# Categorical Quantum Mechanics
## *An Introduction*

Chris Heunen and Jamie Vicary

Department of Computer Science, University of Oxford
16 Lectures, Hilary Term 2015

# Contents

# Chapter 0

# Basics

Solid foundations for this book would be given by traditional first courses in category theory and quantum computing. However, there is not much material that is truly essential, and this chapter gives an introduction to these areas from first principles, making this book self-contained. What distinguishes this chapter from the rest of this book is that everything here can be found in more detail in many other standard texts (see the notes at the end of this chapter for references).

This material is presented in three sections. Section 0.1 gives an introduction to category theory, and in particular the category $\mathbf{Set}$ 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 computation, including the standard interpretation of states, dynamics and measurement.

## 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 isomorphism, 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 two 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*:

$$h \circ (g \circ f) = (h \circ g) \circ f; \tag{1}$$

- *identity*:

$$\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A. \tag{2}$$

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 $\mathrm{id}_A$. This seems like a simple point, but in fact it is a significant departure from much of classical mathematics, in which particular structures (like groups) play a much 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 very well, since Russell's paradox prevents a set of all sets. However, such set-theoretical issues will not play a role in this book, and we will use set theory naively throughout.

### 0.1.2 The category $\mathbf{Set}$

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 $f: a \mapsto f(a)$ 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 ($\mathbf{Set}$, $\mathbf{FSet}$).** The category $\mathbf{Set}$ of sets and functions is defined as follows:

- **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 $g \circ f: a \mapsto g(f(a))$;
- **the identity morphism** on $A$ is the function $\mathrm{id}_A: a \mapsto a$.

Define the category $\mathbf{FSet}$ to be the restriction of $\mathbf{Set}$ to finite sets.

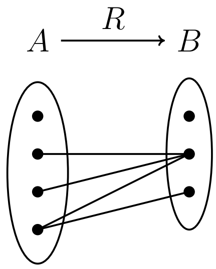
### 0.1.3 The category $\mathbf{Rel}$

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 $b \in B$ are such that $(a, b) \in R$, then 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.

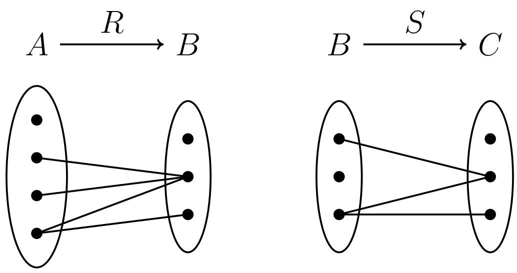
We can think of a relation $A \xrightarrow{R} B$ in a dynamical way, as indicating the possible ways in which elements of $A$ can evolve into elements of $B$. This suggests the following sort of picture:



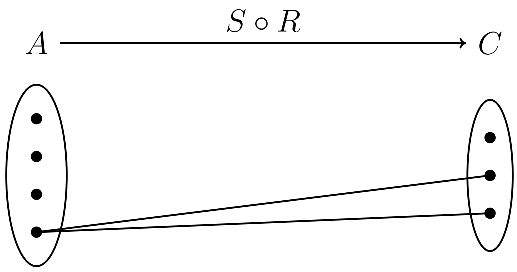

(3)

It 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 be related 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:

$$S \circ R := \{(a, c) \mid \exists b \in B \colon aRb \text{ and } bSc\} \subseteq A \times C \tag{4}$$

We can write this differently as

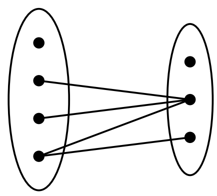
$$a\,(S \circ R)\,c \;\Leftrightarrow\; \bigvee_b (bSc \wedge aRb), \tag{5}$$

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:

$$(g \circ f)_{ij} = \sum_k g_{ik} f_{kj} \tag{6}$$

This suggests another way to interpret a relation: as a matrix of truth values. For the example relation (3), this gives the following matrix, where we write 0 for false and 1 for true:

$$A \xrightarrow{R} B$$



$$\rightsquigarrow \quad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{7}$$

Composition of relations is then just given by ordinary matrix multiplication, with logical disjunction and conjunction replacing $+$ and $\times$.

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, whereas matrix composition tells us the *amplitude* for this to happen.

The intuition we have developed leads to the following definition of the category $\mathbf{Rel}$.

**Definition 0.5** ($\mathbf{Rel}$, $\mathbf{FRel}$)**.** The category $\mathbf{Rel}$ of sets and relations is defined as follows:

- **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

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

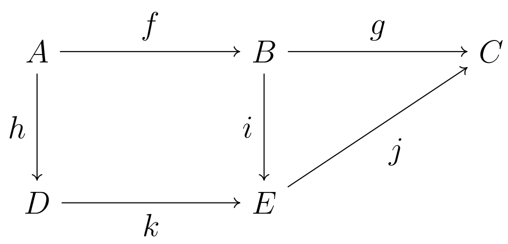
- **the identity morphism** on $A$ is the relation $\{(a,a) \in A \times A \mid a \in A\}$.

Define the category $\mathbf{FRel}$ to be 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 a way they can be composed. Here is an example:




(8)

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.

**Definition 0.6** (Domain, codomain, endomorphism)**.** 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*.

**Definition 0.7** (Isomorphism, isomorphic)**.** A morphism $A \xrightarrow{f} B$ is an *isomorphism* when there is a morphism $B \xrightarrow{f^{-1}} A$ satisfying the following equations:

$$f^{-1} \circ f = \mathrm{id}_A \qquad\qquad f \circ f^{-1} = \mathrm{id}_B \tag{9}$$

We then say that $A$ and $B$ are *isomorphic*, and write $A \simeq B$.

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

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

$$g \overset{(2)}{=} g \circ \mathrm{id} \overset{(9)}{=} g \circ (f \circ g') \overset{(1)}{=} (g \circ f) \circ g' \overset{(9)}{=} \mathrm{id} \circ g' \overset{(2)}{=} g'. \qquad \square$$

**Example 0.9.** Let us see what isomorphisms are like in our example categories:

- in **Set**, the isomorphisms are exactly the bijections of sets;
- in **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 $aRb \Leftrightarrow f(a) = b$;
- in **Vect** and **Hilb** (see Section 0.2), the isomorphisms are the bijective morphisms.

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

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

**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.

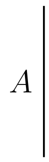
Finally, let us mention some important ways of constructing new categories from given ones.

**Definition 0.12.** 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.** 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 $B \xrightarrow{g} D$.

### 0.1.5 Graphical notation

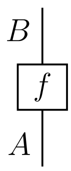
There is a graphical notation for morphisms and their composites. Draw an object $A$ as follows:




(10)

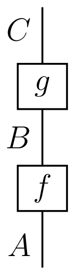
It's just a line. In fact, you should think of it as a picture of the identity morphism $A \xrightarrow{\mathrm{id}_A} A$. Remember: in category theory, the morphisms are more important than the objects.

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



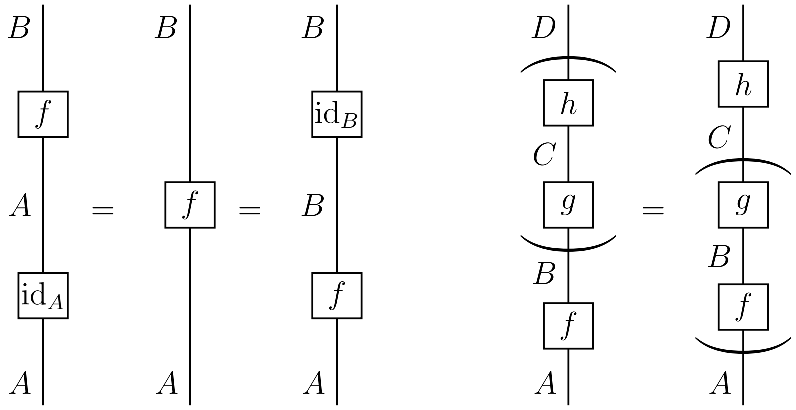

(11)

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:




(12)

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:




(13)

To make these laws immediately obvious, we choose to not depict the identity morphisms $\mathrm{id}_A$ 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; we usually draw it horizontally, and call it algebra.

## 0.1.6 Functors and natural transformations

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 0.14** (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 $A \xrightarrow{f} B$ 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 $\mathbf{C}$.

These are also called *covariant* functors. There are also *contravariant* functors that reverse the direction of morphisms: a contravariant functor $\mathbf{C} \to \mathbf{D}$ is a covariant functor $\mathbf{C}^{\mathrm{op}} \to \mathbf{D}$, and satisfies $F(g \circ f) = F(f) \circ F(g)$, where $\circ$ denotes composition in $\mathbf{C}$.

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 0.15.** 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 $B \simeq F(A)$.

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

**Definition 0.16** (Natural transformation, natural isomorphism)**.** Given functors $F\colon \mathbf{C} \to F\mathbf{D}$ and $G\colon \mathbf{C} \to \mathbf{D}$, a *natural transformation* $\zeta : F \Rightarrow G$ 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 $\mathbf{C}$.

$$\begin{array}{ccc} F(A) & \xrightarrow{\zeta_A} & G(A) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(B) & \xrightarrow[\zeta_B]{} & G(B) \end{array} \tag{14}$$

If every component $\zeta_A$ is an isomorphism then $\zeta$ is called a *natural isomorphism*, and $F$ and $G$ are said to be *naturally isomorphic*.

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

**Proposition 0.17** (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 $\mathrm{id}_D \simeq F \circ G$.* □

We revisit the notion of equivalence from a different perspective in Section 8.1.

Many important concepts in mathematics can be defined in a simple way using functors and natural transformations.

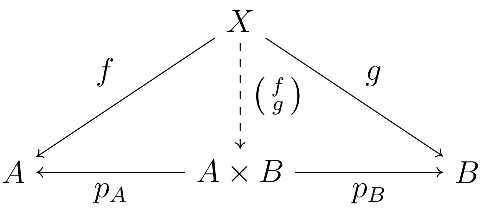
**Example 0.18.** A *group representation* is a functor $\mathbf{G} \to \mathbf{Vect}$, where $\mathbf{G}$ is a group seen as a category with one object (see Definition 0.11.) An *intertwiner* is a natural transformation between these functors.

### 0.1.7 Products and equalizers

Products and equalizers are recipes for finding objects and morphisms with *universal properties*, with great practical use in category theory. They are special cases of the theory of *limits*, which would form an important part of a typical category theory course.

To get the idea, it is useful to think about the disjoint union $S+T$ of sets $S$ and $T$. It is not 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.

**Definition 0.19** (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 $p_B \circ \left(\begin{smallmatrix} f \\ g \end{smallmatrix}\right) = g$. We can summarize these relationships with the following diagram:




A *coproduct* is the dual notion, obtained by reversing the directions of all the arrows in this diagram. Given object $A$ 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 $\left(\begin{smallmatrix} f & g \end{smallmatrix}\right) : A+B \to X$ such that $\left(\begin{smallmatrix} f & g \end{smallmatrix}\right) \circ i_A = f$ and $\left(\begin{smallmatrix} f & g \end{smallmatrix}\right) \circ i_B = g$.

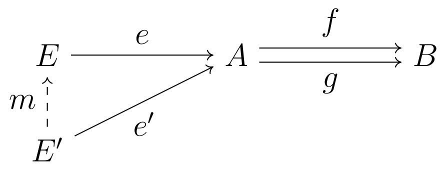
A category may or may not have products or coproducts. In our main example categories they do exist, as we now examine.

**Example 0.20.** Products and coproducts take the following form in our main example categories:

- in **Set**, products are given by the Cartesian product, and coproducts by the disjoint union;
- in **Rel**, products and coproducts are both given by the disjoint union;
- in **Vect** and **Hilb** (see Section 0.2), products and coproducts are both given by direct sum.

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 doesn't allow us to inspect elements in a direct way, but we can use equalizers to get the same information using a universal property.

**Definition 0.21.** 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 $e' = e \circ m$:




We may think of an equalizer as the largest part of $A$ on which $f$ and $g$ agree. In **Set**, it is given by $\{a \in A \mid f(a) = g(a)\}$. A *kernel* of a morphism $A \xrightarrow{f} B$ is an equalizer of $f$ and the *zero* morphism $A \xrightarrow{0} B$, which we will meet in Section 2.2. Again, equalizers may or may not exist in a particular category.

**Example 0.22.** 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 $E \rightarrowtail eA$.
- The category **Rel** does not have all equalizers. To see this, consider the following sketch argument. Consider the relations $\{1, 2, 3, 4\} \xrightarrow{R,S} \{\bullet\}$ given by the subsets $R = \{1, 2\}$ and $S = \{3, 4\}$. Then we can immediately give relations $\{\bullet\} \xrightarrow{T_i} \{1, 2, 3, 4\}$ which satisfy $R \circ T_i = S \circ T_i$, as the subsets $T_1 = \{1, 3\}$, $T_2 = \{1, 4\}$, $T_3 = \{2, 3\}$ and $T_4 = \{2, 4\}$. None of these relations factor through any of the others, so they must each form separate components of an equalizer, if it exists. Now consider $T_0 = \{1, 2, 3, 4\}$. It satisfies $R \circ T_0 = S \circ T_0$, and so must factor uniquely through any equalizer; but $T_0 = T_1 + T_4 = T_2 + T_3$, and so it factors non-uniquely through the part of the equalizer we have already constructed. Thus the equalizer cannot exist.

  This non-example fails in **Vect**, because the analogues of $T_1$, $T_2$, $T_3$ and $T_4$ can each be written in terms of the other three: for example, $T_4 = \frac{1}{2}(T_2 + T_3 - T_1)$. We cannot do this in **Rel** because there is no way to 'subtract' relations.

We also introduce the important ideas of idempotents and splittings.

**Definition 0.23** (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 morphisms $A \xrightarrow{g} B$ and $B \xrightarrow{h} A$ such that $f = h \circ g$ and $g \circ h = \mathrm{id}_B$.

A splitting of an idempotent $A \xrightarrow{f} A$ is given exactly by an equalizer of $f$ and $\mathrm{id}_A$.

## 0.2 Hilbert spaces

This section introduces the mathematical formalism that underlies quantum computing: 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 0.24** (Complex vector space)**.** A *complex 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 $u, v, w \in V$ and $a, b \in \mathbb{C}$:

- additive associativity: $u + (v + w) = (u + v) + w$;
- additive commutativity: $u + v = v + u$;
- additive unit: $v + 0 = v$;
- additive inverses: there exists a $-v \in V$ such that $v + (-v) = 0$;
- additive distributivity: $a \cdot (u + v) = (a \cdot u) + (a \cdot v)$
- scalar unit: $1 \cdot v = v$;
- scalar distributivity: $(a + b) \cdot v = (a \cdot v) + (b \cdot v)$;
- scalar compatibility: $a \cdot (b \cdot v) = (ab) \cdot v$.

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

**Definition 0.25** (Linear map, antilinear map)**.** A *linear map* is a function $f\colon V \to W$ between vector spaces, with the following properties, for all $u, v \in V$ and $a \in \mathbb{C}$:

$$f(u + v) = f(u) + f(v) \tag{15}$$
$$f(a \cdot v) = a \cdot f(v) \tag{16}$$

An *anti-linear map* is a function that also satisfies (15), but instead of (16), has the additional property

$$f(a \cdot v) = a^* \cdot f(v), \tag{17}$$

where the star denotes complex conjugation.

We can use these definitions to build a category of vector spaces.

**Definition 0.26 (Vect, FVect).** The category **Vect** of vector spaces and linear maps is defined as follows:

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

We define the category **FVect** to be the restriction of **Vect** to finite-dimensional vector spaces.

Any morphism $f\colon V \to W$ in **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 0.27.** The *direct sum* of vector spaces $V$ and $W$ is the vector space $V \oplus W$, whose elements are pairs $(v, w)$ of elements $v \in V$ and $w \in W$, with entrywise addition and scalar multiplication.

Direct sums are both products and coproducts in the category **Vect**.

### 0.2.2 Bases and matrices

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

**Definition 0.28.** 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.

**Definition 0.29.** 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 $f(v_j)_i$. Composition of linear maps then corresponds to matrix multiplication (6). This directly leads to a category.

**Definition 0.30.** The skeletal category $\mathbf{Mat}_{\mathbb{C}}$ is defined as follows:

- **objects** are natural numbers $0, 1, 2, \ldots$;
- **morphisms** $n \to m$ are matrices of complex numbers 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. This can be made using the category theory we have developed in Section 0.1.

**Proposition 0.31.** *There is an equivalence of categories* $\mathbf{Mat}_{\mathbb{C}} \to \mathbf{FVect}$*, sending* $n \mapsto \mathbb{C}^n$*, and a matrix to its associated linear map.*

*Proof.* Because every finite-dimensional Hilbert 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 a square matrix, the trace is an important operation.

**Definition 0.32.** For a square matrix with entries $m_{ij}$, its *trace* is the number $\sum_i m_{ii}$ given by the sum of the entries on the main diagonal.

### 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 0.33.** An *inner product* on a vector space $V$ is a function $\langle - | - \rangle \colon V \times V \to \mathbb{C}$ that is:

- *conjugate-symmetric*: for all $v, w \in V$,

$$\langle v|w\rangle = \langle w|v\rangle^*, \tag{18}$$

- *linear* in the second argument: for all $u, v, w \in V$ and $a \in \mathbb{C}$,

$$\langle v|a \cdot w\rangle = a \cdot \langle v|w\rangle, \tag{19}$$

$$\langle u|v + w\rangle = \langle u|v\rangle + \langle u|w\rangle; \tag{20}$$

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

$$\langle v|v\rangle \geq 0, \tag{21}$$

$$\langle v|v\rangle = 0 \Rightarrow v = 0. \tag{22}$$

**Definition 0.34.** 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 structure given by

$$\langle a|b\rangle := a^* b, \tag{23}$$

where $a^* \in \mathbb{C}$ denotes the complex conjugate of $a \in \mathbb{C}$.

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

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

**Definition 0.35.** 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.

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 adding in 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 0.36** (Bounded linear map)**.** A linear map $f\colon H \to K$ between Hilbert spaces is *bounded* when there exists a number $b \in \mathbb{R}$ such that $\|f(v)\| \leq b \cdot \|v\|$ for all $v \in H$.

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

Hilbert spaces and bounded linear maps form a category. For the purposes of modelling phenomena in quantum computation, this category will be the main example that we use throughout the book.

**Definition 0.37 (Hilb, FHilb).** The category **Hilb** of Hilbert spaces and bounded linear maps is defined as follows:

- **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.

We define the category **FHilb** to be 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 inner products can be modelled categorically, using the idea of *daggers*.

Hilbert space have a more discerning notion of basis.

**Definition 0.38** (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 the infinite sum $\sum_i a_i e_i$ converges to $a$.

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

Any orthogonal family of elements is automatically linearly independent. For finite-dimensional Hilbert spaces, the ordinary notion of basis as a vector space is still useful, as given by Definition 0.28. 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 0.39.** 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 $\langle (v_1, w_1)|(v_2, w_2)\rangle = \langle v_1|v_2\rangle + \langle w_1|w_2\rangle$.

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**, 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* $\{v \in V \mid \forall u \in U \colon \langle u|v\rangle = 0\}$.

For some bounded linear maps, we can define a notion of trace.

**Definition 0.40** (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 bases, then it converges for all orthonormal bases, and the trace is independent of the chosen basis. Also, in the finite-dimensional case, the trace defined in this way agrees with the matrix trace of Definition 0.32.

### 0.2.4 Adjoints

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

**Definition 0.41.** 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 $u \in H$ and $v \in K$:

$$\langle f(u)|v\rangle = \langle u|f^\dagger(v)\rangle. \tag{24}$$

The existence of the adjoint follows from the Riesz representation theorem for Hilbert spaces, which we do not cover here. It follows immediately from (24) by uniqueness of adjoints that they also satisfy the following properties:

$$(f^\dagger)^\dagger = f, \tag{25}$$

$$(g \circ f)^\dagger = f^\dagger \circ g^\dagger, \tag{26}$$

$$\mathrm{id}_H{}^\dagger = \mathrm{id}_H. \tag{27}$$

Taking adjoints is an *anti-linear* operation.

We can use adjoints to define various specialized classes of linear maps.

**Definition 0.42.** 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 $f^\dagger \circ f = \mathrm{id}_A$ 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;
- 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 0.43** (Bra, ket)**.** Given an element $v \in H$ of a Hilbert space, its *ket* $\mathbb{C} \xrightarrow{|v\rangle} H$ is the linear map $a \mapsto av$. Its *bra* $H \xrightarrow{\langle v|} \mathbb{C}$ is the linear map $w \mapsto \langle v|w\rangle$.

You can check that $|v\rangle^\dagger = \langle v|$. The reason for this notation is demonstrated by the following calculation:

$$\left(\mathbb{C} \xrightarrow{|v\rangle} H \xrightarrow{\langle w|} \mathbb{C}\right) = \left(\mathbb{C} \xrightarrow{\langle w|\circ|v\rangle} \mathbb{C}\right) = \left(\mathbb{C} \xrightarrow{\langle w|v\rangle} \mathbb{C}\right) \tag{28}$$

In the final expression here, we identify the number $\langle w|v\rangle$ with the linear map that sends $1 \mapsto \langle w|v\rangle$. We see that the inner product (or 'bra-ket') $\langle w|v\rangle$ breaks into a composite of a bra $\langle w|$ and a ket $|v\rangle$. Originally due to Paul Dirac, this is traditionally called *Dirac notation*.

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

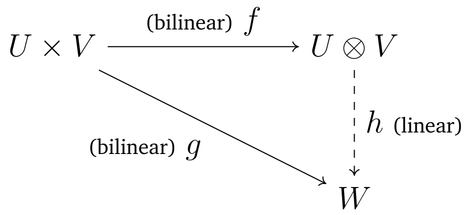
**Definition 0.44.** For a Hilbert space $H$, its *dual Hilbert space* $H^*$ is the vector space $\mathbf{Hilb}(H, \mathbb{C})$.

A Hilbert space is isomorphic to its dual in an anti-linear way: the map $H \to H^*$ given by $|v\rangle \mapsto \varphi_v = \langle v|$ is an invertible bounded anti-linear function. The inner product on $H^*$ is given by $\langle \varphi_v|\varphi_w\rangle_{H^*} = \langle v|w\rangle_H$.

### 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: 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 0.45.** 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 $g = h \circ f$.




The function $f$ usually stays anonymous and is written as $(u, v) \mapsto u \otimes v$. Thus arbitrary elements of $U \otimes V$ take the form $\sum_{i=1}^{n} a_i u_i \otimes v_i$ for $a_i \in \mathbb{C}$, $u_i \in U$, and $v_i \in V$. 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 $(f_1 \otimes f_2)(u_1 \otimes u_2) = f_1(u_1) \otimes f_2(u_2)$ for $u_1 \in U_1$ and $u_2 \in U_2$. In this way, the tensor product becomes a functor $\otimes\colon \mathbf{Vect} \times \mathbf{Vect} \to \mathbf{Vect}$.

**Definition 0.46.** The *tensor product of Hilbert spaces* $H$ and $K$ is the following Hilbert space $H \otimes K$: take the tensor product of vector spaces; give it the inner product $\langle u_1 \otimes v_1 | u_2 \otimes v_2 \rangle = \langle u_1 | v_1 \rangle \cdot \langle u_2 | v_2 \rangle$; complete it. 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 0.47** (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*:

$$(f \otimes g) := \begin{pmatrix} \big(f_{11} g\big) & \big(f_{12} g\big) & \cdots & \big(f_{1n} g\big) \\ \big(f_{21} g\big) & \big(f_{22} g\big) & \dots & \big(f_{2n} g\big) \\ \vdots & \vdots & \ddots & \vdots \\ \big(f_{m1} g\big) & \big(f_{m2} g\big) & \dots & \big(f_{mn} g\big) \end{pmatrix}. \tag{29}$$

## 0.3 Quantum information

In general, the state of a quantum system is represented by a vector in a Hilbert space. More specifically, quantum information theory deals with generalizations of the fundamental bits of computer science, namely *qubits*.

### 0.3.1 State spaces

Classical computer science often consider 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 0.48.** 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 with square norm equal to 1:

$$\langle v|v\rangle = 1 \tag{30}$$

A pure state of a qubit is therefore a vector of the form

$$v = \begin{pmatrix} a \\ b \end{pmatrix},$$

with $a, b \in \mathbb{C}$, which is normalized when $|a|^2 + |b|^2 = 1$. In Section 0.3.4 we will encounter a more general notion of state.

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

**Definition 0.49.** For the Hilbert space $\mathbb{C}^n$, the *computational basis* is the orthonormal basis given by the following vectors:

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \qquad |1\rangle := \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \qquad \cdots \qquad |n-1\rangle := \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \tag{31}$$

For a qubit, we can use this to write an arbitrary state in the form $v = a|0\rangle + b|1\rangle$. The following alternative qubit basis also plays an important role.

**Definition 0.50.** 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 $v \in H$ to a normalised state $f(v) \in H$. 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 an axiom 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, product states and entangled states are defined as follows.

**Definition 0.51** (Product state, entangled state)**.** For a compound system with state space $H \otimes K$, a *product state* is a state of the form $v \otimes w$ with $v \in H$ and $w \in K$. 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 $|v\rangle \in H$ and $|w\rangle \in K$ are chosen states, we will often write $|vw\rangle \equiv |v\rangle \otimes |w\rangle$ for their product state.

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

**Definition 0.52.** 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 0.63 later in this chapter.)

### 0.3.3 Pure states

For a quantum system in a pure state, the most basic notion of measurement is a *projection-valued measure*. The *standard interpretation* of quantum mechanics, sometimes called the *Copenhagen interpretation*, gives a set of rules that tell us what happens to the quantum state when a projection-valued measurement takes place, and the probabilities of the different outcomes.

**Definition 0.53** (Projection-valued measure, nondegenerate)**.** A *projection-valued measure (PVM)* on a Hilbert space $H$ is a family of projections $H \xrightarrow{p_i} H$ with the following properties:

$$\textstyle\sum_i p_i = \text{id}_H \tag{32}$$

$$p_i \circ p_j = \begin{cases} p_i & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases} \tag{33}$$

The PVM is nondegenerate if the following additional condition is satisfied for all $i$:

$$\mathrm{Tr}(p_i) = 1 \tag{34}$$

Recall from Definition 0.42 that projections are maps satisfying $p = p^\dagger = p \circ p$.

**Lemma 0.54.** *For a finite-dimensional Hilbert space, nondegenerate projection-valued measures correspond to orthonormal bases, up to phase.*

*Proof.* For an orthonormal basis $|i\rangle$, we can define a nondegenerate PVM by $p_i := |i\rangle\langle i|$. Conversely, for every projector $p$ with $\mathrm{Tr}(p) = 1$ there is a ket $|i\rangle$ such that $p = |i\rangle\langle i|$, unique up to multiplication by a unit complex number $e^{i\theta}|i\rangle$. □

When a projection-valued measurement is applied to a Hilbert space, it will have a unique outcome, given by one of the projections. This outcome will be probabilistic, with distribution described by the Born rule.

**Definition 0.55** (Born rule)**.** For a projection-valued measure $\{p_i\}$ on a system in a normalized state $v \in H$, the *probability of outcome* $i$ is $\langle v|p_i|v\rangle$.

From the definition of a projection-valued measurement, the total probability across all outcomes is 1:

$$\textstyle\sum_i \langle v|p_i|v\rangle \overset{(15)}{=} \langle v|(\sum_i p_i)|v\rangle \overset{(32)}{=} \langle v|v\rangle \overset{(30)}{=} 1 \tag{35}$$

After a measurement, the new state of the system is $p_i(v)$, 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 not necessarily normalized. If the new state is not zero, it can be normalized in a canonical way, giving $p_i(v)/\|p_i(v)\|$.

## 0.3.4 Mixed states

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 $v \in H$, and another that will produce it in state $w \in H$. 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 0.56** (Density matrix, normalized)**.** A *density matrix* on a Hilbert space $H$ is a positive map $H \xrightarrow{\rho} H$. A density matrix is *normalized* when $\mathrm{Tr}(\rho) = 1$.

Recall from Definition 0.42 that $\rho$ is positive when there exists some $g$ with $\rho = g^\dagger \circ g$. Density matrices are more general than pure states, since every pure state $v \in H$ gives rise to a density matrix $\rho = |v\rangle\langle v|$ in a canonical way.

**Definition 0.57** (Pure state, mixed state)**.** A density matrix $\rho\colon H \to H$ is *pure* when $\rho = |\psi\rangle\langle\psi|$ for some $\psi \in H$; generally it is *mixed*.

**Definition 0.58.** For a 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 sum of density matrices, which corresponds physically to the idea of probabilistic choice between alternative states.

**Definition 0.59** (Convex sum)**.** For nonnegative real numbers $p, q$ with $p+q = 1$, the *convex sum* of density matrices $H \xrightarrow{\rho,\sigma} H$ is the density matrix $H \xrightarrow{p\cdot\rho+q\cdot\sigma} H$.

In the standard approach to quantum theory, the density matrix $p \cdot \rho + q \cdot \sigma$ describes the state of a system produced by a machine that promises to output state $\rho$ with probability $p$, and state $\sigma$ with probability $q$. Every mixed state can be produced by a convex combination of some number of pure states, which are not unique, and the convex sum of distinct density matrices is always a mixed state.

There is standard notion of measurement for density matrices, which generalizes the projection-valued measure appropriate for pure states.

**Definition 0.60.** A *positive operator-valued measure (POVM)* on a Hilbert space $H$ is a family of positive maps $H \xrightarrow{f_i} H$ satisfying

$$\textstyle\sum_i f_i = \mathrm{id}_H. \tag{36}$$

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 0.61** (Born rule for POVMs)**.** For a positive operator-valued measure $\{f_i\}$ on a system with normalized density matrix $H \xrightarrow{\rho} H$, the *probability of outcome* $i$ is $\langle\psi|f_i|\psi\rangle$.

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

**Definition 0.62.** For Hilbert spaces $H$ and $K$, the *partial trace over* $K$ is the unique linear map $\mathrm{Tr}_K\colon \mathbf{Hilb}(H \otimes K, H \otimes K) \to \mathbf{Hilb}(H, H)$ satisfying $\mathrm{Tr}_K(\rho \otimes \sigma) = \mathrm{Tr}(\sigma) \cdot \rho$.

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

$$\mathrm{Tr}_K(f) = \textstyle\sum_i (\mathrm{id}_H \otimes \langle i|) \circ f \circ (\mathrm{id}_H \otimes |i\rangle). \tag{37}$$

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

We can use partial traces to give a definition of maximally entangled state.

**Definition 0.63.** A pure state $v \in H \otimes K$ is *maximally entangled* when tracing out either $H$ or $K$ from $|v\rangle\langle v|$ gives a maximally mixed state; explicitly this means the following, for $c, c' \in \mathbb{C}$:

$$\mathrm{Tr}_H(|v\rangle\langle v|) = c \cdot \mathrm{id}_K \qquad \mathrm{Tr}_K(|v\rangle\langle v|) = c' \cdot \mathrm{id}_H \tag{38}$$

When $|v\rangle$ is normalized, its trace will be a normalized density matrix, and we will then have $c = \dim^{-1}(H)$ and $c' = \dim^{-1}(K)$.

Up to unitary there is only one maximally entangled state for each system, as the following lemma shows; we will prove it in **??**.

**Lemma 0.64.** *Any two maximally entangled states $v, w \in H \otimes K$ are related by $(f \otimes \mathrm{id}_K)(v) = w$ for a unique unitary $H \xrightarrow{f} H$.* □

### 0.3.5 Quantum teleportation

Quantum teleportation is a beautiful and simple procedure, which demonstrates some of the counterintuitive properties of quantum information. There are 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.

**Definition 0.65** (Teleportation of a qubit)**.** The procedure is as follows.

1. Alice and Bob share a pair of maximally entangled qubits, in the Bell state. We write $Q_A$ for Alice's qubit and $Q_B$ for Bob's qubit.

2. Alice prepares her initial qubit $Q_I$ which she would like to teleport to Bob.

3. Alice measures the system $Q_I \otimes Q_A$ in the Bell basis (see Definition 0.52.)

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 $Q_B$, depending on which Bell state $|\mathrm{Bell}_i\rangle$ was measured by Alice:

$$f_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad f_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad f_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad f_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{39}$$

At the end of the procedure, Bob's qubit $Q_B$ is guaranteed to be in the same state in which $Q_I$ was at the beginning. This may seem surprising, since only two bits worth of classical information has been passed from Alice to Bob. Later in this book, we will see several categorical models of quantum teleportation, and see abstractly why the procedure 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. As a good first textbook, we recommend [**?**, **?**, **?**]; excellent advanced textbooks are [**?**, **?**].

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, we refer to [**?**].

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, we recommend [**?**]. The quantum teleportation protocol was discovered in 1993 by Bennett, Brassard, Crépeau, Jozsa, Peres, and Wootters [**?**], and has been performed experimentally many times since, over distances as large as 16 kilometers.

# 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 **Hilb**, **Set** and **Rel** can be given a monoidal structure. We also introduce a visual notation called the graphical calculus, which provides an intuitive and powerful way to work with them.

## 1.1 Monoidal structure

### 1.1.1 Introduction

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 that isomorphism 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 $D$:

$$
\begin{array}{ccc}
(A \otimes I) \otimes B & \xrightarrow{\quad \alpha_{A,I,B} \quad} & A \otimes (I \otimes B) \\
& {\scriptstyle \rho_A \otimes \mathrm{id}_B} \searrow \qquad \swarrow {\scriptstyle \mathrm{id}_A \otimes \lambda_B} & \\
& A \otimes B &
\end{array}
\tag{1.1}
$$

$$
\begin{array}{ccc}
\big(A \otimes (B \otimes C)\big) \otimes D & \xrightarrow{\alpha_{A,B\otimes C,D}} & A \otimes \big((B \otimes C) \otimes D\big) \\
{\scriptstyle \alpha_{A,B,C} \otimes \mathrm{id}_D} \nearrow & & \searrow {\scriptstyle \mathrm{id}_A \otimes \alpha_{B,C,D}} \\
\big((A \otimes B) \otimes C\big) \otimes D & & A \otimes \big(B \otimes (C \otimes D)\big) \\
{\scriptstyle \alpha_{A\otimes B,C,D}} \searrow & & \nearrow {\scriptstyle \alpha_{A,B,C\otimes D}} \\
& (A \otimes B) \otimes (C \otimes D) &
\end{array}
\tag{1.2}
$$

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

The idea behind the definition of a monoidal category is that any way of 'reorganizing' a collection of systems using $\alpha$, $\lambda$, $\rho$ and their inverses, under composition and tensor product, is equal to any other. 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 (as long as we apply them correctly, of course.)

Two examples of such 'reorganizing' operations are given by the triangle equation (1.1) and pentagon equation (1.2). In each case, the clockwise and anticlockwise paths give equal ways to transform one system into another. The reason these equations are given special status in the definition is that, perhaps surprisingly, they are sufficient to ensure every such well-typed commutes. 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 $\alpha$, $\lambda$, $\rho$ 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 1.4.2.)

Our first example of a monoidal structure is on the category **Hilb**, whose structure as a category was given in Definition 0.37.

**Definition 1.3.** The monoidal structure on the category **Hilb**, and also by restriction on **FHilb**, is defined in the following way:

- **the tensor product** $\otimes\colon \mathbf{Hilb}\times\mathbf{Hilb}\to\mathbf{Hilb}$ 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 $(u\otimes v)\otimes w \mapsto u\otimes(v\otimes w)$ for all $u\in H$, $v\in J$ and $w\in K$;
- **left unitors** $\mathbb{C}\otimes H \xrightarrow{\lambda_H} H$ are the unique linear maps satisfying $1\otimes u\mapsto u$ for all $u\in H$;
- **right unitors** $H\otimes\mathbb{C} \xrightarrow{\rho_H} H$ are the unique linear maps satisfying $u\otimes 1\mapsto u$ for all $u\in H$.

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 correctly describes the state space of a composite system in quantum theory.

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

**Definition 1.4.** The monoidal structure on the category **Set**, and also by restriction on **FSet**, is defined as follows for all $a\in A$, $b\in B$ and $c\in C$:

- **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 given by $\big((a,b),c\big)\mapsto \big(a,(b,c)\big)$;
- **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 (and will be discussed in Section 4.4). This is an example of a general phenomenon (see Exercise 1.4.11): if a category has products, then these can be used to give a monoidal structure on the category. The same is true for coproducts, which in **Set** are given by disjoint union. The category **Set** can also be given nonstandard tensor products whose action on objects takes the form $A\otimes B := A+B+(A\times B)$; see Exercise 1.4.12.

This highlights an important difference between the standard tensor products on **Hilb** and **Set**: while the tensor product on **Set** comes from a categorical product, the tensor product on **Hilb** does not. (See also Chapter 4 and Exercise 2.5.2.) We will discover many more differences between **Hilb** and **Set**, which provide insight into the differences between quantum and classical information.

There is a canonical monoidal structure on the category **Rel**, which was introduced as a category in Definition 0.5.

**Definition 1.5.** The monoidal structure on the category $\mathbf{Rel}$ is defined in the following way, for all $a \in A$, $b \in B$, $c \in C$ and $d \in D$:

- **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 $\big((a,b),c\big) \sim \big(a,(b,c)\big)$;
- **left unitors** $I \times A \xrightarrow{\lambda_A} A$ are the relations defined by $(\bullet, a) \sim a$;
- **right unitors** $A \times I \xrightarrow{\rho_A} A$ are the relations defined by $(a, \bullet) \sim a$.

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 the structure on $\mathbf{Hilb}$.

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

**Theorem 1.6** (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:*

$$(g \circ f) \otimes (j \circ h) = (g \otimes j) \circ (f \otimes h) \tag{1.3}$$

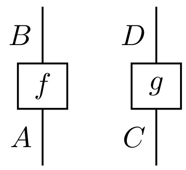
*Proof.* This holds because of properties of the category $\mathbf{C} \times \mathbf{C}$, and from the fact that $\otimes \colon \mathbf{C} \times \mathbf{C} \to \mathbf{C}$ is a functor:

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

Recall that the functoriality property for a functor $F$ says that $F(g \circ f) = F(g) \circ F(f)$. □

## 1.1.2 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:




(1.4)

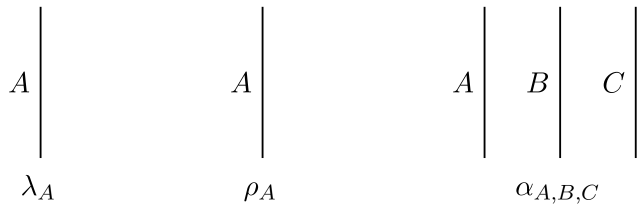
The idea is that $f$ and $g$ represent processes taking place at the same time on distinct systems. Inputs are drawn at the bottom, and outputs are drawn at the top; in this sense, “time” runs upwards. This extends the basic one-dimensional notation for categories outlined in Section 0.1.5. Whereas the graphical calculus for ordinary categories was one-dimensional, or *linear*, the graphical calculus for monoidal categories is two-dimension,al 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 examine in Section 1.3, 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:

(1.5)

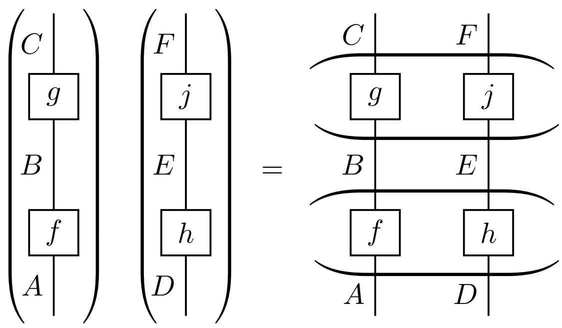
The left unitor $I \otimes A \xrightarrow{\lambda_A} A$, the right unitor $A \otimes I \xrightarrow{\rho_A} A$ and the associator $(A \otimes B) \otimes C \xrightarrow{\alpha_{A,B,C}} A \otimes (B \otimes C)$ are also simply not depicted:




(1.6)

The coherence of $\alpha$, $\lambda$ and $\rho$ 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 (see Section 1.3), it doesn't matter that their graphical calculus encodes no information.

Now consider the graphical representation of the interchange law (1.3):




(1.7)

We use brackets to indicate how we are forming the diagrams on each side. Dropping the brackets, we see the interchange law is in fact very natural; what seemed to be a mysterious algebraic identity becomes very clear from the graphical perspective.

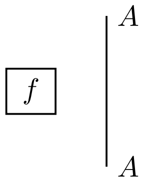
The point of the graphical calculus is that all of the superficially complex aspects of the algebraic definition of monoidal categories—the unit law, the associativity law, associators, left unitors, right unitors, the triangle equation, the pentagon equation, the interchange law—melt away, allowing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

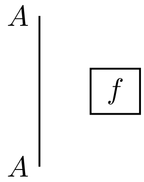
Before we can state a theorem that establishes correctness of the graphical calculus, we must introduce the idea of isotopy.

**Definition 1.7.** Two diagrams are *isotopic* when one can be deformed continuously into the other, keeping the boundaries fixed.

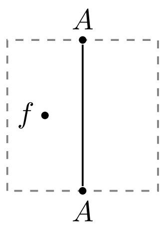
For the purposes of this definition, diagrams are assumed to lie in a rectangular region of the plane, with input wires terminating at the lower boundary and output wires terminating at the upper boundary. We also call this *planar isotopy*. Morphism boxes are treated as points with zero size.

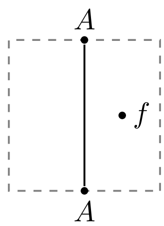
**Example 1.8.** A morphism $I \xrightarrow{f} I$ in a monoidal category gives rise to two morphisms $A \to A$, namely $A \xrightarrow{\lambda_A^{-1}} I \otimes A \xrightarrow{f \otimes \mathrm{id}_A} I \otimes A \xrightarrow{\lambda_A} A$ and $A \xrightarrow{\rho_A^{-1}} A \otimes I \xrightarrow{\mathrm{id}_A \otimes f} A \otimes I \xrightarrow{\rho_A} A$. Their diagrams look as follows:



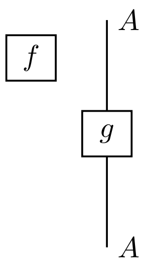

To regard them as diagrams viable to isotopy, we must fix the ends of wires in bounding boxes.

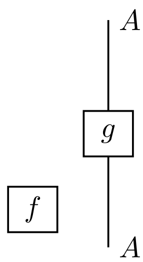



We can now see that these two diagrams are not isotopic. Thinking of this as a wire and a dot trapped between two pieces of glass, there is no way we can continuously deform one diagram into the other. Thus the two morphisms $A \to A$ are in general not the same.

On the other hand, the following two diagrams are clearly isotopic:




The following theorem says that therefore, for any morphisms $I \xrightarrow{f} I$ and $A \xrightarrow{g} A$ in any monoidal category, the morphisms $A \xrightarrow{\lambda_A^{-1}} I \otimes A \xrightarrow{f \otimes \mathrm{id}_A} I \otimes A \xrightarrow{\lambda_A} A \xrightarrow{g} A$ and $A \xrightarrow{g} A \xrightarrow{\lambda_A^{-1}} I \otimes A \xrightarrow{f \otimes \mathrm{id}_A} I \otimes A \xrightarrow{\lambda_A} A$ are equal.

**Theorem 1.9** (Correctness of the graphical calculus for monoidal categories)**.** *A well-formed 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.*

This 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-formed, 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 for all such $f$ and $g$, $P(f, g) \Rightarrow Q(f, g)$. *Completeness* is the reverse assertion, that $Q(f, g) \Rightarrow P(f, g)$ for all such $f$ and $g$.

Proving soundness is straightforward: there are only a finite number of axioms, and one just has to check that they are all valid in terms of planar isotopy of diagrams. Correctness is much harder, and beyond this scope of this book: 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 value of the morphism in the monoidal category unchanged.

Let's take a closer look at the condition that the equation $f = g$ must be well-formed. Firstly, $f$ and $g$ must have the same source and the same target. 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 source objects, and so the equation is not well-formed, 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, but the equation $f = g$ would not be well-formed since it would be making use of this 'accidental' equality. For a careful examination of the well-formed property, see Section 1.3.4.

### 1.1.3 States and effects

If a mathematical structure lives as an object of 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 gives us a generalized categorical notion of state.

**Definition 1.10.** 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.

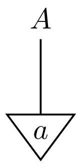
**Example 1.11.** We now examine what the states are in our three example categories:

- in $\mathbf{Hilb}$, points 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 $\mathbf{Set}$, points of a set $A$ are functions $\{\bullet\} \to A$, which correspond to elements of $A$ by considering the image of $\bullet$;
- in $\mathbf{Rel}$, points 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 points $I \xrightarrow{a} A$. A monoidal category is *monoidally well-pointed* if for all parallel pairs of morphisms $A \otimes B \xrightarrow{f,g} C \otimes D$, we have $f = g$ when $f \circ (a \otimes b) = g \circ (a \otimes b)$ for all states $I \xrightarrow{a} A$ and $I \xrightarrow{b} B$.

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 domain objects. 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 **Set**, **Rel**, **Vect**, and **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 $H \otimes K$.

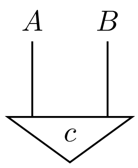
To emphasize that states $I \xrightarrow{a} A$ have the empty picture (1.5) as their domain, we will draw them as triangles instead of boxes.




(1.8)

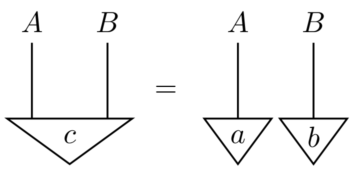
## 1.1.4 Product states and entangled states

For objects $A$ and $B$ of a monoidal category, a morphism $I \xrightarrow{c} A \otimes B$ is a *joint state* of $A$ and $B$. We depict it graphically in the following way.




(1.9)

**Definition 1.13.** 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 $I \xrightarrow{b} B$:




(1.10)

**Definition 1.14.** 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 1.15.** Joint states, product states, and entangled states look as follows in our example categories:

- in **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 **Rel**:
  - **joint states** of $A$ and $B$ are subsets of $A \times B$;
  - **product states** are subsets $U \subseteq A \times B$ such that, for some $V \subseteq A$ and $W \subseteq B$, $(v, w) \in U$ if and only if $v \in V$ and $w \in W$;
  - **entangled states** are subsets of $A \times B$ that are not of this form.

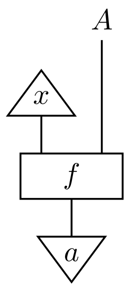
This hints at why entanglement can be difficult to understand intuitively: classically, in the processes encoded by the category **Set**, it cannot occur. However, if we allow nondeterministic behaviour as encoded by **Rel**, then an analogue of entanglement does appear.

### 1.1.5 Effects

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

**Definition 1.16.** 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, an interesting diagram would be this one:




(1.11)

This 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 that the outcome $x$ does occur. An effect can be thought of as a *postselection*: we run our entire experiment repeatedly, only accepting the result when we find that our measurement had the specified outcome.

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

**Example 1.17.** 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 $\mathbf{Hilb}$, we require $a$, $f$ and $x$ to be partial isometries. The rules of quantum mechanics then 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 is impossible exactly when the overall state is zero.
- In nondeterministic classical physics, as described by $\mathbf{Rel}$, we need put no particular requirements on $a$, $f$ and $x$ — they 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, that means this particular sequence of a state preparation, a dynamics step, and 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'.

# 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

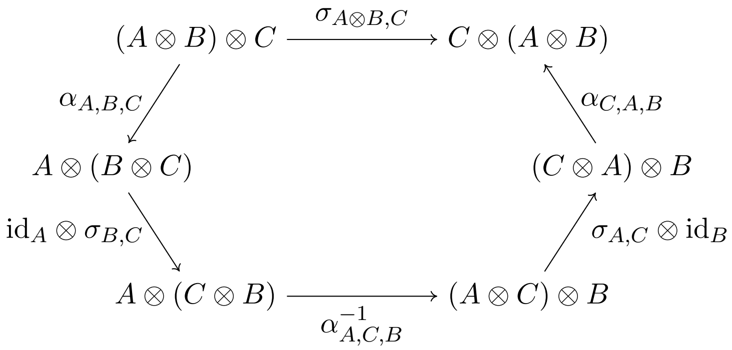
We first consider braided monoidal categories.

**Definition 1.18.** A *braided monoidal category* is a monoidal category equipped with a natural isomorphism

$$A \otimes B \xrightarrow{\sigma_{A,B}} B \otimes A \tag{1.12}$$

satisfying the following *hexagon equations*:

$$\begin{array}{ccccc} & A \otimes (B \otimes C) & \xrightarrow{\sigma_{A,B\otimes C}} & (B \otimes C) \otimes A & \\ \alpha^{-1}_{A,B,C} \swarrow & & & & \nwarrow \alpha^{-1}_{B,C,A} \\ (A \otimes B) \otimes C & & & & B \otimes (C \otimes A) \\ \sigma_{A,B} \otimes \mathrm{id}_C \searrow & & & & \nearrow \mathrm{id}_B \otimes \sigma_{A,C} \\ & (B \otimes A) \otimes C & \xrightarrow[\alpha_{B,A,C}]{} & B \otimes (A \otimes C) & \end{array} \tag{1.13}$$




(1.14)

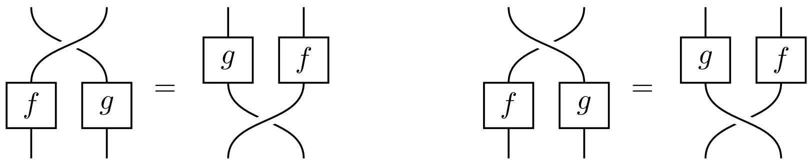
We include the braiding in our graphical notation like this:


(1.15)

Invertibility then takes the following graphical form:

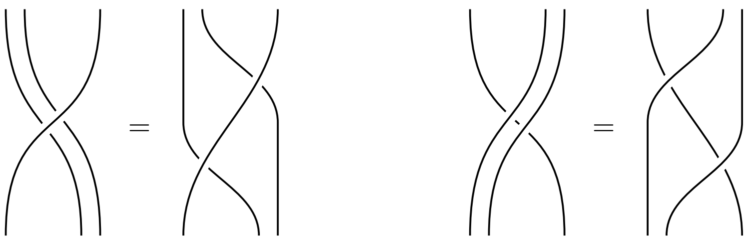
(1.16)

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




(1.17)

The hexagon equations have the following graphical representations:



(1.18)

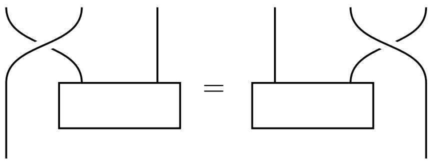
Each of these equations has two strands close to each other on the left-hand side, to indicate that we are treating them as a single composite object for the purposes of the braiding. We see that the hexagon equations are saying something quite straightforward: to braid with a tensor product of two strands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

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.

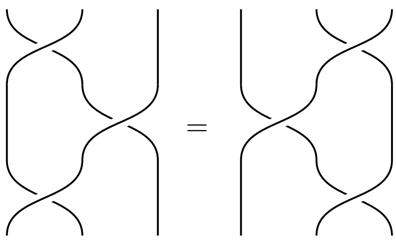
Braided monoidal categories have a sound and complete graphical calculus, as established by the following theorem. The notion of isotopy it uses is now three-dimensional, that is, the diagrams are assumed to lie in a cube, with input wires terminating at the lower face and output wires terminating at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

**Theorem 1.19** (Correctness of graphical calculus for braided monoidal categories). *A well-formed 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:



(1.19)



(1.20)

This is Exercise 1.4.6 at the end of this chapter. Equation (1.20) is called the *Yang–Baxter equation*, which plays an important role in the mathematical theory of knots.

We now give some examples of braided monoidal categories. 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 1.20.** Our example 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 $b \in B$.

In fact these are all symmetric monoidal structures, which we explore in Section 1.2.2.

### 1.2.2 Symmetric monoidal categories

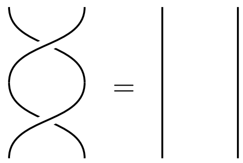
In our example categories **Hilb**, **Rel** and **Set**, the braidings satisfy an extra property that makes them very easy to work with.

**Definition 1.21.** A braided monoidal category is *symmetric* when

$$\sigma_{B,A} \circ \sigma_{A,B} = \mathrm{id}_{A\otimes B} \tag{1.21}$$

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

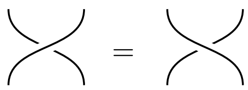
Graphically, condition (1.21) has the following representation.



(1.22)

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

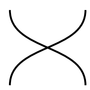
**Lemma 1.22.** *In a symmetric monoidal category* $\sigma_{A,B} = \sigma^{-1}_{B,A}$*, with the following graphical representation:*



(1.23)

*Proof.* Combine (1.16) and (1.22). □

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



(1.24)

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. See Section 1.3 for more details about what it means for diagrams in the graphical language to be the same.

Suppose we imagine our diagrams as curves embedded in four-dimensional space. Then we can smoothly deform one crossing into the other, in the manner of equation (1.23), by making use of the extra dimension. In this sense, symmetric monoidal categories have a four-dimensional graphical notation. The following correctness theorem therefore uses the four-dimensional version of isotopy.

**Theorem 1.23** (Correctness of the graphical calculus for symmetric monoidal categories)**.** *A well-formed equation between morphisms in a symmetric monoidal category follows from the axioms if and only if it holds in the graphical language up to four-dimensional isotopy.*

The following gives a nice example of a symmetric monoidal categories, with a physics flavour.

**Example 1.24.** For a finite group $\mathbf{G}$, there is a symmetric monoidal category $\mathbf{Rep}(\mathbf{G})$ of finite-dimensional representations of $\mathbf{G}$, defined as follows:

- **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 the symmetry on $\mathbf{Vect}$.

## 1.3 Coherence

This section proves the Coherence Theorem 1.2, and the resulting soundness of the graphical calculus. To do so, we first discuss a particularly simple kind of monoidal categories, called strict. 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 1.31, which says that any monoidal category is monoidally equivalent to a strict one. From there we prove the Coherence Theorem, and the soundness of the graphical calculus. It is not really 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.

### 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 all isomorphisms $\alpha_{A,B,C}$, $\lambda_A$ and $\rho_A$ are identities.

The category $\mathbf{Mat}_{\mathbb{C}}$ of Definition 0.30 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 (29);
- **the monoidal unit** is the natural number 1;
- **associators, left unitors and right unitors** are the identity matrices.

The Strictification Theorem 1.31 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. However, *not* every monoidal category is *monoidally* equivalent to a strict, skeletal category. If you have to choose, it often turns out that skeletality is the more useful property to have. Nonetheless, notice that the monoidal category $\mathbf{Mat}_{\mathbb{C}}$ of Definition 1.26 is both strict and skeletal at the same time.

### 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* $F\colon \mathbf{C} \to \mathbf{D}$ between monoidal categories is a functor equipped with natural isomorphisms

$$(F_2)_{A,B}\colon F(A)\otimes F(B) \to F(A\otimes B) \tag{1.25}$$

$$F_0\colon I \to F(I) \tag{1.26}$$

making the following diagrams commute:

$$\begin{array}{ccc}
\big(F(A)\otimes F(B)\big)\otimes F(C) & \xrightarrow{\alpha_{F(A),F(B),F(C)}} & F(A)\otimes\big(F(B)\otimes F(C)\big) \\
{\scriptstyle (F_2)_{A,B}\otimes \mathrm{id}_{F(C)}}\downarrow & & \downarrow{\scriptstyle \mathrm{id}_{F(A)}\otimes (F_2)_{B,C}} \\
F(A\otimes B)\otimes F(C) & & F(A)\otimes F(B\otimes C) \\
{\scriptstyle (F_2)_{A\otimes B,C}}\downarrow & & \downarrow{\scriptstyle (F_2)_{A,B\otimes C}} \\
F\big((A\otimes B)\otimes C\big) & \xrightarrow[F(\alpha_{A,B,C})]{} & F\big(A\otimes (B\otimes C)\big)
\end{array} \tag{1.27}$$

$$\begin{array}{ccc}
F(A)\otimes I & \xrightarrow{\rho_{F(A)}} & F(A) \\
{\scriptstyle \mathrm{id}_{F(A)}\otimes F_0}\downarrow & & \downarrow{\scriptstyle F(\rho_A^{-1})} \\
F(A)\otimes F(I) & \xrightarrow[(F_2)_{A,I}]{} & F(A\otimes I)
\end{array}
\qquad
\begin{array}{ccc}
I\otimes F(A) & \xrightarrow{\lambda_{F(A)}} & F(A) \\
\downarrow{\scriptstyle F_0\otimes \mathrm{id}_{F(A)}} & & \downarrow{\scriptstyle F(\lambda_A^{-1})} \\
F(I)\otimes F(A) & \xrightarrow[(F_2)_{I,A}]{} & F(I\otimes A)
\end{array} \tag{1.28}$$

**Definition 1.28.** A *monoidal equivalence* is a monoidal functor that is an equivalence as a functor.

Similarly, natural transformation between monoidal functors have some coherence properties of their own.

**Definition 1.29** (Monoidal natural transformation)**.** Let $F, G\colon \mathbf{C} \to \mathbf{D}$ be monoidal functors between monoidal categories. A *monoidal natural transformation* is a natural transformation $\mu\colon F \Rightarrow G$ making the following diagrams commute:

$$
\begin{array}{ccc}
F(A)\otimes F(B) & \xrightarrow{(F_2)_{A,B}} & F(A\otimes B) \\
{\scriptstyle \mu_A\otimes\mu_B}\downarrow & & \downarrow{\scriptstyle \mu_{A\otimes B}} \\
G(A)\otimes G(B) & \xrightarrow[(G_2)_{A,B}]{} & G(A\otimes B)
\end{array}
\qquad
\begin{array}{ccc}
 & \nearrow^{F_0} & F(I) \\
I & & \downarrow{\scriptstyle \mu_I} \\
 & \searrow_{G_0} & G(I)
\end{array}
\tag{1.29}
$$

**Example 1.30.** The equivalence $R\colon \mathbf{Mat}_{\mathbb{C}} \to \mathbf{FHilb}$ of Proposition 0.31 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 (1.28). Equation (1.27) is also satisfied by this definition. Thus $R$ is a monoidal functor. □

### 1.3.3 Strictification

We now prove the Strictification Theorem by 'going one level up' from monoidal categories to monoidal functors, using the 'higher' coherence properties of their own that monoidal functors have to satisfy.

**Theorem 1.31** (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 $(F, \gamma)$ consisting of a functor $F\colon \mathbf{C} \to \mathbf{C}$ and a natural isomorphism

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

We can think of $\gamma$ 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 $\mathbf{C}$:

$$
\begin{array}{ccc}
F(A)\otimes B & \xrightarrow{\gamma_{A,B}} & F(A\otimes B) \\
{\scriptstyle \theta_A\otimes \mathrm{id}_B}\downarrow & & \downarrow{\scriptstyle \theta_{A\otimes B}} \\
F'(A)\otimes B & \xrightarrow[\gamma'_{A,B}]{} & F'(A\otimes B)
\end{array}
\tag{1.30}
$$

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 $\delta$ 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

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

It can be checked 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 functor $L\colon \mathbf{C} \to \mathbf{D}$ given by

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

We can think of this functor as "multiplying on the left". We will show that $L$ is a full, 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 $\rho$. 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:

$$\begin{array}{ccccccc}
A \otimes C & \xrightarrow{\rho_A^{-1} \otimes \mathrm{id}_C} & (A \otimes I) \otimes C & \xrightarrow{\alpha_{A,I,C}} & A \otimes (I \otimes C) & \xrightarrow{\mathrm{id}_A \otimes \lambda_C} & A \otimes C \\
{\scriptstyle f \otimes \mathrm{id}_C}\downarrow & & {\scriptstyle \theta_I \otimes \mathrm{id}_C}\downarrow & & \downarrow{\scriptstyle \theta_{I \otimes C}} & & \downarrow{\scriptstyle \theta_C} \\
B \otimes C & \xrightarrow[\rho_B^{-1} \otimes \mathrm{id}_C]{} & (B \otimes I) \otimes C & \xrightarrow[\alpha_{B,I,C}]{} & B \otimes (I \otimes C) & \xrightarrow[\mathrm{id}_A \otimes \lambda_C]{} & B \otimes C
\end{array}$$

The left square commutes by definition of $f$, the middle square by (1.30), and the right square by naturality of $\theta$. Moreover, the rows both equal the identity by the triangle identity (1.1). Hence $\theta_C = f \otimes \mathrm{id}_C$, and so $\theta = L(f)$.

We now show that $F$ is a monoidal functor. Define the isomorphism $F_0\colon I \to L(I)$ to be $\lambda^{-1}$, and define $(F_2)_{A,B}\colon L(A) \otimes L(B) \to L(A \otimes B)$ 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 (1.30) is just the pentagon identity (1.2) of $\mathbf{C}$. Verifying equations (1.28) comes down to the fact that $\lambda_I = \rho_I$ (see Exercise 1.4.2) and the triangle identity (1.1). Because $\mathbf{D}$ is strict, equation (1.27) comes down the pentagon identity (1.2) of $\mathbf{C}$.

Finally, let $\mathbf{C_s}$ be the subcategory of $\mathbf{D}$ encompassing 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. □

The Strictification Theorem means that, if you prefer, you can always strictify your monoidal category to obtain an equivalent one for which $\alpha$, $\lambda$ and $\rho$ are all identities.

### 1.3.4 The coherence theorem

We now derive the Coherence Theorem from the Strictification Theorem. To state the former, we have to be more precise about what Definition 1.1 coyly called 'well-formed' equations. 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 $((A \otimes B) \otimes C) \otimes D$ 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 1.32** (Coherence for monoidal categories)**.** *Let $v(A, \ldots, Z)$ and $w(A, \ldots, Z)$ be bracketings in a monoidal category $\mathbf{C}$. Any two transformations $\theta, \theta'\colon v \Rightarrow w$ built from $\alpha$, $\alpha^{-1}$, $\lambda$, $\lambda^{-1}$, $\rho$, $\rho^{-1}$, $\mathrm{id}$, $\otimes$, and $\circ$ are equal.*

*Proof.* Let $F\colon \mathbf{C} \to \mathbf{C_s}$ be the monoidal equivalence from Theorem 1.31. Inductively define a morphism $F_v\colon v(F(A), \ldots, F(Z)) \to F(v(A, \ldots, Z))$ in $\mathbf{C_s}$ by setting $F_{()} = F_0$, $F_{(A)} = F(A)$, and $F_{(x)\otimes(y)} = F_2 \circ (F_x \otimes F_y)$. Define $F_w$ similarly. Then the following diagram in $\mathbf{C_s}$ commutes:

$$\begin{array}{ccc}
v(F(A), \ldots, F(Z)) & \xrightarrow{\theta_{(F(A), \ldots, F(Z))}} & w(F(A), \ldots, F(Z)) \\
{\scriptstyle F_v}\downarrow & & \downarrow{\scriptstyle F_w} \\
F(v(A, \ldots, Z)) & \xrightarrow[F(\theta_{(A, \ldots, Z)})]{} & F(w(A, \ldots, Z))
\end{array}$$

The same diagram for $\theta'$ commutes similarly. But as $\mathbf{C_s}$ is a strict monoidal category, and $\theta$ and $\theta'$ are built from coherence isomorphisms, we must have $\theta_{(F(A), \ldots, F(Z))} = \theta'_{(F(A), \ldots, F(Z))} = \mathrm{id}$. Since $F_v$ and $F_w$ are by construction isomorphisms, it follows from the diagram above that $F(\theta_{(A, \ldots, Z)}) = F(\theta'_{(A, \ldots, Z)})$. Finally, $F$ is an equivalence, so there is a functor $G\colon \mathbf{C_s} \to \mathbf{C}$ such that $G \circ F$ is naturally isomorphic to the identity functor. So $G(F(\theta_{(A, \ldots, Z)})) = G(F(\theta'_{(A, \ldots, Z)}))$, and hence $\theta_{(A, \ldots, Z)} = \theta'_{(A, \ldots, Z)}$. □

Notice that the transformations $\theta, \theta'$ 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 1.31 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, Theorems 1.19 and 1.23. We will not go into details of the proofs, but just record the statements here.

**Definition 1.33** (Braided monoidal functor, symmetric monoidal functor)**.** A *braided monoidal functor* is a monoidal functor $\mathbf{C} \xrightarrow{F} \mathbf{D}$ between braided monoidal categories, that additionally makes the following diagrams commute:

$$\begin{array}{ccc} F(A) \otimes F(B) & \xrightarrow{\sigma_{F(A),F(B)}} & F(B) \otimes F(A) \\ {\scriptstyle (F_2)_{A,B}} \downarrow & & \downarrow {\scriptstyle (F_2)_{B,A}} \\ F(A \otimes B) & \xrightarrow[F(\sigma_{A,B})]{} & F(B \otimes A) \end{array} \tag{1.31}$$

A *symmetric monoidal functor* is a braided monoidal functor between symmetric monoidal categories.

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

**Theorem 1.34** (Strictification for braided monoidal categories). *Every braided monoidal category has a braided monoidal equivalence to a strict braided monoidal category. Every symmetric monoidal category has a symmetric monoidal equivalent to a strict symmetric 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 (1.17) and (1.20). By the correctness of the graphical calculus for braided monoidal categories, Theorem 1.19, 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 1.35** (Coherence for braided monoidal categories). *Let $v(A, \ldots, Z)$ and $w(A, \ldots, Z)$ be bracketings in a braided monoidal category* **C**. *Any two transformations $\theta, \theta' \colon v \Rightarrow w$ built from $\alpha$, $\alpha^{-1}$, $\lambda$, $\lambda^{-1}$, $\rho$, $\rho^{-1}$, $\sigma$, $\sigma^{-1}$, $\mathrm{id}$, $\otimes$, 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 1.32 for monoidal categories and the Correctness Theorem 1.19 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 1.36** (Coherence for symmetric monoidal categories). *Let $v(A, \ldots, Z)$ and $w(A, \ldots, Z)$ be bracketings in a braided monoidal category* **C**. *Any two transformations $\theta, \theta' \colon v \Rightarrow w$ built from $\alpha$, $\alpha^{-1}$, $\lambda$, $\lambda^{-1}$, $\rho$, $\rho^{-1}$, $\sigma$, $\sigma^{-1}$, $\mathrm{id}$, $\otimes$, 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 the Corollary 1.35, and the correctness of the graphical calculus for symmetric monoidal categories, Theorem 1.23. □

## 1.4 Exercises

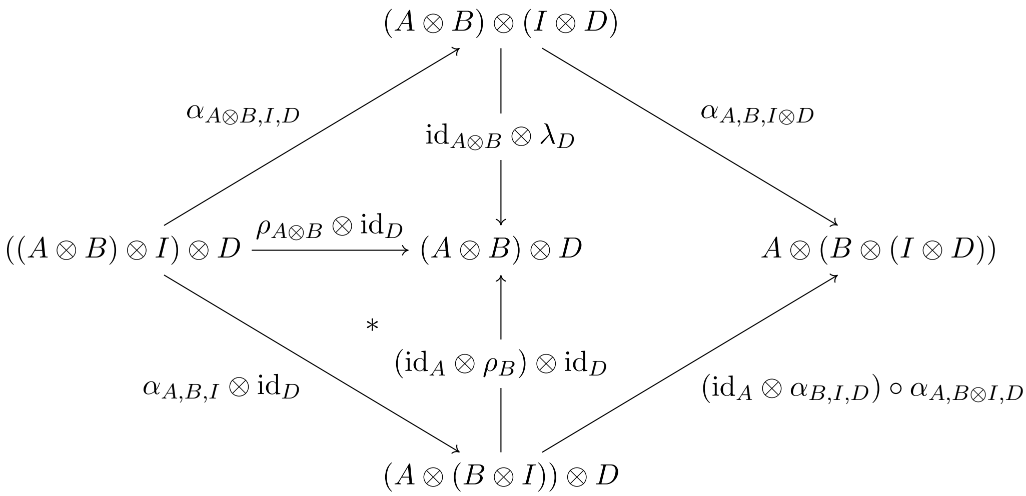
**Exercise 1.4.1.** Let $A, B, C, D$ be objects in a monoidal category. Construct a morphism

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

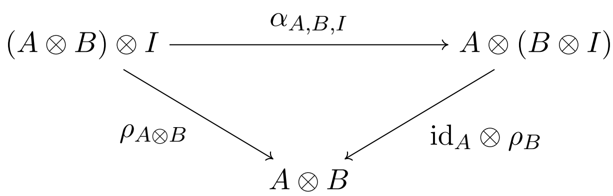
Can you find another?

**Exercise 1.4.2.** Suppose you are given the data of a monoidal category satisfying (1.1) and (1.2).

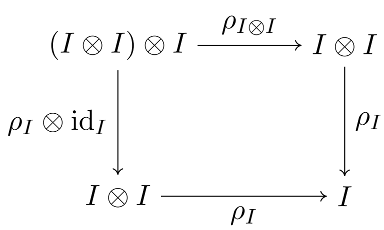
(a) Prove that the marked triangle in the diagram below commutes. (Hint: consider the rest of the diagram first, including the outside, and use naturality and invertibility of the associator and unitors.)




(b) Prove that the following triangle commutes.




(c) Prove that the following square commutes.



(d) Use your answers to (a)–(c) to conclude that $\rho_I = \lambda_I$.

**Exercise 1.4.3.** Let $(\mathbb{C}, \otimes, I)$ be a monoidal category, and suppose given the data of a braiding $\sigma$.

(a) Prove that the following diagrams commute

$$\begin{array}{ccc} A \otimes I & \xrightarrow{\sigma} & I \otimes A \\ & {\scriptstyle\rho}\searrow \quad \nearrow{\scriptstyle\lambda} & \\ & A & \end{array} \qquad \begin{array}{ccc} I \otimes A & \xrightarrow{\sigma} & A \otimes I \\ & {\scriptstyle\lambda}\searrow \quad \nearrow{\scriptstyle\rho} & \\ & A & \end{array}$$

(b) Show that the following diagram commutes

$$\begin{array}{ccccccc} (A \otimes B) \otimes C & \xrightarrow{\alpha} & A \otimes (B \otimes C) & \xrightarrow{\mathrm{id} \otimes \sigma} & A \otimes (C \otimes B) & \xrightarrow{\alpha} & (A \otimes C) \otimes B \\ {\scriptstyle \sigma \otimes \mathrm{id}}\downarrow & & & & & & \downarrow{\scriptstyle \sigma \otimes \mathrm{id}} \\ (B \otimes A) \otimes C & & & & & & (C \otimes A) \otimes B \\ {\scriptstyle \alpha}\downarrow & & & & & & \downarrow{\scriptstyle \alpha} \\ B \otimes (A \otimes C) & & & & & & C \otimes (A \otimes B) \\ {\scriptstyle \mathrm{id} \otimes \sigma}\downarrow & & & & & & \downarrow{\scriptstyle \mathrm{id} \otimes \sigma} \\ B \otimes (C \otimes A) & \xrightarrow[\alpha]{} & (B \otimes C) \otimes A & \xrightarrow[\sigma \otimes \mathrm{id}]{} & (C \otimes B) \otimes A & \xrightarrow[\alpha]{} & C \otimes (B \otimes A) \end{array}$$

(Hint: fill in the inside of the diagram with smaller commuting ones.)

**Exercise 1.4.4.** 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 $A \xrightarrow{f,g} A$.

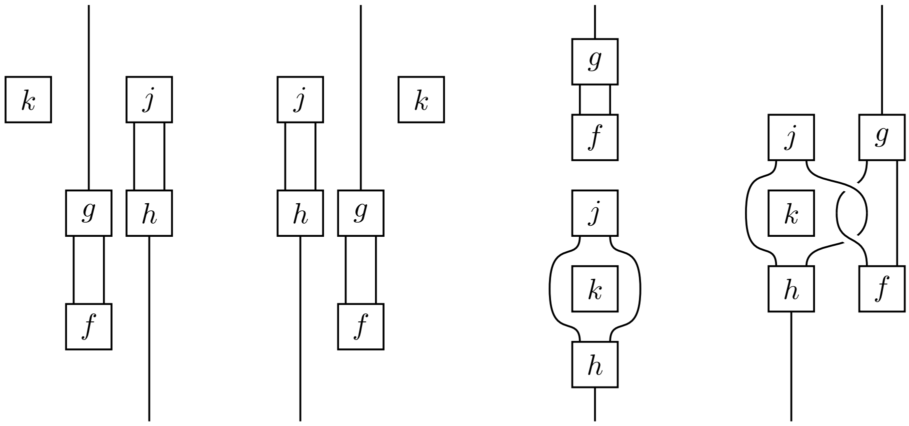
(b) $(f \otimes (g \circ h)) \circ k = (\mathrm{id} \otimes f) \circ ((g \otimes h) \circ k)$, for $A \xrightarrow{k} B \otimes C$, $C \xrightarrow{h} B$ and $B \xrightarrow{f,g} B$.

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

**Exercise 1.4.5.** Consider the following diagrams in the graphical calculus:



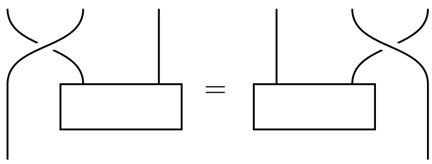

(1) (2) (3) (4)

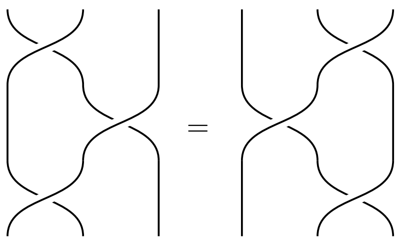
(a) Which of the diagrams (1), (2) and (3) are equal as morphisms in a monoidal category?

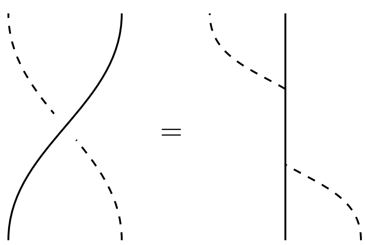
(b) Which of the diagrams (1), (2), (3) and (4) are equal as morphisms in a braided monoidal category?

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

**Exercise 1.4.6.** Prove the following graphical equations directly using the axioms of a braided monoidal category:

(a) 

(b) 

(c) 

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

**Exercise 1.4.7.** Look at Definition 0.47 of the Kronecker product.

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

(b) What might go wrong if you try to include infinite-dimensional Hilbert spaces in a strict, skeletal category as in Definition 1.26?

**Exercise 1.4.8.** Recall that an entangled state of objects $A$ and $B$ is a state of $A \otimes B$ that is not a product state.

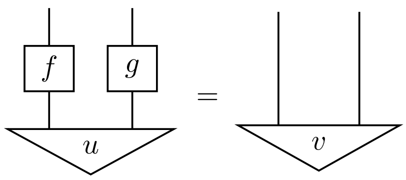
(a) Which of these states of $\mathbb{C}^2 \otimes \mathbb{C}^2$ in $\mathbf{Hilb}$ are entangled?

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

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

$$\begin{aligned}&\{(0,0),(0,1)\}\\&\{(0,0),(0,1),(1,0)\}\\&\{(0,1),(1,0)\}\\&\{(0,0),(0,1),(1,0),(1,1)\}\end{aligned}$$

**Exercise 1.4.9.** We say that two joint states $I \xrightarrow{u,v} A \otimes B$ are *locally equivalent*, written $u \sim v$, 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 1.4.10.** Recall equation (1.11) 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 $u$ 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 $x \circ f \circ u$ occur? How about $y \circ f \circ u$?

(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 $U$ be the state $\{0\}$, let $X$ be the effect $\{0\}$, and let $Y$ be the effect $\{1\}$. Can the history $X \circ R \circ U$ occur? How about $Y \circ R \circ U$?

**Exercise 1.4.11.** Show that if a category has products, they can be used to construct a symmetric monoidal structure.

**Exercise 1.4.12.** Show that **Set** is 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 1.4.13.** Let $\mathbf{C}$ and $\mathbf{D}$ be monoidal categories. Suppose that $F \colon \mathbf{C} \to \mathbf{D}$ is a functor, that $\varphi_{A,B} \colon F(A) \otimes F(B) \to F(A \otimes B)$ is a natural isomorphism satisfying (1.27), and that there exists some isomorphism $\psi \colon I \to F(I)$. Define $\varphi_I \colon I \to F(I)$ as the composite

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

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

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

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

(b) Show that $\varphi_I$ satisfies (1.28), making $(F, \varphi)$ into a monoidal functor.

# Notes and further reading

Symmetric monoidal categories were introduced independently by Bénabou and Mac Lane in 1963 [**?**, **?**]. 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 [**?**, **?**]. There are some caveats to our formulation of the Coherence Theorem 1.2 – that all "well-formed" equations are satisfied; see [**?**] and 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 graphical language dates back to 1971, when Penrose used it to abbreviate tensor contraction calculations [**?**]. It was formalized for monoidal categories by Joyal and Street in 1991 [**?**], who later also introduced and generalized to braided monoidal categories [**?**]. The latter paper is also the source of the streamlined proof of the Strictification Theorem 1.31. Freyd and Yetter [**?**] introduced the braided monoidal category of crossed $G$-sets. For a modern survey, focusing on soundness and completeness of the graphical calculus, see [**?**].

The relevance of monoidal categories for quantum theory was emphasized originally by Abramsky and Coecke [**?**, **?**], and was also popularized by Baez [**?**] 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, zero-dimensional spaces, addition of linear operators, direct sums, matrices and inner products. We will see how to use these to model important features of quantum mechanics such as classical data and superposition.

## 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 $f(a) = a \cdot f(1)$. 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 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 $u, v, w \in A$ an associativity law $u(vw) = (uv)w$ and a unit law $1v = v = v1$. 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: $T = \emptyset$ and $F = \{(\bullet, \bullet)\}$. Working out the composition in **Rel** gives the following multiplication table:

| | F | T |
|---|---|---|
| F | F | F |
| T | F | T |

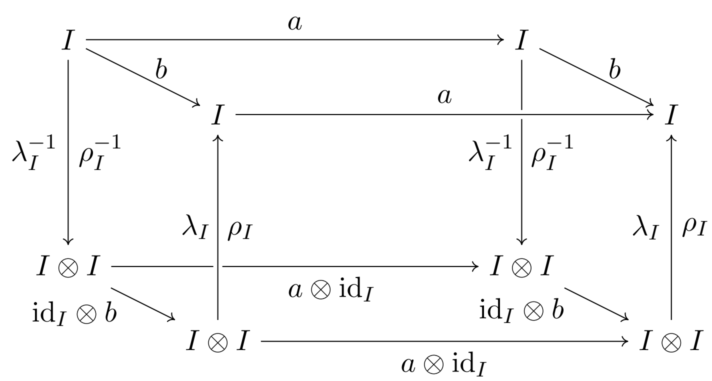
  Hence we can recognize the scalars in **Rel** as the Boolean truth values {true, false} under conjunction.

## 2.1.1 Commutativity

Multiplication of complex numbers is commutative: $ab = ba$. 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 $I \xrightarrow{a,b} I$:




(2.1)

The four side cells of the cube commute by naturality of $\lambda_I$ and $\rho_I$, and the bottom cell commutes by an application of the interchange law of Theorem 1.6. Hence we have $ab = ba$. 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.

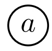
- In **Hilb**: multiplication of complex numbers is commutative.

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

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

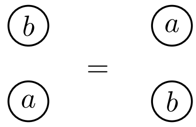
### 2.1.2 Graphical calculus

We draw scalars as circles:




(2.2)

Commutativity of scalars then has the following graphical representation:




(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 $a \in \mathbb{C}$ is a scalar and $f$ a linear map, then $af$ 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 $I \xrightarrow{a} I$ and a morphism $A \xrightarrow{f} B$, the *left scalar multiplication* $A \xrightarrow{a \bullet f} B$ is the following composite:

$$\begin{array}{ccc} A & \xrightarrow{\quad a \bullet f \quad} & B \\ {\scriptstyle \lambda_A^{-1}} \big\downarrow & & \big\uparrow {\scriptstyle \lambda_B} \\ I \otimes A & \xrightarrow{\quad a \otimes f \quad} & I \otimes B \end{array} \tag{2.4}$$

This abstract scalar multiplication satisfies many properties we are familiar with from scalar multiplication of vector spaces, as the following lemma explores.

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

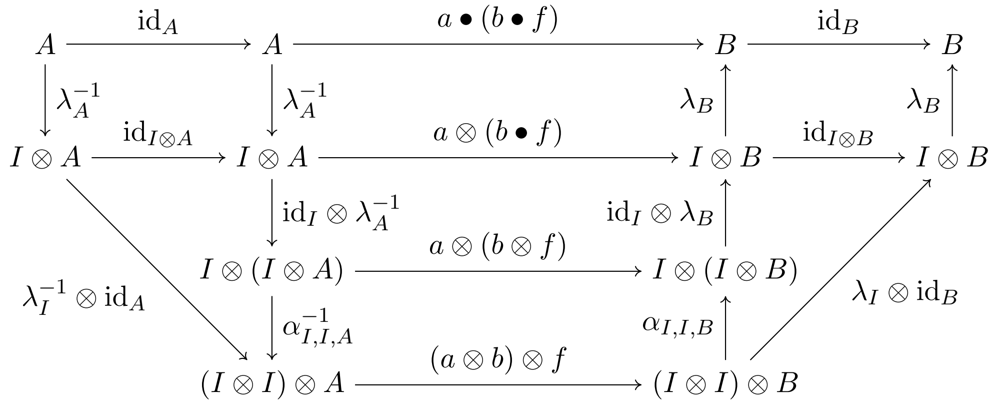
*(a)* $\mathrm{id}_I \bullet f = f$;

*(b)* $a \bullet b = a \circ b$;

*(c)* $a \bullet (b \bullet f) = (a \bullet b) \bullet f$;

*(d)* $(b \bullet g) \circ (a \bullet f) = (b \circ a) \bullet (g \circ f)$.

*Proof.* These statements all follow straightforwardly from the graphical calculus, thanks to Theorem 1.9. We also give the direct algebraic proofs. Part (a) follows directly from naturality of $\lambda$. For part (b), diagram (2.1) shows that $a \circ b = \lambda_I \circ (a \otimes b) \circ \lambda_I^{-1} = a \bullet b$. Part (c) follows from the following diagram that commutes by coherence:




Part (d) follows from the interchange law of Theorem 1.6. □

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

- In **Hilb**: if $a \in \mathbb{C}$ is a scalar and $H \xrightarrow{f} K$ a morphism, then $H \xrightarrow{a \bullet f} K$ is the morphism $v \mapsto af(v)$.
- 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 $v, w \in \mathbb{C}^2$ is a linear combination $av + bw$ of them for scalars $a, b \in C$. We dealt with the scalar multiplication in the previous section; in this section we focus 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 $v \mapsto 0$. This linear map is characterized by saying that it factors through the zero-dimensional vector space $V \to \{0\} \to W$. Specifically, there is a unique linear map $\{0\} \to V$, namely $0 \mapsto 0$, and a unique linear map $V \to \{0\}$, namely $v \mapsto 0$. This characterization makes sense in arbitrary categories.

**Definition 2.8** (Terminal object, initial object)**.** An object $1$ is *terminal* if for any object $A$ there is a unique morphism $A \to 1$. An object $0$ is *initial* if for any object $A$ there is a unique morphism $0 \to A$.

**Definition 2.9** (Zero object, zero morphism)**.** An object $0$ is a *zero object* when it is both initial and terminal. 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 2.10.** *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 $B \to B$. But then $A$ and $B$ must be isomorphic via the unique morphisms $A \to B$ and $B \to A$. A similar argument holds for terminal objects. This immediately implies that zero objects are also unique up to unique isomorphism. □

**Lemma 2.11.** *Composition with a zero morphism always gives a zero morphism; that is, for any objects $A$, $B$ and $C$, and any morphism $A \xrightarrow{f} B$, we have the following:*

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

**Example 2.12.** 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, to build superpositions of qubit states we need to use vector addition. More generally, given linear maps $V \xrightarrow{f,g} W$ between vector spaces we can form their sum $V \xrightarrow{f+g} W$, which is another linear map. We can phrase such a *superposition rule* in terms of categorical structure alone.

**Definition 2.13** (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:**
$$u_{B,C} \circ u_{A,B} = u_{A,C} \tag{2.11}$$

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

**Example 2.14.** Both **Hilb** and **Rel** have a superposition rule; **Set** does not.

- In **Hilb** the superposition rule is addition of linear maps, given by $(f+g)(v) = f(v)+g(v)$.
- In **Rel**, the superposition rule is given by union of subsets: $R+S = R \cup S$. In the matrix representation of relations (7), this corresponds to entrywise disjuction.
- **Set** cannot be given a superposition rule. If it had one there would be a unit morphism $A \xrightarrow{u_{A,\emptyset}} \emptyset$, but there are no such functions for nonempty sets $A$.

The following lemma shows the connection between zero morphisms and superposition rules.

**Lemma 2.15.** *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 this 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 2.16.** *If a monoidal category has a zero object and a superposition rule, its scalars form a* commutative semiring with an absorbing zero*, which is a set equipped with commutative, associative multiplication and addition operations with the following properties:*

$$
\begin{aligned}
(a+b)c &= ac+bc \\
a(b+c) &= ab+ac \\
a+b &= b+a \\
a+0 &= 0+a \\
a0 = 0 &= 0a
\end{aligned}
$$

*Proof.* The first four properties follow directly from Definition 2.13: 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 2.15. □

**Example 2.17.** Thus we can extend 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).

### 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 $v \mapsto (v, 0)$ and $w \mapsto (0, w)$. 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 $(v, w) \mapsto v$ and $(v, w) \mapsto w$. Moreover, the latter reconstruction operation can undo the former deconstruction operation because $(v, w) = (v, 0) + (0, w)$. Using superposition rules, we can phrase this structure in any category.

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

$$\mathrm{id}_{A_i} = p_i \circ i_i \tag{2.12}$$

$$0_{A_i, A_j} = p_i \circ i_j \tag{2.13}$$

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

for all $i \neq j$. This generalizes to an arbitrary finite number of objects.

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 $p_i$ 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 0.19 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 $p_2 \circ \begin{pmatrix} f_1 \\ f_2 \end{pmatrix}$. 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, 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 2.10.

**Example 2.20.** Both **Hilb** and **Rel** have biproducts of finite lists of 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 $(v, w) \mapsto v$ and $(v, w) \mapsto w$. Injections $i_H \colon H \to H \oplus K$ and $i_K \colon K \to H \oplus K$ are given by $v \mapsto (v, 0)$ and $w \mapsto (0, w)$.
- In **Rel**, the disjoint union $A \sqcup B$ of sets provides biproducts. Projections $A \sqcup B \to A$ and $A \sqcup B \to B$ are given by $a \sim a$ and $b \sim b$. Injections $A \to A \sqcup B$ and $B \to A \sqcup B$ 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. We now prove that superposition rules are unique in the presence of biproducts.

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

*Proof.* Write $+$ and $\boxplus$ for the two superposition rules. Then we do the following computation for any $A \xrightarrow{f,g} B$, where $A \xrightarrow{i_1, i_2} A \oplus A \xleftarrow{p_1, p_2} A$ 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 full biproduct structure is not needed here, so if we wanted we could weaken the hypotheses. □

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.

### 2.2.4 Matrix notation

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

$$A \oplus B \xrightarrow{\begin{pmatrix} f & h \\ g & j \end{pmatrix}} C \oplus D \tag{2.15}$$

as shorthand for the following map:

$$A \oplus B \xrightarrow{(i_C \circ f \circ p_A) + (i_D \circ g \circ p_A) + (i_C \circ h \circ p_B) + (i_D \circ j \circ p_B)} C \oplus D \tag{2.16}$$

Matrices with any finite number of rows and columns are defined in a similar way.

**Definition 2.22** (Matrix notation)**.** 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:

$$\big(f_{m,n}\big) \equiv \begin{pmatrix} f_{11} & f_{12} & \cdots & f_{1N} \\ f_{21} & f_{22} & \cdots & f_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ f_{M1} & f_{M2} & \cdots & f_{MN} \end{pmatrix} := \sum_{m,n} (i_n \circ f_{m,n} \circ p_m) \tag{2.17}$$

**Lemma 2.23** (Matrix representation)**.** *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 only:

$$\begin{aligned} f &\overset{(2)}{=} \mathrm{id}_{C\oplus D} \circ f \circ \mathrm{id}_{A\oplus B} \\ &\overset{(2.14)}{=} \big((i_C \circ p_C) + (i_D \circ p_D)\big) \circ f \circ \big((i_A \circ p_A) + (i_B \circ p_B)\big) \\ &\overset{\substack{(2.9)\\(2.10)}}{=} i_C \circ (p_C \circ f \circ i_A) \circ p_A + i_C \circ (p_C \circ f \circ i_B) \circ p_B \\ &\qquad + i_D \circ (p_D \circ f \circ i_A) \circ p_A + i_D \circ (p_D \circ f \circ i_B) \circ p_B \\ &\overset{(2.17)}{=} \begin{pmatrix} p_C \circ f \circ i_A & p_C \circ f \circ i_B \\ p_D \circ f \circ i_A & p_D \circ f \circ i_B \end{pmatrix} \end{aligned}$$

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

**Lemma 2.24.** *Morphisms between biproduct objects are equal if and only if their matrix entries are equal.*

*Proof.* WRITE OUT. □

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

$$\mathrm{id}_{A\oplus B} = \begin{pmatrix} \mathrm{id}_A & 0_{B,A} \\ 0_{A,B} & \mathrm{id}_B \end{pmatrix} \tag{2.18}$$

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

**Proposition 2.25.** *Matrices compose in the following way:*

$$\big(g_{jk}\big) \circ \big(f_{ij}\big) = \big(\textstyle\sum_j g_{ij} \circ f_{jk}\big) \tag{2.19}$$

*Proof.* We demonstrate this with the following calculation:

$$\begin{aligned}(g_{xy}) \circ (f_{yz}) &\equiv \left(\sum_{w,x} (i_w \circ g_{w,x} \circ p_x)\right) \circ \left(\sum_{y,z} (i_y \circ f_{y,z} \circ p_z)\right) \\ &= \sum_{w,x,y,z} (i_w \circ g_{w,x} \circ p_x \circ i_y \circ f_{y,z} \circ p_z) \\ &= \sum_{w,x,z} (i_w \circ g_{w,x} \circ f_{x,z} \circ p_z)\end{aligned}$$

This 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:

$$\begin{pmatrix} s & p \\ q & r \end{pmatrix} \circ \begin{pmatrix} f & g \\ h & j \end{pmatrix} = \begin{pmatrix} (s \circ f) + (p \circ h) & (s \circ g) + (p \circ j) \\ (q \circ f) + (r \circ h) & (q \circ g) + (r \circ j) \end{pmatrix} \tag{2.20}$$

**Example 2.26.** 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 $\{\texttt{false}, \texttt{true}\}$–valued matrices, 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 2.16, 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.

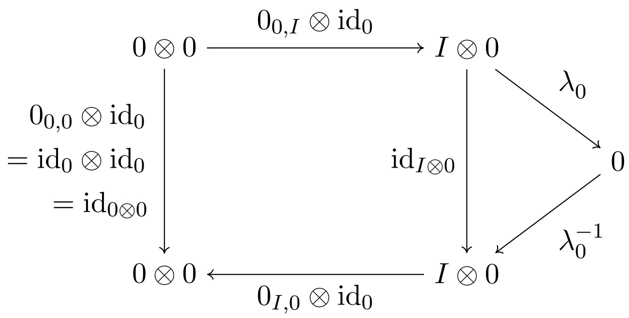
**Lemma 2.27.** *In a monoidal category with a zero object,* $0 \otimes 0 \simeq 0$.

*Proof.* First note that $I \otimes 0$, being isomorphic to $0$, is a zero object. Consider the 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 $\mathrm{id}_0$ as $0$ is a zero object. Composing in the other direction also gives the identity, as the following diagram shows:




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

## 2.3 Daggers

In Definition 0.37 of the category of Hilbert spaces, one aspect seemed 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 functor*, 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 $K \xrightarrow{f^\dagger} H$. We can encode this action as a functor.

**Definition 2.28.** 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 is the identity on objects, meaning that $\mathrm{id}_H{}^\dagger = \mathrm{id}_H$ for all objects $H$, and it is 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 $\mathbb{C} \xrightarrow{v,w} H$ be states of some Hilbert space $H$. The following calculation shows that the scalar $\mathbb{C} \xrightarrow{w} H \xrightarrow{v^\dagger} \mathbb{C}$ is equal to the inner product $\langle v|w\rangle$:

$$\begin{aligned}(\mathbb{C} \xrightarrow{w} H \xrightarrow{v^\dagger} \mathbb{C}) &\equiv v^\dagger(w(1)) \\ &\overset{(23)}{=} \langle 1|v^\dagger(w(1))\rangle \\ &\overset{(24)}{=} \langle v|w\rangle \end{aligned} \tag{2.21}$$

So the functor taking adjoints contains all the information required to reconstruct the inner products on our Hilbert spaces. Since we used the inner products to define this functor in the first place, we see that knowing the functor taking adjoints is *equivalent* to knowing the inner products.

This suggests a way to generalize the idea of 'inner products' to arbitrary categories, using the following structure.

**Definition 2.29** (Dagger functor, dagger category)**.** A *dagger functor* 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 functor.

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

$$(g \circ f)^\dagger = f^\dagger \circ g^\dagger \tag{2.22}$$

$$\mathrm{id}_H{}^\dagger = \mathrm{id}_H \tag{2.23}$$

$$(f^\dagger)^\dagger = f \tag{2.24}$$

The identity-on-objects and contravariant properties mean that if $A \xrightarrow{f} B$, we must have $B \xrightarrow{f^\dagger} A$. The involutive property says that $(f^\dagger)^\dagger = f$.

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

**Definition 2.30.** 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 functor would give an bijection between these sets for all $A$ and $B$, which is not possible.

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 functor is possible. The category **FVect** containing only finite-dimensional objects *can* be equipped with a dagger functor: one way to do this is by assigning an inner product to every object, and then constructing the associated adjoints. However, it does not come with a *canonical* dagger functor.

A different use daggers is in classical probability theory, to construct the Bayesian converse of conditional probability distributions.

**Definition 2.31.** The dagger category **Bayes** is defined as follows:

- **objects** $(A, p)$ are finite sets $A$ equipped with *prior probability distributions*, functions $p : A \to \mathbb{R}^+$ such that $\sum_{a \in A} p(a) = 1$;
- **morphisms** $(A, p) \xrightarrow{f} (B, q)$ are *conditional probability distributions*, functions $f : A \times B \to \mathbb{R}^{\geq 0}$ 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 functor** is the *Bayesian converse*, acting on $f : A \times B \to \mathbb{R}^{\geq 0}$ to give $f^\dagger : B \times A \to \mathbb{R}^{\geq 0}$, defined as $f^\dagger(b, a) := f(a, b) q(b) / p(a)$.

Note that the Bayesian converse is always well-defined since we require our prior probability distributions to be nonzero at every point.

In a dagger category we give special names to some basic properties of morphisms. These generalize the terms in Definition 0.42 usually reserved for bounded linear maps between Hilbert spaces.

**Definition 2.32.** 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 $f = f^\dagger$;
- a *projector* when $f = f^\dagger$ and $f \circ f = f$;
- *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 projector;
- *positive* when $f = g^\dagger \circ g$ for some bounded linear map $H \xrightarrow{g} K$.

We will use the unitarity property particularly often, usually in its graphical representation:

(2.25)

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 functor is an important structure for us, and for most of this book we will require compatibility with it. In the search for good definitions, it is useful to see this as a sort of guiding principle, which we summarize as the *way of the dagger*. Sometimes this compatibility comes for free, as in the following example.

**Lemma 2.33.** *In a dagger category with a zero object,* $0^\dagger_{A,B} = 0_{B,A}$.

*Proof.* This is immediate from functoriality:

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

## 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 2.34** (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 the natural isomorphisms $\alpha$, $\lambda$ and $\rho$ 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 2.35.** Both **Hilb** and **Rel** are symmetric monoidal dagger categories.

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

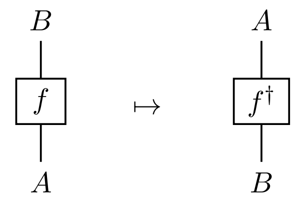
$$\begin{aligned}
&\langle (f \otimes g)^\dagger (v_1 \otimes w_1) | v_2 \otimes w_2 \rangle \\
&\quad = \langle v_1 \otimes w_1 | (f \otimes g)(v_2 \otimes w_2) \rangle \\
&\quad = \langle v_1 \otimes w_1 | f(v_2) \otimes g(w_2) \rangle \\
&\quad = \langle v_1 | f(v_2) \rangle \langle w_1 | g(w_2) \rangle \\
&\quad = \langle f^\dagger(v_1) | v_2 \rangle \langle g^\dagger(w_1) | w_2 \rangle \\
&\quad = \langle (f^\dagger \otimes g^\dagger)(v_1 \otimes w_1) | v_2 \otimes w_2 \rangle .
\end{aligned}$$

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

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

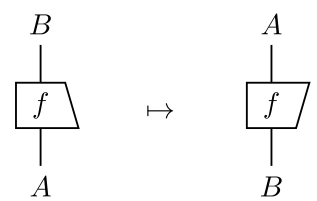
In each case the coherence isomorphisms $\lambda, \rho, \alpha, \sigma$ are also clearly unitary.

We depict taking daggers in the graphical calculus by flipping the graphical representation about a horizontal axis as follows.




(2.26)

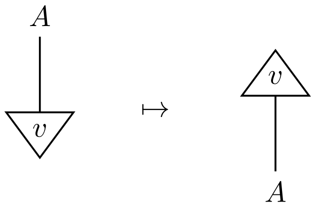
To help differentiate between these morphisms, we will draw morphisms in a way that breaks their symmetry. Taking daggers then has the following representation.




(2.27)

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

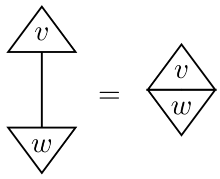
In particular, in a monoidal dagger category, we can use this notation for morphisms $I \xrightarrow{v} A$ representing a state. This gives a representation of the adjoint morphism $A \xrightarrow{v^\dagger} I$ as follows.




(2.28)

We have described how 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 functor gives a correspondence between states and effects.

Equation (2.21) 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 $\langle v|w\rangle$ of two states $I \xrightarrow{v,w} H$.

$\langle v|w\rangle =$ 


(2.29)

Notice that the right-hand side 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 transpose matrices, 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 2.36** (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 2.37.** While ordinary biproducts are unique up to isomorphism, dagger biproducts are unique up to *unitary* isomorphism.

- In $\mathbf{Rel}$, every biproduct is a dagger biproduct.
- In $\mathbf{Hilb}$, 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 functor.

You might expect a property like $(f \oplus g)^\dagger = f^\dagger \oplus g^\dagger$ to be required to ensure 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 our definition of dagger biproduct.

**Lemma 2.38** (Adjoint of a matrix)**.** *In a dagger category with dagger biproducts, the adjoint of a matrix is its conjugate transpose:*

$$\begin{pmatrix} f_{11} & f_{12} & \cdots & f_{1n} \\ f_{21} & f_{22} & \cdots & f_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ f_{m1} & f_{m2} & \cdots & f_{mn} \end{pmatrix}^\dagger = \begin{pmatrix} f_{11}^\dagger & f_{21}^\dagger & \cdots & f_{m1}^\dagger \\ f_{12}^\dagger & f_{22}^\dagger & \cdots & f_{m2}^\dagger \\ \vdots & \vdots & \ddots & \vdots \\ f_{1n}^\dagger & f_{2n}^\dagger & \cdots & f_{mn}^\dagger \end{pmatrix} \tag{2.30}$$

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

$$\begin{aligned}
\begin{pmatrix} f_{11} & f_{12} & \cdots & f_{1n} \\ f_{21} & f_{22} & \cdots & f_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ f_{m1} & f_{m2} & \cdots & f_{mn} \end{pmatrix}^\dagger
&\overset{(2.17)}{=} \left( \sum_{n,m} i_n \circ f_{n,m} \circ i_m^\dagger \right)^\dagger \\
&\overset{(2.14)}{=} \left( \sum_p i_p \circ i_p^\dagger \right) \circ \left( \sum_{n,m} i_n \circ f_{n,m} \circ i_m^\dagger \right)^\dagger \circ \left( \sum_q i_q \circ i_q^\dagger \right) \\
&\overset{\substack{(2.9)\\(2.10)}}{=} \sum_{p,q} i_p \circ i_p^\dagger \circ \left( \sum_{n,m} i_n \circ f_{n,m} \circ i_m^\dagger \right)^\dagger \circ i_q \circ i_q^\dagger \\
&\overset{(2.22)}{=} \sum_{p,q} i_p \circ \left( i_q^\dagger \circ \left( \sum_{n,m} i_n \circ f_{n,m} \circ i_m^\dagger \right) \circ i_p \right)^\dagger \circ i_q^\dagger \\
&\overset{\substack{(2.9)\\(2.10)}}{=} \sum_{p,q} i_p \circ \left( \sum_{n,m} i_q^\dagger \circ i_n \circ f_{n,m} \circ i_m^\dagger \circ i_p \right)^\dagger \circ i_q^\dagger \\
&\overset{(2.12)}{=} \sum_{n,m} i_m \circ (f_{n,m})^\dagger \circ i_n^\dagger
\end{aligned}$$

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

It follows from this that daggers interact well with superposition.

**Corollary 2.39.** *In a dagger category with dagger biproducts, daggers distribute over addition:*

$$(f+g)^\dagger = f^\dagger + g^\dagger \tag{2.31}$$

*Proof.* We perform the following calculation:

$$\begin{aligned}
(f+g)^\dagger &\overset{(2.19)}{=} \left( \begin{pmatrix} f & g \end{pmatrix} \circ \begin{pmatrix} \mathrm{id}_B \\ \mathrm{id}_B \end{pmatrix} \right)^\dagger \overset{(2.22)}{=} \begin{pmatrix} \mathrm{id}_B \\ \mathrm{id}_B \end{pmatrix}^\dagger \circ \begin{pmatrix} f & g \end{pmatrix}^\dagger \\
&\overset{(2.30)}{=} \begin{pmatrix} \mathrm{id}_B & \mathrm{id}_B \end{pmatrix} \circ \begin{pmatrix} f^\dagger \\ g^\dagger \end{pmatrix} \overset{(2.19)}{=} f^\dagger + g^\dagger
\end{aligned}$$

This completes the proof. □

## 2.4 Modelling measurement

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

### 2.4.1 Probabilities

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

**Definition 2.40** (Probability)**.** If $I \xrightarrow{v} A$ is a state, and $A \xrightarrow{x} I$ an effect, in a monoidal dagger category, set

$$\text{Prob}(x, v) = v^\dagger \circ x^\dagger \circ x \circ v \colon I \to I. \tag{2.32}$$

**Example 2.41.** In our example categories, probabilities match with our interpretation.

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

### 2.4.2 Complete and disjoint sets of effects

Given a set of effects $A \xrightarrow{x_i} I$, we want an abstract understanding of when it tells us as much as possible about a system. The first property we require is completeness.

**Definition 2.42.** A set of effects $A \xrightarrow{x_i} I$ is *complete* if every nonzero process yields some effect; that is, for all morphisms $B \xrightarrow{f} A$ with $f \neq 0_{B,A}$, there is some $x_i$ such that $x_i \circ f \neq 0_{B,I}$.

The second property we require is that the effects are perfectly disjoint: if we prepare the system in state $x_i^\dagger$ and observe it with our set of effects, we can only get the outcome $x_i$.

**Definition 2.43.** A set of effects is *disjoint* if

$$x_i \circ x_i^\dagger = \text{id}_I, \qquad\qquad x_i \circ x_j^\dagger = 0_{I,I} \tag{2.33}$$

for $i \neq j$.

We can use biproducts to characterize complete sets of effects in the following way.

**Lemma 2.44.** *Complete disjoint sets of effects $A \xrightarrow{x_n} I$ correspond exactly to morphisms $A \xrightarrow{x} \bigoplus_{n=1}^N I$ with empty kernel, such that $x^\dagger$ is an isometry.*

*Proof.* A set of effects $A \xrightarrow{x_n} I$ correspond exactly to a column matrix $A \xrightarrow{x} \bigoplus_{n=1}^N I$. For this to have empty kernel is exactly the completeness condition. For $x^\dagger$ to be an isometry corresponds to the disjointness condition:

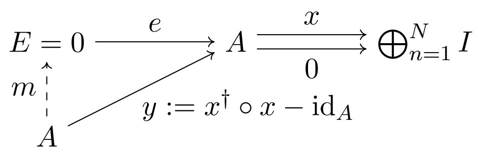
$$x \circ x^\dagger = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_N \end{pmatrix} \circ \begin{pmatrix} x_1^\dagger & x_2^\dagger & \cdots & x_N^\dagger \end{pmatrix} = \begin{pmatrix} x_1 \circ x_1^\dagger & x_1 \circ x_2^\dagger & \cdots & x_1 \circ x_N^\dagger \\ x_2 \circ x_1^\dagger & x_2 \circ x_2^\dagger & \cdots & x_2 \circ x_N^\dagger \\ \vdots & \vdots & \ddots & \vdots \\ x_N \circ x_1^\dagger & x_N \circ x_2^\dagger & \cdots & x_N \circ x_N^\dagger \end{pmatrix}$$

$$= \begin{pmatrix} \mathrm{id}_I & 0_{I,I} & \cdots & 0_{I,I} \\ 0_{I,I} & \mathrm{id}_I & \cdots & 0_{I,I} \\ \vdots & \vdots & \ddots & \vdots \\ 0_{I,I} & 0_{I,I} & \cdots & \mathrm{id}_I \end{pmatrix}$$

This completes the proof. □

**Lemma 2.45.** *Given a complete set of effects in a category with equalizers and invertible superposition rule, the biproduct* $A \xrightarrow{x} \bigoplus_{n=1}^{N} I$ *is unitary.*

*Proof.* Consider the following diagram:




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 $x \circ x^\dagger = \mathrm{id}_{\bigoplus^N I}$, this demonstrates that $x$ is unitary. □

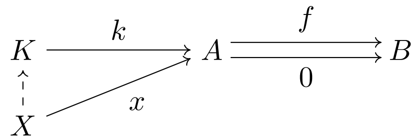
**Example 2.46.** Let us examine complete disjoint sets of effects in our example categories.

- **Hilb** has equalizers and an invertible superposition rule, so by Lemma 2.45 complete disjoint sets of effects correspond to unitary morphisms $H \simeq \mathbb{C}^n$. This is just the same as an orthonormal basis for $H$.
- In **Rel**, a complete disjoint set effects for a set $S$ is a partition of the set into subsets.

### 2.4.3 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 the abstract and that we can use 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 $f$, as follows.

**Definition 2.47** (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 $k$.



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

**Example 2.48.** 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 subspace $\ker(f) = \{v \in H \mid f(v) = 0\}$, or rather, the inclusion of this subspace into $H$. This is a dagger kernel rather than just a kernel because $\ker(f)$ is a closed subspace of $H$ rather than just any subspace.
- 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 2.5.6.

In general dagger categories with a zero object, not all morphisms have dagger kernels. The following lemma shows that the morphisms we are interested in from the perspective of the Born rule do always have dagger kernels.

**Lemma 2.49.** *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. □

It follows that zero is a dagger kernel of the matrix (**??**) for any complete set of effects $\{A \xrightarrow{a_i} I\}$ in a monoidal dagger category with a zero object and dagger biproducts. This means that if $I \xrightarrow{v} A$ is any state, then at least one of the histories $I \xrightarrow{v} A \xrightarrow{x_i} I$ must occur.

Dagger kernels also have a good influence on our abstraction of inner products.

**Lemma 2.50** (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 $f^\dagger \circ f = 0$, there is unique $A \xrightarrow{m} K$ with $f = k \circ m$. But then

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

If $I \xrightarrow{v} A$ is a state, nondegeneracy implies that $(I \xrightarrow{v} A \xrightarrow{v^\dagger} I) = 0$ if and only if $v = 0$. This is a good property, since we interpret $I \xrightarrow{v} A \xrightarrow{v^\dagger} I$ as the result of measuring the system $A$ in state $v$ immediately after preparing it in state $v$. The outcome is zero precisely when this history cannot possibly have occurred, so $v$ must have been an impossible state to begin with.

## 2.5 Exercises

**Exercise 2.5.1.** Recall Definition 2.18.

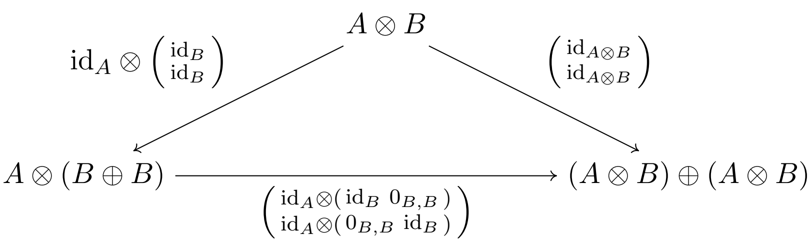
(a) Show that the biproduct of a pair of objects is unique up to a unique isomorphism.

(b) Suppose that a category has biproducts of pairs of objects, and a zero object. Show that this forms part of the data making the category into a monoidal category.

**Exercise 2.5.2.** Show that all joint states are product states when $A \otimes B$ is a product of $A$ and $B$. 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.




**Exercise 2.5.5.** 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 2.5.6.** 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?

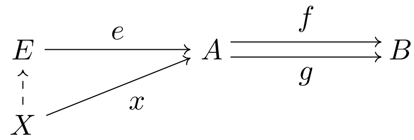
(g) Show that every biproduct in $\mathbf{Rel}$ is a dagger biproduct.

**Exercise 2.5.7.** 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 2.5.8.** 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 $e$.




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 2.5.9.** 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 $\mathbf{Rel}$.

# 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 [**?**]. 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 [**?**]. Superposition rules more formally known as enrichment in commutative monoids, and play an important role in such embedding theorems. See also [**?**] for an overview.

Self-duality in the form of involutive endofunctors on categories has been considered as early as 1950 [**?**, **?**]. A link between adjoint functors and adjoints in Hilbert spaces was made precise in 1974 [**?**]. The systematic exploitation of dagger functors in the way we have been using them started with Selinger in 2007 [**?**].

Using different terminology, Lemma 2.3 was proved in 1980 by Kelly and Laplaza [**?**]. The realization that endomorphisms of the tensor unit behave as scalars was made explicit by Abramsky and Coecke in 2004 [**?**, **?**]. Heunen proved an analogue of Mitchell's embedding theorem for $\mathbf{Hilb}$ in 2009 [**?**]. Conditions under which the scalars embed into the complex numbers are due to Vicary [**?**].

# Chapter 3

# Dual objects

Dualizability is a property of an object that means the wire representing it in the graphical calculus can bend. It has a fundamental topological interpretation, while at the same time giving a powerful categorical model for entangled states. Dual objects lie at the heart of many modern developments in mathematics, topology and quantum information.

## 3.1 Dual objects

**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:

$$\begin{array}{ccccc} L & \xrightarrow{\rho_L^{-1}} & L \otimes I & \xrightarrow{\mathrm{id}_L \otimes \eta} & L \otimes (R \otimes L) \\ {\scriptstyle \mathrm{id}_L}\downarrow & & & & \downarrow{\scriptstyle \alpha^{-1}_{L,R,L}} \\ L & \xleftarrow[\lambda_L]{} & I \otimes L & \xleftarrow[\varepsilon \otimes \mathrm{id}_L]{} & (L \otimes R) \otimes L \end{array} \tag{3.1}$$

$$\begin{array}{ccccc} R & \xrightarrow{\lambda_R^{-1}} & I \otimes R & \xrightarrow{\eta \otimes \mathrm{id}_R} & (R \otimes L) \otimes R \\ {\scriptstyle \mathrm{id}_R}\downarrow & & & & \downarrow{\scriptstyle \alpha_{R,L,R}} \\ R & \xleftarrow[\rho_R]{} & R \otimes I & \xleftarrow[\mathrm{id}_R \otimes \varepsilon]{} & R \otimes (L \otimes R) \end{array} \tag{3.2}$$

When $L$ is both left and right dual to $R$, we simply call $L$ a *dual* of $R$.

We 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.


(3.3)

The unit $I \xrightarrow{\eta} R \otimes L$ and counit $L \otimes R \xrightarrow{\varepsilon} I$ are drawn as bent wires:


(3.4)

This notation is chosen because of the attractive form it gives to the duality equations:


(3.5)

Because of their graphical form, they are also called the *snake equations*.

These equations add *orientation* to the two-dimensional graphical calculus of monoidal categories. Physically, $\eta$ 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.** We now see what dual objects look like in our example categories.

- The monoidal category $\mathbf{FHilb}$ has all duals. Every finite-dimensional Hilbert space $H$ is both right dual and left dual to its dual Hilbert space $H^*$ (see Definition 0.44), in a canonical way. (Of course, this explains the origin of the terminology.) The counit $H \otimes H^* \xrightarrow{\varepsilon} \mathbb{C}$ of the duality $H \dashv H^*$ is given by the following map:

$$\varepsilon : |\phi\rangle \otimes \langle\psi| \mapsto \langle\psi|\phi\rangle \tag{3.6}$$

  The unit $\mathbb{C} \xrightarrow{\eta} H^* \otimes H$ is defined as follows, for any orthonormal basis $|i\rangle$:

$$\eta : 1 \mapsto \sum_i \langle i| \otimes |i\rangle \tag{3.7}$$

  These definitions sit together rather oddly, since $\eta$ seems basis-dependent, while $\varepsilon$ is clearly not. In fact the same value of $\eta$ is obtained whatever orthonormal basis is used, as is made clear by Lemma 3.5 below.

- Infinite-dimensional Hilbert spaces do not have duals. For an infinite-dimensional Hilbert space, the definitions of $\eta$ and $\varepsilon$ are no good, as they do not give bounded linear maps. In Corollary 3.57 later in this section, we show 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 $S$, the relations $1 \xrightarrow{\eta} S \times S$ and $S \times S \xrightarrow{\varepsilon} 1$ are defined in the following way, where we write $\bullet$ for the unique element of the 1-element set:

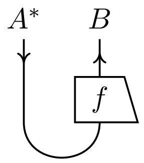
$$\bullet \sim_\eta (s, s) \text{ for all } s \in S \tag{3.8}$$
$$(s, s) \sim_\varepsilon \bullet \text{ for all } s \in S \tag{3.9}$$

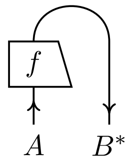
- In $\mathbf{Mat}_{\mathbb{C}}$, every object $n$ is its own dual, with a canonical choice of $\eta$ and $\varepsilon$ given as follows:

$$\eta : 1 \mapsto \sum_i |i\rangle \otimes |i\rangle \qquad\qquad \varepsilon : |i\rangle \otimes |j\rangle \mapsto \delta_{ij} 1 \tag{3.10}$$

The category $\mathbf{Set}$ only has duals for sets of size 1. To understand why, it helps to introduce the *name* and *coname* of a morphism.

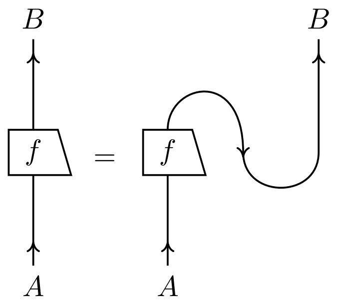
**Definition 3.3.** In a monoidal category with dualities $A \dashv A^*$ and $B \dashv B^*$, given a morphism $A \xrightarrow{f} B$, we define its *name* $I \xrightarrow{\ulcorner f \urcorner} A^* \otimes B$ and *coname* $A \otimes B^* \xrightarrow{\llcorner f \lrcorner} I$ as the following morphisms:




(3.11)

Morphisms can be recovered from their names or conames, as we can demonstrate by making use of the snake equations:




(3.12)

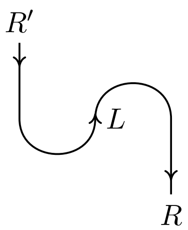
In $\mathbf{Set}$ the monoidal unit object 1 is terminal, and so all conames $A \otimes B^* \xrightarrow{\llcorner f \lrcorner} 1$ must be equal. If $\mathbf{Set}$ had duals for objects this would then imply that all functions $A \xrightarrow{f} B$ are equal, which is only the case for $A = \emptyset$ (the empty set), or $B = 1$. It can be immediately checked that $\emptyset$ does not have a dual, because there can be no morphism $1 \to \emptyset \times \emptyset^*$ for any value of $\emptyset^*$. The 1-element set does have a dual since it is the monoidal unit, as established by Lemma 3.6 below.

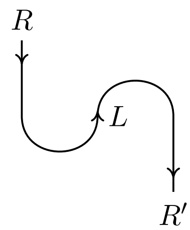
### 3.1.1 Basic properties

The first thing we show is that duals are well-defined up to canonical isomorphism.

**Lemma 3.4.** *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:




(3.13)

It follows from the snake equations that these are inverse to each other. Conversely, if $L \dashv R$ and $R \xrightarrow{f} R'$ is an isomorphism, then we can construct a duality $L \dashv R'$ as follows:

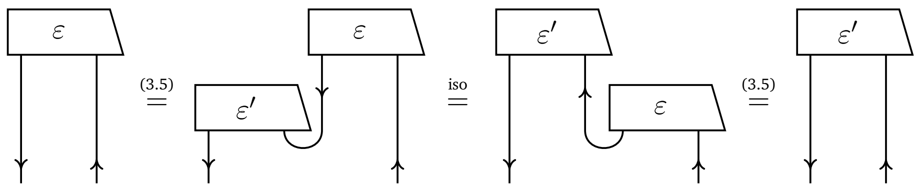

(3.14)

An isomorphism $L \simeq L'$ allows us to produce a duality $L' \dashv R$ in a similar way. □

The next lemma shows that given a duality, the unit determines the counit, and vice-versa.

**Lemma 3.5.** *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.* For the first case, we use the following graphical argument.




The second case is similar. □

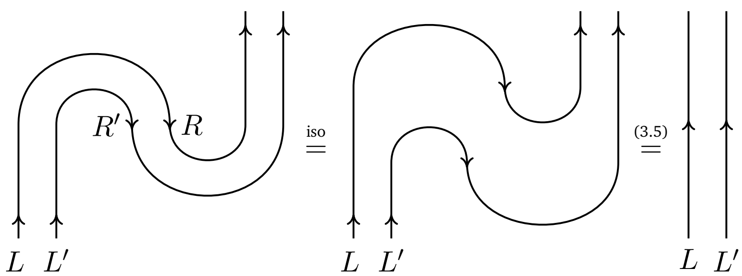
The following lemma shows that dual objects interact well with the monoidal structure.

**Lemma 3.6.** *In a monoidal category, $I \dashv I$.*

*Proof.* Taking $\eta = \lambda_I^{-1} \colon I \to I \otimes I$ 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. □

**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, as follows:

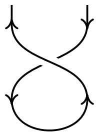



The other snake equation follows similarly. □

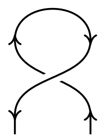
If the monoidal category has a braiding then a duality $L \dashv R$ gives rise to a duality $R \dashv L$, as the next lemma investigates.

**Lemma 3.8.** *In a braided monoidal category,* $L \dashv R \Rightarrow R \dashv L$.

*Proof.* Suppose we have $(L, R, \eta, \varepsilon)$ witnessing the duality $L \dashv R$. Then we construct a duality $(R, L, \eta', \varepsilon')$ as follows, where we use the ordinary graphical calculus for the duality $(L, R, \eta, \varepsilon)$:

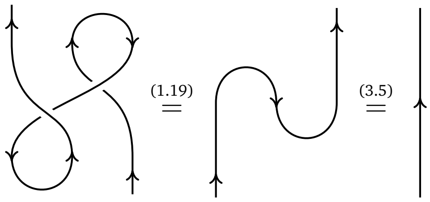


$I \xrightarrow{\eta'} L \otimes R$



$R \otimes L \xrightarrow{\varepsilon'} I$

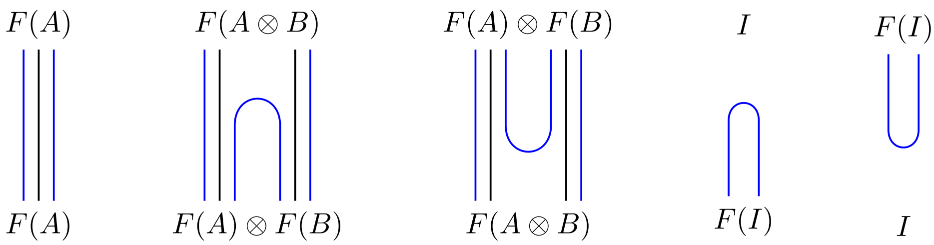
Writing out one of the snake equations for these new duality morphisms, we see that they are satisfied by using properties of the swap map and the snake equations for the original duality morphisms $\eta$ and $\varepsilon$:




The other snake equation can be proved in a similar way. □

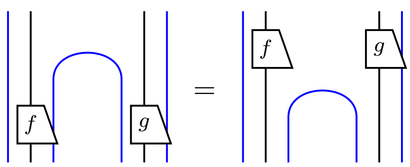
## 3.1.2 Duals and monoidal functors

We can denote the structure of a monoidal functor like this:



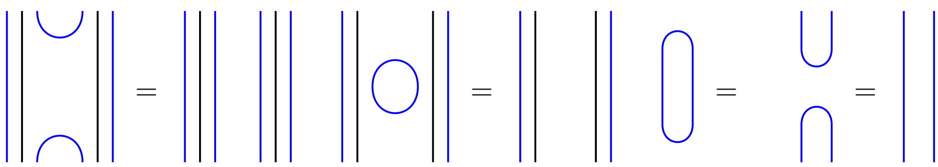

(3.15)

Naturality means that morphisms can pass through:



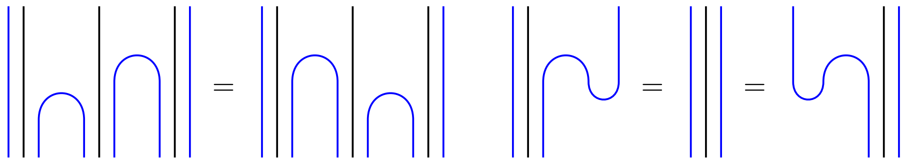

(3.16)

These are inverse to each other, yielding the following equations:




(3.17)

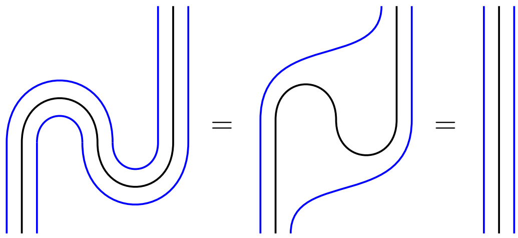
Finally, the coherence equations take the following form:



(3.18)

**Theorem 3.9.** *Monoidal functors preserve duals.*

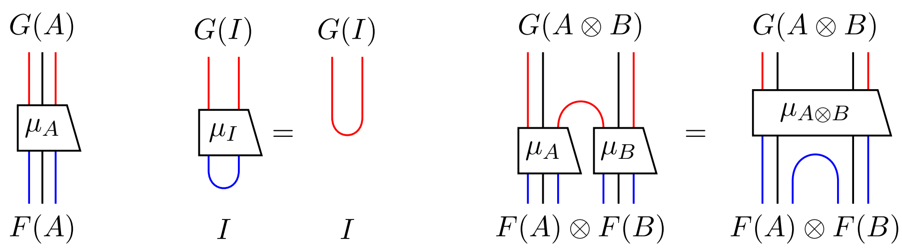
*Proof.* If we apply our monoidal functor to the unit and counit, we can show that the duality equations are still satisfied:



(3.19)

The other duality equation can be proved in a similar way. □

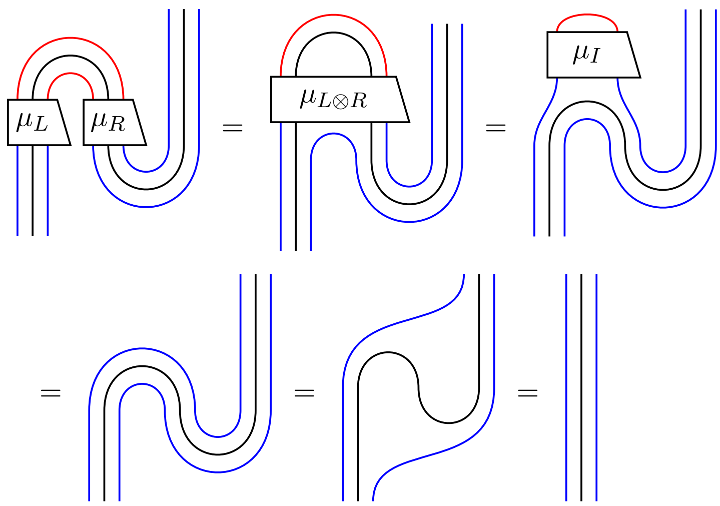
Given two monoidal functors $F, G : \mathbf{C} \to \mathbf{D}$ and a monoidal natural transformation $\mu\colon F \Longrightarrow G$, we can denote its properties like this:




(3.20)

**Theorem 3.10.** *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. Then if $A \in \mathrm{Ob}(\mathbf{C})$ has a left or a right dual, $F(A) \xrightarrow{\mu_A} G(A)$ is invertible.*

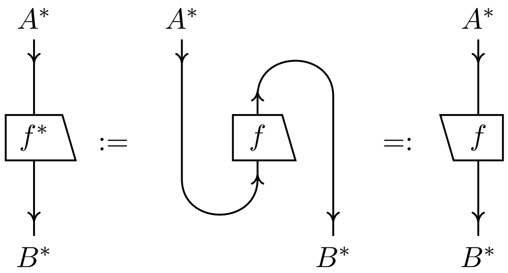
*Proof.* Choose $A = L$ with $L \dashv R$ in $\mathbf{C}$. Then we perform the following computation:



The rest of the proof uses similar techniques. □

Choosing duals for objects gives a strong structure that extends functorially to morphisms.

**Definition 3.11.** For a morphism $A \xrightarrow{f} B$ and chosen dualities $A \dashv A^*$, $B \dashv B^*$, the *right dual* $B^* \xrightarrow{f^*} A^*$ is defined in the following way:

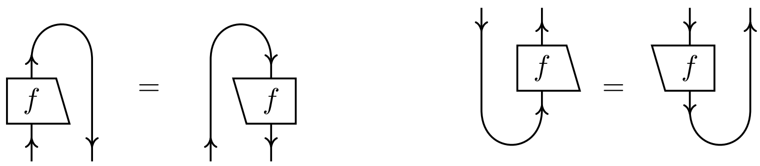



(3.21)

We represent this graphically by rotating the box representing $f$, as shown in the third image above.

The dual can 'slide' along the cups and the caps representing our dualities.

**Lemma 3.12.** *In a monoidal category with chosen dualities $A \dashv A^*$ and $B \dashv B^*$, the following equations hold for all morphisms $A \xrightarrow{f} B$:*

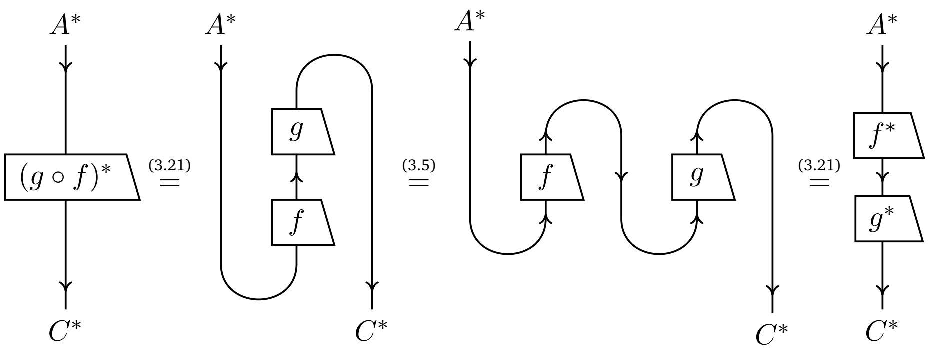



(3.22)

*Proof.* Direct from writing out the definitions of all the components involved. □

**Lemma 3.13.** *Let* **C** *be a monoidal category in which every object $X$ has a chosen right dual $X^*$. There exists a functor $(-)^*: \mathbf{C}^{op} \to \mathbf{C}$, called the* right-duals functor*, defined as $(X)^* = X^*$ on objects and as $(f)^* = f^*$ on morphisms.*

*Proof.* Let $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$. Then we perform the following calculation:



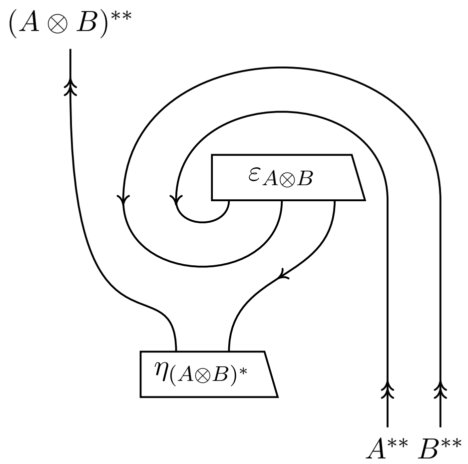

Similarly, $(\mathrm{id}_A)^* = \mathrm{id}_{A^*}$ follows directly from the snake equations. □

**Example 3.14.** Let's see how the right duals functor acts for our example categories, with chosen right duals as given by Example 3.2.

- In **FVect** and **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 **Rel**, the dual of a relation is its converse. So the right duals functor and the dagger functor have the same action: $R^* = R^\dagger$ for all relations $R$.

**Lemma 3.15.** *For a monoidal category with chosen right duals for objects, the double duals functor* $(-)^{**} : \mathbf{C} \to \mathbf{C}$ *is monoidal.*

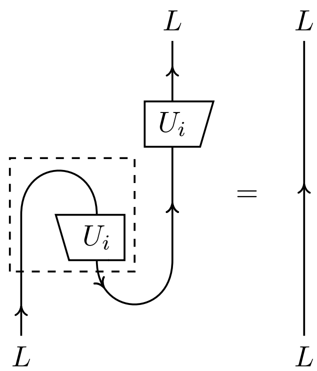
*Proof.* The isomorphism $A^{**} \otimes B^{**} \simeq (A \otimes B)^{**}$ looks like this:




Showing this satisfies the monoidal functor axioms is a big calculation! MAKE THIS AN EXERCISE. □

### 3.1.3 Abstract teleportation

The most fundamental procedure we will cover is abstract teleportation, which can be defined in any monoidal dagger category with duals. We will see that in **Hilb** it reduces to quantum teleportation, and in **Rel** it models classical encrypted communication.

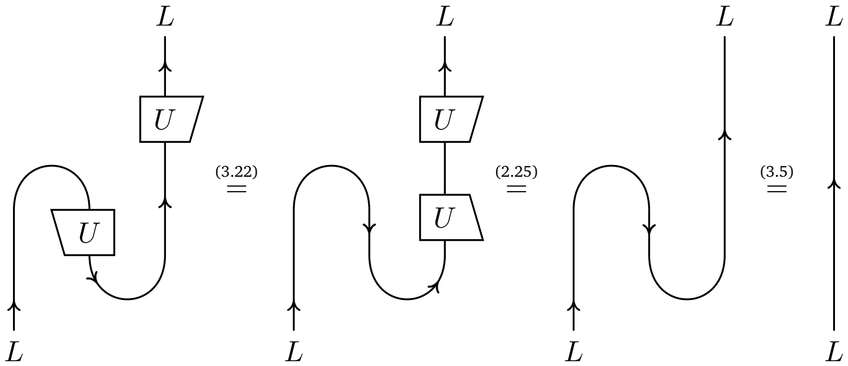



(3.23)

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 $\eta$, 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 $\varepsilon \circ (\mathrm{id}_L \otimes U_*)$.
4. Perform a unitary operation $U$ on the remaining system.

Ignoring the dashed box, we can use the graphical calculus to simplify the history:



(3.24)

By rotating the box $U$ along the path of the wire, using the unitary property of $U$, and then using a snake equation to straighten out the wire, we see the history equals the identity. So if the events described in (3.23) come to pass, then the result is for the original system to be transmitted unaltered.

For us to be sure that the state of the system is transmitted correctly, we require that the some history of this form necessarily takes place; that is, we requite the components in the dashed box in 3.23 to form a complete, disjoint set of effects, as discussed in Section 2.4.2.

**Example 3.16.** Let's instantiate abstract teleportation in our running example categories.

- We now consider implementing this abstract teleportation 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 $U_i$:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{3.25}$$

  The construction of (**??**) gives rise to the following family of effects:

$$\begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 & -1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & -1 & 0 \end{pmatrix} \tag{3.26}$$

  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 result is obtained at the measurement step. This scheme is precisely conventional qubit teleportation.

- We can also implement the abstract teleportation procedure in $\mathbf{Rel}$. For the simplest implementation, choose $L = R = 2 := \{0, 1\}$, and $\eta^\dagger = \varepsilon = \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}$. In $\mathbf{Rel}$ there are only two unitaries of type $2 \to 2$, as the unitaries are exactly the permutations (see Exercise 2.5.6):
$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{3.27}$$
Choose these as the family of unitaries $U_i$. This gives rise to the following family of effects:
$$\begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix} \tag{3.28}$$
These form a complete set of effects, since they partition the set. Thus we obtain a correct implementation of the abstract teleportation procedure. This procedure is usually known as *encrypted communication via a one-time pad*.

### 3.1.4 Interaction with linear structure

In the presence of duals for objects, the tensor structure interacts well with the linear structure, such as superposition rule, biproducts and zero objects. This indicates a fundamental relationship between the graphical calculus and linear structure, which is not yet completely understood.

We start by analyzing tensor products with zero objects and morphisms.

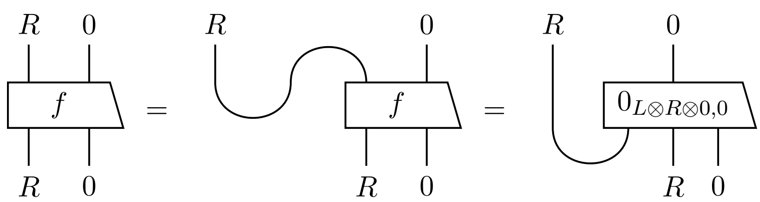
**Lemma 3.17.** *In a monoidal category with a zero object* $0$*:*

*(a)* $0 \dashv 0$*;*

*(b) if* $L \dashv R$*, then*
$$L \otimes 0 \simeq R \otimes 0 \simeq 0 \simeq 0 \otimes L \simeq 0 \otimes R. \tag{3.29}$$

*Proof.* Because $0 \otimes 0 \simeq 0$ by Lemma 2.27, 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 others inverse, showing that $R \otimes 0 \simeq 0$. The other claims follow similarly. □

**Corollary 3.18.** *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:*
$$f \otimes 0_{C,D} = 0_{A \otimes C, B \otimes D}, \tag{3.30}$$
$$0_{C,D} \otimes f = 0_{C \otimes A, D \otimes B}. \tag{3.31}$$

*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 3.17(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. □

The next lemma shows that tensor products distribute over biproducts on the level of objects, provided the necessary dual objects exist.

**Lemma 3.19.** *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:*

$$f = \begin{pmatrix} \mathrm{id}_A \otimes \begin{pmatrix} \mathrm{id}_B & 0_{C,B} \end{pmatrix} \\ \mathrm{id}_A \otimes \begin{pmatrix} 0_{B,C} & \mathrm{id}_C \end{pmatrix} \end{pmatrix}$$

$$A \otimes (B \oplus C) \underset{g}{\overset{f}{\rightleftarrows}} (A \otimes B) \oplus (A \otimes C)$$

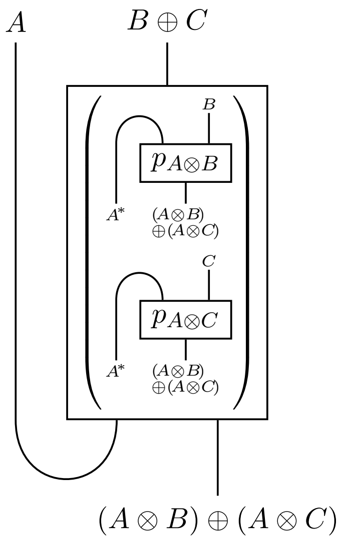
$$g = \begin{pmatrix} \mathrm{id}_A \otimes \begin{pmatrix} \mathrm{id}_B \\ 0_{B,C} \end{pmatrix} & \mathrm{id}_A \otimes \begin{pmatrix} 0_{C,B} \\ \mathrm{id}_C \end{pmatrix} \end{pmatrix}$$

*Proof.* To begin, we use Corollary 3.18 to perform the matrix computation

$$\begin{aligned} f \circ g &= \begin{pmatrix} \mathrm{id}_A \otimes (\mathrm{id}_B + 0_{B,B}) & \mathrm{id}_A \otimes (0_{C,B} + 0_{C,B}) \\ \mathrm{id}_A \otimes (0_{B,C} + 0_{B,C}) & \mathrm{id}_A \otimes (0_{C,C} + \mathrm{id}_C) \end{pmatrix} \\ &= \begin{pmatrix} \mathrm{id}_{A\otimes B} & 0_{A\otimes C, A\otimes B} \\ 0_{A\otimes B, A\otimes C} & \mathrm{id}_{A\otimes C} \end{pmatrix} = \mathrm{id}_{(A\otimes B)\oplus(A\otimes C)}. \end{aligned}$$

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 $f$. Supposing that ${}^*A \dashv A$, consider the following morphism:

$g' :=$




We have depicted it using a combination of the matrix calculus and the 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 can be shown 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 on the level of morphisms, as the following lemma shows.

**Lemma 3.20.** *In a monoidal category with biproducts and a zero object, 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:*

$$(f \otimes g) + (f \otimes h) = f \otimes (g + h) \tag{3.32}$$

$$(g \otimes f) + (h \otimes f) = (g + h) \otimes f \tag{3.33}$$

*Proof.* Compose the morphisms of Lemma 3.19 for $B = C$ to obtain the identity on $A \otimes (C \oplus C)$. Applying the interchange law shows that this identity equals

$$A \otimes (C \oplus C) \xrightarrow{\mathrm{id}_A \otimes \begin{pmatrix} \mathrm{id}_C & 0_{C,C} \\ 0_{C,C} & 0_{C,C} \end{pmatrix} + \mathrm{id}_A \otimes \begin{pmatrix} 0_{C,C} & 0_{C,C} \\ 0_{C,C} & \mathrm{id}_C \end{pmatrix}} A \otimes (C \oplus C). \tag{3.34}$$

Now, by further applications of the matrix calculus and the interchange law, we see that

$$f \otimes (g + h) = \big(\mathrm{id}_B \otimes \big(\mathrm{id}_D \quad \mathrm{id}_D\big)\big) \circ \left(f \otimes \begin{pmatrix} g & 0 \\ 0 & h \end{pmatrix}\right) \circ \left(\mathrm{id}_A \otimes \begin{pmatrix} \mathrm{id}_C \\ \mathrm{id}_C \end{pmatrix}\right). \tag{3.35}$$

Inserting the identity in the form of morphism (3.34), 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 (3.35), we show the following:

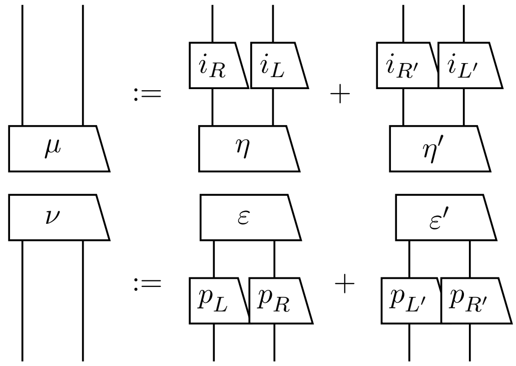
$$\begin{aligned} f \otimes (g + h) &= \big(\mathrm{id}_B \otimes \big(\mathrm{id}_D \quad \mathrm{id}_D\big)\big) \circ \left(f \otimes \begin{pmatrix} g & 0 \\ 0 & 0 \end{pmatrix} + f \otimes \begin{pmatrix} 0 & 0 \\ 0 & h \end{pmatrix}\right) \circ \left(\mathrm{id}_A \otimes \begin{pmatrix} \mathrm{id}_C \\ \mathrm{id}_C \end{pmatrix}\right) \\ &= f \otimes \left(\big(\mathrm{id}_D \quad \mathrm{id}_D\big) \circ \begin{pmatrix} g & 0 \\ 0 & 0 \end{pmatrix} \circ \begin{pmatrix} \mathrm{id}_C \\ \mathrm{id}_C \end{pmatrix}\right) + f \otimes \left(\big(\mathrm{id}_D \quad \mathrm{id}_D\big) \circ \begin{pmatrix} 0 & 0 \\ 0 & h \end{pmatrix} \circ \begin{pmatrix} \mathrm{id}_C \\ \mathrm{id}_C \end{pmatrix}\right) \\ &= (f \otimes g) + (f \otimes h) \end{aligned}$$

The equation $(g + h) \otimes f = (g \otimes f) + (h \otimes f)$ can be proved similarly. □

Finally, we show that taking biproducts preserves dual objects.

**Lemma 3.21.** *In a monoidal category with duals and biproducts, $L \dashv R$ and $L' \dashv R'$ imply $L \oplus L' \dashv R \oplus R'$.*

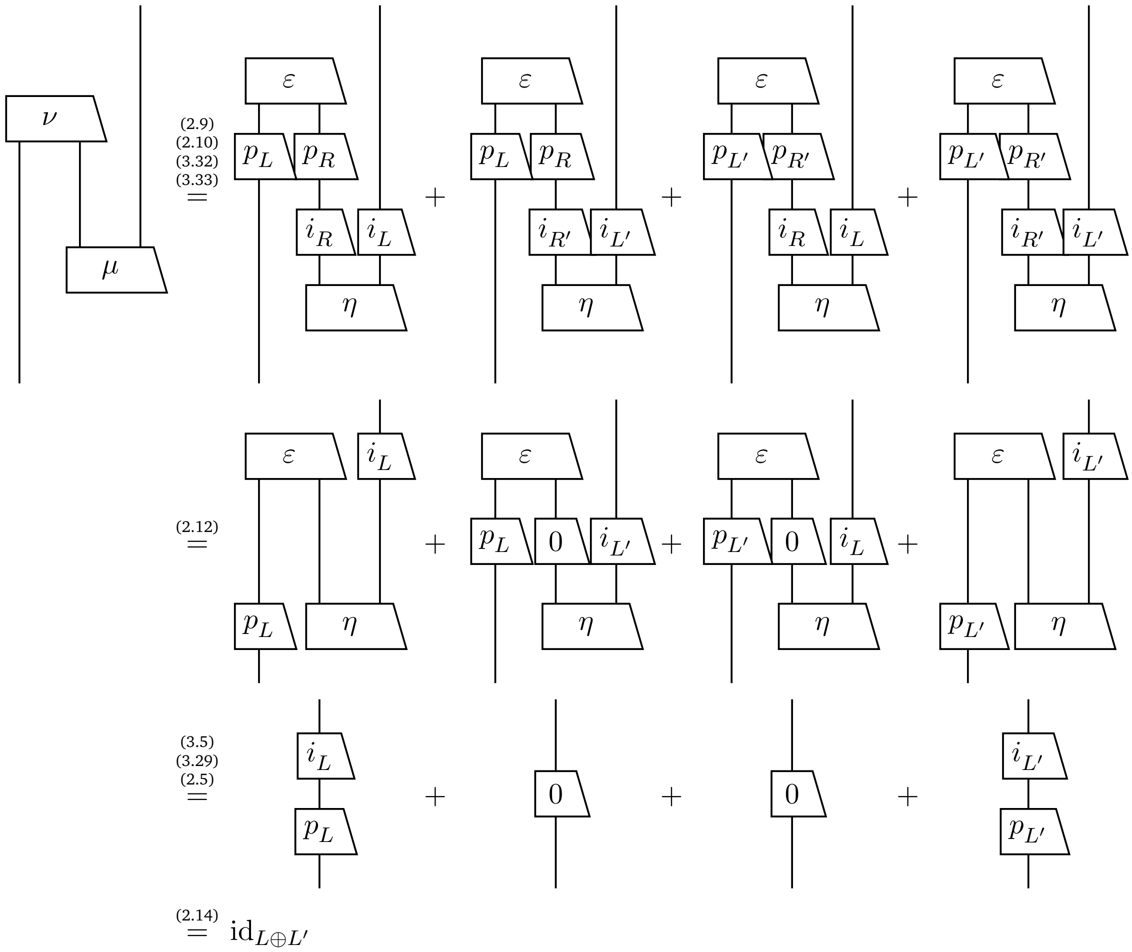
*Proof.* Let $I \xrightarrow{\eta} R \otimes L$, $L \otimes R \xrightarrow{\varepsilon} I$, $I \xrightarrow{\eta'} R' \otimes L'$ and $L' \otimes R' \xrightarrow{\varepsilon'} I$ be maps witnessing the dualities, and write $L \xrightarrow{i_L} L \oplus L'$, $L' \xrightarrow{i_{L'}} L \oplus L'$, $R \xrightarrow{i_R} R \oplus R'$ 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 $L \oplus L' \dashv R \oplus R'$:



(3.36)

(3.37)

The first snake equation (3.5) can then be established as follows:

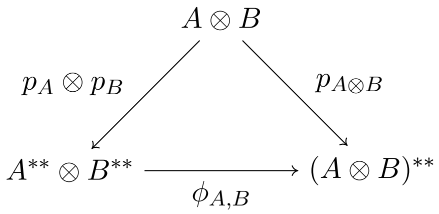


The second snake equation can be established with a similar argument. □

## 3.2 Pivotality

For a finite-dimensional vector space, there is an isomorphism $V^{**} \simeq V$. In this section we will see categorically why this map exists and is invertible, and investigate the strong extra properties it gives to the graphical calculus.

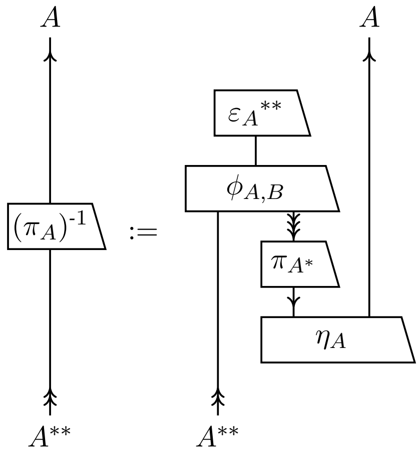
**Definition 3.22.** A monoidal category with right duals is *pivotal* when it is equipped with a monoidal natural transformation $A \xrightarrow{p_A} A^{**}$. Concretely, this means $p_A$ must satisfy the following equations, where $(A \otimes B)^{**} \xrightarrow{\phi_{A,B}} A^{**} \otimes B^{**}$ and $I^{**} \xrightarrow{\psi} I$ are the canonical isomorphisms arising from Lemma 3.6 and 3.7:




$$p_I = \psi \qquad (3.38)$$

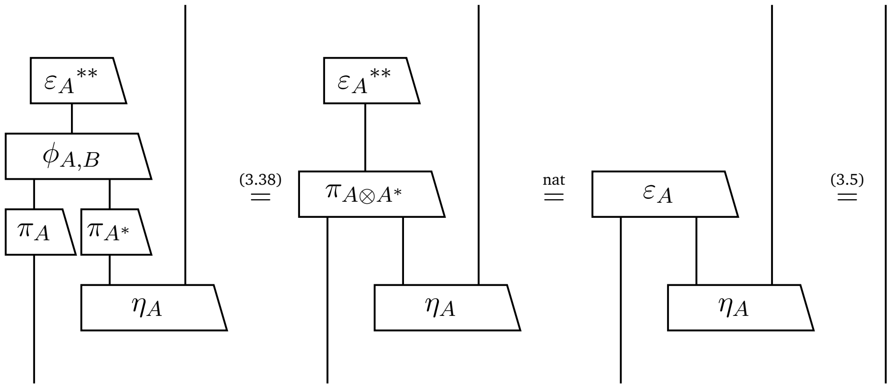
By Lemma 3.7 we have dualities $A \otimes B \dashv B^* \otimes A^* \dashv A^{**} \otimes B^{**}$. Thus by Lemma 3.4, we have $(A \otimes B)^{**} \simeq A^{**} \otimes B^{**}$.

**Lemma 3.23.** *In a pivotal category, the morphisms* $A \xrightarrow{\pi_A} A^{**}$ *are invertible, with inverses given as follows:*




(3.39)

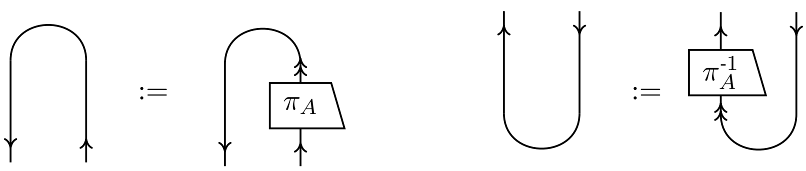
*Proof.* This follows from Theorem 3.10. We give the following explicit proof:




(3.40)

□

In the graphical calculus for a pivotal category, we make the following definitions:

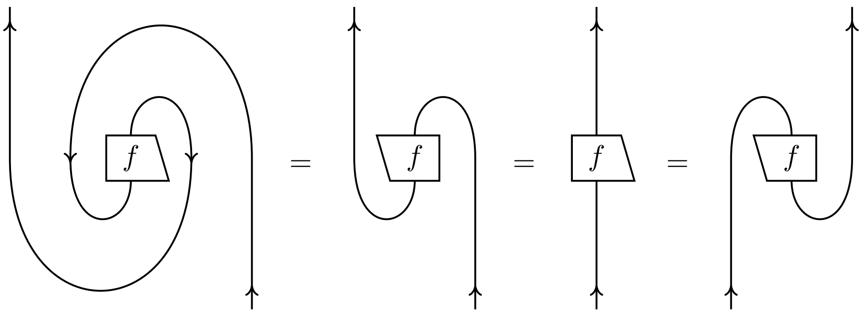



(3.41)

This allows us to extend the notation of (3.21) for rotated boxes to arbitrary rotations, giving us a powerful and natural graphical calculus.

**Theorem 3.24** (Correctness of the graphical calculus for pivotal categories)**.** *A well-formed equation between morphisms in a pivotal category 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:

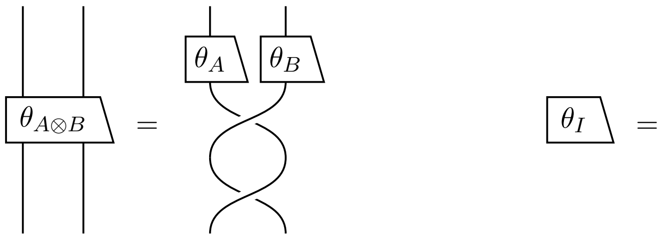



(3.42)

**Proposition 3.25.** *A pivotal monoidal category has left duals for all objects.*

*Proof.* WRITE OUT. □

**Definition 3.26** (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:

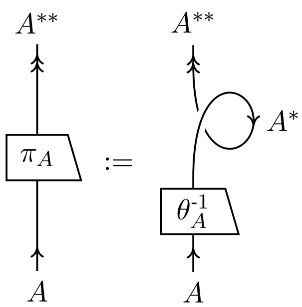



(3.43)

The second equation here says $\theta_I = \mathrm{id}_I$.

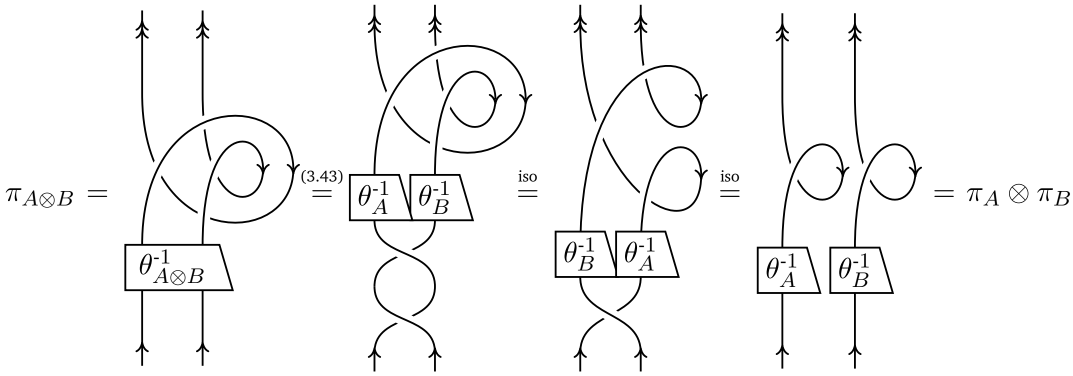
**Theorem 3.27.** *For a braided monoidal category with duals, any pivotal structure uniquely induces a twist structure, and vice versa.*

*Proof.* Suppose we have a twist structure $\theta_A : A \to A$. Then define a pivotal structure as follows:




(3.44)

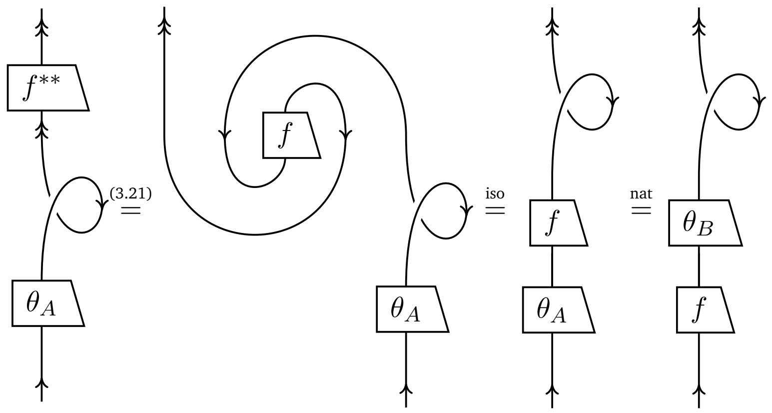
We must verify that it is a monoidal natural transformation, and that it is natural. For the monoidal property, perform the following calculation:



(3.45)

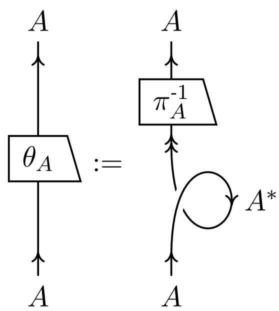
Here for simplicity we have suppressed the canonical isomorphism $(A \otimes B)^{**} \simeq A^{**} \otimes B^{**}$.

To check naturality, we give the following calculation for some $A \xrightarrow{f} B$:



(3.46)

Conversely, use a pivotal structure to define a balanced structure:



(3.47)

The balanced equations can then be demonstrated using the pivotality equations, with a similar calculation to the one given above. Clearly the constructions (3.44) and (3.47) are each other's inverse. □

### 3.2.1 Compact categories and ribbon categories

When a braided monoidal category with duals is symmetric, there is a canonical choice of balancing.

**Definition 3.28.** A *compact category* is a pivotal symmetric monoidal category with duals, equipped with the identity balancing $\theta_A = \mathrm{id}_A$.

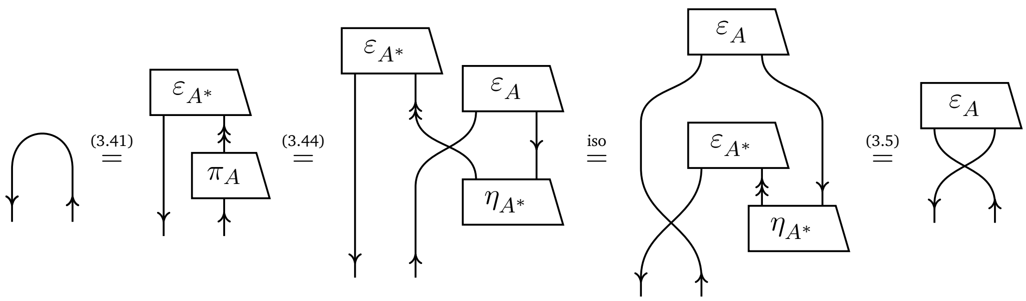
Our example categories **Hilb**, **Vect**, **Rel** and **Set** are all compact categories. Note that in general, other balancings may exist: that is, it is possible for a symmetric monoidal category with duals and a balancing *not* to be a compact category.

**Lemma 3.29.** **??***In a compact category, the following equations hold:*


(3.48)

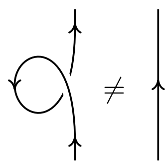

(3.49)

*Proof.* Let's prove the second equation of (3.48):



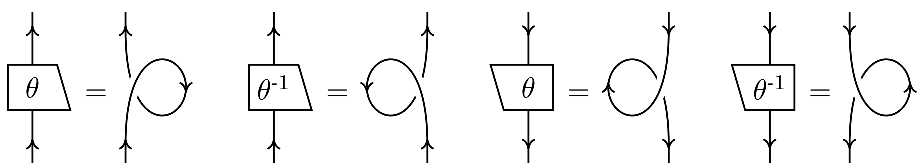

The others can be proved in a similar way. □

When using the graphical calculus for braided pivotal categories, we need to be careful with loops on a single strand. We might think that we can straighten out the loop to get the identity would follow from correctness of the graphical calculus for braided pivotal categories, see Theorem 3.35 below. But this isn't legal, because the correctness theorem only allows *planar* oriented isotopy, not spatial oriented isotopy:

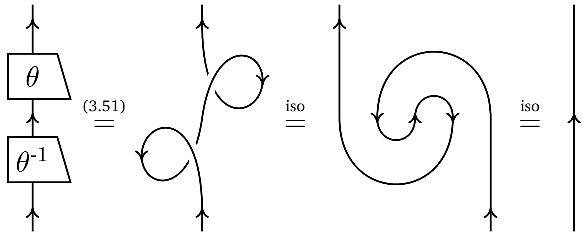

(3.50)

In fact, a loop on a single strand is directly related to the twist.

**Lemma 3.30.** *In a braided pivotal category, the following equations hold:*


(3.51)

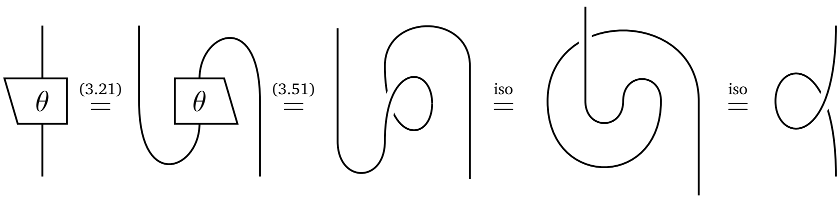
*Proof.* The first of these comes directly from equation (3.47) giving the twist in terms of the pivotal structure, using equations (3.41) defining the graphical calculus for a pivotal category. To verify the expression for $\theta^{-1}$:



(3.52)

The equation $\theta \circ \theta^{-1} = \mathrm{id}$ can be checked in a similar way. Since inverses in a category are unique (see Lemma 0.8), this proves that our expression for $\theta^{-1}$ is correct.

We demonstrate the graphical form of $\theta^*$ as follows:



(3.53)

The graphical form for $(\theta^{-1})^*$ can be demonstrated in a similar way. □

In a balanced monoidal category with duals, it is natural to ask the twist to be compatible with the duals in the following way.

**Definition 3.31.** A *ribbon* or *tortile* category is a balanced monoidal category with duals, such that $(\theta_A)^* = \theta_{A^*}$.

We can characterize the ribbon property nicely in terms of the graphical calculus.

**Lemma 3.32.** *A balanced monoidal category with duals is a ribbon category if and only if either of these equivalent equations are satisfied:*

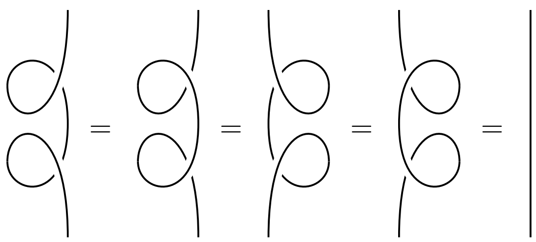

(3.54)

*Proof.* TO BE WRITTEN OUT. □

**Corollary 3.33.** *A compact category is a ribbon category.*

*Proof.* Equations (3.54) must hold thanks to Equation (3.49). □

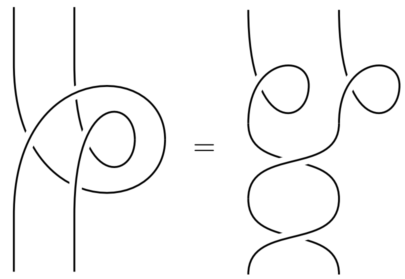
**Lemma 3.34.** *In a ribbon category, the following equations hold:*


(3.55)

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 3.35** (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 by cutting long, thin strips from a piece of paper. Use them to verify equations (3.54) and (3.55), and also the balancing equation (3.43) specialized to ribbon categories:

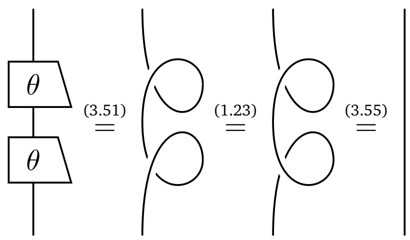


(3.56)

In a symmetric ribbon category, there is a strong constraint on the value of $\theta$. Remember that a symmetric ribbon category is not necessarily a compact category, which would have $\theta = \mathrm{id}$.

**Lemma 3.36.** *In a symmetric ribbon category,* $\theta^2 = \mathrm{id}$.

*Proof.* We prove this in the following way:




(3.57)

Intuitively, if a ribbon is allowed to pass through itself, a double twist can always be removed. □

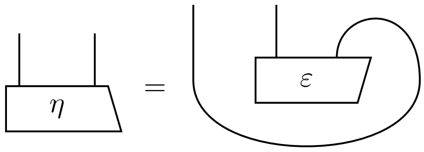
**Example 3.37.** Since they are symmetric monoidal categories with duals, our example categories $\mathbf{FHilb}$, $\mathbf{FVect}$, $\mathbf{Mat}_{\mathbb{C}}$ and $\mathbf{Rel}$ are all compact categories.

## 3.2.2 Dagger duality

**Lemma 3.38.** *In a monoidal dagger category,* $L \dashv R \Leftrightarrow R \dashv L$.

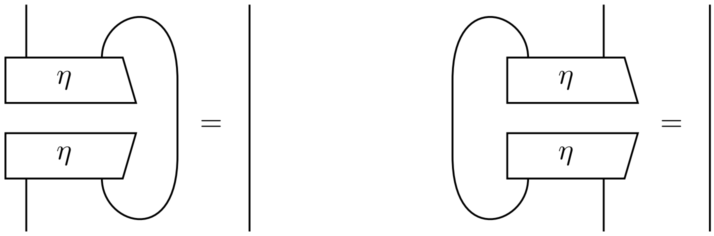
*Proof.* Follows directly from the axiom $(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger$ of a monoidal dagger category. □

**Definition 3.39.** 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 $A \otimes A^* \xrightarrow{\varepsilon} I$, satisfying the following condition:




(3.58)

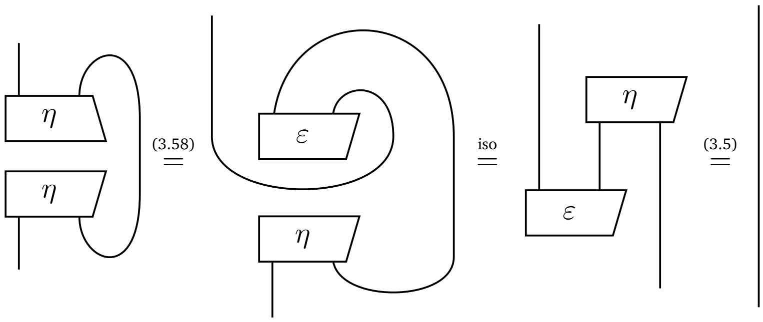
**Definition 3.40.** In a dagger category with a pivotal structure, a *maximally entangled state* is a bipartite state for which tracing out either system gives the identity:




(3.59)

**Lemma 3.41.** *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.* Using the dagger dual condition (3.58), we can verify the first equation of (3.59) in the following way:

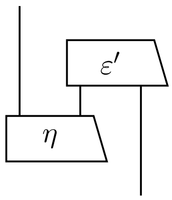



(3.60)

The other equation, and the reverse implication, can be proved in a similar way. □

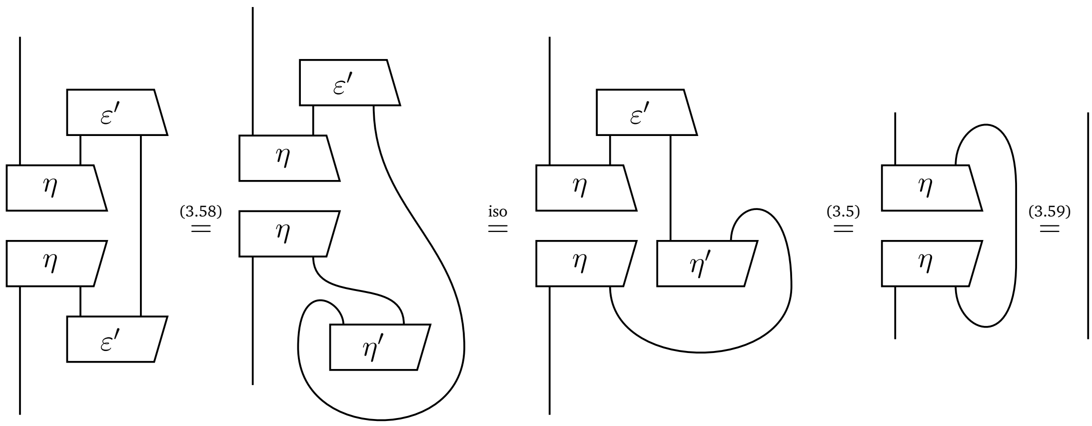
**Lemma 3.42.** *In a dagger category with a pivotal structure, dagger duals are unique up to unique unitary isomorphism.*

*Proof.* Given dagger duals $(L \vdash R, \eta, \varepsilon)$ and $(L \vdash R', \eta', \varepsilon')$, we construct an isomorphism $R \simeq R'$ as for Lemma 3.4 as follows:




(3.61)

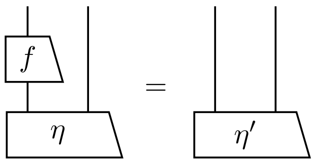
To establish the first part of the unitarity condition, we perform the following calculation:




The second part of unitarity can be proven similarly. Uniqueness is also straightforward to demonstrate. □

Putting the previous results together proves the following theorem about maximally-entangled states.

**Theorem 3.43.** *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 the following equation:*

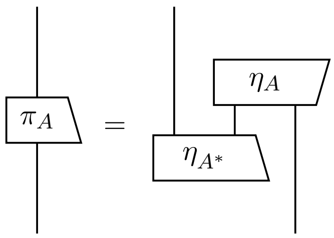



(3.62)

*Proof.* This follows from Lemmas 3.41 and 3.42. □

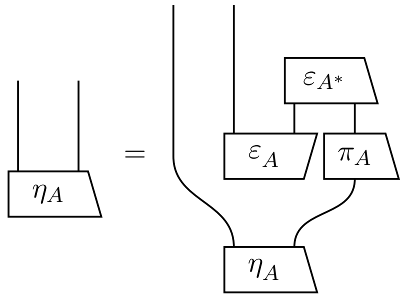
**Definition 3.44.** A *pivotal dagger category* is a dagger category with a pivotal structure, such that the chosen right duals are all dagger duals.

**Proposition 3.45.** *In a pivotal dagger category, the pivotal structure is given by the following composite:*



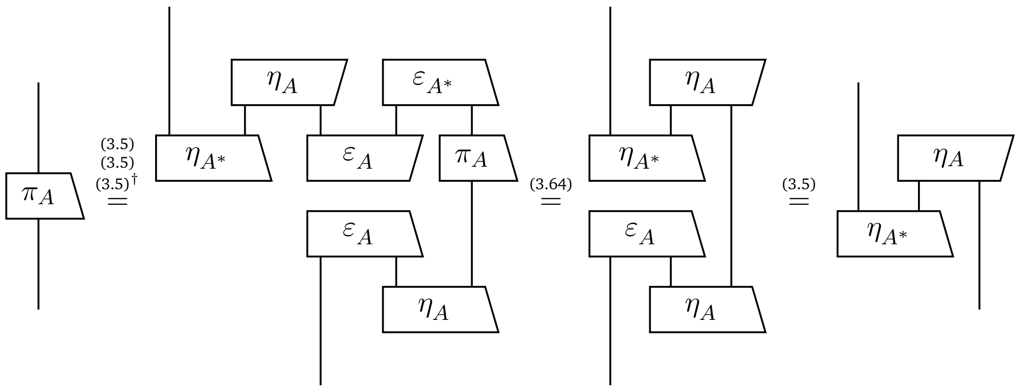

(3.63)

*Proof.* In explicit notation, the dagger duals property (3.58) takes the following form:



(3.64)

We can then do the following calculation:



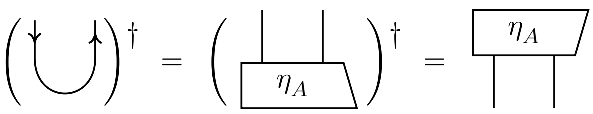
(3.65)

This completes the proof. □

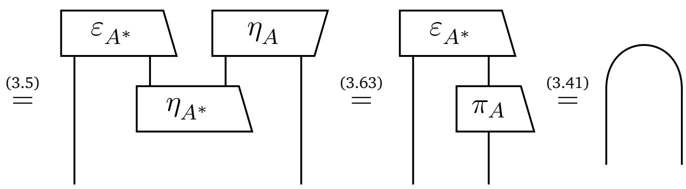
**Lemma 3.46.** *In a dagger pivotal category, the following equations hold:*

(3.66)

*Proof.* We prove the first of these in the following way:



(3.67)



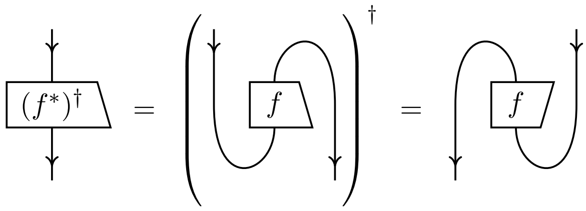
(3.68)

The second then follows by Lemma 3.5. □

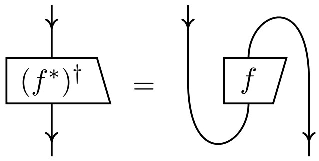
**Lemma 3.47.** *In a pivotal dagger category, every morphism $f$ satisfies the following equation:*

$$(f^*)^\dagger = (f^\dagger)^* \tag{3.69}$$

*Proof.* We compute both sides as follows:




(3.70)




(3.71)

These are isotopic, and hence equal by Theorem 3.35. □

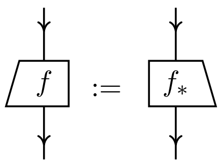
**Definition 3.48.** On a pivotal dagger category, *conjugation* $(-)_*$ is defined as the composite of the dagger functor and the right-duals functor:

$$(-)_* := (-)^{*\dagger} = (-)^{\dagger *} \tag{3.72}$$

Since taking daggers is the identity on objects we have $A_* := A^*$. Also, since $(-)^*$ and taking daggers are both contravariant, the conjugation functor is covariant.

Since taking daggers and the right-duals functor are both contravariant, conjugation is a covariant functor.

We denote conjugation graphically by flipping the morphism box about a vertical axis:




(3.73)

**Definition 3.49** (Ribbon dagger category, compact dagger category)**.** A *ribbon dagger category* is a braided pivotal dagger category with unitary braiding and twist.

A *compact dagger category* is a symmetric pivotal dagger category with unitary symmetry, and $\theta = \mathrm{id}$.

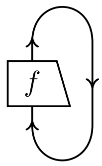
**Example 3.50.** Our example categories $\mathbf{FHilb}$, $\mathbf{Mat}_{\mathbb{C}}$ and $\mathbf{Rel}$ are all dagger compact closed.

- 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.

### 3.2.3 Traces and dimensions

Square matrices have an important construction, the trace, which plays a fundamental role in linear algebra. In this section we see how traces arise categorically in pivotal categories.

**Definition 3.51** (Trace)**.** In a pivotal category, the *trace* of a morphism $A \xrightarrow{f} A$, denoted $\mathrm{Tr}_A(f)$, is the following scalar:



(3.74)

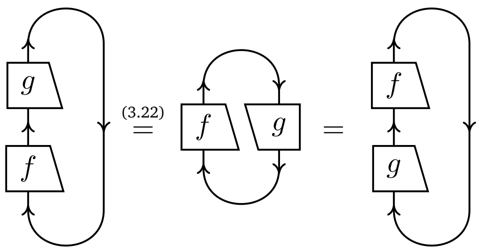
A trace can also be defined for a braided monoidal category, but we focus on the pivotal notion here; see Exercise 3.3.6 to investigate this.

**Definition 3.52.** In a pivotal category, the dimension of an object $A$ is the scalar $\dim(A) := \mathrm{Tr}_A(\mathrm{id}_A)$.

This abstract trace operation, like its concrete cousin from linear algebra, enjoys the familiar cyclic property.

**Lemma 3.53.** *In a pivotal category, morphisms $A \xrightarrow{f} B$ and $B \xrightarrow{g} A$ satisfy* $\mathrm{Tr}_A(g \circ f) = \mathrm{Tr}_B(f \circ g)$.

*Proof.* We can show this graphically in the following way:



(3.75)

The morphism $g$ slides around the circle, and ends up underneath the morphism $f$. □

**Example 3.54.** We now investigate the trace in our example categories.

- To determine $\mathrm{Tr}_H(f)$ for a morphism $H \xrightarrow{f} H$ in **FHilb**, substitute equations (3.7) and (3.6) into the definition of the abstract trace (3.74). Then $\mathrm{Tr}_H(f) = \sum_i \langle i|f|i\rangle$, 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 $\dim(H) = \mathrm{Tr}_H(\mathrm{id}_H)$ equals the usual dimension of $H$.
- For **Rel**, see Exercise 3.3.11.

Abstract traces satisfy many properties familiar from linear algebra.

**Lemma 3.55.** *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) $\mathrm{Tr}_I(s) = s$*;*

(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 3.20 and compatibility of addition with composition as in equation (2.9). For property (b), use the cyclic property of Lemma 3.53:

$$\begin{aligned}
&\mathrm{Tr}_{A\oplus B}\begin{pmatrix} f & g \\ h & j \end{pmatrix} \\
&= \mathrm{Tr}_{A\oplus B}(i_A \circ f \circ p_A) + \mathrm{Tr}_{A\oplus B}(i_A \circ g \circ p_B) + \mathrm{Tr}_{A\oplus B}(i_B \circ h \circ p_A) + \mathrm{Tr}_{A\oplus B}(i_B \circ j \circ p_B) \\
&= \mathrm{Tr}_A(f \circ p_A \circ i_A) + \mathrm{Tr}_A(g \circ p_B \circ i_A) + \mathrm{Tr}_B(h \circ p_A \circ i_B) + \mathrm{Tr}_B(j \circ p_B \circ i_B) \\
&= \mathrm{Tr}_A(f) + \mathrm{Tr}_B(j).
\end{aligned}$$

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 3.18, 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 3.56.** *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 3.55. Property (d) follows from the cyclic property of the trace demonstrated in Lemma 3.53: 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 3.57.** *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 3.56 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 $\mathbf{Rel}$, since we have $\mathrm{id}_1 + \mathrm{id}_1 = \mathrm{id}_1$ in that category. 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 $S \simeq S \cup 1$.

## 3.3 Exercises

**Exercise 3.3.1.** Recall the notion of local equivalence from Exercise 1.4.9. 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 $\phi$ is an entangled state if and only if $M_\phi$ 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 $f^{\mathrm{T}}$ 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 3.3.2.** 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 $\eta, \eta'$ 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 3.3.3.** Let $L \dashv R$ in $\mathbf{FVect}$, with unit $\eta$ and counit $\varepsilon$. 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 **FVect** is of the following *standard form* for a basis $\{l_i\}$ of $L$ and a basis $\{r_i\}$ of $R$:

$$\eta(1) = \sum_i r_i \otimes l_i, \qquad \varepsilon(l_i \otimes r_j) = \delta_{ij}. \tag{3.76}$$

**Exercise 3.3.4.** Let $L \dashv R$ be dagger dual objects in **FHilb**, with unit $\eta$ and counit $\varepsilon$.

(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 **FHilb** has the standard form (3.76) for *orthonormal* bases $\{l_i\}$ of $L$ and $\{r_i\}$ of $R$.

**Exercise 3.3.5.** Show that any duality $L \dashv R$ in **Rel** 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 **Rel** is the same as choosing an isomorphism $R \to L$, and that dual objects in **Rel** are automatically dagger dual objects.

**Exercise 3.3.6.** In a braided monoidal category, if $L \dashv R$, we can define a *braided trace* in the following way:

$$\mathrm{Tr}^{\beta}_A(f) \;:=\; \text{[BRAIDED TRACE PICTURE]} \tag{3.77}$$

Show that this has the following properties:

(a) Independent of the chosen duality $L \dashv R$

(b) EXPAND THIS QUESTION.

**Exercise 3.3.7.** Find some ribbons, or make some by cutting long, thin strips from a piece of paper. Use them to verify equations (3.54), (3.55) and (3.56).

**Exercise 3.3.8.** 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 3.3.9.** Show that in a monoidal category where all idempotents split, if there are morphisms $I \xrightarrow{\eta} R \otimes L$ and $L \otimes R \xrightarrow{\varepsilon} I$ satisfying the first snake equation (3.5), then $L$ has a right dual.

**Exercise 3.3.10.** Show that it's enough to use $\eta, \varepsilon$ in one snake equation, and $\eta, \varepsilon'$ in the other snake equation. It then follows that $\varepsilon = \varepsilon'$. WRITE THIS MORE CLEARLY.

**Exercise 3.3.11.** Show that the trace in **Rel** shows whether a relation has a fixed point.

**Exercise 3.3.12.** Let **C** be a compact dagger category.

(a) Show that $\mathrm{Tr}_A(f)$ 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 $\mathrm{Tr}_A(g \circ f)$ is positive when $A \xrightarrow{f,g} A$ are positive morphisms.

**Exercise 3.3.13.** Let $A \xrightarrow{f} A$ and $B \xrightarrow{g} B$ be morphisms in a braided monoidal category. 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 3.3.14.** Show that if $L \dashv R$ are dagger dual objects, then $\dim(L)^\dagger = \dim(R)$.

**Exercise 3.3.15.** In the category **Hilb**, define

$$H \odot K := \begin{cases} H & \text{if } \dim(K) = 0, \\ K & \text{if } \dim(H) = 0, \\ \mathbb{C} & \text{otherwise.} \end{cases}$$

Show that $(\mathbf{Hilb}, \odot, \mathbb{C})$ is a monoidal category, in which any object is its own dual. Conclude that Corollary 3.57 ("infinite-dimensional spaces cannot have duals") crucially depends on the monoidal structure.

**Exercise 3.3.16.** 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 **Rel**.

(b) Show that this is a compact dagger category under tensor product of vector spaces.

(c) Show that the scalars are the Boolean semiring.

**Exercise 3.3.17.** Let $\mathbf{D}$ be a dagger category in which every morphism is an isometry, and let $\mathbf{C}$ be any dagger compact category. Consider the category $\mathbf{C}^{\mathbf{D}}$, 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 $\mathbf{C}^{\mathbf{D}}$ is a dagger compact category.

**Exercise 3.3.18.** Suppose $\mathbf{C}$ and $\mathbf{D}$ are monoidal categories and $F \colon \mathbf{C} \to \mathbf{D}$ is a monoidal functor. Show that if $L \dashv R$ in $\mathbf{C}$, then $F(L) \dashv F(R)$ in $\mathbf{D}$.

# 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 [**?**]. They were subsequently studied first from the perspective of categorical algebra [**?**, **?**], and later in relation to linear logic [**?**, **?**]. Categories with duals and their graphical calculi were surveyed exhaustively by Selinger [**?**].

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 [**?**]. 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 [**?**]. Compact categories are also sometimes called compact closed categories, see Exercise 4.5.4. Dual objects forms an important ingredient in so-called modular tensor categories [**?**], which have received a lot of study because they model topological quantum computing [**?**].

Abstract traces in monoidal categories were introduced by Joyal, Street and Verity in 1996 [**?**]. Definition 3.51 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 [**?**]. 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 3.10 is due to Saavedra Rivano [**?**]. The link between abstract traces and traces of matrices was made explicit by Abramsky and Coecke in 2005 [**?**]. The use of compact categories in foundations of quantum mechanics was initiated in 2004 by Abramsky and Coecke [**?**]. This was the article that initiated the study of categorical quantum mechanics. The formulation in terms of daggers is due to Selinger in 2007 [**?**]. All of this builds on work on coherence for compact categories by Kelly and Laplaza [**?**].

# Chapter 4

# Monoids and comonoids

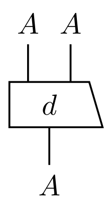
The tensor product of a monoidal category allows us to consider multiplications on its objects, leading to the notion of a monoid. In fact, this notion is so important, that one can almost say the entire reason for defining monoidal categories is that one can define monoids in them. This chapter investigates 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 a categorical no-deleting and no-cloning theorems in Sections 4.2.2 and 4.3, 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 4.4.

## 4.1 Monoids and comonoids

Let's start by making the notions of copying and deleting more precise in our setting of monoidal categories.

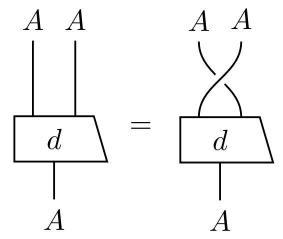
### 4.1.1 Comonoids

Clearly, copying should be an operation of type $A \xrightarrow{d} A \otimes A$. We draw it in the following way:




(4.1)

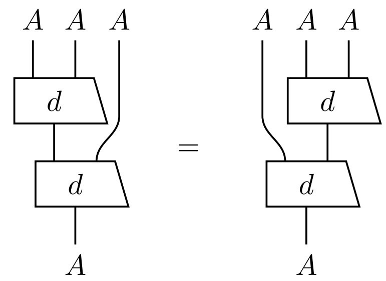
What does it mean that $d$ copies information? First, it shouldn't matter if we switch both output copies, corresponding to the requirement that $d = \sigma_{A,A} \circ d$:




(4.2)

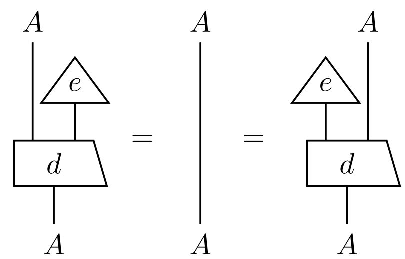
It doesn't matter which braiding we choose here, because this equation is equivalent to the one in which we choose the other braiding.

Secondly, if we make a third copy, if shouldn't matter if we make it from the first or the second copy. We can formulate this abstractly as $\alpha_{A,A,A} \circ (d \otimes \mathrm{id}_A) \circ d = (\mathrm{id}_A \otimes d) \circ d$, with the following graphical representation:




(4.3)

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 $\lambda_A \circ (e \otimes \mathrm{id}_A) \circ d$:




(4.4)

These three properties together constitute the structure of a *comonoid* on $A$.

**Definition 4.1** (Comonoid). A *comonoid* in a monoidal category is a triple $(A, d, e)$ of an object $A$ and morphisms $A \xrightarrow{d} A \otimes A$ and $A \xrightarrow{e} I$ satisfying equations (4.3) and (4.4). If the monoidal category is braided and equation (4.2) holds, the comonoid is called *cocommutative*.

The map $d$ is called the *comultiplication*, and $e$ is called the *counit*. Properties (4.3) and (4.4) are *coassociativity* and *counitality*.

**Example 4.2.** Here are some comonoids in our example monoidal categories.

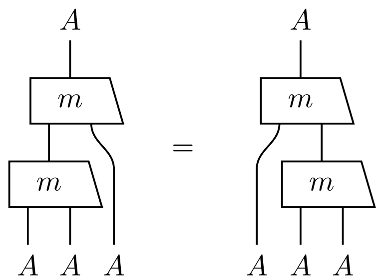
- In **Set**, the tensor product is in fact a Cartesian product. It therefore follows from counitality (4.4) that any object $A$ carries a unique cocommutative comonoid structure with comultiplication $A \xrightarrow{d} A \times A$ given by $d(a) = (a, a)$, and the unique function $A \to 1$ as counit.
- In **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 (4.4) 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 (4.2) is $g \sim (h^{-1}g, h)$ 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 $e_i \mapsto 1$.

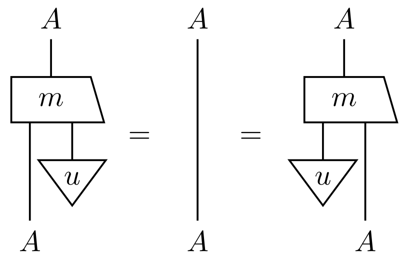
### 4.1.2 Monoids

Dualizing everything gives the more well-known notion of a *monoid*.

**Definition 4.3** (Monoid)**.** A *monoid* in a monoidal category is a triple $(A, m, u)$ of an object $A$, a morphism $A \otimes A \xrightarrow{m} A$, and a point $I \xrightarrow{u} A$, satisfying the following two equations called *associativity* and *unitality*:

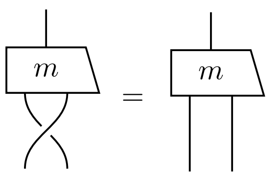



(4.5)




(4.6)

In a braided monoidal category, a monoid is called *commutative* when the following equation holds.




(4.7)

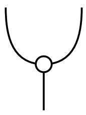
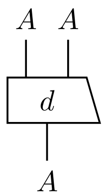
Again, the choice of braid is arbitrary here: this condition is equivalent to the one using the inverse braiding.

**Example 4.4.** There are many examples of monoids:

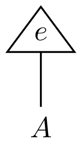
- The tensor unit $I$ in any monoidal category can be equipped with the structure of a monoid, with $m = \rho_I$ $(= \lambda_I)$ and $u = \mathrm{id}_I$.
- A monoid in **Set** gives the ordinary mathematical notion of a monoid. Any group is an example.
- A monoid in **Vect** is called an *algebra*. The 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 pointwise multiplication; 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.

### 4.1.3 Graphical calculus

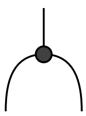
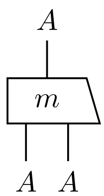
We will use a simpler graphical calculus for comultiplications, counits, multiplications and units. This is worth doing since we will be working with monoids and monoids so much.

 instead of 

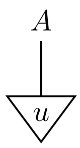
(4.8)

 instead of 

(4.9)

 instead of 

(4.10)

 instead of 

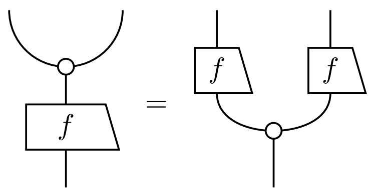
(4.11)

Here 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 $m = d^\dagger$ and $u = e^\dagger$, and in that case we will use the same colour dots for all of these structures.

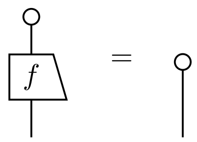
### 4.1.4 Combining monoids

A choice of bases $\{d_i\}$ and $\{e_j\}$ for finite-dimensional Hilbert spaces $H$ and $K$ makes them into comonoids as in Example 4.2. The functions $f\colon \{d_i\} \to \{e_j\}$ play a special role: they respect the comultiplication and counit. For example, in Chapter 5 we will in fact see that this equation characterizes functions between orthonormal bases completely. This is an example of a *comonoid homomorphism*. Given a monoidal category, we can build a new category whose objects are comonoids, and whose morphisms are comonoid homomorphisms.

**Definition 4.5.** 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 $e' \circ f = e$. These equations have the following graphical representations:




(4.12)




(4.13)

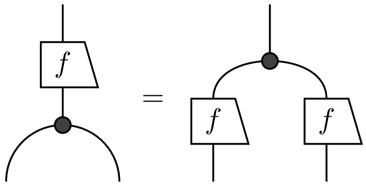
The visual impression is that the morphism $f$ is copied by $d'$, and deleted by $e'$. Comonoid homomorphisms compose associatively, and the identity morphism is always a comonoid homomorphism, so comonoids and comonoid homomorphisms form a valid category.

**Example 4.6.** Consider again the comonoids of Example 4.2.

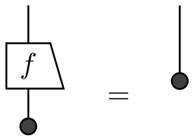
- In $\mathbf{Set}$, any function $f\colon A \to B$ is a comonoid homomorphism: by definition $(f \times f)(a, a) = \big(f(a), f(a)\big)$, and $A \xrightarrow{f} B \to I$ equals the unique function $A \to I$.
- In $\mathbf{Rel}$, any surjective homomorphism $f\colon G \to H$ of groups is a comonoid homomorphism. The left-hand side of (4.12) 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 (4.13) come down to the relation $1 \sim f(1) = 1$.
- In $\mathbf{FHilb}$, any function $f\colon \{d_i\} \to \{e_j\}$ between orthonormal 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 $e(f(d_j)) = 1 = e(d_j)$.

We can define a monoid homomorphism in a similar way.

**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 $u' = f \circ u$. These equations have the following graphical representations:




(4.14)




(4.15)

Again we can use this notion to form 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, as the following lemma shows.

**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:*

(4.16)

*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.

We can form the product of two monoids in a very similar way.

**Example 4.9.** Products of the comonoids of Example 4.2 are as follows.

- The product comonoid on sets $A$ and $B$ in **Set** is simply the unique comonoid on $A \times B$.
- The product comonoid of groups $G$ and $H$ in **Rel** is the comonoid of the product group $G \times H$ with multiplication $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$.
- The product of comonoids on Hilbert spaces $H$ and $K$ in **FHilb** 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.** *If* $(A, d, e)$ *is a comonoid in a monoidal dagger category, then* $(A, d^\dagger, e^\dagger)$ *is a monoid.*

*Proof.* Equations (4.5) and (4.6) are just (4.3) and (4.4) 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 $(g, h) \sim gh$.

# 4.2 Closure

This section considers higher-order features of compact categories. We introduce an important class of examples of monoids, and prove a no-deleting theorem for compact categories. To prepare for this, we first revisit names of morphisms.

## 4.2.1 Names and conames

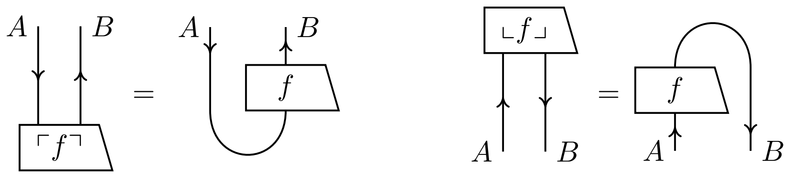
Up to now we have mostly considered objects and morphisms up to 'first order': we think of morphisms as a transformation of the *input* type into the *output* type. But sometimes we would like to talk about transformations of morphisms into morphisms. For example, when we have a superposition rule as in $\mathbf{FHilb}$, addition of matrices yields a new matrix.

Indeed, the monoidal category $\mathbf{FHilb}$ is able to handle 'higher order' morphisms. Namely, if $H$ and $K$ are finite-dimensional Hilbert spaces, then the set

$$\{H \xrightarrow{f} K \mid f \text{ linear}\} \tag{4.17}$$

is again a vector space, with pointwise operations such as $(f + g)(x) = f(x) + g(x)$. Moreover, the so-called *Hilbert–Schmidt inner product* or *trace inner product* $\langle f | g \rangle = \mathrm{Tr}(f^\dagger \circ g)$ makes it into a Hilbert space again. (In fact, this is the homset $\mathbf{FHilb}(H, K)$ itself!) Thus we can talk about transformations of morphisms as being just ordinary morphisms by encoding morphisms as vectors in function spaces. This is made precise in the definition of names and conames, that we repeat from Definition 3.3.

**Definition 4.11** (Name, coname)**.** The *name* of a morphism $A \xrightarrow{f} B$ in a compact category is the morphism $\ulcorner f \urcorner = (\mathrm{id}_{A^*} \otimes f) \circ \eta_A \colon I \to A^* \otimes B$. Its *coname* is the morphism $\llcorner f \lrcorner = \varepsilon_B \circ (f \otimes \mathrm{id}_{B^*}) \colon A \otimes B^* \to I$.



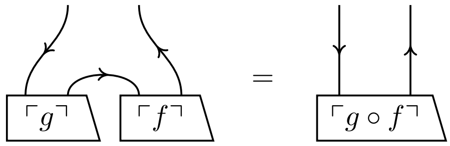

(4.18)

Hence we can think of an object $A$ in a compact category as an *output* type, and its dual $A^*$ as the corresponding *input* type. This is also called *map-state duality* or the *Choi-Jamiołkowski isomorphism*.

### 4.2.2 Monoids of operators

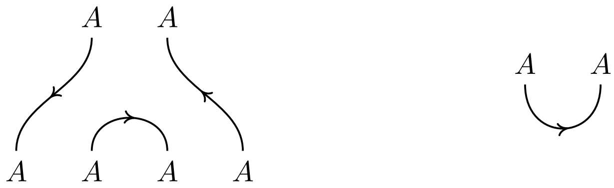
One of the most important features of matrices is that they can be multiplied. In other words, linear maps $\mathbb{C}^n \to \mathbb{C}^n$ can be composed. Using the closure properties of the previous subsection we can *internalize* this, to see that the vector space $\mathbb{M}_n$ of Example 4.4 is 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 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 $I \xrightarrow{\ulcorner g \circ f \urcorner} A^* \otimes A$:



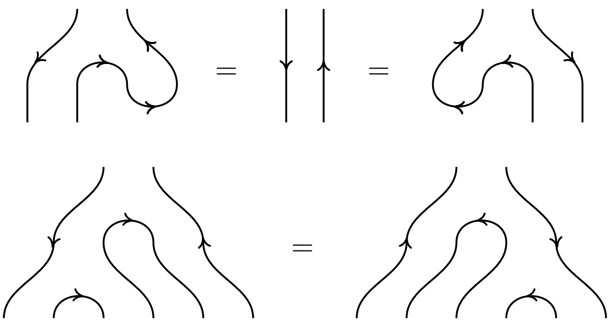

Thus the object $A^* \otimes A$ canonically becomes a monoid. We will call it the *pair of pants* monoid.

**Lemma 4.12.** *If $A \dashv A^*$ are dual objects in a monoidal category, then $A^* \otimes A$ is canonically a monoid. The multiplication and unit are given by:*




(4.19)

*Proof.* Straightforward graphical manipulation shows:

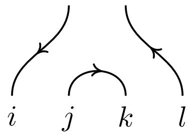



Hence this definition satisfies unitality and associativity. □

**Example 4.13.** The pair of paints algebra on the object $\mathbb{C}^n$ in the category **FHilb** 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.

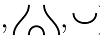
This is clearly a bijection. Furthermore, it respects multiplication; using the decorated notation from Section **??**:

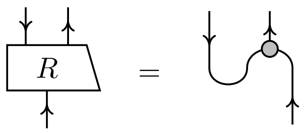



$$= \begin{bmatrix} \langle i| \otimes |l\rangle & \text{if } j = k, \\ 0 & \text{if } j \neq k \end{bmatrix} \quad \longmapsto \quad \begin{bmatrix} e_{il} & \text{if } j = k, \\ 0 & \text{if } j \neq k \end{bmatrix} = e_{ij}e_{kl}.$$

Similarly, it respects units, and is therefore a monoid homomorphism. □

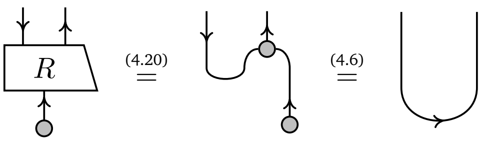
Pair of pants monoids are universal, in the sense that any monoid embeds into a pair of pants monoid. To explain this, think of Cayley's theorem: any group $G$ can be regarded as a subgroup of a symmetric one. A symmetric group $\mathrm{Sym}(A)$ consists of all bijections $A \to A$ on a set $A$, which form a group under composition. The embedding $R\colon G \to \mathrm{Sym}(G)$ is given by the *regular representation* $g \mapsto R_g$, where $R_g(h) = g \cdot h$. While originally stated for groups, this trick already works for monoids: any monoid $M$ is a submonoid of $\mathbf{Set}(M, M)$. By taking names and conames, we can move from an injective homomorphism $M \xrightarrow{R} \mathbf{Set}(M, M)$ to a relation $M \to M^* \times M$, where the latter carries the canonical pair of paints structure. The following proposition shows that this works abstractly, too.

**Proposition 4.14.** *Any monoid* ($A$, ) *in a monoidal category on an object with a dual* $A \dashv A^*$ *allows a monic monoid homomorphism* $R$ *into* ($A^* \otimes A$, ).

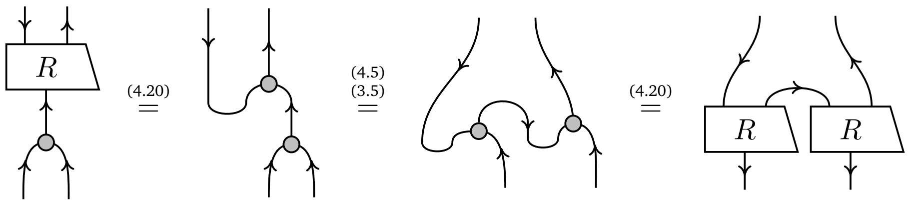



(4.20)

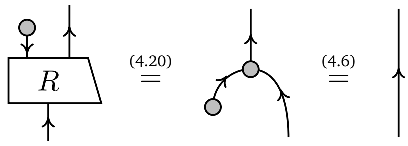
*Proof.* The morphism $R$ preserves units:




It also preserves multiplication:




where the middle equation uses associativity and the snake equation. Finally, $R$ has a left inverse:




It follows that $R$ is monic as required. □

### 4.2.3 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 of composition and tensor products. 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 4.15** (Uniform deleting). A monoidal category has *uniform deleting* if there is a natural transformation $A \xrightarrow{e_A} I$ with $e_I = \mathrm{id}_I$, making the following diagram commute for all objects $A$ and $B$:

$$\begin{array}{ccc} & A \otimes B & \\ {}^{e_A \otimes e_B} \swarrow & & \searrow {}^{e_{A\otimes B}} \\ I \otimes I & \xrightarrow[\lambda_I]{} & I \end{array} \tag{4.21}$$

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 4.16** (Preorder). A *preorder* is a category that has at most one morphism $A \to B$ for any pair of objects $A, B$.

From our viewpoint, preorders are degenerate categories; they are uninteresting, as there is only one way to process a system – there are no dynamics.

**Theorem 4.17** (No deleting). *If a compact category has uniform deleting, then it must be a preorder.*

*Proof.* Let $A \overset{f,g}{\longrightarrow} B$ be morphisms. Naturality of $e$ makes the following diagram commute.

$$\begin{array}{ccc} A \otimes B^* & \xrightarrow{e_{A\otimes B^*}} & I \\ {\scriptstyle \llcorner f \lrcorner} \downarrow & & \downarrow {\scriptstyle \mathrm{id}_I} \\ I & \xrightarrow{e_I} & I \end{array} \tag{4.22}$$

But because deleting is uniform, $e_I = \mathrm{id}_I$. So $\llcorner f \lrcorner = e_{A\otimes B^*}$, and similarly $\llcorner g \lrcorner = e_{A\otimes B^*}$. Hence $f = g$. □

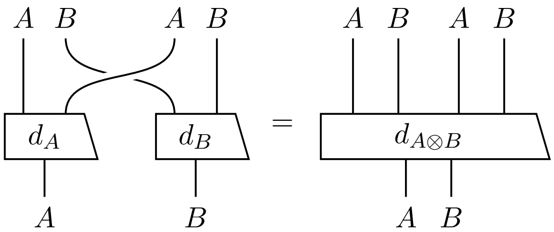
## 4.3 Cloning

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.

### 4.3.1 Uniform copying

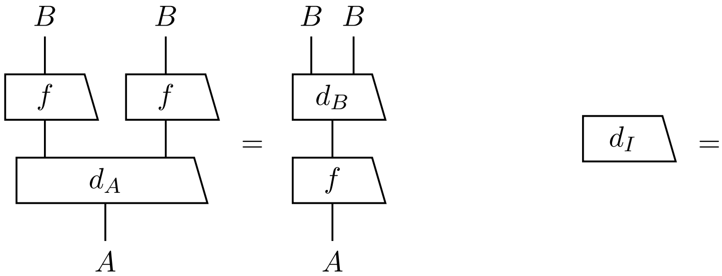
Uniform deleting meant deleting something straight away is the same as processing it for a while first and then deleting the result. We want a similar definition to say that a copying procedure is uniform. It shouldn't matter whether we copy something first and then process both copies, or process the 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 4.18** (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 (4.2) and (4.3), and making the following diagram commute for all objects $A, B$.




(4.23)

Naturality and $d_I = \rho_I^{-1}$ graphically look like this for arbitrary $A \xrightarrow{f} B$:

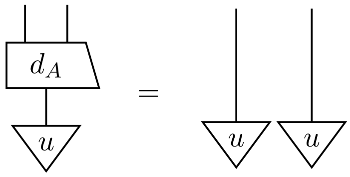



(4.24)

**Example 4.19.** 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 (4.23) are the function $A \times B \to A \times B \times A \times B$ given by $(a, b) \mapsto (a, b, a, b)$.

To justify calling the notion of Definition 4.18 copying, we now observe that it actually copies states.

**Definition 4.20** (Copyable state)**.** A state $I \xrightarrow{u} A$ of an object $A$ in a braided monoidal category with a copying map $A \xrightarrow{d_A} A \otimes A$ is *copyable* when:

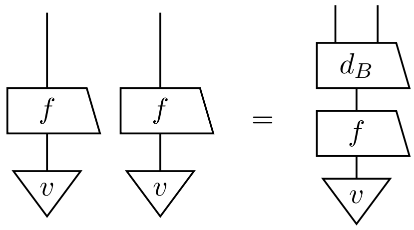



(4.25)

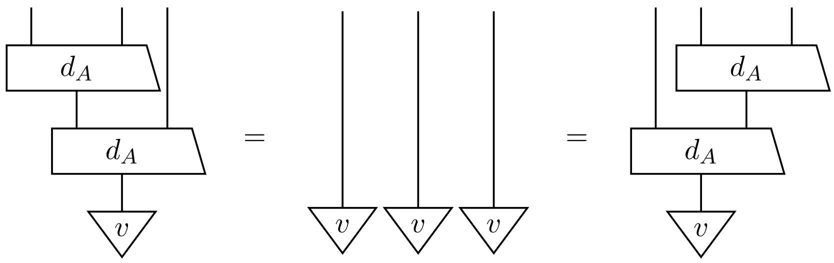
**Proposition 4.21.** *Consider a braided monoidal category equipped with maps $A \xrightarrow{d_A} A \otimes A$ for each object A. If the maps $d_A$ provide uniform copying, then any state is copyable. The converse holds when the category is monoidally well-pointed.*

*Proof.* If there is uniform copying, then, by naturality of the copying maps, we have $d_A \circ u = (u \otimes u) \circ \rho_I^{-1}$ for each state $I \xrightarrow{u} A$.

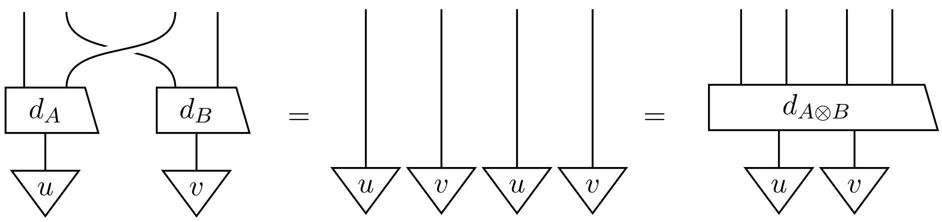
Now suppose the category is monoidally well-pointed and any state is copyable. In particular, the state $I \xrightarrow{\mathrm{id}_I} I$ is then copyable, which means $d_I = \rho_I^{-1}$. To see that $d_A$ is natural, let $I \xrightarrow{v} A$ be a state and $A \xrightarrow{f} B$ any morphism. By monoidal well-pointedness, it suffices to show that




But that is just copyability of the state $I \xrightarrow{f \circ v} B$. Associativity (4.5) and commutativity (4.7) similarly follow from well-pointedness. For example:




because any state $I \xrightarrow{v} A$ is copyable. Finally, we have to verify equation (4.23). This is where we need monoidal well-pointedness, rather than mere well-pointedness:




for all states $I \xrightarrow{u} A$ and $I \xrightarrow{v} B$. □

Hence our definition of uniform copying coincides with the usual one in monoidally well-pointed categories such as **Set**, **Rel**, and **Hilb**. Definition 4.18 is more general and makes sense for non-well-pointed categories, too.

### 4.3.2 Discrete and indiscrete categories

You might have expected Example 4.19: in classical physics, as modeled in $\mathbf{Set}$, you *can* uniformly copy states. The no-cloning theorem says something about quantum physics, which we have modeled by compact categories, which $\mathbf{Set}$ 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 up to scalars there is only one operator $A \to A$ on each object $A$. Let's investigate such categories.

**Definition 4.22** (Discrete category, indiscrete category)**.** A category is *discrete* when the only morphisms are identities. A category is *indiscrete* when there is a unique morphism $A \to B$ for each two objects $A$ and $B$. Such categories are completely determined by their set of objects.

Notice that discrete and indiscrete categories are automatically dagger categories, and in fact groupoids.

**Example 4.23.** Any group $(G, +, 0)$ gives rise to 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 $0 \in G$; the tensor product of objects is $g \otimes h = g + h$; the tensor product of morphisms is $\mathrm{id}_g \otimes \mathrm{id}_h = \mathrm{id}_{g+h}$. The monoidal category is symmetric precisely when the group $G$ is abelian. Every object $g$ in this category has a dual $-g$.

*Proof.* The associators are the identity morphisms $(g + h) + k = g + (h + k)$, and left and right unitors are the identity morphisms $0 + g = g = g + 0$; these are natural by construction. The pentagon and triangle equalities hold by construction. The cup is the identity morphism $0 = (-g) + g$, the cap is the identity morphism $g + (-g) = 0$. The snake equations hold by construction. □

The category of the previous example is discrete, and therefore cannot have uniform copying: unless $g = 0$ there is no morphism $g \to g + g$ at all. Rather than having no morphisms between different objects, we can also put a unique morphism between any two different objects, to make a group into a strict monoidal indiscrete category with duals. More generally, we may put any number of morphisms between two different objects, and still have a strict monoidal category with duals, as the following example shows.

**Example 4.24.** Any group $(G, +, 0)$ and commutative monoid $(M, \cdot, 1)$ give rise to a strict monoidal dagger category with duals:

- objects are $g \in G$;
- morphisms $g \to h$ are $m \in M$;
- taking daggers turns $g \xrightarrow{m} h$ into $h \xrightarrow{m} g$;
- composition of $g \xrightarrow{m} h$ and $h \xrightarrow{n} k$ is $g \xrightarrow{mn} k$;
- identities are $\mathrm{id}_g = 1$;
- tensor product of objects is $g \otimes h = g + h$;
- tensor product of morphisms $g \xrightarrow{m} h$ and $g' \xrightarrow{m'} h'$ is $g + g' \xrightarrow{mm'} h + h'$;

- the unit object is $0$;
- dual objects are $g^* = -g$.

If $G$ is abelian then the category is a compact dagger category.

*Proof.* Associators and unitors are as in Example 4.23; these are natural by construction. The triangle and pentagon equations also hold as before, but we have to verify functoriality of the tensor product. This comes down to $mnop = monp$ for all $m, n, o, p \in M$, which is satisfied by commutativity of $M$. Hence the category is strict monoidal.

Taking daggers is clearly contravariant and involutive, and the coherence isomorphisms are unitary, so we have a strict monoidal dagger category. The snake equations hold by construction.

If $G$ is abelian, the identity maps $g + h = h + g$ are natural by construction, and satisfy the hexagon equations, making for a compact dagger category. □

Note that the scalars in the previous example are given by the monoid $M$ itself.

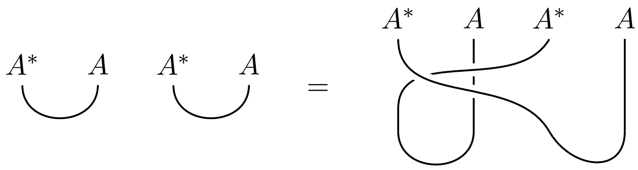
**Lemma 4.25.** *The category of Example 4.24 has uniform copying for abelian groups $G$ and monoids $M$ satisfying $m = m^2$ for all $m \in M$.*

*Proof.* Take the copying maps to be $d_g = 1\colon g \to g + g$. Clearly $d_0 = \rho_0$, and these maps are associative and commutative. Equation (4.23) holds by construction. Naturality comes down to idempotency $m = m^2$. □

### 4.3.3 No-cloning

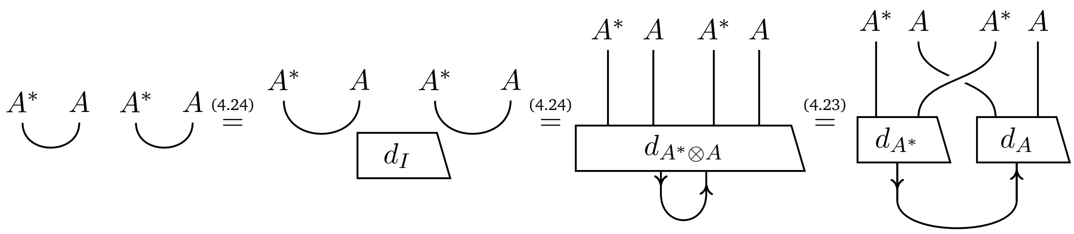
We are ready to prove our categorical no-cloning theorem, starting with a preparatory lemma.

**Lemma 4.26.** *If a braided monoidal category with duals has uniform copying, then*

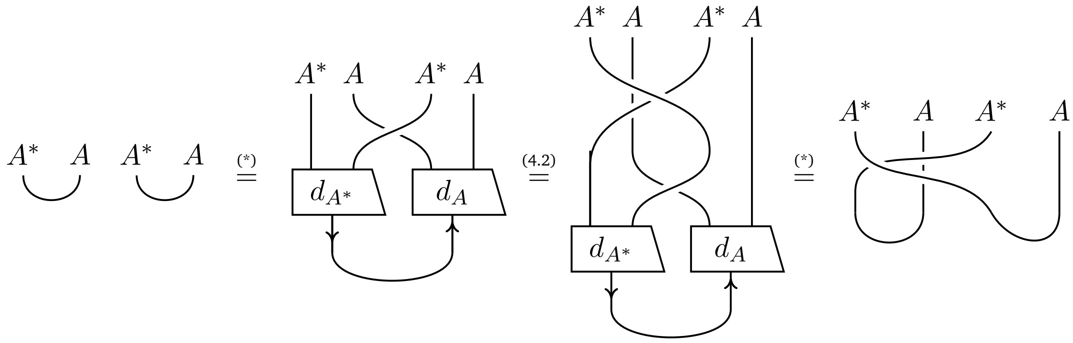



(4.26)

*Proof.* First, consider the following equalities.



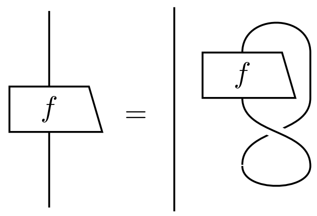
Let's temporarily call this equation $(*)$. Then:




This is precisely what we wanted to prove. □

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.

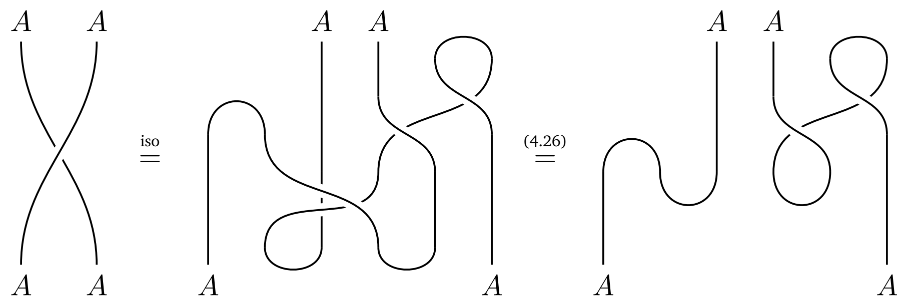
**Theorem 4.27** (No cloning)**.** *If a braided monoidal category with duals has uniform copying, then every endomorphism is a scalar multiple of the identity:*




(4.27)

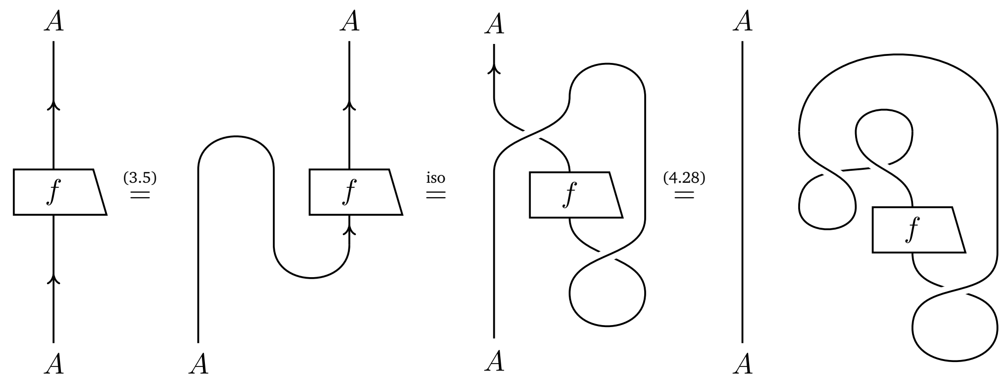
Notice that the scalar is the trace of $f$ as defined for braided monoidal categories in Exercise 3.3.6.

*Proof.* First, graphical manipulation shows:

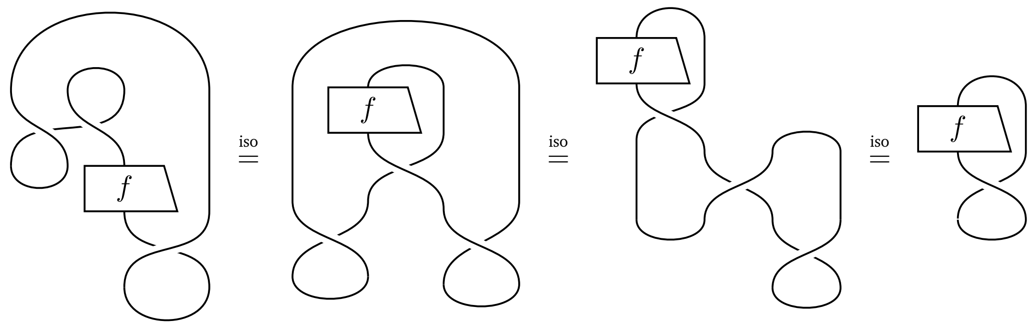



(4.28)

For any endomorphism $A \xrightarrow{f} A$ we now get:




The scalar on the right just evaluates to the trace:




This completes the proof. □

Thus, if a compact category has uniform copying, all endo-homsets are 1-dimensional, in the sense that they are in bijection with the scalars. Hence, in this sense, all objects are 1-dimensional, and the category degenerates.

The converse of the previous theorem does not hold: the category of Example 4.23 has 1-dimensional endo-homsets, and is braided monoidal with duals, but does not have uniform copying. Example 4.24 comes closer to characterizing compact categories with uniform copying; see also Exercise 4.5.7.

## 4.4 Products

Let's forget about duals for this section. What happens when a symmetric monoidal category has both uniform copying and deleting? When we phrase the latter property right, it turns out to imply that the tensor product is an actual categorical product.

### 4.4.1 Terminal objects

We first investigate uniform deleting further. As we saw in the no-deleting Theorem 4.17, for a compact category this capability means the category must be a preorder. In that case, if there is a morphism $A \to I$ at all, then it is the only one. This is intimately related to the tensor unit $I$ being a *terminal object*. Let us just repeat the definition.

**Definition 4.28.** An object $I$ is *terminal* when there is a unique morphism $A \to I$ for every object $A$.

We saw examples of terminal objects in 2.12: the zero objects of **Hilb** and **Rel**, and the singleton set in **Set**. For another example, let's temporarily go back to the compact case. The following lemma proves that, in that case, uniform deleting implies that $I$ is terminal. But in general, $I$ being terminal is strictly stronger than uniform deleting.

**Corollary 4.29.** *Let* $\mathbf{C}$ *be a monoidal category.*

- *If the tensor unit* $I$ *is terminal, then* $\mathbf{C}$ *has uniform deleting.*
- *If* $\mathbf{C}$ *is duals and uniform deleting, then its tensor unit* $I$ *is terminal.*

*Proof.* 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 equation (4.21). For the second part, notice that any object $A$ has at least one morphism $A \to I$, namely $e_A$. By the no-deleting theorem 4.17, this must be the only morphism of that type. □

## 4.4.2 Cartesian categories

Now we can make precise when tensor products are (categorical) products. We will clearly need uniform copying and deleting. Additionally, the copying and deleting operators have to form comonoids, and the tensor unit has to be terminal.

**Definition 4.30.** A category that has a terminal object and products for all pairs of objects is called *cartesian*.

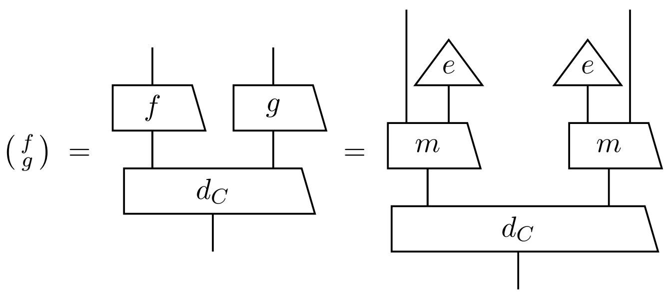
**Theorem 4.31.** *The following are equivalent for a symmetric monoidal category:*

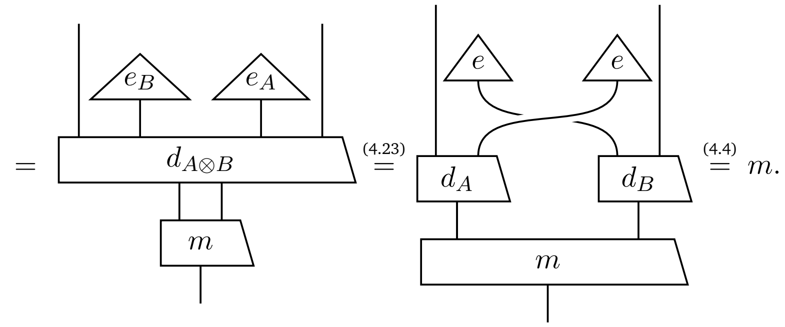
- *it is Cartesian: tensor products are products and the tensor unit is terminal;*
- *it has uniform copying and deleting,* $I$ *is terminal, and equation* (4.4) *holds.*

*Proof.* If the category is Cartesian, it is trivial to see that the unique morphism $A \xrightarrow{e_A} I$ and $d_A = \begin{pmatrix} \mathrm{id}_A \\ \mathrm{id}_A \end{pmatrix}$ provide uniform copying and deleting operators that moreover satisfy (4.4). Moreover, $I$ is by definition terminal.

For the converse, 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 $\left(\begin{smallmatrix} f \\ g \end{smallmatrix}\right) = (f \otimes g) \circ d$.

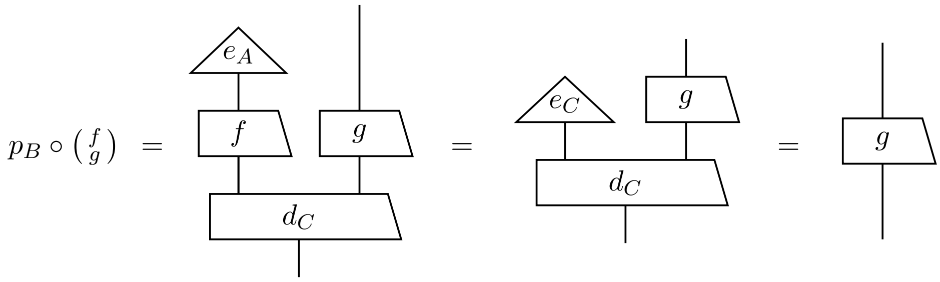
First, suppose $C \xrightarrow{m} A \otimes B$ satisfies $p_A \circ m = f$ and $p_B \circ m = g$. Then:






The second equality is our assumption, and 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 are all equal to $\binom{f}{g}$.

Finally, we show that $\binom{f}{g}$ indeed satisfies $p_A \circ \binom{f}{g} = f$ and $p_B \circ \binom{f}{g} = g$.




The first equality holds by definition, the second equality is naturality of $e$, and the last equality is equation (4.4). Similarly $p_A \circ \binom{f}{g} = f$. □

## 4.5 Exercises

**Exercise 4.5.1.** Let $(A, d, e)$ be a comonoid in a monoidal category. Show that a comonoid homomorphism $I \xrightarrow{a} A$ is 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 is a comonoid homomorphism.

**Exercise 4.5.2.** This exercise is about *property* versus *structure*; the latter is something you have to choose, the former is something that exists uniquely (or not).

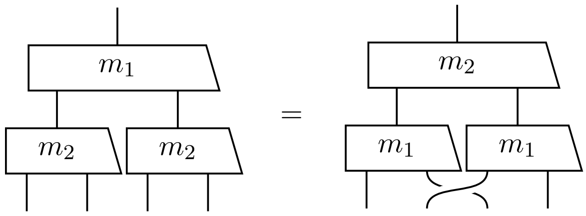
(a) Show that if a monoid $(A, m, u)$ in a monoidal category has a map $I \xrightarrow{u'} A$ satisfying $m \circ (\mathrm{id}_A \otimes u') = \rho_A$ and $\lambda_A = m \circ (u' \otimes \mathrm{id}_A)$, then $u' = u$. Conclude that unitality is a property.

(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) If $(\mathbf{C}, \otimes, I)$ is a symmetric monoidal category, 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 4.5.3.** This exercise is about the *Eckmann–Hilton argument*, concerning interacting monoid structures on a single object 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:

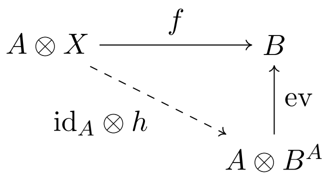



(a) Show that $u_1 = u_2$.

(b) Show that $m_1 = m_2$.

(c) Show that $m_1$ is commutative.

**Exercise 4.5.4.** Let $A$ and $B$ be objects in a symmetric monoidal category. Their *exponential* is an object $B^A$ together with a map $A \otimes B^A \xrightarrow{\text{ev}} B$ such that every morphism $A \otimes X \xrightarrow{f} B$ allows a unique morphism $X \xrightarrow{h} B^A$ with $f = \text{ev} \circ (\text{id}_A \otimes h)$.




The category is called *closed* when every pair of objects has an exponential. Show that any monoidal category in which every object has a left dual is closed.

**Exercise 4.5.5.** 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 objects 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 4.5.6.** A *semigroup* in a monoidal category is an object $A$ together with a morphism $A \otimes A \xrightarrow{m} A$ that satisfies the associative law (4.5). Recall from Exercise 1.4.12 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 4.5.7.** An *ideal* of a commutative monoid $(M, \cdot, 1)$ is a subset $I \subseteq M$ such that $nm \in I$ and $mn \in I$ for $n \in I$ and $m \in M$. Alter the category $\mathbf{C}$ of Example 4.24 as follows. Leave $\mathbf{C}(g, g) = M$, but for each $g \in G$, choose an ideal $I_g$ of $M$, in such a way that $I_{h-g} \cap I_{k-h} \subseteq I_{k-g}$. Set $\mathbf{C}(g, h) = I_{h-g}$.

(a) Show that the altered version is a well-defined monoidal subcategory of the original.

(b) Show that the altered version becomes a discrete category when we choose each $I_g = \emptyset$; compare Example 4.23.

(c) Show that if a commutative monoid $(M, \cdot, 1)$ satisfies $m = m^2$ for all $m \in M$, then $mn = 1$ implies $m = n = 1$.

(d) Show that if the altered version for an abelian group $G$ has uniform copying, then we have to choose each $I_g = M$, and so revert to the category of Example 4.24.

**Exercise 4.5.8.** 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, although a gap was filled by Jordan in 1870 [**?**].

The no-cloning theorem was proved in 1982 independently by Wootters and Zurek, and Dieks [**?**, **?**]. The categorical version we presented here is due to Abramsky in 2010 [**?**]. The no-deleting theorem we presented is due to Coecke and was also published in that paper.

Theorem 4.31 is 'folklore': it has long been known by category theorists, but seems never to have been published. Jacobs gave a logically oriented account in 1994 [**?**]. Terminal objects figure prominently in a categorical quantum mechanics approach to relativity [**?**]. It should be mentioned here that, in compact categories, products are automatically biproducts, which was proved by Houston in 2008 [**?**].

The notion of closure of monoidal categories from Exercise 4.5.4 is the starting point for a large area called *enriched* category theory [**?**]. It also plays an important role in categorical logic, where it encodes implications between logical formulae.

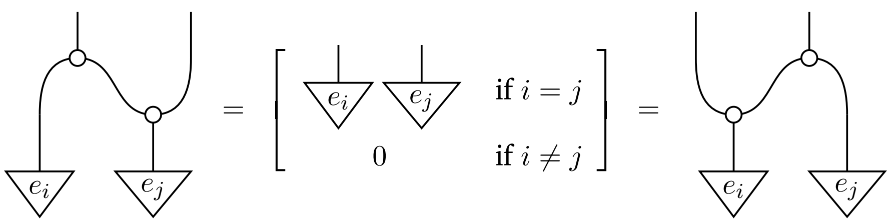
# Chapter 5

# Frobenius structures

In this chapter we deal with Frobenius structures: a monoid and a comonoid that interact according to the so-called Frobenius law. We will justify the Frobenius law in terms of coherence between taking daggers and closure of a compact category in Section 5.3, and study its basic consequences in Section 5.1. We classify all Frobenius structures in **FHilb** and **Rel** in Section 5.4: in the former they come down to operator algebras, in the latter they become groupoids. 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. It turns out that the graphical calculus is very satisfying for Frobenius structures, and we prove that any diagram built up from Frobenius structures is equal to one of a very simple normal form in Section 5.2. 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.

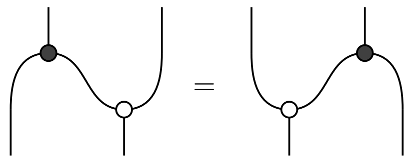
## 5.1 Frobenius structures

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 multiplication  is the comparison map given by $e_i \otimes e_i \mapsto e_i$ and $e_i \otimes e_j \mapsto 0$ for $i \neq j$. These copying and comparison maps cooperate in the following way:




This type of behaviour between a monoid and a comonoid is called the *Frobenius law*. In this commutative case it means that it doesn't matter whether we compare something with a copy or with the original. We now proceed straight away with the general definition, leaving its justification to 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)

We already saw that any choice of ortogonal 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 $z \mapsto z \cdot 1_G$. 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**:

$$\begin{aligned} &= \{((g,h), gh) \mid g, h \in G\} \colon G \times G \to G, \\ &= \{(\bullet, 1_G)\} \colon 1 \to G. \end{aligned} \tag{5.2}$$

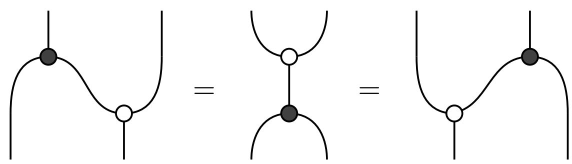
More generally, any *groupoid* $\mathbf{G}$ induces a Frobenius structure in **Rel** on the set $G$ of all morphisms in $\mathbf{G}$:

$$\begin{aligned} &= \{((g,f), g \circ f) \mid \mathrm{dom}(g) = \mathrm{cod}(f)\}, \\ &= \{(\bullet, \mathrm{id}_x) \mid x \in \mathrm{Ob}(\mathbf{G})\}. \end{aligned} \tag{5.3}$$

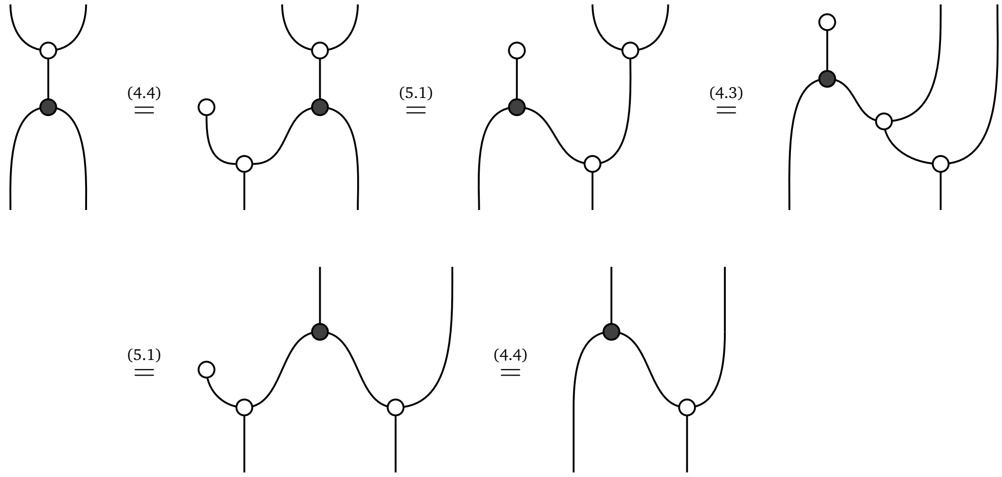
This gives a Frobenius structure, because both sides of the Frobenius law (5.1) evaluate to $(g, h) \sim (a, b \circ h)$ for all $a, b$ satisfying $g = a \circ b$ and $\mathrm{cod}(h) = \mathrm{dom}(b)$.

Frobenius structures automatically satisfy a further equality.

**Lemma 5.4.** *Any Frobenius structure satisfies the following equalities:*

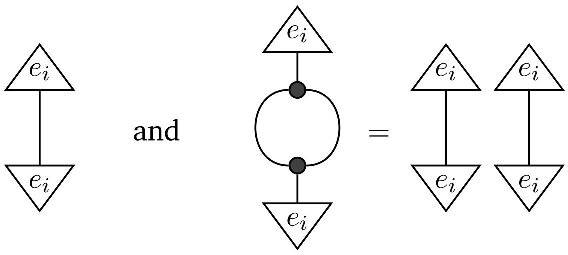

(5.4)

*Proof.* We prove one half graphically; the other then follows from the Frobenius law.



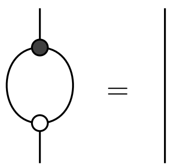

These equations use, respectively: counitality, the Frobenius law, coassociativity, the Frobenius law, and counitality. □

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 norm of $e_i$ and its square as:




Thus we can characterize when the basis is orthonormal in terms of the Frobenius structure as follows. Notice that this extra property is the other way in which a monoid and comonoid can interact than the Frobenius law.

**Definition 5.5.** In a monoidal category, a pair consisting of a monoid $(A,$ , $)$ and a comonoid $(A,$ , $)$ is *special* when  is a right inverse of :



(5.5)

**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 comultiplication is the dagger of the comultiplication. We will mostly be interested in this compatibility.

**Definition 5.7** (Dagger Frobenius structure)**.** A Frobenius structure $(A,$ , , , $)$ in a dagger monoidal category is *dagger Frobenius structure* when  $=$  and  $=$ .

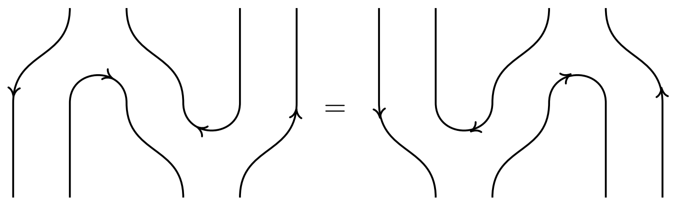
We call a Frobenius structure *commutative* when its monoid is commutative and its comonoid is cocommutative. For dagger Frobenius structures, this is equivalent to commutativity of the monoid.

**Example 5.8.** The Frobenius structure in **FHilb** induced by a choice of orthogonal basis is a (commutative) dagger Frobenius structure. So are the Frobenius structures from Examples 5.2 and 5.3.

The following lemma gives an example, and also explains the terminology.

**Lemma 5.9.** *If $A \dashv A^*$ are dagger dual objects in a dagger monoidal category, the pair of pants monoid of Lemma 4.12 is a dagger Frobenius structure.*

*Proof.* The comultiplication and counit are the upside-down versions of the multiplication and unit. The Frobenius law



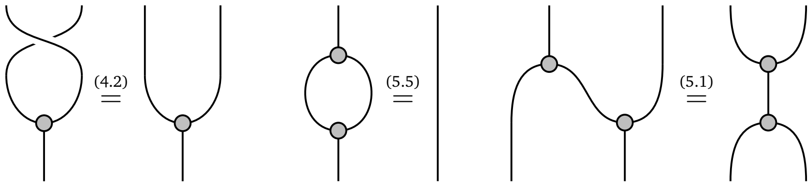
is readily verified. □

By Example 4.13, the algebra $\mathbb{M}_n$ of $n$-by-$n$ complex matrices is therefore a 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”, we think of this as a positive statement about *classical* objects (“you *can* copy their classical states”).

**Definition 5.10** (Classical structure)**.** A *classical structure* is a dagger Frobenius structure in a braided monoidal dagger category that is special and commutative.

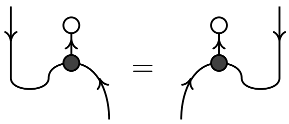
**Example 5.11.** The group algebra of Example 5.2 is a classical structure when the group is abelian. The groupoid Frobenius structure of Example 5.3 is a classical structure when the groupoid is *abelian*, in the sense that all morphisms are endomorphisms and $f \circ g = g \circ f$ for all endomorphisms $f, g$ of the same object. An abelian groupoid is essentially a list of abelian groups. Notice that abelian groupoid are skeletal.

There is quite some redundancy in the requirements we have put on classical structures. Because of cocommutativity (4.2), we only need to require one half of counitality (4.4) and one half of the Frobenius identity (5.4). In fact, we need not have mentioned (co)associativity, because it is implied by speciality (5.5) and the Frobenius law (5.1). Also, in the presence of dual objects, the Frobenius law (5.1) implies unitality (4.4). (See Exercise 5.7.2.) Hence to check that ($A$, , ) is a classical structure, we only need to verify the following properties:



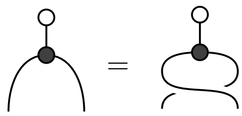

Notice that the pair of pants Frobenius structures from Lemma 5.9 are hardly ever commutative (by the no-cloning Theorem 4.27, unless $A \simeq I$). However, they do satisfy a similar property called *symmetry*.

**Definition 5.12** (Symmetric Frobenius structure)**.** A Frobenius structure in a monoidal category is *symmetric* when:



(5.6)

In a braided monoidal category, this is equivalent to:



(5.7)

**Example 5.13.** We have already seen examples of symmetric Frobenius structures:

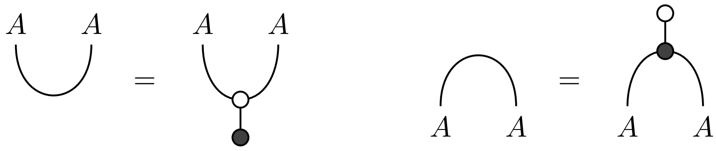
- Pair of pants algebras are always symmetric. In the category **FHilb** this comes down to the fact that the trace of matrices is cyclic: $\mathrm{Tr}(ab) = \mathrm{Tr}(ba)$.
- The group algebra of Example 5.2 is always symmetric. The left-hand side of (5.7) sends $g \otimes h$ to 1 if $gh = 1$ and 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 (5.7) 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 $h = g^{-1}$.

See Exercise 5.7.9 for an example of a Frobenius algebra that is not symmetric.

## 5.1.2 Self-duality and nondegenerate forms

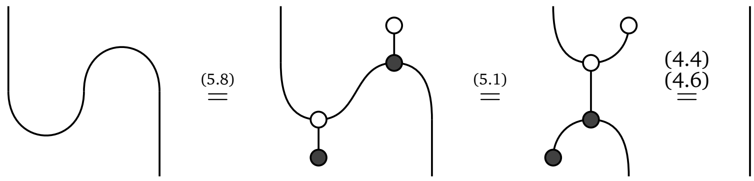
Let's now consider some properties of general Frobenius structures. First of all, they are closely related to dual objects.

**Theorem 5.14** (Frobenius structures have duals)**.** *If an object $A$ in a monoidal category carries a Frobenius structure $(A, \ , \ , \ , \ )$, then $A \dashv A$ is self-dual (in the sense of Definition 3.1) with the following cap and cup:*




(5.8)

*Proof.* We prove the first snake equation (3.5) using the definitions of the cups and caps, the Frobenius law, and unitality and counitality:

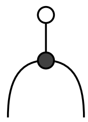


The other snake equation is proved similarly. □

It follows from the previous theorem that, if we would choose a dagger Frobenius structure on every object in a given monoidal category, then that category would have duals. However, by the collapse theorems of Chapter 4, we cannot hope to choose this Frobenius structure in a uniform way. But we can use this contrapositively, which motivates Definition 5.10 once more, coming full circle from Chapter 4.

The converse to the previous theorem can be used to characterize Frobenius structures, as in the following lemma.

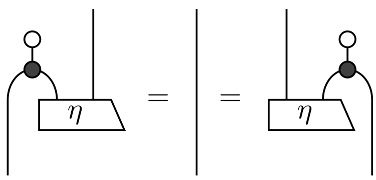
**Proposition 5.15** (Frobenius structures by non-degenerate form)**.** *In a monoidal category, a monoid $(A, \ , \ )$ forms a Frobenius structure with a comonoid $(A, \ , \ )$ if and only if it allows a* nondegenerate form*, a map* $\ \colon A \to I$ *making the composite*



(5.9)

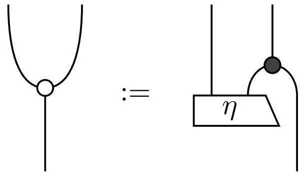
*part of a self-duality $A \dashv A$.*

*Proof.* One direction follows immediately from Theorem 5.14, by taking the counit for the nondegenerate form. 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:



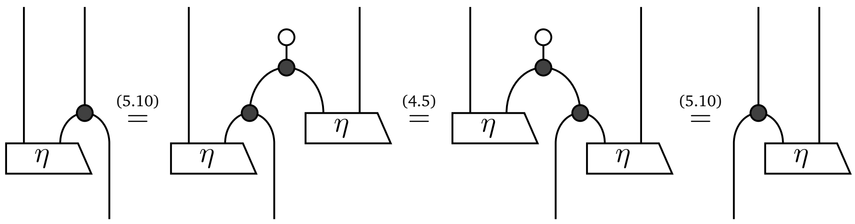

(5.10)

Use the map $\eta$ to define a comultiplication in the following way:




(5.11)

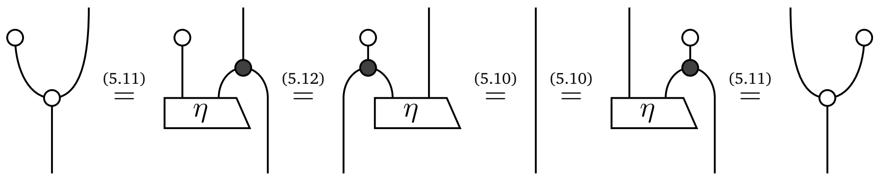
The following computation shows that we could have defined the comultiplication with the $\eta$ on the left or the right, using the nondegeneracy property, associativity, and the nondegeneracy property again:



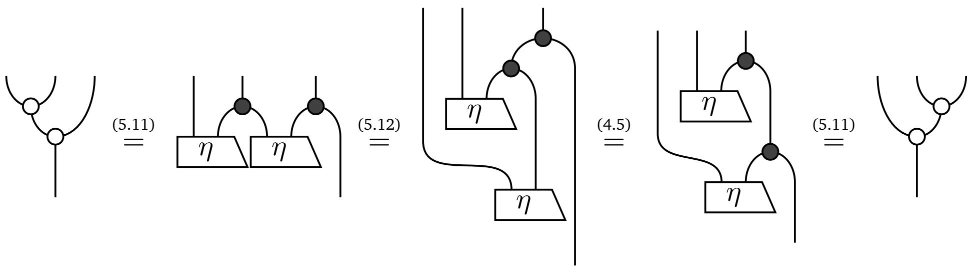

(5.12)

We must show that our new comultiplication satisfies coassociativity and counitality, and the Frobenius law (5.1). For the counit, choose the nondegenerate form.

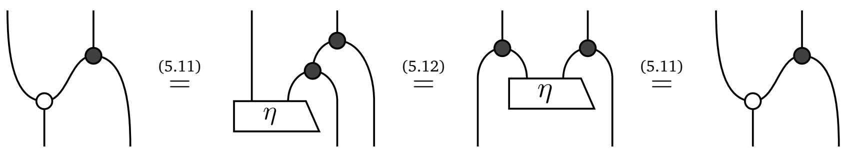
Counitality is the easiest property to demonstrate, using the definition of the comultiplication, symmetry of the comultiplication, nondegeneracy twice, and definition of the comultiplication:




To see coassociativity, we 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:

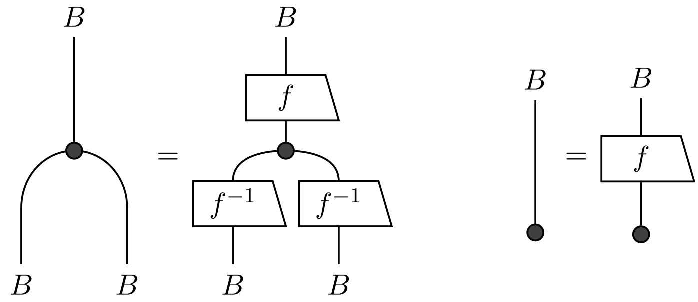



This completes the proof. □

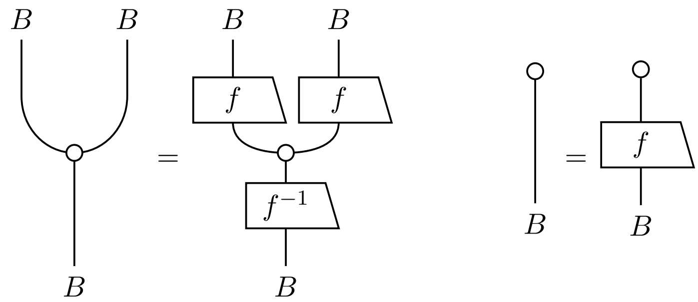
### 5.1.3 Homomorphisms

We now investigate properties of a map that preserves Frobenius structure.

**Lemma 5.16** (Frobenius algebras transport across isomorphisms)**.** *Let*  *be a Frobenius structure in a monoidal category, and* $A \xrightarrow{f} B$ *an isomorphism. The following furnishes* $B$ *with Frobenius structure:*




(5.13)




(5.14)

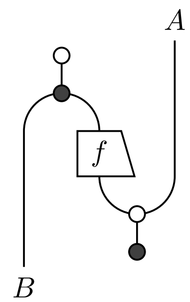
This Frobenius structure is called the *transport* across $f$ of the given one.

*Proof.* Straightforward graphical manipulation. □

**Definition 5.17.** A *homomorphism of Frobenius structures* is a morphism that is simultaneously a monoid homomorphism and a comonoid homomorphism.

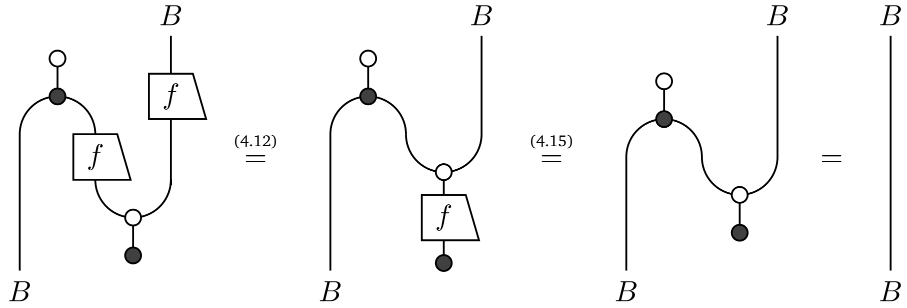
**Lemma 5.18.** *In a monoidal category, a homomorphism of Frobenius structures is invertible, and the inverse is again a homomorphism of Frobenius structures.*

*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:



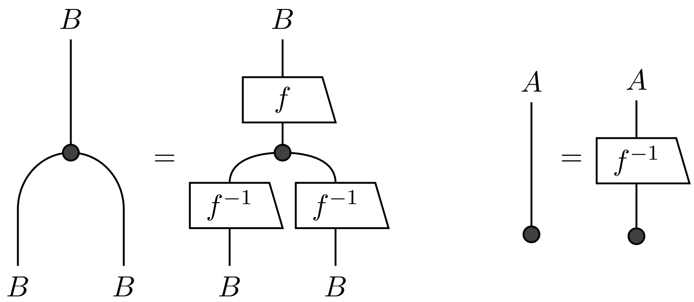

(5.15)

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 5.14. The other composite equals the identity by a similar argument.

Substituting (5.15) and straightforward graphical manipulation shows that:

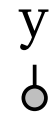



It now follows from Lemma 5.16 that $f^{-1}$ is again a homomorphism of Frobenius algebras. $\square$

## 5.2 Normal forms

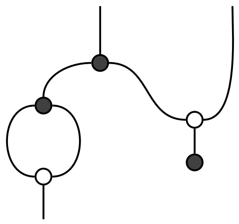
In general there are two ways to think about the graphical calculus:

- a diagram represents a morphism: it is just a shorthand to write down a linear map, for example, in the category **FHilb**;
- a diagram is an entity in its own right: it can be manipulated by replacing a part by an equal diagram.

The first viewpoint doesn't care that many different diagrams represent the same morphism. The second viewpoint takes different representation diagrams seriously, giving a combinatorial or graph theoretic flavour. A *normal form* theorem connects the two, by proving that all diagrams representing a fixed morphism can be rewritten into a canonical diagram called the normal form. This should remind you of the Coherence Theorem 1.2. As you might expect, there are only so many ways you can comultiply (using ), discard (using ), fuse (using ) and create (using ) information. In fact, there is only one! We will give two different proofs: one for general Frobenius structures, and one for commutative ones.

### 5.2.1 Normal forms for Frobenius structures

We start by viewing a morphism as a combinatorial entity, and use discrete mathematics to count and manipulate its pieces. Consider any morphism $A^{\otimes m} \to A^{\otimes n}$ built out of the ingredients of a Frobenius structure $(A, \mu, \eta, \delta, \epsilon)$ in a monoidal category. For example, in the graphical calculus:



We can think of it as a graph: the wires are edges, and each $\circ$ or $\bullet$ is a vertex, as is the end of each input or output wire. The example above furthermore has 1 enclosed region. We say such a morphism is *connected* when it has a graphical representation in which there is a path from any input wire to any output wire. By convention, scalars $A^{\otimes 0} \to A^{\otimes 0}$, *i.e.* those morphisms inducing the empty graph, are not connected.

**Lemma 5.19.** *Let $(A, \mu, \eta, \delta, \epsilon)$ be a Frobenius structure in a monoidal dagger category. Any connected morphism $A^{\otimes m} \to A^{\otimes n}$ built out of finitely many pieces $\mu, \eta, \delta, \epsilon$ and* id *using $\circ$ and $\otimes$ satisfies*

$$\#(\mu) = m + \#(\eta) + g - 1, \tag{5.16}$$

$$\#(\delta) = n + \#(\epsilon) + g - 1, \tag{5.17}$$

*where $g$ is the number of enclosed regions in the diagram.*

*Proof.* Because there are no braids, the graph is planar. Hence Euler's formula applies: $v - e + f = 2$, with $v$ the number of vertices, $e$ the number of edges, and $f$ the number of enclosed regions plus 1 for the 'outer' region enclosed by the edge of the paper. We have $v = m + n + \#(\mu) + \#(\delta) + \#(\eta) + \#(\epsilon)$ vertices and $f = g + 1$. The number of edges is $e = \frac{1}{2}\big(m + n + 3\#(\mu) + 3\#(\delta) + \#(\eta) + \#(\epsilon)\big)$. Putting it together gives

$$2 - 2g - m - n = \#(\eta) + \#(\epsilon) - \#(\mu) - \#(\delta). \tag{5.18}$$

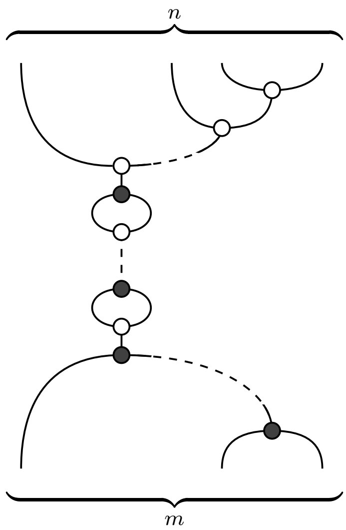
Of these, the number of internal input edges is $m + 2\#(\mu) + \#(\delta) + \#(\epsilon)$, and the number of internal output edges is $n + 2\#(\delta) + \#(\mu) + \#(\eta)$. Since $m$ plus the former has to match $n$ plus the latter, we get

$$m + \#(\delta) + \#(\eta) = n + \#(\mu) + \#(\epsilon). \tag{5.19}$$

Substituting (5.19) into (6.24) now gives (5.16) and (5.17). □

Now we are ready to describe a strategy to rewrite any connected diagram into a normal form representing the same morphism.

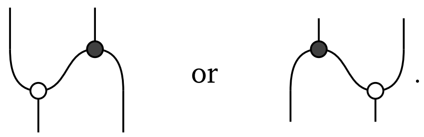
**Theorem 5.20** (Noncommutative spider theorem)**.** *Let* $(A, [mult], [unit], [comult], [counit])$ *be a Frobenius structure in a monoidal category. Any connected morphism* $A^{\otimes m} \to A^{\otimes n}$ *built out of finitely many pieces* [mult], [unit], [comult], [counit] *and* id *using* $\circ$ *and* $\otimes$ *equals the following* normal form*:*



(5.20)

*Morphisms built from* [mult], [unit], [comult], [counit], id, $\otimes$, $\circ$ *can be built from normal forms with* $\otimes$*.*

*Proof.* Consider one of the building blocks [mult]. Our strategy will be to push it down until it comes before any [comult]. What can we meet on our way down? If we meet a [unit], we can use unitality (4.6) and the [mult] vanishes. By Lemma 5.19, there are enough pieces [mult] to spend on getting rid of all the [unit]; we will be left with $m + g - 1$ pieces [mult]. We might also meet another [mult]. In this case we can use associativity (4.5) to push our chosen one below the one we meet. Finally, we can meet a [comult]. This can happen in two ways:



In both cases the Frobenius law (5.1) lets us push the [mult] below the [comult]. This will happen $m - 1$ times, leaving $g$ pieces [mult] remaining above a [comult].

In the same way, we can push up all the [comult], getting rid of all [counit] in the process, until $n - 1$ of them are above any [mult], and $g$ of them remain below a [mult].

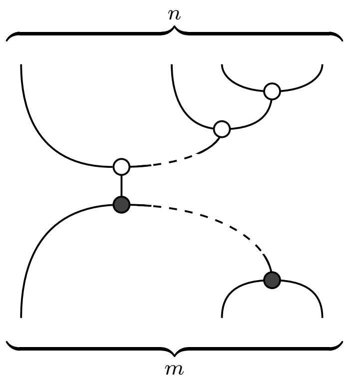
We are down to the case $m = n = 1$, with an equal number $g$ of pieces [mult] and [comult]. The bottom piece must be a [comult]. Take a [mult] and, using the same strategy as before, push it down until hits the bottom [comult], forming a single [loop]. Iterating this leaves us with a chain of $g$ components [loop], giving the desired normal form. □

The previous theorem is called the Spider Theorem because the normal form (5.20) looks a bit like an $(m + n)$–legged spider.

### 5.2.2 Normal forms for classical structures

Next we consider the commutative case of classical structures. It turns out that we can add braidings and still expect the same normal form. Like in the noncommutative case, we first have an combinatorial auxiliary lemma. This time the graph is not necessarily planar any longer, so we cannot speak about the number of enclosed regions. But it is still a graph, and it makes sense to ask whether it has cycles such as [cycle].

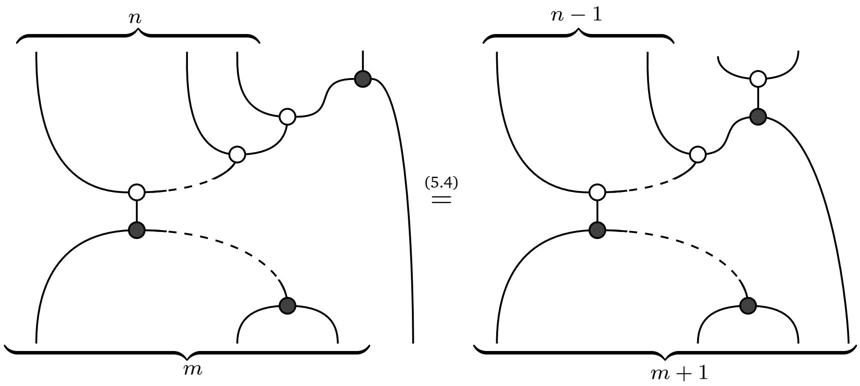
**Lemma 5.21.** *Let $(A, \text{[mult]}, \text{[unit]}, \text{[comult]}, \text{[counit]})$ be a commutative Frobenius algebra in a braided monoidal category, and consider a connected morphism $A^{\otimes m} \to A^{\otimes n}$ built out of finitely many pieces [mult], [unit], [comult], [counit],* $\mathrm{id}$*, and* $\sigma$*, using* $\circ$ *and* $\otimes$*. If its graph contains no cycles, then the morphism equals the following normal form:*




(5.21)

*Proof.* First, observe that the normal form (5.21) stays the same when we pre- or postcompose with braidings: by (co)associativity we can make sure the braid is directly below (or above) a (co)multiplication, and by (co)commutativity it then vanishes.

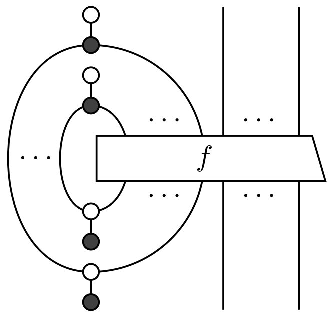
We proceed by induction on the number of vertices. The base case, of a single vertex, is trivial, as the diagram must be one of [mult], [unit], [comult], [counit]. For the induction step, assume that all diagrams with $N$ vertices can be brought in normal form, and consider a diagram with $N+1$ vertices. We may assume that the extra vertex is on the rightmost input or output leg of a diagram with $N$ vertices, which is in normal form. Because there are no cycles, that leaves six cases. Four cases are easy: a [counit] on the top right of (5.21), a [unit] on the bottom right, a [comult] on the top right, or a [mult] on the bottom right. The remaining two cases are symmetric: we treat a [mult] on the top right.




If $n = 0$ we were already done, so we may assume $n \geq 1$. By the Frobenius law we can rewrite the morphism as above. But then by the induction hypothesis the right-hand side is precisely the desired normal form. □

**Theorem 5.22** (Spider theorem). *Let $(A, \text{[mult]}, \text{[unit]}, \text{[comult]}, \text{[counit]})$ be a commutative Frobenius structure in a braided monoidal category. Any connected morphism $A^{\otimes m} \to A^{\otimes n}$ built out of* *finitely many pieces* , , , , id*, and* $\sigma$*, using* $\circ$ *and* $\otimes$*, equals the* normal form (5.20). *Hence any morphism built from finitely many* , , , , id*, and* $\sigma$ *using* $\circ$ *and* $\otimes$*, can be built from normal forms with* $\otimes$ *and* $\sigma$*.*

*Proof.* Using braidings, we can make sure that the diagram looks as follows for a connected morphism $f$ built from the basic building blocks without cycles.




Applying Lemma 5.21 to $f$ results in a connected diagram without braids. So applying Theorem 5.20 now completes the proof. □

**Corollary 5.23.** *Let* $(A, , )$ *be a classical structure in a braided monoidal dagger category. Any connected morphism* $A^{\otimes m} \to A^{\otimes n}$ *built out of finitely many pieces* , , id*, and* $\sigma$*, using* $\circ$ *and* $\otimes$*, equals the normal form* (5.21).

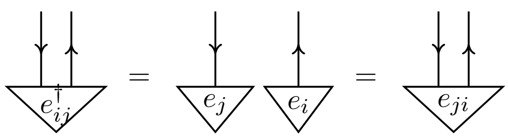
*Proof.* The in the middle of (5.21) disappear by speciality. □

## 5.3 The Frobenius law

Operators $A \to A$ 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 4.2.2. In the presence of daggers, this monoid picks up additional structure. This section proves that the resulting coherence property between dagger and closure is exactly the Frobenius law, by taking daggers into account in the Cayley embedding of Proposition 4.14. Thus Frobenius structures are motivated by the 'way of the dagger' .

### 5.3.1 Involutive monoids

Any operator $H \xrightarrow{f} H$ gives rise to another operator $H \xrightarrow{f^\dagger} H$. However, in the category **Hilb**, this operation $f \mapsto f^\dagger$ is anti-linear (see Section 0.2). So, if we try to transfer it to the pair of pants monoid $A = H^* \otimes H$, it does not correspond to a morphism $A \to A$, which would after all have to be linear. Rather, it corresponds to a morphism $A \xrightarrow{i} A^*$. However, by our conventions, $A^* = (H^* \otimes H)^* \simeq H^* \otimes H^{**} \simeq H^* \otimes H = A$! Indeed, in the matrix algebra of Example 4.13, $e_{ij}^\dagger = e_{ji}$, so in a pair of pants monoid we cannot see this involution graphically:



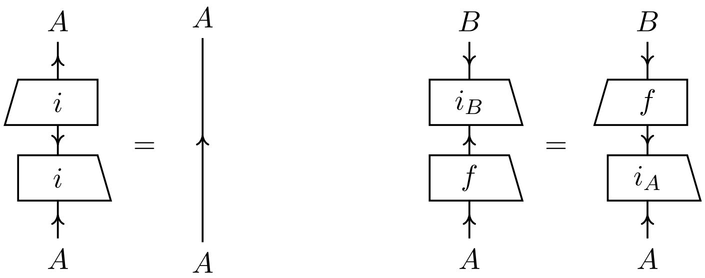
This information is hidden in the type of the involution $A \xrightarrow{i} A^*$, or rather, in our convention of choice of dual object $(A \otimes B)^* = B^* \otimes A^*$.

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)**.** *If $(A, m, u)$ is a monoid in a monoidal dagger category* **C***, and $A \dashv A^*$ is a dagger dual object, then $(A^*, m_*, u_*)$ is a monoid too.*

*Proof.* It follows from Lemma 3.15 that $(A^*, m^*, u^*)$ is a monoid in $\mathbf{C}^{\mathrm{op}}$; see Exercise 4.5.8. Since taking daggers is also a monoidal functor, that means $(A^*, m_*, u_*)$ is a monoid in **C** by Lemma 3.47. □

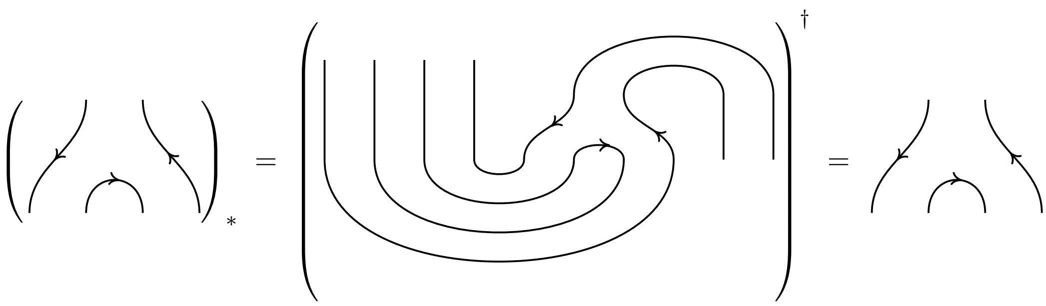
**Definition 5.25** (Involutive monoid)**.** A monoid $(A,$ ⅄ $,$ ⫯ $)$ on a object with a dagger dual is an *involutive monoid* when it comes equipped with an *involution*: a morphism of monoids $A \xrightarrow{i} A^*$ satisfying $i_* \circ i = \mathrm{id}_A$. A *morphism of involutive monoids* is a monoid homomorphism $A \xrightarrow{f} B$ satisfying $i_B \circ f = f_* \circ i_A$.




(5.22)

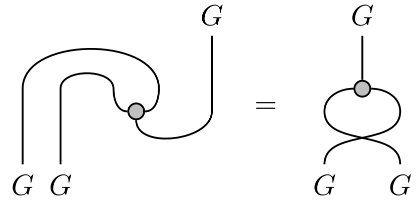
**Example 5.26.** The matrix algebra $\mathbb{M}_n$ of Example 4.13 is an involutive monoid in **FHilb**. The opposite monoid $\mathbb{M}_n^*$ is the same set of $n$-by-$n$ complex matrices, with the same unit, but with the opposite multiplication: $ab$ in $\mathbb{M}_n^*$ is the ordinary matrix multiplication $ba$ in $\mathbb{M}_n$. There is a canonical involution $\mathbb{M}_n \to \mathbb{M}_n^*$, given by the complex conjugate transpose $f \mapsto f^\dagger$.

More generally, the pair of pants algebras $A^* \otimes A$ of Lemma 4.12 are involutive in any monoidal dagger category, with the identity map as involution, because of our choice of conventions:




**Example 5.27.** The Frobenius structure $(G,$ ⅄ $,$ ⫯ $)$ in **Rel** induced by a groupoid **G** as in Example 5.3 is involutive. First, observe that the opposite monoid $G^*$ is induced by

the opposite groupoid $\mathbf{G}^{\mathrm{op}}$, since its multiplication is:

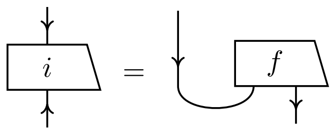



There is a canonical involution $G \to G^*$ given by $g \sim g^{-1}$. Note that this is a homomorphism of monoids, but not a functor of groupoids, because it only has to act on morphisms of $\mathbf{G}$ and not on objects.

## 5.3.2 Dagger closure

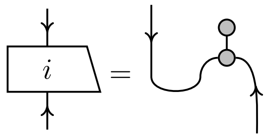
Proposition 4.14 showed that sets of operators that are closed under composition correspond to submonoids of a pair of pants monoid. Sets of operators that are closed under composition and dagger should correspond to involutive submonoids of a pair of pants. The following proposition characterizes when this is the case.

A monoid $(A,$ ⅄, ⫯$)$ having an involution $i$ can also be phrased in terms of having a map $A \otimes A \xrightarrow{f} I$:



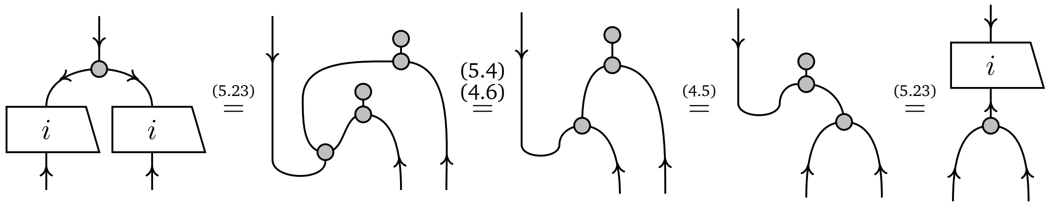

A canonical choice for such a map would be : $A \otimes A \to I$. For a pair of pants monoid as in the beginning of this section, this would give $i = \mathrm{id}_{H^* \otimes H}$. Compare also Proposition 5.15.

**Proposition 5.28.** *Let $A \dashv A^*$ be dual objects and $(A,$ ⅄, ⫯$)$ a monoid in a monoidal dagger category. Then $(A,$ ⅄, ⫯$)$ is a dagger Frobenius structure if and only if the following map makes the monoid involutive, and the embedding of Proposition 4.14 a morphism of involutive monoids:*



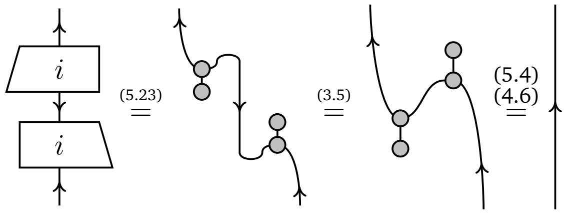

(5.23)

*Proof.* Assume that the Frobenius law (5.1) holds. We first prove that $i$ respects multiplication as in equation 4.14:



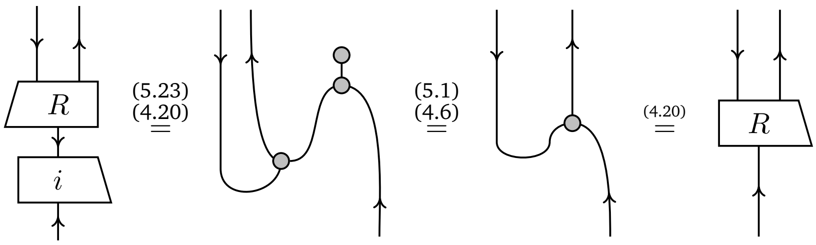

The second equation uses Lemma 5.4 and unitality, the third associativity.

That $i$ preserves units is trivial. Second, we show that $i$ is indeed involutive:



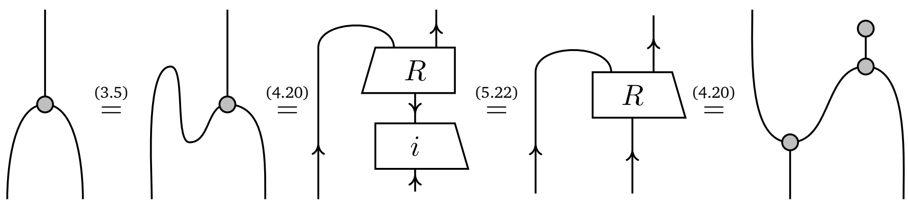

The second equation is the snake identity, and last equation uses the Frobenius law and unitality. Thus the monoid is involutive.

Third, we show that the Cayley embedding $R$ of Proposition 4.14 respects involutions. Because the involution on $A^* \otimes A$ is simply the identity, this means $R_* \circ i = R$:



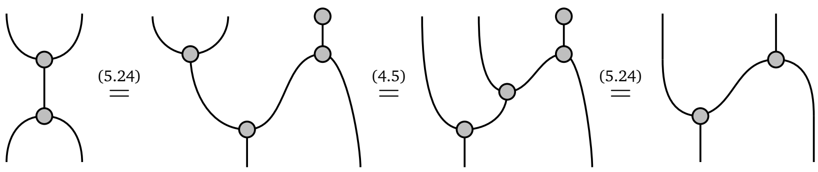

The derivation again used the Frobenius law and unitality.

Now for the converse. Assume that $R$ respects the involution. Then:




(5.24)

Hence:




The first and last step used (5.24), the middle step associativity. Invoking Lemma 5.4 now completes the proof. □

Thus, if we want to think of operators as monoids, 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 4.13; hence classical structures in **FHilb** must copy an orthonormal basis as in Example; and special dagger Frobenius structures in **Rel** must be induced by a groupoid as in Example 5.3.

### 5.4.1 Operator algebras

To classify the special dagger Frobenius structures in **FHilb**, we are going to have to use some results that are beyond the scope of this book. First, combine Proposition 5.28 and Example 4.13 to find the following: dagger Frobenius structures in **FHilb** correspond to subsets $A \subseteq \mathbb{M}_n$ that are closed under addition, scalar multiplication, matrix multiplication, matrix adjoint, and that contain the identity matrix.

The matrix algebra $\mathbb{M}_n$, and hence its subalgebra $A$, has a final piece of structure, namely a *norm*:

$$\|a\| = \min\{c \geq 0 \mid \|ax\| \leq c\|x\| \text{ for all } x \in \mathbb{C}^n\} \tag{5.25}$$

for $a \in \mathbb{M}_n$. This norm satisfies $\|a^\dagger a\| = \|a\|^2$ and $\|ab\| \leq \|a\|\|b\|$ for all matrices $a$ and $b$, and is the unique one that does so.

In fact, these conditions are enough to characterize subsets $A \subseteq \mathbb{M}_n$ as above! They are called *C*-algebras*. One of the main results is the *Gelfand–Neumark–Segal embedding*, and it proves more generally precisely what Proposition 5.28 did abstractly, namely that any finite-dimensional operator algebra embeds into $\mathbb{M}_n$ for some $n$. Well, there is one caveat: the embedding $A \to \mathbb{M}_n$ must not only preserve multiplication and involution, but also the norm. Tracking through Proposition 5.28, it turns out that this corresponds to the Frobenius structure being special. However, in finite dimension all norms are equivalent, and indeed we may rescale the inner product on $A$ by the scalar $k(A)$ given by Definition 3.52. We will see this rescaling in action in more detail in Remark 7.27. The following theorem summarizes all this.

**Theorem 5.29** (Gelfand–Neumark). *Any dagger Frobenius structure in* **FHilb** *is the transport of a special one, and special dagger Frobenius structures in* **FHilb** *are precisely finite-dimensional C*-algebras.* □

If $A \subseteq \mathbb{M}_m$ and $B \subseteq \mathbb{M}_n$ are operator algebras, then so is their direct sum $A \oplus B \subseteq \mathbb{M}_{m+n}$. Indeed, if $(A, \curlywedge_{\circ})$ and $(B, \curlywedge_{\bullet})$ are dagger Frobenius structures in a compact dagger category with dagger biproducts, then so is $A \oplus B$. Using the matrix calculus of Lemma 2.23 and the distributivity of Lemma 3.19, the multiplication and unit are given by

$$\begin{pmatrix} \curlywedge_{\circ} & 0 & 0 & 0 \\ 0 & 0 & 0 & \curlywedge_{\bullet} \end{pmatrix} : (A \oplus B) \otimes (A \oplus B) \to A \oplus B, \qquad \begin{pmatrix} \curlywedge_{\circ} \\ \curlywedge_{\bullet} \end{pmatrix} : I \to A \otimes B. \tag{5.26}$$

See also Exercise 5.7.8 and Lemma 7.42. But taking direct sums of matrix algebras is the only freedom there is in finite-dimensional operator algebras, as the following theorem shows. Its proof is based on the Artin–Wedderburn theorem, which is beyond the scope of this book.

**Theorem 5.30** (Artin–Wedderburn). *Any finite-dimensional C*-algebra is of the form* $A \simeq \mathbb{M}_{k_1} \oplus \cdots \oplus \mathbb{M}_{k_n}$ *for natural numbers* $n, k_1, \ldots, k_n$. □

Thus any dagger Frobenius structure $(A, \curlywedge)$ in **FHilb** is (isomorphic to) one of the form $\mathbb{M}_{k_1} \oplus \cdots \oplus \mathbb{M}_{k_n}$. Via the Cayley or Gelfand–Neumark–Segal embedding, we may think of them as algebras of matrices that are block diagonal. This restriction to block diagonal form is caused physically by *superselection rules*.

### 5.4.2 Orthonormal bases

Of course the matrix algebra $\mathbb{M}_n$ is not commutative as soon as $n \geq 2$. In particular, if $\curlywedge$ is commutative, we must have $k_1 = \cdots = k_n = 1$ and so $A \simeq \mathbb{C} \oplus \cdots \oplus \mathbb{C}$! The following corollary follows immediately.

**Corollary 5.31.** *For a finite-dimensional Hilbert space, there are exact correspondences between:*

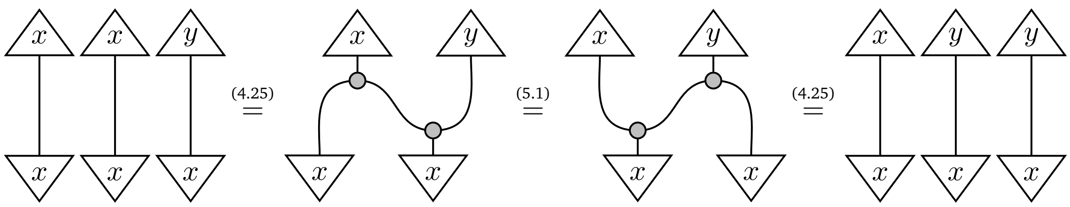
- *orthogonal bases and commutative dagger Frobenius structures;*
- *orthonormal bases and classical structures.* □

We can now recognize the transport Lemma 5.16 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.

Let's make all this use of high-powered machinery more concrete. We saw in Section 5.1 that copying any orthonormal basis of a finite-dimensional Hilbert space makes it into a classical structure, as is easy to verify. Corollary 5.31 is the converse: every classical structure in **FHilb** is of this form. Given a classical structure, we can retrieve an orthonormal basis by its set of copyable states, discussed in Section 4.3. The following lemmas form part of the proof of Corollary 5.31.

**Lemma 5.32.** *Nonzero copyable states of a dagger Frobenius structure in* **FHilb** *are orthogonal.*

*Proof.* Let $x, y$ be nonzero copyable states and assume that $\langle x|y\rangle \neq 0$. Then:



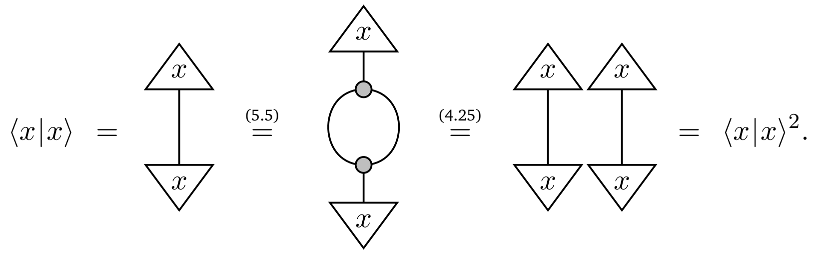

In other words, $\langle x|x\rangle\langle x|x\rangle\langle y|x\rangle = \langle x|x\rangle\langle y|x\rangle\langle y|x\rangle$. Since $x \neq 0$ also $\langle x|x\rangle \neq 0$. So we can divide to get $\langle x|x\rangle = \langle x|y\rangle$. Similarly we can find $\langle y|x\rangle = \langle y|y\rangle$. Hence these inner products are all in $\mathbb{R}$, and are all equal. But then

$$\langle x - y|x - y\rangle = \langle x|x\rangle - \langle x|y\rangle - \langle y|x\rangle + \langle y|y\rangle = 0,$$

so $x - y = 0$. □

**Lemma 5.33.** *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 $x$ has a norm that squares to itself:



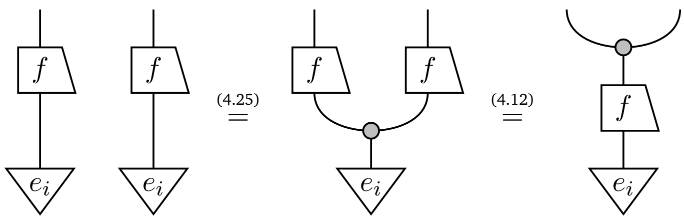

If $x$ is nonzero then $\langle x|x\rangle$ must be nonzero, so dividing by it shows that $\|x\| = 1$. □

The difficult part of proving Corollary 5.31 is that the copyable states of a classical structure are not only orthonormal, they span the whole space; this is where the powerful theorems that are beyond the scope of this book come in.

Using Corollary 5.31, we can prove a converse to Example 4.6: every comonoid homomorphism between classical structures in **FHilb** is a function between the corresponding orthonormal bases.

**Corollary 5.34.** *In* **FHilb***, a morphism between two commutative dagger Frobenius structures acts as a function on copyable states if and only if it is a comonoid homomorphism.*

*Proof.* By linear extension, the comonoid homomorphism condition (4.12) 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 Corollary 5.31. This gives the following equation:

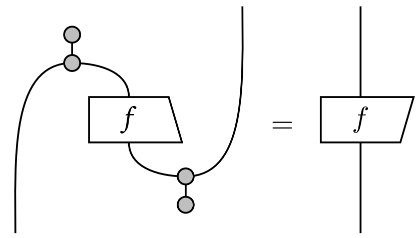



Here the first equality expresses the fact that the state $e_i$ is copyable, and the second equality is the comonoid homomorphism condition. Hence $f(e_i)$ is itself a copyable state. Thus (4.12) holds if and only if $f$ sends copyable states to copyable states. The counit preservation condition (4.13) follows, because the counit 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.

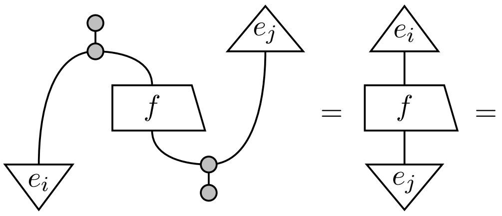
**Lemma 5.35.** *Comonoid homomorphisms between classical structures in* **FHilb** *are self-*

*conjugate:*



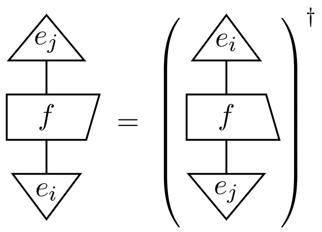

(5.27)

*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 we can do this calculation:




$$= \begin{bmatrix} 1 & \text{if } e_i = f(e_j) \\ 0 & \text{if } e_i \neq f(e_j) \end{bmatrix}^\dagger = \begin{bmatrix} 1 & \text{if } e_i = f(e_j) \\ 0 & \text{if } e_i \neq f(e_j) \end{bmatrix}$$

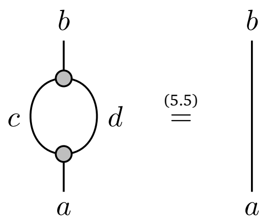
Thus (5.27) holds. □

## 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.

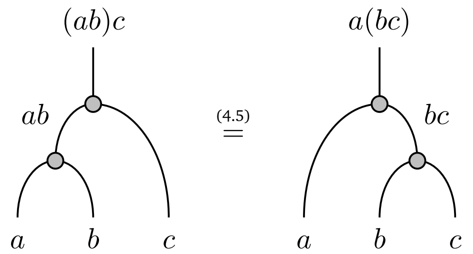
**Theorem 5.36.** *Special dagger Frobenius structures in* $\mathbf{Rel}$ *correspond exactly to groupoids.*

*Proof.* Let $(A, M, U)$ be a special dagger monoid-comonoid pair in $\mathbf{Rel}$. 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 **??**:



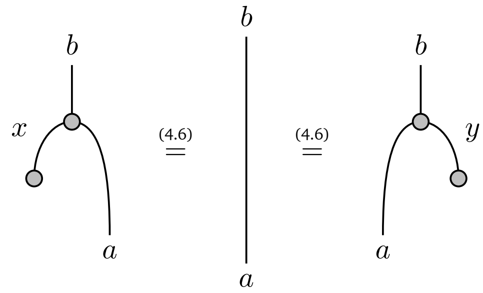
On the right-hand side, two elements $a, b \in A$ are only related by the identity relation if they are equal. So the same must be true on the left-hand side. Thus: if two elements $c, d \in A$ multiply to give two elements $a, b \in A$ — that is, both $b\,M\,(c, d)$ and $a\,M\,(c, d)$ hold — it must be the case that $a = b$. This says exactly that if two elements can be multiplied, then their product is unique. As a result we may simply write $ab$ for the product of $a$ and $b$, remembering that this only makes sense if the product 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:

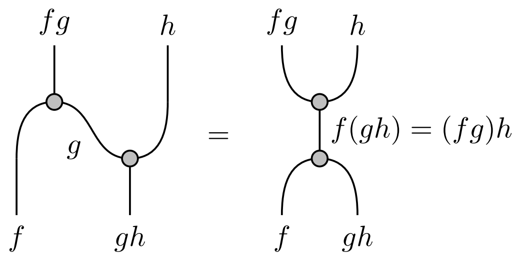



Here $x, y \in U \subseteq A$ are units, determined by the unit $1 \xrightarrow{U} A$ of the monoid. The first equality says that all $a, b$ allow some $x \in U$ with $xa = b$ if and only if $a = b$. The second equality says that $ay = b$ for some $y \in U$ if and only $a = b$. Put differently: multiplying on the left or the right by a element of $U$ is either undefined, or gives back the original element.

What happens when multiplying elements from $U$ together? Well, 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.

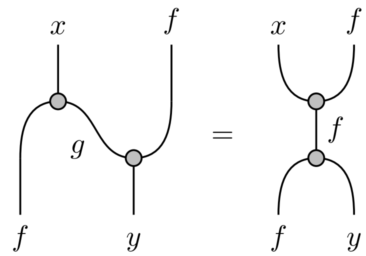
Lastly, can an element $a \in A$ have two left identities — is it possible for distinct $x, x' \in U$ to satisfy $xa = a = x'a$? This would imply $a = xa = x(x'a) = (xx')a$, which is undefined, as we have seen. So every element has a unique left identity, and similarly every element has a unique right identity.

Altogether, this gives exactly the data to define a category. Let $U$ be the set of objects, and $A$ the set of arrows. Suppose $f, g, h \in A$ are arrows 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:



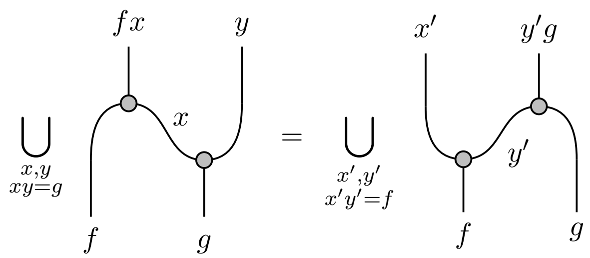

If $fg$ and $gh$ are defined then the left-hand side is defined, and hence the right hand side must also be defined.

To show that every arrow 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 $f$.

Finally, consider the other direction of the theorem: start with a groupoid. Write $A$ for its set of arrows and $U$ for the subset of identities. Then we consider the triple $(A, M, U)$ in $\mathbf{Rel}$, where $M$ is the partial composition operation of arrows in the category. This is single-valued when it is defined, so $M$ is special. Every arrow has a right and left unit, and morphism composition is associative when it is defined, making $(A, M, U)$ a special dagger monoid in $\mathbf{Rel}$. To establish the Frobenius law (5.1), evaluate it on arbitrary input $(f, g)$.




On the left we obtain output $\cup_{x,y|xy=g}(fx, y)$, on the right $\cup_{x',y'|x'y'=f}(x', y'g)$. Making the change of variables $x' = fx$ and $y' = yg^{-1}$, the condition $x'y' = f$ becomes $fxyg^{-1} = f$, which is equivalent to $xy = g$. So the two composites above are indeed equal, establishing the Frobenius law. $\square$

Notice that, using the previous theorem, Proposition 4.14 specializes precisely to Cayley's original theorem.

Note also that the nondegenerate form of Proposition 5.15 is the coname of the function $g \mapsto g^{-1}$; see also Example 5.27.

Classifying the pair of pants Frobenius structures of Lemmas 4.12 and 5.9 leads us back to the indiscrete categories of Section 4.3.2, as the following Corollary shows.

**Corollary 5.37.** *Quantum structures in* $\mathbf{Rel}$ *are precisely* indiscrete groupoids*, i.e. groupoids where there is precisely one morphism between each two objects.*

*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 defined.

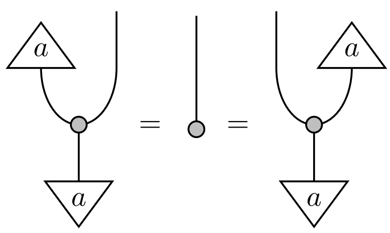
**Corollary 5.38.** *In* $\mathbf{Rel}$*, classical structures exactly correspond to abelian groupoids.*

*Proof.* An immediate consequence of Theorem 5.36. □

# 5.5 Phases

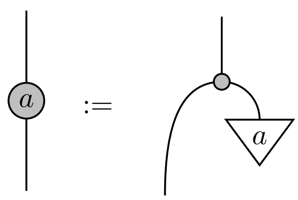
In quantum information theory, an interesting family of maps are *phase gates*: diagonal matrices whose diagonal entries are complex numbers of norm 1. For a particular Hilbert space equipped with a basis, these form a group under composition, which we will call the *phase group*. This turns out to work fully abstractly: any Frobenius structure in any monoidal dagger category gives rise to a phase group.

**Definition 5.39** (Phase)**.** Let $(A, , )$ be a Frobenius structure in a monoidal dagger category. A state $I \xrightarrow{a} A$ is called a *phase* when:




(5.28)

Its *(right) phase shift* is the following morphism $A \to A$:

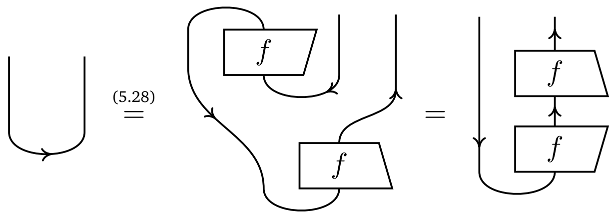



(5.29)

For the classical structure copying an orthonormal basis $\{e_i\}$ in **FHilb**, a vector $a = a_1e_1 + \cdots a_ne_n$ is a phase precisely when each scalar $a_i$ lies on the unit circle: $|a_i|^2 = 1$. For another example, the unit of a Frobenius structure is always a phase. The following lemma gives more examples.

**Lemma 5.40.** *The phases of a pair of pants Frobenius structure* $(A^* \otimes A, ⁄\!\!\cap\!\!\backslash, \cup)$ *are the names of unitary operators* $A \to A$.

*Proof.* The name of an operator $A \xrightarrow{f} A$ is a phase when:




But this precisely means $f \circ f^\dagger = \mathrm{id}_A$ by the snake equations (3.5). The other, symmetric, equation defining phases similarly comes down to $f^\dagger \circ f = \mathrm{id}_A$. □

**Example 5.41** (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 5.42** (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 (5.28) defining phases reads

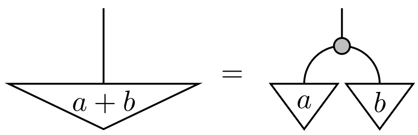
$$\{g^{-1}h \mid g, h \in a\} = \{1_G\} = \{hg^{-1} \mid g, h \in a\}.$$

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.

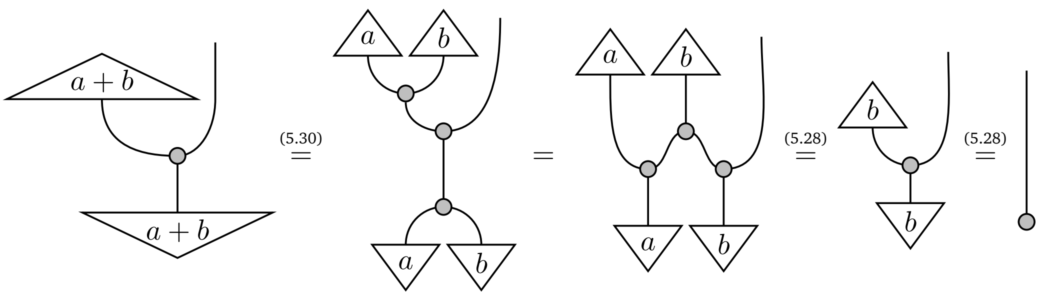
**Proposition 5.43** (Phase group). *Let $(A, \cdot, \cdot)$ be a dagger Frobenius structure in a monoidal dagger category. Its phases form a group with unit $\cdot$ under the following addition:*



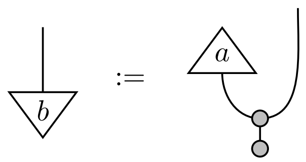
(5.30)

*The phases of a classical structure in a braided monoidal dagger category form an abelian group.*

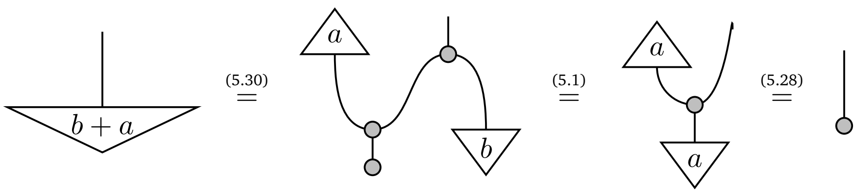
*Proof.* First we show that (5.30) is again a well-defined phase:




The second equality follows from the noncommutative Spider Theorem 5.20. As the other equation of (5.28) follows similarly, the set of phases form a monoid by associativity (4.5). Fix a phase $a$ and set:




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 4.5.2.) Clearly this group will be abelian when the Frobenius structure is commutative. □

The group of the previous proposition is called the *phase group*. Equivalently, the phase shifts form a group under composition.

**Example 5.44.** The group operation on the phases of the pair of pants Frobenius structure of Lemma 5.40, which are names of unitary morphisms $A \xrightarrow{f} A$, is simply taking the name of composition of operators.

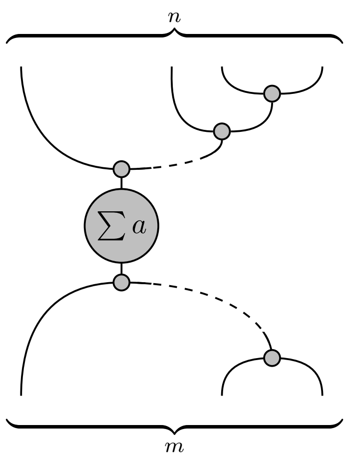
The group operation on the phases $U(k_1) \times \cdots \times U(k_n)$ of a Frobenius structure $\mathbb{M}_{k_1} \oplus \cdots \oplus \mathbb{M}_{k_n}$ in **FHilb** of Example 5.41 is simply entrywise multiplication. In particular, the group operation on a classical structure as multiplication of diagonal matrices.

The group operation on the phases $G$ of a Frobenius structure in $\mathbf{Rel}$ induced by a group $G$as in Example 5.42 is by definition the multiplication of $G$ itself. Hence the phase group of the Frobenius structure $G$ in $\mathbf{Rel}$ is $G$ itself.

## 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 5.45** (Phased spider theorem)**.** *Let* $(A, \tinymult, \tinyunit)$ *be a classical structure in a braided monoidal dagger category. Any connected morphism* $A^{\otimes m} \to A^{\otimes n}$ *built out of finitely many* $\tinymult, \tinyunit, \mathrm{id}, \sigma$ *and phases using* $\circ$*,* $\otimes$*, and* $\dagger$*, equals*




(5.31)

*where* $a$ *ranges over all the phases used in the diagram.*

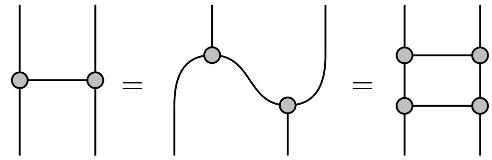
*Proof.* Using braidings we can first make sure all the phases dangle at the bottom right of the diagram. Next we can apply Corollary 5.23. By definition (5.30) of the phase group, the phases on the bottom right, together with the multiplications $\tinymult$ above them, reduce to a single phase $\sum a$ on the bottom right. Finally, another application of Corollary 5.23 turns the diagram into the desired form (5.31). $\square$

## 5.5.3 State transfer

We're now going to apply our knowledge of classical structures to analyze the quantum state transfer protocol. This procedure transfers the quantum state of a

Hilbert space $H$ from one system to another, with a probability of success given by $1/\dim(H)^2$. Interest in state transfer lies in the fact that all the procedures involved are state preparations or measurements: no unitary dynamics takes place. It is related to quantum teleportation which we will study in Section 5.6.3, a procedure which is more sophisticated but which transmits the state correctly every time.

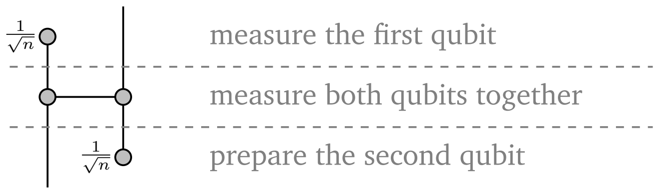
By virtue of the spider theorem, we can be quite lax when drawing wires connected by classical structures. They are all the same morphism anyway. For example:



(5.32)

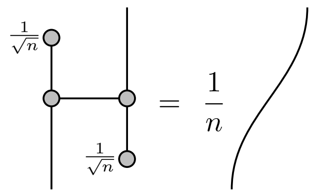
is a projection $H \otimes H \to H \otimes H$.

Define the procedure for state transfer graphically by the following diagram:




(5.33)

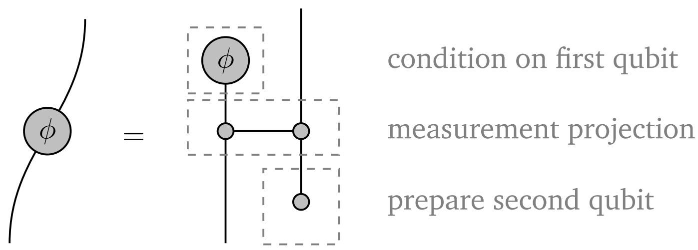
We can easily simplify this diagram using the spider theorem:




(5.34)

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.

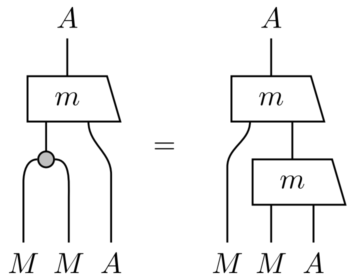
By using the phased spider theorem, Corollary 5.45, we can also easily achieve the extra challenge of applying a phase gate in the process of transferring the state, by the following adapted protocol.



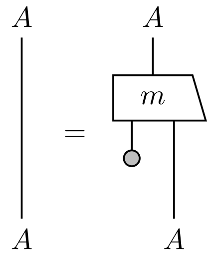

## 5.6 Modules

In this section we will use classical structures to give mathematical structure to the notion of quantum measurement. The idea is as follows. As we saw in Section 5.3, observables correspond to states of pair of pants structures $A^* \otimes A$. In fact, a monoid $A$ always embeds into $A^* \otimes A$; 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 5.46** (Module)**.** For a monoid $(M, \curlywedge, \circ)$ in a monoidal category, a *module* is an object $A$ equipped with a map $M \otimes A \xrightarrow{m} A$ satisfying the following equations:




(5.35)



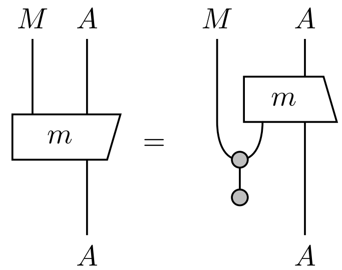

(5.36)

The morphism $m$ is called an *action* of the monoid $(M, \curlywedge, \circ)$ on the object $A$. More precisely, this is a *left module*, with *right modules* similarly defined with action $A \otimes M \to A$. We will only consider left modules in this book, so just refer to them as modules.

**Example 5.47.** 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 $g \otimes a \mapsto f(g)(a)$.

In the presence of a dagger, there is an additional compatibility to consider.

**Definition 5.48** (Dagger module)**.** In a monoidal dagger category, a *dagger module* for a dagger Frobenius structure $(M, \curlywedge, \circ)$ is a module action $M \otimes A \xrightarrow{m} A$ satisfying:




(5.37)

For example, the multiplication $\curlywedge : M \otimes M \to M$ of a dagger Frobenius structure is the action of a dagger module on itself.

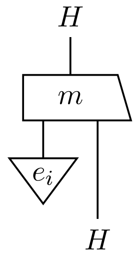
**Example 5.49.** A *unitary representation* of a group $G$ is a group homomorphism $G \xrightarrow{f} U(n)$. These correspond precisely to the dagger modules of the group algebra $A$ of $G$: if we put the effect $A \xrightarrow{g^\dagger} I$ for $g \in G$ on the top left in equation (5.37), the left-hand 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): an orthogonal family $\{p_1, \ldots, p_n\}$ of projections $H \xrightarrow{p_i} H$ satisfying $p_1 + \cdots + p_n = \mathrm{id}_H$.

**Lemma 5.50.** *Let* $(M, \text{⋏}, \text{⫯})$ *be a classical structure in* **Hilb**. *A dagger module for* $M$ *acting on* $H$ *corresponds to a projection-valued measure on* $H$ *with* $\dim(M)$ *outcomes.*

*Proof.* The module $M \otimes H \xrightarrow{m} H$ is determined by the following morphisms $p_i$:




(5.38)

for copyable states $e_i \in M$. First, by associativity (5.35), speciality (5.5), and copyability (4.25) 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 (5.37) gives $p_i = p_i^\dagger$. Third, since $\text{⫯} = \sum_i e_i$, also $\sum_i p_i = \mathrm{id}_H$. Hence $\{p_i\}$ form a PVM. In fact, this argument works both ways: 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 (5.38) corresponds to one $p_i$. □

Thus we may think of the adjoint $A \to M \otimes A$ of a dagger module as a *measurement*: starting with a state of system $A$, we end up with classical information $M$ and a possibly different state of the system $A$ after measurement.

We can also consider such measurements in other categories, such as **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 $g^{-1}a$.

**Lemma 5.51.** *Consider a classical structure in* **Rel** *induced by an abelian groupoid* $\mathbf{G}$. *A dagger module acting on a set* $A$ *corresponds to a functor from* $\mathbf{G}$ *to the symmetric group* $\mathrm{Sym}(A)$ *of bijections on* $A$.

Such functors $R\colon \mathbf{G} \to \mathrm{Sym}(A)$ are called $\mathbf{G}$-*actions*, and written $R(g)(a) = ga$.

*Proof.* Conditions (5.35), (5.36), and (5.37) correspond to

$$(g \circ h, a) \sim c \iff \exists b\colon (g, a) \sim b, (h, b) \sim c, \tag{5.39}$$

$$(\mathrm{id}_A, a) \sim b \iff a = b, \tag{5.40}$$

$$(g, a) \sim b \iff (g^{-1}, b) \sim a. \tag{5.41}$$

First, we prove that $(g, a) \sim b$ and $(g, a) \sim b'$ imply $b = b'$. By (5.41) we get $(g^{-1}, b) \sim a$. Next $(\mathrm{id}_{\mathrm{cod}(g)}, b) \sim b'$ by (5.39). But then $b = b'$ by (5.40). Hence the relation is in fact a function $R\colon G \times A \to A$.

Moreover, the functions $R_g\colon A \to A$ defined by $R_g(a) = b$ when $(g, a) \sim b$ are bijections. With this knowledge, we can rewrite the above conditions as

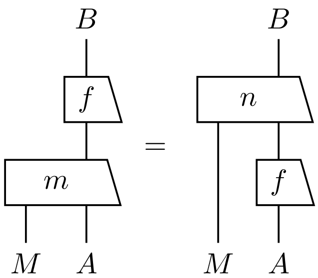
$$
\begin{aligned}
R_{g \circ h} &= R_h \circ R_g, \\
R_{\mathrm{id}} &= \mathrm{id}_X, \\
R_{g^{-1}} &= R_g^{-1}.
\end{aligned}
$$

But this is precisely a **G**-action on $A$. □

### 5.6.2 Module morphisms

Following a measurement, the only allowed quantum dynamics are the *controlled operations*. These are the unitary maps which do not change the result of the measurement. Mathematically, these are the *module homomorphisms* for the module action.

**Definition 5.52.** Given a monoid $(M, , )$ in a monoidal category 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:

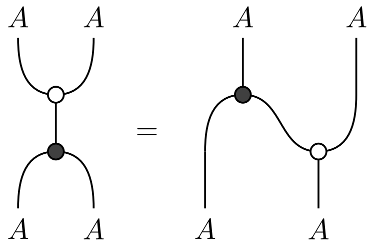



(5.42)

As the following lemma shows, the module homomorphism condition (5.42) gives another characterization of Frobenius structures.

**Lemma 5.53** (Frobenius structure via modules)**.** *A monoid and comonoid on the same object* $(A, , , , )$ *form a Frobenius structure if and only if* *is a module homomorphism for the action of* $A$ *on itself given by* .

*Proof.* The module homomorphism Definition 5.52 for $m =$ , $n =$ $\otimes\, \mathrm{id}_A$ and $f =$ reads



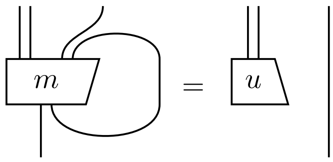

(5.43)

which is equivalent to the Frobenius law by Lemma 5.4. □

### 5.6.3 Pure quantum teleportation

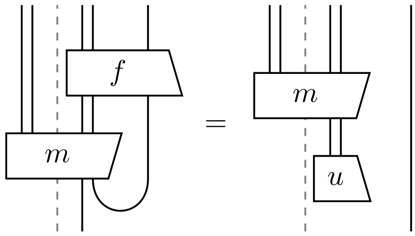
Frobenius structures and their modules allow a treatment of quantum teleportation without using biproducts. The advantage is that this is purely graphical.

**Proposition 5.54.** *A dagger Frobenius structure* $(A \otimes A, m, u)$ *on a product system in a dagger monoidal category describes measurement in a teleportation protocol if and only if:*



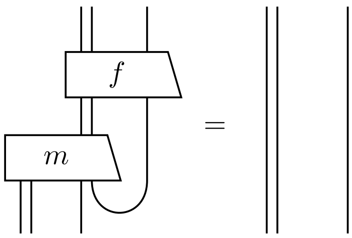
(5.44)

*Proof.* Successful execution of a quantum teleportation protocol corresponds to:

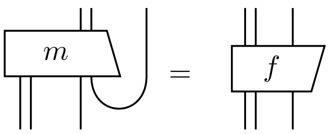


(5.45)

Bending down the top-left $A \otimes A$ wires using Theorem 5.14 gives:

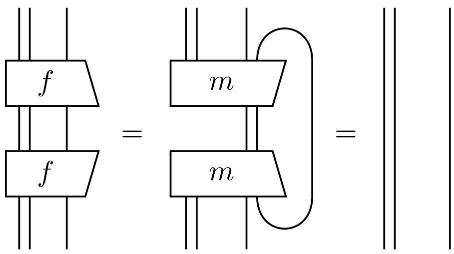



Compose both sides with $f^\dagger$ at the top:



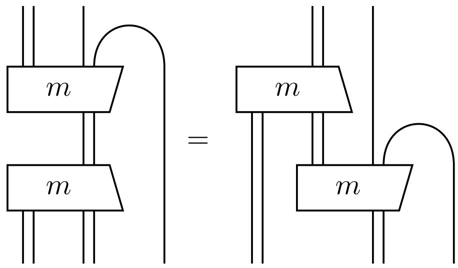
(5.46)

Using this description of $f^\dagger$, evaluate $f \circ f^\dagger = \mathrm{id}_{(A\otimes A)\otimes A}$ as follows:



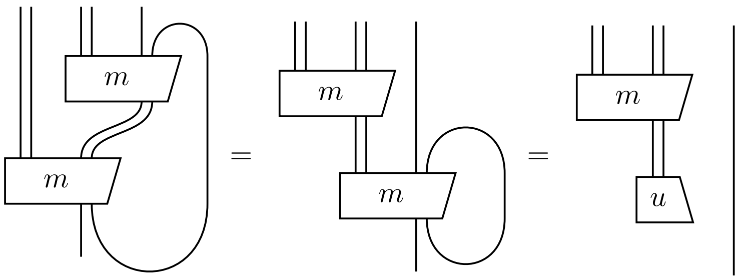

Composing with the unit $I \xrightarrow{u} A \otimes A$ of the classical structure on the bottom-left leg and applying the unit law gives (5.44) as required.

For this to make physical sense, the morphism $f$ must be a controlled operation. Using the adjoint of (5.46) as $f$, condition (5.42) becomes:




But this holds by the noncommutative Spider Theorem 5.20.

Conversely, suppose a dagger Frobenius structure satisfies (5.45). Then taking $f$ to be the adjoint of (5.46) will give a valid controlled operation by the argument just given. All that remains to show is that it correctly implements quantum teleportation, as in(5.45). To verify this, simply plug in the definition of $f$:




This completes the proof. □

## 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 a braided monoidal category, the tensor product of Frobenius structures is again a Frobenius structure.

(b) Show that, in a braided monoidal category, the tensor product of symmetric Frobenius structures is again a symmetric Frobenius structures.

(c) Show that, in a braided 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 braided monoidal dagger categories. 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 ($m \circ \sigma = m$). Given a dual object $A \dashv A^*$, construct a map $I \xrightarrow{u} A$ such that unitality ($m \circ (\mathrm{id} \otimes u) = \mathrm{id}$) holds.

**Exercise 5.7.3.** Recall that a set $\{x_0, \ldots, x_n\}$ of vectors in a vector space is *linearly independent* when $\sum_{i=0}^{n} z_i x_i$ 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.

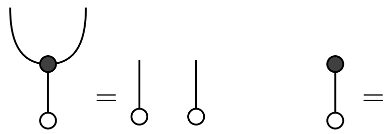
(b) A *cycle* in a category is a series of morphisms $A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} A_3 \cdots A_n \xrightarrow{f_n} A_1$. For finite **G**, show that a phase corresponds to a union of cycles that cover all objects of **G**. Find a phase on the indiscrete category on $\mathbb{Z}$ that is not a union of cycles.

(c) A groupoid is *totally disconnected* when all morphisms are endomorphisms. Show that for such 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 $(F(A), F(m), F(u), F(d), F(e))$ is a Frobenius structure in **D**. (See also Exercises 3.3.18 and 4.5.8.)

**Exercise 5.7.6.** Let $(A,$ $)$ be a symmetric Frobenius structure in braided monoidal category. Suppose it is *disconnected*, in the sense that:



Prove that $\dim(A) = 1$. Summarize the consequences in **Hilb** and **Rel**.

**Exercise 5.7.7.** This question is on describing teleportation using Frobenius structures.

(a) Show that a Bell state measurement on $\mathbb{C}^2$ gives rise to a classical structure on $\mathbb{C}^2 \otimes \mathbb{C}^2$ satisfying equation (5.44).

(b) Develop an account of encrypted communication in **Rel** using classical structures and modules. For inspiration, read again the discussion at the end of Chapter 3.

**Exercise 5.7.8.** Prove that the biproduct of dagger Frobenius structures in a monoidal dagger category with dagger biproducts, with multiplication as in (5.26), is again a dagger Frobenius structures.

**Exercise 5.7.9.** Pick a basis $\{e_{11}, e_{12}, e_{21}, e_{22}\}$ for $A = \mathbb{C}^4 \in$ **FHilb**. Define  $:=$

$e_{11} + e_{22} \colon I \to A$ and define $\curlywedge \colon A \otimes A \to A$ by

$$e_{ij} \otimes e_{kl} \mapsto \begin{cases} e_{il} & \text{if } j = k \text{ and } (i = j \text{ or } k = l), \\ 0 & \text{otherwise.} \end{cases}$$

(a) Show that $\curlywedge$ maps $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \otimes \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ to $\begin{pmatrix} ae & af+bh \\ ce+dg & dh \end{pmatrix}$.

(b) Show that $\varphi \colon A \to I$, given by $e_{ii} \mapsto 1$ and $e_{ij} \mapsto 0$ for $i \neq j$, satisfies the requirements of Proposition 5.15. Conclude that $(A, \curlywedge, \bullet, \varphi)$ is part of a Frobenius structure (but not a dagger one).

(c) Show that this Frobenius structure is not symmetric.

# 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 [**?**]. Great advances were made by Nakayama in 1941, who coined the name [**?**]. The formulation with multiplication and comultiplication we use is due to Lawvere in 1967 [**?**], and was rediscovered by Quinn in 1995 [**?**] and Abrams in 1997 [**?**]. Dijkgraaf realized in 1989 that the category of commutative Frobenius structures is equivalent to that of 2-dimensional topological quantum field theories [**?**]. For a comprehensive treatment, see the monograph by Kock [**?**]. The noncommutative spider theorem 5.20 was proved using the homotopy theory of 2-dimensional surfaces with boundary by Abrams [**?**]. The combinatorial proof we gave is due to Kock [**?**]. The inductive proof we gave for the commutative spider theorem is due to Kissinger [**?**].

Coecke and Pavlović first realized in 2007 that commutative Frobenius structures could be used to model the flow of classical information [**?**]. That paper also describes quantum measurement in terms of modules for the first time. Corollary 5.31, that classical structures in **FHilb** correspond to orthonormal bases, was proved in 2009 by Coecke, Pavlović and Vicary [**?**]. In 2011, Abramsky and Heunen adapted Definition 5.10 to generalize this correspondence to infinite dimensions in **Hilb** [**?**], and Vicary generalized it to the noncommutative case [**?**].

Operator algebra is a venerable field of study in functional analysis, with breakthroughs by Gelfand in 1939 and von Neumann in 1936 [**?**, **?**]. For a first introduction see [**?**]. We have only considered finite dimension, and indeed the correspondence between C*-algebras and Frobenius structures breaks in infinite dimension [**?**]. Terminology warning: the involution of a C*-algebra is typically denoted $*$, which matches our † rather than our $*$.

Theorem 5.36, that classical structures in **Rel** are groupoids, was proven by Pavlović in 2009 [**?**], and generalized to the noncommutative case by Heunen, Contreras and Cattaneo in 2012 [**?**].

The phase group was made explicit by Coecke and Duncan in 2008 [**?**], and later Edwards in 2009 [**?**, **?**], in the commutative case. The state transfer protocol is important in efficient measurement-based quantum computation. It is due to Perdrix in 2005 [**?**].

# Chapter 6

# Complementarity

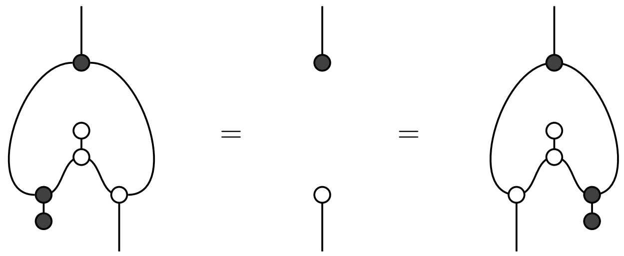
This chapter studies what happens when we have *two* interacting Frobenius structures. Specifically, we are interested in when they are "maximally incompatible", or *complementary*, and give a definition that makes sense in arbitrary categories in Section 6.1. We will see that it comes down to the usual 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. In the presence of a dagger, we characterize complementarity in terms of a canonical morphism being isometric. This is exemplified by discussing the Deutsch–Jozsa algorithm in Section 6.2, where the canonical morphism plays the role of an oracle function. Section 6.3 links complementarity to the subject of quantum groups. It turns out that this well-studied notion gives rise to a stronger form of complementarity that we characterize. Finally, Section 6.4 discusses how 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.

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 dagger functors.

## 6.1 Complementarity

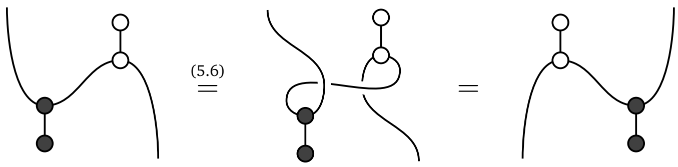
Consider two measurements of a qubit: one in the basis $\{\binom{1}{0}, \binom{0}{1}\}$, and one in the basis $\{\binom{1}{1}/\sqrt{2}, \binom{1}{-1}/\sqrt{2}\}$. If we perform the first measurement first, the qubit will collapse to either $\binom{1}{0}$ or $\binom{0}{1}$; in either case, the second measurement will give probability $1/2$ for both of its outcomes. In other words: one measurement provides no information whatsoever about the other observable, and vice versa. This is a simple form of Heisenberg's uncertainty principle. We can formulate providing no information categorically as the graphical diagram disconnecting, leading to the following definition.

**Definition 6.1** (Complementary Frobenius structures). Two symmetric dagger Frobenius structures and on the same object in a braided monoidal dagger category are *complementary* when:



(6.1)

The roles of the black and white dots in the previous definition are not obviously interchangeable. Because it concerns symmetric Frobenius structures, however:




(6.2)

Therefore, we could have added two more equalities to (6.1), and 'black is complementary to white' is indeed equivalent to 'white is complementary to black'.

**Example 6.2** (Mutually unbiased bases)**.** Two bases $\{d_i\}$ and $\{e_j\}$ for a finite-dimensional Hilbert space $H$ are *complementary*, or *mutually unbiased*, when $|\langle d_i|e_j\rangle|^2$ is independent of $i$ and $j$. For orthogonal bases, this means

$$|\langle d_i|e_j\rangle|^2 = \frac{\|d_i\|^2\|e_j\|^2}{\dim(H)} \tag{6.3}$$

for all indices $i$ and $j$.

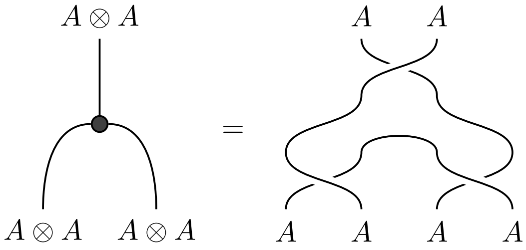
Let $(H, )$ be the commutative Frobenius structure in **FHilb** induced by an orthogonal basis $\{d_i\}$ of $H$, and $(H, )$ that induced by an orthogonal basis $\{e_j\}$. These Frobenius structures are complementary when the bases are mutually unbiased. To see this, put a state $e_j$ on the bottom of (6.1) and an effect $d_i^\dagger$ on top, and use well-pointedness.

We will see the converse of this example in Subsection 6.1.1.

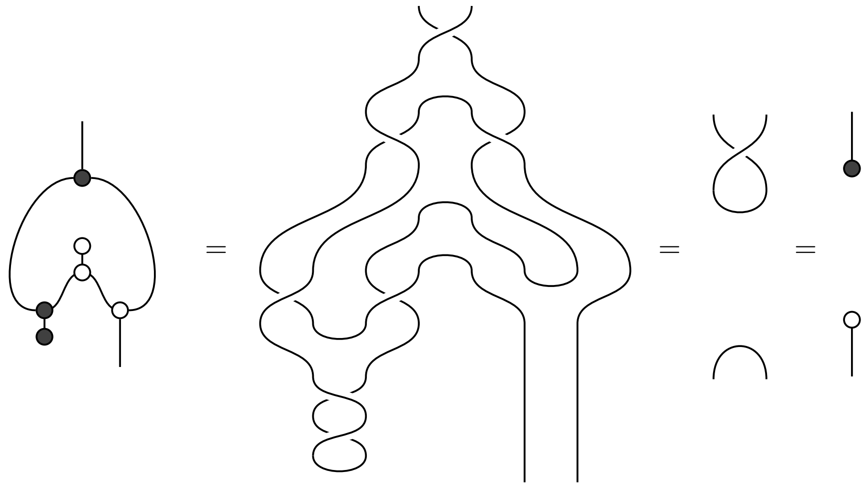
The next lemma provides a large stock of examples of complementary Frobenius structures.

**Lemma 6.3.** *If $A$ is a dagger self-dual object in a braided monoidal category, then the following two Frobenius structures on $A \otimes A$ are complementary: the pair of pants from Lemma 5.9, and its transport across the braiding $\sigma_{A,A}$ as in Lemma 5.16.*

*Proof.* Denote the pair of pants Frobenius structure from Lemma 5.9 by white dots, and its transport across the braiding, the 'twisted knickers', by black dots:




Then straightforward diagrammatic calculation shows:




The other identity in (6.1) follows similarly. □

Combined with Theorem 5.14, the previous lemma says that any symmetric dagger Frobenius structure on $A$ gives rise to a complementary pair of Frobenius structures on $A \otimes A$ in any braided monoidal dagger category.

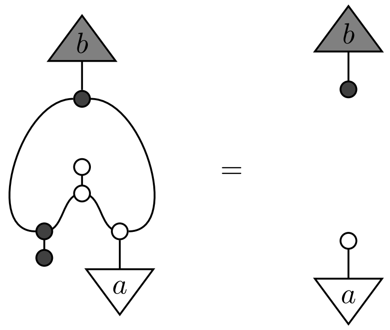
### 6.1.1 Complementary bases

In Example 6.2 we saw that mutually unbiases bases give rise to complementary classical structures in **FHilb**. This subsection proves the converse: complementary classical structures in **FHilb** correspond to mutually unbiased bases.

**Proposition 6.4** (Complementarity in **FHilb**)**.** *The following are equivalent for two commutative dagger Frobenius structures on $H$ in* **FHilb***:*

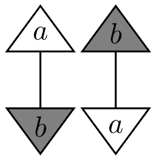
- *they are complementarity;*
- *their orthogonal bases of nonzero copyable states are mutually unbiased, the nonzero copyable states of each basis have the same length, and the product of these two lengths is $\sqrt{\dim(H)}$.*

*Proof.* The complementarity equation (6.1) holds if and only if



(6.4)

for all copyable states $a$ of the white basis and $b$ of the black basis. The left-hand side expands to:



$$= |\langle a|b\rangle|^2$$

The right-hand side of (6.4) equals 1, so complementarity is equivalent to

$$|\langle \tilde{a}|\tilde{b}\rangle|^2 = \frac{1}{|a|^2|b|^2}. \tag{6.5}$$

where tildes represent normalized versions of the states: $\tilde{a} = a/\|a\|$.

In this case

$$1 = \langle \tilde{b}|\tilde{b}\rangle = \sum_a \langle \tilde{b}|\tilde{a}\rangle\langle \tilde{a}|\tilde{b}\rangle = \sum_a \frac{1}{|a|^2|b|^2} = \frac{1}{|b|^2}\sum_a \frac{1}{|a|^2}, \tag{6.6}$$

so $|b|^2 = \sum_a |a|^{-2}$, and all the vectors in the black basis have the same length; and a similar argument shows the same for the white basis. Defining a constant $N = |a|^{-2}|b|^{-2}$, calculation (6.6) gives $1 = \sum_a N = N(\sum_a 1) = N\dim(H)$, so $N = \dim(H)^{-1}$. So it follows from (6.5) that

$$|\langle a|b\rangle|^2 = \frac{|a|^2|b|^2}{\dim(H)}$$

showing that the bases are mutually unbiased.

For the converse, build two commutative dagger Frobenius structures whose nonzero copyable states are exactly the given basis elements. Then (6.5) follows from mutual unbiasedness by the assumption $|a||b| = \sqrt{\dim(H)}$. □

**Example 6.5** (Pauli bases)**.** Here are three bases of the Hilbert space $\mathbb{C}^2$:

$$X \text{ basis:} \quad \left\{ \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} \right\} \tag{6.7}$$

$$Y \text{ basis:} \quad \left\{ \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix} \right\} \tag{6.8}$$

$$Z \text{ basis:} \quad \left\{ \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix} \right\} \tag{6.9}$$

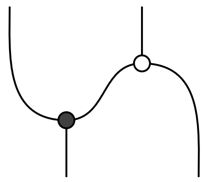
These are all mutually complementary. The terminology is explained by the fact that these bases consist of eigenvectors of the three Pauli matrices that measure spin in the $X$, $Y$ and $Z$ coordinates of a particle in three-dimensional space.

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.

### 6.1.2 Dagger complementarity

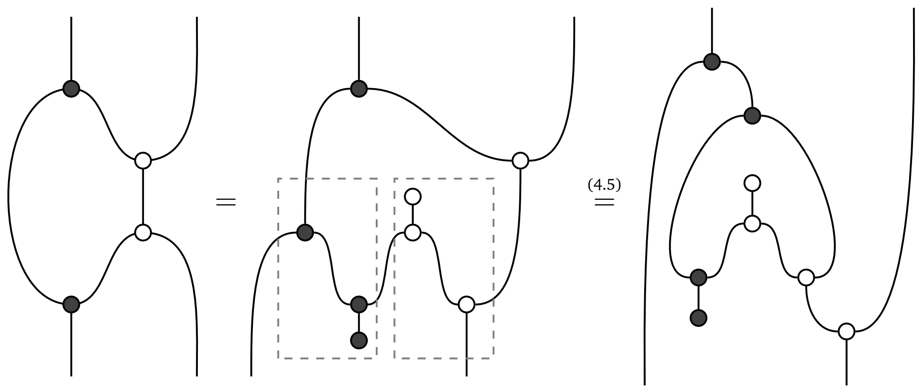
Complementarity an equality of morphisms built from the (co)multiplication and (co)unit of a Frobenius structure. We can also characterize complementarity in terms of daggers, namely as some canonical morphism being unitary. This is the content of the following proposition.

**Proposition 6.6.** *Two symmetric dagger Frobenius structures in a braided monoidal dagger category are complementary if and only if the following endomorphism is unitary:*



(6.10)

*Proof.* Composing (6.10) with its adjoint, we obtain:




(6.11)

Here, the first equality follows from two applications of the noncommutative spider Theorem 5.20 to the dashed areas. Now, if complementarity (6.1) holds then (6.11) equals the identity. Conversely, if the right-hand side of (6.11) 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 (6.1). Therefore the left identity in (6.1) holds if and only if (6.10) is an isometry. A similar argument composing (6.10) with its adjoint in the other order corresponds to the right-hand equality of complementarity (6.1). □

### 6.1.3 Complementary groupoids

Now we investigate what complementarity means in our other example category $\mathbf{Rel}$. It turns out to be a phenomenon similar to mutual unbiasedness. The construction in the following example is a lot like that of Lemma 6.3.

**Example 6.7.** Let $G$ and $H$ be nontrivial groups. Set $A = G \times H$. Let $\mathbf{G}$ be the totally disconnected 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 $\mathbf{G}$ and $\mathbf{H}$ give rise to complementary Frobenius structures.

*Proof.* Consider the left-hand side of (6.1). It expands to

$$\{(a,b) \mid \exists x \in A \colon b = x^{-1} \circ (x \bullet a)\},$$

where we write $\bullet$ for the composition in $\mathbf{G}$, and $\circ$ for the composition in $\mathbf{H}$, and the inverse is taken in $\mathbf{H}$. This set clearly contains the right-hand side of (6.1), which is

$$\{(\mathrm{id}_g, \mathrm{id}_h) \mid g \in \mathrm{Ob}(\mathbf{G}), h \in \mathrm{Ob}(\mathbf{H}))\}.$$

Now consider the rest,

$$\{(a,b) \mid \exists x \colon x \text{ is not an identity in } \mathbf{G}, \text{ and } b = x^{-1} \circ (x \bullet a)\}.$$

Remember that we cannot compose any two morphisms in a groupoid; they have to have matching domain and codomain. By construction, the expression $b = x^{-1} \circ (x \bullet a)$ is only well-defined when $x^{-1} = x$, and then becomes $b = x \circ (x \bullet a)$. But since $a$ is not an identity, $x \bullet a \neq x$, so $x \bullet a$ and $x$ are not composable in $\mathbf{H}$. So the left-hand and right-hand sides of (6.1) 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 6.8** (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* $a \mapsto \big(\mathrm{dom}_{\mathbf{G}}(a), \mathrm{dom}_{\mathbf{H}}(a)\big)$ *is bijective.*

*Proof.* Write $\bullet$ for the multiplication in $\mathbf{G}$, and $\circ$ for that in $\mathbf{H}$. By Proposition 6.6, complementarity is equivalent to unitarity of the morphism (6.10). Unitaries in $\mathbf{Rel}$ are exactly the bijective functions (see Exercise 2.5.6). 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 $e$ and $a$ have the same codomain in $\mathbf{H}$. Thus complementarity holds if and only if for all objects $g$ of $\mathbf{G}$ and $h$ of $\mathbf{H}$ there is a unique $e \in A$ with $\mathbf{G}$-domain $g$ and $\mathbf{H}$-domain $h$. □

In particular: two classical structures in $\mathbf{Rel}$ corresponding to abelian groupoids $\mathbf{G}$ and $\mathbf{H}'$ are complementary exactly when $\mathbf{G}(g,g) \simeq \mathrm{Ob}(\mathbf{H})$ and $\mathbf{H}(h,h) \simeq \mathrm{Ob}(\mathbf{G})$ for each object $g$ of $\mathbf{G}$ and $h$ of the transport $\mathbf{H}$ of $\mathbf{H}'$ across some isomorphism (see Lemma 5.16). In this sense Example 6.7 is the only possible example of complementary classical structures in $\mathbf{Rel}$, up to the generalization that you can 'mix and match' groups.

In $\mathbf{FHilb}$, any classical structure allows a complementary one. The following corollary shows that 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.

**Corollary 6.9.** *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 out of an object* $g$ *is independent of* $g$.

*Proof.* One direction is obvious. We will prove the other, by building a complementary groupoid $\mathbf{H}$.

First off, we may assume that $\mathbf{G}$ is not empty without loss of generality. Pick some object $g_0$, and set $B = \bigcup_{g \in \mathrm{Ob}(\mathbf{G})} \mathbf{G}(g_0, g)$. Construct $\mathbf{H}$ by defining $\mathrm{Ob}(\mathbf{H}) = B$, setting $\mathbf{H}(h, h') = \emptyset$ for distinct $h, h' \in B$, and making the set $\mathbf{H}(h,h) = \mathrm{Ob}(\mathbf{G})$ into a group in some way. For example, 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 $U \cdot V = (U \cup V) \setminus (U \cap V)$ as multiplication. This makes $\mathbf{H}$ into a well-defined groupoid.

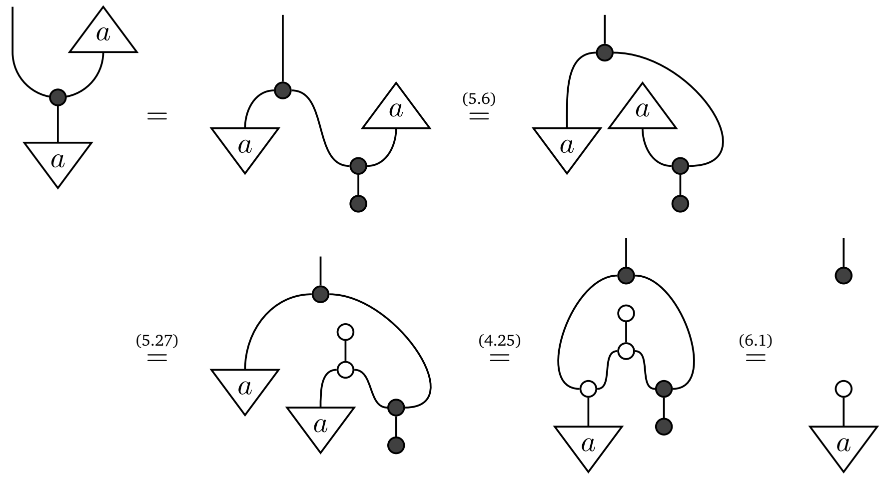
Write $A$ for the set of morphisms of $\mathbf{G}$. Because the cardinality of $B$ is independent of $g_0$ by assumption, the map $a \mapsto \big(\mathrm{dom}_{\mathbf{G}}(a), \mathrm{dom}_{\mathbf{H}}(a)\big)$ is a bijection $A \to \mathrm{Ob}(\mathbf{G}) \times B$. Hence $\mathbf{G}$ and $\mathbf{H}$ satisfy condition (b) of the previous proposition, and are therefore complementary. □

### 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 using column vector notation defined by the other basis, then up to an overall scalar factor, each entry will be unitary. We captured this abstractly with the notion of a *phase* for a Frobenius structure, introduced in Definition 5.39. In other words, a state is unbiased for a dagger Frobenius structure when its phase shift is unitary.

**Lemma 6.10.** *If two symmetric dagger Frobenius structures in a braided monoidal dagger category are complementary, then, up to an idempotent scalar, a state that is self-conjugate and copyable for one is a phase for the other.*

*Proof.* Using the graphical calculus:




These equalities used, in order: the noncommutative spider theorem, symmetry, self-conjugateness, copyability, and complementarity. It follows from copyability that the scalar is idempotent. □

It so happens that the converse of the previous lemma also holds in **FHilb**. This is not the case in **Rel**, see Exercise 6.5.3.

## 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 typical of quantum algorithms that decide on a solution without relying on approximation. The Deutsch–Jozsa algorithms solve 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 difference between no information flow and maximum information flow. In this section we discuss the algorithm and prove its correctness categorically.

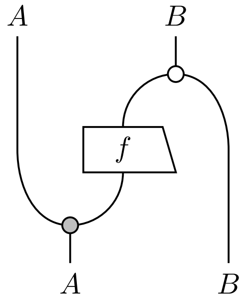
The Deutsch–Jozsa algorithm addresses the following problem. Suppose we have a 2-valued function $A \xrightarrow{f} \{0,1\}$ on a finite set $A$. If the function $f$ takes just a single value on every element of $A$, it is called *constant*. Another possibility is that the function takes the value $0$ on exactly half the elements of $A$, and takes the value $1$ on the other half; in this case it is called *balanced*. Of course, most functions will be 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 these properties holds.

The best classical strategy is rather simple. We have no knowledge of the structure of the function $f$ in general, so we must simply 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 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 $f$ 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 $f$. In a quantum setting, we can only apply unitary gates; so we have to linearize the function $A \xrightarrow{f} \{0,1\}$ to an *oracle*, a unitary map that we can use in the quantum computation.

**Definition 6.11** (Oracle)**.** An *oracle* in a monoidal category is a morphism $A \xrightarrow{f} B$ together with Frobenius structures $\odot$ on $A$ and $\circ$ on $B$ such that the following morphism is unitary:




(6.12)

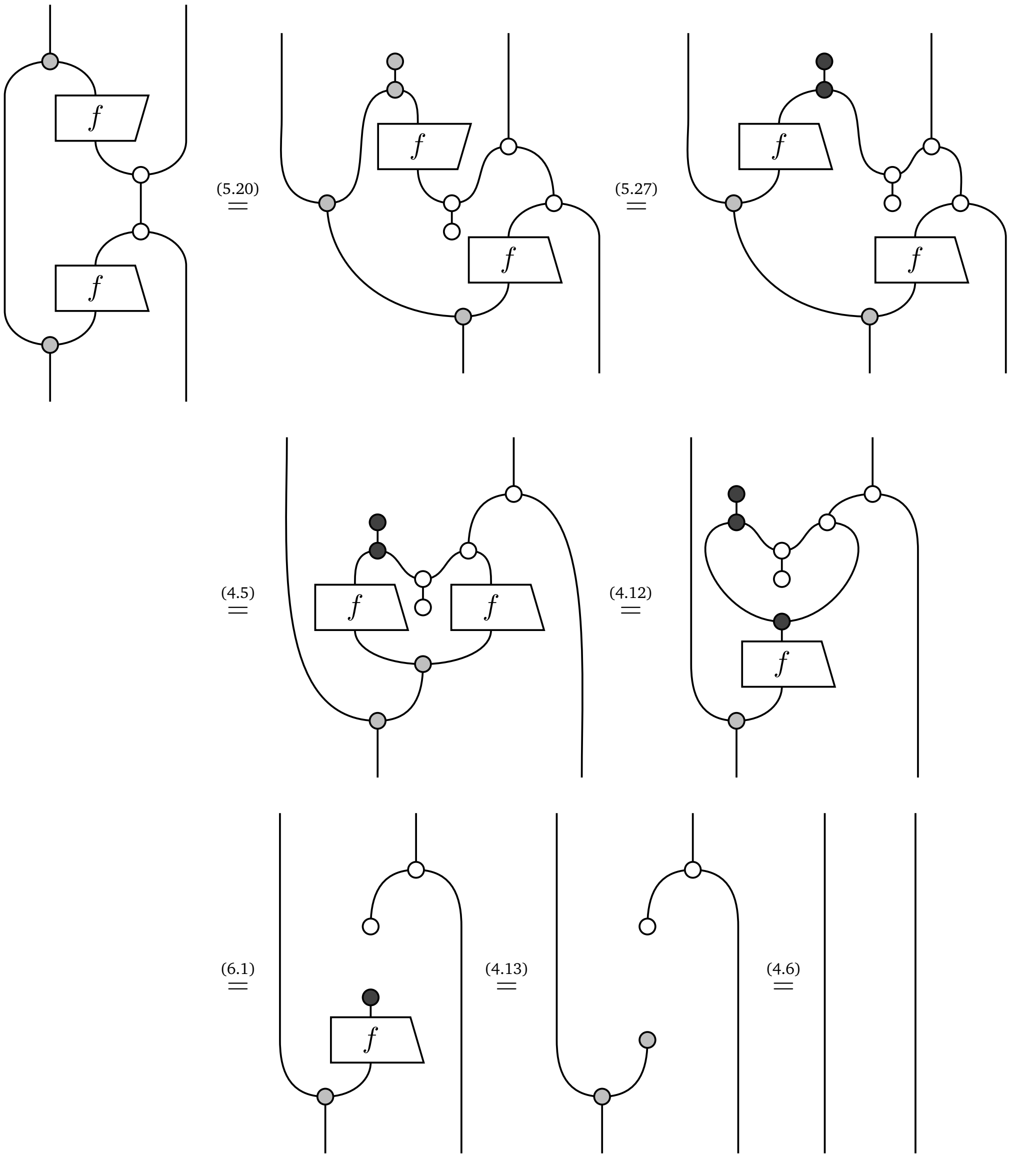
**Example 6.12.** Let $A \xrightarrow{f} B$ be a morphism of $\mathbf{FSet}$. Write $H$ for the $|A|$-dimensional Hilbert space with orthonormal basis $\{a \in A\}$, and $K$ for the Hilbert space with orthonormal basis $B$. The function $f$ induces a morphism $H \to K$ in $\mathbf{FHilb}$ that extends the function $a \mapsto f(a)$. Now choose an orthogonal basis $\{e_i\}$ for $K$ that is mutually unbiased to $B$, with length $\|e_i\|^2 = \dim(K)$. With this basis as the white Frobenius structure, the map (6.12) sends $a \otimes e_i$ to $\langle e_i | f(a)\rangle a \otimes e_i$, where the coefficients have amplitude $|\langle e_i | f(a)\rangle|^2 = \|e_i\|^2 \|f(a)\|^2 / \dim(K) = 1$ by (6.3). Hence (6.12) is unitary, and the morphism $H \to K$ is an oracle. Because it extends the function $f$, we say it is an *oracle for* $f$.

Notice that this makes the function $A \xrightarrow{f} B$ invertible not unlike the *Toffoli gate*, which would change it into the function $A \times B \to A \times B$ given by $(a, b) \mapsto (a, f(a) \oplus b)$, if $A$ and $B$ would consist of binary strings and $\oplus$ was the exclusive or. The change of basis from $B$ to a mutually unbiased one plays the role of a *Fourier transform*.

In fact, the previous example is typical: we now prove that any oracle extends a function between bases. Recall from Corollary 5.34 that functions between bases are comonoid homomorphisms between classical structures, and from Lemma 5.35 that the latter are always self-conjugate.

**Proposition 6.13.** *Let* $(A, \odot)$, $(B, \bullet)$ *and* $(B, \circ)$ *be symmetric dagger Frobenius structures in a braided monoidal dagger category. A self-conjugate comonoid homomorphism* $(A, \odot) \xrightarrow{f} (B, \bullet)$ *is an oracle* $(A, \odot) \to (B, \circ)$ *if and only if* $\bullet$ *is complementary to* $\circ$.

*Proof.* Suppose  and  are complementary, and compose (6.12) 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 (6.12) and its adjoint in the other order similarly gives the identity. Thus $f$ is an oracle.

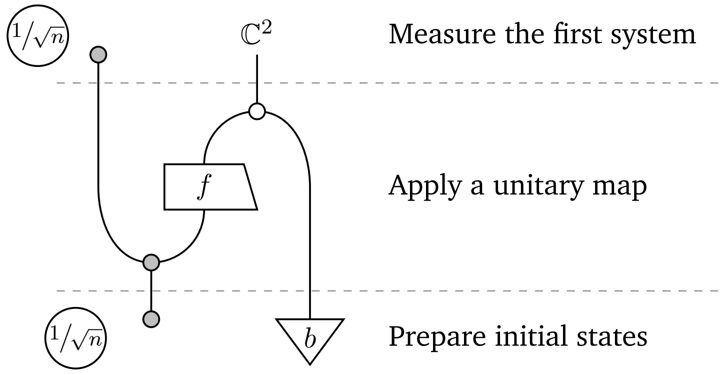
Conversely, if $f$ is an oracle, composing the above computation with a white unit on the bottom right and a gray counit on the top left shows the left equation of (6.1). A similar argument to the composition of (6.12) with its adjoint in the other order gives the other equation, showing that  and  are complementary. □

Notice that the previous proposition resembles Proposition 6.6, just with a morphism $f$ 'in the middle'.

### 6.2.2 The Deutsch–Jozsa algorithm

We can now state the procedure of the Deutsch–Jozsa algorithm itself.

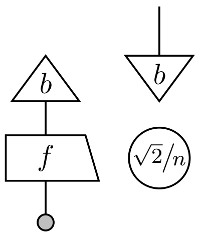
**Definition 6.14** (The Deutsch–Jozsa algorithm)**.** Say that $A$ has $n$ elements, and let $A \xrightarrow{f} \{0,1\}$ be the given function. Extend it to an oracle $H \to \mathbb{C}^2$ as in Example 6.12; the two complementary bases on $\mathbb{C}^2$ are the computational basis and the $X$ basis 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**:




(6.13)

The dashed horizontal lines separate the different stages of the procedure. In the language of states and effects of Sections 1.1.3 and 2.4: first prepare two systems in initial states, one in the maximally entangled 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 entangled effect for the gray classical structure. The diagram (6.13) 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 6.15.** *The Deutsch–Jozsa algorithm* (6.13) *simplifies to:*




(6.14)

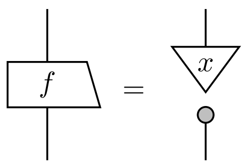
*Proof.* Duplicate the copyable state $\sqrt{2}b$ through the white dot in (6.13), and apply the noncommutative Spider Theorem 5.20 to the cluster of gray dots. □

## 6.2.3 Correctness

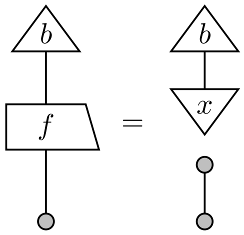
We now set out to prove correctness of the Deutsch–Jozsa algorithm.

**Lemma 6.16** (The constant case)**.** *If the function $A \xrightarrow{f} \{0,1\}$ is constant, then the history described in diagram* (6.13) *is certain.*

*Proof.* Suppose $f(a) = x$ for all $a \in A$. Then the oracle $H \xrightarrow{f} \mathbb{C}^2$ decomposes as:



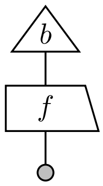
Thus the amplitude of the main component of the quantum history (6.14) is:




Hence the norm of (6.14) is 1. □

**Lemma 6.17** (The balanced case)**.** *If the function* $A \xrightarrow{f} \{0,1\}$ *is balanced, then the history described in diagram* (6.13) *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 (6.14) is 0. □

**Theorem 6.18** (Deutsch–Jozsa is correct)**.** *The Deutsch–Jozsa algorithm* (6.13) *correctly identifies constant functions* $A \xrightarrow{f} \{0,1\}$.

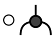
*Proof.* The squared norm of the state (6.14) is the probability of the history occurring. The previous two lemmas show that the history (6.13) is a perfect test for discriminating constant and balanced functions. □

## 6.3 Bialgebras

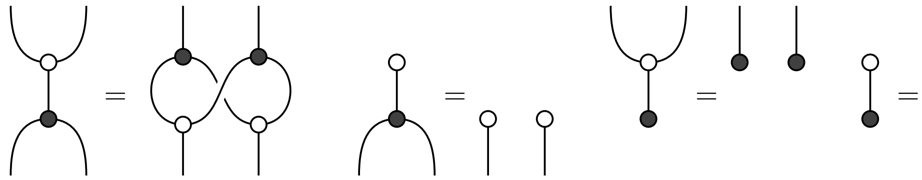
As we saw in Proposition 6.4, complementary classical structures **FHilb** are mutually unbiased bases. One common way to construct mutually unbiased bases is the following. Let $G$ be a finite group, and consider the Hilbert space for which $\{g \in G\}$ is an orthonormal basis. Defining

 $: g \mapsto g \otimes g$  $: g \mapsto 1$ (6.15)

 $: g \otimes h \mapsto gh$  $: 1 \mapsto \sum_{g \in G} g$ (6.16)

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 6.19** (Bialgebra, dagger bialgebra)**.** A *bialgebra* in a braided monoidal category consists of a monoid ( , ) and a comonoid ( , ) on the same object, satisfying the following *bialgebra laws*:



(6.17)

The last equation is not missing a picture, because we are drawing $\mathrm{id}_I$ as the empty picture (1.5). 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 6.20.** 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:

$$A \xrightarrow{\binom{\mathrm{id}_A}{\mathrm{id}_A}} A \oplus A \qquad 0 \xrightarrow{0_{0,A}} A \qquad A \oplus A \xrightarrow{(\mathrm{id}_A\ \mathrm{id}_A)} A \qquad A \xrightarrow{0_{A,0}} 0$$

- Any monoid $M$ is a bialgebra in **Set**, by choosing

$$: m \mapsto (m, m) \qquad : m \mapsto \bullet \qquad : (m, n) \mapsto mn \qquad : \bullet \mapsto 1_M.$$

  Notice that  and  can also make $M$ into a Frobenius structure in **Rel** as in Example 5.3, but with different  and .

- Any monoid $M$ in **FSet** induces a bialgebra in **FHilb** as follows. Let $(A, , )$ be the group algebra; see Example 5.2. Define

$$: m \mapsto m \otimes m \qquad\qquad : m \mapsto 1_M.$$

  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 **FSet** satisfying some additional properties always arise from groups like this.

  Any monoid in **Set** induces a bialgebra in **Rel** in a similar way.

- The space of complex polynomials in one variable $\mathbb{C}[x]$ gives rise to a commutative dagger bialgebra in **Hilb**. The Hilbert space in question, also called *Fock space* has $\{1, x, x^2, x^3, \ldots\}$ as an orthonormal basis, and multiplication $: \mathbb{C}[x] \otimes \mathbb{C}[x] \to \mathbb{C}[x]$ is defined by

$$x^n \otimes x^m \mapsto \sqrt{\frac{(m+n)!}{m!\,n!}}\, x^{m+n}.$$

  This is a heuristic idea, since the resulting linear map $\mathbb{C}[x] \otimes \mathbb{C}[x] \to \mathbb{C}[x]$ is unbounded, and hence not technically a morphism in **Hilb**. However, the categorical approach can still be extremely useful.

The following concise formulation is a good way to remember the bialgebra laws; compare Lemma 5.53.

**Lemma 6.21.** *The following are equivalent in a braided monoidal category:*

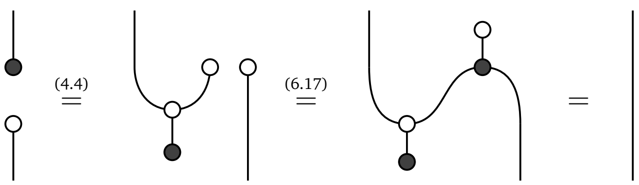
- *a comonoid $(A, , )$ and monoid $(A, , )$ form a bialgebra;*
- *and are comonoid homomorphisms;*
- *and are monoid homomorphisms.*

*Proof.* The canonical comonoid structure on $A \otimes A$ is that of Lemma 4.8. Unfolding what it means for  to be a comonoid homomorphism: comultiplication preservation gives the first of the bialgebra laws (6.17); 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 opposite extremes. The following theorem shows that both cannot happen simultaneously, except in the trivial case. What leads to the degeneracy is the fact that the Frobenius law (5.1) equates *connected* diagrams, whereas the bialgebra laws (6.17) equate connected diagrams with *disconnected* ones.

**Theorem 6.22** (Frobenius bialgebras are trivial)**.** *If a monoid $(A, , )$ and comonoid $(A, , )$ form both a Frobenius structure and a bialgebra in a braided monoidal category, then $A \simeq I$.*

*Proof.* We will show that  and  are inverse morphisms. The bialgebra laws (6.17) already require $\circ = \mathrm{id}_I$. For the other composite:




The first equality is counitality, the second equality is the first bialgebra law, and the last equality follows from Theorem 5.14. □

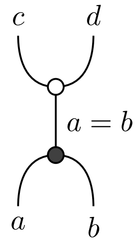
### 6.3.1 Strong complementarity

We now investigate the relationship between complementarity and bialgebras.

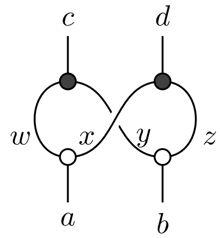
**Lemma 6.23.** *Any two complementary special dagger Frobenius structures in* **Rel** *form a bialgebra.*

The bialgebra structure is between the monoid part of one structure and the comonoid part of the other. This must be the case, since we saw that Frobenius bialgebras are trivial in Theorem 6.22.

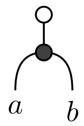
*Proof.* Using Proposition 6.8, we may assume that we are dealing with a group $(G, \circ, 1)$ and an indiscrete groupoid $(G, \bullet)$ on the same set of morphisms. Then:



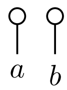

$$\iff \exists w, x, y, z \in G\colon \begin{bmatrix} a = w \circ x \\ b = y \circ z \\ c = w \bullet y \\ d = x \bullet z \end{bmatrix} \iff$$




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 6.8. □

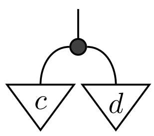
Hence, in **Rel**, the bialgebra law is a property hidden behind complementarity, and we may add it for free. In **FHilb** the situation is different: complementarity Frobenius structures often do not form a bialgebra, as the following counterexample demonstrates.

**Example 6.24.** 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 (black dot). The orthogonal basis $\{\begin{pmatrix} e^{i\varphi} \\ e^{i\theta}\end{pmatrix}, \begin{pmatrix} e^{i\varphi} \\ -e^{i\theta}\end{pmatrix}\}$ gives it a Frobenius structure (white dot). These two Frobenius structures are complementary, but can only form a bialgebra if $\varphi = 2\varphi$ and $\theta = 2\theta \bmod 2\pi$.

*Proof.* Write $\{a, b\}$ for the computational basis, and $\{c, d\}$ for the other one. Complementarity follows from Proposition 6.4: the two bases are mutually unbiased as $|\langle a|c\rangle|^2 = |e^{i\theta}|^2 = 1 = |\langle a|d\rangle|^2$ equals $\| \langle b|c\rangle|^2 = |e^{i\varphi}|^2 = 1 = |\langle b|d\rangle|^2$, and the product of lengths of basis vectors satisfies

$$\|a\|^2\|c\|^2 = \langle c|c\rangle = |e^{i\varphi}|^2 + |e^{i\theta}|^2 = 2 = \dim(\mathbb{C}^2).$$

Plugging in $c \otimes d$, the first bialgebra law (6.17) holds if and only if the state




$$= \begin{pmatrix} e^{2i\varphi} \\ -e^{2i\theta} \end{pmatrix}$$

is copyable for (white dot) — that is, when it is one of $c$ or $d$. But that is only the case when $\varphi = 2\varphi$ and $\theta = 2\theta \bmod 2\pi$. □

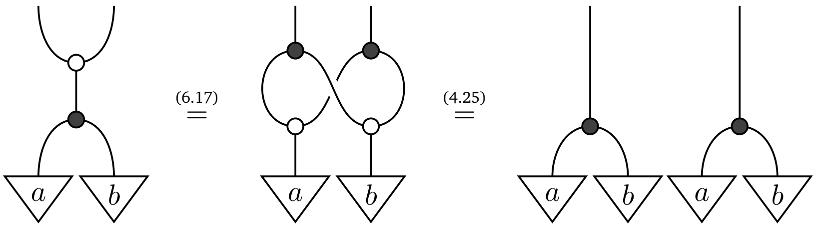
This motivates the following definition.

**Definition 6.25** (Strong complementarity)**.** In a braided monoidal dagger category, two dagger symmetric Frobenius structures are *strongly complementary* when they are complementary, and also form a bialgebra.

Example 6.24 showed that strong complementarity is strictly stronger than complementarity. Strongly complementary pairs of Frobenius algebras enjoy extra properties, such as the following.

**Lemma 6.26.** *Let and be dagger Frobenius structures that form a bialgebra in a braided monoidal dagger category. The set of copyable states for is a monoid under .*

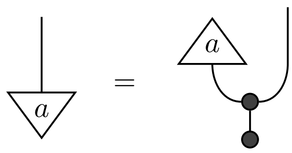
*Proof.* Associativity (4.5) is immediate. Unitality (4.6) comes down to the third bialgebra law (6.17): is copyable for . We have to prove well-definedness. Let $a$ and $b$ be copyable states for . Then:




Hence -copyable states are indeed closed under . □

Note the resemblance of the previous lemma to the phase group (5.30). The following corollary takes this similarity further.

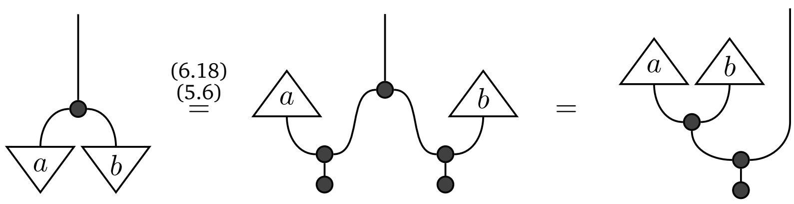
**Corollary 6.27.** *Let and be symmetric dagger Frobenius structures that form a bialgebra in a braided monoidal dagger category. The set of copyable states $a$ for satisfying*




(6.18)

*is a group under .*

*Proof.* Notice that is *self-conjugate* in the sense of (6.18). The proof that self-conjugate states have inverses is the same as in Proposition 5.43. We have to prove well-definedness. Suppose states $a$ and $b$ satisfy (6.18). Then:




The last equation follows from the noncommutative Spider theorem 5.20 and symmetry (5.6). Hence self-conjugate states are indeed closed under . □

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 (6.15) and (6.16), are in fact the only way to generate strongly complementary pairs in **FHilb**.

**Theorem 6.28.** *Pairs of symmetric dagger Frobenius structures that form a bialgebra in* **FHilb***, one of which is commutative, correspond to finite groups via* (6.15) *and* (6.16).

*Proof.* We already saw that (6.15) and (6.16) 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 bialgebra on $H$ in **FHilb**. If is commutative, then its nonzero copyable states form an orthogonal basis for $H$. By Corollary 6.27 and Lemma 5.35, these form a group under . 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 space whose dimension is not a prime power.

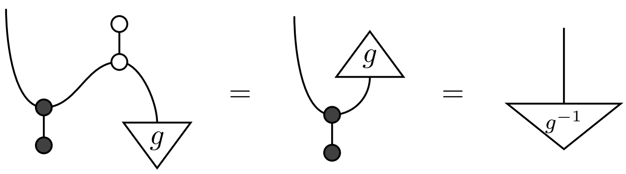
We can now also prove the converse of Example 6.24.

**Corollary 6.29.** *If two symmetric dagger Frobenius structures in* **FHilb** *form a bialgebra and one of them is commutative, then they are complementary.*

*Proof.* By the previous theorem, (6.15) and (6.16) define the Frobenius structures from a finite group $G$. In that case, the bialgebra laws (6.17) are easily verified by hand: both sides of the first bialgebra law evaluate to $g \otimes h \mapsto gh \otimes gh$; the second bialgebra law becomes $g \otimes h \mapsto 1$; the third $1 \mapsto 1_G \otimes 1_G$; and the fourth $1 \mapsto 1$. □

## 6.3.2 Hopf algebras

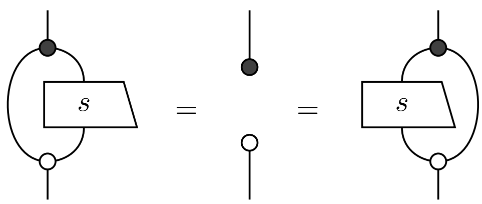
By Theorem 6.28, for (strongly) complementary symmetric dagger Frobenius structures in **FHilb**, one of which is commutative, the map (6.2) is the linear extension of the inverse operation $g \mapsto g^{-1}$ of a group:




The very same calculation holds for complementary Frobenius structures in **Rel**, because we may assume that is a group and is a totally disconnected groupoid thanks to Proposition 6.8.

This leads to the following definition.

**Definition 6.30** (Antipode, Hopf algebra)**.** An *antipode* for a monoid $(A, \ , \ )$ and comonoid $(A, \ , \ )$ in a monoidal category is a morphism $A \xrightarrow{s} A$ satisfying the following equations:




(6.19)

A bialgebra in a braided monoidal category equipped with an antipode is called a *Hopf algebra*, and (6.19) is called the *Hopf law*.

Strongly complementary symmetric dagger Frobenius structures are by definition Hopf algebras, with (6.2) as antipode. There are many Hopf algebras that do not arise in this way. Hopf algebras are also called *quantum groups*; the following theorem shows that they indeed generalize groups.

**Theorem 6.31.** *Hopf algebras in* $\mathbf{Set}$ *are exactly groups.*

*Proof.* Suppose that $(G, [\text{black multiplication}], [\text{black unit}], [\text{white comultiplication}], [\text{white counit}], s)$ is a Hopf algebra in $\mathbf{Set}$. Then $(G, [\text{black multiplication}], [\text{black unit}])$ is a monoid (in $\mathbf{Set}$). Define inverses by $g^{-1} = s(g)$. Because [white comultiplication] must be the map $g \mapsto (g, g)$ (see Exercise 4.5.2), it follows from the Hopf law (6.19) that $g^{-1}g = 1 = gg^{-1}$, and hence that $G$ is a group.

Conversely, let $G$ be a group. Defining

$$[\text{white comultiplication}]\colon g \mapsto (g, g) \qquad [\text{white counit}]\colon g \mapsto \bullet$$
$$[\text{black multiplication}]\colon (g, h) \mapsto gh \qquad [\text{black unit}]\colon \bullet \mapsto 1$$
$$s\colon g \mapsto g^{-1}$$

gives $G$ the structure of a Hopf algebra. □

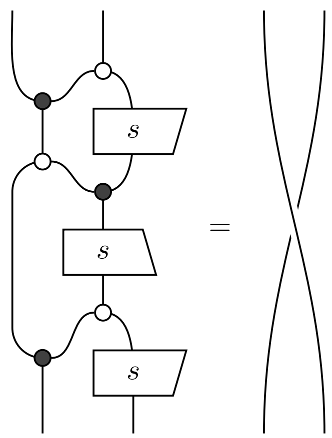
# 6.4 Qubit gates

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 show that a basic property of quantum computation really holds more generally, and only depends on (strong) complementarity: namely, a swap gate can be built using three CNOT 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.

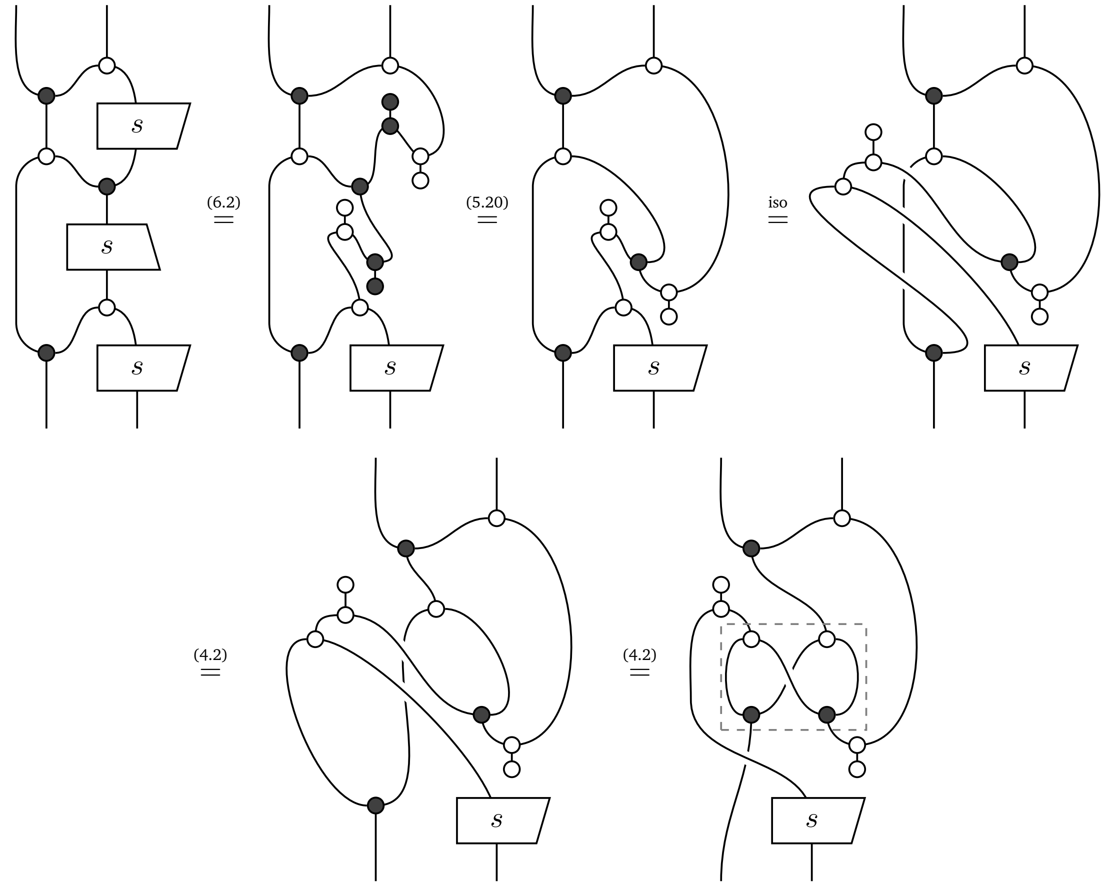
**Theorem 6.32** (Swap via three CNOTs)**.** *Let* $([\text{black multiplication}], [\text{black unit}])$ *and* $([\text{white comultiplication}], [\text{white counit}])$ *be complementary classical structures in a braided monoidal dagger category. If they are strongly complementary, then the following equation holds, where* $s$ *is the morphism* (6.2)*:*




(6.20)

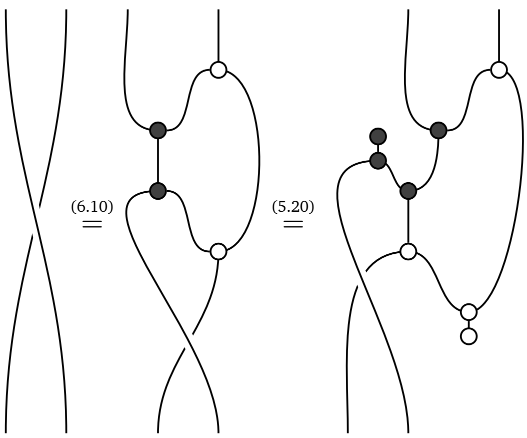
*In fact, equation* (6.20) *holds if and only if the first equation of* (6.17) *does.*

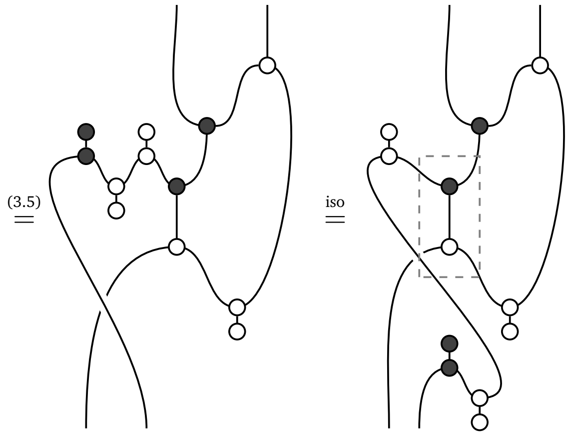
*Proof.* First, rewrite the left-hand side of (6.20):




The second equality uses the (noncommutative) black spider Theorem 5.20, the fourth uses cocommmutativity of , and fifth uses the (commutative) white spider Theorem 5.22.

Rewrite the right-hand side similarly:






The first equality comes from Proposition 6.6.

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 bits 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 (6.10), and three of the form (6.2).

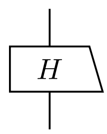
**Example 6.33.** In the category **FHilb**, fix $A$ to be the qubit $\mathbb{C}^2$. And we will let ( , ) be defined by the computational basis $\{|0\rangle, |1\rangle\}$, and ( , ) by the $X$ basis from Example 6.5. Then the three antipodes (6.2) become identities.

Furthermore, the three unitaries of the form (6.10) indeed reduce to three CNOT gates. 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 $|0\rangle$.

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{6.21}$$

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 Lemma 5.16).

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \tag{6.22}$$

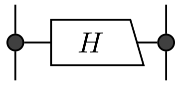



## 6.4.2 Controlled phases

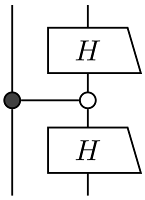
In addition to the CNOT gate, we can now also define the CZ gate abstractly. This gate performs a $Z$ phase shift on the second qubit when the first (control) qubit is $|1\rangle$, and leaves it alone when the first qubit is $|0\rangle$.

In the following lemma, we will draw dots loosely, as in Section 5.5.3. This is allowed, because we are dealing with classical structures.

**Lemma 6.34.** *The CZ gate in* **FHilb** *can be defined as follows.*

*CZ* :=  (6.23)

*Proof.* We can rewrite equation (6.23) as follows.

CZ $\overset{(5.13)}{=}$ 

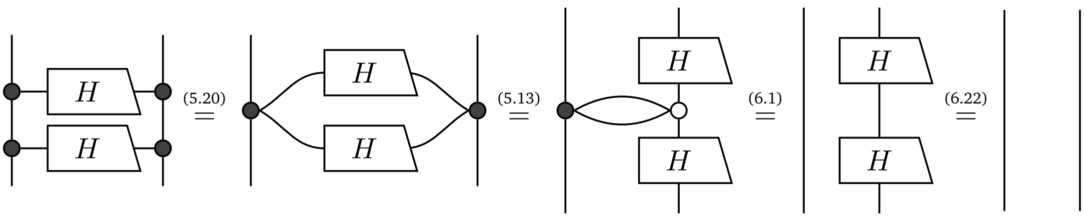
Hence

$$\text{CZ} = (\text{id} \otimes H) \circ \text{CNOT} \circ (\text{id} \otimes H) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

This is indeed the controlled Z gate. □

**Proposition 6.35** (CZ has order two)**.** *If* $(A,$ $)$ *and* $(A,$ $)$ *are complementary classical structures in a braided monoidal dagger category, and* $A \xrightarrow{H} A$ *satisfies* $H \circ H = \text{id}_A$*, then* (6.23) *makes sense and satisfies CZ* $\circ$ *CZ* $= \text{id}$.

*Proof.* Easy graphical manipulation:

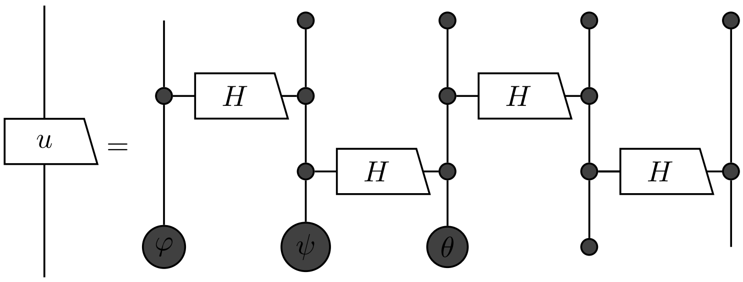


The third equality uses Proposition 6.6. □

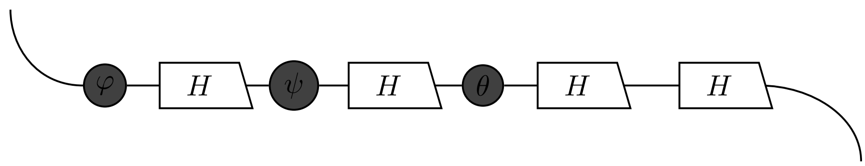
### 6.4.3 Single qubit gates

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 $\varphi, \psi, \theta$ such that $u = Z_\theta \circ X_\psi \circ Z_\varphi$, where $Z_\theta$ is the unitary rotation in the $Z$ basis over angle $\theta$, and $X_\varphi$ in the $X$ basis over angle $\varphi$. Therefore we can implement such unitaries abstractly using just CZ-gates and Hadamard gates.

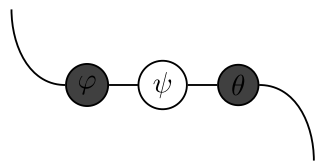
**Theorem 6.36.** *If a unitary* $\mathbb{C}^2 \xrightarrow{u} \mathbb{C}^2$ *in* **FHilb** *has Euler angles* $\varphi, \psi, \theta$*, then:*

 (6.24)

*Proof.* By using the Phased spider Corollary 5.45 equation (6.24) reduces to



But by Lemma 5.16, this is just:

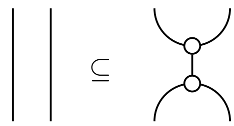


which equals $u$, by definition of the Euler angles. □

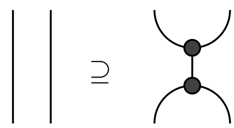
## 6.5 Exercises

**Exercise 6.5.1.** Let $(G, \circ)$ and $(G, \bullet)$ be two complementary groupoids (see Proposition 6.8).

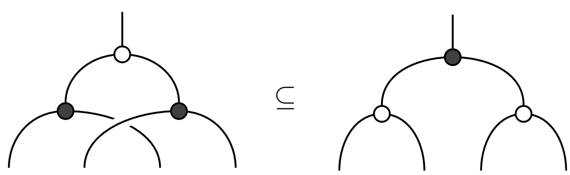
(a) Assume that $(G, \circ)$ is a group. Show that:



(b) Assume that $(G, \circ)$ is a group. Show that:



(c) Assume that the corresponding Frobenius structures in $\mathbf{Rel}$ form a bialgebra. Show that:



Compare this to the Eckmann–Hilton property of Exercise 4.5.3.

**Exercise 6.5.2.** Let $A$ be a set with a prime number of elements. Show that pairs of complementary Frobenius structures on $A$ in $\mathbf{Rel}$ correspond to groups whose underlying set is $A$.

**Exercise 6.5.3.** Consider a special dagger Frobenius structure in $\mathbf{Rel}$ corresponding to a groupoid $\mathbf{G}$.

(a) Show that 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 Lemma 6.10 is false.

**Exercise 6.5.4.** We can recognize whether a monoid-comonoid pair is a bialgebra or a Hopf algebra by inspecting its category of modules and module homomorphisms (see Section 5.6). Consider a bialgebra in a monoidal category $\mathbf{C}$.

(a) Show that the category of modules is also a monoidal category under the tensor product inherited from $\mathbf{C}$.

(b) Show that the bialgebra is in fact a Hopf algebra when the category of modules is compact.

(c) Show that the category of modules is compact when the bialgebra is a Hopf algebra.

**Exercise 6.5.5.** 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 $\tinycomult[blackdot] \colon \mathbb{C}^n \to \mathbb{C}^n \otimes \mathbb{C}^n$ by $e_i \mapsto e_i \otimes e_i$, and $\tinymult[whitedot] \colon \mathbb{C}^n \otimes \mathbb{C}^n \to \mathbb{C}^n$ by $e_i \otimes e_j \mapsto e_{L_{ij}}$. Show that these two morphisms in **FHilb** satisfy the first bialgebra law (6.17). (Hint: use Proposition 6.6.) Note that $\tinymult[whitedot]$ need not be associative or unital.

**Exercise 6.5.6.** This exercise is about *property* versus *structure*. (See also Exercise 4.5.2.)

(a) Suppose that a category $\mathbf{C}$ has products. Show that any monoid in $\mathbf{C}$ has a unique bialgebra structure.

(b) Is being a Hopf algebra a property or a structure? In other words: can a bialgebra have more than one antipode?

**Exercise 6.5.7.** Let $F \colon \mathbf{C} \to \mathbf{D}$ be a monoidal dagger functor between monoidal dagger categories. Suppose that $(A, \tinymult[blackdot], \tinyunit[blackdot], \tinycomult[blackdot], \tinycounit[blackdot])$ and $(A, \tinymult[whitedot], \tinyunit[whitedot], \tinycomult[whitedot], \tinycounit[whitedot])$ 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 [**?**]. Its mathematical formulation in terms of mutually unbiased bases is due to Schwinger in 1960 [**?**]. The abstract formulation in terms of classical structures we used was first given by Coecke and Duncan in 2008 [**?**]. (Terminology warning: some authors require complementary Frobenius structures to be special, leading to an extra scalar factor in Definition 6.1.) Strong complementarity was first discussed in that article, too, and the ensuing Theorem 6.28 is due to Coecke, Duncan, Kissinger and Wang in 2012 [**?**]. The relationship between Latin squares and complementary structures explored in Exercise 6.5.5 is due to Ben Musto in 2014.

The abstract description of the Deutsch–Jozsa algorithm is due to Vicary in 2013 [**?**]. That paper includes the observation of Proposition 6.6, 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 [**?**]. See also work by Duncan and Perdrix from 2009 for more abstract results on Euler angles [**?**].

Bialgebras and Hopf algebras are the starting point for the theory of quantum groups [**?**, **?**]. They have been around in algebraic form since the 1960s, when Heinz Hopf first studied them [**?**]. Graphical notation for them is becoming more standard now, with so-called Sweedler notation as a middle ground [**?**].

# 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. 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 dagger compact 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 central *CP–construction*. 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 quantum systems and only classical systems. Section 7.3 axiomatizes the former subcategory, and treats full-blown quantum teleportation categorically, complete with mixed states and classical communication. Section 7.4 considers the latter subcategory, and considers no-broadcasting theorems as mixed versions of the no-cloning theorem of Section 4.3. Finally, Section 7.5 shows that the CP–construction respects linear structure.

## 7.1 Completely positive maps

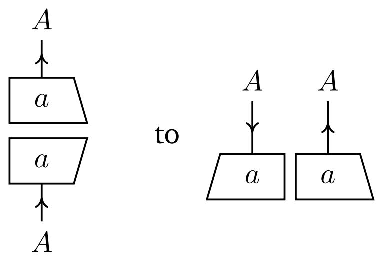
In this section we investigate evolution of mixed states of systems, by which we mean procedures that send mixed states to mixed states. First, we define mixed states themselves, as in Section 0.3.4, and then extrapolate. It turns out that the evolutions we are after correspond to completely positive 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 7.29).

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). 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)**.** 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*.

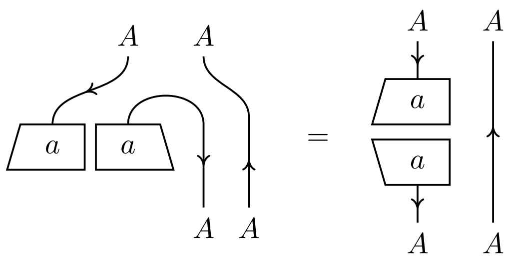
We will sometimes write $\sqrt{m}$ for $f$ to indicate that $m$ has a 'square root' and is hence positive. However, notice that such a morphism $\sqrt{m}$ is by no means unique.

**Example 7.2.** In our example categories:

- Positive matrices in **FHilb** come down to linear maps $\mathbb{C} \to \mathbb{M}_n$ that send 1 to a positive matrix $f \in \mathbb{M}_n$; use Example 4.13. Pure states correspond to positive matrices of rank 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 0.57.
- Positive matrices $I \to A \times A$ in **Rel** come down to subsets $R \subseteq A \times A$ that are symmetric and satisfy $aRa$ when $aRb$; see Exercise 2.5.6. 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 generalise from pure states to mixed states. The final two steps of our process reformulate and generalize this further.

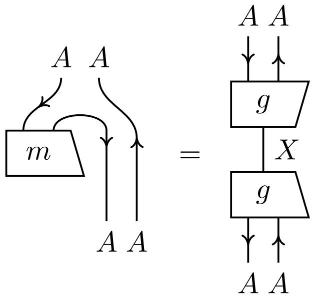
The third step is a conceptual leap, that moves from the positive matrix $I \xrightarrow{m} A^* \otimes A$ to the map $A^* \otimes A \to A^* \otimes A$ that multiplies on the left with the matrix $m$; compare also the Cayley embedding of Proposition 4.14:




(7.2)

This morphism is clearly positive. The following lemma shows the converse, so that this reformulation again loses no information.

**Lemma 7.3.** *If a morphism $I \xrightarrow{m} A^* \otimes A$ in* **FHilb** *satisfies*

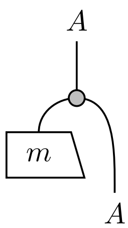


(7.3)

*then it is a positive matrix.*

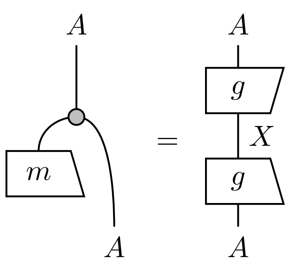
*Proof.* For any morphism $H \xrightarrow{f} H$ in **FHilb**, it follows from the Kronecker product (29) that $f \otimes \mathrm{id}_K$ is a block diagonal matrix; the $\dim(K)$ many diagonal blocks are simply the matrix of $f$. Hence $f \otimes \mathrm{id}_K$ is diagonalizable precisely when $f$ is, and the eigenvalues of $f \otimes \mathrm{id}_K$ are simply ($\dim(K)$ many copies of) the eigenvalues of $f$. In particular, $f \otimes \mathrm{id}_K$ 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. □

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)**.** A *mixed state* of a dagger Frobenius structure $(A, \text{—}, \text{—})$ in a monoidal dagger category is a morphism $I \xrightarrow{m} A$ satisfying



(7.4)

for some object $X$ and some morphism $A \xrightarrow{g} X$.

We will sometimes write $\sqrt[\circ]{m}$ instead of $g$, even though it is not unique.

**Example 7.5.** In our example categories:

- Recall from Example 4.13 that the pair of pants monoid on $A = \mathbb{C}^n$ in $\mathbf{FHilb}$ 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 0.57.

  In general, recall from Theorem 5.29 dagger Frobenius structures in $\mathbf{FHilb}$ correspond to finite-dimensional C*-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.

- Recall from Theorem 5.36 that special dagger Frobenius structure in $\mathbf{Rel}$ 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 2.5.6, 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

As we have seen in Sections 5.3.2 and 5.4.1, we may think of Frobenius structures as comprising *observables*, *i.e.* self-adjoint operators $A \to A$. In this section we will develop 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 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). Let $(A, \tinymult, \tinyunit)$ and $(B, \tinymult, \tinyunit)$ be dagger Frobenius structures in a dagger monoidal category. 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 2.32; luckily contexts will hardly arise where it's difficult to differentiate between the two notions.

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 so-called *completely positive* maps.

**Definition 7.7** (Completely positive map)**.** Let $(A, \mult, \unit)$ and $(B, \mult, \unit)$ be dagger Frobenius structures in a dagger monoidal category. 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 $(E, \blackmult, \blackunit)$.

The next two subsections investigate the completely positive maps in our example categories **FHilb** and **Rel**.

### 7.1.3 Evolution and measurement

In the category **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 **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 4.13 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 measurement with $n$ outcomes (see Definition 0.53). 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 Lemma 7.20 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 measurement (see Definition 0.60), $|i\rangle \mapsto p_i$ 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 measurement. Hence a completely positive map from a pair of pants Frobenius structure to a classical structure corresponds to a *measurement*, generalizing Lemma 5.50.

- A completely positive map $\mathbb{C} \to A^* \otimes A$ is precisely (the *preparation* of) a mixed state. This 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 **Rel** of sets and relations, Frobenius structures correspond to groupoids by Theorem 5.36. Just like completely positive maps in $\mathbf{FHilb}$ only care about positivity, and not the multiplication of the involved Frobenius structure, completely positive maps in $\mathbf{Rel}$ only care about inverses, and not the multiplication of the groupoids.

**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.** *A morphism* $\mathbf{G} \xrightarrow{R} \mathbf{H}$ *in the category* $\mathbf{Rel}$ *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. □

The characterisation of completely positive maps in $\mathbf{Rel}$ of the previous proposition is the source of many ways in which $\mathbf{Rel}$ differs from $\mathbf{FHilb}$. 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 be quantum but turn out to be 'accidentally' true in $\mathbf{FHilb}$. See for example Section 7.4.2 later. For another example: a positive map between Frobenius structures in $\mathbf{FHilb}$, 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 (mere) 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 $(-1,-1) \in R$. □

## 7.2 Categories of completely positive maps

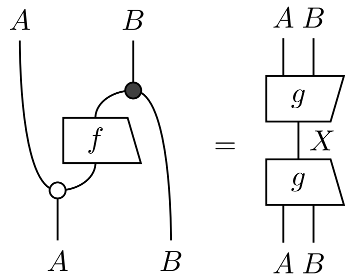
This section describes the main construction of the chapter: starting with a category of pure states, it constructs the corresponding category of mixed states. We start by characterizing Definition 7.7 of completely positive maps from an operational form into a more convenient structural form.

### 7.2.1 The CP–condition

As we saw in Example 7.5, a mixed state of a Frobenius structure $(A, \curlywedge, \circ)$ is the special case of a completely positive map $I \to A$. The condition characterizing when a map is completely positive that we will end up with is a generalization of equation (7.4).

For this proof, we will need the same mild assumption as we did in the third step of Section 7.1.1. Namely that if $(A, \curlywedge, \circ)$ is a dagger Frobenius structure and $f \otimes \mathrm{id}_A$ 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 $\circ\!\!\circ$ 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**.

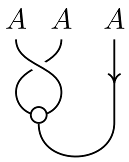
**Lemma 7.12** (CP–condition)**.** *Let $(A, \curlywedge, \circ)$ and $(B, \curlywedge, \bullet)$ be dagger Frobenius structures in a braided monoidal dagger category that is positively monoidal. If $A \xrightarrow{f} B$ is completely positive, then*




(7.5)

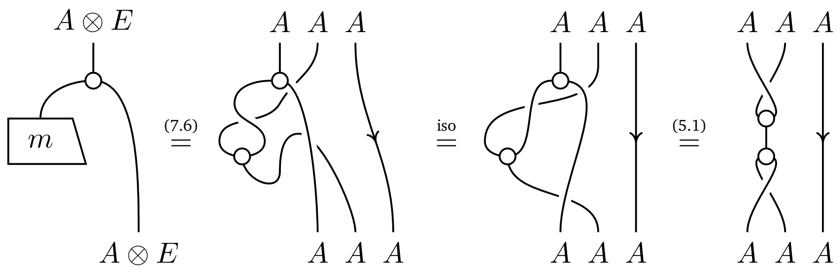
*for some object $X$ and some morphism $A \otimes B \xrightarrow{g} X$.*

*Proof.* Let $E$ be the pair of pants monoid $A \otimes A^*$, and define $I \xrightarrow{m} A \otimes E$ as:



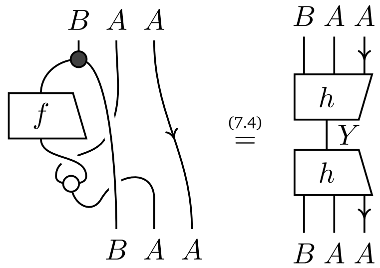

(7.6)

Then $m$ is a mixed state:



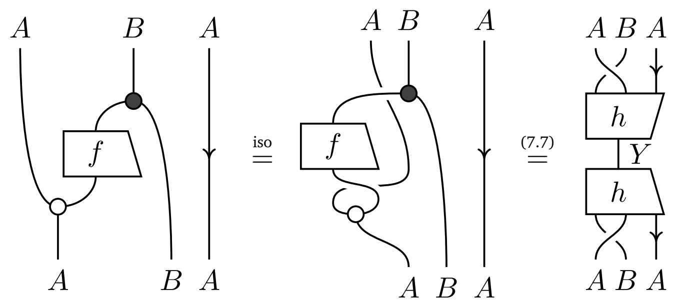

The first equality just unfolds the definition of $m$, whereas the third equality uses the

Frobenius law. Now $(f \otimes \mathrm{id}_E) \circ m$ is a mixed state:




(7.7)

for some object $Y$ and morphism $h$. Hence:

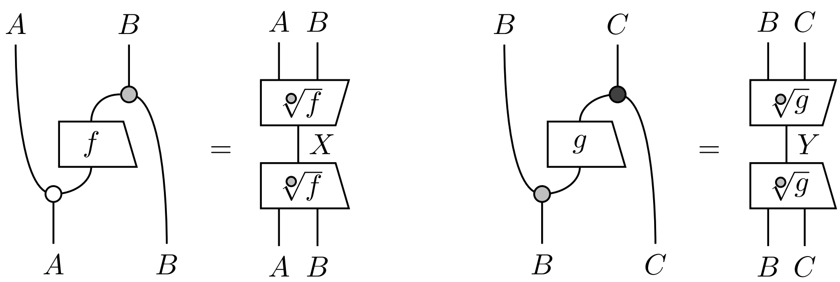



Because the category is positively monoidal, equation (7.5) now follows. □

Equation (7.5) is called the *CP–condition*. Notice the similarity to the oracles of Definition 6.11; that required the left-hand side to be unitary, whereas the CP–condition requires it to be positive. The object $X$ is also 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 mixed state $(f \otimes \mathrm{id}) \circ m$ is also called the *Choi–matrix*; 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 first need two preparatory lemmas showing that the CP–condition is well-behaved with respect to composition and tensor products.

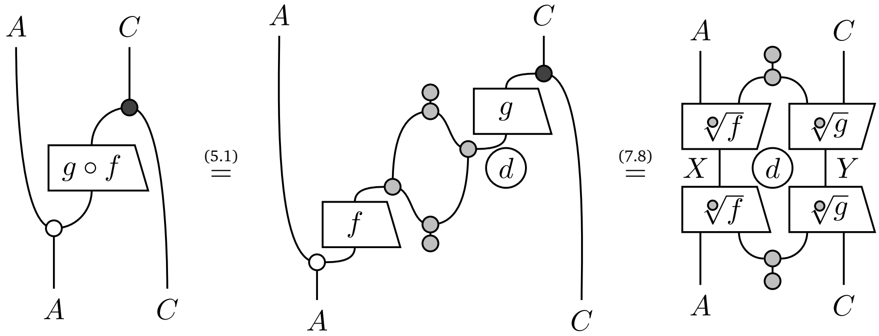
**Lemma 7.13** (CP maps compose). *Let* $(A, ⋏, ⫯)$*,* $(B, ⋏, ⫯)$*, and* $(C, ⋏, ⫯)$ *be dagger Frobenius structures in a monoidal dagger category. Assume* $d \bullet ⦽ = \mathrm{id}_B$ *for some positive scalar* $d$*. If* $A \xrightarrow{f} B$ *and* $B \xrightarrow{g} C$ *satisfy the CP–condition* (7.5)*, then so does* $A \xrightarrow{g \circ f} C$*.*

*Proof.* Say:




(7.8)

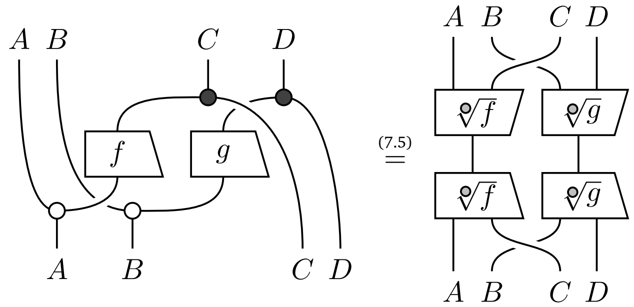
for objects $X, Y$ and morphisms $\sqrt[\circ]{f}$, $\sqrt[\circ]{g}$. Then:




This uses the Frobenius law to insert a 'handle' $d \bullet \varphi$. □

**Lemma 7.14** (Product CP maps)**.** *If* $(A, \curlywedge, \circ) \xrightarrow{f} (B, \curlywedge, \bullet)$ *and* $(C, \curlywedge, \circ) \xrightarrow{g} (D, \curlywedge, \bullet)$ *are maps between dagger Frobenius structures in a braided monoidal dagger category that satisfy the CP–condition* (7.5)*, then so is* $(A, \curlywedge, \circ) \otimes (C, \curlywedge, \circ) \xrightarrow{f \otimes g} (B, \curlywedge, \circ) \otimes (D, \curlywedge, \circ)$.

*Proof.* Suppose $\sqrt[\circ]{f}$ and $\sqrt[\circ]{g}$ are Kraus morphisms for $f$ and $g$. Then:




This proves the lemma. □

## 7.2.2 Stinespring's theorem

We can now prove that the CP–condition characterizes completely positive maps. Notice that the proof of Lemma 7.12 did not need arbitrary ancilla systems $E$, and pair of pants monoids sufficed. The following theorem will also record that.

**Theorem 7.15** (Stinespring)**.** *Let* $(A, \curlywedge, \circ)$ *and* $(B, \curlywedge, \circ)$ *be special dagger Frobenius structures and* $A \xrightarrow{f} B$ *a morphism in a braided monoidal dagger category that is positively monoidal. The following are equivalent:*

*(a)* $f$ *is completely positive;*

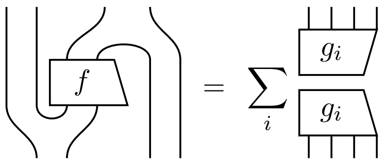
*(b)* $f \otimes \mathrm{id}_E$ *is a positive map for all objects* $X$*, where* $E = (X^* \otimes X, \curlywedge, \cup)$*;*

*(c)* $f$ *satisfies the CP–condition* (7.5).

*Proof.* Clearly (a) implies (b). Lemma 7.12 shows that (b) implies (c). Finally, to show that (c) implies (a), let $I \xrightarrow{m} (A, \curlywedge, \circ) \otimes (E, \curlywedge, \circ)$ be a mixed state. Then $m$ is a completely positive map and so satisfies the CP–condition. Hence, by Lemmas 7.13 and 7.14, also $(f \otimes \mathrm{id}_E) \circ m$ satisfies the CP–condition and is thus a mixed state. □

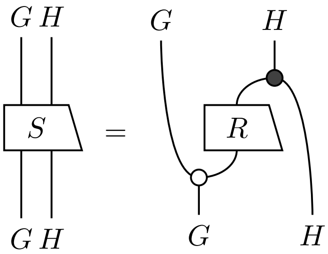
**Example 7.16.** Let's unpack what the previous theorem says in our example categories **FHilb** and **Rel**.

- 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 **Rel**, a relation $\mathbf{G} \xrightarrow{R} \mathbf{H}$ between groupoids satisfies the CP–condition when the relation




$$= \{((g_1, h_1), (g_2, h_2)) \mid (g_2^{-1} \circ g_1)R(h_2 \circ h_1^{-1})\}$$

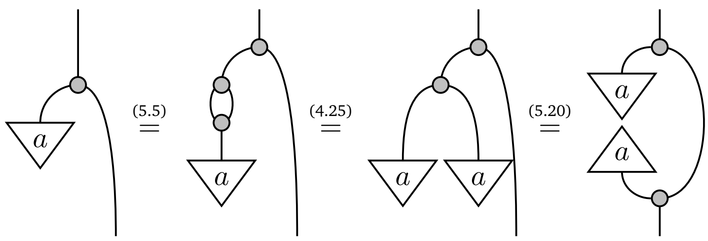
  is positive. This is the case when it is symmetric and satisfies $(g, h)S(g, h)$ when $(g, h)S(g', h')$ (see Exercise 2.5.6), matching Proposition 7.10 as follows.

  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 7.17.** *Any copyable state $I \xrightarrow{a} A$ of a classical structure $(A,$ ⋏ $,$ ⫯$)$ in a braided monoidal dagger category is a completely positive map.*

*Proof.* Graphical manipulation:




This used specialness, copyability, 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 $\mathbf{C}$ modeling pure states, and lifts it to a new compact dagger category $\mathrm{CP}[\mathbf{C}]$ of mixed states.

**Definition 7.18** (CP–construction)**.** Let $\mathbf{C}$ be a monoidal dagger category. Define a new category $\mathrm{CP}[\mathbf{C}]$ as follows: objects are special dagger Frobenius structures in $\mathbf{C}$, and morphisms are completely positive maps.

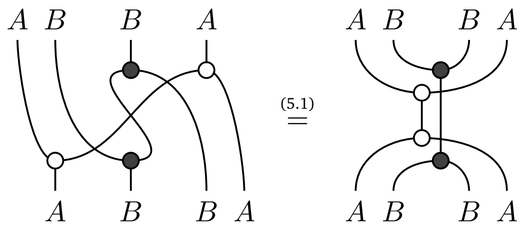
Note that $\mathrm{CP}[\mathbf{C}]$ is indeed a well-defined category: identities in $\mathbf{C}$ satisfy the CP–condition precisely because of the Frobenius law, and Lemma 7.13 shows that composition preserves the CP–condition. The CP–construction preserves much more than being a category, as we investigate next.

**Proposition 7.19** (CP preserves tensors)**.** *If $\mathbf{C}$ is a braided monoidal dagger category, then $\mathrm{CP}[\mathbf{C}]$ is a monoidal category:*

- *the tensor product of objects is that of Lemma 4.8;*
- *the tensor product of morphisms is well-defined by Lemma 7.14;*
- *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 $\alpha$, $\lambda$, and $\rho$, are inherited from $\mathbf{C}$.*

*If $\mathbf{C}$ is a symmetric monoidal category, then so is $\mathrm{CP}[\mathbf{C}]$.*

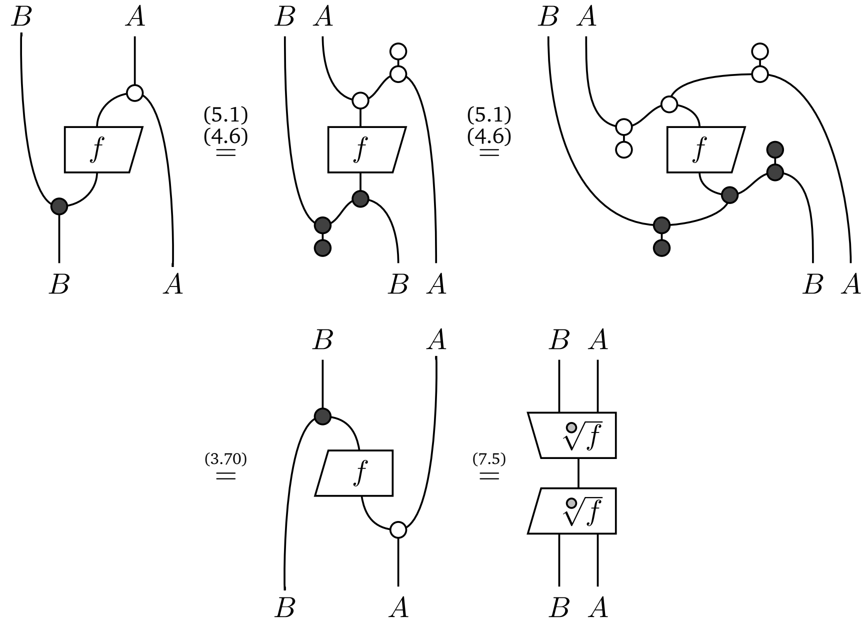
*Proof.* The tensor unit $I$ is a well-defined special dagger Frobenius structure by the coherence theorem. (For the tensor product of objects, see also Exercise 5.7.1.) Using these definitions of $\otimes$ and $I$, the unitary coherence isomorphisms $\alpha$, $\lambda$, and $\rho$, from $\mathbf{C}$ trivially satisfy the CP–condition. Thus $\mathrm{CP}[\mathbf{C}]$ is a well-defined monoidal category. If $\mathbf{C}$ is additionally symmetric, the swap maps satisfy the CP–condition by the Frobenius law:




Hence, in that case, $\mathrm{CP}[\mathbf{C}]$ is symmetric monoidal. □

**Lemma 7.20** (CP preserves daggers)**.** *Let $(A, \circ, \circ)$ and $(B, \bullet, \bullet)$ be special dagger Frobenius structures in a braided monoidal dagger category. If $A \xrightarrow{f} B$ satisfies the CP–condition* (7.5)*, then so does $B \xrightarrow{f^\dagger} A$.*

*Proof.* We show that $f^\dagger$ satisfies the CP–condition.




The first two equations use the Frobenius law and unitality, the last one the definition of transpose. □

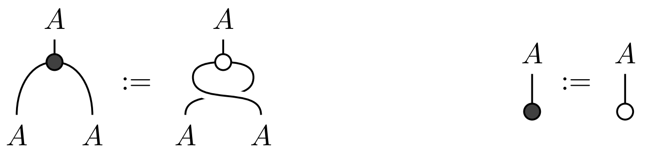
The previous lemma sets up a perfect duality between the Schrödinger and Heisenberg pictures. In particular, Example 7.8 goes through for arbitrary braided monoidal dagger categories: measurements are completely positive maps from a classical structure to an arbitrary dagger Frobenius structure, and controlled preparations go in the opposite direction.

**Corollary 7.21.** *If* **C** *is a (symmetric) monoidal dagger category, so is* CP[**C**].

*Proof.* Combine Proposition 7.19 and Lemma 7.20. □

We can now prove the closure property stated in the introduction to this chapter: using the CP–construction, we do not need to step outside the realm of compact dagger categories.

**Lemma 7.22** (CP preserves duals)**.** *Let* $(A, ⅄, ⫯)$ *be a special dagger Frobenius structure in a braided monoidal dagger category* **C**. *Define:*

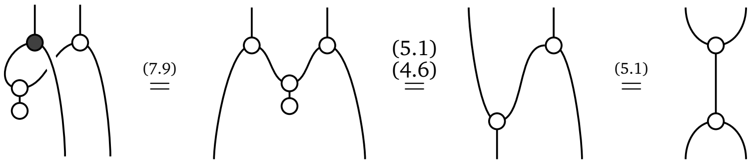



(7.9)

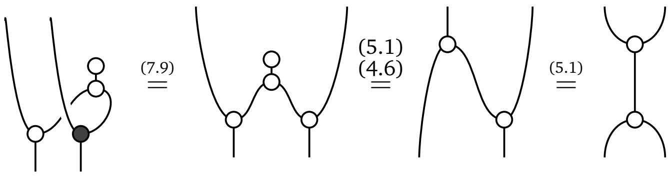
*Then* $(A, ⅄, ⫯)$ *is an object dual to* $(A, ⅄, ⫯)$ *in* CP[**C**]. *If* **C** *is symmetric monoidal, then both objects are dagger dual in* CP[**C**].

*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 completely positive map and hence a well-defined morphism in $\mathrm{CP}[\mathbf{C}]$, by checking the CP–condition:

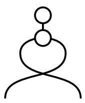
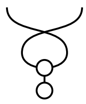



The first equality unfolds definitions and uses naturality of braiding, and the last two apply the Frobenius law and unitality. Similarly,  := $: L \otimes R \to I$ is completely positive:

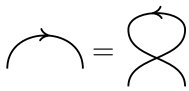



Because composition in $\mathrm{CP}[\mathbf{C}]$ is as in $\mathbf{C}$, the snake equations come down precisely to the Frobenius law. Thus  and  witness that $L \dashv R$ in $\mathrm{CP}[\mathbf{C}]$.

Finally, suppose $\mathbf{C}$ is symmetric monoidal. In that case it follows from Lemma 7.20 and Proposition 7.19 that

 :=  $: L \otimes R \to I$  :=  $: R \otimes L \to I$

are completely positive maps, as both are the composition of the completely positive swap map and the adjoint of a map we have already shown to be completely positive. The snake equations again come down to the Frobenius law. By definition:



so in this case $L$ and $R$ are dagger dual objects in $\mathrm{CP}[\mathbf{C}]$. □

The following theorem summarizes all the structure preserved by the CP–construction. It might look like compactness is fabricated out of thin air. But note that Frobenius structures have duals by Theorem 5.14, so that the result of the CP–construction starting with $\mathbf{C}$ is the same as that starting with the compact subcategory of $\mathbf{C}$ of objects with duals.

**Theorem 7.23** (CP is compact)**.** *If* $\mathbf{C}$ *is a braided monoidal dagger category, then* $\mathrm{CP}[\mathbf{C}]$ *is a monoidal dagger category with duals. If* $\mathbf{C}$ *is a symmetric monoidal dagger category, then* $\mathrm{CP}[\mathbf{C}]$ *is a compact dagger category.*

*Proof.* Combine Corollary 7.21 and Lemma 7.22. □

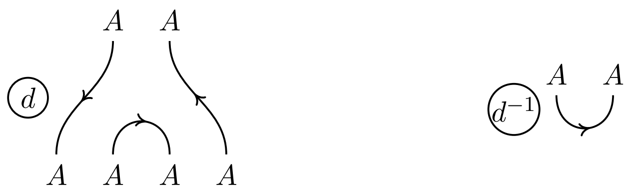
**Example 7.24.** As for examples:

- It follows immediately from Theorems 5.29 and 7.15 that $\mathrm{CP}[\mathbf{FHilb}]$ is the category of finite-dimensional C*-algebras and completely positive maps, and that this is a compact dagger category. This is, of course, the category we modeled the CP–construction on in the first place. In fact, by Corollary 3.57 and Theorem 5.14 we can even say that $\mathrm{CP}[\mathbf{Hilb}]$ is the same category of finite-dimensional operator algebras and completely positive maps.
- Similarly, Theorem 5.36 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 Quantum structures

As we have seen in Section 5.4.1, special dagger Frobenius structures fall on a spectrum. 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 nontrivial observable does not commute with some other observable. We will therefore also call such Frobenius structures *quantum structures*.

**Definition 7.25** (Quantum structure)**.** A *quantum structure* is a dagger Frobenius structure on $A^* \otimes A$ in a monoidal dagger category of the form




(7.10)

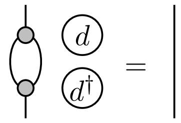
for an object $A$ and an invertible scalar $I \xrightarrow{d} I$.

**Example 7.26.** In our example categories **FHilb** and $\mathbf{Rel}$:

- By Example 4.13, the quantum structures in **FHilb** are precisely the algebras $\mathbb{M}_n$ of $n$-by-$n$ matrices under matrix multiplication. The normalizing scalar there is (necessarily) $d = 1/\sqrt{n}$. These are the operator algebras that are 'maximally noncommutative'.
- In $\mathbf{Rel}$, similarly, the quantum structures are indiscrete groupoids by Corollary 5.37. The normalizing scalar there is (necessarily) $d = 1$. These are the groupoids that are as far away from abelian groupoids (classical structures) as possible.

Quantum structures are not quite pair of pants because of the normalizing scalar. In this section we will therefore work with a corresponding variation $\overline{\mathrm{CP}}[\mathbf{C}]$ of $\mathrm{CP}[\mathbf{C}]$, which is really just an equivalent reformulation of the CP–construction.

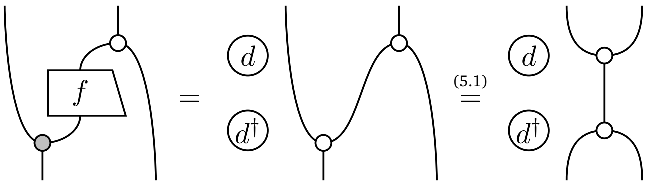
**Remark 7.27** (Normalizability)**.** Look back at the proof that $\mathrm{CP}[\mathbf{C}]$ is a well-defined monoidal dagger category, especially Lemma 7.13. We could have defined a more liberal category $\overline{\mathrm{CP}}[\mathbf{C}]$, whose morphisms are still completely positive maps, but whose objects are dagger Frobenius structures $(A, \curlywedge, \circ)$ in $\mathbf{C}$ that are *normalizable*, in the sense that




(7.11)

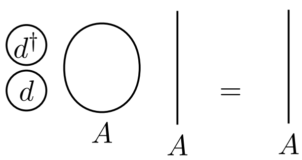
for some invertible scalar $I \xrightarrow{d} I$. However, this extra freedom is only there in appearance. Any object of $\overline{\mathrm{CP}}[\mathbf{C}]$ is isomorphic to some object of $\mathrm{CP}[\mathbf{C}]$. Therefore $\overline{\mathrm{CP}}[\mathbf{C}]$ and $\mathrm{CP}[\mathbf{C}]$ are monoidally equivalent monoidal dagger categories.

*Proof.* Let $(A, \curlywedge, \circ)$ be a normalizable dagger Frobenius structure. Define $\bar{\curlywedge} := d \bullet \curlywedge$ and $\bullet := d^{-1} \bullet \circ$. Unfolding the definitions shows that $(A, \bar{\curlywedge}, \bullet)$ is a well-defined dagger Frobenius structure, and that it is special. Now define $f := d \bullet \mathrm{id}_A : A \to A$. We show that this is a completely positive map $(A, \bar{\curlywedge}, \bullet) \to (A, \curlywedge, \circ)$ by verifying the CP–condition:




Similarly, $f^{-1} := d^{-1} \bullet \mathrm{id}_A : A \to A$ is a completely positive map. As these two maps are inverses, we conclude that $(A, \curlywedge, \circ) \simeq (A, \bar{\curlywedge}, \bullet)$ in $\overline{\mathrm{CP}}[\mathbf{C}]$. □

Note that the Frobenius structure (7.10) is special if:

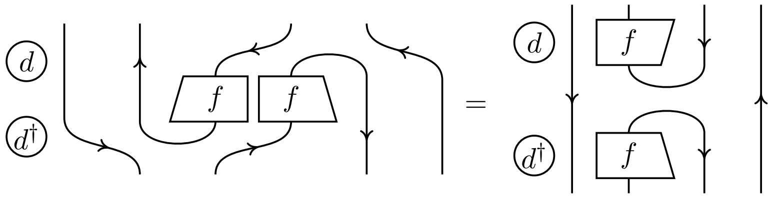



(7.12)

An object $A$ in a monoidal category is called *positive-dimensional* when there exists a scalar $d$ satisfying (7.12). A monoidal category is called *positive-dimensional* when all its objects are. This mild property holds in both **Hilb** and **Rel**.

**Proposition 7.28** (CP embeds **C**)**.** *Let* $\mathbf{C}$ *be a braided monoidal dagger category that is positive-dimensional. There is a functor* $\overline{P} : \mathbf{C} \to \overline{\mathrm{CP}}[\mathbf{C}]$ *defined by letting* $\overline{P}(A)$ *be the quantum structure* (7.10) *on* $A^* \otimes A$*, and by* $\overline{P}(f) = f_* \otimes f$ *on morphisms. It is a monoidal functor that preserves daggers.*

*Proof.* Let $A \xrightarrow{f} B$ in $\mathbf{C}$. We have to show that $\overline{P}(f)$ is completely positive.

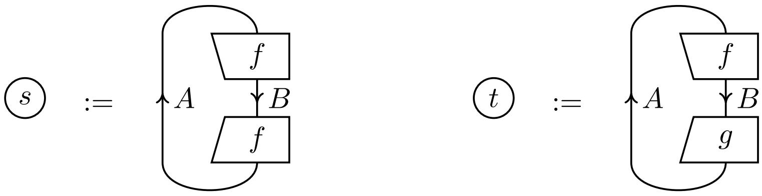



Daggers and tensor products in $\overline{\mathrm{CP}}[\mathbf{C}]$ are by definition as in $\mathbf{C}$. The only other subtlety is that we have to fix a choice of scalar $d$ for each object $A$. □

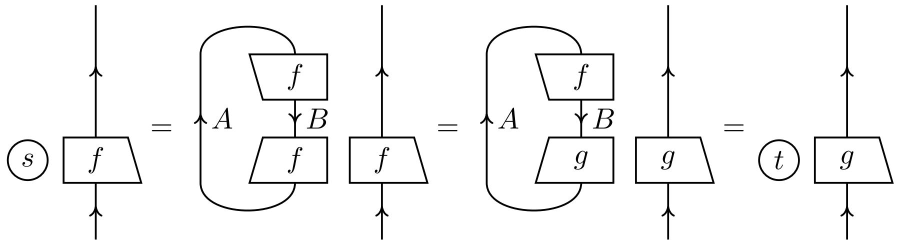
Combining the previous proposition with the equivalence of Remark 7.27 gives a functor $P\colon \mathbf{C} \to \mathrm{CP}[\mathbf{C}]$. We regard it as embedding the pure world of $\mathbf{C}$ into the mixed world of $\mathrm{CP}[\mathbf{C}]$. We say 'embedding', but the functor $P$ is not faithful. 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.

**Lemma 7.29** (CP kills phases)**.** *Let $\overline{P}$ be the functor of Proposition 7.28. If $\overline{P}(f) = \overline{P}(g)$ for $A \xrightarrow{f,g} B$, there are $I \xrightarrow{s,t} I$ with $s \bullet f = t \bullet g$ and $s^\dagger \bullet s = t^\dagger \bullet t$.*

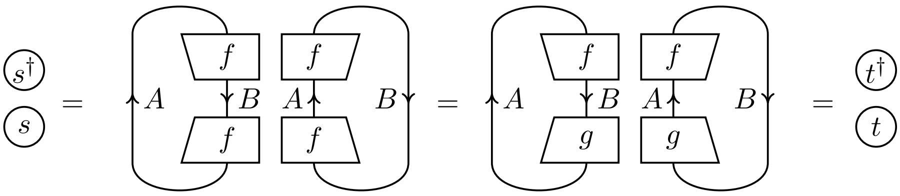
*Proof.* Define:




Then:



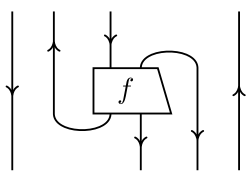

And:




Notice that this proof is completely graphical and does not depend on anything like angles. □

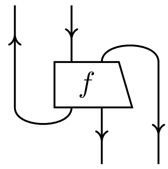
## 7.3.1 The category of quantum structures

We can define the subcategory $\overline{\mathrm{CP}}_{\mathrm{q}}[\mathbf{C}]$ of $\overline{\mathrm{CP}}[\mathbf{C}]$ of all quantum structures. Its image $\mathrm{CP}_{\mathrm{q}}[\mathbf{C}]$ under the equivalence of Remark 7.27 is a subcategory of $\mathrm{CP}[\mathbf{C}]$. We can describe it as follows. Objects of $\mathrm{CP}_{\mathrm{q}}[\mathbf{C}]$ are pair of pants monoids $A^* \otimes A$ in $\mathbf{C}$ (without any normalizing scalar); we can abbreviate these to just the object $A$ of $\mathbf{C}$ itself. The CP–condition then simplifies to requiring that




(7.13)

be a positive map. For positively monoidal $\mathbf{C}$, the morphisms $A \to B$ in $\mathrm{CP_q}[\mathbf{C}]$ simplify further to a morphism $A^* \otimes A \xrightarrow{f} B^* \otimes B$ whose Choi–matrix



(7.14)

is positive. In fact, the category $\mathrm{CP_q}[\mathbf{C}]$ is well-defined with such morphisms (by the same reasoning as in Lemma 7.13, whether $\mathbf{C}$ is positively monoidal or not; see also Exercise 7.6.8).

**Definition 7.30** (The category $\mathrm{CP_q}$)**.** Let $\mathbf{C}$ be a compact dagger category. The category $\mathrm{CP_q}[\mathbf{C}]$ has the same objects as $\mathbf{C}$. A morphism $A \to B$ in $\mathrm{CP_q}[\mathbf{C}]$ is a morphism $A^* \otimes A \xrightarrow{f} B^* \otimes B$ whose Choi–matrix (7.14) is positive.

All results hold as before: 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 7.28.

**Example 7.31.** 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 $B$.

## 7.3.2 Environment structures

In categories of the form $\mathrm{CP_q}[\mathbf{C}]$, any object $A$ allows a morphism $A \xrightarrow{\top_A} I$, namely $\frown$. 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 $\top_A \circ \ulcorner m \urcorner = \mathrm{Tr}(m) \colon I \to I$ by Definition 3.51. Notice that this form of 'discarding the information in $A$' is not uniform, and therefore gives no contradiction with the no-deleting Theorem 4.17. In this section we axiomatize whether a given abstract category is of the form $\mathrm{CP_q}[\mathbf{C}]$ in this way.

**Definition 7.32** (Environment structure)**.** An *environment structure* for a compact dagger category $\mathbf{C}^{\mathrm{pure}}$ consists of the following data:

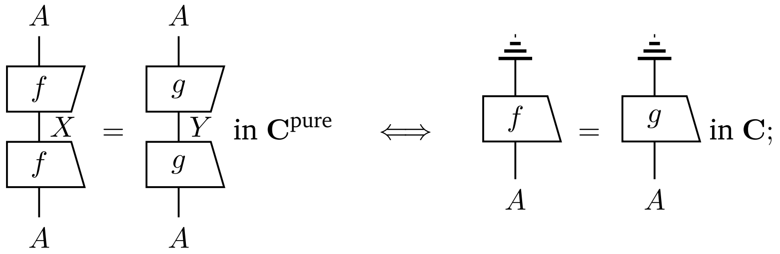
- a compact dagger category $\mathbf{C}$ of which $\mathbf{C}^{\mathrm{pure}}$ is a compact dagger subcategory with the same objects;
- for each object $A$, a morphism $A \xrightarrow{\top_A} I$ in $\mathbf{C}$, depicted as $\top$.

Furthermore, this data must satisfy the following properties:

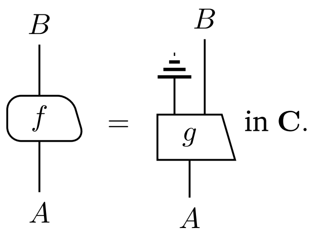
(a) $\top_I = \mathrm{id}_I$ and $\top_{A \otimes B} = (\top_A \otimes \top_B) \circ \lambda_I$;

(7.15)

(b) for all $A \xrightarrow{f} X$ and $A \xrightarrow{g} Y$ in $\mathbf{C}^{\text{pure}}$: $f^\dagger \circ f = g^\dagger \circ g$ if and only if $\top_X \circ f = \top_Y \circ g$;


(7.16)

(c) for each $A \xrightarrow{f} B$ in $\mathbf{C}$ there is $A \xrightarrow{g} X \otimes B$ in $\mathbf{C}^{\text{pure}}$ such that:


(7.17)

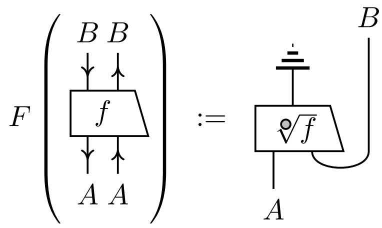
Morphisms in $\mathbf{C}$ are depicted with round corners.

Intuitively, we think of $\mathbf{C}^{\text{pure}}$ as consisting of pure states, and the supercategory $\mathbf{C}$ of containing mixed states. Condition (7.17) then reads 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.

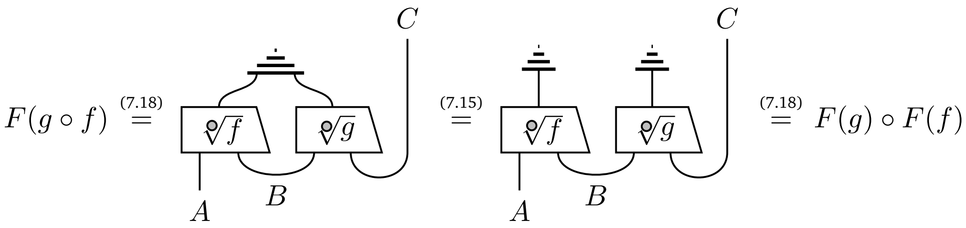
Starting with a compact dagger category $\mathbf{C}^{\text{pure}}$, write $\mathbf{D}^{\text{pure}}$ for the image of the functor $P \colon \mathbf{C}^{\text{pure}} \to \mathrm{CP_q}[\mathbf{C}^{\text{pure}}]$ (defined by $P(A) = A$ and $P(f) = f_* \otimes f$). Explicitly, $\mathbf{D}^{\text{pure}}$ is the subcategory of $\mathrm{CP_q}[\mathbf{C}^{\text{pure}}]$ whose morphisms can be written with ancilla $I$. (Don't forget that the functor $P$ is not faithful, see Proposition 7.28!) This dagger category $\mathbf{D}^{\text{pure}}$ is again compact. Then $\mathbf{D}^{\text{pure}}$ has an environment structure with $\mathbf{D} = \mathrm{CP_q}[\mathbf{C}^{\text{pure}}]$, and $\top_A$ given by $\curvearrowleft$. Conversely, having an environment structure is essentially the same as working with a category of completely positive morphisms, as the following theorem shows.

**Theorem 7.33.** *If a compact dagger category $\mathbf{C}^{pure}$ comes with an environment structure, then there is an invertible functor $F \colon \mathrm{CP_q}[\mathbf{C}^{pure}] \to \mathbf{C}$ that satisfies $F(A) = A$ on objects and $F(f \otimes g) = F(f) \otimes F(g)$ on morphisms.*

*Proof.* Define $F$ by $F(A) = A$ on objects, and as follows on morphisms:


(7.18)

This is well-defined by $\Rightarrow$ of (7.16). It is also functorial:



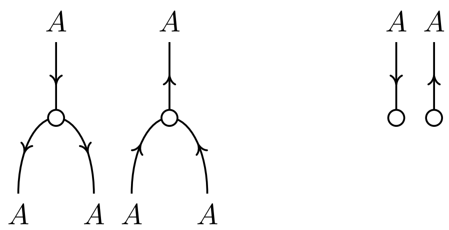

Here, the first equality follows from Lemma 7.13, and the second from (7.15). It is obvious that the functor $F$ is invertible: the direction $\Leftarrow$ of (7.16) shows that it is faithful, and (7.17) shows that it is full. Finally, it follows from Lemma 7.14 and (7.15) that $F(f \otimes g) = F(f) \otimes F(g)$. $\square$

Environment structures give us 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.

### 7.3.3 Quantum teleportation

This section brings together almost all the material covered so far to discuss quantum teleportation. We already saw versions in Sections **??** (for pure states, postselected) and 5.6.3 (for pure states, with classical communication); this version can teleport mixed states with two 'bits' of classical communication. We start by observing that we can lift (complementary) classical structures from a setting of pure states to a setting of mixed states. (This is not a coincidence, because the functor from Proposition 7.28 is a symmetric monoidal functor; see Exercise 5.7.5.)

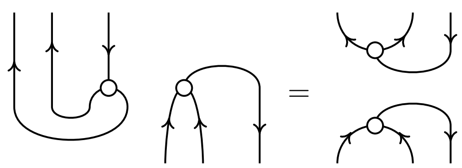
**Lemma 7.34.** *If* $(A,$ , $)$ *is a Frobenius structures in a braided monoidal category* $\mathbf{C}$*, then*



(7.19)

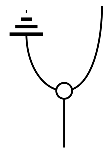
*is a Frobenius structure in* $\mathrm{CP_q}[\mathbf{C}]$*. If two Frobenius structures in* $\mathbf{C}$ *are complementary, so are the two Frobenius structures in* $\mathrm{CP_q}[\mathbf{C}]$.

*Proof.* We check that (7.14) is positive:



The axioms for Frobenius structures are simply verified 'side by side'. The same holds for the complementarity axiom between the two Frobenius structures. $\square$

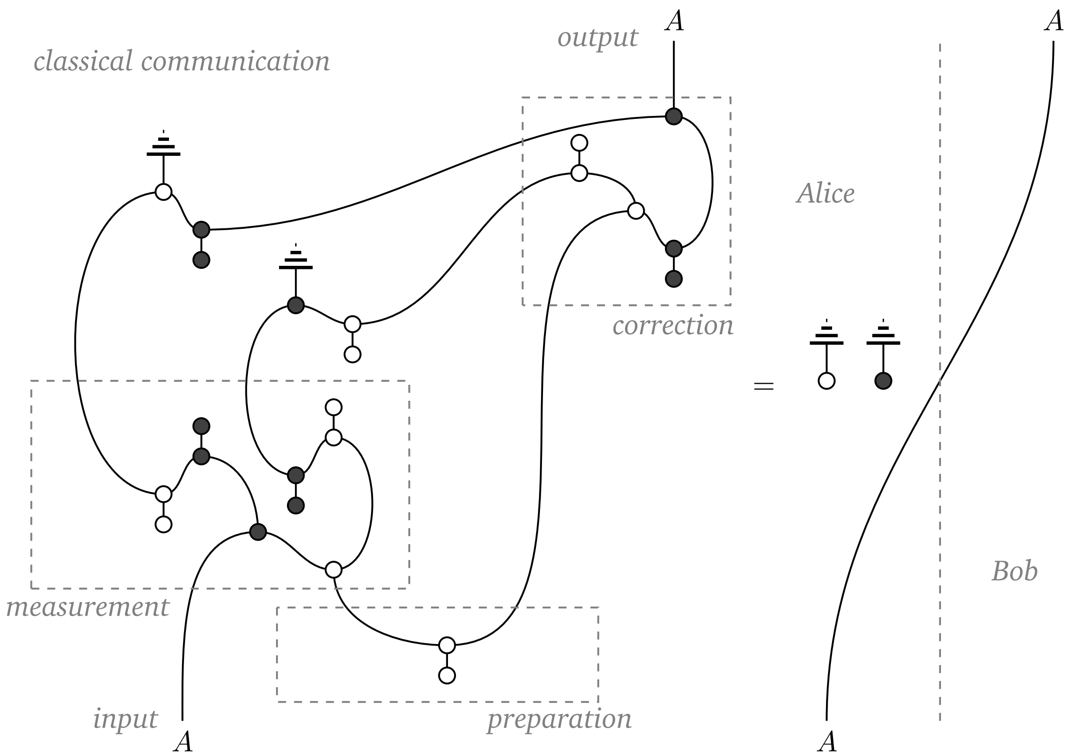
To model classical communication, use environment structures to speak of



(7.20)

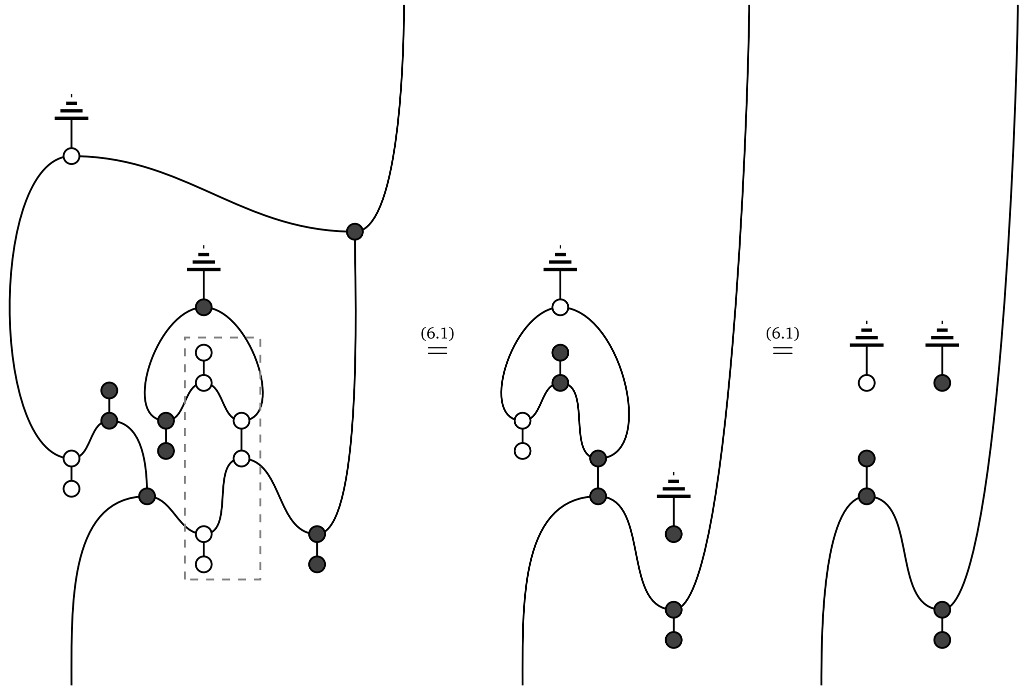
as a channel that carries classical information encoded in the Frobenius structure. Consider what it does in CP[**FHilb**]. The Frobenius structure corresponds to a choice of orthogonal bases. The channel leaves a state $|i\rangle\langle i|$ undisturbed, but sends a state $|i\rangle\langle j|$ to zero when $i \neq j$. In other words, it zeroes out off-diagonal elements of the density matrix you feed it. This is called *decoherence*, and makes sure that only classical information, as encoded in the basis chosen by the Frobenius structure, survives the channel.

**Theorem 7.35.** *If* $(A, \ , \ )$ *and* $(A, \ , \ )$ *are complementary symmetric dagger Frobenius structures in a braided monoidal dagger category* **C**, *of which is commutative, then the following equation holds in* $\mathrm{CP_q}[\mathbf{C}]$:




*Proof.* Let's start with the left-hand side. An application of commutative spider

Theorem 5.20 to the indicated white dots transforms it into:




The first equality uses complementarity and an application of the noncommutative black spider Theorem 5.20, and the second uses complementarity again. Finally, by a simple black snake equation (3.5), this equals the right-hand side of the equation in the statement of the theorem. □

Notice that the classical communication in the previous theorem is only classical in the sense that it is 'copied' by the two Frobenius structures, one of which does not even have to be commutative. 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 $\mathbb{C}^2$ for $A$, and the classical structures induced by the $X$ and $Z$ bases from Example 6.5, the previous theorem precisely shows the correctness of the quantum teleportation protocol. Moreover, notice that we have modeled it entirely using tensor products and composition (and not biproducts), which was one of the main goals of this book.

## 7.4 Classical structures

At the other end of the spectrum of special dagger Frobenius structures, opposite to quantum structures, are classical structures. This section considers completely positive maps to and from classical structures. Just like for quantum structures, we can consider the full subcategory of $\mathrm{CP}[\mathbf{C}]$ of classical structures.

**Definition 7.36** (The category $\mathrm{CP_c}$)**.** Let **C** be a braided monoidal dagger category. The category $\mathrm{CP_c}[\mathbf{C}]$ has as objects classical structures in **C**. Its morphisms are completely positive maps.

Again, as before, if $\mathbf{C}$ is compact, then so is $\mathrm{CP_c}[\mathbf{C}]$. In fact, according to Lemma 7.22, 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.

### 7.4.1 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 7.37.** The category $\mathrm{CP_c}[\mathbf{FHilb}]$ is monoidally equivalent to the following: objects are natural numbers, and morphisms $m \to n$ are $m$-by-$n$ matrices whose entries are nonnegative real numbers. The maps that preserve counit correspond to those matrices whose rows sum up to one, *i.e. stochastic matrices*.

*Proof.* In $\mathbf{FHilb}$, classical structures $(H, \delta, \varepsilon)$ correspond to a choice of orthonormal basis on $H$ by Corollary 5.31. 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 7.15, 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 $\langle j|f|i\rangle$.

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 $\sum_{i=1}^n \langle j|f|i\rangle = 1$. $\square$

The previous example is consistent with the morphisms between classical structures we studied in Chapter 5. Corollary 5.34 showed that comonoid homomorphisms between classical structures correspond to matrices where every column has a single entry one and zeroes otherwise. These are the *deterministic* maps within the stochastic setting of the previous example. Lemma 5.35 showed that these are self-conjugate, which means that their matrix entries are real numbers.

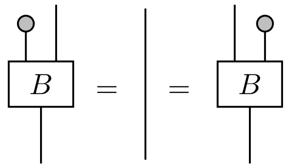
### 7.4.2 Broadcasting

We now come full circle after Chapter 4, which showed that that compact dagger categories do not support uniform copying and deleting. However, that does not yet guarantee they model quantum mechanics. Classical mechanics might have 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' maps $A \to I$ in $\mathrm{CP}[\mathbf{C}]$ more generally than the environment structure maps in $\mathrm{CP_q}[\mathbf{C}]$. The following lemma shows that $\varepsilon^\dagger$ plays that role anywhere in $\mathrm{CP}[\mathbf{C}]$, not just in $\mathrm{CP_q}[\mathbf{C}]$.

**Lemma 7.38.** *Let $(A, \delta, \varepsilon)$ be a dagger Frobenius structure in a braided monoidal dagger category $\mathbf{C}$. Then $\varepsilon$ is completely positive. If additionally $(A, \delta, \varepsilon)$ is a classical structure, then $\delta$ is completely positive.*

*Proof.* Verifying the CP–condition for  just comes down to unitality and the fact that the identity is positive. If  is commutative, the CP–condition for  can be rewritten into positive form easily using the noncommutative spider Theorem 5.20. □

**Definition 7.39.** let $\mathbf{C}$ be a braided monoidal dagger category. A *broadcasting map* for an object $(A,$ , $)$ of $\mathrm{CP}[\mathbf{C}]$ is a morphism $A \xrightarrow{B} A \otimes A$ in $\mathrm{CP}[\mathbf{C}]$ satisfying the following equation:



(7.21)

The object $(A,$ , $)$ is called *broadcastable* if it allows a broadcasting map.

Notice that the previous definition concerns just a single object, and is therefore much weaker than Definition 4.18.Nevertheless, we can prove it holds for all classical structures.

**Lemma 7.40.** *Let $\mathbf{C}$ be a braided monoidal dagger category. Classical structures are broadcastable objects in* $\mathrm{CP}[\mathbf{C}]$.

*Proof.* Let $(A,$ , $)$ be a classical structure. We will show that  is a broadcasting map. It clearly satisfies (7.21), so it suffices to show that it is a well-defined morphism in $\mathrm{CP}[\mathbf{C}]$. This follows directly from Lemma 7.38. □

In $\mathbf{FHilb}$, the converse to the previous lemma holds; this is the so-called *no-broadcasting theorem*. So a dagger Frobenius structure in $\mathbf{FHilb}$ is broadcastable if and only if it is a classical structure. However, this is not the case in $\mathbf{Rel}$. Call a category *totally disconnected* when its only morphisms are endomorphisms. Totally disconnected groupoids are the extreme opposite of indiscrete ones.

**Lemma 7.41.** *Broadcastable objects in* $\mathrm{CP}[\mathbf{Rel}]$ *are precisely totally disconnected groupoids.*

*Proof.* Let $\mathbf{G}$ be a totally disconnected groupoid, and write $G$ for its set of morphisms. We will show that the morphism $G \xrightarrow{B} G \times G$ in $\mathbf{Rel}$ 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, $B$ is readily seen to respect inverses, so it is a well-defined morphism in $\mathrm{CP}[\mathbf{Rel}]$. When interpreted in $\mathbf{Rel}$, the broadcastability equation (7.21) reads

$$\begin{aligned} \{(g,g) \mid g \in G\} &= \{(g,h) \mid (g, (\mathrm{id}_{\mathrm{cod}(h)}, h)) \in B\} \\ &= \{(g,h) \mid (g, (h, \mathrm{id}_{\mathrm{dom}(h)})) \in B\}. \end{aligned} \tag{7.22}$$

This equation is satisfied because $\mathbf{G}$ is totally disconnected, and so $B$ is a broadcasting map for $\mathbf{G}$.

Conversely, suppose that a groupoid $\mathbf{G}$ is broadcastable. Then there is a morphism $B$ in $\mathbf{Rel}$ respecting inverses and satisfying (7.22). Let $g$ be a morphism in $\mathbf{G}$. Because

$R$ respects inverses, there is an object $C$ of $\mathbf{G}$ such that $(g, (\mathrm{id}_C, g)) \in B$. Next, equation (7.22) and the fact that $R$ respects inverses give $(\mathrm{id}_{\mathrm{dom}(g)}, (\mathrm{id}_C, \mathrm{id}_{\mathrm{dom}(g)})) \in B$ and $C = \mathrm{dom}(g)$. But also $(g^{-1}, (\mathrm{id}_C, g^{-1})) \in B$. So, using (7.22) again, we also have $(\mathrm{id}_{\mathrm{cod}(g)}, (\mathrm{id}_C, \mathrm{id}_{\mathrm{cod}(g)}))$ and $C = \mathrm{cod}(g)$. Hence $\mathrm{dom}(g) = \mathrm{cod}(g)$. Thus $\mathbf{G}$ is totally disconnected. □

# 7.5 Interaction with linear structure

For the final section of this chapter, we investigate how the CP–construction interacts with biproducts, much like in Section 3.1.4. The answer turns out to be very satisfying: if $\mathbf{C}$ has dagger biproducts, then so does $\mathrm{CP}[\mathbf{C}]$. The first lemma handles the level of objects.

**Lemma 7.42.** *If $(A, m_A, u_A)$ and $(B, m_B, u_B)$ are dagger Frobenius structures in a monoidal dagger category with dagger biproducts, then*

$$m_{A\oplus B} = \begin{pmatrix} m_A \circ (p_A \otimes p_A) \\ m_B \circ (p_B \otimes p_B) \end{pmatrix} : (A \oplus B) \otimes (A \oplus B) \to (A \oplus B) \tag{7.23}$$

$$u_{A\oplus B} = \begin{pmatrix} u_A \\ u_B \end{pmatrix} : I \to A \oplus B \tag{7.24}$$

*make $A \oplus B$ into a dagger Frobenius structure. Furthermore, the zero object uniquely carries a dagger Frobenius structure*

$$m_0 = 0\colon 0 \otimes 0 \to 0, \qquad\qquad u_0 = 0\colon I \to 0. \tag{7.25}$$

*Proof.* Associativity and unitality were already mentioned in (5.26) and Exercise 5.7.8. For example, unitality:

$$\begin{aligned}
& m_{A\oplus B} \circ (u_{A\oplus B} \otimes \mathrm{id}_{A\oplus B}) \\
&= \big((i_A \circ m_A \circ (p_A \otimes p_A)) + (i_B \circ m_B \circ (p_B \otimes p_B))\big) \circ \\
&\quad \big(((i_A \circ u_A) \otimes \mathrm{id}_{A\oplus B}) + ((i_B \circ u_B) \otimes \mathrm{id}_{A\oplus B})\big) \\
&= \big(i_A \circ m_A \circ (u_A \otimes p_A)\big) + \big(i_B \circ m_B \circ (u_B \otimes p_B)\big) \\
&= (i_A \circ p_A) + (i_B \circ p_B) \\
&= \mathrm{id}_{A\oplus B}.
\end{aligned}$$

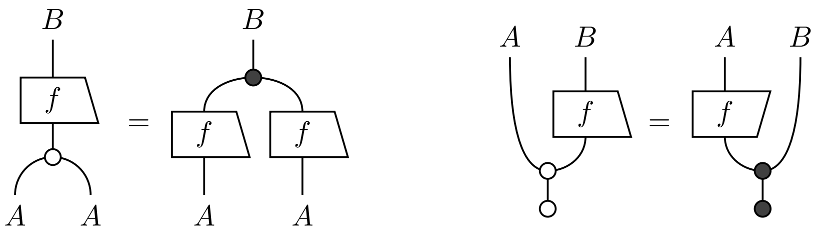
Associativity is very similar. So is speciality:

$$\begin{aligned}
& m_{A\oplus B} \circ m^\dagger_{A\oplus B} \\
&= \begin{pmatrix} m_A \circ (p_A \otimes p_A) \\ m_B \circ (p_B \otimes p_B) \end{pmatrix} \circ \Big( (i_A \otimes i_A) \circ m_A^\dagger \quad (i_B \otimes i_B) \circ m_B^\dagger \Big) \\
&= \begin{pmatrix} m_A \circ m_A^\dagger & 0 \\ 0 & m_B \circ m_B^\dagger \end{pmatrix} \\
&= \mathrm{id}_{A\oplus B}.
\end{aligned}$$

The Frobenius law follows similarly. □

Next we move to the level of morphisms. We first show an easy way to show that a morphism is completely positive.

**Definition 7.43** (Involutive homomorphism)**.** An *involutive homomorphism* is a morphism $(A, \circ, \circ) \xrightarrow{f} (B, \bullet, \bullet)$ between dagger Frobenius structures in a monoidal dagger category satisfying:

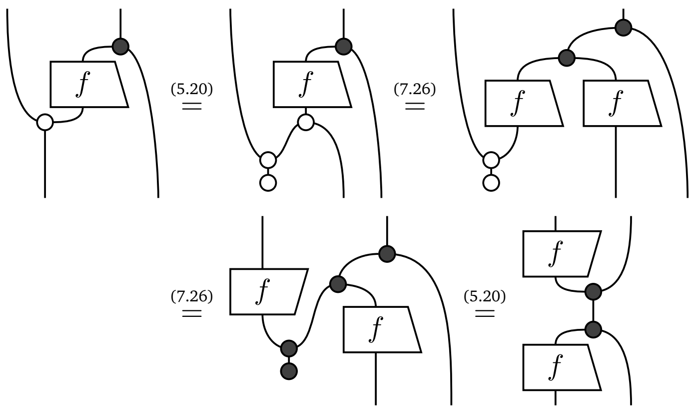



(7.26)

Notice that this notion is weaker than that of homomorphism of Frobenius structures, and hence escapes Lemma 5.18. Instead, the second equation in (7.26) is precisely (5.22) 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 7.44.** *Involutive homomorphisms are completely positive.*

*Proof.* Verify the CP–condition:

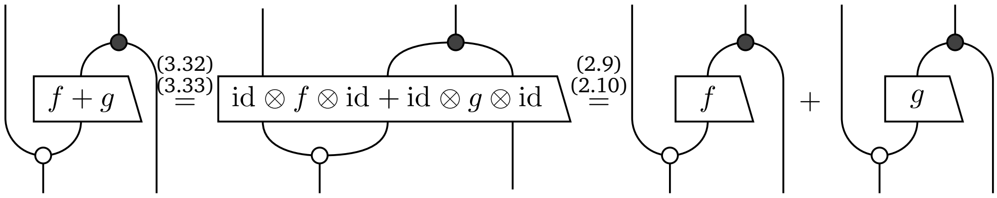


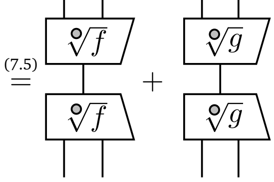

The second and third equalities follow from equation (7.26), the others from the noncommutative spider Theorem 5.20. □

Now we can prove that the CP–construction respects biproducts.

**Lemma 7.45.** *Let* **C** *be a braided monoidal dagger category with duals. If* **C** *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 2.23 and 3.20, we see that




$$\begin{pmatrix} \sqrt[\circ]{f}^\dagger \circ \sqrt[\circ]{f} & 0 \\ 0 & \sqrt[\circ]{g}^\dagger \circ \sqrt[\circ]{g} \end{pmatrix}$$

$$= \begin{pmatrix} \sqrt[\circ]{f} & 0 \\ 0 & \sqrt[\circ]{g} \end{pmatrix}^\dagger \circ \begin{pmatrix} \sqrt[\circ]{f} & 0 \\ 0 & \sqrt[\circ]{g} \end{pmatrix}$$

is positive. □

**Theorem 7.46.** *If a braided monoidal dagger category* **C** *with duals has biproducts, then so does* CP[**C**].

*Proof.* By Lemma 7.45 it suffices to prove that the object $A \oplus B$ of CP[**C**] defined in Lemma 7.42 is a dagger biproduct of $(A, \cdot, \cdot)$ and $(B, \cdot, \cdot)$. All we have to do is show that the morphisms $A \xrightarrow{i_A} A \oplus B$, $B \xrightarrow{i_B} A \oplus B$, $A \oplus B \xrightarrow{p_A} A$, and $A \oplus B \xrightarrow{p_B} B$ in **C** are involutive homomorphisms.

- First consider the map $A \xrightarrow{i_A} A \oplus 0$. By the definition in Lemma 7.42, $m_{A\oplus B} = i_A \circ m_A \circ (p_A \otimes p_A) + i_B \circ m_B \circ (p_B \otimes p_B)$ 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 3.18. Thus $i_A$ is an involutive homomorphism. A similar argument works for $i_B$.

- It follows immediately from the previous point that $A \oplus B \xrightarrow{p_A} A$ is also an involutive homomorphism, as is $p_B$.

So these four morphisms are completely positive by Lemma 7.44. Since they 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. □

## 7.6 Exercises

**Exercise 7.6.1.** Take $A = B = \mathbb{C}^2$ in **FHilb** and recall Definition 0.62 of partial trace.

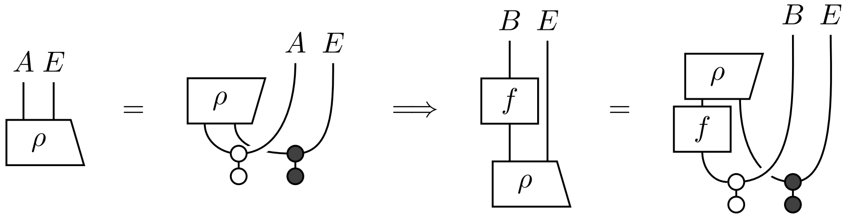
(a) Find density matrices $\rho_A$ on $A$ and $\rho_B$ on $B$ such that there is no density matrix $\rho$ on $A \otimes B$ satisfying $\mathrm{Tr}_A(\rho) = \rho_B$ and $\mathrm{Tr}_B(\rho) = \rho_A$.

(b) Conclude that $A \xleftarrow{\mathrm{Tr}_B} A \otimes B \xrightarrow{\mathrm{Tr}_A} B$ is not a categorical product in $\mathrm{CP}[\mathbf{FHilb}]$.

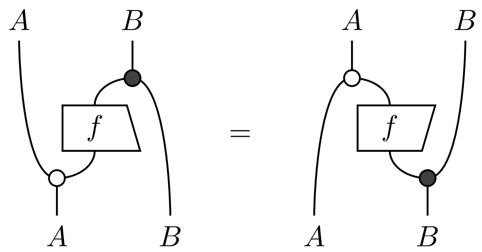
**Exercise 7.6.2.** Recall from Theorem 7.33 that a category of the form $\mathrm{CP}[\mathbf{C}]$ always has a notion of trace $A \xrightarrow{\top_A} I$. Would Theorem 7.23 still hold if we insisted that morphisms in $\mathrm{CP}[\mathbf{C}]$ preserve trace?

**Exercise 7.6.3.** Show that a density matrix is precisely a mixed state in the category **FHilb** that preserves the counit, in the sense that $\varphi \circ \rho = \mathrm{id}_I$.

**Exercise 7.6.4.** Call a morphism $f$ between dagger Frobenius structures $(A, \curlywedge, \circ)$ and $(B, \curlywedge, \circ)$ in a symmetric monoidal dagger category *completely self-adjoint* when for all Frobenius algebras $(E, \curlywedge, \bullet)$:




Show that a morphism is completely self-adjoint if and only if its Choi–matrix is self-adjoint:




(Hint: emulate the proof of Theorem 7.15.)

**Exercise 7.6.5.** Show that any quantum structure is symmetric (as a Frobenius structure).

**Exercise 7.6.6.** Recall monoidal equivalences from Section 1.3. Suppose we adapt Definition 7.32 as follows: there is a monoidal functor $F\colon \mathbf{C}^{\mathrm{pure}} \to \mathbf{C}$ 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:

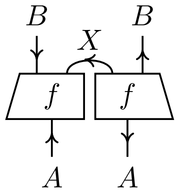
(a) equation (7.15) holds;

(b) for all $A \xrightarrow{f} X$ and $A \xrightarrow{g} Y$ in $\mathbf{C}^{\mathrm{pure}}$: we have $f^\dagger \circ f = g^\dagger \circ g$ in $\mathbf{C}^{\mathrm{pure}}$ 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 $\mathbf{C}^{\mathrm{pure}}$ such that $f = (\top_{F(X)} \otimes \mathrm{id}_{F(B)}) \circ F(g)$.

Show that the following adaptation of Theorem 7.33 holds: there is a monoidal equivalence $\mathrm{CP_q}[\mathbf{C}^{\mathrm{pure}}] \to \mathbf{C}$ that acts as $A \mapsto F(A)$ on objects.

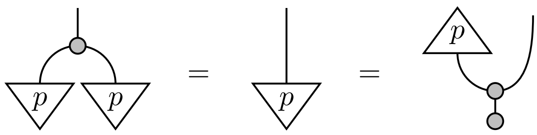
**Exercise 7.6.7.** Show that the following is an alternative description of $\mathrm{CP_q}[\mathbf{C}]$ for a compact dagger category: objects are those of $\mathbf{C}$, morphisms $A \to B$ are morphisms $A^* \otimes A \to B^* \otimes B$ of the form




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 7.6.8.** One way to state Theorem 5.30 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 $\mathbf{Rel}$.

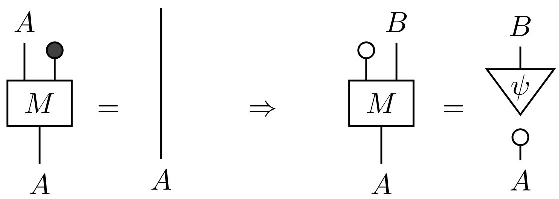
**Exercise 7.6.9.** A *projection* of a dagger Frobenius structure $(A, \text{multiplication}, \text{unit})$ is a morphism $I \xrightarrow{p} A$ satisfying:




Show that in $\mathbf{Rel}$, projections correspond to subgroupoids (*i.e.* subcategories that are groupoids themselves.)

**Exercise 7.6.10.** Let $A$ be an object in a compact dagger category. Assume that $(A^* \otimes A, \text{multiplication}, \text{unit})$ is commutative. Show that all morphisms $A \to A$ equal the identity up to a scalar. (Hint: use the results of Chapter 4.)

**Exercise 7.6.11.** The *Heisenberg uncertainty principle* states that no information can be obtained from a quantum structure without disturbing its state. More precisely: if $(A, \text{multiplication}, \text{unit})$ is a quantum structure, $(B, \text{multiplication}, \text{unit})$ is a classical structure, and $A \xrightarrow{M} A \otimes B$ a completely positive map, then:



(7.27)

for some state $I \xrightarrow{\psi} B$. It holds for $\mathbf{Hilb}$. Give a counterexample to show that it fails in $\mathbf{Rel}$.

**Exercise 7.6.12.** Show that the CP–construction is a monoidal functor from the following category to itself: objects are positively monoidal compact dagger categories, morphisms are monoidal functors that preserve daggers.

## 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 [?]; the commutative case had already been established by Gelfand in 1943 [?]. Their major breakthrough lies in the notion of injectivity, as proved by Arveson in 1969 in [?]. This last work proves the fact we mentioned, that positive maps between commutative operator algebras are automatically completely positive.

Quantum information theory could be said to have grown out of operator algebra theory, and repurposed completely positive maps. See also the textbooks [?, ?]. This started around 1970 with the independent proofs of Choi in mathematics [?] and Kraus in physics [?] of their theorems. See also the tutorial [?].

The $\mathrm{CP_q}$-construction is originally due to Selinger in 2007 [?]. 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 [?]. Coecke, Heunen, and Kissinger extended the $\mathrm{CP_q}$–construction to all symmetric Frobenius structures rather than just quantum structures in 2013 [?]. Finally, the link to linear structures is due to Heunen, Kissinger, and Selinger [?]. The presentation in this chapter simplifies this development, and breaks with terminology from the literature: our $\mathrm{CP_q}$ is called CPM there, our $\mathrm{CP_c}$ is called $\mathrm{Stoch}$ there, and our $\mathrm{CP}$ is called $\mathrm{CP}^*$ there.

Environment structures are due to Coecke [?, ?]. This chapter leaves open the question how to characterize categories of the form $\mathrm{CP_c}[\mathbf{C}]$ or $\mathrm{CP}[\mathbf{C}]$. This involves the relationship between Frobenius structures in $\mathbf{C}$ and Frobenius structures in $\mathrm{CP}[\mathbf{C}]$, which is in general a difficult question [?].

The no-broadcasting theorem was proved in 1996 and is due to Barnum, Caves, Jozsa, Fuchs and Schumacher [?, ?]. The moral of the no-broadcasting results of Lemma 7.41 (and also the Heisenberg uncertainty of Exercise 7.6.12) could be read as: commutativity is not the “right” conceptual notion of classicality. This is a good example of the foundational results discussed in the introduction.

# Chapter 8

# Monoidal bicategories

Higher category theory is a generalization of category theory, in which morphisms can be composed in more than one way. In this chapter we introduce symmetric monoidal bicategories, and their graphical calculus based on surfaces. We investigate duality in monoidal bicategories, and see how the theory of commutative dagger-Frobenius algebras emerges from this in an elegant way. We then study the bicategory of 2–Hilbert spaces, the 'categorification' of ordinary Hilbert spaces, and show how we can use it to reason about quantum procedures.

## 8.1 Symmetric monoidal bicategories

In this section we begin by introducing bicategories and their graphical calculus. We define equivalences and dualities in bicategories, and prove that every equivalence can be promoted to a dual equivalence. We then define monoidal bicategories using the graphical calculus, and investigate their properties. There is a rich theory of duality in monoidal bicategories, and we show how it captures the properties of oriented surfaces, and use it to derive the axioms of a commutative dagger-Frobenius algebra.

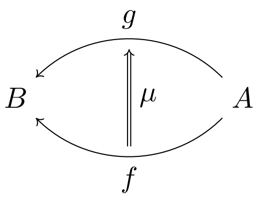
### 8.1.1 Introduction

We now give the definition of a bicategory, and at the same time the pasting diagram notation that is the traditional way to denote the elements of a bicategory. We draw the 1-morphism arrows of a pasting diagram from right to left, because this makes the notation for horizontal composition more intuitive.

**Definition 8.1.** A *bicategory* $\mathbf{C}$ consists of the following data:

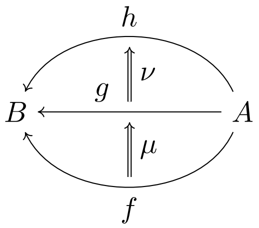
- a collection $\mathrm{Ob}(\mathbf{C})$ of *objects*;
- for any two objects $A, B$, a category $\mathbf{C}(A, B)$, with objects called *1-morphisms* $f$ drawn as $A \xrightarrow{f} B$, and morphisms $\mu$ called *2-morphisms* drawn as $f \overset{\mu}{\Longrightarrow} g$, or in full

form as follows:



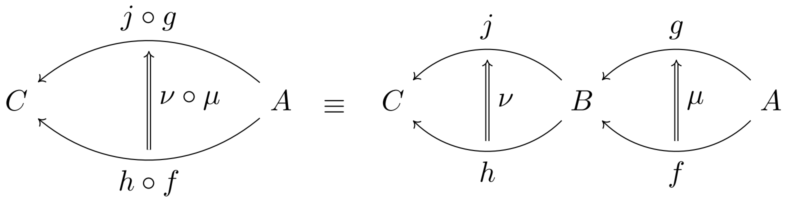
(8.1)

- for any two composable 2-morphisms in $\mathbf{C}(A,B)$ of type $f \overset{\mu}{\Longrightarrow} g$ and $g \overset{\nu}{\Longrightarrow} h$, an operation called *vertical composition* given by their composite as morphisms in $\mathbf{C}(A,B)$, denoted $f \overset{\nu\cdot\mu}{\Longrightarrow} h$ or in full form as follows:



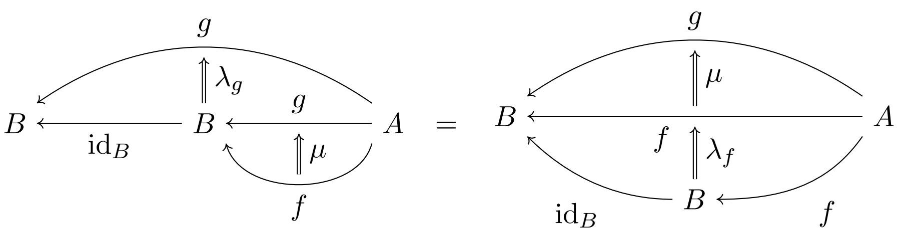
(8.2)

- for any triple of objects $A, B, C$ a functor $\circ : \mathbf{C}(A,B) \times \mathbf{C}(B,C) \to \mathbf{C}(A,C)$ called *horizontal composition*, with action on 1-morphisms and 2-morphisms drawn as follows:

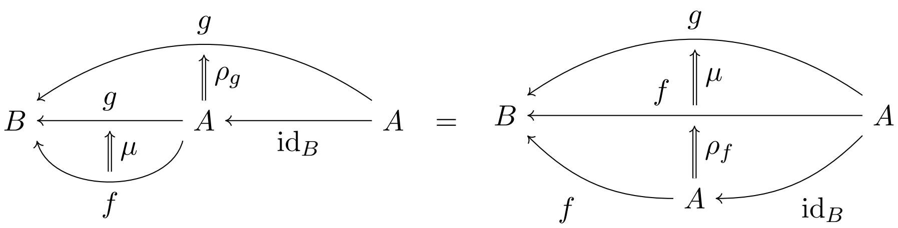


(8.3)

- 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 $f \overset{\mu}{\Longrightarrow} g$:



(8.4)



(8.5)

- for any triple of 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 for all $f \xRightarrow{\mu} f'$, $g \xRightarrow{\nu} g'$ and $h \xRightarrow{\sigma} h'$ we have $(\sigma \circ (\nu \circ \mu)) \cdot \alpha_{h,g,f} = \alpha_{h',g',f'} \cdot ((\sigma \circ \nu) \circ \mu)$.

This structure is required to be coherent, meaning that any well-formed diagram built from the components of $\alpha$, $\lambda$, $\rho$ and their inverses under horizontal and vertical composition must commute.

The theory of coherence for bicategories is essentially identical to the theory for monoidal categories, as examined in detail in Chapter 1. In particular, the data for a bicategory 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 $D \xrightarrow{j} E$:

$$\begin{array}{ccc} (g \circ \mathrm{id}_B) \circ f & \xRightarrow{\alpha_{g,\mathrm{id}_g,f}} & g \circ (\mathrm{id}_B \circ f) \\ & {\scriptstyle \rho_g \circ \mathrm{id}_f} \searrow \qquad \swarrow {\scriptstyle \mathrm{id}_g \circ \lambda_f} & \\ & g \circ f & \end{array} \tag{8.6}$$

$$\begin{array}{ccccc} & \big(j \circ (h \circ g)\big) \circ f & \xRightarrow{\alpha_{j,h\circ g,f}} & j \circ \big((h \circ g) \circ f\big) & \\ {\scriptstyle \alpha_{j,h,g} \circ \mathrm{id}_f} \nearrow & & & & \searrow {\scriptstyle \mathrm{id}_j \circ \alpha_{h,g,f}} \\ \big((j \circ h) \circ g\big) \circ f & & & & j \circ \big(h \circ (g \circ f)\big) \\ & {\scriptstyle \alpha_{j\circ h,g,f}} \searrow & & \nearrow {\scriptstyle \alpha_{j,h,g\circ f}} & \\ & & (j \circ h) \circ (g \circ f) & & \end{array} \tag{8.7}$$

This similarity to the theory of coherence for monoidal categories is no coincidence. In fact, bicategories are direct generalizations of monoidal categories.

**Theorem 8.2.** *A monoidal category is the same as a bicategory with one object.*

*Proof.* The correspondence is immediate from the definitions. We sketch it with the following table:

| **Monoidal category** | **One-object bicategory** |
|---|---|
| Objects | 1-morphisms |
| Morphisms | 2-morphisms |
| Composition | Vertical composition |
| Tensor product | Horizontal composition |
| Unit object | Identity 1-morphism |

(8.8)

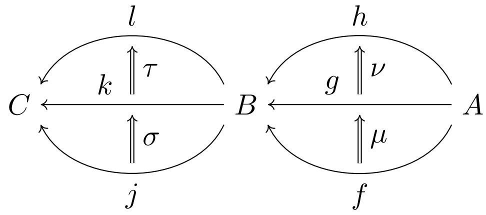
The transformations $\alpha$, $\lambda$ and $\rho$ are the same for both structures. □

**Definition 8.3** (Strict bicategory, 2-category)**.** A bicategory is *strict*, or a *2-category*, when the 2-morphisms $\alpha$, $\lambda$ and $\rho$ are the identity at every stage.

Just as for monoidal categories, an interchange law

$$(\tau \cdot \sigma) \circ (\nu \cdot \mu) = (\tau \circ \nu) \cdot (\sigma \circ \mu) \tag{8.9}$$

holds for bicategories, meaning that the following composite is well-defined:

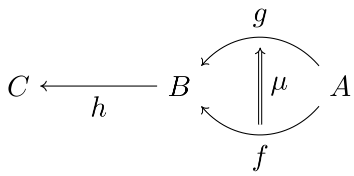



(8.10)

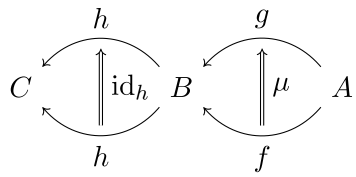
Because of the interchange law, rather than defining the full horizontal composition in a bicategory, it is enough to define *whiskering*.

**Definition 8.4.** In a bicategory, a *whiskering* of a 2-morphism $\mu$ is its horizontal composite with an identity 2-morphism:

$h \circ \mu \quad =$

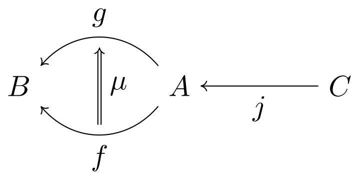



$:=$

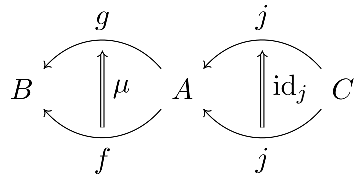



(8.11)

$\mu \circ j \quad =$




$:=$




(8.12)

Using the interchange law, we can express any horizontal composite as the vertical composite of whiskered 2-morphisms, for example where $f \overset{\mu}{\Rightarrow} g$ and $g \overset{\nu}{\Rightarrow} h$:

$$\mu \circ \nu \overset{(1)}{=} (\mathrm{id} \cdot \mu) \circ (\nu \cdot \mathrm{id}) \overset{(8.9)}{=} (\mathrm{id} \circ \nu) \cdot (\mu \circ \mathrm{id}) \tag{8.13}$$

Just as **Set** is an important motivating example of a category, so an important role is played by **Cat**, the bicategory of categories, functors and natural transformations.

**Definition 8.5.** The bicategory **Cat** is defined as follows:

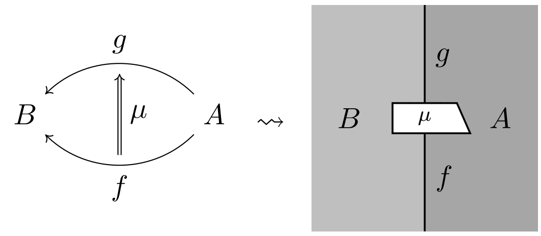
- **objects** are categories;
- **1-morphisms** are functors;
- **2-morphisms** are natural transformations;
- **vertical composition** is componentwise composition of natural transformations, with $(\mu \cdot \nu)_A := \mu_A \circ \nu_A$;
- **whiskering** is given by $(F \circ \mu)_A = F(\mu_A)$ and $(\mu \circ G)_A = \mu_{G(A)}$.

In fact, **Cat** is a strict bicategory, since composition of functors is strictly associative and unital.

### 8.1.2 Graphical calculus

There is a graphical calculus for bicategories, which is directly related to the graphical calculus for monoidal categories studied in Chapter 1: since a monoidal category is simply a bicategory with one object, the graphical calculus for monoidal categories is a special case for the graphical calculus for bicategories.

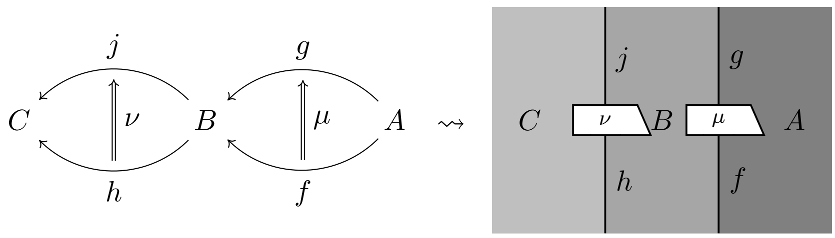
In this more general graphical calculus, objects are represented by regions, 1-morphisms by vertically-oriented lines, and 2-morphisms by vertices:



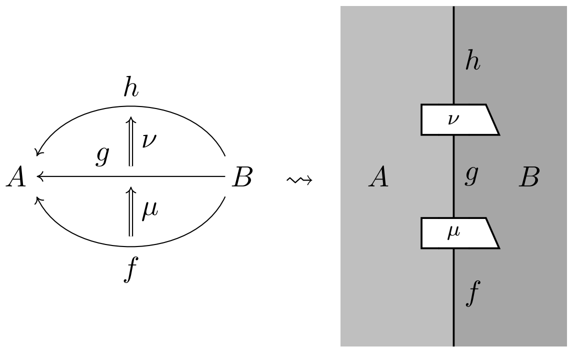

(8.14)

To translate a pasting diagram into the graphical calculus, there is 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 is represented by horizontal juxtaposition, and vertical composition is represented by vertical juxtaposition:




$= \nu \circ \mu$ (8.15)




$= \nu \cdot \mu$ (8.16)

When using the graphical notation, as for monoidal categories, the structures $\lambda$, $\rho$ and $\alpha$ are not depicted. There is also a correctness theorem, as we would expect.

**Theorem 8.6** (Correctness of the graphical calculus for a bicategory)**.** *A well-formed equation between 2-morphisms in a bicategory follows from the axioms if and only if it holds in the graphical language up to planar isotopy.*

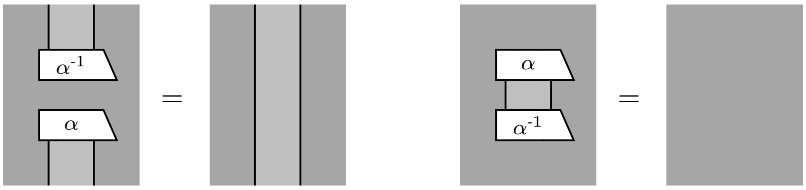
If we have only a single object $A$, which we may as well denote by a region coloured white, then the graphical calculus is identical to that of a monoidal category. This is just as we should expect, given Theorem 8.2.

We can use the graphical calculus to give a geometrical formulation of equivalence, in the style of Proposition 0.17. When applied in $\mathbf{Cat}$, this is equivalent to the traditional Proposition 0.17.

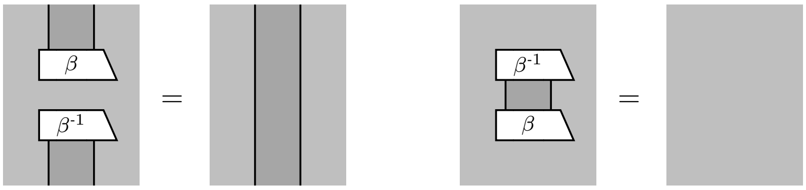
**Definition 8.7.** In a bicategory, an *equivalence* is a pair of objects $A$ and $B$, a pair of 1-morphisms $A \xrightarrow{F} B$ and $B \xrightarrow{G} A$, and invertible 2-morphisms $G \circ F \overset{\alpha}{\Longrightarrow} \mathrm{id}_A$ and $\mathrm{id}_B \overset{\beta}{\Longrightarrow} F \circ G$:

(8.17)

The invertibility equations take the following form:



(8.18)



(8.19)

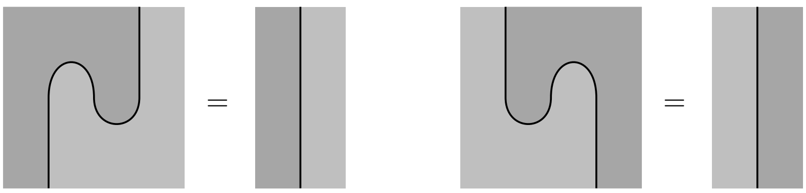
## 8.1.3 Duals for 1-morphisms

In a bicategory a 1-morphism $L$ can have a right dual $R$, and we write $L \dashv R$ for this situation. When the bicategory has one object it is just a monoidal category, and we recover the notion of dual objects in a monoidal category as studied in Chapter 3.

**Definition 8.8.** In a bicategory, a 1-morphism $A \xrightarrow{L} B$ has a *right dual* $B \xrightarrow{R} A$ when there are 2-morphisms $G \circ F \overset{\alpha}{\Longrightarrow} \mathrm{id}_A$ and $\mathrm{id}_B \overset{\beta}{\Longrightarrow} F \circ G$

(8.20)

satisfying the snake equations:



(8.21)

This concept of duality generalizes the classic idea of an adjunction, a central concept in category theory.

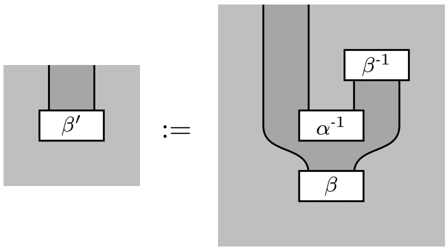
**Example 8.9.** In **Cat**, a duality $F \dashv G$ is exactly an adjunction $F \dashv G$ between $F$ and $G$ as functors.

It may seem that the concept of adjunction has been absent from this book. But thanks to this example, we see that in its generalized form, it has in fact been absolutely central.

We now prove a nontrivial theorem relating equivalences and duals. This is an abstract version of the classic theorem that every equivalence of categories can be promoted to an adjoint equivalence.

**Theorem 8.10.** *In a bicategory, every equivalence gives rise to a dual equivalence.*

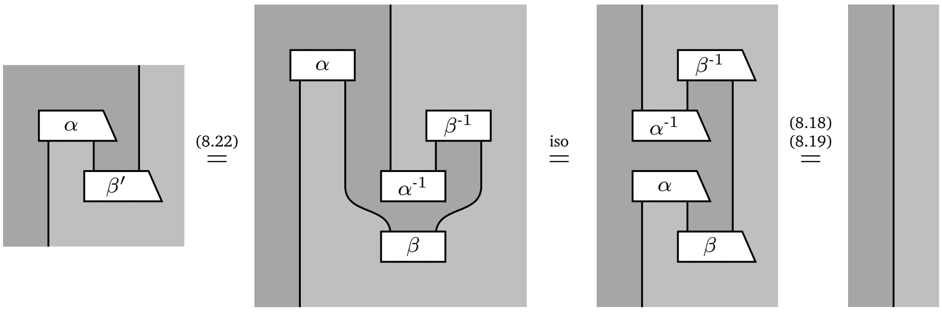
*Proof.* Suppose we have an equivalence in a bicategory in the manner of Definition 8.7, witnessed by invertible 2-morphisms $\alpha$ and $\beta$. Then we will build a new equivalence witnessed by $\alpha$ and $\beta'$, with $\beta'$ defined in the following way:




(8.22)

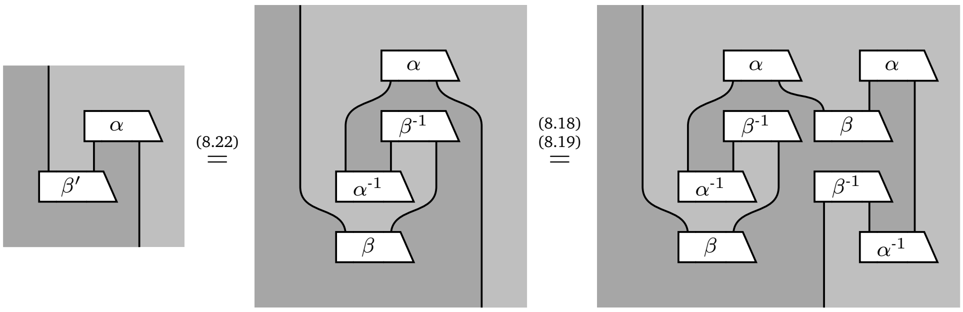
Since $\alpha'$ is composed from invertible 2-morphisms it must itself be invertible, and so it is clear that $\alpha'$ and $\beta$ still give an equivalence.

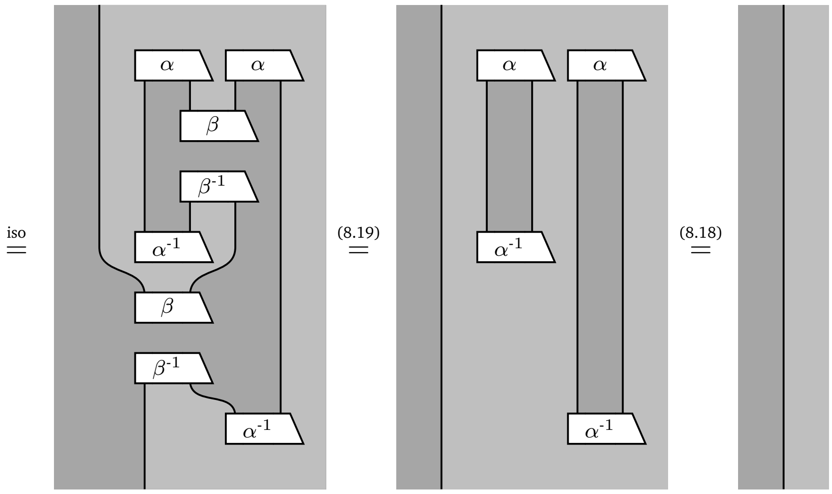
We now demonstrate that the adjunction equations are satisfied. The first adjunction equation takes following form:




(8.23)

The second is demonstrated as follows:






(8.24)

This completes the proof. □

Since monoidal categories are the same as bicategories with one object, we immediately have the following corollary.

**Corollary 8.11.** *In a monoidal category, if $A \otimes B \simeq B \otimes A \simeq I$, then $A \dashv B$ and $B \dashv A$.*

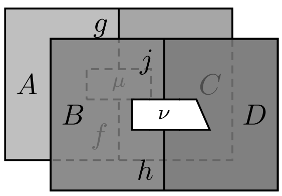
## 8.1.4 Monoidal bicategories

The algebraic definition of monoidal bicategory is extremely long, taking several pages to state. The graphical calculus, however, remains comprehensible and practical, continuing a trend we have seen throughout this book. We will take advantage of this and skip the algebraic definition, giving the graphical calculus directly. Formally, it is of course important that the algebraic definition exists, and that the graphical calculus is sound and complete for it; see the notes at the end of this chapter for more details.

To present the graphical calculus, we illustrate several of its main features by example: *tensor product*, *interchange*, and the *unit object*. The graphical calculus for a monoidal bicategory is 3-dimensional, and we use the dimension coming out of the page to indicate this third dimension, with a slightly angled perspective to make the pictures easier to understand.

**Definition 8.12.** The graphical calculus for a monoidal bicategory consists of the following components.

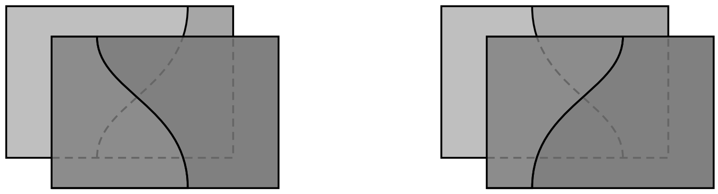
- **Tensor product.** Given 2-morphisms $f \overset{\mu}{\Longrightarrow} g$ and $h \overset{\nu}{\Longrightarrow} j$, the graphical representation of their *tensor product* 2-morphism $\mu \boxtimes \nu$ is given by 'layering' $\mu$ below $\nu$:




(8.25)

In this diagram we have $f \boxtimes h \xrightarrow{\mu \boxtimes \nu} g \boxtimes j$, 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*:

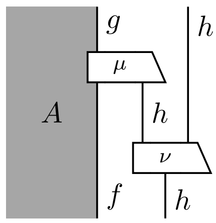


(8.26)

  This process itself gives a 2-morphism, which is called an *interchanger*. It is invertible, with two diagrams given above being each others' inverse.

  NATURALITY FOR INTERCHANGE.

- **Unit object.** A monoidal bicategory has a *unit object* $I$. This is represented by a 'blank' region, unlike other objects which are represented by shaded regions. Here is an example diagram involving the unit object, 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 $h \overset{\nu}{\Longrightarrow} h \circ h$:

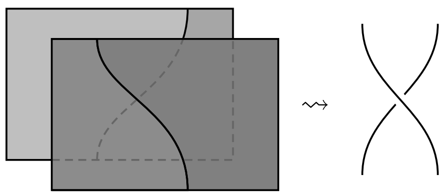



(8.27)

The basic rule governing the graphical calculus is encapsulated by this theorem.

**Theorem 8.13** (Correctness of the graphical calculus for monoidal bicategories)**.** *A well-formed equation between 2-morphisms in a monoidal bicategory follows from the axioms if and only if it holds in the graphical language up to 3-dimensional isotopy.*

An interesting phenomenon arises when we combine interchangers and the unit object. Consider the interchange diagrams (8.26), but with all 4 planar regions now labelled by the unit object:



(8.28)

We obtain exactly the graphical representation of a braid, which we have seen before in Section 1.2 as the graphical calculus for a braided monoidal category. Formally, the following theorem can be proved.

**Theorem 8.14.** *In a monoidal bicategory* $\mathbf{C}$*, then* $\mathbf{C}(I, I)$ *is a braided monoidal category.*

SYLLEPTIC MONOIDAL BICATEGORY.
SYMMETRIC MONOIDAL BICATEGORY.

**Example 8.15.** The bicategory **Cat** admits a monoidal structure, which we sketch as follows:

- **tensor product** $\mathbf{C} \times \mathbf{D}$ is the cartesian product of categories, which extends in a natural way to functors and natural transformations;
- the **unit object** is the category **1** with a single morphism.

### 8.1.5 Duals for objects

In a monoidal bicategory, an object has a right dual when the surface representing it in the graphical calculus can be 'folded' in a well-behaved way.

**Definition 8.16.** In a monoidal bicategory, an object $A$ has a *right dual* $B$ when it can be equipped with 1-morphisms called *folds*

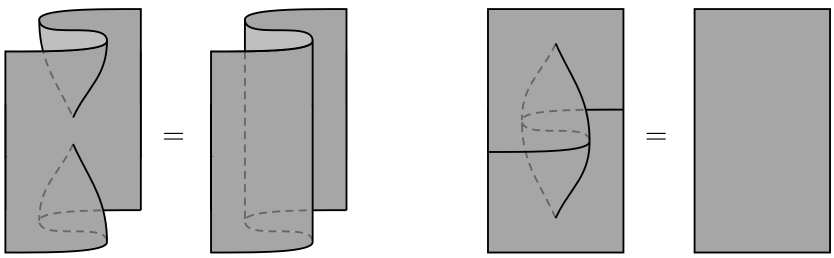

(8.29)

and invertible 2-morphisms called *cusps*:

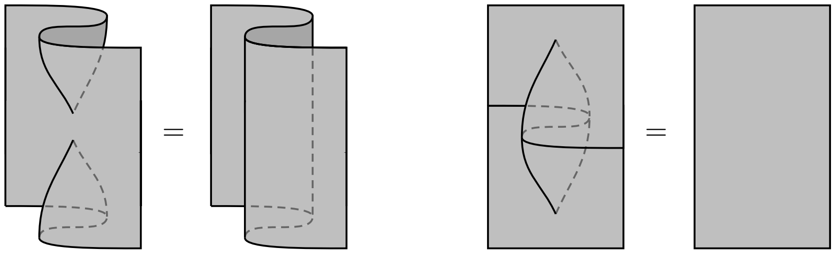
(8.30)

(8.31)

The invertibility equations take the following graphical form:

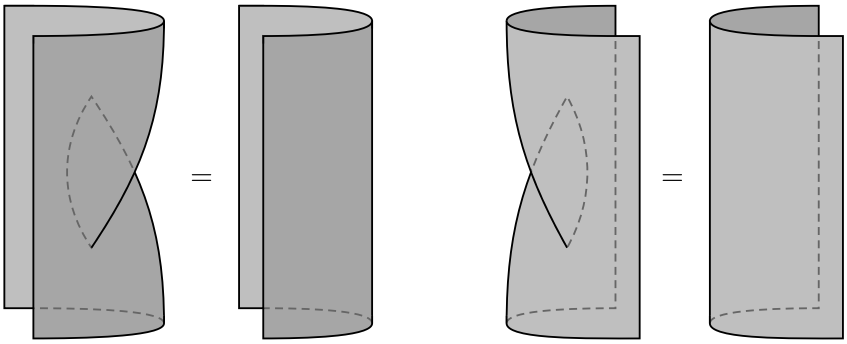



(8.32)



(8.33)

**Definition 8.17.** In a monoidal bicategory, a dual pair of objects is *coherent* when the *swallowtail equations* are satisfied:



(8.34)

Notice the use of the interchanger moves (8.26) on the left-hand sides of each equation.

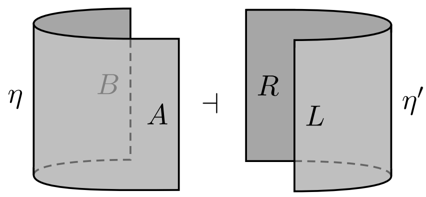
It turns out that, just as with an equivalence in a bicategory, these extra equations come for free.

**Theorem 8.18.** *In a monoidal bicategory, every dual pair of objects gives rise to a coherent dual pair.*

*Proof sketch.* This is proved in a similar way to Theorem 8.10; some of the cusp 2-morphisms are modified to give a new family of cusps, which can be shown to satisfy the swallowtail equations. See the notes at the end of this chapter for more information. □

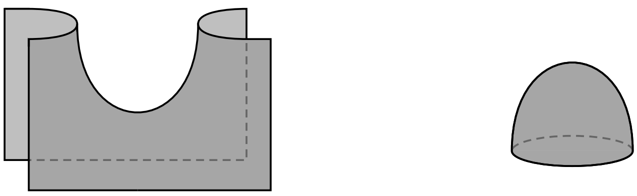
## 8.1.6 Oriented structure

To capture all the structure of oriented manifolds, we must further require that our fold morphisms (8.29) themselves have duals. To see what phenomena arise, let's investigate the case that the 2-morphism $\eta$ from (8.29) has a right dual $\eta'$:



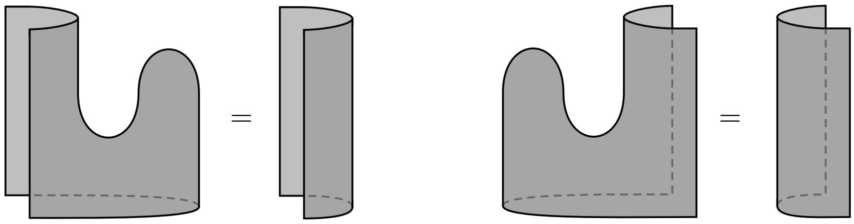

(8.35)

This duality has a unit and counit, which we draw as follows:



(8.36)

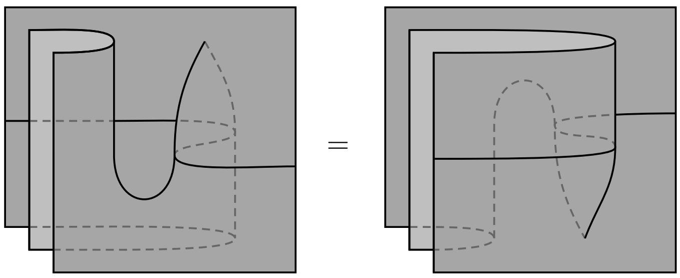
The snake equations (8.21) for the duality then look this:



(8.37)

We can interpret these equations as statements about isotopy of surfaces: for each equation, the left-hand side can be continuously deformed into the right-hand side, while keeping the boundary fixed.

**Definition 8.19.** In a monoidal bicategory, 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 $\varepsilon' \dashv \varepsilon$, and such that the resulting structures satisfy the *cusp flip equations*. We draw one of the cusp flip equations here:

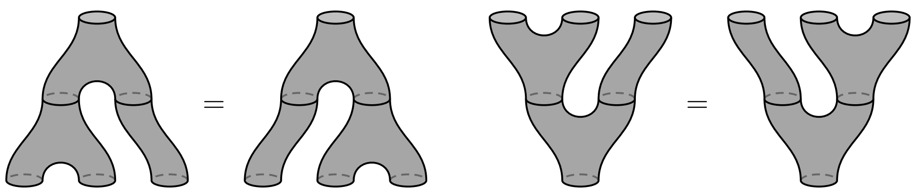


(8.38)

Each side of the equation involves one saddle 2-morphism and one cusp 2-morphism. The other cusp flip equations can be obtained from this one by reflections and rotations.

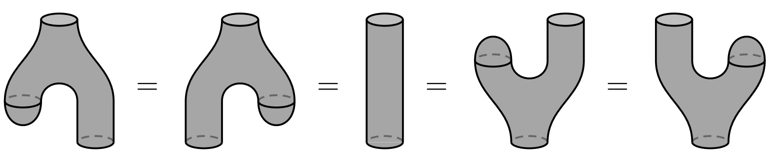
The graphical calculus of an oriented duality is sound for oriented surfaces: if a well-formed equation is provable under the axioms, then the associated oriented surfaces are isotopic. In particular, we can use the structure of an oriented duality to demonstrate the existence of a commutative Frobenius algebra in the braided monoidal category $\mathbf{C}(I, I)$.

**Theorem 8.20.** *An oriented structure in a monoidal bicategory induces a commutative dagger-Frobenius structure in the monoidal category of scalars.*

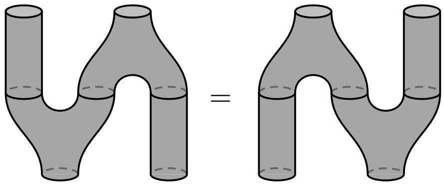


(8.39)

(8.40)



(8.41)



(8.42)

*Proof.* For each equation, we first note that the oriented surfaces on each side are isotopic. These isotopies are nontrivial to visualize for the commutativity equations (8.40). To see the isotopy, imagine starting with the left-hand side of the first of these equations. Grab hold of the 'shoulders', and rotate them clockwise as seen from above by a half-turn, leaving the boundaries fixed; this then gives the right-hand side.

Some of these equations can be proved quite easily. Equations (8.39) and (8.42) hold due to the interchange law for bicategories (8.9), and equations (8.41) follow from the snake equations (8.37).

The commutativity equations (8.40) have much more interesting proofs, requiring many applications of the axioms of an oriented duality:

[EXPLICIT PROOF OF COMMUTATIVITY OF PANTS]

[THIS WILL BE BEAUTIFUL! IT HAS NEVER BEFORE APPEARED IN PRINT.]

This completes the proof. □

## 8.2 2–Hilbert spaces

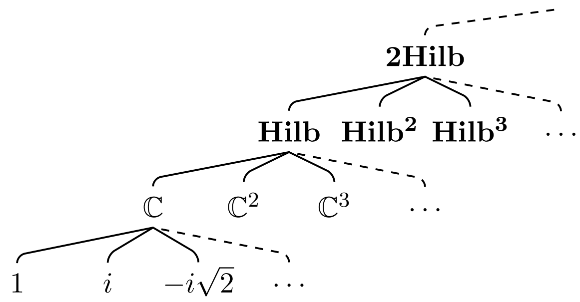
A 2–Hilbert space is a *category* with extra structure. 2–Hilbert spaces are 'categorifications' of ordinary Hilbert spaces, which are *sets* with extra structure. In this section we will see how 2–Hilbert spaces are defined, and look at the structures they support, which categorify the ordinary linear algebra structures of a Hilbert space. We will also show that every commutative dagger-Frobenius algebra in **Hilb** arises from an oriented duality in **2Hilb**.

### 8.2.1 Categorification

Categorification is the systematic replacement of set-based structures with category-based 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 monoidal categories as categorifications of ordinary monoids: the associativity and unit laws of a monoid become the natural isomorphisms $\alpha$, $\lambda$ and $\rho$, which are required to satisfy the triangle (1.1) and pentagon (1.2) laws in order to have good coherence properties. This issue of coherence does not arise for monoids, and so we see that categorification is not an automatic or algorithmic process; original mathematical work could be required to discover the fully-fledged categorified structure, which might not be unique.

2–Hilbert spaces are categorifications of ordinary Hilbert spaces, and organize themselves into a 2-category **2Hilb** which is a categorification of **Hilb**. This is analogous to the relationship between Hilbert spaces and complex numbers, with **Hilb** being a categorification of $\mathbb{C}$. The nested relationship between these structures is illustrated by the following diagram:




(8.43)

Instead of working with individual complex numbers directly, we can 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. Along with the other Hilbert spaces, they form a category **Hilb**, which is the 1-dimensional 2–Hilbert space. And the 2–Hilbert spaces themselves (**Hilb**, $\mathbf{Hilb}^2$, $\mathbf{Hilb}^3$, ...) form a bicategory **2Hilb**. This can itself be interpreted as the 1-dimensional 3–Hilbert space, and it is expected that the chain of definitions continues for all natural numbers.

### 8.2.2 Definition

We begin by introducing the basic theory of 2–Hilbert spaces.

**Definition 8.21.** A *$H^*$-category* $\mathbf{C}$ is a dagger category with the following properties:

- $\mathbf{C}(A, B)$ is a Hilbert space for each pair of objects $A$, $B$;
- composition is linear, satisfying

$$f \circ (g + h) = (f + g) \circ (f + h), \tag{8.44}$$
$$(f + g) \circ h = (f + h) \circ (g + h); \tag{8.45}$$

- the dagger is antilinear, satisfying

$$(s \bullet f + t \bullet g)^\dagger = s^\dagger \bullet f + t^\dagger \bullet g; \tag{8.46}$$

- for all morphisms $A \xrightarrow{f} B$, $B \xrightarrow{g} C$ and $A \xrightarrow{h} C$ we have

$$\langle g \circ f, h \rangle = \langle f, g^\dagger \circ h \rangle = \langle g, h \circ f^\dagger \rangle. \tag{8.47}$$

$H^*$-categories have got a nice connection to Frobenius algebras.

**Definition 8.22** (2–Hilbert space, Cauchy completeness)**.** A *2–Hilbert space* is a **Hilb**–dagger category which is *Cauchy complete*, meaning that it has all finite biproducts and all idempotents split.

Note how closely this matches the definition of an ordinary Hilbert space, as a Cauchy-complete inner product space; for more details, see the Notes at the end of this chapter.

There are many structural analogies between Hilbert spaces and 2–Hilbert spaces, which motivates the theory.

- Hilbert spaces have zero elements, while 2–Hilbert spaces have zero objects;
- Hilbert spaces have sums of elements $v + w$, while 2–Hilbert spaces have biproducts $A \oplus B$;
- in a Hilbert space we can multiply an element by any complex number, while in a 2–Hilbert space we can multiply an object by any Hilbert space;
- Hilbert spaces have an equality $\overline{\langle v|w\rangle} = \langle w|v\rangle$, while 2–Hilbert spaces have an isomorphism $\mathbf{H}(A,B)^* \simeq \mathbf{H}(B,A)$ given by the dagger structure;
- every finite-dimensional Hilbert space is of the form $\mathbb{C}^n$ up to isomorphism, while every finite-dimensional 2–Hilbert space is of the form $\mathbf{Hilb}^n$ up to equivalence.

The first of these is that, just as for Hilbert spaces, a 2–Hilbert space is determined up to equivalence by its dimension.

**Definition 8.23.** For a 2–Hilbert space $\mathbf{H}$, a *basis* is a set of mutually-nonisomorphic objects of $\mathbf{H}$, such that every object in $\mathbf{H}$ is a biproduct of elements of the basis in an essentially unique way.

**Definition 8.24.** In a 2–Hilbert space, an object $X$ is *simple* if $\mathrm{Hom}(X,X) \simeq \mathbb{C}$, or alternatively if it is not a zero object and there are no nonzero objects $Y$, $Z$ with $Y \oplus Z \simeq X$.

**Lemma 8.25.** *Every 2–Hilbert space has a basis, and any two bases have the same cardinality.*

*Proof.* That every 2–Hilbert space has a basis is shown in [**?**, Corollary 12].

For the second part, we first note that every element $X$ of a basis must be a simple object. For suppose $X \simeq 0$; then $X \simeq X \oplus X$, and the uniqueness condition is violated. Suppose also that $X \simeq Y \oplus Z$: then they themselves could by formed by taking a biproduct of basis elements, hence $X$ could also. But $X$ is itself a basis element, which contradicts the uniqueness part of the definition of a basis. Suppose now that we have two distinct bases $B$ and $B'$ for a 2–Hilbert space. Then any $b \in B$, must be a biproduct $b = \bigoplus_i b'_i$ of elements $b'_i \in B'$. But since $b$ is simple, we must in fact have $b \simeq b'$ for some $b' \in B'$. It is clear that this mapping $b \mapsto b'$ is a bijection, and so the bases have the same cardinality. □

The cardinality of a basis for a 2–Hilbert space $\mathbf{H}$ is called its *dimension*, and written $\dim(\mathbf{H})$.

**Lemma 8.26.** *Two 2–Hilbert spaces are equivalent if and only if they the same dimension.*

*Proof.* Suppose that two 2–Hilbert spaces $H_1$, $H_2$ are equivalent; then we can use the equivalence to transfer a basis of one onto the other, and then by Lemma 8.25 we see the bases must have the same cardinality. Suppose conversely the bases $B_1$ and $B_2$ have the same cardinality; then choose any bijection $\phi : B_1 \to B_2$, and define a functor $F : H_1 \to H_2$ as $F(b) := \phi(b)$ on basis elements of $H_1$, which we extend linearly by the property that $F(X \oplus Y) \simeq F(X) \oplus F(Y)$. Such a functor will be an equivalence. □

Given these results, we see that for every finite-dimensional 2–Hilbert space $H$, there is an equivalence

$$H \simeq \mathbf{Hilb}^{\dim(H)}, \tag{8.48}$$

where the right-hand side represents the Cartesian product of $\dim(H)$ copies of the category of finite-dimensional Hilbert spaces. This gives an analogy once again to the theory of ordinary Hilbert spaces, where for every finite-dimensional Hilbert space $J$, we have an isomorphism

$$J \simeq \mathbb{C}^{\dim(J)}. \tag{8.49}$$

2–Hilbert spaces are therefore quite tractable mathematical objects: up to equivalence, their objects are simply $n$-tuples of finite-dimensional Hilbert spaces, and their morphisms are $n$-tuples of linear maps.

Taking advantage of this structure theorem, we will in general restrict our attention to 2–Hilbert spaces of the form $\mathbf{Hilb}^n$ where $n$ is a natural number. In $\mathbf{Hilb}^n$ there are $n$ isomorphism classes of simple objects, of which a convenient family of representatives are $(\mathbb{C}, 0, \ldots, 0)$, $(0, \mathbb{C}, \ldots, 0)$, …, $(0, 0, \ldots, \mathbb{C})$. This family of objects provides a basis for $\mathbf{Hilb}^n$.

### 8.2.3 Matrix notation

A linear functor $\mathbf{Hilb}^n \to \mathbf{Hilb}^m$ is completely defined up to isomorphism by its action on a basis of simple objects of $\mathbf{Hilb}^n$, each of which will be mapped by $F$ to an object of $\mathbf{Hilb}^m$. We can use this to represent a linear functor as a matrix of Hilbert spaces:

$$\begin{pmatrix} F_{1,1} & F_{1,2} & \cdots & F_{1,n} \\ F_{2,1} & F_{2,2} & \cdots & F_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ F_{m,1} & F_{m,2} & \cdots & F_{m,n} \end{pmatrix} \tag{8.50}$$

This is analogous to the matrix representation of a bounded linear map between finite-dimensional Hilbert spaces with chosen basis.

Up to isomorphism, composition of functors is given by matrix composition, with biproduct and tensor product taking the place of addition and multiplication for ordinary matrix multiplication. For example, we can compose functors $\mathbf{Hilb}^2 \to \mathbf{Hilb}^2$ in the following way:

$$\begin{aligned} &\begin{pmatrix} G_{1,1} & G_{1,2} \\ G_{2,1} & G_{2,2} \end{pmatrix} \circ \begin{pmatrix} H_{1,1} & H_{1,2} \\ H_{2,1} & H_{2,2} \end{pmatrix} \\ &\simeq \begin{pmatrix} (G_{1,1} \otimes H_{1,1}) \oplus (G_{1,2} \otimes H_{2,1}) & (G_{1,1} \otimes H_{1,2}) \oplus (G_{1,2} \otimes H_{2,2}) \\ (G_{2,1} \otimes H_{1,1}) \oplus (G_{2,2} \otimes H_{2,1}) & (G_{2,1} \otimes H_{1,2}) \oplus (G_{2,2} \otimes H_{2,2}) \end{pmatrix} \end{aligned} \tag{8.51}$$

This is only isomorphic to the composite, rather than strictly equal, since composition of functors is strictly associative, but this composition operation is not. We have a tradeoff here that is common in higher category theory: by making our space of 1-cells easier to understand, a form of *skeletality*, we lose good properties of composition of 1-cells, a form of *strictness*.

We can also use the matrix calculus to describe objects of our 2–Hilbert spaces. Up to isomorphism, objects of a 2–Hilbert space $\mathbf{Hilb}^n$ correspond to functors $\mathbf{Hilb} \to \mathbf{Hilb}^n$, by considering the value taken by the functor on the object $\mathbb{C}$ in $\mathbf{Hilb}$. Using the matrix notation, an object $(H_1, \ldots, H_n)$ of $\mathbf{Hilb}^n$ corresponds to the following functor:

$$\begin{pmatrix} H_1 \\ H_2 \\ \vdots \\ H_n \end{pmatrix} \tag{8.52}$$

The action of functors on objects can be calculated (up to isomorphism) by composition of functors.

### 8.2.4 Natural transformations

A natural transformation $L : F \Rightarrow G$ between two matrices is given by a family of bounded linear maps $L_{i,j} : F_{i,j} \to G_{i,j}$. We write this as a matrix of linear maps, in the following way:

$$\begin{pmatrix} F_{1,1} & F_{1,2} \\ F_{2,1} & F_{2,2} \end{pmatrix} \xrightarrow{\begin{pmatrix} L_{1,1} & L_{1,2} \\ L_{2,1} & L_{2,2} \end{pmatrix}} \begin{pmatrix} G_{1,1} & G_{1,2} \\ G_{2,1} & G_{2,2} \end{pmatrix} \tag{8.53}$$

Vertical composition of 2-cells, 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 do not describe directly here.

There is a dagger functor † on **2Hilb**, in the sense of Section 2.3. In our matrix representation, it sends matrices of linear maps to matrices of their adjoints. So acting on the example above, it gives the following result:

$$\begin{pmatrix} G_{1,1} & G_{1,2} \\ G_{2,1} & G_{2,2} \end{pmatrix} \xrightarrow{\begin{pmatrix} {L_{1,1}}^\dagger & {L_{1,2}}^\dagger \\ {L_{2,1}}^\dagger & {L_{2,2}}^\dagger \end{pmatrix}} \begin{pmatrix} F_{1,1} & F_{1,2} \\ F_{2,1} & F_{2,2} \end{pmatrix} \tag{8.54}$$

This †-operation acts as the identity on objects and 1-morphisms.

### 8.2.5 Adjoints

Every linear functor between finite-dimensional 2–Hilbert spaces has a simultaneous left and right adjoint. In terms of the matrix formalism, this is constructed by constructing the dual Hilbert space for each entry in the matrix, and then taking the transpose of the matrix. This is analogous to the conjugate transpose operation that constructs the adjoint of a matrix representing a linear map between Hilbert spaces.

To take a concrete example, the adjoint $F^\dagger$ to the functor $F$ presented above in expression (8.50) has the following form:

$$\begin{pmatrix} F^*_{1,1} & F^*_{2,1} & \cdots & F^*_{m,1} \\ F^*_{1,2} & F^*_{2,2} & \cdots & F^*_{m,2} \\ \vdots & \vdots & \ddots & \vdots \\ F^*_{1,n} & F^*_{2,n} & \cdots & F^*_{m,n} \end{pmatrix} \tag{8.55}$$

To present the adjunction $F \dashv F^\dagger$, we must construct natural transformations $\mathrm{id}_{\mathbf{Hilb}_n} \overset{\sigma}{\Rightarrow} F^\dagger \circ F$ and $F \circ F^\dagger \overset{\tau}{\Rightarrow} \mathrm{id}_{\mathbf{Hilb}_m}$. These are defined in the following way, given unit and counit maps $\eta_{i,j} : \mathbb{C} \to F^*_{i,j} \otimes F_{i,j}$ and $\varepsilon_{i,j} : F_{i,j} \otimes F^*_{i,j} \to \mathbb{C}$:

$$\sigma = \begin{pmatrix} \bigoplus_j \eta_{1,j} & 0 & \cdots & 0 \\ 0 & \bigoplus_j \eta_{2,j} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \bigoplus_j \eta_{n,j} \end{pmatrix} \tag{8.56}$$

$$\tau = \begin{pmatrix} \bigoplus_j \varepsilon_{j,1} & 0 & \cdots & 0 \\ 0 & \bigoplus_j \varepsilon_{j,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \bigoplus_j \varepsilon_{j,n} \end{pmatrix} \tag{8.57}$$

Conversely, every adjunction $F \dashv F^\dagger$ is of this form for some family of unit and counit maps. Taking the adjoint of each of these linear maps gives data for the opposite adjunction $F^\dagger \dashv F$.

### 8.2.6 Monoidal structure

### 8.2.7 Oriented dualities

As a monoidal bicategory, **2Hilb** contains oriented dualities, given as follows.

**Lemma 8.27.** *Oriented dagger-dualities in* **2Hilb** *correspond up to equivalence to ...*

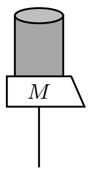
*Proof.* □

## 8.3 Modelling quantum procedures

We now show how we can use oriented dualities in **2Hilb** to model and reason about quantum procedures, connecting the material in Sections 8.1 and 8.2 with the rest of the book.

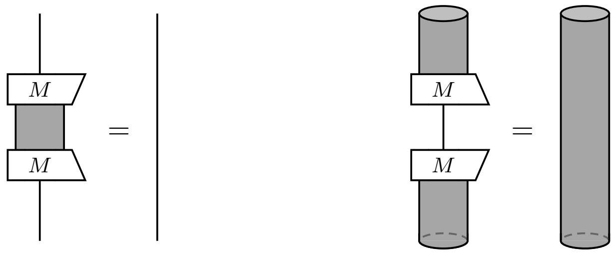
### 8.3.1 Measurement and controlled operations

Quantum measurement is represented by a unitary 2-morphism of the following type:



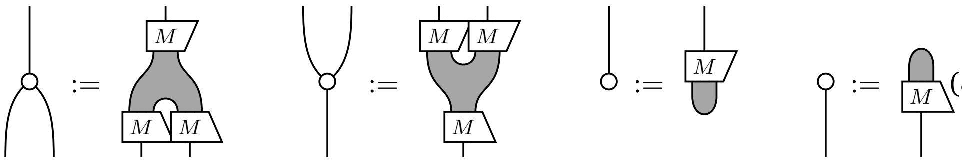

(8.58)

The unitarity equations take the following form:



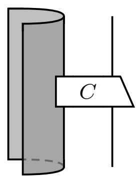

(8.59)

**Definition 8.28.** For a measurement, its *associated dagger Frobenius structure* is constructed as follows:



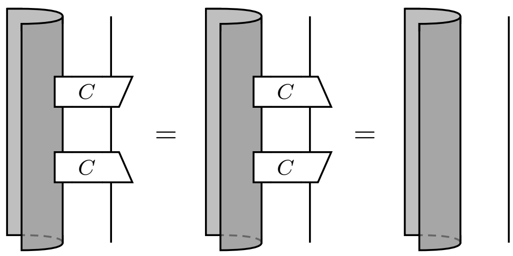

(8.60)

A controlled operation is represented by a 2-morphism of the following type:



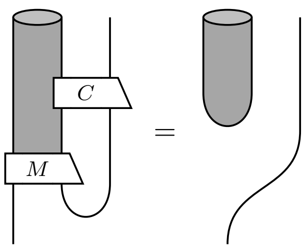

(8.61)

The unitarity equations take the following form:



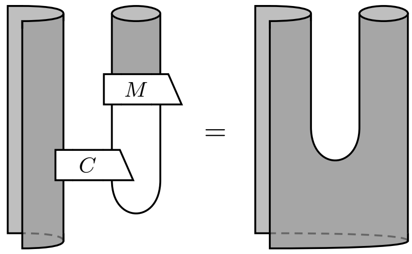

(8.62)

## 8.3.2 Quantum teleportation




(8.63)

### 8.3.3 Quantum dense coding



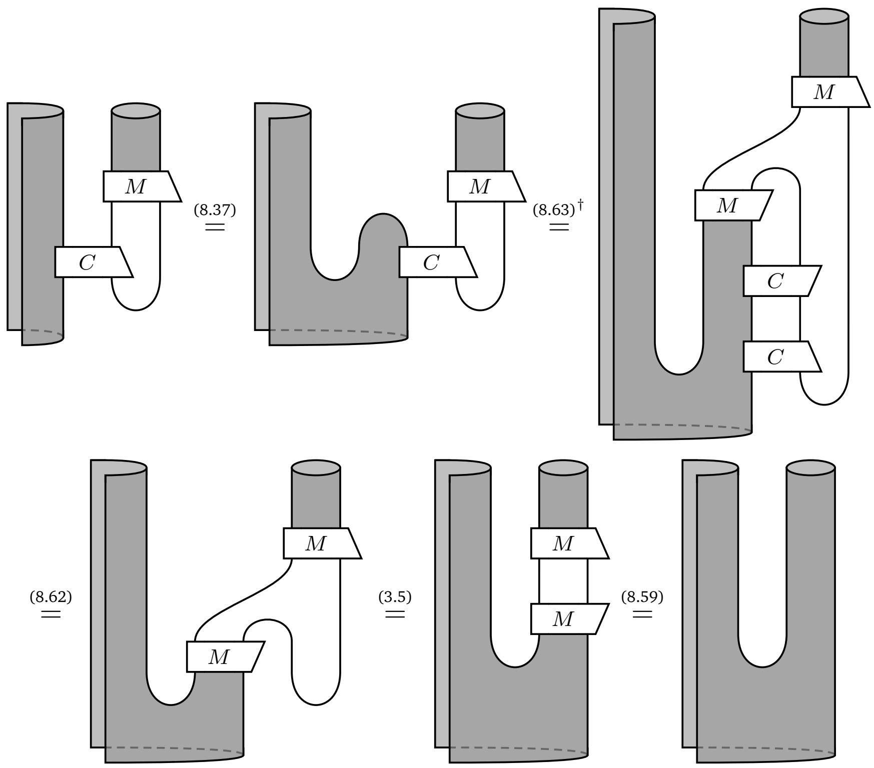

(8.64)

### 8.3.4 Equivalence

We can use the surface calculus to demonstrate the equivalence between teleportation and dense coding.

**Theorem 8.29.** *The definitions of dense coding and quantum teleportation are equivalent.*

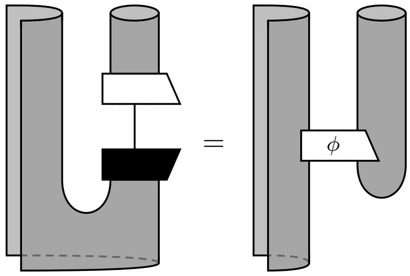
*Proof.* We derive the dense coding equation from the teleportation equation in the following way. First we deform the surface, then we use the dagger of the teleportation equation. The $C$ and $C^\dagger$ then cancel, allowing us to use the snake equation to straighten a wire, and then finally use unitarity of $M$.




The converse proof of quantum teleportation from dense coding is similar. □

### 8.3.5 Complementarity

**Definition 8.30.** Two measurements on the same Hilbert space satisfy the *2-complementarity condition* when there exists a unitary 2-morphism $\phi$ satisfying the following equation:

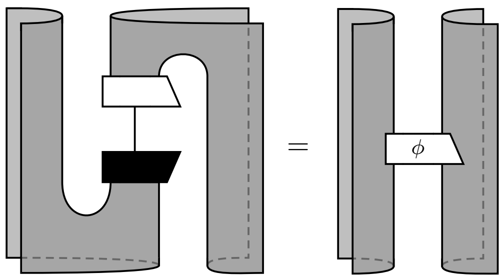



(8.65)

**Theorem 8.31.** *For a pair of measurements on a Hilbert space, the following are equivalent:*

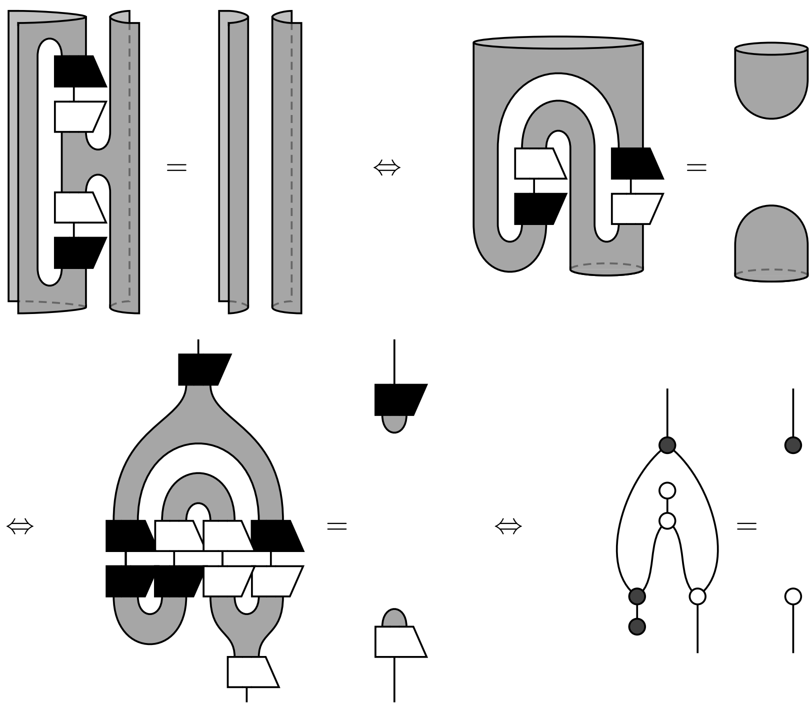
1. *they satisfy the 2-complementarity condition of Equation* (8.66)*;*
2. *their associated dagger-Frobenius algebras of Definition 8.28 satisfy the traditional complementarity condition of Definition 6.1.*

*Proof.* Taking the 2-complementarity condition and bending down the top-right part of the surface, we obtain the following equivalent condition:




(8.66)

This says exactly that the composite on the left-hand side is unitary. We write out the unitarity condition and rearrange it as follows:



This completes the proof. □

### 8.3.6 Teleportation from complementarity

We have seen in Section

## 8.4 Exercises

**Exercise 8.4.1.** Show that for a Hilbert space $\mathbf{H}$, then $\mathbf{2Hilb}(\mathbf{H},\mathbf{H})$ is a pivotal category, with tensor product given by composition of linear functors.

**Exercise 8.4.2.** IDEA: PROFUNCTOR EXAM QUESTION
MORE EXERCISES NEEDED.

# Notes and further reading

Higher-dimensional categories were first hinted at by Grothendieck [**?**]. For a modern overview, see [**?**]. 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—and $n$-categories have an $n$-dimensional graphical calculus; see [**?**].

Higher-dimensional algebra in physics: Baez, Dolan.

2-Hilbert spaces: Baez, Kapranov and Voevodsky.

2–Hilbert spaces via Cauchy completion: Bartlett, Lawvere.

2-dualizability: Schommer-Pries [**?**], Bartlett [**?**]

Relationship to CP: Heunen, Vicary and Wester.

# Index