preserves counits when $\sum_{i=1}^{n} \langle j|f|i\rangle = 1$. □

The previous example is consistent with the morphisms between classical structures studied in Chapter 5. Corollary 5.37 showed that comonoid homomorphisms between classical structures correspond to matrices where every column has a single 1, and all the other entries 0. These are the *deterministic* maps within the stochastic setting of the previous example. Lemma 5.38 showed that these are self-conjugate, which means that their matrix entries are real numbers.

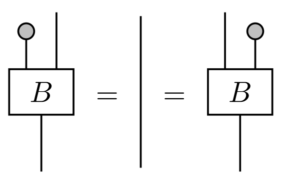
7.3.2 Broadcasting

We now come full circle after Chapter 4, which showed that compact dagger categories do not support uniform copying and deleting. That fact does not yet guarantee that they model quantum mechanics. Classical mechanics might have uniform copying, and quantum mechanics might not, but statistical mechanics has no copying either. What sets quantum mechanics apart is the fact that *broadcasting* of unknown mixed states is impossible. Before we can get to the precise definition, we have to make sure that there exist *discarding* morphisms $A \to I$ in $\mathrm{CP}[\mathbf{C}]$.

Lemma 7.30. *In a braided monoidal dagger category, given a dagger Frobenius structure $(A, \curlywedge, \bullet)$, then $\bullet$ satisfies the CP condition. If additionally $(A, \curlywedge, \bullet)$ is a commutative, then $\curlywedge$ satisfies the CP condition.*

Proof. Verifying the CP condition (7.5) for $\bullet$ just comes down to unitality and the fact that the identity is positive. If $\curlywedge$ is commutative, the CP condition for $\curlywedge$ can be verified using the spider Theorem 5.21. □

Definition 7.31. In a braided monoidal dagger category **C**, given a dagger Frobenius structure $(A, \curlywedge, \bullet)$, a *broadcasting map* is a morphism $(A, \curlywedge, \bullet) \xrightarrow{B} (A \otimes A, \curlywedge\curlywedge, \bullet\,\bullet)$ in $\mathrm{CP}[\mathbf{C}]$ satisfying the following equation:



(7.11)

The structure $(A, ,)$ is called *broadcastable* if it admits a broadcasting map.

Notice that the definition of broadcasting concerns just a single object, and is therefore much weaker than Definition 4.21 of uniform copying. It is therefore reasonable that every classical structure has a broadcasting map.

Lemma 7.32. *In a braided monoidal dagger category, commutative dagger Frobenius structures are broadcastable.*

Proof. Let $(A, ,)$ be a classical structure; we will show that is a broadcasting map. It clearly satisfies (7.11), so it suffices to show that it is a well-defined morphism in $\mathrm{CP}[\mathbf{C}]$. This follows directly from Lemma 7.30. $\square$

In **FHilb**, the converse to the previous lemma holds; this is the so-called *no-broadcasting theorem*. So a dagger Frobenius structure in **FHilb** is broadcastable if and only if it is a classical structure. However, this is not the case in **Rel**. Recall that a groupoid is skeletal when its only morphisms are endomorphisms.

Lemma 7.33. *In* **Rel***, a dagger Frobenius structure is broadcastable precisely when it corresponds to a skeletal groupoid.*

Proof. Let $\mathbf{G}$ be a skeletal groupoid, and write G for its set of morphisms. We will show that the morphism $G \xrightarrow{B} G \times G$ in **Rel** given by

$$B = \{\big(g, (\mathrm{id}_{\mathrm{dom}(g)}, g)\big) \mid g \in G\} \cup \{\big(g, (g, \mathrm{id}_{\mathrm{dom}(g)})\big) \mid g \in G\}$$

is a broadcasting map. First of all, B respects inverses because $\mathrm{id}_{\mathrm{dom}(g)} = \mathrm{id}_{\mathrm{dom}(g^{-1})}$ by total disconnectedness, so B is a well-defined morphism in $\mathrm{CP}[\mathbf{Rel}]$. When interpreted in **Rel**, the broadcastability equation (7.11) reads

$$\{(g, g) \mid g \in G\} = \{(g, h) \mid (g, (\mathrm{id}_C, h)) \in B \text{ for some object } C\} \tag{7.12}$$
$$\{(g, g) \mid g \in G\} = \{(g, h) \mid (g, (h, \mathrm{id}_C)) \in B \text{ for some object } C\}. \tag{7.13}$$

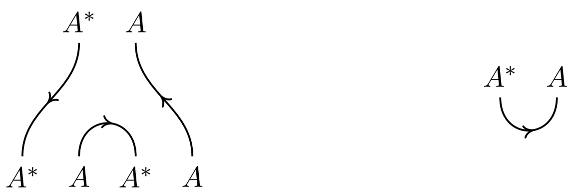
These equations are satisfied by construction of B, and so B is a broadcasting map for $\mathbf{G}$.

Conversely, suppose that a groupoid $\mathbf{G}$ is broadcastable, so that there is a morphism B in **Rel** respecting inverses and satisfying (7.12) and (7.13). Let g be a morphism in $\mathbf{G}$. There is an object C of $\mathbf{G}$ such that $(g, (\mathrm{id}_C, g)) \in B$ by (7.12). Since B respects inverses, then also $(\mathrm{id}_{\mathrm{dom}(g)}, (\mathrm{id}_C, \mathrm{id}_{\mathrm{dom}(g)})) \in B$. But then $C = \mathrm{dom}(g)$ by (7.13). On the other hand, as B respects inverses also $(g^{-1}, (\mathrm{id}_C, g^{-1})) \in B$. Again because B respects inverses then $(\mathrm{id}_{\mathrm{cod}(g)}, (\mathrm{id}_C, \mathrm{id}_{\mathrm{cod}(g)})) \in B$, and so $C = \mathrm{cod}(g)$ by (7.13). Hence $\mathrm{dom}(g) = \mathrm{cod}(g)$, and $\mathbf{G}$ is skeletal. $\square$

7.4 Quantum structures

Special dagger Frobenius structures fall on a spectrum, as discussed in Section 5.4.1. At the one extreme are the commutative ones. In this case all observables modeled by the Frobenius structure commute with each other, which is why we also call them classical structures. In a Frobenius structure in the middle of the spectrum, some pairs of observables will commute, but others will not. These Frobenius structures form a hybrid of classical observables and quantum observables. On the other extreme of the spectrum lie Frobenius structures that are 'completely noncommutative' in the sense that every observable that commutes with all others must be trivial. This section studies the subcategory of completely positive maps between such Frobenius structures. We define them simply as pair of pants.

Definition 7.34 (Quantum structure)**.** In a monoidal dagger category, given a dagger duality $A \dashv A^*$, a *quantum structure* is a dagger Frobenius structure on $A^* \otimes A$ of the following form:



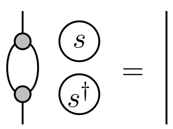
(7.14)

Example 7.35. We now examine quantum structures in **Hilb** and **Rel**.

- By Example 4.12, the quantum structures in **FHilb** are precisely the algebras $\mathbb{M}_n$ of n-by-n matrices. These are the operator algebras that are 'maximally noncommutative'.
- In **Rel**, the quantum structures are indiscrete groupoids by Corollary 5.42. These are the groupoids that are as far away from abelian groupoids (classical structures) as possible.

The matrix algebra $\mathbb{M}_n$ in the previous example is not a special Frobenius structure, and hence does not live in CP[**FHilb**]. We could have made it special by inserting a normalizing scalar (of $\frac{1}{\sqrt{n}}$) to remedy this. The following remark shows that it is harmless to disregard this difference, which we will do in the rest of this chapter.

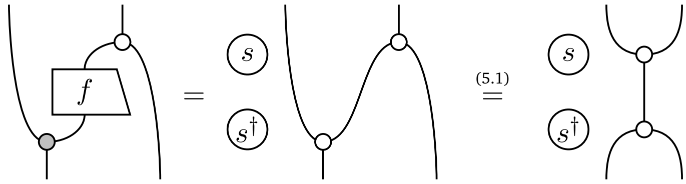
Remark 7.36 (Normalizability)**.** Look back at the proof that CP[**C**] is a well-defined monoidal dagger category, especially Lemma 7.16. We could have defined a more liberal category, whose morphisms are still those satisfying the CP condition, but whose objects are symmetric dagger Frobenius structures $(A, \cdot, \cdot)$ in the braided monoidal dagger category **C** that are *normalizable*, in the sense that



(7.15)

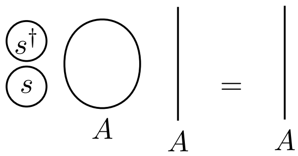
for some invertible scalar $I \xrightarrow{s} I$. However, any object of the new category is isomorphic to some object of CP[**C**]. Therefore the new category and CP[**C**] are monoidally equivalent as monoidal dagger categories.

Proof. Let $(A, \cdot, \cdot)$ be a normalizable symmetric dagger Frobenius structure. Define $= s \bullet$ and $= s^{-1} \bullet$. Unfolding the definitions shows that $(A, \cdot, \cdot)$ is a well-defined symmetric dagger Frobenius structure, and that it is special. Now define $f = s \bullet \mathrm{id}_A \colon A \to A$. We verify that this map $(A, \cdot, \cdot) \to (A, \cdot, \cdot)$ satisfies the CP condition:



Similarly, $f^{-1} = s^{-1} \bullet \mathrm{id}_A \colon A \to A$ satisfies the CP condition. As these two maps are inverses, we conclude that $(A, \ , \ ) \simeq (A, \ , \ )$ in the new category. □

Every object A with a dagger dual A^* in a monoidal dagger category $\mathbf{C}$ gives rise to a quantum structure on $A^* \otimes A$. Hence you might think that $\mathbf{C}$ lives inside $\mathrm{CP}[\mathbf{C}]$. But this is only true up to the normalization we are disregarding as in the previous remark. We need $\mathbf{C}$ to be *positive-dimensional*, in the sense that for each object A there is a scalar s satisfying:

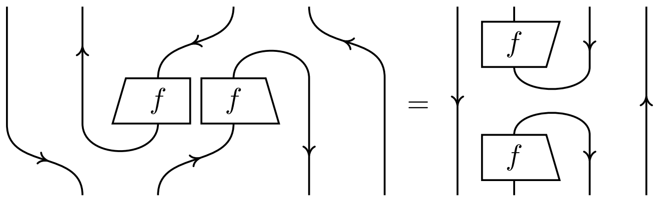


(7.16)

This mild property holds in both **Hilb** and **Rel**. The following proposition is the only time we will need this normalization.

Proposition 7.37 (CP embeds $\mathbf{C}$). *Let $\mathbf{C}$ be a braided monoidal dagger category with dagger duals that is positive-dimensional. There is a functor $P \colon \mathbf{C} \to \mathrm{CP}[\mathbf{C}]$ defined by letting $P(A)$ be the normalized pair of pants on $A^* \otimes A$, and by $P(f) = f_* \otimes f$ on morphisms. It is a monoidal functor. Moreover, if $\mathbf{C}$ is a compact dagger category, this functor preserves daggers.*

Proof. Let $A \xrightarrow{f} B$ in $\mathbf{C}$. We have to show that $P(f)$ satisfies the CP condition.



Daggers and tensor products in $\mathrm{CP}[\mathbf{C}]$ are by definition as in $\mathbf{C}$. □

Thus the pure world of $\mathbf{C}$ is 'embedded' inside the mixed world of $\mathrm{CP}[\mathbf{C}]$. But although we say 'embedded', the functor P is not faithful. It is only faithful up to a global phase, which is precisely what you would expect when regarding pure states as a special case of mixed states. Recall that a scalar $I \xrightarrow{s} I$ is a phase when its absolute value $s^\dagger \bullet s$ is id_I.

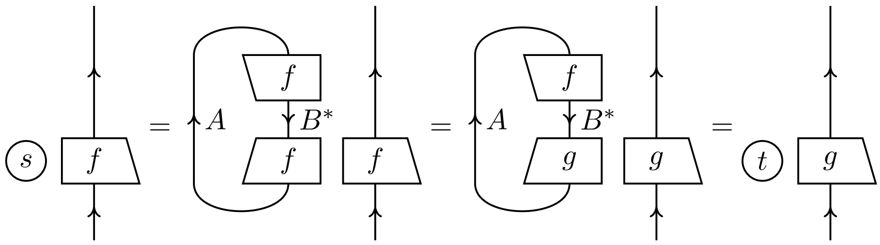
Lemma 7.38 (CP kills at most phases). *Given a braided monoidal dagger category with dagger duals which is positive-dimensional, let P be the functor of Proposition 7.37 and $A \xrightarrow{f,g} B$.*

(a) If $P(f) = P(g)$, then $s \bullet f = t \bullet g$ for some $I \xrightarrow{s,t} I$ with $s^\dagger \bullet s = t^\dagger \bullet t$.

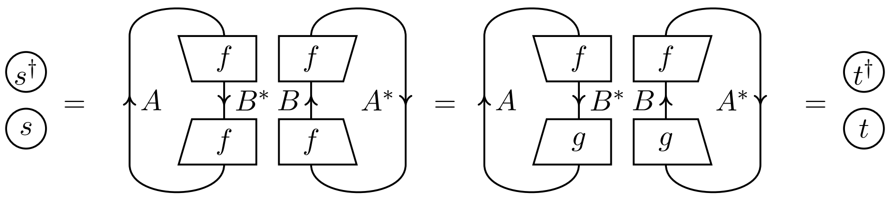
(b) If phases $I \xrightarrow{s,t} I$ satisfy $s \bullet f = t \bullet g$, then $P(f) = P(g)$.

Proof. The second part is obvious. For the first part, define:

Then:



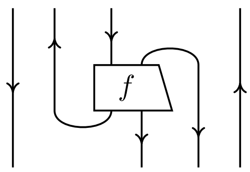
And:



Notice that this proof is completely graphical. □

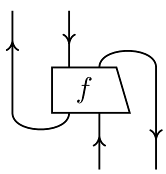
7.4.1 The category of quantum structures

Consider the subcategory of $\mathrm{CP}[\mathbf{C}]$ of all quantum structures in $\mathbf{C}$ and all CP morphisms between them. It can be described as follows. Objects are pair of pants monoids $A^* \otimes A$ in $\mathbf{C}$; we can abbreviate these to just the object A of $\mathbf{C}$ itself. The CP condition then simplifies to requiring



(7.17)

to be a positive morphism. For positively monoidal $\mathbf{C}$, the morphisms $A \to B$ simplify further to a morphism $A^* \otimes A \xrightarrow{f} B^* \otimes B$ whose Choi matrix



(7.18)

is positive.

Definition 7.39 (The $\mathrm{CP_q}$ construction)**.** Given a compact dagger category $\mathbf{C}$, we define the category $\mathrm{CP_q}[\mathbf{C}]$ as follows: objects are objects of $\mathbf{C}$, and morphisms $A \xrightarrow{f} B$ are morphisms $A^* \otimes A \xrightarrow{f} B^* \otimes B$ with positive Choi matrix.

Analogous results to those established in Section 7.2 also hold here; in particular, if $\mathbf{C}$ is a compact dagger category, then so is $\mathrm{CP_q}[\mathbf{C}]$. However, we may only regard $\mathrm{CP_q}[\mathbf{C}]$ as a subcategory of $\mathrm{CP}[\mathbf{C}]$ when $\mathbf{C}$ is positive-dimensional, as in Proposition 7.37.

Example 7.40. In our example categories:

- The category $\mathrm{CP_q}[\mathbf{FHilb}]$ consists of finite-dimensional Hilbert spaces H and completely positive maps $H^* \otimes H \to K^* \otimes K$. These are precisely the completely positive maps between matrix algebras.
- The category $\mathrm{CP_q}[\mathbf{Rel}]$ consists of sets A and relations $A \times A \to B \times B$ satisfying $(a, a) \sim (b, b)$ and $(a', a) \sim (b', b)$ when $(a, a') \sim (b, b')$. These are precisely the inverse-respecting relations between indiscrete groupoids with objects A and B.

7.4.2 Environment structures

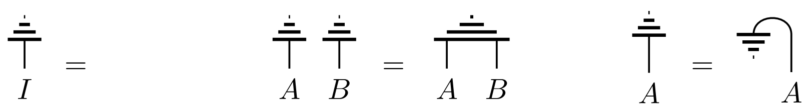
In categories of the form $\mathrm{CP_q}[\mathbf{C}]$, any object A allows a morphism $A \to I$, namely . We can think of this morphism as *tracing out* the system A: if $I \xrightarrow{\ulcorner m \urcorner} A^* \otimes A$ is the matrix of a map $A \xrightarrow{m} A$, then $\circ \ulcorner m \urcorner = \mathrm{Tr}(m) \colon I \to I$ by Definition 3.59. Notice that this form of 'discarding the information in A' is not uniform, and therefore gives no contradiction with the no-deleting Theorem 4.20. This subsection axiomatizes whether a given abstract category is of the form $\mathrm{CP_q}[\mathbf{C}]$ in this way.

Definition 7.41 (Environment structure)**.** On a compact dagger category $\mathbf{C}^{\mathrm{pure}}$, an *environment structure* consists of the following data:

- a compact dagger category $\mathbf{C}$ of which $\mathbf{C}^{\mathrm{pure}}$ is a compact dagger subcategory;
- for each object A in $\mathbf{C}^{\mathrm{pure}}$, a *discarding* morphism $\colon A \to I$ in $\mathbf{C}$.

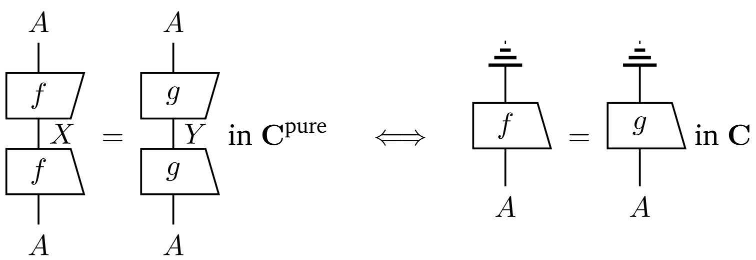
Furthermore, this data must satisfy the following properties:

- the discarding morphisms respect tensor products and dual objects:



(7.19)

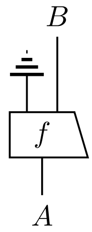
- the discarding morphisms are epimorphic up to composing with the adjoint:



(7.20)

An *environment structure with purification* must additionally satisfy:

- every morphism $A \to B$ in $\mathbf{C}$ is of the form



(7.21)

for $A \xrightarrow{f} X \otimes B$ in $\mathbf{C}^{\text{pure}}$.

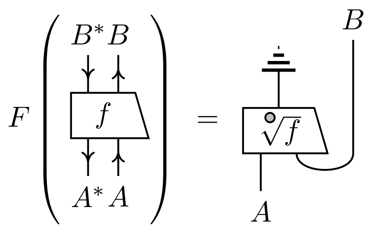
Notice that it follows from (7.21) that $\mathbf{C}$ and $\mathbf{C}^{\text{pure}}$ must have the same objects.

Intuitively, we think of $\mathbf{C}^{\text{pure}}$ as consisting of pure states, and the larger category $\mathbf{C}$ as containing mixed states. Condition (7.21) then says that every mixed state can be purified by extending the system. The idea behind the ground symbol is that the ancilla system becomes the 'environment', into which our system is plugged.

Given a compact dagger category $\mathbf{C}^{\text{pure}}$, consider its image $P(\mathbf{C}^{\text{pure}})$ under the embedding of Proposition 7.37. Explicitly, it is the subcategory of $\mathrm{CP}_{\mathrm{q}}[\mathbf{C}^{\text{pure}}]$ whose morphisms can be written with ancilla I. It has an environment structure with purification where the discarding maps are ⌒. Conversely, having an environment structure with purification is essentially the same as working with a category of completely positive morphisms, as the following theorem shows.

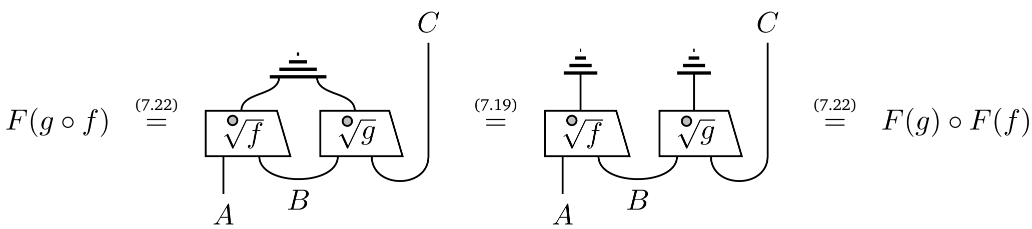
Theorem 7.42. *Given a compact dagger category $\mathbf{C}^{pure}$ equipped with an environment structure with purification, there is an invertible functor $F\colon \mathrm{CP}_{\mathrm{q}}[\mathbf{C}^{pure}] \to \mathbf{C}$ that satisfies $F(A) = A$ on objects, $F(f \otimes g) = F(f) \otimes F(g)$ on morphisms, and preserves daggers.*

Proof. Define F by $F(A) = A$ on objects, and as follows on morphisms:

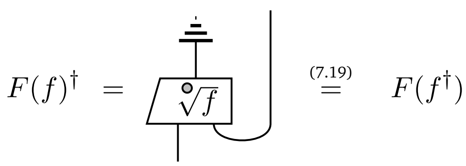


(7.22)

This is well-defined by ⇒ of (7.20). It is also functorial:



Here, the first equality follows from Lemma 7.16, and the second from (7.19). It follows from Lemma 7.17 and (7.19) that $F(f \otimes g) = F(f) \otimes F(g)$. It preserves daggers by Proposition 7.25:



Finally, it is obvious that the functor F is invertible: the direction $\Leftarrow$ of (7.20) shows that it is faithful, and (7.21) shows that it is full. $\square$

Environment structures are a convenient way to graphically handle categories of quantum structures and completely positive maps, because we do not have to 'double' the pictures all the time.

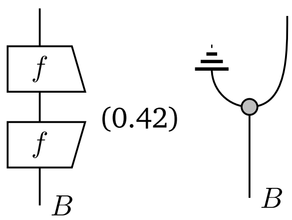
7.5 Decoherence

Having studied the special cases of subcategories of classical structures and of quantum structures, we now return to the CP construction itself. This section extends the axiomatization of categories of quantum structures using environment structures to an axiomatization of any category of the form $\mathrm{CP}[\mathbf{C}^{\mathrm{pure}}]$. This will enable us to discuss quantum teleportation once more, this time for mixed states. The idea is to use the relationship between objects of $\mathrm{CP}[\mathbf{C}^{\mathrm{pure}}]$ and Frobenius structures in $\mathbf{C}^{\mathrm{pure}}$.

If $(A, \circ)$ is an quantum structure, and $(B, \bullet)$ a classical structure, we interpret morphisms $f\colon A \to B$ as measurements of A with outcomes in B. After all, we could copy the result in B of such a measurement arbitrarily often. Similarly, we interpret morphisms $B \to A$ as preparations of the quantum system A controlled by B, just like in Example 7.8.

Now, if we start with some classical information, use it to prepare a quantum system, and then immediately measure, we should end up with the same classical information we started with. Indeed, in the category $\mathrm{CP}[\mathbf{FHilb}]$ it holds that $f^\dagger \circ f = \mathrm{id}_A$, just as in (0.41).

Decoherence (see Section 0.3.5) tells us what happens the other way around, when we measure a quantum system, and then immediately use the classical result to prepare a state of a quantum system. According to equation (0.42), a density matrix $A \xrightarrow{m} A$ turns into the diagonal matrix $\sum_i \mathrm{Tr}(|i\rangle\langle i|m)|i\rangle\langle i|$ with the same diagonal entries as m. Observe that we may write the trace in this expression abstractly using environment structures in $\mathrm{CP}[\mathbf{FHilb}]$:



This reformulation provides another reading of decoherence: it represents the idea that the measurement result is immediately and redundantly copied into the environment; for example, into every photon that is reflected from the needle of the measuring device.

The following definition abstracts this decoherence behaviour. Evidence that this is a good abstraction comes later from Theorem 7.44, which shows that it exactly characterizes categories of the form $\mathrm{CP}[\mathbf{C}^{\mathrm{pure}}]$.

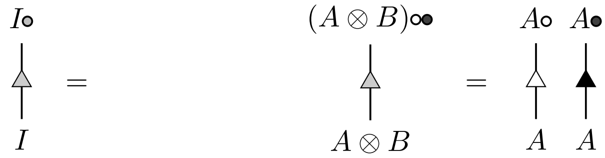
Definition 7.43. On a compact dagger category $\mathbf{C}^{\mathrm{pure}}$, a *decoherence structure* consists of the following data:

- an environment structure $\mathbf{C}$ with discarding maps ⏚;

- for each special symmetric dagger Frobenius structure (A, μ, η) in $\mathbf{C}^{\mathrm{pure}}$, an object $A_\circ$ in $\mathbf{C}$, and a *measuring* morphism $\vartriangle\colon A \to A_\circ$ in $\mathbf{C}$.

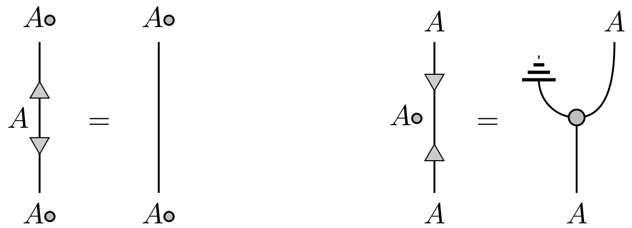
Furthermore, this data must satisfy the following properties:

- the measuring morphisms respect tensor products:



(7.23)

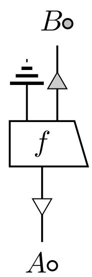
- the measuring maps are coisometric, and isometric up to discarding:



(7.24)

A decoherence structure with *purification* must additionally satisfy:

- every morphism in $\mathbf{C}$ is of the form



(7.25)

for some morphism f in $\mathbf{C}^{\mathrm{pure}}$.

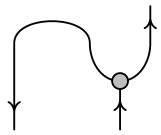
Notice that it follows from (7.25) that each object of $\mathbf{C}$ must be of the form $A_\circ$ for some special dagger Frobenius structure (A, μ, η) in $\mathbf{C}^{\mathrm{pure}}$.

When (A, μ, η) is a classical structure, we can interpret the morphism $\vartriangle\colon A \to A_\circ$ as a *measurement* as in Example 7.8. We can then read the first equation of (7.24) as *classical coding*: if we encode classical data into quantum data, immediately measuring the quantum data retrieves the original classical data again. As with environment structures, equation (7.25) models *purification*: every mixed state can be made pure by considering a larger system.

The second equation of (7.24) explains the name decoherence structure. This decoherence, makes sure that only classical information, as encoded in the basis chosen by the Frobenius structure, survives the channel. It has nothing to do with coherence of monoidal categories.

Given a positive-dimensional compact dagger category $\mathbf{C}^{\mathrm{pure}}$, consider its image $P(\mathbf{C}^{\mathrm{pure}})$ under the embedding of Proposition 7.37. This subcategory of $\mathbf{C} = \mathrm{CP}[\mathbf{C}^{\mathrm{pure}}]$ has a decoherence structure with purification where:

- the discarding map on $(A^* \otimes A, \;, \;)$ is ;
- the measuring map $(A^* \otimes A, \;, \;) \to (A^* \otimes A, \;, \;)_{\circ} = (A, \;, \;)$ is:

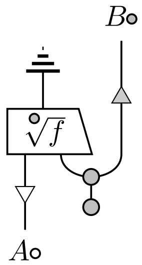


Here we used that a Frobenius structure in $P(\mathbf{C}^{\mathrm{pure}})$ must be induced by one in $\mathbf{C}^{\mathrm{pure}}$ by Lemma 7.38.

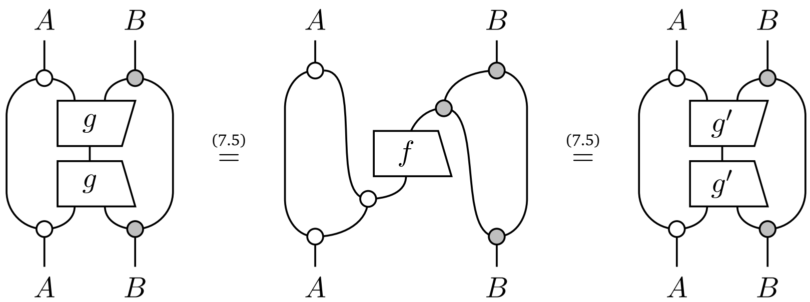
Conversely, the following theorem shows that having a decoherence structure with purification characterizes categories of the form $\mathrm{CP}[\mathbf{C}^{\mathrm{pure}}]$.

Theorem 7.44. *If a compact dagger category* $\mathbf{C}^{pure}$ *is equipped with a decoherence structure with purification, then there is an invertible functor* $F\colon \mathrm{CP}[\mathbf{C}^{pure}] \to \mathbf{C}$ *that preserves daggers and satisfies* $F(f \otimes g) = F(f) \otimes F(g)$.

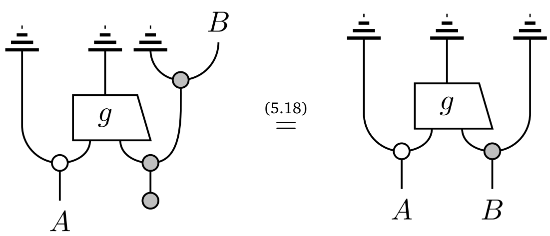
Proof. Define F as follows. On objects, $F(A, \;, \;) = A_{\circ}$. On a morphism $f\colon A \to B$ in $\mathbf{C}^{\mathrm{pure}}$, define:

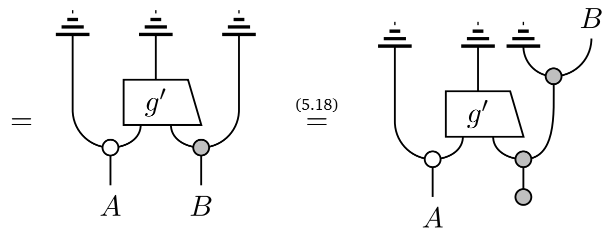
$F(f) =$ 

We first verify that F is well-defined by showing that the above definition does not depend on the choice of $\sqrt[\circ]{f}$. If g, g' are both Kraus morphisms, then:

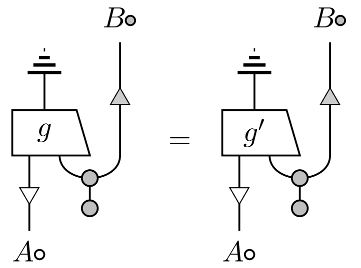


By (7.19) and (7.20), this holds if and only if:



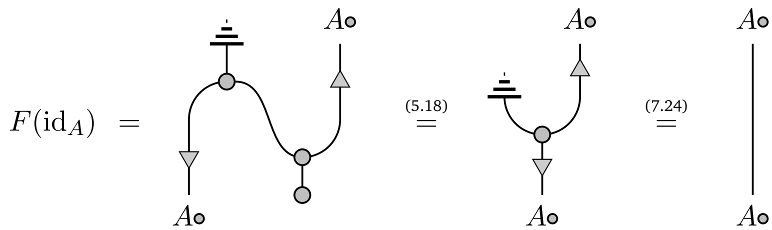


This, in turn, by (7.24), holds if and only if:

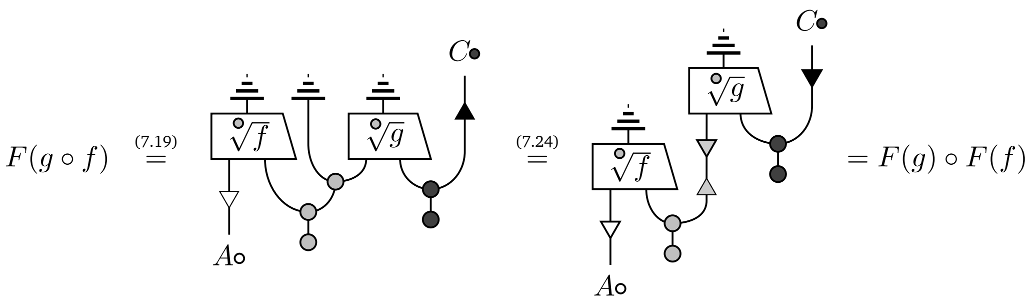


Thus F is well-defined. In fact, this also shows that F is faithful.

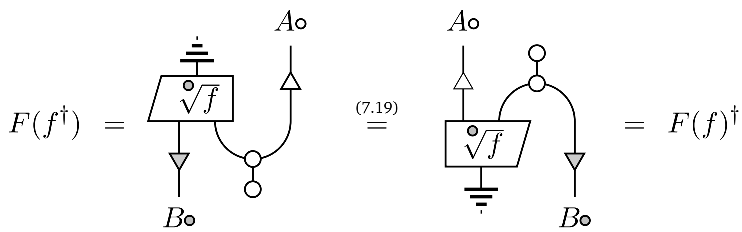
Next, notice that F preserves identities, since we may take $\sqrt[\circ]{\mathrm{id}_A} =$:



To show that F preserves composition, choose a slightly different Kraus morphism for $g \circ f$ than in Lemma 7.16:

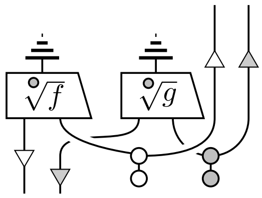


Turning to daggers, by Proposition 7.25:



As for tensor products, by Lemma 7.17:

$$F(f \otimes g) \overset{(7.19)}{\underset{(7.23)}{=}}$$



$$\overset{\text{iso}}{=} \quad F(f) \otimes F(g)$$

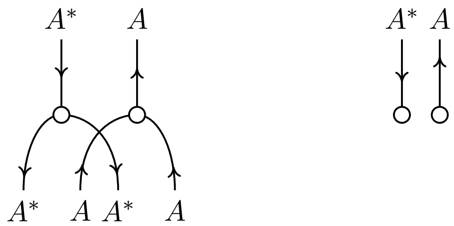
Finally, it follows from (7.25) that F is full and surjective on objects, and so invertible. □

Decoherence structures are a convenient way to handle categories of completely positive maps graphically.

7.5.1 Quantum teleportation

It is time to bring together almost all the material covered so far to discuss quantum teleportation once again. We already saw versions in Sections 1.1.4 (for pure states, postselected) and 5.6.3 (for pure states, with classical communication). The version we now describe can teleport mixed states with two 'bits' of classical communication. Start by observing that (complementary) classical structures lift from a setting of pure states to a setting of mixed states. (This is not a coincidence, because the functor from Proposition 7.37 is a symmetric monoidal functor; see Exercise 5.7.5.)

Lemma 7.45. *In a compact dagger category* $\mathbf{C}$*, if* $(A, \,, \,)$ *is a classical structure, then the following multiplication and unit give a classical structure on* $(A^* \otimes A, \,, \,)$ *in* $\mathrm{CP}[\mathbf{C}]$*:*



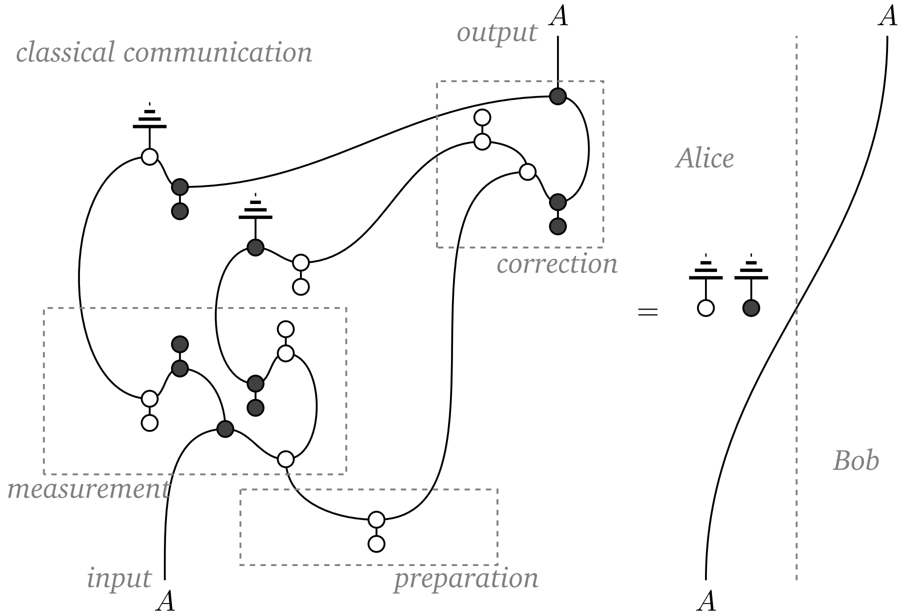
(7.26)

Furthermore, if two classical structures in $\mathbf{C}$ *in* $\mathbf{C}$ *are complementary, then so are the induced two classical structures in* $\mathrm{CP}[\mathbf{C}]$.

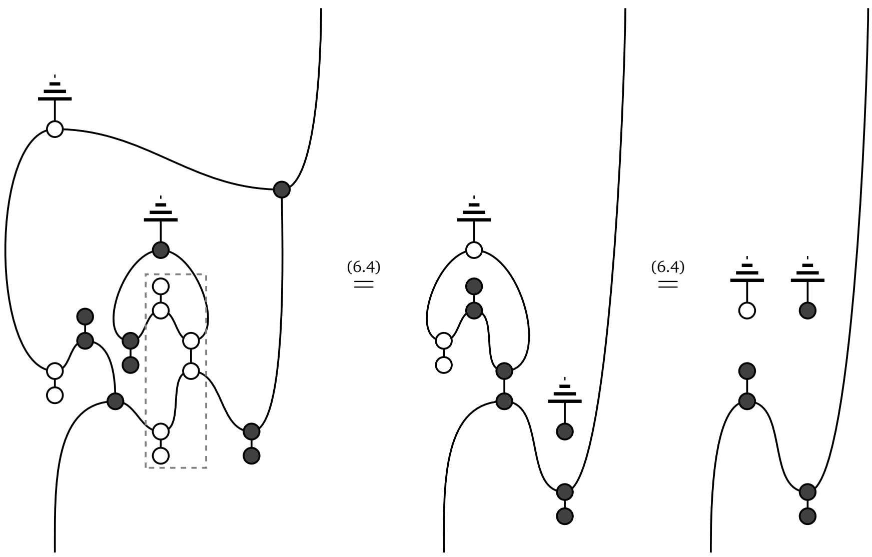
Proof. It suffices to verify that the multiplication is a well-defined morphism, that is, that (7.18) is positive. But this follows from the spider Theorem 5.22. The axioms for Frobenius structures are verified similarly. The same holds for the complementarity axiom between the two Frobenius structures. □

We are now ready to treat quantum teleportation using only tensor products and composition (and not biproducts), which was one of the main goals of this book, for mixed states.

Theorem 7.46. *In a compact dagger category* **C***, if* $(A, \curlywedge_{\circ}, \circ)$ *and* $(A, \curlywedge_{\bullet}, \bullet)$ *are complementary classical structures, then the following equation holds in* $\mathrm{CP}[\mathbf{C}]$*:*



Proof. Let's start with the left-hand side. Repeated application of the Frobenius law and associativity to the indicated white dots transforms the left-hand side into:



The first equality uses complementarity and an application of the black spider Theorem 5.21, and the second uses complementarity again. Finally, by a simple black snake equation (3.4), this equals the right-hand side of the equation in the statement of the theorem. □

The diagram in the previous theorem might look like a Christmas tree. That's because it's an *implementation* of the quantum teleportation protocol, that looks inside the dashed boxes and tells you precisely how to build each one. The *specification* instead treats the dashed rectangles as black boxes, giving the exact picture on page 3 in the Introduction.

Notice that the classical communication in the previous theorem is only classical in the sense that it is 'copied' by the two classical structures. Also, the fact that two 'bits' worth of classical communication are needed refers to the two classical channels used. These two Frobenius structures might have more than two copyable states.

Nevertheless, if we take **FHilb** for **C**, the Hilbert space $\mathbb{C}^2$ of a qubit for A, and the classical structures induced by the X and Z bases from Example 6.5 for the white and black Frobenius structures, the previous theorem precisely shows the correctness of the quantum teleportation protocol. To be precise, the object A in $\mathrm{CP}[\mathbf{C}]$ is the algebra $\mathbb{M}_2$ of 2-by-2 complex matrices. The white structure has $|+\rangle\langle+|$ as unit, and the comultiplication copies the basis $|i\rangle\langle j|$ of $\mathbb{M}_2$. Similarly, the black unit is $|0\rangle\langle 0|$, and the black comultiplication copies the basis $|\pm\rangle\langle\pm|$ of $\mathbb{M}_2$. Hence the box labeled 'preparation' creates the entangled state

$$|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |0\rangle\langle 1| + |1\rangle\langle 0| \otimes |1\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1| \in \mathbb{M}_2 \otimes \mathbb{M}_2.$$

The two classical communication maps $\mathbb{M}_2 \to \mathbb{M}_2$ perform decoherence in their respective bases: $|i\rangle\langle j| \mapsto \delta_{ij}|i\rangle\langle j|$ for one classical channel, and for the other

$$|+\rangle\langle+| \mapsto |+\rangle\langle+|, \quad |+\rangle\langle-| \mapsto 0, \quad |-\rangle\langle+| \mapsto 0, \quad |-\rangle\langle-| \mapsto |-\rangle\langle-|.$$

The measurement is the Hadamard map $\mathbb{M}_2 \otimes \mathbb{M}_2 \to \mathbb{M}_2 \otimes \mathbb{M}_2$ given by:

$$\begin{aligned} |\pm\rangle\langle\pm| \otimes |i\rangle|j\rangle &\mapsto (-1)^{\delta_{ij}}|\pm\rangle\langle\pm| \otimes |i\rangle|j\rangle, \\ |\pm\rangle\langle\mp| \otimes |i\rangle|j\rangle &\mapsto -(-1)^{\delta_{ij}}|\pm\rangle\langle\mp| \otimes |i\rangle|j\rangle. \end{aligned}$$

Note that we could have taken the decoherence maps into the measurement box to enforce a classical outcome in addition to using them to show that the communication is indeed classical. Finally, Bob's correction is precisely to apply the unitary maps (3.13) from Example 3.17, controlled by the bits on the two classical communication wires.

7.6 Interaction with linear structure

For the final section of this chapter, we investigate how the CP construction interacts with biproducts, much like in Section 3.3. The answer turns out to be very satisfying: if **C** has dagger biproducts, then so does $\mathrm{CP}[\mathbf{C}]$. The first lemma handles the level of objects.

Lemma 7.47. *In a monoidal dagger category with dagger biproducts, if (A, m_A, u_A) and (B, m_B, u_B) are dagger Frobenius structures, then the following make $A \oplus B$ into a dagger Frobenius structure:*

$$m_{A\oplus B} = \begin{pmatrix} m_A \circ (p_A \otimes p_A) \\ m_B \circ (p_B \otimes p_B) \end{pmatrix} : (A \oplus B) \otimes (A \oplus B) \to (A \oplus B) \tag{7.27}$$

$$u_{A\oplus B} = \begin{pmatrix} u_A \\ u_B \end{pmatrix} : I \to A \oplus B \tag{7.28}$$

If A and B are special, then so is $A \oplus B$. If A and B are symmetric, then so is $A \oplus B$. Furthermore, the zero object uniquely carries a dagger Frobenius structure, as follows:

$$m_0 = 0\colon 0 \otimes 0 \to 0, \qquad u_0 = 0\colon I \to 0. \tag{7.29}$$

Proof. Associativity and unitality were already mentioned in (5.25) and Exercise 5.7.8. For example, unitality:

$$
\begin{aligned}
&m_{A\oplus B} \circ (u_{A\oplus B} \otimes \mathrm{id}_{A\oplus B}) \\
&= \big((i_A \circ m_A \circ (p_A \otimes p_A)) + (i_B \circ m_B \circ (p_B \otimes p_B))\big) \circ \\
&\quad \big(((i_A \circ u_A) \otimes \mathrm{id}_{A\oplus B}) + ((i_B \circ u_B) \otimes \mathrm{id}_{A\oplus B})\big) \\
&= \big(i_A \circ m_A \circ (u_A \otimes p_A)\big) + \big(i_B \circ m_B \circ (u_B \otimes p_B)\big) \\
&= (i_A \circ p_A) + (i_B \circ p_B) \\
&= \mathrm{id}_{A\oplus B}.
\end{aligned}
$$

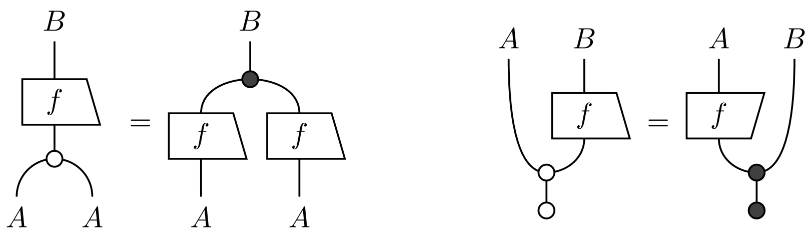
Associativity is very similar. So is speciality:

$$
\begin{aligned}
&m_{A\oplus B} \circ m^\dagger_{A\oplus B} \\
&= \begin{pmatrix} m_A \circ (p_A \otimes p_A) \\ m_B \circ (p_B \otimes p_B) \end{pmatrix} \circ \begin{pmatrix} (i_A \otimes i_A) \circ m^\dagger_A & (i_B \otimes i_B) \circ m^\dagger_B \end{pmatrix} \\
&= \begin{pmatrix} m_A \circ m^\dagger_A & 0 \\ 0 & m_B \circ m^\dagger_B \end{pmatrix} \\
&= \mathrm{id}_{A\oplus B}.
\end{aligned}
$$

Symmetry, and the Frobenius law, follow similarly. □

Next we move to the level of morphisms. We first give an easy way to show that a morphism is completely positive.

Definition 7.48 (Involutive homomorphism)**.** In a monoidal dagger category, given dagger Frobenius structures $(A, \,, \,)$ and $(B, \,, \,)$, an *involutive homomorphism* is a morphism $A \xrightarrow{f} B$ satisfying:

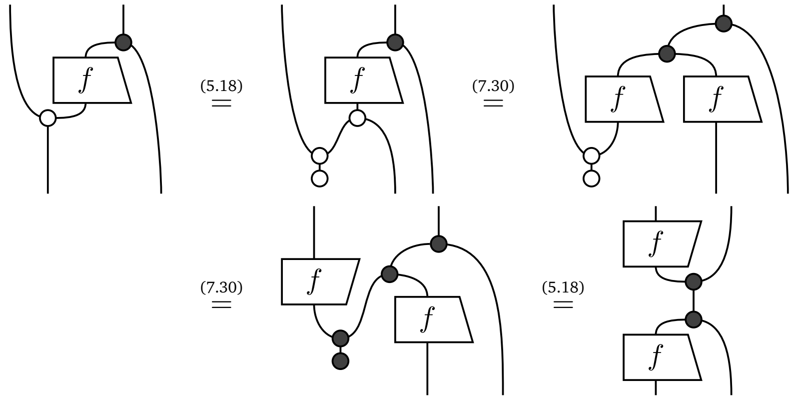


(7.30)

Notice that this notion is weaker than that of homomorphism of Frobenius structures, and hence escapes Lemma 5.19. Instead, the second equation in (7.30) is precisely (5.20) from Definition 5.25, saying that the morphism preserves the canonical involution of Frobenius structures. The following lemma shows that such morphisms are always completely positive, even if they do not necessarily respect (co)units.

Lemma 7.49. *Involutive homomorphisms satisfy the CP condition.*

Proof. Verify the CP condition:

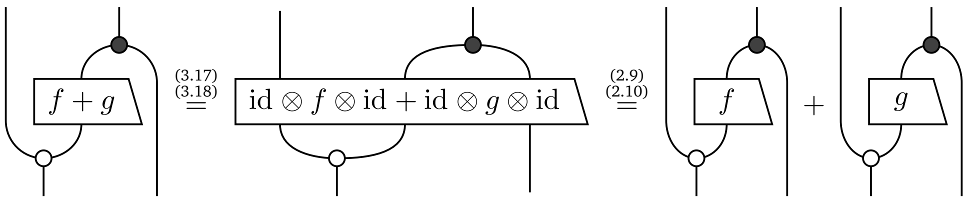


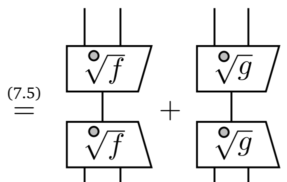
The second and third equalities follow from equation (7.30), the others from the noncommutative spider Theorem 5.21. □

Now we can prove that the CP construction respects biproducts. Because we defined biproducts in terms of a superposition rule, we first make sure that the CP construction respects superposition rules.

Lemma 7.50. *If a braided monoidal dagger category* $\mathbf{C}$ *with duals has a superposition rule, then so does* $\mathrm{CP}[\mathbf{C}]$.

Proof. Suppose that morphisms $A \xrightarrow{f,g} B$ satisfy the CP condition (7.5); we have to show that $f+g$ does, too. Using Lemmas 2.26 and 3.22, we see that the following composite is positive:





$$\overset{(2.18)}{=} \begin{pmatrix} \sqrt[\circ]{f}^{\dagger} \circ \sqrt[\circ]{f} & 0 \\ 0 & \sqrt[\circ]{g}^{\dagger} \circ \sqrt[\circ]{g} \end{pmatrix}$$

$$= \begin{pmatrix} \sqrt[\circ]{f} & 0 \\ 0 & \sqrt[\circ]{g} \end{pmatrix}^{\dagger} \circ \begin{pmatrix} \sqrt[\circ]{f} & 0 \\ 0 & \sqrt[\circ]{g} \end{pmatrix}$$

Notice that the last two equalities are allowed to speak about matrices by Lemma 3.21. □

Theorem 7.51. *If a braided monoidal dagger category* $\mathbf{C}$ *with duals has dagger biproducts, then so does* $\mathrm{CP}[\mathbf{C}]$.

Proof. By Lemma 7.50 it suffices to prove that the object $A \oplus B$ of $\mathrm{CP}[\mathbf{C}]$ defined in Lemma 7.47 is a dagger biproduct of $(A, \circ\!\!\!\!\curlywedge, \circ)$ and $(B, \bullet\!\!\!\!\curlywedge, \bullet)$. We will show that the morphisms $A \xrightarrow{i_A} A \oplus B$ and $B \xrightarrow{i_B} A \oplus B$ are involutive homomorphisms.

First consider the map $A \xrightarrow{i_A} A \oplus 0$. By the definition in Lemma 7.47, $m_{A\oplus B} = i_A \circ m_A \circ (p_A \otimes p_A) + i_B \circ m_B \circ (p_B \otimes p_B)$ and $u_{A\oplus B} = i_A \circ u_A + i_B \circ u_B$. Hence $m_{A\oplus B} \circ (i_A \otimes i_A) = i_A \circ m_A$, and

$$\begin{aligned}
&(i_A^\dagger \otimes \mathrm{id}_{A\oplus B}) \circ m_{A\oplus B}^\dagger \circ u_{A\oplus B} \\
&= (p_A \otimes \mathrm{id}_{A\oplus B}) \circ \big((i_A \otimes i_A) \circ m_A^\dagger \circ p_A + (i_B \otimes i_B) \circ m_B^\dagger \circ p_B\big) \\
&\quad \circ (i_A \circ u_A + i_B \circ u_B) \\
&= (p_A \otimes \mathrm{id}_{A\oplus B}) \circ \big((i_A \otimes i_A) \circ m_A^\dagger \circ u_A + (i_B \otimes i_B) \circ m_B^\dagger \circ u_B\big) \\
&= (\mathrm{id}_A \otimes i_A) \circ m_A^\dagger \circ u_A,
\end{aligned}$$

where the last equation uses Corollary 3.20. Thus i_A is an involutive homomorphism. A similar argument works for i_B.

By Lemma 7.49, i_A and i_B therefore satisfy the CP condition. By Proposition 7.25, so do their daggers p_A and p_B. Since these four morphisms satisfy (2.14) in **C**, they do so too in CP[**C**], which after all has the same composition and daggers. This finishes the proof. □

7.7 Exercises

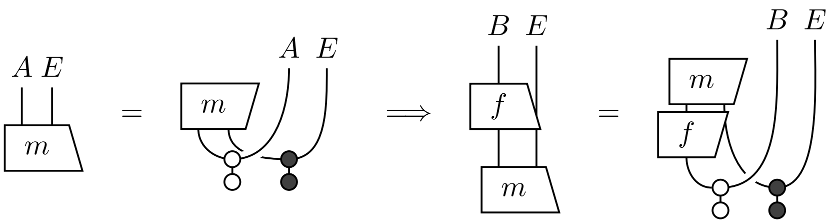
Exercise 7.7.1. Take $A = B = \mathbb{C}^2$ in **FHilb** and recall Proposition 0.71 of partial trace.

(a) Find two density matrices m, m' on $A \otimes B$ satisfying $\mathrm{Tr}_A(m) = \mathrm{Tr}_A(m')$ and $\mathrm{Tr}_B(m) = \mathrm{Tr}_B(m')$.
(b) Conclude that $A \xleftarrow{\mathrm{Tr}_B} A \otimes B \xrightarrow{\mathrm{Tr}_A} B$ is not a categorical product in CP[**FHilb**].

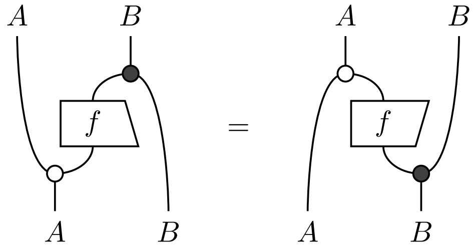
Exercise 7.7.2. Recall from Theorem 7.42 that a category of the form CP[**C**] always has a notion of trace $A \xrightarrow{\top_A} I$. Would Proposition 7.26 still hold if we insisted that morphisms in CP[**C**] preserve trace?

Exercise 7.7.3. Show that a normalized density matrix on a Hilbert space H (see Definition 0.65) is precisely a mixed state of the quantum structure on H (see Example Example 7.35) in the category **FHilb** that preserves the counit, in the sense that $\circ\, m = \mathrm{id}_I$.

Exercise 7.7.4. Call a morphism f between dagger Frobenius structures $(A, ,)$ and $(B, ,)$ in a symmetric monoidal dagger category *completely self-adjoint* when for all Frobenius structures $(E, ,)$ and all mixed states m:



Show that a morphism is completely self-adjoint if and only if its Choi matrix is self-adjoint:



(Hint: emulate the proof of Theorem 7.18.)

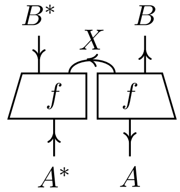
Exercise 7.7.5. Show that any quantum structure is symmetric (as a Frobenius structure) in a braided monoidal dagger category.

Exercise 7.7.6. Recall monoidal equivalences from Section 1.3. Suppose we adapt Definition 7.41 as follows: there is a monoidal functor $F\colon \mathbf{C}^{\text{pure}} \to \mathbf{C}$ that is essentially surjective on objects, and for each $A \in \mathrm{Ob}(\mathbf{C})$ there is a morphism $A \xrightarrow{\top_A} I$ in $\mathbf{C}$ satisfying:

(a) equation (7.19) holds;
(b) for all $A \xrightarrow{f} X$ and $A \xrightarrow{g} Y$ in $\mathbf{C}^{\text{pure}}$: we have $f^\dagger \circ f = g^\dagger \circ g$ in $\mathbf{C}^{\text{pure}}$ if and only if $\top_{F(X)} \circ F(f) = \top_{F(Y)} \circ F(g)$ in $\mathbf{C}$;
(c) for each $F(A) \xrightarrow{f} F(B)$ in $\mathbf{C}$ there is $A \xrightarrow{g} X \otimes B$ in $\mathbf{C}^{\text{pure}}$ such that $f = (\top_{F(X)} \otimes \mathrm{id}_{F(B)}) \circ F(g)$.

Show that the following adaptation of Theorem 7.42 holds: there is a monoidal equivalence $\mathrm{CP_q}[\mathbf{C}^{\text{pure}}] \to \mathbf{C}$ that acts as $A \mapsto F(A)$ on objects.

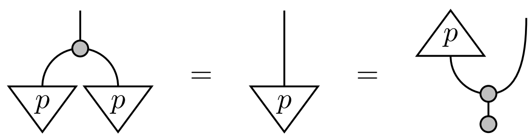
Exercise 7.7.7. Show that the following is an alternative description of $\mathrm{CP_q}[\mathbf{C}]$ for a compact dagger category: objects are those of $\mathbf{C}$, morphisms $A \to B$ are morphisms $A^* \otimes A \to B^* \otimes B$ of the form



for some $A \xrightarrow{f} X \otimes B$ in $\mathbf{C}$. (Don't forget to check that composition, tensor product, and dagger, are well-defined!)

Exercise 7.7.8. One way to state Theorem 5.31 is: any object in $\mathrm{CP}[\mathbf{FHilb}]$ is a biproduct of objects in $\mathrm{CP_q}[\mathbf{FHilb}]$. Give a counterexample to show that this does not hold with $\mathbf{FHilb}$ replaced by $\mathbf{Rel}$.

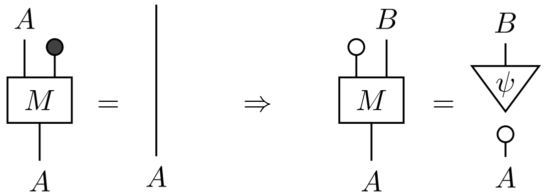
Exercise 7.7.9. A *projection* of a dagger Frobenius structure $(A, \text{multiplication}, \text{unit})$ is a morphism $I \xrightarrow{p} A$ satisfying:



Show that in $\mathbf{Rel}$, projections correspond to subgroupoids (*i.e.* subcategories that are groupoids themselves.)

Exercise 7.7.10. Let A be an object in a compact dagger category. Assume that $(A^* \otimes A, ,)$ is commutative. Show that all morphisms $A \to A$ equal the identity up to a scalar. (Hint: use the results of Chapter 4.)

Exercise 7.7.11. The *Heisenberg uncertainty principle* can be formulated as saying that no information can be obtained from a quantum structure without disturbing its state. More precisely: if $(A, ,)$ is a quantum structure, $(B, ,)$ is a classical structure, and $A \xrightarrow{M} A \otimes B$ a completely positive map, then:



(7.31)

for some state $I \xrightarrow{\psi} B$. It holds for **Hilb**. Give a counterexample to show that it fails in **Rel**.

Exercise 7.7.12. Show that the CP construction is a monoidal functor from the following monoidal category to itself: objects are positively monoidal compact dagger categories, morphisms are monoidal functors that preserve daggers, and the monoidal product is the (Cartesian) product of categories.

Notes and further reading

The use of completely positive maps originated for algebraic reasons in operator algebra theory, and dates back at least to 1955, when Stinespring proved his dilation theorem [135]; the commutative case had already been established by Gelfand in 1943 [67]. Their major breakthrough lies in the notion of injectivity, as proved by Arveson in 1969 in [8]. This last work proves the fact we mentioned that positive maps between commutative operator algebras are automatically completely positive. Operator algebra has a long history as a framework for quantum theory, including statistical mechanics, and has implicitly been used in quantum information theory since its emergence as an independent field around 1990. In particular, quantum information theory repurposed completely positive maps. See also the textbooks [26, 115]. This started around 1970 with the independent proofs of Choi in mathematics [34] and Kraus in physics [97] of their theorems. See also the tutorial [95].

The CP_q construction is originally due to Selinger in 2007 [131]. Coecke and Heunen subsequently realized in 2011 that compactness is not necessary for the construction, and it therefore also works for infinite-dimensional Hilbert spaces [41]. Coecke, Heunen, and Kissinger extended the CP_q construction to all symmetric Frobenius structures rather than just quantum structures in 2013 [42]. Finally, the link to linear structure is due to Heunen, Kissinger, and Selinger in 2014 [75]. The presentation in this chapter simplifies this development, and breaks with terminology from the literature.

Environment structures are due to Coecke in 2007 [36, 46]. The ground symbol was first used by Coecke and Perdrix in 2010 [49]. The axiomatization basically shows that categories of the form $\mathrm{CP}_\mathrm{q}[\mathbf{C}]$ are the free ones on $\mathbf{C}$ with environment structures. Cunningham and Heunen extended this in 2015 [51] to show that $\mathrm{CP}[\mathbf{C}]$ is the free category on $\mathbf{C}$ with decoherence structure. In general, the relationship between Frobenius structures in $\mathbf{C}$ and Frobenius structures in $\mathrm{CP}[\mathbf{C}]$ seems to be a difficult open question [72, 77].

The no-broadcasting theorem was proved in 1996 and is due to Barnum, Caves, Jozsa, Fuchs and Schumacher [18, 17]. The moral of the no-broadcasting results of Lemma 7.33 (and also the Heisenberg uncertainty of Exercise 7.7.11, see [76]) could be interpreted as saying that commutativity is not the 'correct' conceptual notion of classicality. This is a good example of the foundational results discussed in the Introduction.

Chapter 8

Monoidal 2-categories

Higher category theory generalizes category theory by allowing morphisms to compose in more than one way. This chapter ties previous chapters together using this perspective. Section 8.1 introduces symmetric monoidal 2-categories, and their graphical calculus based on surfaces; we investigate duality in monoidal 2-categories, and see how the theory of commutative dagger Frobenius structures emerges from this in an elegant way. Section 8.2 introduces 2-Hilbert spaces, the 'categorification' of ordinary Hilbert spaces, and investigates their properties. These techniques are then put to use in Section 8.3, which studies quantum teleportation and quantum dense coding from a higher-categorical perspective.

8.1 Monoidal 2-categories

After introducing 2-categories and their graphical calculus, this section defines equivalences and dualities in 2-categories, and proves that every equivalence can be promoted to a dual one. Next, monoidal 2-categories are defined using the graphical calculus. There is a rich theory of duality in monoidal 2-categories, which is tightly related to properties of oriented surfaces, and lets us derive the axioms of Frobenius structures from more fundamental structures. The formal theory of monoidal 2-categories is highly technical, and we will mostly avoid it by relying on the graphical calculus; this makes our treatment informal in places, but has the advantage that we can quickly reach some substantial results.

8.1.1 2-categories

To define 2-categories, we will use the traditional pasting diagram notation. Drawing the 1-morphisms from right to left to makes the notation for horizontal composition more intuitive. What we call a '2-category' has historically often been called a 'bicategory'.

Definition 8.1. A *2-category* $\mathbf{C}$ consists of the following data:

- a collection $\mathrm{Ob}(\mathbf{C})$ of *objects*;
- for every pair of objects A and B, a category $\mathbf{C}(A, B)$, with objects called *1-morphisms* denoted $A \xrightarrow{f} B$, and morphisms μ called *2-morphisms* denoted $f \overset{\mu}{\Longrightarrow} g$,

drawn as:

$$\begin{tikzcd}[column sep=huge] B & A \arrow[l, bend right=50, "g"'] \arrow[l, bend left=50, "f"] \arrow[l, phantom, "\Uparrow\mu"] \end{tikzcd}$$

for 2-morphisms $f \overset{\mu}{\Longrightarrow} g$ and $g \overset{\nu}{\Longrightarrow} h$ in $\mathbf{C}(A, B)$, call the composite in $\mathbf{C}(A, B)$ their *vertical composition*, denote it as $f \overset{\nu \cdot \mu}{\Longrightarrow} h$, and draw it as:

$$\begin{tikzcd}[column sep=huge] B & A \arrow[l, bend right=60, "h"'] \arrow[l, "g" description] \arrow[l, bend left=60, "f"] \arrow[l, phantom, shift right=3ex, "\Uparrow\nu"] \arrow[l, phantom, shift left=3ex, "\Uparrow\mu"] \end{tikzcd}$$

- for every three objects A, B, C, a functor $\circ \colon \mathbf{C}(A, B) \times \mathbf{C}(B, C) \to \mathbf{C}(A, C)$ called *horizontal composition*, whose action on 1-morphisms and 2-morphisms is drawn as follows:

$$\begin{tikzcd}[column sep=huge] C & A \arrow[l, bend right=50, "j \circ g"'] \arrow[l, bend left=50, "h \circ f"] \arrow[l, phantom, "\Uparrow \nu \circ \mu"] \end{tikzcd} = \begin{tikzcd}[column sep=large] C & B \arrow[l, bend right=50, "j"'] \arrow[l, bend left=50, "h"] \arrow[l, phantom, "\Uparrow\nu"] & A \arrow[l, bend right=50, "g"'] \arrow[l, bend left=50, "f"] \arrow[l, phantom, "\Uparrow\mu"] \end{tikzcd}$$

- for any object A, a 1-morphism $A \xrightarrow{\mathrm{id}_A} A$ called the *identity 1-morphism*;
- for any 1-morphism $A \xrightarrow{f} B$, invertible 2-morphisms $f \circ \mathrm{id}_A \overset{\rho_f}{\Longrightarrow} f$ and $\mathrm{id}_B \circ f \overset{\lambda_f}{\Longrightarrow} f$ called the *left and right unitors*, satisfying the following naturality conditions for all $f \overset{\mu}{\Longrightarrow} g$:

$$\begin{tikzcd} B & B \arrow[l, "\mathrm{id}_B"] & A \arrow[l, "g"'] \arrow[l, bend left=60, "f"] \arrow[l, phantom, shift left=2ex, "\Uparrow\mu"] \arrow[ll, bend right=50, "g"'] \arrow[ll, phantom, shift right=4ex, "\Uparrow\lambda_g"] \end{tikzcd} = \begin{tikzcd} B & & A \arrow[ll, bend right=40, "g"'] \arrow[ll, "f" description] \arrow[ll, phantom, shift right=3ex, "\Uparrow\mu"] \arrow[dl, bend left, "f"] \\ & B \arrow[ul, bend left, "\mathrm{id}_B"] \arrow[u, phantom, "\Uparrow\lambda_f"] & \end{tikzcd}$$

$$\begin{tikzcd} B & A \arrow[l, "g"'] \arrow[l, bend left=60, "f"] \arrow[l, phantom, shift left=2ex, "\Uparrow\mu"] & A \arrow[l, "\mathrm{id}_B"] \arrow[ll, bend right=50, "g"'] \arrow[ll, phantom, shift right=4ex, "\Uparrow\rho_g"] \end{tikzcd} = \begin{tikzcd} B & & A \arrow[ll, bend right=40, "g"'] \arrow[ll, "f" description] \arrow[ll, phantom, shift right=3ex, "\Uparrow\mu"] \arrow[dl, bend left, "\mathrm{id}_B"] \\ & A \arrow[ul, bend left, "f"] \arrow[u, phantom, "\Uparrow\rho_f"] & \end{tikzcd}$$

- for any three 1-morphisms $A \xrightarrow{f} B$, $B \xrightarrow{g} C$ and $C \xrightarrow{h} D$, an invertible 2-morphism $(h \circ g) \circ f \xRightarrow{\alpha_{h,g,f}} h \circ (g \circ f)$ called the *associator*, such that $(\sigma \circ (\nu \circ \mu)) \cdot \alpha_{h,g,f} = \alpha_{h',g',f'} \cdot ((\sigma \circ \nu) \circ \mu)$ for all $f \overset{\mu}{\Longrightarrow} f'$, $g \overset{\nu}{\Longrightarrow} g'$ and $h \overset{\sigma}{\Longrightarrow} h'$.

This structure is required to be coherent, meaning that any well-formed diagram built from identities and the components of α, λ, ρ, and their inverses, using horizontal and vertical composition, commutes.

Coherence for 2-categories is essentially the same as for monoidal categories, as examined in detail in Section 1.3, and we do not treat it again here. In particular, the data for a 2-category is coherent if and only if the triangle and pentagon equations are satisfied for all $A \xrightarrow{f} B$, $B \xrightarrow{g} C$, $C \xrightarrow{h} D$ and $D \xrightarrow{j} E$:

$$\begin{tikzcd}
(g \circ \mathrm{id}_B) \circ f \arrow[rr, Rightarrow, "\alpha_{g,\mathrm{id}_g,f}"] \arrow[dr, Rightarrow, "\rho_g \circ \mathrm{id}_f"'] & & g \circ (\mathrm{id}_B \circ f) \arrow[dl, Rightarrow, "\mathrm{id}_g \circ \lambda_f"] \\
& g \circ f &
\end{tikzcd} \tag{8.1}$$

$$\begin{tikzcd}
& \big(j \circ (h \circ g)\big) \circ f \arrow[rr, Rightarrow, "\alpha_{j,h\circ g,f}"] & & j \circ \big((h \circ g) \circ f\big) \arrow[dr, Rightarrow, "\mathrm{id}_j \circ \alpha_{h,g,f}"] & \\
\big((j \circ h) \circ g\big) \circ f \arrow[ur, Rightarrow, "\alpha_{j,h,g} \circ \mathrm{id}_f"] \arrow[drr, Rightarrow, "\alpha_{j\circ h,g,f}"'] & & & & j \circ \big(h \circ (g \circ f)\big) \\
& & (j \circ h) \circ (g \circ f) \arrow[urr, Rightarrow, "\alpha_{j,h,g\circ f}"'] & &
\end{tikzcd} \tag{8.2}$$

This similarity to coherence for monoidal categories is no coincidence, because 2-categories directly generalize monoidal categories.

Theorem 8.2. *A monoidal category is the same as a 2-category with one object.*

Proof. The correspondence, which we summarize with the following table, is immediate from the definitions:

Monoidal category	**One-object 2-category**
Objects	1-morphisms
Morphisms	2-morphisms
Composition	Vertical composition
Tensor product	Horizontal composition
Unit object	Identity 1-morphism

The transformations α, λ and ρ are the same for both structures. □

Just as strictness is an important possible property of monoidal categories, the same is true for 2-categories. As mentioned at the beginning of this chapter, recall that what we are calling a 'strict 2-category' has historically often been called a '2-category'.

Definition 8.3 (Strict 2-category)**.** A 2-category is *strict* when all the members of the families of 2-morphisms α, λ and ρ are identities.

Just as for monoidal categories, an interchange law

$$(\tau \cdot \sigma) \circ (\nu \cdot \mu) = (\tau \circ \nu) \cdot (\sigma \circ \mu) \tag{8.3}$$

holds for 2-categories, arising from the way that horizontal composition is defined as functor out of a product category. It means that the following composite is well-defined:

$$\begin{tikzcd}
C & B \arrow[l, "k" description] \arrow[l, bend right=60, "l"'] \arrow[l, bend left=60, "j"] \arrow[l, phantom, shift right=3, "\Uparrow\tau"] \arrow[l, phantom, shift left=3, "\Uparrow\sigma"] & A \arrow[l, "g" description] \arrow[l, bend right=60, "h"'] \arrow[l, bend left=60, "f"] \arrow[l, phantom, shift right=3, "\Uparrow\nu"] \arrow[l, phantom, shift left=3, "\Uparrow\mu"]
\end{tikzcd}$$

Because of the interchange law, we don't need to know directly the horizontal composite of a 2-morphism with another 2-morphism; we will see that it can be computed in terms of the composite of a 2-morphism with a 1-morphism, called a *whiskering*.

Definition 8.4. In a 2-category, a *whiskering* of a 2-morphism μ is its horizontal composite with an identity 2-morphism:

$$h \circ \mu \;=\; \begin{tikzcd}
C & B \arrow[l, "h"] & A \arrow[l, bend right=60, "g"'] \arrow[l, bend left=60, "f"] \arrow[l, phantom, "\Uparrow\mu"]
\end{tikzcd} \;=\; \begin{tikzcd}
C & B \arrow[l, bend right=60, "h"'] \arrow[l, bend left=60, "h"] \arrow[l, phantom, "\Uparrow\mathrm{id}_h"] & A \arrow[l, bend right=60, "g"'] \arrow[l, bend left=60, "f"] \arrow[l, phantom, "\Uparrow\mu"]
\end{tikzcd}$$

$$\mu \circ j \;=\; \begin{tikzcd}
B & A \arrow[l, bend right=60, "g"'] \arrow[l, bend left=60, "f"] \arrow[l, phantom, "\Uparrow\mu"] & C \arrow[l, "j"]
\end{tikzcd} \;=\; \begin{tikzcd}
B & A \arrow[l, bend right=60, "g"'] \arrow[l, bend left=60, "f"] \arrow[l, phantom, "\Uparrow\mu"] & C \arrow[l, bend right=60, "j"'] \arrow[l, bend left=60, "j"] \arrow[l, phantom, "\Uparrow\mathrm{id}_j"]
\end{tikzcd}$$

With the interchange law we can express any horizontal composite of 2-morphisms as the vertical composite of whiskered 2-morphisms. For example if $f \overset{\mu}{\Longrightarrow} g$ and $g \overset{\nu}{\Longrightarrow} h$, we can compose them horizontally as follows:

$$\mu \circ \nu \overset{(0.1)}{=} (\mathrm{id} \cdot \mu) \circ (\nu \cdot \mathrm{id}) \overset{(8.3)}{=} (\mathrm{id} \circ \nu) \cdot (\mu \circ \mathrm{id}) \tag{8.4}$$

Just as **Set**, the category of sets, is an important motivating example of a category, an important motivating example of a 2-category is **Cat**, the 2-category of categories.

Definition 8.5. The 2-category **Cat** is defined as follows:

- **objects** are categories;
- **1-morphisms** are functors;
- **2-morphisms** are natural transformations;
- **vertical composition** is componentwise: $(\mu \cdot \nu)_A = \mu_A \circ \nu_A$;
- **horizontal composition** is composition of functors;
- **whiskering** is given by $(F \circ \mu)_A = F(\mu_A)$ and $(\mu \circ G)_A = \mu_{G(A)}$.

In fact, $\mathbf{Cat}$ is a strict 2-category, since composition of functors is strictly associative and unital.

Finally, note that any 2-category induces a category in a canonical way, by identifying isomorphic 1-morphisms.

Definition 8.6. Given a 2-category $\mathbf{C}$, its *quotient category* $Q(\mathbf{C})$ is defined as follows:

- **objects** are the same as for $\mathbf{C}$;
- **morphisms** are isomorphism classes of 1-morphisms in $\mathbf{C}$;
- **composition** and **identities** are inherited from $\mathbf{C}$.

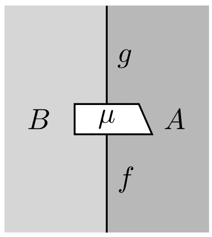
Since composition in $\mathbf{C}$ is associative and unital up to isomorphism, composition in $Q(\mathbf{C})$ will be exactly associative and unital, as required.

8.1.2 Graphical calculus

There is a graphical calculus for 2-categories, directly related to that of monoidal categories in Chapter 1: since a monoidal category is the special case of a 2-category with one object, the graphical calculus for monoidal categories is a special case for the graphical calculus for 2-categories.

Represent objects as regions, 1-morphisms as vertically-oriented lines, and 2-morphisms as vertices:

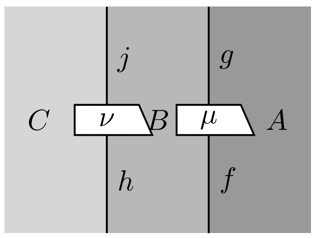
$$\begin{tikzcd} B & A \arrow[l, bend right, "g"'] \arrow[l, bend left, "f"] \arrow[l, phantom, "\Uparrow\mu"] \end{tikzcd} \quad \rightsquigarrow$$



Pasting diagrams translate into the graphical calculus via a simple rule: objects change from vertices to regions; 1-morphisms change from horizontally-oriented lines to vertically-oriented lines; and 2-morphisms change from regions to vertices. In this sense, the graphical calculus is the *dual* of the pasting diagram notation.

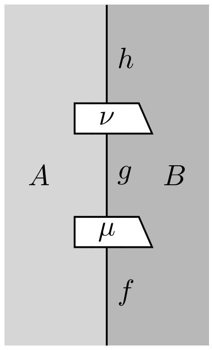
Horizontal composition becomes horizontal juxtaposition, and vertical composition becomes vertical juxtaposition:

$$\begin{tikzcd} C & B \arrow[l, bend right, "j"'] \arrow[l, bend left, "h"] \arrow[l, phantom, "\Uparrow\nu"] & A \arrow[l, bend right, "g"'] \arrow[l, bend left, "f"] \arrow[l, phantom, "\Uparrow\mu"] \end{tikzcd} \quad \rightsquigarrow$$



$$= \nu \circ \mu$$

$$\begin{tikzcd} A & & B \arrow[ll, bend right=60, "h"'] \arrow[ll, "g"' near start] \arrow[ll, bend left=60, "f"] \arrow[ll, phantom, shift right=3ex, "\Uparrow \nu"] \arrow[ll, phantom, shift left=3ex, "\Uparrow \mu"] \end{tikzcd} \quad \rightsquigarrow$$



$= \nu \cdot \mu$

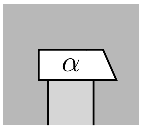
As for monoidal categories, λ, ρ and α are not drawn.

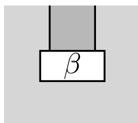
Theorem 8.7 (Correctness of the graphical calculus for a 2-category)**.** *A well-formed equation between 2-morphisms in a 2-category follows from the axioms if and only if it holds in the graphical language up to planar isotopy.*

If there is only a single object A, which we may as well denote by a region coloured white, then the graphical calculus is identical to that of a monoidal category, just as Theorem 8.2 suggests.

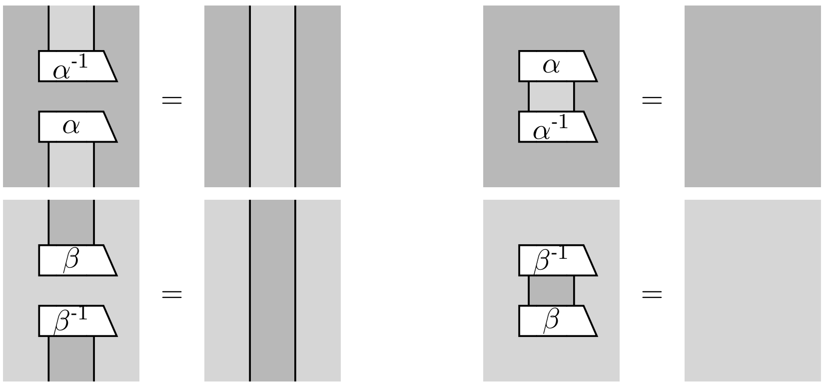
The graphical calculus gives a geometrical formulation of equivalence. When applied in **Cat**, this exactly corresponds to Definition 0.21.

Definition 8.8. An *equivalence* in a 2-category consists of a pair of objects A and B, a pair of 1-morphisms $A \xrightarrow{F} B$ and $B \xrightarrow{G} A$, and invertible 2-morphisms $G \circ F \overset{\alpha}{\Longrightarrow} \mathrm{id}_A$ and $\mathrm{id}_B \overset{\beta}{\Longrightarrow} F \circ G$:





The invertibility equations are drawn as follows:



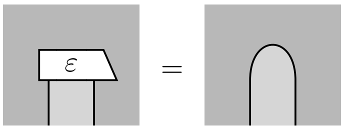
(8.5)

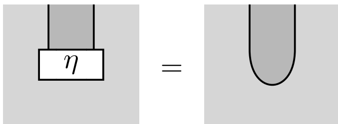
(8.6)

8.1.3 Dual 1-morphisms

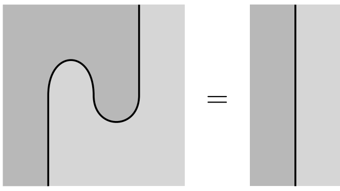
In a 2-category a 1-morphism L can have a right dual R, denoted $L \dashv R$. When the 2-category has one object this reduces to the notion of dual objects in a monoidal category of Definition 3.1.

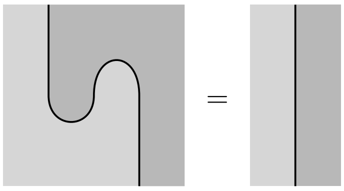
Definition 8.9. A 1-morphism $A \xrightarrow{F} B$ in a 2-category has a *right dual* $B \xrightarrow{G} A$ when there are 2-morphisms $F \circ G \overset{\varepsilon}{\Longrightarrow} \mathrm{id}_A$ and $\mathrm{id}_B \overset{\eta}{\Longrightarrow} G \circ F$, drawn as





that satisfy the snake equations:





(8.7)

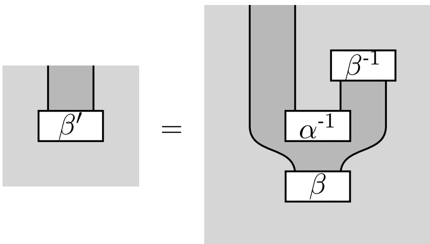
2-categorical duals generalize the classic idea of an adjunction. It may seem that adjunctions, which are central to category theory, have been absent from this book. The following example shows that it has in fact been absolutely central.

Example 8.10. A duality $F \dashv G$ in **Cat** is exactly an adjunction $F \dashv G$ between functors F and G.

The next theorem nontrivially relates equivalences and duals. It is an abstract version of a classic theorem that says that every equivalence of categories (as defined in Definition 0.17 and Definition 0.21) can be promoted to an adjoint one.

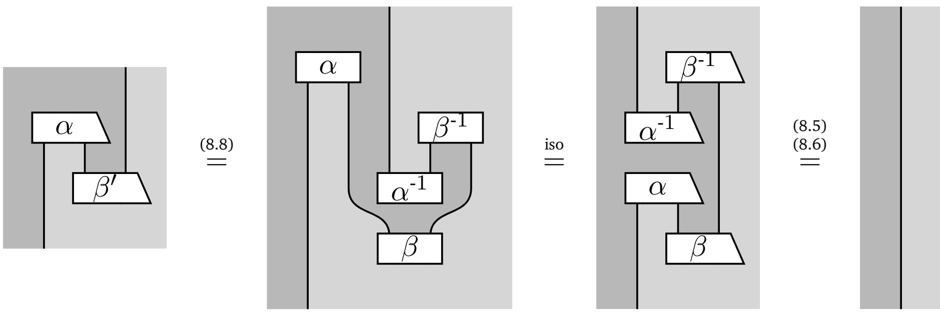
Theorem 8.11. *In a 2-category, every equivalence gives rise to a dual equivalence.*

Proof. Suppose we have an equivalence in a 2-category as in Definition 8.8, witnessed by invertible 2-morphisms α and β. Build a new equivalence witnessed by α and a new 2-morphism β', defined as follows:

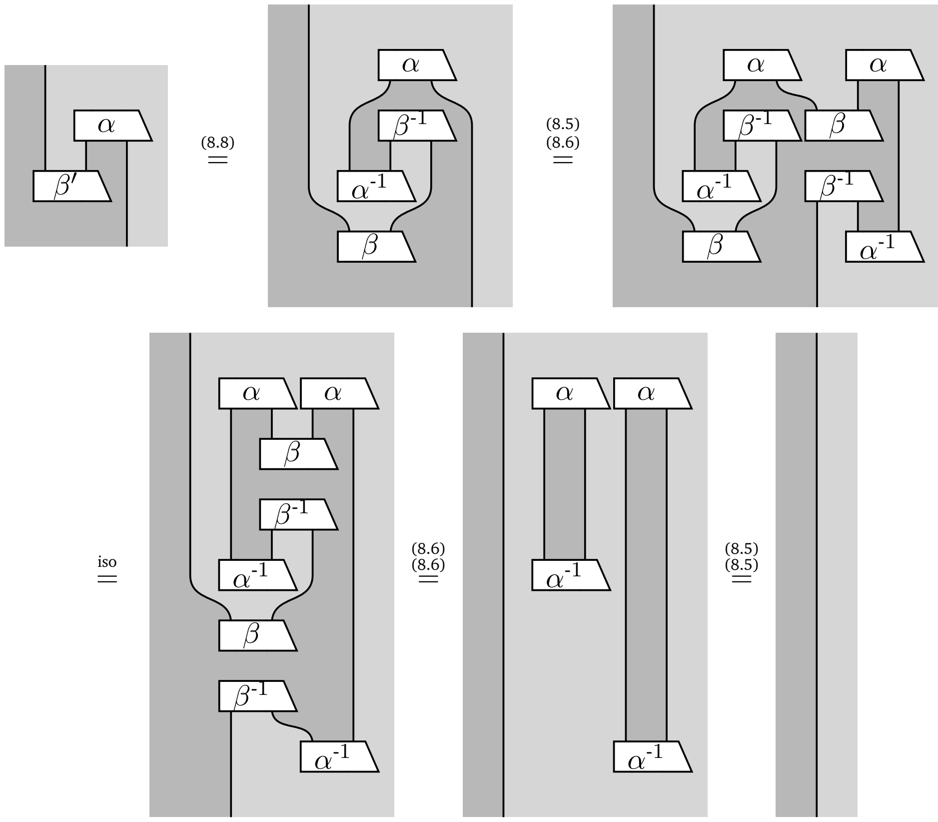


(8.8)

Since β' is composed from invertible 2-morphisms it must itself be invertible, and so it is clear that α and β' still give an equivalence. To verify the first snake equation (8.7):



To verify the second snake equation:



This completes the proof. □

Note the nontrivial role played by isotopy in this proof, as parts of the diagram are moved around extensively. In fact, it is fair to say that the isotopy parts of the argument are more complex than the algebraic parts. This is a common theme in higher category theory: as the dimension increases, so does the complexity of the corresponding notion of isotopy, along with the importance of having a clear understanding of how it interacts with the algebraic aspects of the theory.

We can leverage Theorem 8.2 to extract a nontrivial consequence of this for a monoidal category.

Corollary 8.12. *In a monoidal category, if* $A \otimes B \simeq B \otimes A \simeq I$, *then* $A \dashv B$ *and* $B \dashv A$.

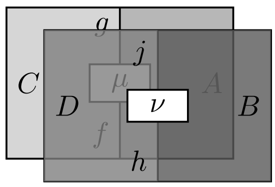
Proof. Combine Theorem 8.2 and Theorem 8.11. □

8.1.4 Monoidal 2-categories

The precise algebraic definition of monoidal 2-category requires several pages. The graphical calculus, however, remains comprehensible and practical. We give the graphical definition directly, and skip the algebraic definition, allowing us to start working with monoidal 2-categories almost immediately. While it is generally expected that the graphical calculus is sound and complete for the formal algebraic definition, this has not yet been established in the literature (see the Notes at the end of this chapter for more details.) For this reason, it should be remembered that our development is to some extent informal.

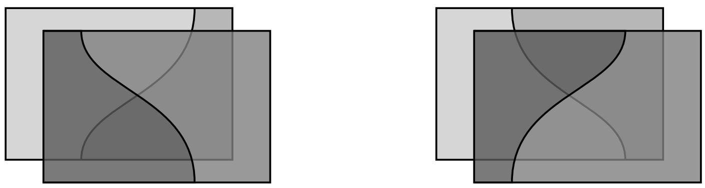
This subsection is a user's guide to the graphical calculus for monoidal 2-categories. We illustrate several main features informally and by example: tensor products, interchange, and the unit object. The graphical calculus for a monoidal 2-category is 3-dimensional, including an axis coming out of the page, which we draw with a slightly angled perspective to help understanding. The animating idea is that we are working with surfaces, lines and vertices in 3-dimensional space, with equality given by ambient isotopy.

- **Tensor product.** The *tensor product* $\mu \boxtimes \nu$ of 2-morphisms $f \overset{\mu}{\Rightarrow} g$ and $h \overset{\nu}{\Rightarrow} j$ is drawn by layering μ below ν:



  In this diagram $f \boxtimes h \xRightarrow{\mu\boxtimes\nu} g \boxtimes j$, with $A \boxtimes B \xrightarrow{f\boxtimes h} C \boxtimes D$ and $A \boxtimes B \xrightarrow{g\boxtimes j} C \boxtimes D$.

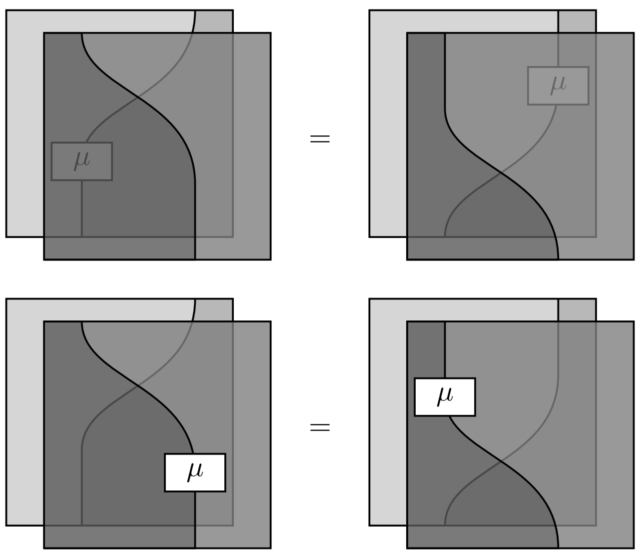
- **Interchange.** Components can move freely in their separate layers. In particular, the order of appearance of 1-morphisms in separate sheets can be interchanged:



(8.9)

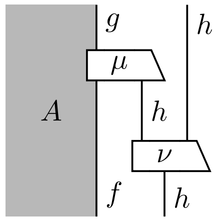
  This process itself gives a 2-morphism, which is called an *interchanger*. It is invertible, with the two diagrams given above being each others' inverse.

- **Naturality of interchange.** Vertices can be pulled through interchangers:



(8.10)

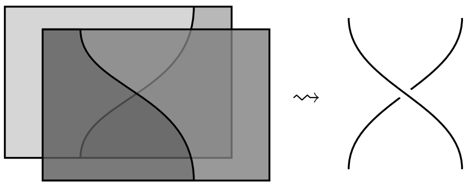
- **Tensor unit.** There is a *unit object* I, represented by a blank region; other objects are represented by shaded regions. Here is an example diagram, built from objects A and I, 1-morphisms $A \xrightarrow{f,g} I$ and $I \xrightarrow{h} I$, and 2-morphisms $f \circ h \overset{\mu}{\Longrightarrow} g$ and $h \overset{\nu}{\Longrightarrow} h \circ h$:



This graphical calculus, when stated formally, is expected to have the following property.

Conjecture 8.13 (Correctness of the graphical calculus for monoidal 2-categories)**.** A well-formed equation between 2-morphisms in a monoidal 2-category follows from the axioms if and only if it holds in the graphical language up to 3-dimensional isotopy.

An interesting thing happens when interchangers and the unit object combine. Consider an interchange diagram (8.9) with all four regions labelled by the unit object:



Instead of a 'back sheet' and a 'front sheet', there are now just two wires, with one passing in front of another. This is exactly the graphical representation of the braiding of Section 1.2. Recalling from Theorem 8.2 that $\mathrm{Hom}_{\mathbf{C}}(A, A)$ is a monoidal category leads to the following analogue of Lemma 2.3, which showed that scalars commute.

Proposition 8.14. *In a monoidal 2-category* $\mathbf{C}$*, the monoidal category Hom*$_{\mathbf{C}}(I, I)$ *is braided.*

Here is an important example of a monoidal 2-category.

Example 8.15. The 2-category $\mathbf{Cat}$ admits a monoidal structure, with product given by Cartesian product of categories, and unit object given by the category $\mathbf{1}$ with one object and one morphism.

Definition 8.6 showed how to turn a 2-category into a category, by identifying isomorphic 1-morphisms. This construction preserves the monoidal structure.

Proposition 8.16. *Given a monoidal 2-category* $\mathbf{C}$*, its quotient category* $Q(\mathbf{C})$ *can be given a canonical monoidal structure.*

Given the level of rigour we are working at, we do not prove this here, but it is easy to understand geometrically. Given a 3-dimensional diagram in the graphical calculus for a monoidal 2-category, its source and target (that is, its lower and upper boundaries) will be 2-dimensional diagrams, denoting morphisms in the graphical calculus of $Q(\mathbf{C})$ as a monoidal category. The 3-dimensional diagram as a whole can then be interpreted as the frames of a movie, showing how the lower boundary is equal to the upper boundary, as morphisms of $Q(\mathbf{C})$.

Different braidings are possible on monoidal categories of various dimensions, with different consequences for the graphical calculus. There is a pattern to the number of braidings at each categorical dimension. To see this, note that ordinary monoids can be commutative, and that monoidal categories can be braided or symmetric. You may now suspect that monoidal 2-categories will have three distinct types of braiding structure. This is indeed the case: they are called braided, sylleptic and symmetric. A *braided* structure comprises, for all pairs of objects A, B, a 1-morphism $\sigma_{A,B} \colon A \boxtimes B \to B \boxtimes A$, in the usual way. A *sylleptic* structure comprises a braided structure together with an invertible *syllepsis* 2-morphism $\pi_{A,B} \colon \sigma_{B,A} \circ \sigma_{A,B} \Rightarrow \mathrm{id}_{A \boxtimes B}$ which witnesses that the braiding is self-inverse. A *symmetric* structure is a sylleptic structure satisfying:

$$\pi_{B,A} \circ \mathrm{id}_{\sigma_{A \boxtimes B}} = \mathrm{id}_{\sigma_{B \boxtimes A}} \circ \pi_{A,B}$$

This brief introduction of braidings omits many axioms and is far from complete, but gives a sense of the way that each definition builds upon the previous one.

These additional structures can be seen as arising from additional dimensions of the graphical calculus, just as we saw in Section 1.2 for monoidal categories: the graphical calculus is 2-dimensional for monoidal categories, 3-dimensional for braided monoidal categories, and 4-dimensional for symmetric monoidal categories. For monoidal 2-categories, the graphical calculus behaves as follows: it is 3-dimensional for monoidal 2-categories, 4-dimensional for braided monoidal 2-categories, 5-dimensional for sylleptic monoidal 2-categories, and 6-dimensional for symmetric monoidal 2-categories. There is an obvious pattern here, and the general case is a prediction of the *delooping hypothesis*: monoidal n-categories can be equipped with $n+1$ different braidings, with the kth braiding relating to the geometry of $(n+k+1)$-dimensional manifolds. Concretely, for monoidal 2-categories, the syllepsis arises as a way for the braiding to 'pass through itself' by passing into the 5th dimension; there are two distinct ways this can happen, which themselves become isotopic in the presence of a 6th dimension.

8.1.5 Dual objects

Just like an object in a monoidal category has a right dual when its wire can be bent in the graphical calculus in a well-behaved way, an object in a monoidal 2-category has a right dual when its surface can be folded in the graphical calculus in a well-behaved way.

Definition 8.17. In a monoidal 2-category, an object A has a *right dual* B, written $A \dashv B$, when it can be equipped with 1-morphisms called *folds*

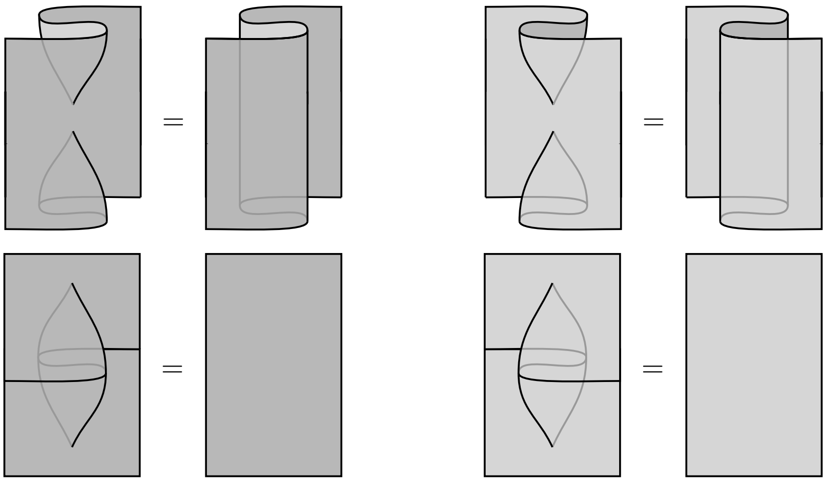
(8.11)

and invertible 2-morphisms called *cusps*:

(8.12)

(8.13)

Invertibility of the cusps takes the following graphical form:



(8.14)

Just like right duals in a monoidal category are unique up to isomorphism (see Lemma 3.4), right duals in a monoidal 2-category are unique up to equivalence.

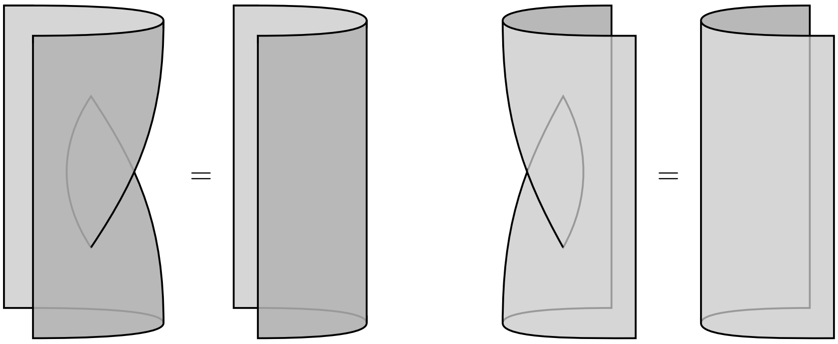
Proposition 8.18. *In a monoidal 2-category, if objects L, R, R' satisfy dualities $L \dashv R$ and $L \dashv R'$, then R and R' are canonically equivalent.*

Proof. Exactly the same as the proof of Lemma 3.4; just replace equalities with isomorphisms. We still have the derivation (3.8) and its variants, but rather than a proof of an equality, this now defines an isomorphism between the source 1-morphism and the target 1-morphism. □

This is a bit disappointing — it's too easy! Even thought we've gone from monoidal categories to monoidal 2-categories, the proofs don't seem to have got fundamentally richer or more complicated. We now add some further structure to address this.

Dual objects in a monoidal category sometimes satisfy the following equations, which say that they behave in a simple way.

Definition 8.19. A pair of dual objects in a monoidal 2-category is *coherent* when the *swallowtail equations* are satisfied, along with their vertically-flipped variants:



(8.15)

Note the interchange 2-morphism (8.9) at the centres of the left-hand sides of each equation.

Coherent duals allow us to prove an extension of Proposition 8.18.

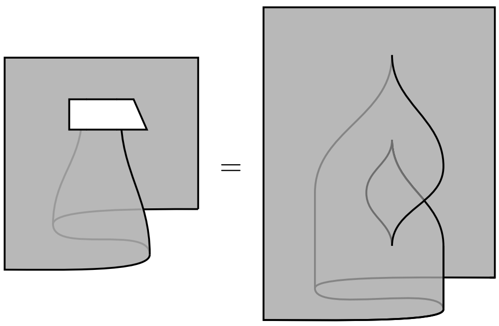
Theorem 8.20. *In a monoidal 2-category, if objects L, R, R' satisfy coherent dualities $L \dashv R$ and $L \dashv R'$, then R and R' are canonically adjoint equivalent.*

The proof of the previous theorem is rich and interesting, requiring nontrivial use of 3-dimensional isotopy; see Exercise 8.4.2.

By Theorem 8.11, every equivalence in a 2-category gives rise to an adjoint equivalence, satisfying certain extra equations. Similarly, in a monoidal 2-category, every duality gives rise to a coherent duality.

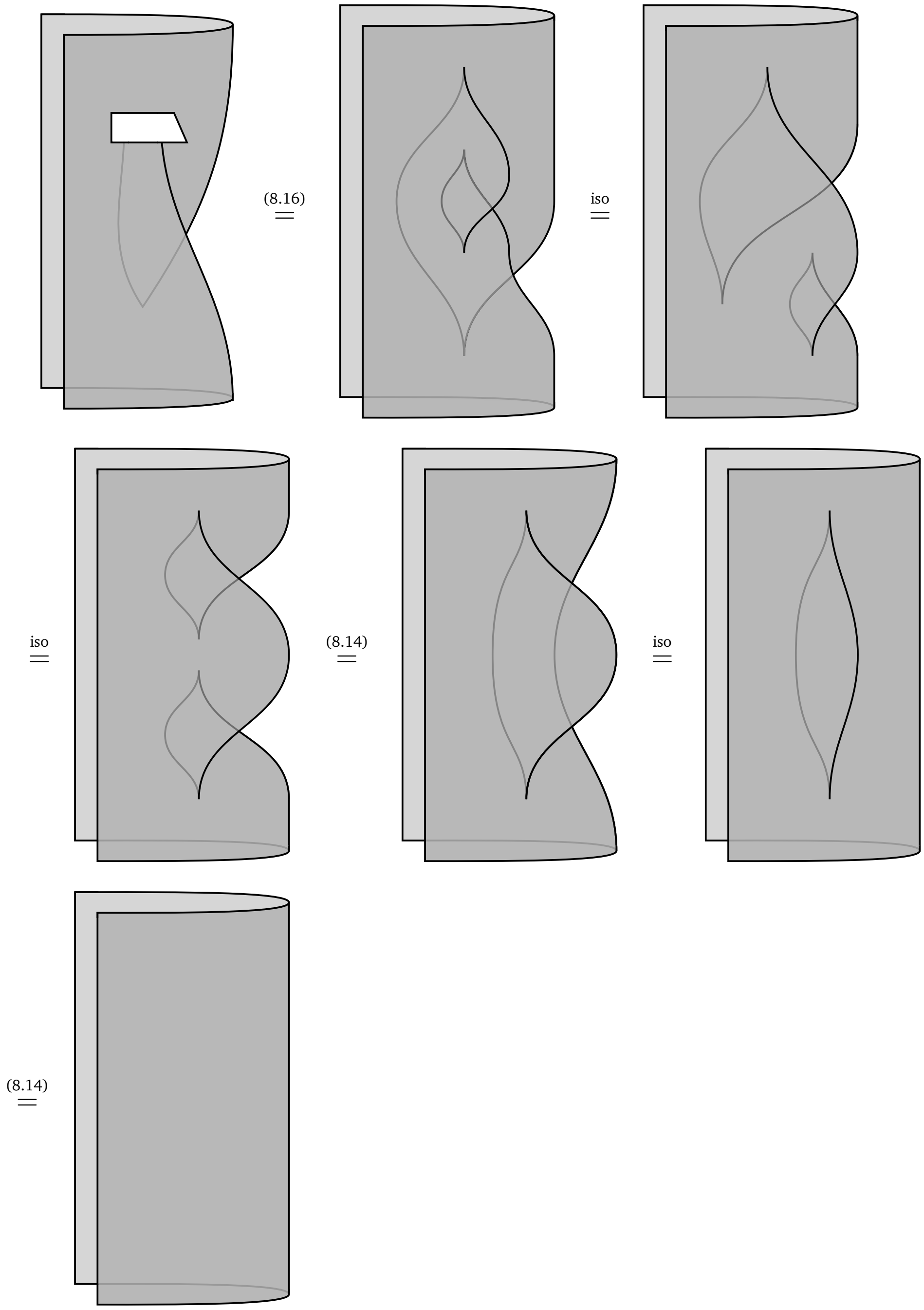
Theorem 8.21. *In a monoidal 2-category, every dual pair of objects gives rise to a coherent dual pair.*

Proof. The given dual pair comes equipped with four 2-morphisms, namely the cusps (8.12) and (8.13). We will keep the cusps (8.13) the same, but change the cusps (8.12), and show that the resulting data gives a coherent dual pair. Replace the right-hand 2-morphism in (8.12) with the following composite:



(8.16)

This is a composite of three cusps and an interchanger. Since its components are invertible, the composite is invertible. Define the replacement for the left-hand 2-morphism in (8.12) as the inverse of the composite just defined. We now have a new system of cusps: the ones just defined, and (8.13). To verify the first swallowtail equation:

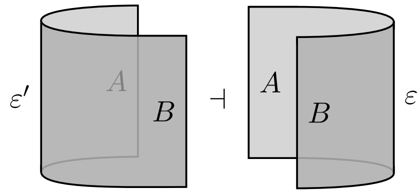


The second swallowtail equation is similar. □

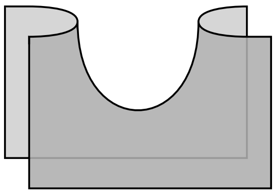
8.1.6 Oriented structure

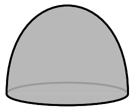
To capture the structure of oriented surfaces, we further require that the folds (8.11) themselves have duals. For example, let us consider the case that the 1-morphism ε

from (8.11) has a left dual ε':

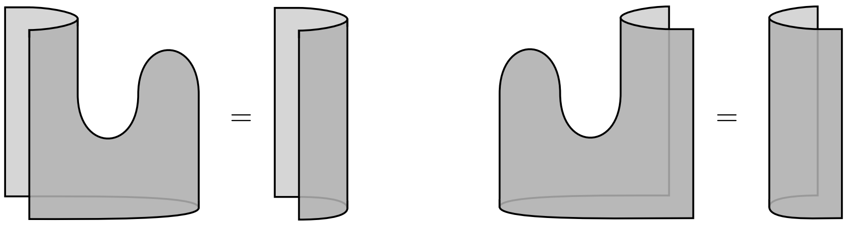


This duality has unit and counit 2-morphisms, drawn as if they were pieces of surfaces:





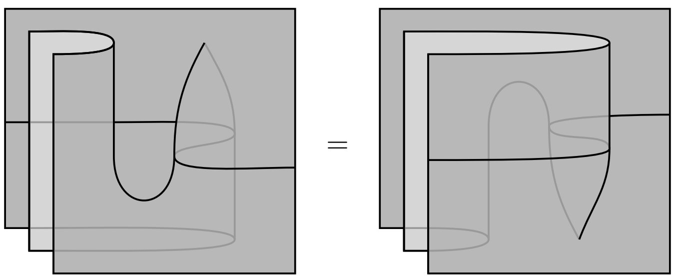
This is purely notation, but is motivated by the fact that we will require them to behave like pieces of surfaces, just as the cup and cap of (3.4) were required to behave like pieces of string. The snake equations (8.7) for the duality then look like this:



(8.17)

These equations may be interpreted as statements about homotopy of surfaces: for each equation, the left-hand side can be continuously deformed into the right-hand side, while keeping the boundary fixed.

Definition 8.22. In a monoidal 2-category, an *oriented duality* is a pair of objects A and B with coherent dual pairs $(A \dashv B, \eta, \varepsilon)$ and $(B \dashv A, \varepsilon', \eta')$, such that $\eta \dashv \eta'$, $\eta' \dashv \eta$, $\varepsilon \dashv \varepsilon'$ and $\varepsilon' \dashv \varepsilon$, satisfying the *cusp flip equation*, as well as its reflections and rotations:

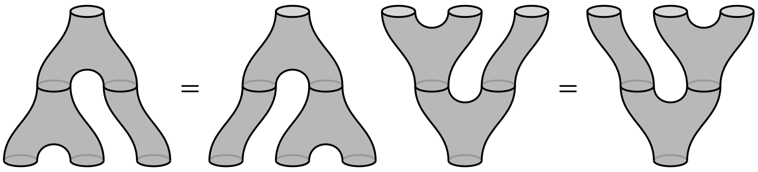


Each side of the equation involves one saddle 2-morphism and one cusp 2-morphism.

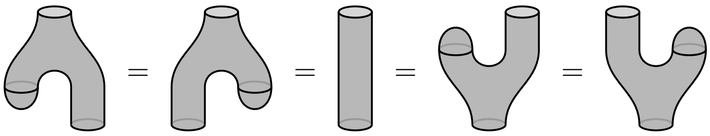
Conjecture 8.23 (Correctness of the graphical calculus for oriented dualities)**.** A well-formed equation involving the data of an oriented duality follows from the axioms if and only if the associated oriented surfaces are isotopic as immersions in $\mathbb{R}^3$.

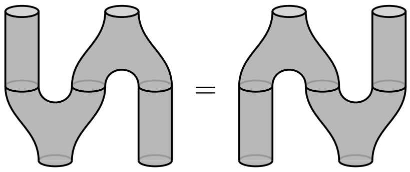
A duality $A \dashv A^*$ in a monoidal category yields a monoid on $A \otimes A^*$, as in Lemma 4.11. Furthermore, it forms a Frobenius structure as in Lemma 5.9. The object $A \otimes A^*$ can be thought of geometrically as built from 2 points with opposite orientations, giving a 0-sphere. We now consider the generalization of this result to monoidal 2-categories. Given an oriented duality $A \dashv A^*$ in a monoidal 2-category, the composite $\eta^\dagger \circ \eta$ corresponding to a 1-sphere, that is, a circle. This structure carries a *commutative* Frobenius structure.

Theorem 8.24. *An oriented structure in a monoidal 2-category* $\mathbf{C}$ *induces a commutative dagger Frobenius structure in the braided monoidal category* $\mathbf{C}(I, I)$ *of scalars.*


(8.18)

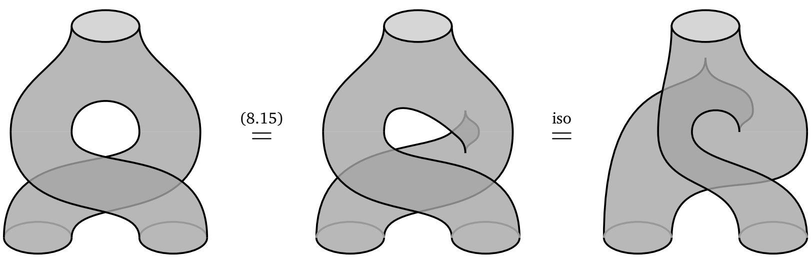

(8.19)

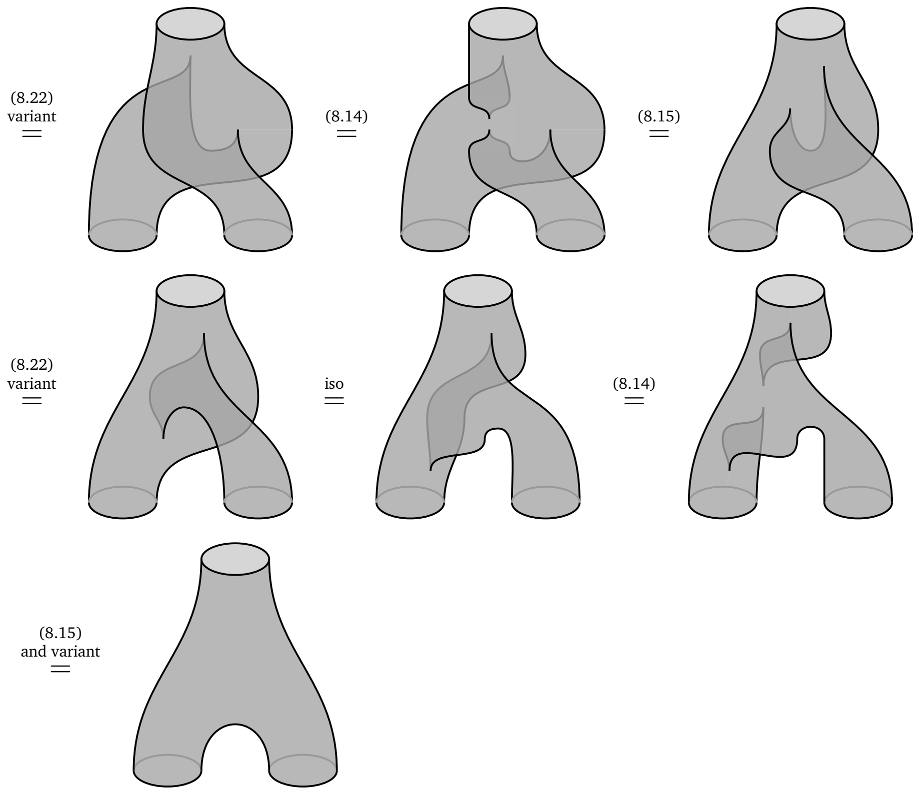

(8.20)


(8.21)

Proof. For each equation, first note that the oriented surfaces on each side are isotopic. For most equations the isotopy is clear, but some are harder to visualise. For example, in the first equation of (8.19), imagine starting with the left-hand side, grabbing the 'shoulders', and rotating them about a vertical axis, clockwise as seen from above, by a half-turn, leaving the boundaries fixed; this then gives the right-hand side. Under Conjecture 8.23 this would establish the theorem.

Without assuming this conjecture, these equations can be proven from the axioms of an oriented duality. Most of these proofs are easy. In particular, equations (8.18) and (8.21) follow from the interchange law for 2-categories (8.3), and equations (8.20) from the snake equations (8.17). The commutativity equations (8.19) have more interesting proofs, requiring many applications of the axioms of an oriented duality, such as the following:





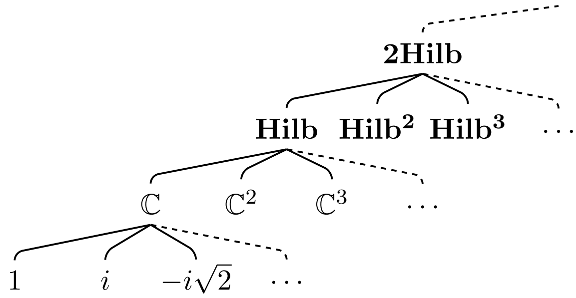
This completes the proof. □

8.2 2-Hilbert spaces

Categorification is the systematic replacement of set-based structures with category-based structures; more generally, it is the replacement of n-categorical structures with $(n+1)$-categorical structures. Sets become categories, functions become functors, and equations become isomorphisms, which might be required to satisfy new equations of their own. A good example is how monoidal categories categorify monoids (in **Set**): the associativity and unit laws of a monoid become the natural isomorphisms α, λ and ρ, which are required to satisfy the triangle (1.1) and pentagon (1.2) equations in order to have good coherence properties. As coherence does not arise for monoids, categorification is not an automatic or algorithmic process; nontrivial work is required to arrive at the correct categorified definitions.

Categorifying a Hilbert space, which is a set with extra structure, gives a 2-Hilbert space, which is a category with extra structure. These 2-Hilbert spaces organize themselves into a 2-category **2Hilb** that categorifies **Hilb**. This is analogous to the relationship between Hilbert spaces and complex numbers, with **Hilb** categorifying $\mathbb{C}$.

There are nested relationship between these structures:



Instead of considering complex numbers individually, we may consider them to form an algebraic structure $\mathbb{C}$ in their own right: the set of complex numbers, which is a the 1-dimensional Hilbert space. The collection of all Hilbert spaces forms the 1-dimensional 2-Hilbert space, which we call **Hilb**. The collection of all 2-Hilbert spaces forms the 1-dimensional 3–Hilbert space, which we call **2Hilb**. It is expected that the chain of definitions continues for all natural numbers, forming a hierarchy of n-vector spaces, although we do not give any details for $n > 2$, and at the time of writing little is known about the cases $n > 3$.

8.2.1 H*-categories

The basic theory of 2-Hilbert spaces is built on the more fundamental notion of H*-category and H*-algebra from Section 5.4.1. In essence, an H*-category is a dagger category whose hom-sets are finite-dimensional Hilbert spaces, with all this structure satisfying consistency relations.

Definition 8.25 (H*-category, H*-algebra). A *inner product category* $\mathbf{C}$ is a dagger category with the following properties, for morphisms f, g, h and complex numbers s, t:

- $\mathbf{C}(A, B)$ is a Hilbert space for each pair of objects A, B;
- composition is bilinear:

$$(s \bullet f) \circ (g + h) = s \bullet (f \circ g) + s \bullet (f \circ h), \tag{8.22}$$
$$(f + g) \circ (s \bullet h) = s \bullet (f \circ h) + s \bullet (g \circ h); \tag{8.23}$$

- the dagger is anti-linear:

$$(s \bullet f + t \bullet g)^\dagger = s^\dagger \bullet f^\dagger + t^\dagger \bullet g^\dagger; \tag{8.24}$$

- for all morphisms $A \xrightarrow{f} B$, $B \xrightarrow{g} C$, and $A \xrightarrow{h} C$, the inner product satisfies:

$$\langle g \circ f, h \rangle = \langle f, g^\dagger \circ h \rangle = \langle g, h \circ f^\dagger \rangle. \tag{8.25}$$

The H*-algebras from Definition 5.29 are simply H*-categories with one object. Hence Example 5.30 is an easy source of examples of H*-categories. Recall that H*-algebras were classified by Theorem 5.31 as direct sums of the form $\bigoplus_i B(H_i, k_i)$, for some finite family of finite-dimensional Hilbert space H_i and positive real numbers k_i.

If we fix a basis for H, we can identify these algebras as finite-dimensional matrix algebras, with an inner product scaled by some number k. The classification results from Chapter 5 then show that every finite-dimensional H*-algebra arises by taking direct sums of algebras of this sort. In particular, Theorem 5.31 says: any finite-dimensional H*-algebra is of the form $\bigoplus_i B(H_i, k_i)$, for some finite family of finite-dimensional Hilbert spaces H_i and positive real numbers k_i.

8.2.2 2-Hilbert spaces

The concept of H*-algebra leads to the definition of 2-Hilbert space, along with an auxiliary notion, Cauchy completeness, which is a categorical analogue of the completeness property of Hilbert spaces.

Definition 8.26. An H*-category is *Cauchy complete* when it has biproducts, and all idempotents split. A *2-Hilbert space* is a Cauchy complete H*-category.

There are many structural analogies between Hilbert spaces and 2-Hilbert spaces, which motivate the theory:

Hilbert spaces	**2-Hilbert spaces**
Set with structure	Category with structure
Cauchy complete inner product space	Cauchy complete H*-category
Zero vector	Zero object
Sums of vectors $v + w$	Biproducts of objects $A \oplus B$
Multiples of vectors with scalar	Tensor of object with Hilbert space
Equality $\overline{\langle v\|w\rangle} = \langle w\|v\rangle$	Isomorphism $\dagger \colon \mathbf{H}(A, B)^* \to \mathbf{H}(B, A)$
Isomorphic to $\mathbb{C}^n$	Equivalent to $\mathbf{FHilb}^n$

We will prove these formally over the course of this section. Recall the notion of split idempotent from Definition 0.29, which we will use quite often.

Proposition 8.27. *Every 2-Hilbert space has a zero object.*

Proof. Let A be an object of the 2-Hilbert space. Since the homsets are Hilbert spaces, there is a canonical zero morphism $A \xrightarrow{0_{A,A}} A$, which is idempotent. By Cauchy completeness, we can split this into morphisms $A \xrightarrow{p} \widehat{0_{A,A}}$ and $\widehat{0_{A,A}} \xrightarrow{i} A$. To see that $\widehat{0_{A,A}}$ is an initial object, let B be an arbitrary object, and let $\widehat{0_{A,A}} \xrightarrow{f} B$ be an arbitrary morphism. Then:

$$f \overset{(0.17)}{=} f \circ p \circ i \circ p \circ i \overset{(0.16)}{=} f \circ p \circ 0_{A,A} \circ i$$

This must equal zero, by linearity of composition in a H*-category. So all morphisms out of $\widehat{0_{A,A}}$ are equal, and thus $\widehat{0_{A,A}}$ is an initial object, and hence a zero object by Lemma 2.36. □

8.2.3 Bases

Simple objects play an important role in the theory of 2-Hilbert spaces, analogous to the role played by basis elements in the theory of ordinary Hilbert spaces.

Definition 8.28. An object A in a 2-Hilbert space $\mathbf{H}$ is *simple* when the H*-algebra $\mathbf{H}(A, A)$ is isomorphic to $B(\mathbb{C}, k)$ for some positive real number k.

Definition 8.29. The *trace* of an endomorphism $A \xrightarrow{f} A$ in a 2-Hilbert space is its trace as an element of the direct sum of matrix algebras $\oplus_i B(H_i, k_i)$ according to Theorem 5.31 and Example 5.30.

Lemma 8.30. *If $A \xrightarrow{f} A$ is a projection in a 2-Hilbert space with trace 1, any splitting $\widehat{f}$ is a simple object.*

Proof. Write $\mathbf{H}$ for the 2-Hilbert space. Build a function $\mathbf{H}(\widehat{f}, \widehat{f}) \to \mathbf{H}(A, A)$ by sending $s\colon \widehat{f} \to \widehat{f}$ to $s' = i_f \circ s \circ p_f\colon f \to f$. Then:

$$s' \circ f \overset{(0.16)}{=} i_f \circ s \circ p_f \circ i_f \circ p_f \overset{(0.17)}{=} i_f \circ s \circ i_f = s'$$

Similarly $f \circ s' = s'$. In a matrix algebra, the only elements that are preserved on the left and right by a 1-dimensional projection f are its scalar multiples $c \bullet f$, for $c \in \mathbb{C}$. But the function $s \mapsto s'$ is injective, since $p_f \circ s' \circ i_f = p_f \circ i_f \circ s \circ p_f \circ i_f = s$ by (0.17). Thus $\mathbf{H}(\widehat{f}, \widehat{f})$ is a matrix algebra admitting a faithful embedding into the complex numbers, and so is 1-dimensional. □

The notion of simple object leads to concept of *basis* for a 2-Hilbert space.

Definition 8.31. A *basis* for a 2-Hilbert space $\mathbf{H}$ is a collection of pairwise nonisomorphic simple objects, such that every object in $\mathbf{H}$ is a finite biproduct of basis elements.

Just as every vector in a Hilbert space is a linear combination of basis elements, every object in a 2-Hilbert space is a biproduct of basis objects.

Proposition 8.32. *If an object A in a 2-Hilbert space is equipped with a complete, orthogonal finite family of projections $A \xrightarrow{x_i} A$, then $A = \bigoplus_i \widehat{x}_i$.*

Proof. Consider two projections $A \xrightarrow{x,y} A$; the general case is similar. To show $A = \widehat{x} \oplus \widehat{y}$, we must verify the biproduct equations (2.12)–(2.14):

$$p_y \circ i_x \overset{(0.17)}{=} p_y \circ i_y \circ p_y \circ i_x \circ p_x \circ i_x \overset{(0.16)}{=} p_y \circ y \circ x \circ i_x \overset{(0.36)}{=} p_y \circ 0 \circ i_x \overset{\substack{(8.22)\\(8.23)}}{=} 0_{\widehat{x},\widehat{y}}$$
$$i_x \circ p_y + i_y \circ p_y \overset{(0.16)}{=} x + y \overset{(0.35)}{=} \mathrm{id}_A$$
$$p_x \circ i_x \overset{(0.17)}{=} \mathrm{id}_{\widehat{x}}$$

The equations $p_x \circ i_y = 0_{\widehat{y},\widehat{x}}$ and $p_y \circ i_y = \mathrm{id}_{\widehat{y}}$ are proved similarly. □

Theorem 8.33. *Every 2-Hilbert space has a basis.*

Proof. Writing $\mathbf{H}$ for the 2-Hilbert space, choose a putative basis by selecting (using the axiom of choice) one representative in each isomorphism class of simple objects in $\mathbf{H}$. It suffices to show that every object of $\mathbf{H}$ is a direct sum of simple objects, because composing with appropriate isomorphisms these direct sums can be recast in terms of our chosen simple objects. For an object A in $\mathbf{H}$, the homset $\mathbf{H}(A, A)$ is an H*-algebra, and by Theorem 5.31 and Example 5.30:

$$\mathbf{H}(A, A) = \bigoplus_i B(H_i, k_i)$$

For each i and j let $p_{i,j}\colon H_i \to H_i$ be a rank-1 projection, such that for each i, the family $p_{i,j}$ is a complete orthogonal family on H_i. Such a family of projections always exists; for example, choose an orthonormal basis for H_i, and choose $p_{i,j}$ to project onto the elements of this basis. Then $A = \bigoplus_{ij} \widehat{p_{i,j}}$ by Proposition 8.32, and by Lemma 8.30 these summands are simple objects. Picking one element from each isomorphism class of simple objects therefore yields a basis. □

8.2.4 Dimension

Next we show that 2-Hilbert spaces have a well-defined notion of dimension.

Lemma 8.34. *In a 2-Hilbert space, if a direct sum of simple objects is again simple, there must be exactly one summand.*

Proof. Consider a direct sum $\bigoplus_i S_i$ of simple objects.If the direct sum had no summands, then $\bigoplus_a S_a = 0$, so there would be a unique morphism $\bigoplus_a S_a \to \bigoplus_a S_a$, contradicting the hypothesis that $\bigoplus_a S_a$ is simple. If it had two or more summands, then the morphisms

$$t_b = \left(\bigoplus_a S_a \xrightarrow{p_b} S_b \xrightarrow{i_b} \bigoplus_a S_a\right)$$

would be a family of commuting morphisms of type $\bigoplus_a S_a \to \bigoplus_a S_a$ which compose to zero, contradicting simplicity of $\bigoplus_a S_a$, since no such pair of elements exist in $B(\mathbb{C})$. □

Proposition 8.35. *All bases of a 2-Hilbert space have the same cardinality.*

Proof. Suppose S_i and T_j are bases of the same 2-Hilbert space. For each i, write S_i as a direct sum of elements of the basis T_j; by Lemma 8.34 this direct sum has a single summand. So for each S_i, there is a unique index $\sigma(i)$ with $S_i \simeq T_{\sigma(i)}$; similarly, for any T_j, there is be a unique $\tau(j)$ with $T_i \simeq S_{\tau(j)}$. Therefore $S_i \simeq T_{\sigma(i)} \simeq S_{\tau(\sigma(i))}$, and so $S_i = S_{\tau(\sigma(i))}$ since distinct elements of a basis are never isomorphic. It follows that $\tau \circ \sigma$ is the identity function on the label set for S_i, and similarly $\sigma \circ \tau$ is the identity on the label set for T_j. Thus the indexing sets of two bases are in bijection. □

Definition 8.36. The *dimension* of a 2-Hilbert space is the cardinality of any basis.

Our next aim is to show that the dimension of a 2-Hilbert space is a complete invariant: two 2-Hilbert spaces are equivalent as 2-categories exactly when they have the same dimension. We start by defining a notion of set-induced product with finite support.

Definition 8.37 (Dimension)**.** For a (possibly infinite) set T, the category $\mathbf{FHilb}^T$ has objects f given by a choice for all $t \in T$ of an object $f(t)$ in $\mathbf{FHilb}$, and morphisms $p\colon f \to f'$ given by a choice for each $t \in T$ of a morphism $p(t)\colon f(t) \to f'(t)$ in $\mathbf{FHilb}$. The *dimension* of an object f is $\dim(f) = \sum_{t\in T} \dim(f(t)) \in [0, \infty]$. The full subcategory category of objects of finite dimension is denoted $\underline{\mathbf{FHilb}^T}$.

Note that $\mathbf{FHilb}^T$ is *not* a 2-Hilbert space for infinite sets T, since if we consider the object f given by $f(t) = \mathbb{C}$ for all $t \in T$, the inner product $\langle f, f\rangle$ would be infinite. But $\underline{\mathbf{FHilb}^T}$ *is* always a 2-Hilbert space.

Lemma 8.38. *For any set T, the category $\underline{\mathbf{FHilb}^T}$ is a 2-Hilbert space.*

Proof. We verify the axioms one at a time. For objects f, f', the set $\underline{\mathbf{FHilb}^T}(f, f')$ is given by $\bigoplus_t \mathbf{FHilb}(f(t), f'(t))$. This yields a Hilbert space, with the inner product of any $p, q\colon f \to f'$ defined as $\langle p, q\rangle = \sum_t \langle p(t), q(t)\rangle$; there are no convergence issues since f, f' are finite-dimensional, and hence the sum has finite support. Axioms (8.22)–(8.25) are verified straightforwardly since they are equational properties of morphisms which hold for $\mathbf{FHilb}$, and thus also for the T-fold Cartesian product $\mathbf{FHilb}^T$ and its full subcategory $\underline{\mathbf{FHilb}^T}$. The equational property of having direct sums must hold similarly, since the direct sum of two finite-dimensional objects is again finite-dimensional. Also, idempotents split in $\mathbf{FHilb}$, and hence in $\mathbf{FHilb}^T$ because it is a T-fold Cartesian product of $\mathbf{FHilb}$, and hence also in $\underline{\mathbf{FHilb}^T}$ since an idempotent on a finite-dimensional object has a finite-dimensional splitting. □

Lemma 8.39. *Given a set T, the 2-Hilbert space $\underline{\mathbf{FHilb}^T}$ has a basis given by objects $\{S_t \mid t \in T\}$, where for all $t' \in T$, we have $S_t(t') = \mathbb{C}$ if $t = t'$, and $f_t(t') = 0$ otherwise.*

Proof. Given an object $f \in \underline{\mathbf{FHilb}^T}$, we write $f|_t \in \underline{\mathbf{FHilb}^T}$ for the object with the property that $f|_t(t') = 0$ when $t \neq t'$, and $f|_t(t') = f(t)$ when $t = t'$; that is, $f|_t$ agrees with f at the object t, but is 0-dimensional everywhere else. If f is finite-dimensional, then so is $f|_t$ for all t, and clearly $f = \bigoplus_t f|_t$, with only a finite number of terms of the direct sum being nonzero. By definition we also have $f|_t = S_t \oplus \cdots \oplus S_t$, with a total of $\dim(f|_t)$ elements in the direct sum, which will again be finite. It follows that every object of the category is a direct sum of elements of the basis. Clearly the elements of the basis are pairwise non-isomorphic, and so the result is established. □

We are now ready to show that a 2-Hilbert space is determined up to linear equivalence by its dimension.

Proposition 8.40. *For any 2-Hilbert space $\mathbf{H}$ with basis $\{S_i \mid i \in B\}$, there is a linear equivalence of categories $\mathbf{H} \simeq \underline{\mathbf{FHilb}^B}$.*

Proof. Build a functor $F\colon \mathbf{H} \to \underline{\mathbf{FHilb}^B}$ as follows. For each object A in $\mathbf{H}$, define $F(A)(i) = \mathbf{H}(S_i, A)$. For each morphism $A \xrightarrow{f} B$, define the action by composition in the obvious way. This functor is essentially surjective on objects, since every object of $\underline{\mathbf{FHilb}^B}$ is a direct sum of objects of the form $F(S_i)$ in a straightforward way; note that finite dimensionality (Definition 8.37) is playing a key role here. This functor is also full and faithful, since by the definition of a basis, every object in $\mathbf{H}$ is a direct sum of simple objects, and then the action of F essentially computes the entries in the matrix calculus associated to the biproduct structure, which we have shown in Corollary 2.27 to be full and faithful. Linearity of the equivalence follows from all constructions in the proof being linear. □

Thus every finite-dimensional 2-Hilbert space is linearly equivalent to a finite Cartesian product of $\mathbf{FHilb}$, just as every finite-dimensional Hilbert space is equivalent to a finite Cartesian product of $\mathbb{C}$: up to equivalence, objects are simply tuples of finite-dimensional Hilbert spaces, and morphisms are tuples of linear maps. For the rest of this chapter, we will work exclusively with 2-Hilbert spaces of the form $\mathbf{FHilb}^{[n]}$, where n is a natural number, and $[n] = \{0, 1, \ldots, n-1\}$ is the canonical totally-ordered set of cardinality n. In $\mathbf{FHilb}^{[n]}$ there are n isomorphism classes of simple objects, with a convenient family $(\mathbb{C}, 0, \ldots, 0)$, $(0, \mathbb{C}, \ldots, 0)$, …, $(0, 0, \ldots, \mathbb{C})$ of representatives. This family of objects provides a canonical basis for $\mathbf{FHilb}^n$, just as the elements $|i\rangle$ form a canonical basis for $\mathbb{C}^n$ (see Definition 0.55.)

8.2.5 The 2-category of 2-Hilbert spaces

2-Hilbert spaces organize into a 2-category.

Definition 8.41. In the 2-category $\mathbf{2Hilb}$:

- **objects** are 2-Hilbert spaces;
- **1-morphisms** are linear functors (see Definition 2.17);
- **2-morphisms** are natural transformations.

Write $\mathbf{2FHilb}$ for the restriction of $\mathbf{2Hilb}$ to finite-dimensional 2-Hilbert spaces. The identities and composition of these 2-categories are as in $\mathbf{Cat}$.

A linear functor $\mathbf{FHilb}^{[n]} \to \mathbf{FHilb}^{[m]}$ is defined up to isomorphism by its action on a basis of simple objects of $\mathbf{FHilb}^{[n]}$. Thus we may represent a linear functor as a matrix of Hilbert spaces:

$$\begin{pmatrix} F_{1,1} & F_{1,2} & \cdots & F_{1,n} \\ F_{2,1} & F_{2,2} & \cdots & F_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ F_{m,1} & F_{m,2} & \cdots & F_{m,n} \end{pmatrix} \tag{8.26}$$

This is analogous to the matrix representation of linear maps between finite-dimensional Hilbert spaces with chosen bases. (More precisely, this is the matrix notation of Section 2.2.4 applied to the category with objects given by linear functors $\mathbf{FHilb}^{[n]} \to \mathbf{FHilb}^{[m]}$, and morphisms given by natural transformations.)

Up to isomorphism, composition of functors is given by matrix composition, with biproduct and tensor product taking the place of addition and multiplication. For example, functors $\mathbf{FHilb}^{[2]} \to \mathbf{FHilb}^{[2]}$ compose as:

$$\begin{aligned} &\begin{pmatrix} G_{1,1} & G_{1,2} \\ G_{2,1} & G_{2,2} \end{pmatrix} \circ \begin{pmatrix} H_{1,1} & H_{1,2} \\ H_{2,1} & H_{2,2} \end{pmatrix} \\ &\simeq \begin{pmatrix} (G_{1,1} \otimes H_{1,1}) \oplus (G_{1,2} \otimes H_{2,1}) & (G_{1,1} \otimes H_{1,2}) \oplus (G_{1,2} \otimes H_{2,2}) \\ (G_{2,1} \otimes H_{1,1}) \oplus (G_{2,2} \otimes H_{2,1}) & (G_{2,1} \otimes H_{1,2}) \oplus (G_{2,2} \otimes H_{2,2}) \end{pmatrix} \end{aligned}$$

This is only an isomorphism, rather than an equality, since unlike composition of functors, this composition operation is not strictly associative. This tradeoff is common in higher category theory: making the 1-morphisms easier to understand, a form of *skeletality*, loses good properties of composition of 1-morphisms, a form of *strictness*. This is a departure from the behaviour of Section 1.3, where $\mathbf{FHilb}$ is monoidally equivalent to a strict, skeletal monoidal category; in contrast, it is *not* expected that $\mathbf{2FHilb}$ is equivalent to a strict, skeletal monoidal 2-category.

The matrix calculus also describes objects of 2-Hilbert spaces. Up to isomorphism, objects of a 2-Hilbert space $\mathbf{FHilb}^{[n]}$ correspond to functors $\mathbf{FHilb} \to \mathbf{FHilb}^{[n]}$, by considering the value taken by the functor on the object $\mathbb{C}$ in $\mathbf{FHilb}$. Using the matrix notation, an object $(H_1, \ldots, H_n)$ of $\mathbf{FHilb}^{[n]}$ thus corresponds to the following functor:

$$\begin{pmatrix} H_1 \\ H_2 \\ \vdots \\ H_n \end{pmatrix}$$

The action of functors on objects is given (up to isomorphism) by functor composition.

A natural transformation $f\colon F \Rightarrow G$ between two matrices of Hilbert spaces is given by a family of bounded linear maps $f_{i,j}\colon F_{i,j} \to G_{i,j}$. We can write this as a matrix of linear maps, as in the following example, where $F, G\colon \mathbf{FHilb}^{[3]} \to \mathbf{FHilb}^{[2]}$:

$$\begin{pmatrix} F_{1,1} & F_{1,2} & F_{1,3} \\ F_{2,1} & F_{2,2} & F_{2,3} \end{pmatrix} \xrightarrow{\begin{pmatrix} f_{1,1} & f_{1,2} \\ f_{2,1} & f_{2,2} \end{pmatrix}} \begin{pmatrix} G_{1,1} & G_{1,2} & G_{1,3} \\ G_{2,1} & G_{2,2} & G_{2,3} \end{pmatrix} \tag{8.27}$$

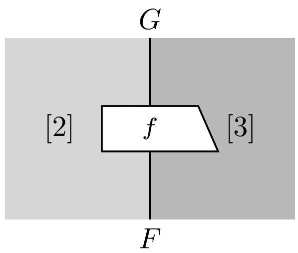
Vertical composition of 2-morphisms, denoted in the graphical calculus by vertical juxtaposition, acts elementwise by composition of linear maps. Horizontal composition and tensor product act in a more complicated way, which we will be able to understand after developing the graphical calculus below.

It follows that two 1-morphisms $\mathbf{FHilb}^{[n]} \to \mathbf{FHilb}^{[m]}$ of the form (8.26) are isomorphic in their hom-category just when the dimensions of the Hilbert spaces in each position in the matrices are the same.

Proposition 8.42. *The quotient category $Q(\mathbf{2FHilb})$ is monoidally equivalent to the monoidal category $\mathbf{Mat}_{\mathbb{N}}$, with objects given by natural numbers and morphisms given by matrices of natural numbers.*

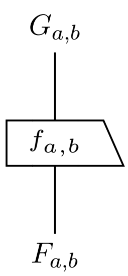
8.2.6 Graphical calculus

In earlier chapters, this book has used the graphical calculus for monoidal categories to work with **Hilb**, with wires representing Hilbert spaces and vertices representing linear maps. Similarly, we can use the graphical calculus for monoidal 2-categories to work with **2Hilb**. Here, regions represent objects, wires represent 1-morphisms, and vertices represent 2-morphisms. For example, the 2-morphism of (8.27) is depicted as follows, where region labels $\mathbf{FHilb}^{[n]}$ are abbreviated to $[n]$:



(8.28)

According to Section 8.2.5, we can take objects to be finite sets, 1-morphisms to be families of finite-dimensional Hilbert spaces, and 2-morphisms to be families of linear maps, with the ‘families’ in each case parameterized by the finite sets associated to the source and target objects. Therefore another way to present diagram (8.28) is as a family of string diagrams in **Hilb**, for each $a \in [2]$ and $b \in [3]$:

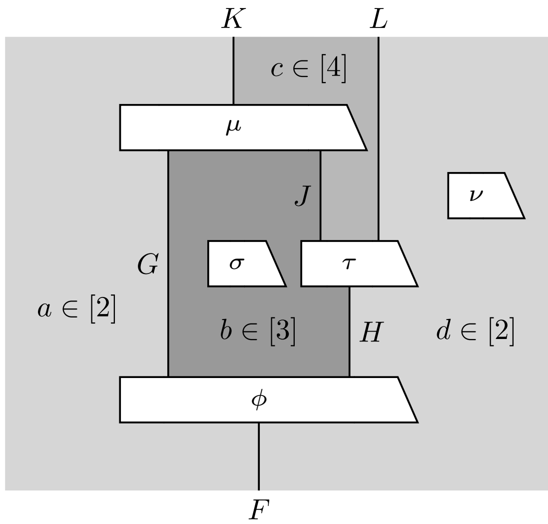


Note in particular that each wire, and the vertex, is parameterized by indices corresponding to both of the regions touching it.

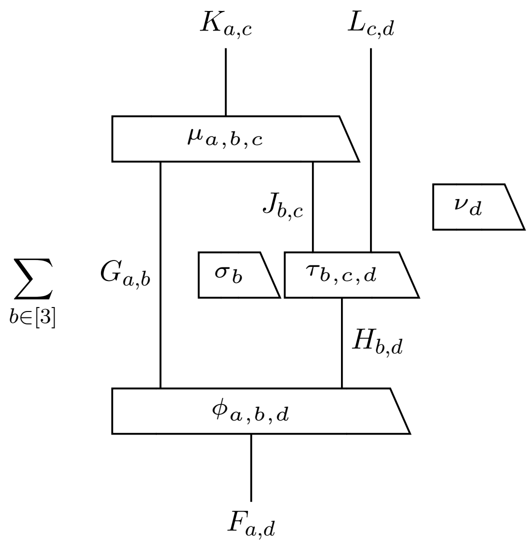
So far this simply restates the insights of Section 8.2.5 in the 2-categorical graphical calculus. But this approach also handles *composite* morphisms in **2Hilb**, with the following additional rules:

- for an open region, we get a free parameter;
- for a closed region, we sum over a bound parameter.

A region is *open* when it extends to the boundary of the diagram, and closed otherwise. For example, given a collection of 1-morphisms $F\colon \mathbf{FHilb}^{[2]}\to\mathbf{FHilb}^{[2]}$, $G\colon \mathbf{FHilb}^{[3]} \to \mathbf{FHilb}^{[2]}$, $H\colon \mathbf{FHilb}^{[2]}\to\mathbf{FHilb}^{[3]}$, $J\colon \mathbf{FHilb}^{[4]}\to\mathbf{FHilb}^{[3]}$, $K\colon \mathbf{FHilb}^{[4]}\to\mathbf{FHilb}^{[2]}$ and $L\colon \mathbf{FHilb}^{[2]}\to \mathbf{FHilb}^{[4]}$, and 2-morphisms $\phi\colon F \Rightarrow G\circ H$, $\sigma\colon \mathrm{id}_{[3]} \Rightarrow \mathrm{id}_{[3]}$, $\tau\colon H \Rightarrow J\circ L$, $\mu\colon G\circ J \Rightarrow K$ and $\nu\colon \mathrm{id}_{[2]} \Rightarrow \mathrm{id}_{[2]}$, we can form the following diagram:



Here the regions are also labelled with auxiliary parameters a, b, c, d; of these, b is bound, and a, c, d are free. Under the rules given above, this composite diagram corresponds to the following family of linear maps:

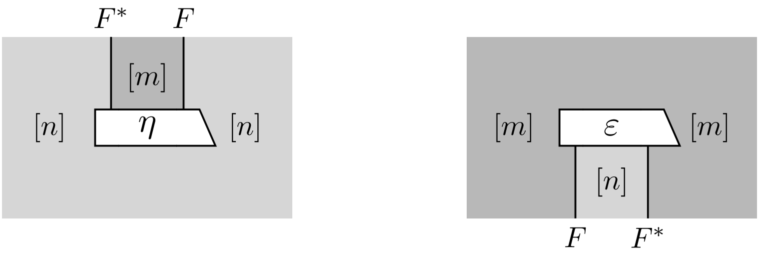


These linear maps have overall type $F_{a,d} \to K_{a,c} \otimes L_{c,d}$.

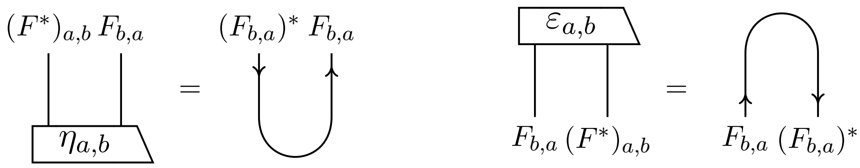
This graphical calculus makes it easy to study dualities, inheriting directly from the dualities in **FHilb**.

Theorem 8.43. *Every 1-morphism in* **2FHilb** *has a right dual.*

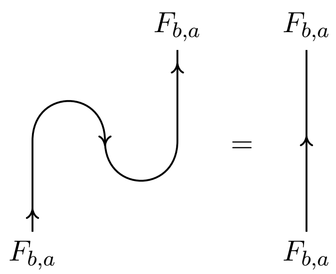
Proof. For a 1-morphism $F\colon \mathbf{FHilb}^{[n]} \to \mathbf{FHilb}^{[m]}$, define a 1-morphism $F^*\colon \mathbf{FHilb}^{[m]} \to \mathbf{FHilb}^{[n]}$ as $(F^*)_{a,b} = (F_{b,a})^*$; that is, the components of F^* are the dual Hilbert spaces of the components of F. To show that $F \dashv F^*$, following Definition 8.9, we must define cup and cap 2-morphisms $\mathrm{id}_{[m]} \overset{\eta}{\Rightarrow} F^* \circ F$ and $F \circ F^* \overset{\varepsilon}{\Rightarrow} \mathrm{id}_{[n]}$, depicted as:



Define η and ε as the following families of linear maps, indexed by $a \in [n]$ and $b \in [m]$, using the notation of Chapter 3 for the unit and counit of a duality in **FHilb**:



The first snake equation (8.7) for the duality $F \dashv F^*$ then corresponds to the following family of equations, for all $a \in [n]$ and $b \in [m]$:



But this follows immediately from the dualities $F_{b,a} \dashv (F_{b,a})^*$ in **FHilb**, and the second snake equation can be established similarly. □

Remark 8.44. It is sometimes convenient to allow two distinct parameters $a, a' \in [n]$ to label the same region, especially when considering an equation between two diagrams with different connectivity. In this case, the rule is that when the two parameters have different values, the associated linear map has value 0. The proof of Theorem 8.49 below exemplifies this.

8.2.7 Deligne tensor product

Just as ordinary Hilbert spaces have a tensor product, so do 2-Hilbert spaces, making **2Hilb** a symmetric monoidal 2-category.

Definition 8.45 (Deligne tensor product)**.** For 2-Hilbert spaces $\mathbf{H}$ and $\mathbf{J}$, their *tensor product* $\mathbf{H} \boxtimes \mathbf{J}$ is the H*-category defined as follows:

- an object is a finite list of pairs (H_p, J_p) with $H_p \in \mathrm{Ob}(\mathbf{H})$ and $J_p \in \mathrm{Ob}(\mathbf{J})$, which by abuse of notation we write as $\bigoplus_p H_p \boxtimes J_p$;
- a morphism $\bigoplus_p H_p \boxtimes J_p \xrightarrow{f} \bigoplus_q H'_q \boxtimes J'_q$ is an element of the Hilbert space

$$\bigoplus_{p,q} \mathbf{H}(H_p, H'_q) \otimes \mathbf{J}(J_p, J'_q);$$

- the identity on $\bigoplus_p H_p \boxtimes J_p$ is defined as $\bigoplus_p \mathrm{id}_{H_p} \otimes \mathrm{id}_{J_p} \in \bigoplus_{p,q} \mathbf{H}(H_p, H_p) \otimes \mathbf{J}(J_q, J_q)$, where we take the diagonal inclusion of the direct sum;
- composition of $\bigoplus_p H_p \boxtimes J_p \xrightarrow{f} \bigoplus_q H'_q \boxtimes J'_q$, $\bigoplus_r H'_r \boxtimes J'_r \xrightarrow{g} \bigoplus_s H''_s \boxtimes J''_s$ is given by the image of $f \otimes g$ under the following composite, which expands and rearranges the terms, projects down to select factors with $q = r$, and then composes:

$$\begin{aligned}
&\Big(\bigoplus\nolimits_{p,q} \mathbf{H}(H_p, H'_q) \otimes \mathbf{J}(J_p, J'_q)\Big) \otimes \Big(\bigoplus\nolimits_{r,s} \mathbf{H}(H'_r, H''_s) \otimes \mathbf{J}(J'_r, J''_s)\Big)\\
&\to \bigoplus\nolimits_{p,q,r,s} \mathbf{H}(H_p, H'_q) \otimes \mathbf{H}(H'_r, H''_s) \otimes \mathbf{J}(J_p, J'_q) \otimes \mathbf{J}(J'_r, J''_s)\\
&\to \bigoplus\nolimits_{p,q,s} \mathbf{H}(H_p, H'_q) \otimes \mathbf{H}(H'_q, H''_s) \otimes \mathbf{J}(J_p, J'_q) \otimes \mathbf{J}(J'_q, J''_s)\\
&\to \bigoplus\nolimits_{p,s} \mathbf{H}(H_p, H''_s) \otimes \mathbf{J}(J_p, J''_s)
\end{aligned} \tag{8.29}$$

- the dagger is defined straightforwardly in terms of the dagger structures on $\mathbf{H}$ and $\mathbf{J}$.

Let's first see that the abuse of notation in the previous definition is justified.

Lemma 8.46. *Concatenation of lists is a dagger biproduct.*

Proof. We illustrate this with a list of length 2; the general case is similar. For $A, B \in \mathrm{Ob}(\mathbf{H})$ and $C, D \in \mathrm{Ob}(\mathbf{J})$, consider $(A, C) \oplus (B, D)$ in $\mathrm{Ob}(\mathbf{H} \boxtimes \mathbf{J})$. Build injection and projection morphisms as follows:

$$\begin{array}{ll}
(A,C) \xrightarrow{i_1} (A,C) \oplus (B,D) & (\mathrm{id} \otimes \mathrm{id}) \oplus (0 \otimes 0) \in \big(\mathbf{H}(A,A) \otimes \mathbf{J}(C,C)\big) \oplus \big(\mathbf{H}(A,B) \otimes \mathbf{J}(C,D)\big)\\
(B,D) \xrightarrow{i_2} (A,C) \oplus (B,D) & (0 \otimes 0) \oplus (\mathrm{id} \otimes \mathrm{id}) \in \big(\mathbf{H}(B,A) \otimes \mathbf{J}(D,C)\big) \oplus \big(\mathbf{H}(B,B) \otimes \mathbf{J}(D,D)\big)\\
(A,C) \oplus (B,D) \xrightarrow{p_1} (A,C) & (\mathrm{id} \otimes \mathrm{id}) \oplus (0 \otimes 0) \in \big(\mathbf{H}(A,A) \otimes \mathbf{J}(C,C)\big) \oplus \big(\mathbf{H}(B,A) \otimes \mathbf{J}(D,C)\big)\\
(A,C) \oplus (B,D) \xrightarrow{p_2} (B,D) & (0 \otimes 0) \oplus (\mathrm{id} \otimes \mathrm{id}) \in \big(\mathbf{H}(A,B) \otimes \mathbf{J}(C,D)\big) \oplus \big(\mathbf{H}(B,B) \otimes \mathbf{J}(D,D)\big)
\end{array}$$

The dagger biproduct equations of Definition 2.39 are verified using the composition law (8.29). $\square$

The Deligne tensor product categorifies the tensor product of Hilbert spaces (as defined in Section 0.2.5).

Lemma 8.47. *The Deligne tensor product is linear in each factor:*

$$\begin{aligned}
\big(\bigoplus\nolimits_p A_p\big) \boxtimes B &\simeq \bigoplus\nolimits_p A_p \boxtimes B\\
A \boxtimes \big(\bigoplus\nolimits_p B_p\big) &\simeq \bigoplus\nolimits_p A \boxtimes B_p
\end{aligned}$$

Proof. We focus on the first of these, for a binary biproduct; the general case is similar. Build morphisms $(A \oplus B) \boxtimes C \xrightarrow{f} (A \boxtimes C) \oplus (B \boxtimes C)$ and $(A \boxtimes C) \oplus (B \boxtimes C) \xrightarrow{g} (A \oplus B) \boxtimes C$ as follows, for $A, B \in \mathrm{Ob}(\mathbf{H})$ and $C \in \mathrm{Ob}(\mathbf{J})$:

$$f = (p_A \otimes \mathrm{id}_C) \oplus (p_B \otimes \mathrm{id}_C) \in (\mathbf{H}(A \oplus B, A) \otimes \mathbf{J}(C, C)) \oplus (\mathbf{H}(A \oplus B, B) \otimes \mathbf{J}(C, C))$$
$$g = (i_A \otimes \mathrm{id}_C) \oplus (i_B \otimes \mathrm{id}_C) \in (\mathbf{H}(A, A \oplus B) \otimes \mathbf{J}(C, C)) \oplus (\mathbf{H}(B, A \oplus B) \otimes \mathbf{J}(C, C))$$

Applying the composition law (8.29), we see that these are inverses as required. □

The Deligne tensor product has a universal property: for 2-Hilbert spaces $\mathbf{H}$, $\mathbf{J}$, $\mathbf{K}$, there is a correspondence between linear functors $\mathbf{H} \boxtimes \mathbf{J} \to \mathbf{K}$ and functors $\mathbf{H} \times \mathbf{J} \to \mathbf{K}$ that are bilinear, in the sense that they are linear separately in each factor.

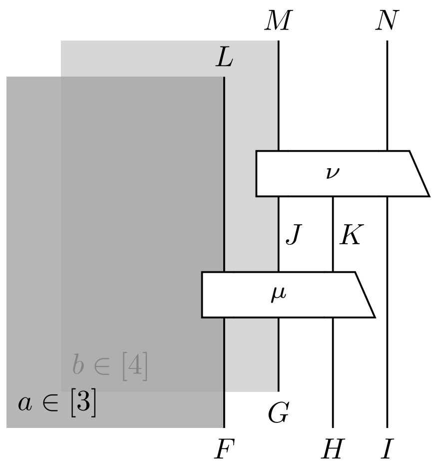
The tensor product of 2-Hilbert spaces interacts well bases. Consequently, the tensor product of 2-Hilbert spaces is again a 2-Hilbert space.

Proposition 8.48. *For sets S, T, there is a linear equivalence*

$$\underline{\mathbf{FHilb}^S} \boxtimes \underline{\mathbf{FHilb}^T} \simeq \underline{\mathbf{FHilb}^{S \times T}}.$$

Proof. Using the notation of Lemma 8.39, write simple objects of $\underline{\mathbf{FHilb}^S}$ and $\underline{\mathbf{FHilb}^T}$ as S_s and S_t for $(s, t) \in S \times T$. By Lemma 8.47, every object of $\underline{\mathbf{FHilb}^S} \boxtimes \underline{\mathbf{FHilb}^T}$ is a direct sum of objects of the form $S_s \boxtimes S_t$. These objects are simple, since their endomorphism algebra is $\mathbb{C} \otimes \mathbb{C} \simeq \mathbb{C}$. □

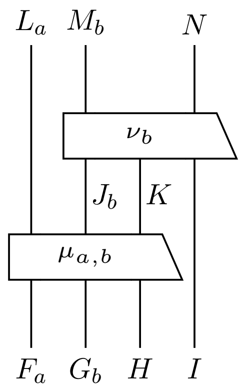
In the graphical calculus for monoidal 2-categories, the tensor product of objects layers one region in front of another, and the unit object is represented by a white region. This also represents the monoidal structure of **2Hilb**. The techniques of Section 8.2.6 still interpret composite diagrams. For example, consider the following diagram:



(8.30)

The left-hand side involves two overlapping layers, the front one parameterized by $a \in [3]$, and the rear one parameterized by $b \in [4]$. This corresponds to the following family of linear maps, parameterized by the open regions $a \in [3]$ and $b \in [4]$, where F_a, G_b, H, I, J_b, K, L_a, M_b and N are Hilbert spaces, and where $\mu_{a,b} \colon F_a \otimes G_b \otimes H \to L_a \otimes J_b \otimes K$

and $\nu_b \colon J_b \otimes K \otimes I \to M_b \otimes N_b$ are linear maps:



(8.31)

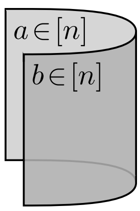
These composites have type $F_a \otimes F_b \otimes H \otimes I \to L_a \otimes M_b \otimes N$. Since (8.30) has no closed regions, (8.31) has no summation.

8.2.8 Dual objects

As promised in Section 8.1.5, we can now prove results about dual objects in **2Hilb**, using the graphical calculus that we have developed.

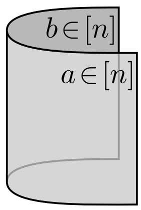
Theorem 8.49. *In the monoidal 2-category* **2Hilb***, every finite-dimensional 2-Hilbert space has a dual.*

Proof. Fix a 2-Hilbert space $\mathbf{H} = \underline{\mathbf{FHilb}^{[n]}}$. For the dual object, choose $\mathbf{H}$ itself. All parameters for labelled surfaces take values in $[n]$, which we simply drop. Define the fold maps F and G by the choices $F_{a,a} = G_{a,a} = \mathbb{C}$ for the diagonal elements, and define them to equal the 0-dimensional Hilbert space otherwise:

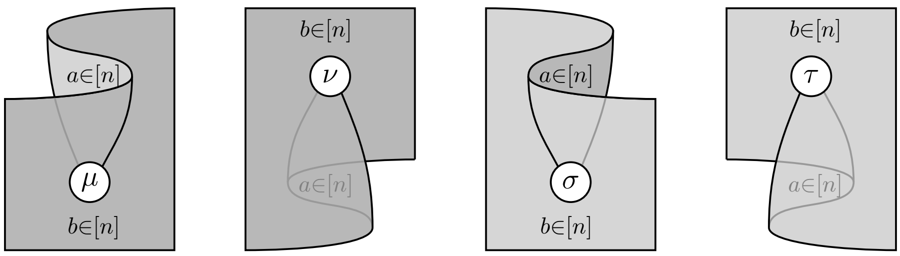


F

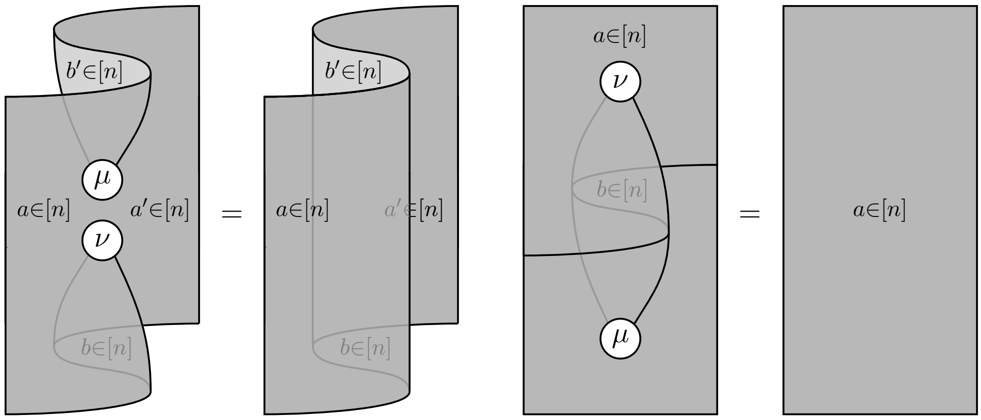
G



Define the cusp maps as follows, with the condition $\mu_{a,a} = \nu_{a,a} = \sigma_{a,a} = \tau_{a,a} = 1$ on the diagonal elements, and with the other elements equal to 0:



To see that μ and ν are inverses:



The first equation labels some regions by multiple parameters, interpreted via Remark 8.44. We verify these equations parameterwise. For the first equation, for fixed parameter values, each side has source $G_{b,a'} \otimes F_{a,b}$ and target $G_{b',a'} \otimes F_{a,b'}$. Therefore if $b \neq a'$, or $a \neq b$, or $b' \neq a'$, or $a \neq b'$, either the source or target is 0-dimensional, and the equation holds vacuously; otherwise $a = a' = b = b'$, and again the equation holds by definition. For the second equation, interpret the left-hand side as a linear map $\mathbb{C} \to \mathbb{C}$, and compute it for all values of $a \in [n]$ as $\sum_b \nu_{a,b}\mu_{a,b}$; by definition of μ and ν this equals 1. Similarly, σ and τ are inverses. $\square$

One could further show that the candidates for μ and ν above also satisfy the swallowtail equations (8.15).

We now study oriented dualities in **2Hilb**. We first introduce a unitarity property for such dualities, which makes use of the dagger structure on the 2-morphisms of **2Hilb**.

Definition 8.50. In **2Hilb**, a *oriented dagger duality* (also sometimes called a *unitary oriented duality*) is an oriented duality that satisfies the following properties:

- the cusps are unitary;
- the dagger of the data for $\eta \dashv \eta'$ gives the data for $\eta' \dashv \eta$, and the dagger of the data for $\varepsilon \dashv \varepsilon'$ gives the data for $\varepsilon' \dashv \varepsilon$.

This definition is a reasonable one: it says that the components of the oriented duality should respect the dagger operations on the hom-categories of **2Hilb**.

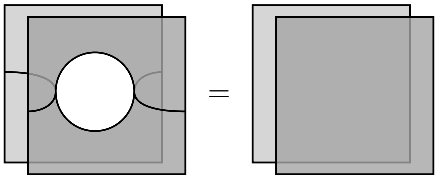
We know from Theorem 8.24 that every oriented duality in **2Hilb** gives rise to a commutative Frobenius structure in **Hilb**, and it follows immediately that every oriented dagger duality in **2Hilb** yields a commutative dagger Frobenius structure in **Hilb**. We now establish that the converse also holds, in the following sense.

Theorem 8.51. *Every commutative dagger Frobenius structure in* **Hilb** *arises from a oriented dagger duality in* **2Hilb** *by transport across a unitary.*

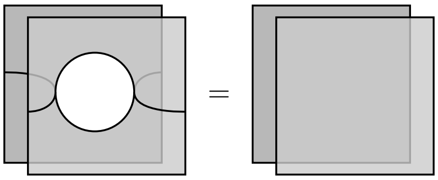
Proof sketch. This can be proved by direct construction. From Theorem 5.36, we know that the data of a commutative dagger Frobenius structure in **Hilb** is equivalent to the data of an orthonormal basis for a finite-dimensional Hilbert space. Such a basis $\{|i\rangle\}$ is defined up to unitary isomorphism by a finite multiset of positive real numbers $c_i = \sqrt{\langle i|i\rangle}$ which represent the lengths of the basis elements. Given this data, we can directly construct the data of a oriented dagger duality, and verify that the necessary conditions are satisfied. Filling in the details of this proof is Exercise 8.4.4. $\square$

Section 5.4.2 equated special commutative dagger Frobenius structures to orthonormal bases. There is a similar specialness property for oriented dualities.

Definition 8.52. An oriented duality is *special* when ‘holes can be cancelled’, in the following sense:



(8.32)



(8.33)

It is clear from Theorem 8.24 that a special oriented dagger duality in **2Hilb** will yield a dagger special commutative Frobenius structure in **Hilb**. Conversely, Theorem 8.51 can be strengthened as follows.

Proposition 8.53. *Every commutative dagger special Frobenius structure in* **Hilb** *arises from a special oriented dagger duality in* **2Hilb** *by transport across a unitary.*

Proof sketch. By direct construction, similar to Theorem 8.51. □

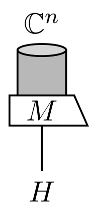
8.3 Quantum procedures

This final section uses oriented dualities in **2Hilb** to model and reason about quantum procedures, connecting Sections 8.1 and 8.2 to the rest of the book.

8.3.1 Measurement and controlled operations

A nondegenerate measurement on a Hilbert space is defined up to phase by an orthonormal basis; see Lemma 0.62. An obvious way to equip a finite-dimension Hilbert space with such a basis is by giving a unitary map $M\colon H \to \mathbb{C}^n$. **??** gives $\mathbb{C}^n$ as the value of the circle induced by an oriented duality in **2Hilb**. This leads to the following definition.

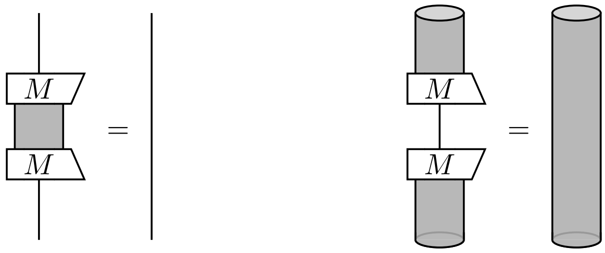
Definition 8.54. In **2Hilb**, given a special oriented dagger duality, a *measurement 2-morphism* is a unitary 2-morphism of the following type:



(8.34)

The source of this 2-morphism is a Hilbert space, representing the state space of some quantum system. The target is the cylinder arising from the special oriented dagger duality; as we saw in Section 8.2.8, the cylinder carries all the structure of a special commutative dagger Frobenius algebra, which allows us to describe copying, comparison, deletion and uniform creation of classical information. In this sense, the 2-morphism maps a quantum system into a classical system, and our interpretation of it as a measurement 2-morphism arises in this way.

The unitarity equations for the measurement 2-morphism look as follows:



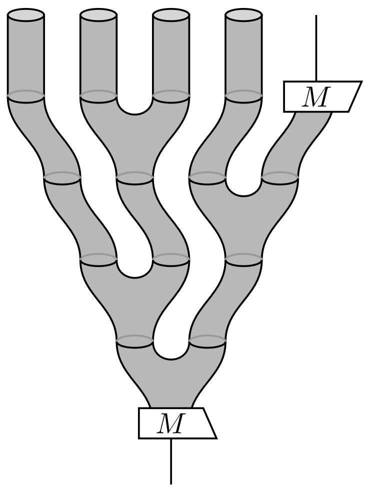
(8.35)

These involve the adjoint $M^\dagger\colon \mathbb{C}^n \to H$, which we can interpret as a *preparation* process, turning the computational basis element $|i\rangle$ into the corresponding quantum state $M^\dagger|i\rangle$.

The second of these equations reformulates (0.41): if you start with some classical information, use it to prepare a quantum system, and then immediately measure, you get back the same classical information.

But the first of these unitarity equations seems to be at odds with decoherence (see Section 0.3.5): it says that if you measure a quantum system, yielding a piece of classical data, and then immediately use that to prepare a state of a quantum system, the result will be the identity; that is, it's as if we didn't measure the quantum system at all. But quantum measurement should be an irrevocable process, not something that can be undone by performing a quantum state preparation.

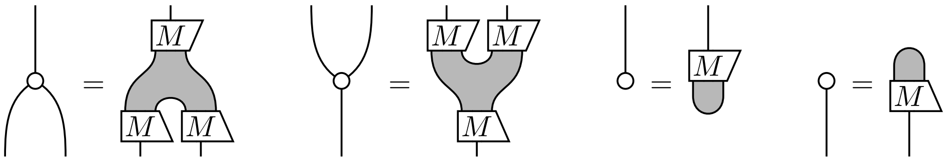
The resolution is as follows. We suppose that the classical measurement outcome is being constantly copied by the physical environment surrounding our experiment. If we follow this copying process, which is essentially unavoidable, with a state preparation, we obtain a dynamical history which can be described as follows using our formalism:



This is a better description of what it means to perform a measurement followed by a preparation, and our axioms do not imply that this yields the identity. The familiar characteristics of measurement, including its essentially irrevocable nature, are understood to largely arise from the way that the measurement result would become inextricably encoded in the environment.

We can go from the higher categorical framework to the monoidal framework, and extract Frobenius structures as follows.

Definition 8.55. For a measurement 2-morphism, its *associated dagger Frobenius structure* is constructed as follows:

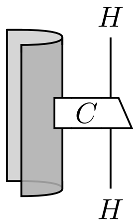


(8.36)

This is clearly a dagger Frobenius structure, since it arises by transporting the dagger Frobenius structure of Theorem 8.24 across the unitary 2-morphism M.

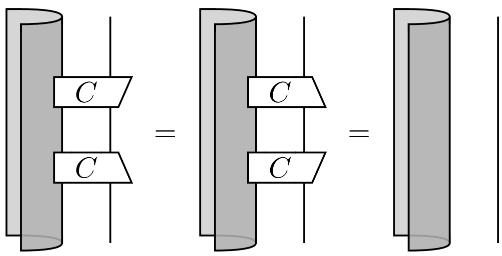
We now move to controlled operations in this setting.

Definition 8.56. In **2Hilb**, a *control 2-morphism* is a unitary of the following type, where the surface corresponds to a normalized oriented duality of dimension n:



(8.37)

The unitarity equations take the following form:



(8.38)

We can understand the linear algebraic content of a control 2-morphism by applying the graphical calculus for monoidal 2-categories, according to which a unitary 2-morphism of the form (8.37) is a parameterized family of unitaries of type $H \to H$. This is precisely the data of a controlled operation, as defined by Definition 0.64.

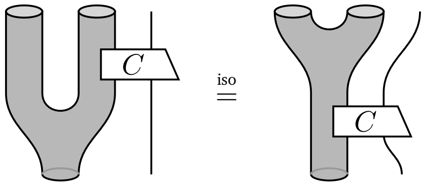
Lemma 5.61 and Example 7.8 showed that controlled operations correspond exactly to unitary module homomorphisms between free modules of classical structures. This is consistent with the 2-categorical perspective.

Lemma 8.57. *The following are equivalent:*

(a) in **Hilb***, a unitary module homomorphism between free modules of classical structures;*

(b) in **2Hilb***, a control 2-morphism for a special dagger oriented duality.*

Proof. This is immediate, since Lemma 5.61 showed that (a) corresponds to a list of unitary operators, which is exactly the data of (b). However, we can also represent the implication (b)⇒(a) in a structural way, exhibiting the module homomorphism condition topologically as follows:



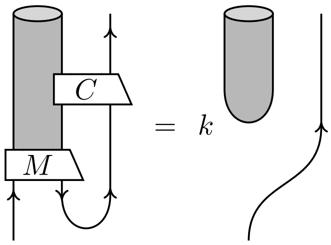
(8.39)

Here the comonoid structure arises from the oriented duality itself, and the proof is entirely geometrical. □

8.3.2 Quantum teleportation

Quantum teleportation involves a measurement and a controlled operation. Since we know how to model these using oriented dualities, we can give a model of the quantum teleportation procedure itself, as follows.

Definition 8.58. The *quantum teleportation equation* for a measurement 2-morphism and a control 2-morphism in **2Hilb** is the following condition, where $k \in \mathbb{C}$ is some invertible scalar factor:



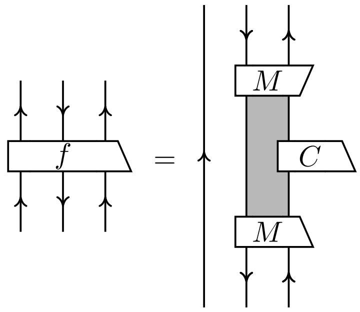
(8.40)

Note that this requires a measurement 2-morphism whose source is a tensor product $H \otimes H^*$ of a Hilbert space and its dual.

This model for quantum teleportation if the fifth that we have seen in this book, with previous models in Section 0.3.6 in terms of linear algebra, Section 3.2.1 in terms of dual objects in monoidal categories, Section 5.6.3 in terms of modules for classical structures, and Section 7.5 in terms of completely positive maps. Each successive version uses additional categorical structure, giving an increasingly high-level perspective from which to understand teleportation as a computational process. This final presentation in terms of oriented dualities is in some sense the most minimal, in the sense that it consists of a single equation, with the necessary algebraic foundations entirely taken care of by the topological notation. Of course, in another sense, it is the most complex, requiring an ambient monoidal 2-category for its very definition. This is a pattern familiar frrom any use of categorical methods: you pay up front for a more sophisticated setting, but once that has been established, the reward is an expressive language with the potential to describe complex processes in a simple way.

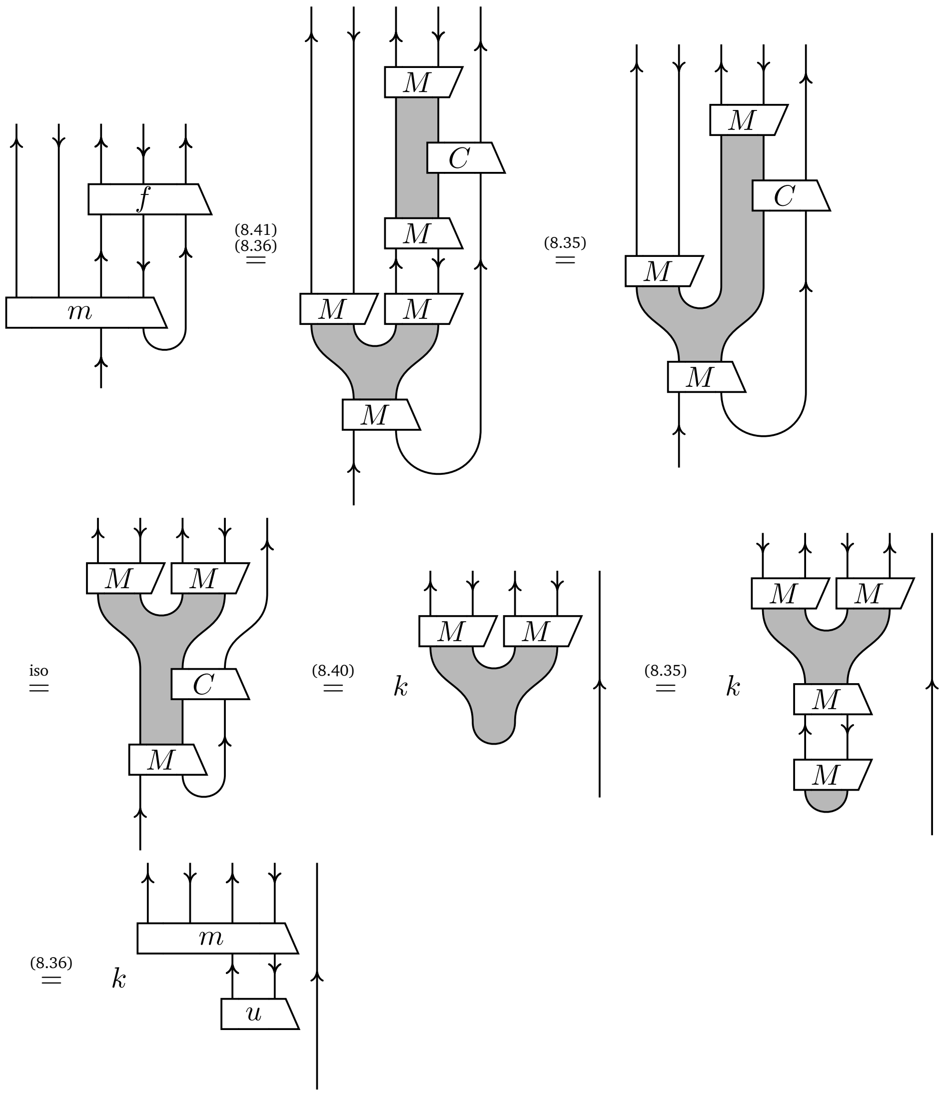
The graphical calculus of **2Hilb** makes it is easy to see that a solution of equation (8.40) yields a solution of (5.51). We define the dagger Frobenius structure via

Definition 8.55, and the module homomorphism f as follows:



(8.41)

Then (5.51) can be verified as follows:

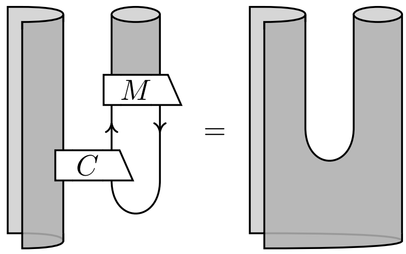


8.3.3 Quantum dense coding

Quantum dense coding is a quantum protocol that transmits two classical bits from one party to another by passing a single qubit. This is surprising, since it seems like a single qubit should be able to encode just one classical bit, with values given by the computational basis states $|0\rangle$ and $|1\rangle$. This surprising capability is driven by an entangled pair of qubits that are shared between the parties, although since this could have been prepared long in the past, before the decision was made as to which 2 bits would be transmitted, it does not provide a straightforward explanation for how it makes the procedure possible.

As with quantum teleportation, quantum dense coding involves a measurement and a controlled operation.

Definition 8.59. The *quantum dense coding equation* for a measurement 2-morphism and a control 2-morphism in **2Hilb** is the following equation, where $k \in \mathbb{C}$ is some invertible scalar factor:



(8.42)

As with the quantum teleportation equation (8.40), the left-hand side describes the protocol, and the right-hand side its intended effect. The protocol consists of the following steps:

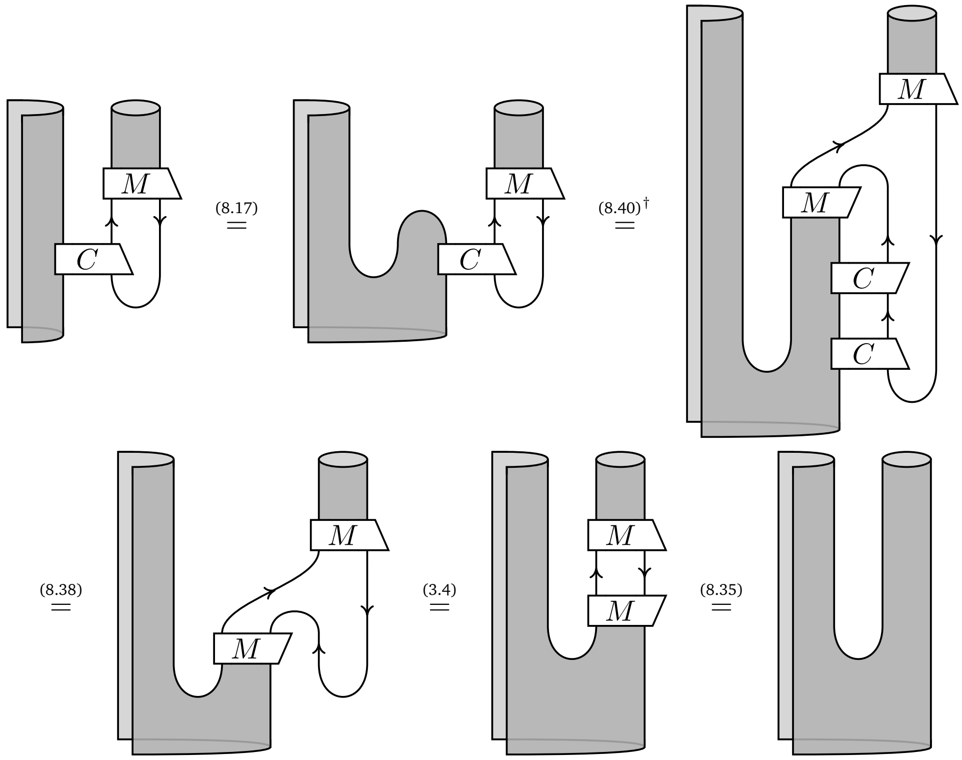
1. begin with a single surface, encoding 2 classical bits;
2. share an entangled state of 2 qubits between the parties;
3. perform a controlled operation on the first qubit;
4. pass the first qubit across;
5. measure both qubits together.

The intended effect, on the right-hand side of (8.42), is that the initial classical data is copied to the second party.

Definition 8.59 describes the protocol abstractly, but it is not clear a priori whether the protocol is possible in reality; that is, whether equation (8.42) has any solutions in **2Hilb**. The following theorem shows that solutions exist, and in fact correspond exactly to solutions of the quantum teleportation equation.

Theorem 8.60. *In* **2Hilb***, a measurement 2-morphism and a control 2-morphism satisfy the teleportation equation* (8.40) *if and only if they satisfy the quantum dense coding equation* (8.42).

Proof. Start with the teleportation equation. Deform the surface, and then use the dagger of the teleportation equation. The C and $C^\dagger$ then cancel, and the snake equation straightens a wire. Finally, use unitarity of M:



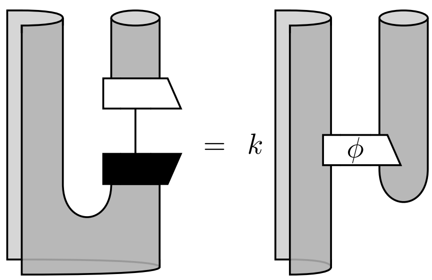
The converse proof, that a solution of the dense coding equation yields a solution of the teleportation equation, is similar. □

8.3.4 Complementarity

Finally, we use the 2-categorical technology of this chapter to study the complementarity of Chapter 6. We will write down a quantum protocol that exhibits the physical phenomenon of complementarity, and then derive the standard complementarity relationship of Definition 6.3.

Physically, complementarity is the phenomenon of two measurement bases which are as different as possible from one another. We use this to obtain the following operational definition.

Definition 8.61. In **2Hilb**, two measurement 2-morphisms (drawn here in black and white) satisfy the *complementarity condition* when there exists a unitary 2-morphism ϕ satisfying the following equation:



(8.43)

Again, the physical content of this condition is that the left-hand side interprets a protocol to be followed, and the right-hand side describes the intended effect. The protocol involves the following steps:

1. input some classical information;
2. copy it;
3. take the second copy, and use it to prepare a quantum system using the black measurement basis;
4. measure this quantum system using the white basis.

If these measurement bases are as unrelated as possible, the initial classical information should be classically uncorrelated to the final measurement outcome. There may still be quantum phase correlations, as these are classically unobservable. The right-hand side of (8.43) describes this procedure:

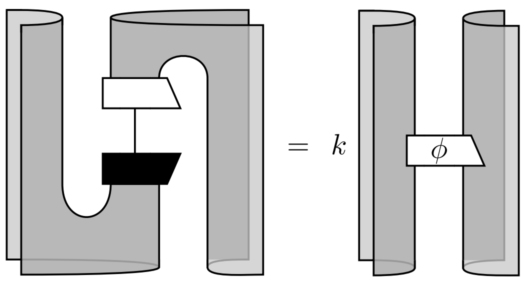
1. input some classical information;
2. independently prepare some additional classical information uniformly at random;
3. apply an arbitrary phase, which may depend on both pieces of classical data.

The following theorem shows that a solution to the complementarity condition corresponds exactly to complementarity as defined in terms of interacting Frobenius structures in Chapter 6.

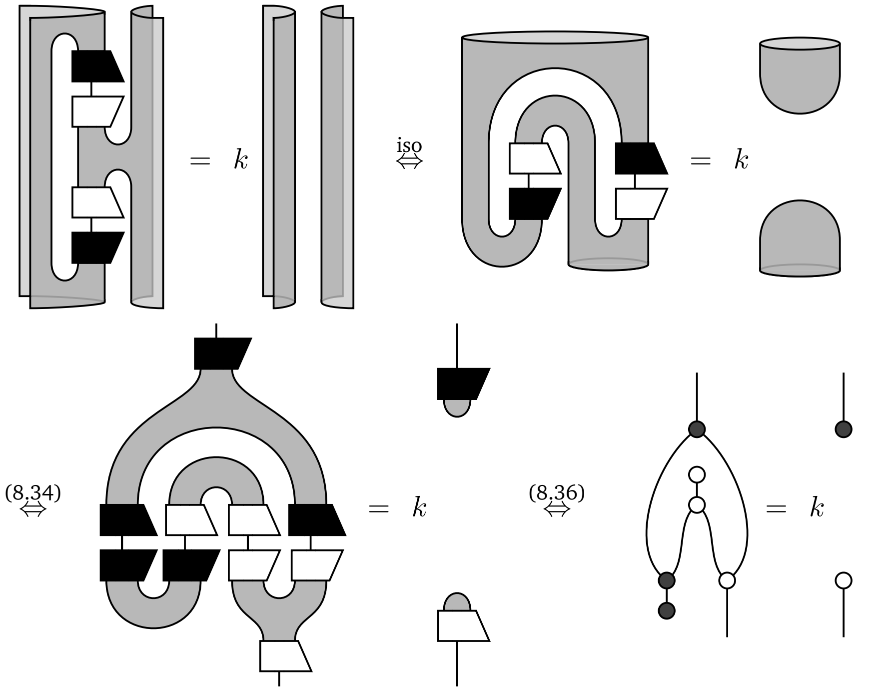
Theorem 8.62. *For a pair of measurements on a Hilbert space, the following are equivalent:*

- *in* **2Hilb***, represented as measurement 2-morphisms, they satisfy the complementarity condition* (8.43)*;*
- *in* **Hilb***, represented as commutative dagger Frobenius structures, they satisfy the complementarity condition of Definition 6.3.*

Proof. Taking the 2-categorical complementarity condition and bending down the top-right part of the surface gives the following equivalent condition:



This says exactly that the composite on the left-hand side is unitary. Write out the unitarity condition and rearrange it as follows:



This completes the proof. $\square$

8.4 Exercises

Exercise 8.4.1. Let H be a Hilbert space. Show that $\mathbf{2Hilb}(\mathbf{H}, \mathbf{H})$ is a pivotal category, with tensor product given by composition of linear functors.

Exercise 8.4.2. Suppose objects L, R, R' in a monoidal 2-category satisfy coherent dualities $L \dashv R$ and $L \dashv R'$. Show that R and R' are canonically adjoint equivalent. (That is, prove Theorem 8.20.)

Exercise 8.4.3. Hadamard + Hadamard + Hadamard = Teleportation, including derivation of the explicit formula.

Exercise 8.4.4. Show that every commutative dagger Frobenius structure in **Hilb** arises from a dagger oriented duality in **2Hilb** by transport across a unitary. (That is, prove Theorem 8.51.)

Notes and further reading

Terminology warning: what we call '2-category' has often been called 'bicategory' or a 'weak 2-category'. Similarly, what we call 'strict 2-category' has been called 'strict bicategory' or '2-category'. As weak higher categories become more important, our terminology is becoming more prevalent.

Higher-dimensional categories were first hinted at by Grothendieck [69]. For a modern overview, see [102]. Monoidal categories are 2-categories with one object; braided monoidal categories are 3-categories with one object and one 1-morphism; symmetric monoidal categories are 4-categories with one object, one 1-morphism and one 2-morphism. It is expected that n-categories have an n-dimensional graphical calculus; see [14].

The study of higher-dimensional categories is sometimes called higher-dimensional algebra. This was first applied to groupoids, mainly by Brown in the 1980s [30]. The importance of higher-dimensional algebra to physics was recognized in the 1990s [50] and popularized by Baez and Dolan in a series of papers from 1995 [15]. The 1997 second installment of the series introduced the notion of 2-Hilbert space [12], building on 1994 purely mathematical work by Kapranov and Voevodsky [87].

It is a classic result from Lawvere, in 1973, that completeness of metric spaces may be cast categorically. Think of the points of a metric space as objects, with the distance between them giving a 'homset'. More precisely, metric spaces are categories enriched over $[0, \infty]$ [100]. The metric space is complete exactly when idempotents split in this enriched category. Bartlett characterized 2-Hilbert spaces via this notion of Cauchy completion in 2009 [20].

Duals in monoidal 2-categories were first studied topologically by Carter in 1997 [32]. This was categorified explicitly in 2009 by Schommer-Pries [127] and Bartlett [20]. Nonoriented dualities were also studied by Stay in 2016 [134]. This led to a combinatorial description of 3-dimensional topological quantum field theories by Bartlett, Douglas, Schommer-Pries, and Vicary, in 2015 [21].

Quantum dense coding, also called superdense coding, was discovered in 1992 by Bennett and Wiesner [25]. All possible teleportation and coding schemes, and their relationships, were worked out by Werner in 2001 [142]. Categorification led to the equational framework in this chapter, by Vicary in 2013 [140, 139].

Finally, to link this chapter to Chapter 7, the relationship between complete positivity and 2-categories was made explicit by Heunen, Vicary, and Wester, in 2014 [77].

Bibliography

Exercise 8.415. Lowell Abrams. *Frobenius algebra structures in topological quantum field theory and quantum cohomology*. PhD thesis, Johns Hopkins University, 1997.

[2] Samson Abramsky. Abstract scalars, loops, and free traced and strongly compact closed categories. In *Algebra and Coalgebra in Computer Science*, CALCO'05, pages 1–30. Springer, 2005.

[3] Samson Abramsky. No-cloning in categorical quantum mechanics. In Simon Gay and Ian Mackey, editors, *Semantic Techniques in Quantum Computation*, pages 1–28. Cambridge University Press, 2010.

[4] Samson Abramsky and Bob Coecke. A categorical semantics of quantum protocols. In *Logic in Computer Science 19*, pages 415–425. IEEE Computer Society, 2004.

[5] Samson Abramsky and Bob Coecke. Abstract physical traces. *Theory and Applications of Categories*, 14(6):111–124, 2005.

[6] Samson Abramsky and Chris Heunen. H*-algebras and nonunital Frobenius algebras: first steps in infinite-dimensional categorical quantum mechanics. *Clifford Lectures, AMS Proceedings of Symposia in Applied Mathematics*, 71:1–24, 2011.

[7] Warren Ambrose. Structure theorems for a special class of Banach algebras. *Transactions of the American Mathematical Society*, 57:364–386, 1945.

[8] William B. Arveson. Subalgebras of C*-algebras. *Acta Mathematica*, 123(1):141–224, 1969.

[9] Steve Awodey. *Category Theory*. Oxford Logic Guides. Oxford University Press, 2006.

[10] Miriam Backens. The ZX-calculus is complete for stabilizer quantum mechanics. *New Journal of Physics*, 16:093021, 2014.

[11] Miriam Backens. The ZX-calculus is complete for the single-qubit Clifford+T group. In Coecke et al. [40], pages 293–303.

[12] John C. Baez. Higher-dimensional algebra II: 2-Hilbert spaces. *Advances in Mathematics*, 127(2):125–189, 1997.

[13] John C. Baez. Quantum quandries: A category-theoretic perspective. In Dean Rickles Steven French and Juha Saatsi, editors, *Structural Foundations of Quantum Gravity*, pages 240–265. Oxford University Press, 2006.

[14] John C. Baez and James Dolan. Higher-dimensional algebra and topological quantum field theory. *Journal of Mathematical Physics*, 36:6073–6105, 1995.

[15] John C. Baez and James Dolan. Higher-dimensional algebra and topological quantum field theory. *Journal of Mathematical Physics*, 36:6073–6105, 1995.

[16] Bojko Bakalov and Alexander Kirillov, Jr. *Lectures on Tensor Categories and Modular Functors*, volume 21 of *University Lecture Series*. American Mathematical Society, 2001.

[17] Howard Barnum, Jonathan Barrett, Matthew Leifer, and Alexander Wilce. A generalized no-broadcasting theorem. *Physical Review Letters*, 99:240501, 2007.

[18] Howard Barnum, Carlton M. Caves, Chris A. Fuchs, Richard Jozsa, and Benjamin Schumacher. Noncommuting mixed states cannot be broadcast. *Physical Review Letters*, 76(15):2818–2821, 1996.

[19] Michael Barr. **-autonomous categories*, volume 752 of *Lecture Notes in Mathematics*. Springer, 1979.

[20] Bruce Bartlett. *On unitary 2-representations of finite groups and topological quantum field theory*. PhD thesis, Department of Mathematics, University of Sheffield, 2008. arXiv:0901.3975.

[21] Bruce Bartlett, Christopher L. Douglas, Christopher Schommer-Pries, and Jamie Vicary. Modular categories as representations of the 3-dimensional bordism 2-category. arXiv:1509.06811, 2015.

[22] E. Batista, S. Caenepeel, and J. Vercruysse. Hopf categories. *Algebras and Representation Theory*, 19(5):1173–1216, 2016.

[23] Jean Bénabou. Categories avec multiplication. *Comptes Rendus de l'Acadmie des Sciences. Série I. Mathmatique*, pages 1887–1890, 1963.

[24] Charles H. Bennett, Giles Brassard, Claue Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895–1899, 1993.

[25] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Physical Review Letters*, 69(20):2881, 1992.

[26] Rejandra Bhatia. *Positive definite matrices*. Princeton University Press, 2007.

[27] Francis Borceux. *Handbook of Categorical Algebra*. Encyclopedia of Mathematics and its Applications 50–52. Cambridge University Press, 1994.

[28] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, and Anton Zeilinger. Experimental quantum teleportation. *Nature*, 390:575–579, 1997.

[29] Richard Brauer and Cecil J. Nesbitt. On the regular representations of algebras. *Proceedings of the National Academy of Sciences of the United States of America*, 23:236–240, 1937.

[30] Ronald Brown. From groupds to groupoids: a brief survey. *Bulleting of the London Mathematical Society*, 19:113–134, 1987.

[31] Aurelio Carboni and Richard F. C. Walters. Cartesian bicategories I. *Journal of Pure and Applied Algebra*, 49:11–32, 1987.

[32] Scott Carter, Masahico Saito, and Joachim Rieger. A combinatorial description of knotted surfaces and their isotopies. *Advances in Mathematics*, 127:1–51, 1997.

[33] Stephen U. Chase and Moss Sweedler. *Hopf algebras and Galois theory*. Number 97 in Lecture Notes in Mathematics. Springer, 1969.

[34] Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear Algebra and Its Applications*, 10(3):285–290, 1975.

[35] Bob Coecke. The logic of entanglement: An invitation. Technical report, University of Oxford, 2003. Computing Laboratory Research Report PRG-RR-03-12.

[36] Bob Coecke. De-linearizing linearity: projective quantum axiomatics from strong compact closure. In Bob Coecke, Prakash Panangaden, and Peter Selinger, editors, *Proceedings of the 5th Workshop on Quantum Physics and Logic*, volume 270 of *Electronic Notes in Theoretical Computer Science*, pages 49–72, 2008.

[37] Bob Coecke and Ross Duncan. Interacting quantum observables. *New Journal of Physics*, 13(4):043016, 2011.

[38] Bob Coecke, Ross Duncan, Aleks Kissinger, and Quanlong Wang. Strong complementarity and non-locality in categorical quantum mechanics. In *Logic in Computer Science*, pages 245–254, 2012.

[39] Bob Coecke, Bill Edwards, and Robert W. Spekkens. Phase groups and the origin of non-locality for qubits. In Duncan and Panangaden [56], pages 15–36.

[40] Bob Coecke, Ichiro Hasuo, and Prakash Panangaden, editors. *Proceedings of the 11th Workshop on Quantum Physics and Logic*, volume 172 of *Electronic Proceedings in Theoretical Computer Science*, 2014.

[41] Bob Coecke and Chris Heunen. Pictures of complete positivity in arbitrary dimension. *Electronic Proceedings in Theoretical Computer Science*, 95:27–35, 2011.

[42] Bob Coecke, Chris Heunen, and Aleks Kissinger. Categories of quantum and classical channels. *Quantum Information Processing*, 15(12):5179–5209, 2016.

[43] Bob Coecke and Matty Hoban, editors. *Proceedings of the 10th Workshop on Quantum Physics and Logic*, volume 171 of *Electronic Proceedings in Theoretical Computer Science*, 2014.

[44] Bob Coecke and Aleks Kissinger. *Picturing quantum processes: a first course in quantum theory and diagrammatic reasoning*. Cambridge University Press, 2017.

[45] Bob Coecke and Raymond Lal. Causal categories: relativistically interacting processes. *Foundations of Physics*, 43(4):458–501, 2012.

[46] Bob Coecke, Éric O. Paquette, and Simon Perdrix. Bases in diagrammatic quantum protocols. In *Mathematical Foundations of Programming Semantics 24*, volume 218 of *Electronic Notes in Theoretical Computer Science*, pages 131–152. Elsevier, 2008.

[47] Bob Coecke and Duško Pavlović. Quantum measurements without sums. In *Mathematics of Quantum Computing and Technology*. Taylor and Francis, 2007.

[48] Bob Coecke, Duško Pavlović, and Jamie Vicary. A new description of orthogonal bases. *Mathematical Structures in Computer Science*, 23(3):555–567, 2013.

[49] Bob Coecke and Simon Perdrix. Environment and classical channels in categorical quantum mechanics. In *Proceedings of the 19th EACSL Annual Conference on Computer Science Logic (CSL)*, volume 6247 of *Lecture Notes in Computer Science*, pages 230–244, 2010.

[50] Louis Crane. 2-d physics and 3-d topology. *Communications in Mathematical Physics*, 35:615–640, 1991.

[51] Oscar Cunningham and Chris Heunen. Axiomatizing complete positivity. In Duncan and Panangaden [56].

[52] Kenneth R. Davidson. *C*-algebras by example*. American Mathematical Society, 1991.

[53] Brian J. Day. Note on compact closed categories. *Journal of the Australian Mathematical Society*, Series A 24(3):309–311, 1977.

[54] Dennis Dieks. Communication by EPR devices. *Physics Letters A*, 92(6):271–272, 1982.

[55] Robbert Dijkgraaf. *A geometric approach to two dimensional conformal field theory*. PhD thesis, University of Utrecht, 1989.

[56] Ross Duncan and Prakash Panangaden, editors. *Proceedings of the 9th Workshop on Quantum Physics and Logic*, volume 158 of *Electronic Proceedings in Theoretical Computer Science*, 2012.

[57] Ross Duncan and Simon Perdrix. Graph states and the necessity of Euler decomposition. In Klaus Ambos-Spies, Benedikt Löwe, and Wolfgang Merkle, editors, *Computability in Europe*, volume 5635 of *Lecture Notes in Computer Science*, pages 167–177. Springer, 2009.

[58] Ross Duncan and Simon Perdrix. Pivoting makes the ZX-calculus complete for real stabilizers. In Coecke and Hoban [43], pages 50–62.

[59] Bill Edwards. *Non-locality in categorical quantum mechanics*. PhD thesis, Oxford University, 2009.

[60] Douglas R. Farenick. *Algebras of Linear Transformations*. Springer, 2001.

[61] Kang Feng Ng and Quanlong Wang. A universal completion of the ZX-calculus. arXiv:1706.09877, 2017.

[62] Peter Freyd. *Abelian Categories: An Introduction to the Theory of Functors*. Harper and Row, 1964.

[63] Peter Freyd and David N. Yetter. Coherence theorems via knot theory. *Journal of Pure and Applied Algebra*, 78:49–76, 1992.

[64] F. Georg Frobenius. Theorie der hyperkomplexen grössen. *Sitzungsberichte der Koniglich Preussischen Akademie Der Wissenschaften*, 24:504–537; 634–645, 1903.

[65] Richard Garner and Daniel Schäppi. When coproducts are biproducts. *Mathematical Proceedings of the Cambridge Philosophical Society*, 161:47–51, 2016.

[66] Israel M. Gelfand. On normed rings. *Doklady Akademii Nauk SSSR*, 23:430–432, 1939.

[67] Israel M. Gelfand. Positive definite operator functions on a commutative group. *Izvestiya Rossiiskoi Akademii Nauk USSR Matematicheskaya*, 7:237–244, 1943.

[68] Brett Giles. *An investigation of some theoretical aspects of reversible computing*. PhD thesis, University of Calgary, 2014.

[69] Alexandre Grothendieck. Pursuing stacks. Documents Mathématiques, Société Mathétique de France, 1983. Letter to Daniel Quillen.

[70] Masahito Hasegawa. On traced monoidal closed categories. *Mathematical Structures in Computer Science*, 19:217–244, 2008.

[71] Chris Heunen. An embedding theorem for Hilbert categories. *Theory and Applications of Categories*, 22(13):321–344, 2009.

[72] Chris Heunen and Sergio Boixo. Completely positive classical structures and sequentializable quantum protocols. *Electronic Proceedings in Theoretical Computer Science*, 95:91–101, 2011.

[73] Chris Heunen, Ivan Contreras, and Alberto S. Cattaneo. Relative Frobenius algebras are groupoids. *Journal of Pure and Applied Algebra*, 217:114–124, 2012.

[74] Chris Heunen and Martti Karvonen. Reversible monadic programming. In *Mathematical Foundations of Programming Semantics*, 2015.

[75] Chris Heunen, Aleks Kissinger, and Peter Selinger. Completely positive projections and biproducts. In Coecke and Hoban [43], pages 71–83.

[76] Chris Heunen and Sean Tull. Categories of relations as models of quantum theory. In Chris Heunen, Peter Selinger, and Jamie Vicary, editors, *Proceedings of the 12th Workshop on Quantum Physics and Logic*, volume 195 of *Electronic Proceedings in Theoretical Computer Science*, pages 247–261, 2015.

[77] Chris Heunen, Jamie Vicary, and Linde Wester. Mixed quantum states in higher categories. In Coecke et al. [40], pages 304–315.

[78] Heinz Hopf. Über die Topologie der Gruppen-Mannigfaltigkeiten und ihrer Verallgemeinerungen. *Annals of Mathematics*, 42:22–52, 1941.

[79] Robin Houston. Finite products are biproducts in a compact closed category. *Journal of Pure and Applied Algebra*, 212(2):394–400, 2008.

[80] Bart Jacobs. Semantics of weakening and contraction. *Annals of Pure and Applied Logic*, 69:73–106, 1994.

[81] Andrzej Jamiołkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Reports on Mathematical Physics*, 3:275–278, 1972.

[82] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. A complete axiomatisation of the ZX-calculus for Clifford+T quantum mechanics. arXiv:1705.11151, 2017.

[83] André Joyal and Ross Street. The geometry of tensor calculus I. *Advances in Mathematics*, 88:55–113, 1991.

[84] André Joyal and Ross Street. An introduction to Tannaka duality and quantum groups. In *Category Theory, Part II*, volume 1488 of *Lecture Notes in Mathematics*, pages 411–492. Springer, 1991.

[85] André Joyal and Ross Street. Braided tensor categories. *Advances in Mathematics*, 102:20–78, 1993.

[86] André Joyal, Ross Street, and Dominic Verity. Traced monoidal categories. *Mathematical Proceedings of the Cambridge Philosophical Society*, 3:447–468, 1996.

[87] Mikhail M. Kapranov and Vladimir Voevodsky. 2-categories and Zamolodchikov tetrahedra equations. *Proceedings of Symposia in Pure Mathematics*, 56(2):177–260, 1994.

[88] Christian Kassel. *Quantum Groups*. Springer, 1995.

[89] Louis H. Kaufmann. *Knots and Physics*. World Scientific, 1994.

[90] Louis H. Kaufmann. Teleportation topology. *Optics and spectroscopy*, 99:227–232, 2005.

[91] Phillip Kaye, Raymond Laflamme, and Michele Mosca. *An introduction to quantum computing*. Oxford University Press, 2007.

[92] G. Max Kelly. Many variable functorial calculus (I). In *Coherence in Categories*, volume 281 of *Lecture Notes in Mathematics*, pages 66–105. Springer, 1970.

[93] G. Max Kelly. *Basic Concepts of Enriched Category Theory*. Cambridge University Press, 1982.

[94] G. Max Kelly and Miguel L. Laplaza. Coherence for compact closed categories. *Journal of Pure and Applied Algebra*, 19:193–213, 1980.

[95] Michael Keyl. Fundamentals of quantum information theory. *Physical Reports*, 369:431–548, 2002.

[96] Joachim Kock. *Frobenius algebras and 2-D Topological Quantum Field Theories*. Number 59 in London Mathematical Society Student Texts. Cambridge University Press, 2003.

[97] Karl Kraus. General state changes in quantum theory. *Annals of Physics*, 64(2):311–335, 1971.

[98] Stephen Lack. Composing PROPs. *Theory and Applications of Categories*, 13:147–163, 2004.

[99] F. William Lawvere. Ordinal sums and equational doctrines. In Beno Eckmann, editor, *Seminar on triples and categorical homology theory*, number 80 in Lecture Notes in Mathematics, pages 141–155, 1967.

[100] F. William Lawvere. Metric spaces, generalized logic, and closed categories. *Rendiconti del Seminario Matematico e Fisico di Milano*, 43(1):135–166, 1973.

[101] F. William Lawvere and Stephen Schanuel. *Conceptual Mathematics: A First Introduction to Categories*. Cambridge University Press, 2009.

[102] Tom Leinster. *Higher operads, higher categories*. Number 298 in London Mathematical Society Lecture Note Series. Cambridge University Press, 2004.

[103] Tom Leinster. *Basic Category Theory*. Cambridge University Press, 2014.

[104] Saunders Mac Lane. Duality for groups. *Bulletin of the American Mathematical Society*, 56(6):485–516, 1950.

[105] Saunders Mac Lane. An algebra of additive relations. *Proceedings of the National Academy of Sciences*, 47:1043–1051, 1961.

[106] Saunders Mac Lane. Natural associativity and commutativity. *Rice University Studies*, 49:28–46, 1963.

[107] Saunders Mac Lane. *Categories for the Working Mathematician*. Springer, 2nd edition, 1971.

[108] Shahn Majid. *Foundations of quantum group theory*. Cambridge University Press, 2000.

[109] Stefan Milius. Relations in categories. Master's thesis, York University, 2000.

[110] Barry Mitchell. *Theory of Categories*. Academic Press, 1965.

[111] Tadasi Nakayama. On Frobeniusean algebras II. *Annals of Mathematics*, 42(1):1–21, 1941.

[112] Eric Nummela. Cayley's theorem for topological groups. *American Mathematical Monthly*, 87(3):202–203, 1980.

[113] Jiannis K. Pachos. *Introduction to Topological Quantum Computation*. Cambridge University Press, 2012.

[114] Paul H. Palmquist. Adjoint functors induced by adjoint linear transformations. *Proceedings of the American Mathematical Society*, 44(2):251–254, 1974.

[115] Vern Paulsen. *Completely bounded maps and operators algebras*. Cambridge University Press, 2002.

[116] Duško Pavlović. Quantum and classical structures in nondeterministic computation. In P. Bruza et al., editor, *Third International symposium on Quantum Interaction*, volume 5494 of *Lecture Notes in Artificial Intelligence*, pages 143–157. Springer, 2009.

[117] Duško Pavlovic. Geometry of abstraction in quantum computation. In *Classical and Quantum Information Assurance Foundations and Practice*, number 09311 in Dagstuhl Seminar Proceedings, 2010.

[118] Roger Penrose. Applications of negative dimensional tensors. In Dominic J. A. Welsh, editor, *Combinatorial mathematics and its applications*, pages 221–244. Academic Press, 1971.

[119] Simon Perdrix. State transfer instead of teleportation in measurement-based quantum computation. *International journal of quantum information*, 3(1):219–223, 2005.

[120] Zoran Petrić. Coherence in substructural categories. *Studia Logica*, 70(2):271–296, 2002.

[121] Frank Quinn. Lectures on axiomatic topological quantum field theory. In *Geometry and quantum field theory*, pages 323–453. American Mathematical Society, 1995.

[122] Robert Raussendorf and Hans J. Briegel. A one-way quantum computer. *Physical Review Letters*, 86(22):5188, 2001.

[123] Michael Reed and Barry Simon. *Methods of Modern Mathematical Physics I: Functional Analysis*. Academic Press, 1980.

[124] Emily Riehl. *Category Theory in Context*. Dover, 2016.

[125] Neantro Saavedra Rivano. *Categories Tanakiennes*, volume 265 of *Lecture Notes in Mathematics*. Springer, 1972.

[126] Léon Rosenfeld. *Foundations of Quantum Physics II*, chapter Complementarity: Bedrock of the quantal description, pages 284–285. Number 7 in Niels Bohr, collected works. Elsevier, 1996.

[127] Christopher Schommer-Pries. *The Classification of Two-Dimensional Extended Topological Field Theories*. PhD thesis, Department of Mathematics, University of California, Berkeley, 2009.

[128] Christian Schröder de Witt and Vladimir Zamdzhiev. The ZX-calculus is incomplete for quantum mechanics. In Coecke et al. [40], pages 285–292.

[129] Julian Schwinger. Unitary operator bases. *Proceedings of the National Academy of Sciences: Physics*, 46:570–579, 1960.

[130] Robert A. G. Seely. Linear logic, $*$-autonomous categories and cofree coalgebras. In *Categories in Computer Science and Logic*, volume 92, pages 371–382. American Mathematical Society, 1989.

[131] Peter Selinger. Dagger compact closed categories and completely positive maps. In Peter Selinger, editor, *Proceedings of the 3rd International Workshop on Quantum Programming Languages*, volume 170 of *Electronic Notes in Theoretical Computer Science*, pages 139–163, 2007.

[132] Peter Selinger. Idempotents in dagger categories. In Peter Selinger, editor, *Proceedings of the 4th International Workshop on Quantum Programming Languages*, volume 210 of *Electronic Notes in Theoretical Computer Science*, pages 107–122, 2008.

[133] Peter Selinger. A survey of graphical languages for monoidal categories. In *New Structures for Physics*, Lecture Notes in Physics. Springer, 2009.

[134] Michael Stay. Compact closed bicategories. *Theory and Applications of Categories*, 31:755–798, 2016.

[135] W. Forrest Stinespring. Positive functions on C*-algebras. *Proceedings of the American Mathematical Society*, pages 211–216, 1955.

[136] Ross Street. *Quantum Groups: a path to current algebra*. Number 19 in Australian Mathematical Society Lecture Series. Cambridge University Press, 2007.

[137] Jamie Vicary. Categorical formulation of finite-dimensional quantum algebras. *Communications in Mathematical Physics*, 304:765–796, 2011.

[138] Jamie Vicary. Completeness of †-categories and the complex numbers. *Journal of Mathematical Physics*, 52:082104, 2011.

[139] Jamie Vicary. Higher semantics of quantum protocols. In *Logic in Computer Science*, pages 606–615, 2012.

[140] Jamie Vicary. Topological structure of quantum algorithms. In *2013 28th Annual ACM/IEEE Symposium on Logic in Computer Science*. Institute of Electrical & Electronics Engineers (IEEE), 2013.

[141] John von Neumann. On rings of operators. *Annals of Mathematics*, 37(1):116–229, 1936.

[142] Reinhard F. Werner. All teleportation and dense coding schemes. *Journal of Physics A*, 34(35):7081–7094, 2001.

[143] William K. Wootters and Wojciech H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[144] David N. Yetter. *Functorial knot theory: categories of tangles, coherence, categorical deformations, and topological invariants*. World Scientific, 2001.

Index