Introduction to Categorical Quantum Mechanics

Chris Heunen and Jamie Vicary

February 20, 2013

Preface

Physical systems cannot be studied in isolation, since we can only observe their behaviour with respect to other systems, such as a measurement apparatus. The central idea of this course is that the ability to group individual systems into compound systems should be taken seriously. We take the action of grouping systems together as a primitive notion, and build models of quantum mechanics from there.

The mathematical tool we use for this is category theory, one of the most wide-ranging parts of modern mathematics. It has become abundantly clear that it provides a deep and powerful language for describing *compositional structure* in an abstract fashion. It provides a unifying language for an incredible variety of areas, including quantum theory, quantum information, logic, topology and representation theory.

These notes will tell this story right from the beginning, focusing on monoidal categories and their applications in quantum information.

Much of this relatively recent field of study is covered only fragmentarily or at the research level, see e.g. [18]. We feel there is a need for a self-contained text introducing categorical quantum mechanics at a more leisurely pace; these notes are intended to fill this space.

Acknowledgement

Thanks to the students who let us use them as guinea pigs for testing out this material! These notes would not exist were it not for the motivation and assistance of Bob Coecke. We are also grateful to Aleks Kissinger, Alex Merry and Daniel Marsden for careful reading and useful feedback on early versions.

Contents

Chapter 0

Background material

The ideal foundations for reading these notes are a familiarity with basic elements of both category theory and quantum computer science. This self-contained chapter fixes our notation and conventions, while briefly recalling the basic notions from both subjects that we will be using in these notes: categories, functors, natural transformations, vector spaces, Hilbert spaces, and tensor products.

0.1 Category theory

Category theory is quite different from other areas of mathematics. While a category is itself just an algebraic structure — much like a group, or a ring, or a field — we can use categories in a powerful way 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 which are formed by these relationships.

In this sense, category theory is more like a 'social science' which studies how individuals behave within a society, than a 'physical science' in which objects are reduced to their internal components. The categorical perspective is that we cannot know the internal structure of the systems we are studying, and we may only learn about them by observing their behaviour from the outside. While at first this seems limiting, in fact it is enormously powerful, as it becomes a very general language for the

description of many diverse structures.

Categories

The view of a category as a collection of objects and relationships between them is axiomatized in the following definition. The crucial point is that relationships should *compose*.

Definition 0.1 (Category)**.** A *category* $\mathbf{C}$ consists of:

- a collection $\mathrm{Ob}(\mathbf{C})$ of *objects*;
- for every two objects A, B a collection $\mathbf{C}(A, B)$ of *morphisms*;
- for every two morphisms $f \in \mathbf{C}(A, B)$ and $g \in \mathbf{C}(B, C)$, a morphism $g \circ f \in \mathbf{C}(A, C)$;
- for every object A a morphism $\mathrm{id}_A \in \mathbf{C}(A, A)$.

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

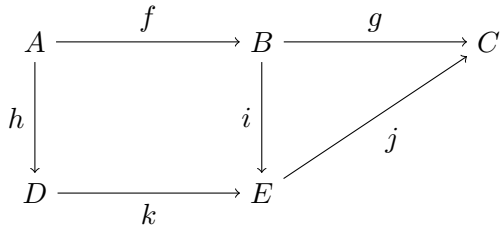
- associativity: $h \circ (g \circ f) = (h \circ g) \circ f$;
- identity: $\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A$.

The prototypical example is the category **Set**, with sets for objects and functions for morphisms.[1] Another example is the category **Vect** whose objects are complex vector spaces and whose morphisms are linear transformations, which we will discuss later on. We will meet more examples in Section 1.3.

We write $A \xrightarrow{f} B$ instead of $f \in \mathbf{C}(A, B)$ when no confusion can arise. Sometimes we will not even bother to name the objects and just talk about the morphism f. Then $A = \mathrm{dom}(f)$ is its *domain*, and $B = \mathrm{cod}(f)$ is its *codomain*.

[1] Our definition of a category refers to 'collections' of objects and morphisms, rather than sets, because sets are too 'small' in general. The category **Set** 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 these notes, and we may use set theory naively.

In category theory we often draw diagrams of morphisms, which indicate the way they can be composed. Here is an example.



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 the associativity property of Definition 0.1. Thus we have two ways to speak about equality of composite morphisms: by algebraic equations, or by commuting diagrams. Of central importance in these notes will be a third way, called the *graphical calculus*, which we introduce in Section 1.2.

A morphism $A \xrightarrow{f} B$ is an *isomorphism* when there exists a morphism $B \xrightarrow{f^{-1}} A$ satisfying $f \circ f^{-1} = \mathrm{id}_B$ and $f^{-1} \circ f = \mathrm{id}_A$. We say in this case that A and B are *isomorphic*. A category in which every morphism is an isomorphism is called a *groupoid*. If the isomorphic objects are all actually equal, then we say the category is *skeletal*.

Any category $\mathbf{C}$ has an *opposite* category $\mathbf{C}^{\mathrm{op}}$, 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 $\mathbf{C}$. If $\mathbf{C}$ and $\mathbf{D}$ are categories, there is a *product category* $\mathbf{C} \times \mathbf{D}$, whose objects are pairs (A, B) of object A from $\mathbf{C}$ and B from $\mathbf{D}$, and whose morphisms are pairs (f, g) of morphisms f in $\mathbf{C}$ and g in $\mathbf{D}$.

Functors

Remember the motto that morphisms are more important than objects. Categories are interesting mathematical objects in their own right. Category theory, the study of categories, takes its own medicine here: there are interesting notions of 'morphisms between categories', as in the following definition.

Definition 0.2 (Functor)**.** Given categories $\mathbf{C}$ and $\mathbf{D}$, a *functor* $F\colon \mathbf{C} \to \mathbf{D}$ is defined by the following data:

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

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 $\mathbf{C}^{\mathrm{op}} \to \mathbf{D}$.

Natural transformations

Going further, there is also an interesting notion of 'morphisms between functors'.

Definition 0.3 (Natural transformation)**.** Given functors $F\colon \mathbf{C} \to \mathbf{D}$ and $G\colon \mathbf{C} \to \mathbf{D}$, a *natural transformation* $\alpha\colon F \to G$ is an assignment for every object A in $\mathbf{C}$ of a morphism $F(A) \xrightarrow{\alpha_A} G(A)$ in $\mathbf{D}$, such that the following diagram commutes for every morphism $A \xrightarrow{f} B$ in $\mathbf{C}$.

$$\begin{array}{ccc} F(A) & \xrightarrow{\alpha_A} & G(A) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(B) & \xrightarrow[\alpha_B]{} & G(B) \end{array}$$

If every component α_A is an isomorphism then α is called a *natural isomorphism*, and F and G are said to be *naturally isomorphic*.

0.2 Hilbert spaces

In the traditional approach to quantum theory, the state space of a quantum system is formalized as a Hilbert space. The linear structure accounts for superposition of states, and the inner product gives the 'amplitudes' of observing one state given that the system is in another. Amplitudes are complex numbers in general, and we convert them to probabilities by taking the square of their absolute value.

The state space of a compound system is given by the tensor product of the state spaces of the component systems. We will now briefly recall each of these notions.

Inner product spaces

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

Definition 0.4 (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 is 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..

A function $f\colon V \to W$ between vector spaces is called *linear* when $f(u+v) = f(u) + f(v)$ for $u, v \in V$, and $f(a \cdot v) = a \cdot f(v)$ for $v \in V$ and $a \in \mathbb{C}$. Vector spaces and linear functions form a category **Vect**.

We will use some more structure on vector spaces. An inner product on a vector space lets us measure amplitudes between two vectors, and lengths of vectors.

Definition 0.5 (Inner product)**.** An *inner product* on a vector space V is a function $\langle -|-\rangle\colon V \times V \to \mathbb{C}$ satisfying the following properties, for $u, v, w \in V$ and $a \in \mathbb{C}$:

- conjugate-symmetric: $\langle v|w\rangle = \langle w|v\rangle^*$ for $v, w \in V$;
- linear in the second argument: $\langle v|a \cdot w\rangle = a \cdot \langle v|w\rangle$,
$$\langle u|v+w\rangle = \langle u|v\rangle + \langle u|w\rangle;$$
- positive definite: $\langle v|v\rangle \geq 0$,
$$\langle v|v\rangle = 0 \text{ if and only if } v = 0.$$

An inner product gives rise to a *norm* $\|v\| := \sqrt{\langle v|v\rangle}$. In turn, we can speak about the distance between two vectors u and v as $\|u - v\|$.

A Hilbert space is a vector space with an inner product in which it makes sense to sum up certain infinite sequences of vectors. The following definition makes this precise.

Definition 0.6 (Hilbert space)**.** A *Hilbert space* is a vector space H with an inner product that is *complete* in the following sense: if a sequence $v_1, v_2, \ldots$ of vectors satisfies $\sum_{i=1}^{\infty} \|v_i\| < \infty$, then there is a vector v such that $\|v - \sum_{i=1}^{n} v_i\|$ tends to zero.

Any vector space with an inner product can be completed to a Hilbert space.

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 $v \in H$.

A set $\{e_i\}$ of vectors is called *orthonormal* when $\langle e_i|e_i\rangle = 1$ for all i and $\langle e_i|e_j\rangle = 0$ for all $i \neq j$. It is called an orthonormal *basis* when every vector can be written as an infinite linear combination of e_i, i.e. when any vector v allows coordinates $v_i \in \mathbb{C}$ for which $\|v - \sum_i v_i \cdot e_i\|$ tends to zero. It is always possible to choose an orthonormal basis, but remember

that Hilbert spaces allow many different orthonormal bases. When there can be no confusion about the chosen orthonormal basis e_i, we sometimes write $|i\rangle$.

The *dimension* of a Hilbert space is the size, or *cardinality*, of an orthonormal basis; this is independent of the orthonormal basis used. We will mostly be concerned with finite-dimensional Hilbert spaces. A finite-dimensional vector space with an inner product is automatically a Hilbert space, and any linear map between finite-dimensional Hilbert spaces is automatically bounded.

If H is a Hilbert space, then so is $\mathbf{Hilb}(H, \mathbb{C})$, the set of bounded linear functions $H \to \mathbb{C}$. Any Hilbert space H has a *dual Hilbert space* H^*, with the same set of vectors as $\mathbf{Hilb}(H, \mathbb{C})$ and the same addition and inner product, but where scalar multiplication is conjugated: $z \cdot v$ in H^* equals $z^* \cdot v$ in $\mathbf{Hilb}(H, \mathbb{C})$. A Hilbert space is always isomorphic to its dual: the map $H \to H^*$ that sends $v \in H$ to the function $w \mapsto \langle v|w\rangle$ is an invertible bounded linear function.

Adjoints

We use the inner product to define the *adjoint* to a linear map.

Definition 0.7 (Adjoint of a bounded linear map)**.** 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 $\phi \in H$ and $\psi \in K$:

$$\langle f(\phi)|\psi\rangle = \langle \phi|f^\dagger(\psi)\rangle. \tag{1}$$

It follows immediately from (1) by uniqueness of adjoints that $(f^\dagger)^\dagger = f$, $(g \circ f)^\dagger = f^\dagger \circ g^\dagger$, and ${\mathrm{id}_H}^\dagger = \mathrm{id}_H$.

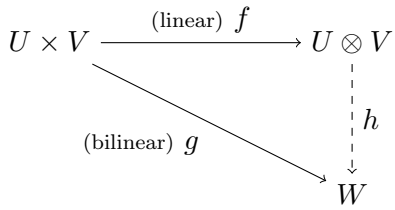
A *partial isometry* is a bounded linear map $f\colon H \to K$ satisfying $f = f \circ f^\dagger \circ f$. This means that $H = \ker(f) \oplus H'$ and that f preserves norm on the Hilbert space H'. This class of maps includes *projections* ($p\colon H \to H$ such that $p \circ p = p = p^\dagger$) and *isometries* ($f\colon H \to K$ such that $f^\dagger \circ f = \mathrm{id}_H$).

Tensor products

If V and W are vector spaces, then so is $V \times W$; this is called the *direct sum* and is also denoted by $V \oplus W$. This way of grouping two vector

spaces is classical, in the sense that states of the direct sum are completely determined by states of the constituent vector spaces. The tensor product is another way to make a new vector space out of two given ones, that allows for entangled states. With some work it 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 0.8 (Tensor product)**.** The *tensor product of vector spaces* U and V is a vector space $U \otimes V$ together with a linear 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 $h\colon U \otimes V$ 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 $\otimes\colon \mathbf{Vect} \times \mathbf{Vect} \to \mathbf{Vect}$.

If V and W carry inner products, we can furnish their direct sum with an inner product by $\langle (v_1,w_1) | (v_2,w_2) \rangle = \langle v_1 | v_2 \rangle + \langle w_1 | w_2 \rangle$. We can also furnish their tensor product as vector spaces with an inner product by $\langle v_1 \otimes w_1 | v_2 \otimes w_2 \rangle = \langle v_1 | w_1 \rangle \cdot \langle v_2 | w_2 \rangle$. If H and K are Hilbert spaces, their direct sum is again a Hilbert space $H \oplus K$, now called their orthogonal direct sum; the completion of their tensor product as vector spaces is again a Hilbert space, that we denote by $H \otimes K$. In this way, the tensor product is a functor $\otimes\colon \mathbf{Hilb} \times \mathbf{Hilb} \to \mathbf{Hilb}$. If $\{e_i\}$ is an orthonormal

basis for 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.

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, linguistics, cognitive science, philosophy, and many other areas, including physics. As a good first textbook, we recommend [7], but the more mathematically inclined might prefer the gold standard [56].

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 [66].

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. They form the core of these notes, as they provide the basic language with which the rest of the material will be developed. We introduce a visual notation called the graphical calculus, which provides an intuitive and powerful way to work with them. We also introduce our main examples of monoidal categories — **Hilb**, **Set** and **Rel** — which will be used as running examples throughout these notes.

1.1 Monoidal categories

Scope

We will soon give the precise mathematical definition of a monoidal category. To appreciate it, it is good to realize first what sort of situation it aims to represent. In general, one can think of objects $A, B, C, \ldots$ of a category as *systems*, and of morphisms $A \xrightarrow{f} B$ as *processes* turning the system A into the system B. This can be applied to a vast range of structures:

- 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;
- or even ingredients in stages of cooking, and recipes to process them from one state to another.

The extra structure of monoidal categories then simply says that we can consider processes occurring *in parallel*, as well as one after the other. In the examples above, one could interpret this as:

- letting separate physical systems evolve simultaneously;
- running computer algorithms in parallel;
- taking products or sums of algebraic or geometric structures;
- proving conjunctions of logical implications by proving both implications;
- chopping carrots while boiling rice.

Monoidal categories provide a general formalism for describing these general sorts of composition. It is perhaps surprising that a nontrivial theory can be developed at all from such simple intuition. But in fact, the theory of monoidal categories is remarkably rich, and provides a potent and elegant language for many developments in modern mathematics, physics and computer science.

Definition and coherence

Definition 1.1 (Monoidal category)**.** A monoidal category is a category $\mathbf{C}$ equipped with the following *data*, satisfying a property called *coherence*:

- a functor $\otimes\colon \mathbf{C} \times \mathbf{C} \to \mathbf{C}$, called the *tensor product*;
- an object $I \in \mathbf{C}$, called the *unit object;*
- a natural isomorphism whose components $(A \otimes B) \otimes C \xrightarrow{\alpha_{A,B,C}} A \otimes (B \otimes C)$ are called the *associators*;

- a natural isomorphism whose components $I \otimes A \xrightarrow{\lambda_A} A$ are called the *left unitors*;
- a natural isomorphism whose components $A \otimes I \xrightarrow{\rho_A} A$ are called the *right unitors*.

The coherence property is that every well-formed equation built from $\circ$, $\otimes$, id, α, α^{-1}, λ, λ^{-1}, ρ and ρ^{-1} is satisfied.

Interesting examples of such equations are the following *triangle* and *pentagon* identities.

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

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

By the coherence property, these diagrams must commute in any monoidal category. Conversely, and perhaps surprisingly, it turns out that these identities (1.1) and (1.2) are sufficient to ensure coherence. The following very important and beautiful theorem, which is too deep for us to prove here, records this.

Theorem 1.2 (Coherence for monoidal categories)**.** *The data for a monoidal category are coherent if and only if identities* (1.1) *and* (1.2) *hold.* □

This theorem implies the nontrivial but useful equation $\rho_I = \lambda_I$ (see Exercise 1.6.2).

Strictness

Some types of monoidal category are particularly simple.

Definition 1.3 (Strict monoidal category)**.** A monoidal category is *strict* if all components of the natural isomorphisms α, λ, and ρ, are identities.

In fact, every monoidal category can be 'made' into a strict one. The following deep theorem, which we state without proof, is tightly related to the Coherence Theorem 1.2.

Theorem 1.4 (Strictification)**.** *Every monoidal category is monoidally equivalent to a strict monoidal category.*

These notes will not give a definition of monoidal equivalence, which determines when two monoidal categories encode the same systems and processes.

This theorem means that, if you prefer, you can always 'strictify' your monoidal category to obtain an equivalent one for which α, λ and ρ are all identities. However, this is sometimes not very useful. For example, you often have some idea of what you want the objects of your category to be — but this might have to be abandoned to construct a strict version of your category. In particular, it's often useful for categories to be *skeletal*, meaning that if any pair A and B of objects are isomorphic, then they are equal. 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.

The interchange law

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

Theorem 1.5 (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 $\bigotimes\colon \mathbf{C} \times \mathbf{C} \to \mathbf{C}$ is a functor.

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

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

1.2 Graphical calculus

We now describe a graphical way to denote the basic protagonists of monoidal categories: objects, morphisms, composition, and tensor product. This graphical calculus faithfully captures the essence of working with monoidal categories. And in fact, in most cases, it makes them a lot easier to work with.

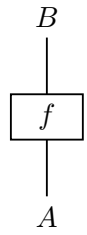
Graphical calculus for ordinary categories

We begin by describing a graphical notation for ordinary categories *without* any monoidal structure. We draw an object A as follows.

(1.4)

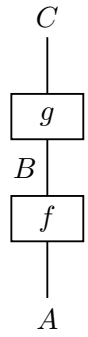
It's just a line. In fact, really, you shouldn't think of this as a picture of the object A; you should think of it as a picture of the identity morphism $A \xrightarrow{\mathrm{id}_A} A$. Remember, in category theory, the morphisms are more important than the objects.

We draw a general morphism $A \xrightarrow{f} B$ as follows, as a box with one 'input' at the bottom, and one 'output' at the top.



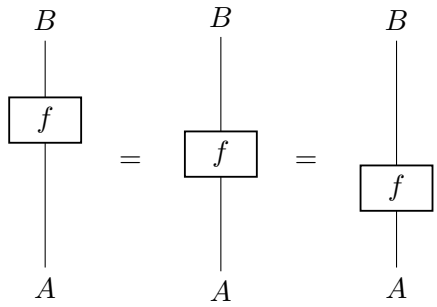
(1.5)

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.



(1.6)

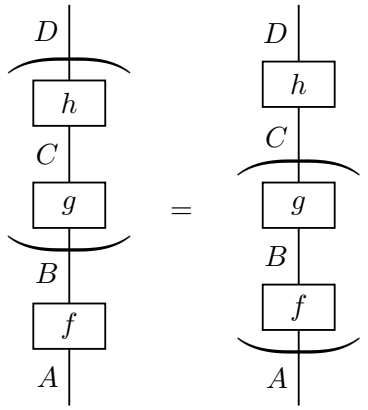
Let's use this to see what the identity law $f \circ \mathrm{id}_A = f = \mathrm{id}_B \circ f$ looks like.



(1.7)

It's completely trivial — we just have to remember that what is important is the *connectivity* of the diagram, not whether our lines are perfectly

straight, or wobble slightly. Categories also have an associativity axiom: given $C \xrightarrow{h} D$, we must have $(h \circ g) \circ f = h \circ (g \circ f)$. Graphically, this becomes the following.



(1.8)

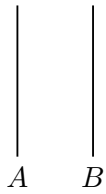
The brackets are here to show how we have built up each picture; they are not part of the notation. This associativity condition is trivial in the graphical representation; again, we just have to remember that only the connectivity of our diagram is important for identifying the morphism that the diagram defines.

So even for ordinary categories without any monoidal structure, the graphical calculus is already useful: it somehow 'absorbs' our axioms, 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 isn't so unfamiliar — we usually draw it horizontally, and call it algebra.

Graphical calculus for monoidal categories

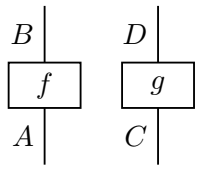
Now let's bring tensor products into the graphical notation. An object $A \otimes B$ — or rather, the morphism $\mathrm{id}_{A \otimes B}$ — is drawn as two lines side-by-

side.



(1.9)

Morphisms and composition are drawn in the same way as for ordinary categories. Given morphisms $A \xrightarrow{f} B$ and $C \xrightarrow{g} D$, we draw $A \otimes C \xrightarrow{f \otimes g} B \otimes D$ in the following way.



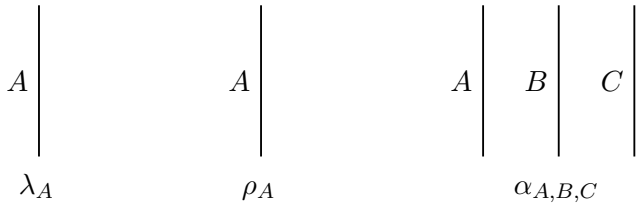
(1.10)

The idea is that f and g represent separate processes, taking place at the same time. Whereas the graphical calculus for ordinary categories was one-dimensional or *linear*, the graphical calculus for monoidal categories is two-dimensional or *planar*. The two dimensions correspond to the two ways to combine morphisms: by categorical composition (vertically) or by tensor product (horizontally).

The monoidal unit object I is drawn as the empty diagram.

(1.11)

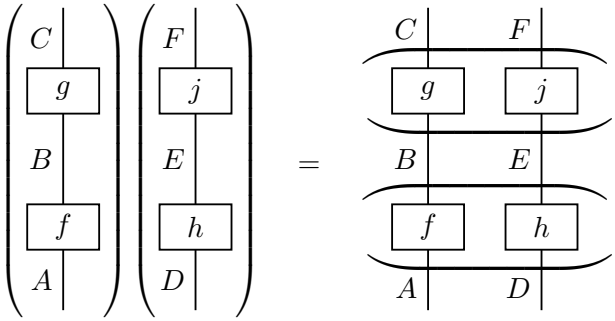
The left unitor $\lambda_A \colon I \otimes A \to A$, the right unitor $\rho_A \colon A \otimes I \to A$ and the associator $\alpha_{A,B,C} \colon (A \otimes B) \otimes C \to A \otimes (B \otimes C)$ are drawn as follows.



(1.12)

They are completely trivial. The coherence of α, λ and ρ is therefore important for the graphical calculus to function: since there can only be a single morphism formed from these natural isomorphisms between any two given objects, it doesn't matter that their graphical calculus encodes no information.

We now consider the graphical representation of the interchange law (1.3).



(1.13)

We use brackets to indicate how we are forming the diagrams on each side. Dropping the brackets, we see that 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 — simply melt away, allowing us to use the formalism much more directly. These features are still there, but they are absorbed into the geometry of the plane, of which our species has an excellent automatic understanding.

It can be formally proven that the morphisms represented by two given diagrams are equal under the axioms of a monoidal category if and only if one diagram can be deformed into the other respecting the geometry of the plane. That is, you can continuously move boxes around in the plane, as long as you don't introduce crossings or allow wires to be detached from the upper and lower boundaries.

1.3 Examples

It is now high time to have some examples. The following three monoidal categories will be our running examples throughout these notes.

Hilbert spaces

Our first example is **Hilb**, the monoidal category of Hilbert spaces, which will play a central role in these notes. We also discuss the closely related categories **FHilb** and $\mathbf{FHilb_{ss}}$. See Section 0.2 for a brief first introduction to the theory of Hilbert spaces.

Definition 1.6. The monoidal category **Hilb** is defined in the following way:

- **Objects** are Hilbert spaces $H, J, K, \ldots$;
- **Morphisms** are bounded linear maps $f, g, h, \ldots$;
- **Composition** is composition of linear maps;
- **Identity maps** are given by the identity linear maps;
- **Tensor product** $\otimes \colon \mathbf{Hilb} \times \mathbf{Hilb} \to \mathbf{Hilb}$ is the tensor product of Hilbert spaces;
- **The unit object** I is the one-dimensional Hilbert space $\mathbb{C}$;
- **Associators** $\alpha_{H,J,K} \colon (H \otimes J) \otimes K \to H \otimes (J \otimes K)$ are the unique linear maps satisfying $|\phi\rangle \otimes \big(|\chi\rangle \otimes |\psi\rangle\big) \mapsto \big(|\phi\rangle \otimes |\chi\rangle\big) \otimes |\psi\rangle$ for all $|\phi\rangle \in H$, $|\chi\rangle \in J$ and $|\psi\rangle \in K$;
- **Left unitors** $\lambda_H \colon \mathbb{C} \otimes H \to H$ are the unique linear maps satisfying $1 \otimes |\phi\rangle \mapsto |\phi\rangle$ for all $|\phi\rangle \in H$;
- **Right unitors** $\rho_H \colon H \otimes \mathbb{C} \to H$ are the unique linear maps satisfying $|\phi\rangle \otimes 1 \mapsto |\phi\rangle$ for all $|\phi\rangle \in H$.

You might have noticed that this definition of **Hilb** makes no mention of the *inner products* on the Hilbert spaces. This structure is crucial for

quantum mechanics, so it's perhaps surprising it hasn't made an appearance here. In fact, in the development of this subject, it took quite a while for people to understand the correct way to deal with it categorically. We will encounter the inner product in Section**??**.

We also define a finite-dimensional variant of **Hilb**.

Definition 1.7. The monoidal category **FHilb** has finite-dimensional Hilbert spaces as objects; the rest of the structure is the same as for **Hilb**, in particular morphisms and tensor products.

This is particularly appropriate for the purposes of quantum information theory, where the main results are often in finite dimensions.

Neither of the monoidal categories **Hilb** or **FHilb** are strict, and neither of them are skeletal. However, for **FHilb**, there is a *monoidally equivalent* monoidal category which *is* strict and skeletal, which we call $\mathbf{FHilb_{ss}}$.

Definition 1.8. The strict, skeletal monoidal category $\mathbf{FHilb_{ss}}$ 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;
- **Tensor product** $\otimes\colon \mathbf{FHilb_{ss}} \times \mathbf{FHilb_{ss}} \to \mathbf{FHilb_{ss}}$ is given by $n \otimes m := nm$ on objects, and on morphisms by Kronecker product of matrices:

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

- **The tensor unit** is the natural number 1;
- **Associators, left unitors and right unitors** are the identity matrices.

Objects n in $\mathbf{Hilb_{ss}}$ can be thought of as the Hilbert space $\mathbb{C}^n$, which are equipped with a privileged basis. Linear maps between such Hilbert spaces can be canonically represented as matrices. In practice, this monoidal category $\mathbf{FHilb_{ss}}$ is the most convenient place to work when doing calculations involving finite-dimensional Hilbert spaces. If you have done calculations with finite-dimensional Hilbert spaces, for example as part of an exercise in quantum computing, you have really been working in this category.

We do not give a full treatment of the notion of *monoidal equivalence* in these notes, but it seems intuitively possible that $\mathbf{FHilb_{ss}}$ somehow 'captures' everything that is important about **FHilb** as a monoidal category.

Sets and functions

While **Hilb** is relevant for *quantum* physics, the monoidal category **Set** is an important setting for *classical* physics.

Definition 1.9. The monoidal category **Set** is defined in the following way:

- **Objects** are sets;
- **Morphisms** are functions;
- **Composition** is function composition;
- **Identity morphisms** are given by the identity functions;
- **Tensor product** is Cartesian product of sets, written '$\times$';
- **The unit object** is a chosen 1-element set $\{\bullet\}$;
- **Associators** $\alpha_{A,B,C} \colon (A \times B) \times C \to A \times (B \times C)$ are the functions given by $\big((a,b),c\big) \mapsto \big(a,(b,c)\big)$ for $a \in A$, $b \in B$, and $c \in C$;
- **Left unitors** $\lambda_A \colon I \times A \to A$ are the functions given by $(\bullet, a) \mapsto a$ for $a \in A$;
- **Right unitors** $\rho_A \colon A \times I \to A$ are the functions given by $(a, \bullet) \mapsto a$ for $a \in A$.

Definition 1.10. The monoidal category **FSet** has finite sets for objects, and the rest of the structure is the same as in **Set**.

If you have studied some category theory, you might know that the Cartesian product in **Set** is a (categorical) *product*. We have an example here of a general phenomenon: if a category has products, then these can be used to give a monoidal structure. The same is true for coproducts, which in **Set** are given by disjoint union.

This gives us an important difference between **Hilb** and **Set**: while the tensor product on **Set** comes from a categorical product, the tensor product on **Hilb** does not. (See also Chapter 6 and Exercise 2.5.3.) We will discover many more differences between **Hilb** and **Set**, which often tells us about the differences between quantum and classical information.

Sets and relations

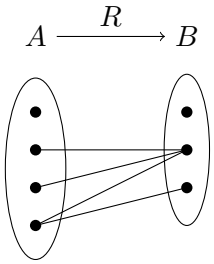
While **Hilb** is a setting for quantum physics and **Set** is a setting for classical physics, **Rel**, the category of sets and relations, is somewhere in the middle. It seems like it should be a lot like **Set**, but in fact, its properties are much more like those of **Hilb**. This makes it an excellent test-bed for investigating different aspects of quantum mechanics from a categorical perspective.

Definition 1.11. 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 for elements of A to evolve into elements of B. This

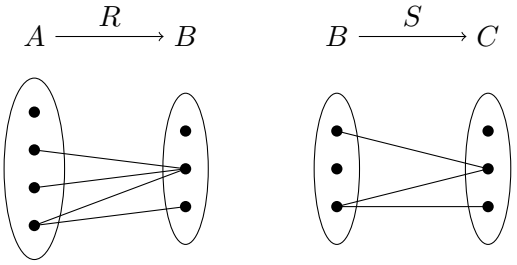
suggests the following sort of picture.



(1.14)

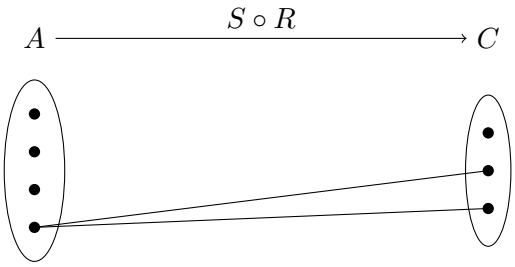
This suggests we interpret a relation as a sort of nondeterministic classical process: each element of A can evolve into any element of B to which it is related. Nondeterminism enters here because an element of A can be related to more than one element of B, so under this interpretation, we cannot predict 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 target of the first equal to the source 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 our example above, this gives

rise to the following composite relation.



This definition of relational composition has the following algebraic form.

$$S \circ R := \{(a, c) \mid \exists b \in B \colon aRb \text{ and } bSc\} \subseteq A \times C \tag{1.15}$$

We can write this differently as

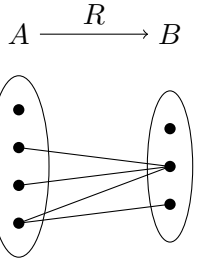
$$a\,(S \circ R)\,c \;\Leftrightarrow\; \bigvee_b (bSc \wedge aRb), \tag{1.16}$$

where $\vee$ represents logical OR, and $\wedge$ represents logical AND.

Comparing this with the definition of matrix multiplication, we see a strong similarity:

$$(g \circ f)_{ij} = \sum_k g_{ik} f_{kj} \tag{1.17}$$

This suggests another way to interpret a relation: as a matrix of truth values. For the example relation (1.14), this gives the following matrix, where we write 0 for false and 1 for true:



$$\leftrightsquigarrow \qquad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \tag{1.18}$$

Composition of relations is then just given by ordinary matrix composition, with OR and AND replacing $+$ and $\times$.

This gives an interesting analogy between quantum mechanics 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 $H \xrightarrow{L} J$ gives us an *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.

Definition 1.12. The monoidal category **Rel** is defined in the following way:

- **Objects** are sets;
- **Morphisms** $A \xrightarrow{R} B$ are relations;
- **Composition** of two relations $A \xrightarrow{R} B$ and $B \xrightarrow{S} C$ is given as in (1.15) above;
- **Identity morphisms** $A \xrightarrow{\mathrm{id}_A} A$ are the relations $\{(a, a) \mid a \in A\} \subseteq A \times A$;
- **Tensor product** is Cartesian product of sets, written '$\times$';
- **The unit object** is a chosen 1-element set $\{\bullet\}$;
- **Associators** $\alpha_{A,B,C} \colon (A \times B) \times C \to A \times (B \times C)$ are the relations defined by $\big((a, b), c\big) \sim \big(a, (b, c)\big)$ for all $a \in A$, $b \in B$ and $c \in C$;
- **Left unitors** $\lambda_A \colon I \times A \to A$ are the relations defined by $(\bullet, a) \sim a$ for all $a \in A$;
- **Right unitors** $\rho_A \colon A \times I \to A$ are the relations defined by $(a, \bullet) \sim a$ for all $a \in A$.

The monoidal category **FRel** is the restriction of the monoidal category **Rel** to finite sets.

1.4 States

States of general objects

Morphisms out of the tensor unit I play a special role in a monoidal category. In many cases we can think of such morphisms as generalized 'states' or 'points', even though the objects might not be sets at all and thus have no recognizable elements, points, or states.

Definition 1.13 (State)**.** In a monoidal category, a *state* of an object A is a morphism $I \to A$.

We now examine what the states are in our three example categories.

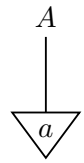
- In **Hilb**, points of a Hilbert space H are linear functions $\mathbb{C} \to H$, which correspond to elements of H by considering the image of $1 \in \mathbb{C}$;
- In **Set**, points of a set A are functions $\{\bullet\} \to A$, which correspond to elements of A by considering the image of $\bullet$;
- In **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 1.14 (Well-pointed)**.** 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 $I \xrightarrow{a} A$.

The idea is that in a well-pointed category, we can tell whether or not morphisms are equal just by seeing how they affect points of their domain objects. The categories **Set**, **Hilb**, and **Rel** are all well-pointed. However, using well-pointedness somewhat goes against the philosophy of category theory that you should not try to use internal structure of objects.

Graphical representation

To emphasize that states $I \xrightarrow{a} A$ have the empty picture (1.11) as their domain, we will draw them as triangles instead of boxes.

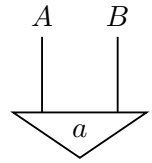


(1.19)

We can think of this dynamically as a *method of preparing* A: we begin with the empty system at the bottom of the diagram, and then after the process occurs, we have an instance of system A. The emphasis here is on the process that takes place, rather than the configuration of A which results.

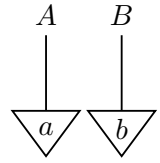
Entanglement and product states

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



(1.20)

A joint state is a *product state*, or *separable*, 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 $I \xrightarrow{b} B$.



(1.21)

An *entangled state* is a joint state which 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.

Let's see what these look like in our example categories.

- In **Hilb**:
  - **Joint states** of H and J are elements of $H \otimes J$;
  - **Product states** are factorizable states;
  - **Entangled states** are elements of $H \otimes J$ 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 $P \subseteq A \times B$ such that, for some $R \subseteq A$ and $S \subseteq B$, $(a, b) \in P$ if and only if $a \in R$ and $b \in S$;
  - **Entangled states** are subsets of $A \times B$ that are not of this form.

This gives us an insight into why entanglement can be difficult for us to understand intuitively: classically, in the worldview encoded by the category **Set**, it simply does not occur. If we allow possibilistic behaviour as encoded by **Rel**, then an analogue of entanglement *can* be described in a classical way.

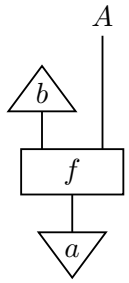
Effects

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

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

Effects are 'opposite' to states, in the sense that states are morphisms of type $I \to A$.

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:



(1.22)

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 b. This does not imply that the effect b was the *only* possible outcome for the measurement; just that by drawing this diagram, we are only interested in the cases when it is. An effect in a string diagrams can be thought of as a *postselection*: we run our entire experiment, only choosing whether to keep the resulting state after checking that our measurement had the correct 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.

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 **Hilb**, we require a, f and b 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 **Rel**, we need put no particular requirements on a, f and b — 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 zero, that means this particular sequence of a state preparation, a dynamics step, and measurement result cannot occur.

Things are very different in **Set**. The monoidal unit object is *terminal* in that category, meaning $\mathrm{Hom}(A, I)$ has only a single element for any object A. So every object has a *unique* effect, and there is no nontrivial notion of 'measurement'. Indeed, the deterministic classical physics encoded by this category is very different from our other example categories, as we will see repeatedly throughout these notes.

1.5 Braiding and Symmetry

We have seen that the graphical calculus for monoidal categories allows us to move around boxes, as long as we don't cut wires or introduce crossings. We now discuss the kinds of monoidal categories for which crossings are allowed.

Braided monoidal categories

We first consider braided monoidal categories.

Definition 1.16. A *braided monoidal category* is a monoidal category $\mathbf{C}$ equipped with a natural isomorphism whose components

$$\sigma_{A,B} \colon A \otimes B \to B \otimes A \tag{1.23}$$

satisfy the following *hexagon identities*.

$$\begin{array}{ccccc}
 & & A \otimes (B \otimes C) & \xrightarrow{\sigma_{A,B\otimes C}} & (B \otimes C) \otimes A \\
 & \nearrow^{\alpha_{A,B,C}} & & & \searrow^{\alpha_{B,C,A}} \\
(A \otimes B) \otimes C & & & & B \otimes (C \otimes A) \\
 & \searrow_{\sigma_{A,B} \otimes \mathrm{id}_C} & & & \nearrow_{\mathrm{id}_B \otimes \sigma_{A,C}} \\
 & & (B \otimes A) \otimes C & \xrightarrow[\alpha_{B,A,C}]{} & B \otimes (A \otimes C)
\end{array} \tag{1.24}$$

$$\begin{array}{ccccc} & & A \otimes (B \otimes C) & \xrightarrow{\sigma^{-1}_{B\otimes C,A}} & (B \otimes C) \otimes A \\ & \nearrow^{\alpha_{A,B,C}} & & & \searrow^{\alpha_{B,C,A}} \\ (A \otimes B) \otimes C & & & & B \otimes (C \otimes A) \\ & \searrow_{\sigma^{-1}_{B,A} \otimes \mathrm{id}_C} & & & \nearrow_{\mathrm{id}_B \otimes \sigma^{-1}_{C,A}} \\ & & (B \otimes A) \otimes C & \xrightarrow[\alpha_{B,A,C}]{} & B \otimes (A \otimes C) \end{array} \tag{1.25}$$

We can include the braiding in our graphical notation by drawing them as:

$\sigma_{A,B} \colon A \otimes B \to B \otimes A$

$\sigma^{-1}_{A,B} \colon A \otimes B \to B \otimes A$

(1.26)

Invertibility then takes the following graphical form:

(1.27)

This captures part of the geometric behaviour of strings.

Since they 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, we see that braided monoidal categories have a three-dimensional or *spatial* notation. Because of this, braided monoidal categories have an important connection to certain three-dimensional quantum field theories.

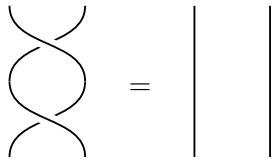
Symmetric monoidal categories

Definition 1.17. A braided monoidal category is *symmetric* when

$$\sigma_{B,A} \circ \sigma_{A,B} = \mathrm{id}_{A \otimes B} \tag{1.28}$$

for all objects A and B.

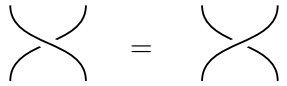
Graphically, this has the following representation.



(1.29)

Intuitively, this means the strings can pass through each other, and there can be no nontrivial linkages.

Lemma 1.18. *In a symmetric monoidal category we have* $\sigma_{A,B} = \sigma_{B,A}^{-1}$, *with the following graphical representation:*



(1.30)

Proof. Combine (1.27) and (1.29). □

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

(1.31)

for both. 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. This relies on an extension of the Coherence Theorem with symmetries. The statement is more involved than that of Theorem 1.2 because $\mathrm{id}_{A \otimes A} \neq \sigma_{A,A}$; basically it says that every diagram built from associators, unitors, and braidings

or symmetries, commutes, as long as all paths have the same underlying permutation.

Suppose we imagine our pictorial diagrams as curves embedded in four-dimensional space. Then we can smoothly deform one crossing into the other, by making use of the extra dimension. In this sense, symmetric monoidal categories have a four-dimensional graphical notation.

Since all our example categories are symmetric monoidal, we will not consider braided monoidal categories explicitly in the rest of these notes. However, many of the theorems that we prove for symmetric monoidal categories also hold for braided monoidal categories.

Examples

Our example categories **Hilb**, **Set** and **Rel** can all be equipped with a symmetry:

- In **Hilb**, $\sigma_{H,K} \colon H \otimes K \to K \otimes H$ is the unique linear map extending $|\phi\rangle \otimes |\psi\rangle \mapsto |\psi\rangle \otimes |\phi\rangle$ for all $|\phi\rangle \in H$ and $\psi \in K$;
- In **Set**, $\sigma_{S,T} \colon S \times T \to T \times S$ is defined by $(s,t) \mapsto (t,s)$ for all $s \in S$ and $t \in T$;
- In **Rel**, $\sigma_{S,T} \colon S \times T \to T \times S$ is the defined by $(s,t) \sim (t,s)$ for all $s \in S$ and $t \in T$.

1.6 Exercises

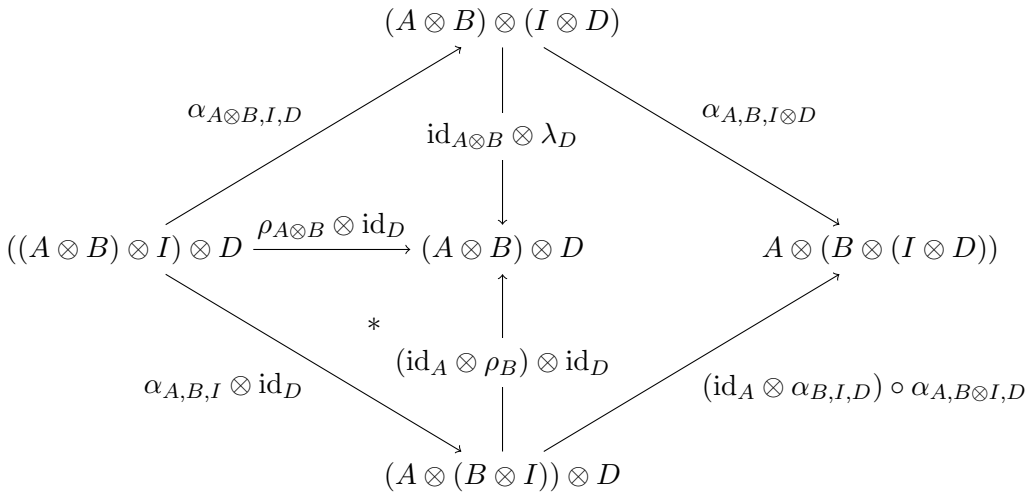
Exercise 1.6.1. Let A, B, C, D be objects in a monoidal category. Construct a morphism

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

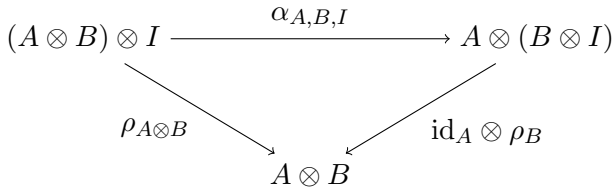
Can you find another?

Exercise 1.6.2. Suppose given the data of a monoidal category satisfying (1.1) and (1.2).

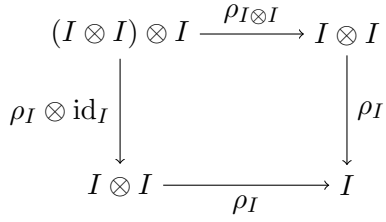
(a) Prove that the marked triangle in the diagram below commutes. (Hint: consider the rest of the diagram first.)



(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 1.6.3. 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 $B \otimes C \xrightarrow{h} D$.

Exercise 1.6.4. Recall Definition 1.8.

(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 1.8?

Exercise 1.6.5. Recall that an entangled state of objects A and B is a state of $A \otimes B$ that is not a product state.

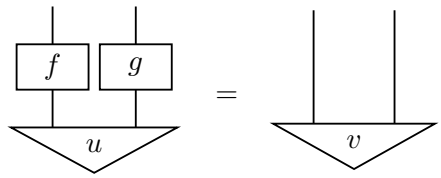
(a) Which of these states of $\mathbb{C}^2 \otimes \mathbb{C}^2$ in **Hilb** are entangled?

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

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

$$\{(0,0),(0,1)\}$$
$$\{(0,0),(0,1),(1,0)\}$$
$$\{(0,1),(1,0)\}$$
$$\{(0,0),(0,1),(1,0),(1,1)\}$$

Exercise 1.6.6. 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 **Rel**.

(c) Write out all 16 states of the object $\{0,1\} \times \{0,1\}$ in **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 1.6.7. Recall equation (1.22) and its interpretation.

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

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

Notes and further reading

(Symmetric) monoidal categories were introduced independently by Bénabou and Mac Lane in 1963 [11, 55]. Early developments centred around the problem of coherence, and were resolved by Mac Lane's Coherence Theorem 1.2. For a comprehensive treatment, see the textbooks [56, 14].

The graphical language dates back to 1971, when Penrose used it to abbreviate tensor contraction calculations [62]. It was formalized for monoidal categories by Joyal and Street in 1991 [41], who later also introduced and generalized to braided monoidal categories [43]. For a modern survey, see [72].

The relevance of monoidal categories for quantum theory was emphasized originally by Abramsky and Coecke [4, 16], and was also popularized by Baez [9] in the context of quantum field theory and quantum gravity. It has since become a popular formalism for work in quantum foundations.

Our remarks about the dimensionality of the graphical calculus are a shadow of higher category theory, as first hinted at by Grothendieck [34]. For a modern overview, see [51]. Monoidal categories are 2-categories with one object, braided monoidal categories are 3-categories with one object and one 1-cell, and symmetric monoidal categories are 4-categories with one object, one 1-cell and one 2-cell — and n-categories have an n-dimensional graphical calculus; see [8].

Chapter 2

Abstract linear algebra

Many aspects of linear algebra can be reformulated as categorical structures. This chapter examines abstractions of the base field, zero-dimensional spaces, addition of linear operators, direct sums, matrices and inner products. These features are essential for modeling features of quantum mechanics such as superposition, although many purposes will not require all of this structure.

2.1 Scalars

States of the tensor unit I play a special role in monoidal categories. They are called the *scalars*, and generalize the idea of a 'base field' in linear algebra. We explore them in our example categories, prove a central commutativity property, and describe their graphical calculus.

Definition and examples

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

A *monoid* is a set S equipped with a multiplication operation, which we write as juxtaposition of elements of S, and a chosen unit element $1 \in S$, satisfying for all $a, b, c \in S$ an associativity law $a(bc) = (ab)c$ and a unit law $1a = a = a1$. 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. They are very different in each of our example categories:

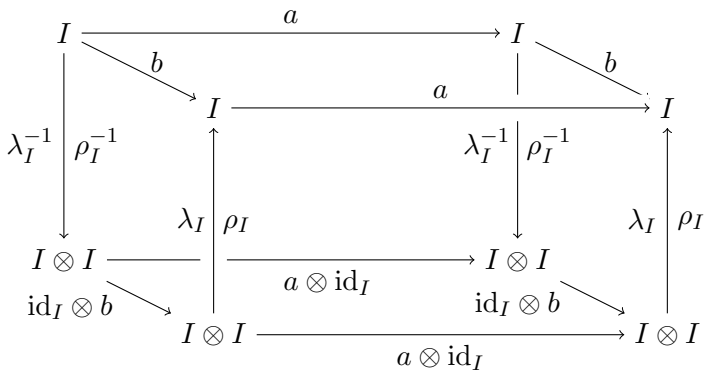
- In **Hilb**, the scalars are $\mathbb{C}$, the complex numbers, under multiplication;
- In **Set**, the scalars are 1, the trivial one-element monoid;
- In **Rel**, the scalars are {true, false} under AND.

Commutativity

In fact, for any monoidal category, the monoid of scalars is commutative.

Lemma 2.2 (Scalars commute)**.** *In a monoidal category, the scalars are commutative.*

Proof. We consider the following diagram, for any two scalars $a, b\colon I \to I$.



(2.1)

The four side cells of the cube commute by naturality of λ_I and ρ_I, and the bottom cell commutes by an application of the interchange law 1.5. Hence we have $ab = ba$. Note the importance of coherence here, as we rely on the fact that $\rho_I = \lambda_I$. □

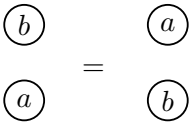
This can be considered the first substantially nontrivial theorem in monoidal category theory. It shows the power of the formalism: from a pure theory of compositionality, we can predict commutativity of the basic elements.

Graphical calculus

To emphasize that scalars $I \xrightarrow{a} I$ have the empty picture (1.11) as both domain and codomain, we draw them as circles, instead of boxes, in the graphical calculus.

(2.2)

Thus commutativity of scalars has the following graphical representation.



(2.3)

This is consistent from the connective property of the graphical calculus: if one diagram can be deformed into another, they have the same value. So once again, we see how a nontrivial property of monoidal categories follows the straightforward geometric planar nature of the graphical calculus.

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. In particular, we can multiply morphisms by scalars.

Definition 2.3 (Left scalar multiplication)**.** Let $I \xrightarrow{a} I$ be a scalar in a monoidal category, and $A \xrightarrow{f} B$ an arbitrary morphism. Define a new morphism $A \xrightarrow{a \bullet f} B$ as the following composite.

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

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

Lemma 2.4 (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:*

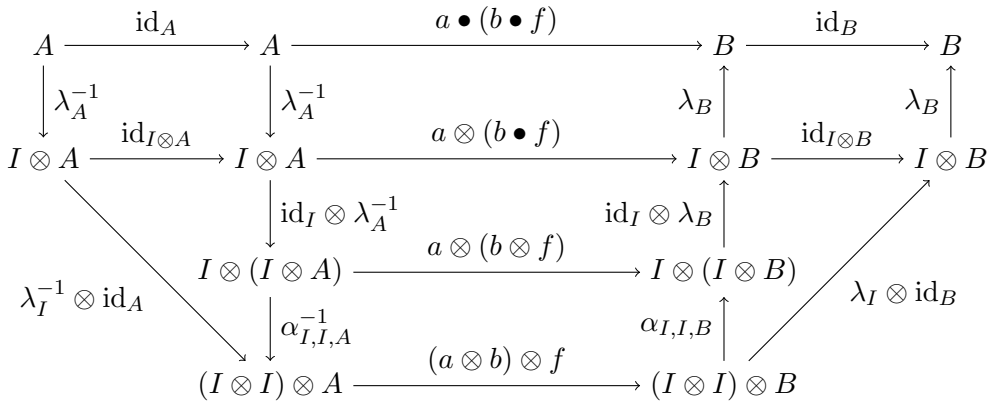
(a) $\mathrm{id}_I \bullet f = f$*;*

(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. Part (a) follows directly from naturality of λ. 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.



(2.4)

Finally, part (d) follows immediately from the interchange law of Theorem 1.5. □

2.2 Superposition

Given linear maps $V \xrightarrow{f,g} W$ between vector spaces, we can form their sum $V \xrightarrow{f+g} W$, another linear map. When $V = \mathbb{C}$ this allows forming superpositions of states, a fundamental part of quantum theory. We analyze this abstractly with the help of various categorical structures.

Zero morphisms

Definition 2.5 (Zero object)**.** An object 1 is *terminal* if for any objects A there is a unique morphism $A \to 1$. An object 0 is *initial* if for any objects A there is a unique morphism $0 \to A$. An object 0 is a *zero object* when it is both initial and terminal. We will also write $\top$ for a terminal object, and $\bot$ for an initial object.

In a category with a zero object, for all objects A and B, there is a unique morphism $A \to 0 \to B$ factoring through the zero object, which we build from the terminal and initial maps. We write this as $A \xrightarrow{0_{A,B}} B$, and call it the *zero morphism*.

Lemma 2.6. *A zero object is unique up to unique isomorphism.*

Proof. If Y and Z are both zero objects, there are unique morphisms $f\colon Y \to Z$ and $g\colon Z \to Y$. But $g \circ f$ must be the unique morphism id_Y, and similarly $f \circ g = \mathrm{id}_Z$. □

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.

Superposition rules

We first define a *superposition rule* on a category, more formally known as an *enrichment in commutative monoids*.

Definition 2.7 (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:**
$$f + g = g + f \tag{2.5}$$

- **Associativity:**
$$(f + g) + h = f + (g + h) \tag{2.6}$$

- **Units:** for all A, B there is a unit morphism $A \xrightarrow{u_{A,B}} B$ such that for all $A \xrightarrow{f} B$:
$$f + u_{A,B} = f \tag{2.7}$$

- **Addition is compatible with composition:**
$$(g + g') \circ f = (g \circ f) + (g' \circ f) \tag{2.8}$$
$$g \circ (f + f') = (g \circ f) + (g \circ f') \tag{2.9}$$

- **Units are compatible with composition:**
$$u_{B,C} \circ u_{A,B} = u_{A,C} \tag{2.10}$$

Both **Hilb** and **Rel** have a superposition rule, while once again **Set** does not. In **Hilb**, it is given by addition of linear maps. In **Rel** it is given by union of subsets, which in the matrix representation of relations corresponds to elementwise OR of matrix entries.

Lemma 2.8. *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.

The existence of a zero object and a superposition rule turns our scalars into a *commutative semiring with an absorbing zero*, which is a

set equipped with commutative, associative multiplication and addition operations with the following properties.

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

In **Hilb** this is the field $\mathbb{C}$. In **Rel** this is {true, false}, with multiplication given by AND and addition given by OR.

Biproducts

In a category with a superposition rule we can define the following structure.

Definition 2.9 (Biproducts)**.** In a category with a zero object and a superposition rule, a *biproduct* of an object A and B is an object $A \oplus B$ equipped with morphisms $A \xrightarrow{i_A} A \oplus B$, $B \xrightarrow{i_B} A \oplus B$, $A \oplus B \xrightarrow{p_A} A$ and $A \oplus B \xrightarrow{p_B} B$, satisfying the following equations.

$$\mathrm{id}_A = p_A \circ i_A \tag{2.11}$$
$$0_{B,A} = p_A \circ i_B \tag{2.12}$$
$$0_{A,B} = p_B \circ i_A \tag{2.13}$$
$$\mathrm{id}_B = p_B \circ i_B \tag{2.14}$$
$$\mathrm{id}_{A\oplus B} = (i_A \circ p_A) + (i_B \circ p_B) \tag{2.15}$$

Biproducts, if they exist, provide a very strong way to 'glue together' objects in a category. The injections i_A and i_B show how the original objects form parts of the biproduct; the projections p_A and p_B show how we can transform the biproduct into either of the original objects; and the equation (2.15) indicates that these original objects together form the whole of the biproduct.

This last property explains why biproducts are not a good choice of monoidal product if we want to model quantum mechanics: all joint states are product states (see also Exercise 2.5.3), there can be no correlations

between different factors. However, this means that biproducts are very suitable to model classical information, and Chapter 6 will discuss this in more depth. The biproduct of a given pair of objects is unique up to a unique isomorphism, by a similar reasoning to Lemma 2.6. Fortunately, a category *can* have different tensor products and biproducts at the same time. We will use this to represent quantum and classical information in a single category. For example, both **Hilb** and **Rel** have biproducts of arbitrary pairs of objects: in **Hilb**, they are given by the *direct sum* of Hilbert spaces, and in **Rel** by disjoint union of sets.

The definition of biproducts above seemed to rely on a chosen superposition rule, but this is only superficial. We now prove that, in the presence of biproducts, superposition rules are unique.

Lemma 2.10 (Unique superposition)**.** *If a category has biproducts and a zero object, then it has a unique superposition rule.*

Proof. First, notice that there necessarily is at least one superposition rule, since in our approach it is required for the definition of biproducts. Observe that $i_1 + i_2$ is the unique morphism $A \to A \oplus A$ satisfying $p_1 \circ (i_1 + i_2) = \mathrm{id}_A = p_2 \circ (i_1 + i_2)$: if $h \colon A \to A \oplus A$ also satisfies $p_1 \circ h = \mathrm{id}_A = p_2 \circ h$, then

$$h = (i_1 \circ p_1 + i_2 \circ p_2) \circ h = i_1 \circ p_1 \circ h + i_2 \circ p_2 \circ h = i_1 \circ \mathrm{id}_A + i_2 \circ \mathrm{id}_A = i_1 + i_2. \tag{2.16}$$

Similarly, if $A \xrightarrow{f,g} B$, then $f \circ p_1 + g \circ p_2$ is the only morphism $A \oplus A \to B$ satisfying $(f \circ p_1 + g \circ p_2) \circ i_1 = f$ and $(f \circ p_1 + g \circ p_2) \circ i_2 = g$. Use this to define a morphism $A \xrightarrow{f \boxplus g} B$ for any $A \xrightarrow{f,g} B$ as follows.

$$A \xrightarrow{i_1 + i_2} A \oplus A \xrightarrow{f \circ p_1 + g \circ p_2} B. \tag{2.17}$$

Thus $f \boxplus g$ is defined *independently* of the chosen superposition rule. Moreover

$$\begin{aligned} f \boxplus g &= (f \circ p_1 + g \circ p_2) \circ (i_1 + i_2) \\ &= (f \circ p_1 \circ (i_1 + i_2)) + (g \circ p_2 \circ (i_1 + i_2)) \\ &= (f \circ (p_1 \circ i_1 + p_1 \circ i_2)) + (g \circ (p_2 \circ i_1 + p_2 \circ i_2)) \\ &= f \circ p_1 \circ i_1 + g \circ p_2 \circ i_2 \\ &= f + g. \end{aligned}$$

Therefore the superposition rule is unique. □

Matrix notation

Biproducts in a category enable a matrix notation for morphisms. For example, for morphisms $A \xrightarrow{f} C$, $A \xrightarrow{g} D$, $B \xrightarrow{h} C$ and $B \xrightarrow{j} D$, the notation

$$A \oplus B \xrightarrow{\begin{pmatrix} f & h \\ g & j \end{pmatrix}} C \oplus D \tag{2.18}$$

will be shorthand for the following map.

$$A \oplus B \xrightarrow{(i_C \circ f \circ p_A) + (i_D \circ g \circ p_A) + (i_C \circ h \circ p_B) + (i_D \circ j \circ p_B)} C \oplus D \tag{2.19}$$

Matrices with any finite number of rows and columns can be used in a similar way.

Lemma 2.11 (Matrix representation)**.** *Every morphism $A \oplus B \xrightarrow{k} C \oplus D$ has a matrix representation.*

Proof. Introducing identities and expanding, rewrite k as follows.

$$\begin{aligned} k &= \mathrm{id}_{C\oplus D} \circ k \circ \mathrm{id}_{A\oplus B} \\ &= \big((i_C \circ p_C) + (i_D \circ p_D)\big) \circ k \circ \big((i_A \circ p_A) + (i_B \circ p_B)\big) \\ &= i_C \circ (p_C \circ k \circ i_A) \circ p_A + i_C \circ (p_C \circ k \circ i_B) \circ p_B \\ &\qquad + i_D \circ (p_D \circ k \circ i_A) \circ p_A + i_D \circ (p_D \circ k \circ i_B) \circ p_B \end{aligned} \tag{2.20}$$

But this is the morphism

$$\begin{pmatrix} p_C \circ k \circ i_A & p_C \circ k \circ i_B \\ p_C \circ k \circ i_A & p_D \circ k \circ i_B \end{pmatrix}, \tag{2.21}$$

which is therefore a matrix representation for k. □

Matrices compose in the way one would expect, with morphism composition replacing multiplication of entries. Notice that composition of morphisms is non-commutative in general, and so the order matters. For example, it follows from the previous lemma that for 2-by-2 matrices,

$$\begin{pmatrix} s & p \\ q & r \end{pmatrix} \circ \begin{pmatrix} f & g \\ h & j \end{pmatrix} = \begin{pmatrix} (s \circ f) + (p \circ h) & (s \circ g) + (p \circ j) \\ (q \circ f) + (r \circ h) & (q \circ g) + (r \circ j) \end{pmatrix}. \tag{2.22}$$

Identity morphisms have a familiar matrix representation:

$$\mathrm{id}_{A\oplus B} = \begin{pmatrix} \mathrm{id}_A & 0_{B,A} \\ 0_{A,B} & \mathrm{id}_B \end{pmatrix} \tag{2.23}$$

Interaction with monoidal structure

In general, linear structure interacts badly with monoidal structure. For example, it isn't true in general that $f\otimes(g+h) = (f\otimes g)+(f\otimes h)$, or 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 **??**.

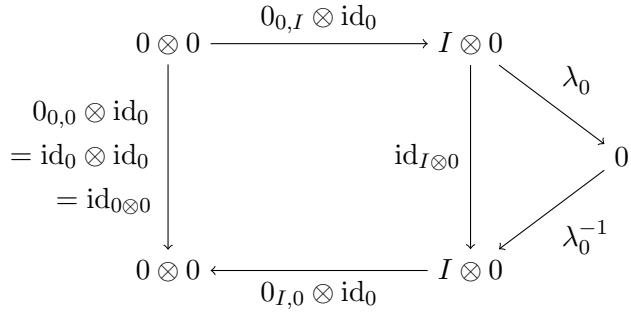
However, the following result holds in general.

Lemma 2.12. *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 the id_0 as 0 is a zero object. Composing in the other direction gives the following.



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

2.3 Adjoints and the dagger

In the definition of the monoidal category of Hilbert spaces, Definition 1.6 above, one peculiarity stood out: it didn't make any use of the inner product. As a result, only the vector space structure of the Hilbert spaces was playing a role. This clearly leaves a gap in our categorical model, since inner products are crucial in quantum theory for computing probabilities. We now investigate how inner products can be described abstractly using a *dagger functor*, a contravariant involutive endofunctor on the category compatible with the monoidal structure.

To describe inner products abstractly, we begin by considering adjoints. Recall that any bounded linear map $H \xrightarrow{f} K$ between Hilbert spaces has a unique adjoint, a bounded linear map $K \xrightarrow{f^\dagger} H$ (see Definition 0.7). For all Hilbert spaces H, J and K and all bounded linear maps $H \xrightarrow{f} J$ and $J \xrightarrow{g} K$, these adjoints have the following properties.

$$(g \circ f)^\dagger = f^\dagger \circ g^\dagger \qquad \mathrm{id}_H{}^\dagger = \mathrm{id}_H \qquad (f^\dagger)^\dagger = f \tag{2.24}$$

These equations tell us that taking adjoints is a functorial process. That is, there is an involutive contravariant functor $\dagger\colon \mathbf{Hilb} \to \mathbf{Hilb}$, satisfying $H^\dagger = H$ on objects, and which takes morphisms to their adjoints. We call this the *adjunction functor*.

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

$$\begin{aligned}(\mathbb{C} \xrightarrow{\phi} H \xrightarrow{\psi^\dagger} \mathbb{C}) &= \psi^\dagger(\phi(1)) \\ &= \langle 1|\psi^\dagger(\phi(1))\rangle \\ &= \langle\psi|\phi\rangle\end{aligned} \tag{2.25}$$

So the adjunction functor 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 adjunction functor is *equivalent* to knowing the inner products.

Dagger categories

This motivates the following abstractions.

Definition 2.13 (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.

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 category **Hilb** is the motivating example of a dagger category, where the dagger is given by adjoints. The category **Rel** can be made into a dagger category, where the dagger is given by taking the 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, since for sets A and B, the set $\mathbf{Set}(A, B)$ of morphisms $A \to B$ contains $|B|^{|A|}$ elements, whereas $\mathbf{Set}(B, A)$ contains $|A|^{|B|}$ elements. A dagger would give an isomorphism between these for all sets A and B, which is obviously not possible.

Another important nonexample 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 $\mathbf{Vect}(V, \mathbb{C})$. The category **FVect** containing only finite-dimensional objects *can* be equipped with a dagger: 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.

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

Definition 2.14. A morphism $A \xrightarrow{f} B$ in a dagger category is:

- the *adjoint* of $B \xrightarrow{g} A$ when $g = f^\dagger$;
- *unitary* when $f \circ f^\dagger = \mathrm{id}_B$ and $f^\dagger \circ f = \mathrm{id}_A$;
- an *isometry* when $f^\dagger \circ f = \mathrm{id}_A$;
- *self-adjoint* when $A = B$ and $f = f^\dagger$;
- *positive* when $A = B$ and $f = g^\dagger \circ g$ for some $A \xrightarrow{g} C$.

In a dagger category, we usually do not care about isomorphisms so much as about unitaries. This is a general phenomenon: whenever a dagger

category has some structure, that structure should cooperate with the dagger. The rest of this chapter investigates this philosophy for tensor products and linear structure. Most of the time we have to require the basic sort of cooperation we want, but sometimes it comes for free. For example, zero objects automatically cooperate well with daggers, as in the following lemma.

Lemma 2.15. *In a dagger category with a zero object,* $0^\dagger_{A,B} = 0_{B,A}$.

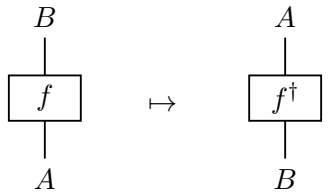
Proof. Immediate from functoriality: $0_{A,B} = (A \to 0 \to B)^\dagger = (B \to 0 \to A) = 0_{B,A}$. □

Dagger monoidal categories

We start by looking at cooperation between a dagger and monoidal structure.

Definition 2.16 (Dagger monoidal category)**.** A *dagger monoidal category* is a monoidal category that is also a dagger category, 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 α, λ and ρ are unitary. A *dagger braided monoidal category* is a dagger monoidal category equipped with a unitary braiding. A *dagger symmetric monoidal category* is a dagger braided monoidal category for which the braiding is a symmetry.

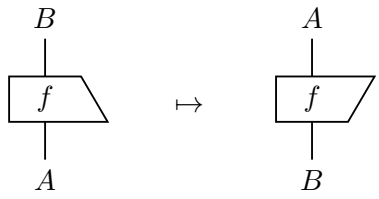
We depict the action of the dagger in the graphical calculus by flipping the graphical representation about a horizontal axis as follows.



(2.26)

To help differentiate between these morphisms, from now on we will draw our morphisms in a way that breaks their symmetry. Applying the dagger

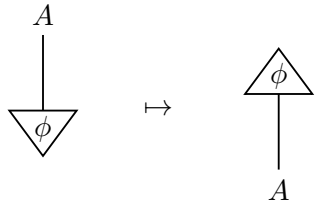
then has the following representation.



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

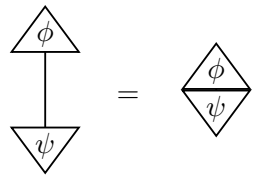


(2.28)

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

Equation (2.25) demonstrated how to recover inner products from the action of the dagger on states. Applying this argument graphically yields the following expression for the inner product $\langle\psi|\phi\rangle$ of two states $I \xrightarrow{\phi,\psi} H$.

$\langle\psi|\phi\rangle$ =



(2.29)

The expression on the right-hand side is simply a rotated form of the traditional bra-ket notation given on the left-hand side! This demonstrates

a close connection between our graphical formalism and the bra-ket notation of Dirac. The graphical notation for monoidal dagger categories is a broad generalization, extending the Dirac notation to arbitrary bounded linear maps, and in fact to arbitrary dagger monoidal categories.

Dagger biproducts

Biproducts can be compatible with a dagger in an important way.

Definition 2.17 (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 $i_B^\dagger = p_B$.

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

Dagger biproducts guarantee good interaction of the dagger and the superposition rule.

Lemma 2.18 (Adjoint of a matrix)**.** *In a dagger category with dagger biproducts, the adjoint of a matrix is its dagger-transpose:*

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

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

properties.

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

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

Corollary 2.19 (Adjoint of a superposition)**.** *In a dagger category with dagger biproducts, the dagger distributes over addition:* $(f+g)^\dagger = f^\dagger + g^\dagger$ *for all morphisms* $A \xrightarrow{f,g} B$*.*

Proof. By the previous lemma, $(f+g)^\dagger = \left(\begin{pmatrix} f & g \end{pmatrix} \circ \begin{pmatrix} \mathrm{id} \\ \mathrm{id} \end{pmatrix} \right)^\dagger = \begin{pmatrix} \mathrm{id} & \mathrm{id} \end{pmatrix} \circ \begin{pmatrix} f^\dagger \\ g^\dagger \end{pmatrix} = f^\dagger + g^\dagger$. □

2.4 The Born rule

Probabilities

If $I \xrightarrow{\psi} A$ is a state and $A \xrightarrow{a} I$ an effect, recall that we interpret the scalar $I \xrightarrow{\psi} A \xrightarrow{a^\dagger} I$ as the probability amplitude of measuring outcome a immediately after preparing state ψ; in bra-ket notation this would be

$\langle a|\psi\rangle$. According to the *Born rule* of quantum mechanics, the *probability* that this history occurred is the square of its absolute value, which would be $|\langle a|\psi\rangle|^2 = \langle\psi|a\rangle \cdot \langle a|\psi\rangle = \langle\psi|a^\dagger \circ a|\psi\rangle$ in bra-ket notation. This makes sense for abstract scalars, as follows.

Definition 2.20 (Probability)**.** If $I \xrightarrow{\psi} A$ is a state, and $A \xrightarrow{a} I$ an effect, in a dagger monoidal category, set

$$\mathrm{Prob}(a, \psi) = \psi^\dagger \circ a^\dagger \circ a \circ \psi \colon I \to I. \tag{2.30}$$

Complete sets of effects

We will now show that these probabilities satisfy familiar properties even in the abstract setting of dagger monoidal categories with dagger biproducts. First, notice that the scalar $\mathrm{Prob}(a, \psi)$ is positive by construction. In particular, it is self-adjoint; in **Hilb**, this comes down to probabilities being positive *real* numbers, rather than general complex numbers. Moreover, if a set of effects is large enough to cover every possible outcome, then these probabilities must add up to one, as we will now discuss.

Definition 2.21 (Complete set of effects)**.** In a dagger monoidal category with dagger biproducts, a set of effects $\{A \xrightarrow{a_i} I \mid i = 1, \ldots, n\}$ is *complete* if

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} : A \to I \oplus I \oplus \cdots \oplus I \tag{2.31}$$

is an isometry.

In **Hilb**, a set of effects $\{H \xrightarrow{\phi_i} \mathbb{C}\}$ is complete when its elements span an orthogonal subspace of $\mathbf{Hilb}(H, \mathbb{C})$. It could be an orthonormal basis for this space, or it could be a basis with extra elements added. Notice that at any rate we must have $n \geq \dim(H)$. In **Rel**, a set of effects $\{A \xrightarrow{a_i} \{\bullet\}\}$ is complete when every element $x \in A$ is related to $\bullet$ by some effect a_i.

Before we prove that the probabilities add up to one, notice that this only makes sense if the state of the system is specified well-enough. In a dagger monoidal category there is a duality between states $I \xrightarrow{\psi} A$ and effects $A \xrightarrow{\psi^\dagger} I$. We interpret $I \xrightarrow{\psi} A \xrightarrow{\psi^\dagger} I$ as the result of measuring

the system A in state ψ immediately after preparing it in state ψ. This had better be the identity. That is, if we want to say something about probabilities, we should only consider isometric states. In **Hilb**, these correspond to vectors of norm one; in **Rel**, these correspond to nonempty subsets.

Proposition 2.22 (The Born rule)**.** *Let* $\{A \xrightarrow{a_i} I \mid i = 1, \ldots, n\}$ *be a complete set of effects in a dagger monoidal category with dagger biproducts, and let* $I \xrightarrow{\psi} A$ *be an isometric state. Then* $\sum_{i=1}^{n} \mathrm{Prob}(a_i, \psi) = 1$.

Proof. By the superposition rule,

$$\sum_{i=1}^{n} \mathrm{Prob}(a_i, \psi) = \sum_{i=1}^{n} \psi^\dagger \circ a_i^\dagger \circ a_i \circ \psi = \psi^\dagger \circ \left(\sum_{i=1}^{n} a_i^\dagger \circ a_i \right) \circ \psi.$$

But since $\{a_i\}$ is a complete set of effects,

$$\sum_{i=1}^{n} a_i^\dagger \circ a_i = \begin{pmatrix} a_1^\dagger & \cdots & a_n^\dagger \end{pmatrix} \circ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}^\dagger \circ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \mathrm{id}_A.$$

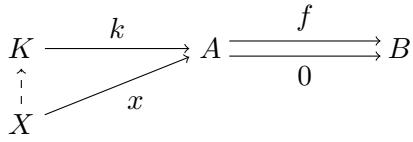
So $\sum_{i=1}^{n} \mathrm{Prob}(a_i, \psi) = \psi^\dagger \circ \psi$. But this is $\mathrm{id}_I = 1$ because ψ is an isometry. □

Thus we can use scalars and biproducts to model the statistics of *classical information*. In later chapters, we will encounter ways to do this without using biproducts. Nevertheless, as we have seen, biproducts, if they exist, are a fundamental property of a categorical model of physical systems.

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. On 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 2.23 (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 $k \circ f = 0_{K,A}$, 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.

Lemma 2.24. *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 (2.31) for any complete set of effects $\{A \xrightarrow{a_i} I\}$ in a dagger monoidal category with a zero object and dagger biproducts. This means that if $I \xrightarrow{\psi} A$ is any possible state, then at least one of the histories $I \xrightarrow{\psi} A \xrightarrow{a_i} I$ must occur.

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

Lemma 2.25 (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 $m \colon A \to K$ 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 $I \xrightarrow{\phi} A$ is a state, nondegeneracy implies that $(I \xrightarrow{\phi} A \xrightarrow{\phi^\dagger} I) = 0$ if and only if $\phi = 0$. This is a good property, since we interpret $I \xrightarrow{\phi} A \xrightarrow{\phi^\dagger} I$ as the result of measuring the system A in state ϕ immediately after preparing it in state ϕ. The outcome is zero precisely when this history cannot possibly have occurred, so ϕ must have been an impossible state to begin with.

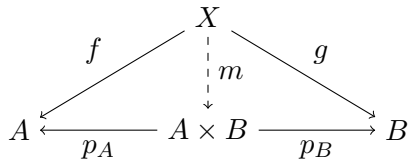
2.5 Exercises

Exercise 2.5.1. Recall Definition 2.9.

(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. 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 $X \xrightarrow{m} A \times B$ with $p_A \circ m = f$ and $p_B \circ m = g$.

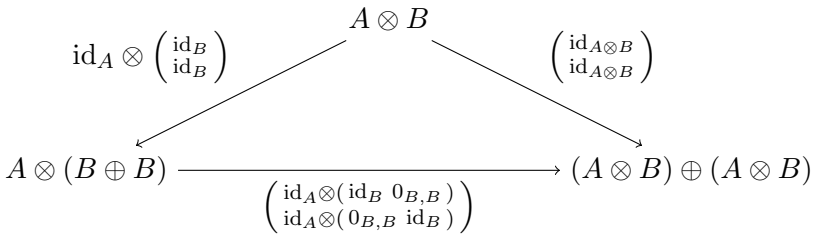


Show that if $(A \oplus B, p_A, p_B, i_A, i_B)$ is a biproduct, then $(A \oplus B, p_A, p_B)$ is a product.

Exercise 2.5.3. 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 2.5.4. Show that any category with products, a zero object, and a superposition rule, automatically has biproducts.

Exercise 2.5.5. Show that the following diagram commutes in any monoidal category with biproducts.



Exercise 2.5.6. Let A and B be objects in a dagger category. Show that if $A \oplus B$ is a dagger biproduct, then i_A is a dagger kernel of p_B.

Exercise 2.5.7. Let $A \xrightarrow{R} B$ be a morphism in **Rel**, with relational converse as dagger.

(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 $a \mathrel{R} b \Rightarrow a \mathrel{R} a$.

(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 **Rel** a dagger kernel?

(f) Is every isometry $A \to A$ in **Rel** unitary?

(g) Show that every biproduct in **Rel** is a dagger biproduct.

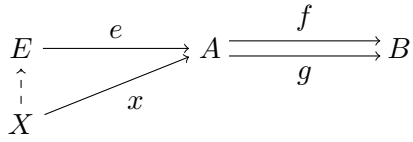
Exercise 2.5.8. Recall the category $\mathbf{FHilb}_{\mathbf{ss}}$ from Definition 1.8.

(a) Show that transposition of matrices makes the monoidal category $\mathbf{FHilb}_{\mathbf{ss}}$ into a dagger monoidal category.

(b) Show that $\mathbf{FHilb}_{\mathbf{ss}}$ does not have dagger kernels under this dagger.

Exercise 2.5.9. Given morphisms $A \xrightarrow{f,g} B$ in a dagger category, a *dagger equalizer* is an isometry $E \xrightarrow{e} A$ satisfying $f \circ e = g \circ e$, with the property

that every morphism $X \xrightarrow{x} A$ satisfying $f \circ x = g \circ x$ factors through e.



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 $\begin{pmatrix} g & f \end{pmatrix} : A \oplus A \to B$);

Notes and further reading

The early uses of category theory were in algebraic topology. Therefore early developments mostly considered categories like **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 [32]. 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 [57]. See also [14] for an overview.

Self-duality in the form of involutive endofunctors on categories has been considered as early as 1950 [53, 54]. A link between adjoint functors and adjoints in Hilbert spaces was made precise in 1974 [59]. The systematic exploitation of daggers in the way we have been using them started with Selinger in 2007 [71].

Using different terminology, Lemma 2.2 was proved in 1980 by Kelly and Laplaza [48]. The realization that endomorphisms of the tensor unit behave as scalars was made explicit by Abramsky and Coecke in 2004 [4, 2]. Heunen proved an analogue of Mitchell's embedding theorem for **Hilb** in 2009 [36]. Conditions

under which the scalars embed into the complex numbers are due to Vicary [76], which also contains results on dagger-biproducts and dagger-equalizers.

Chapter 3

Dual objects

In a monoidal category, some objects have an important property called *dualizability*. In the graphical calculus, this corresponds to the ability to 'bend the wire' representing the object. Quantum-mechanically, this corresponds to the ability to create a generalized Bell state for the object, an entangled state of central importance in quantum information. Dual objects lie at the heart of many modern developments in mathematics, topology and quantum information, and brings these subjects together in new and exciting ways.

3.1 Dual objects

One of the most characteristic features of quantum mechanics is the existence of *entanglement*, that relates the behaviour of two systems even if they are very far apart. If you have studied quantum information at all, you might remember that the amount of entanglement between two systems can be quantified. There are several measures to do so, the most famous probably being (von Neumann) entropy. The most interesting couples of entangled systems are the *maximally entangled* ones, whose entropy is as large as it can possibly be. We model maximal entanglement categorically by a pair of *dual objects*.

Definition

We begin with the definition of dual objects, and show how the graphical calculus gives an elegant way to represent their axioms.

Definition 3.1 (Dual object)**.** An object L in a monoidal category is *left-dual* to an object R, and R is *right-dual* to L, written $L \dashv R$, when it is equipped with morphisms $\eta\colon I \to R \otimes L$ and $\varepsilon\colon L \otimes R \to I$ making the following two diagrams commute.

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

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

The maps η and ε are called the *unit* and *counit*, respectively. When L is both left and right dual to R, we simply call L a *dual* of R.

Graphical representation

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 then drawn as bent wires:

(3.4)

The duality equations then take the following graphical form:

(3.5)

Particularly when drawn graphically, these are also called the *snake equations* because of how they look.

These equations add *orientation* to the two-dimensional graphical calculus of monoidal categories. Physically, η represents a state of $R \otimes L$; a way for it to be brought into being. In fact, we will see later that it represents a *maximally 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.

Examples

Hilbert spaces. Every object in **FHilb** canonically has a dual, namely its dual Hilbert space H^*. To construct the unit and counit maps for a finite-dimensional Hilbert space H, first pick an orthonormal basis $|i\rangle$. Then H^* has an orthonormal basis formed by the functions $\langle i| \colon H \to \mathbb{C}$ defined by $|j\rangle \mapsto \langle i|j\rangle$. Construct $\mathbb{C} \xrightarrow{\eta} H^* \otimes H$ and $H \otimes H^* \xrightarrow{\varepsilon} \mathbb{C}$ as

$$\eta : 1 \mapsto \sum_i \langle i| \otimes |i\rangle, \tag{3.6}$$

$$\varepsilon : |i\rangle \otimes \langle j| \mapsto \langle i|j\rangle. \tag{3.7}$$

We will see below that duals are unique up to isomorphism, so it doesn't matter which basis we picked. Indeed, ε is the evaluation map $x \otimes f \mapsto f(x)$, and η is its adjoint. Hence any basis happens to give rise to the same maps η and ε in **FHilb**.

However, this construction will not work for an infinite-dimensional Hilbert space, as the resulting sum in (3.6) is not well-defined. In fact, Corollary 3.29 below will show that a Hilbert space has a dual if and only if it is finite-dimensional. In this sense, the existence of duals is often interpreted as a finiteness property.

In case $H = \mathbb{C}^2$, the state (3.6) is a maximally entangled state of a two-qubit system, and is also called a *Bell state*. Therefore we can think of the unit map exhibiting a duality as a generalized Bell state.

Compact categories. For a more involved example: the category of representations of a Lie group on a finite-dimensional Hilbert space is symmetric monoidal, and has duals when the group is compact. This example historically lead to the following terminology.

Definition 3.2. A *compact category* is a symmetric monoidal category in which every object has a dual.

In particle physics, particles correspond to particular representations of a Lie group. Ignoring spacetime symmetries, in the standard model of particle physics this group is compact. If a particle corresponds to an object P, then its *antiparticle* corresponds to the dual object P^*. The unit and counit maps then correspond physically to particle-antiparticle creation and annihilation. In this context, the graphical calculus has a different name: *Feynman diagrams*.

Sets. In the category **Rel**, every object is its own dual, even sets of infinite cardinality. For a set S, the maps $1 \xrightarrow{\eta} S \times S$ and $S \times S \xrightarrow{\varepsilon} 1$ are defined in the following way:

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

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

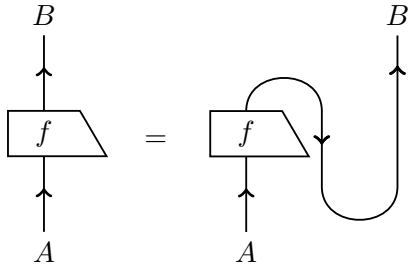
The category **Set** does *not* have duals for objects. To understand why, it helps to introduce the *name* and *coname* of a morphism.

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 $A \otimes B^* \xrightarrow{\ulcorner f \urcorner} I$ as the following morphisms:

(3.10)

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



(3.11)

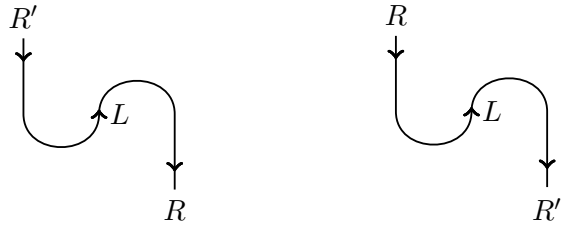
However, in **Set**, the monoidal unit object 1 is terminal, and so all conames must be equal. If **Set** had duals this would then imply that all functions with the same source and target are equal, which is clearly absurd.

Basic properties

One of the most fundamental properties of entanglement is *monogamy of entanglement*. In quantum information theory, this takes the form of an inequality: if systems A, B and C are entangled, the amount of entanglement between A and B, plus the amount of entanglement between B and C, cannot exceed a fixed upper bound. If we take the extremal form of this quantitative inequality, it says: if B is maximally entangled with A, it cannot be entangled with any other system C at all. Intuitively, B can only dole out a given amount of entanglement; so maximal entanglement is monogamous. Since we have modeled maximal entanglement by dual objects, this comes down to the following: if $A \dashv B$ and $C \dashv B$, then A and C must be the same system. Categorically, we cannot actually prove that two objects are equal. The best we can do is to show that they are isomorphic, which the following lemma does.

Lemma 3.4. *If $L \dashv R$ in a monoidal category, then $L \dashv R'$ precisely when $R \simeq R'$. Similarly, if $L \dashv R$, then $L' \dashv R$ precisely when $L \simeq L'$.*

Proof. If $L \dashv R$ and $L \dashv R'$, define maps $R \to R'$ and $R' \to R$ as follows:



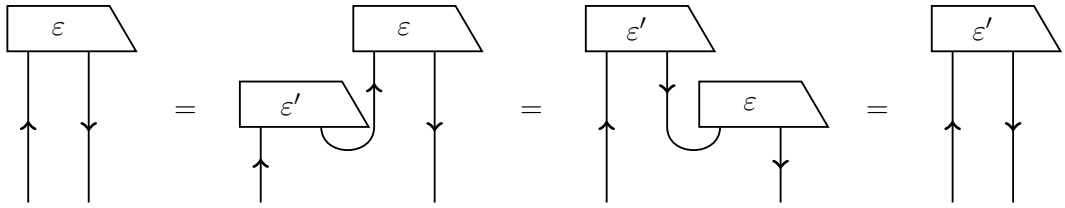
(3.12)

It follows from the snake equations that these are inverse to each other. Conversely, if $L \dashv R$ and $f\colon R \to R'$ is an isomorphism, then the choices $I \xrightarrow{(f \otimes \mathrm{id}_L) \circ \eta} R' \otimes L$ and $L \otimes R' \xrightarrow{\varepsilon \circ (\mathrm{id}_L \otimes f^{-1})} I$ shows that $L \dashv R'$. The symmetric claim follows similarly. □

There is a similar rigidity in the definition of dual objects with respect to unit and counit maps. In the examples of dual objects above, the counit maps determined the unit maps, and vice versa. The following lemma shows that this is not a coincidence.

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.



(3.13)

The second case is similar. □

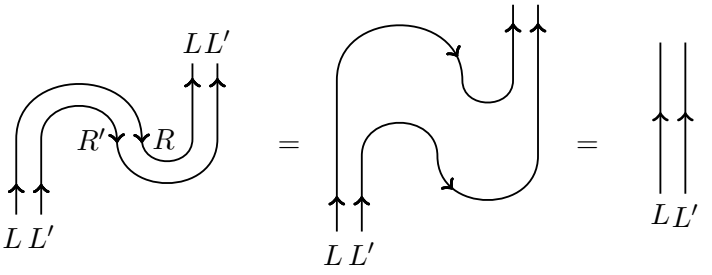
Hence dual objects are unique up to isomorphism in a strong way. Later, we will work with a fixed choice of dual for each object. The

following lemma shows that dual objects interact well with the monoidal structure: whatever choice of dual objects we fix will be coherent with tensor products.

Lemma 3.6. *In a monoidal category, $I \dashv I$, and $L \otimes L' \dashv R' \otimes R$ when $L \dashv R$ and $L' \dashv R'$.*

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 and the fact that $\lambda_I = \rho_I$.

Suppose that $L \dashv R$ and $L' \dashv R'$. We may make the new unit and counit maps from the old ones, and prove one of the snake equations graphically, as follows:



(3.14)

The other snake equation follows similarly. This shows that $L \otimes L' \dashv R' \otimes R$. □

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 3.7. *In a symmetric 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 $(L, R, \eta, \varepsilon)$:

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

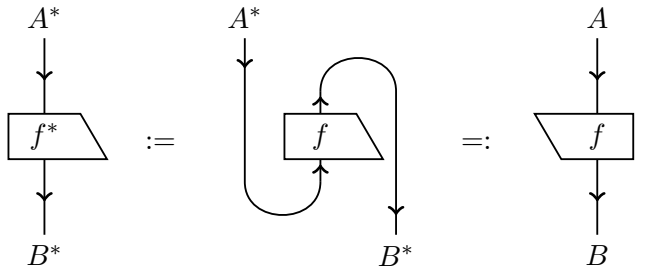
(3.15)

Writing out 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 η and ε. □

3.2 Functoriality

It turns out that choosing duals on objects is so strong that it automatically extends to morphisms.

Definition 3.8. 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:

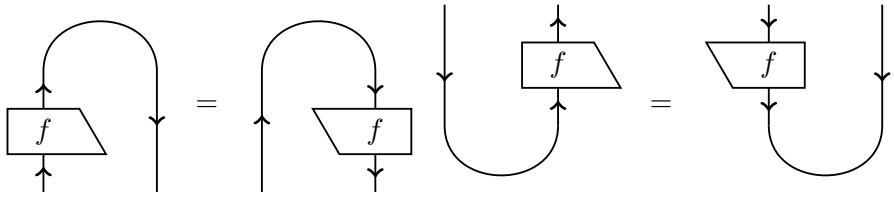


(3.16)

We represent this graphically by rotating the morphism box representing f, as shown in the third image above. Left duals for morphisms could be defined in a similar way.

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

Lemma 3.9. *In a symmetric monoidal category, the following equations hold:*

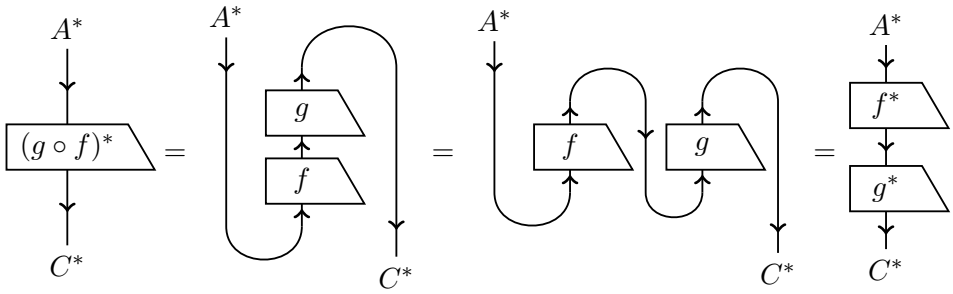


Proof. Direct from writing out the definitions of all the components involved. □

Definition 3.10. For a monoidal category $\mathbf{C}$ in which every object X has a chosen right dual X^*, we define the *right-duals functor* $(-)^* \colon \mathbf{C}^{\mathrm{op}} \to \mathbf{C}$ as $(X)^* := X^*$ on objects, and $(f)^* := f^*$ on morphisms.

Proposition 3.11. *The right-duals functor satisfies the axioms for a functor.*

Proof. Let $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$. Then:



(3.17)

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

3.3 Dagger compact categories

For $L \dashv R$ in a monoidal category that is also a dagger category, in addition to the unit and counit maps of the duality there are also their adjoints, that we represent graphically as follows:

(3.18)

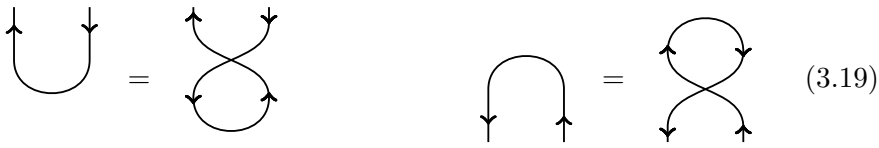
These adjoints provide witnesses for a duality $R \dashv L$, resulting in the following lemma.

Lemma 3.12. *In a dagger monoidal category, $L \dashv R \Rightarrow R \dashv L$.*

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

Definition 3.13. In a symmetric dagger monoidal category, dual objects $L \dashv R$ are said to be *dagger dual objects* when $\varepsilon^\dagger = \sigma_{R,L} \circ \eta$, or equivalently $\varepsilon \circ \sigma_{R,L} = \eta^\dagger$.

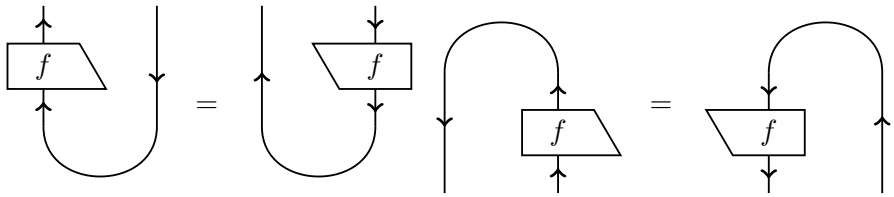
These conditions have the following graphical representation:



(3.19)

For dagger dual objects, we can extend the graphical rules developed in Lemma 3.9 for dual morphisms as follows.

Lemma 3.14. *For dagger dual objects $L \dashv R$, the following equations hold:*



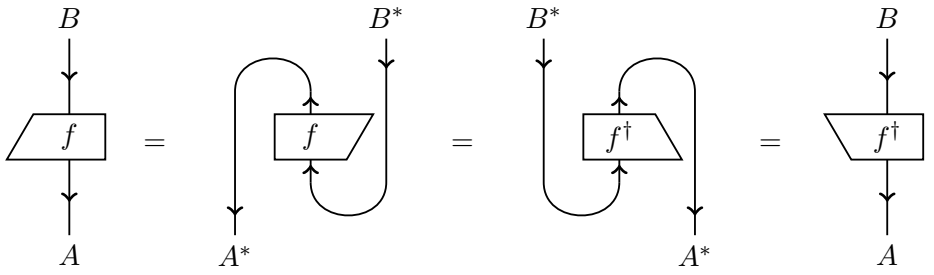
Proof. Unfold the definitions. □

Definition 3.15. A *dagger compact category* is a symmetric dagger monoidal category in which every object is equipped with dagger dual object.

According to the way of the dagger, when constructing the right-duals functor for a dagger compact category, we will always ensure that the chosen right duals for each object are in fact dagger duals.

Lemma 3.16. *On a dagger compact category, the right-duals functor and the dagger commute.*

Proof. Graphically, this is misleadingly simple. For a morphism $A \xrightarrow{f} B$:



(3.20)

Let us also write it out algebraically; the subtlety is the naturality in the indices:

$$\begin{aligned}
(f^*)^\dagger &= \big((\varepsilon_{A^*} \otimes \mathrm{id}_{B^*}) \circ (\mathrm{id}_{A^*} \otimes f \otimes \mathrm{id}_{B^*}) \circ (\mathrm{id}_{A^*} \otimes \eta_{B^*})\big)^\dagger \\
&= (\mathrm{id}_{A^*} \otimes \eta_{B^*}^\dagger) \circ (\mathrm{id}_{A^*} \otimes f^\dagger \otimes \mathrm{id}_{B^*}) \circ (\varepsilon_{A^*}^\dagger \otimes \mathrm{id}_{B^*}) \\
&= (\mathrm{id}_{B^*} \otimes (\varepsilon_A \circ \sigma_{A,A^*})) \circ (\mathrm{id}_{B^*} \otimes f^\dagger \otimes \mathrm{id}_{A^*}) \circ ((\sigma_{B,B^*} \circ \eta_B) \otimes \mathrm{id}_{A^*}) \\
&= (\mathrm{id}_{B^*} \otimes \varepsilon_A) \circ (\mathrm{id}_{B^*} \otimes f^\dagger \otimes \mathrm{id}_{A^*}) \circ (\eta_B \otimes \mathrm{id}_{A^*}) \\
&= (f^\dagger)^*.
\end{aligned}$$

□

The previous lemma makes the following definition of *conjugation* well-defined.

Definition 3.17. On a dagger compact category, *conjugation* $(-)_*$ is defined as the composite of the dagger and the right-duals functor: $A_* := A^*$ on objects, and $f_* := (f^*)^\dagger = (f^\dagger)^* \colon B^* \to A^*$ on morphisms $A \xrightarrow{f} B$.

Since both the dagger and the right-duals functor are contravariant, reversing the direction of morphisms, conjugation is a covariant functor.
Since both the dagger and the right-duals functor are contravariant, reversing the direction of morphisms, conjugation is a covariant functor.

Examples

Hilbert spaces. The category **FHilb** can be given the structure of a dagger compact category using equations (3.6) and (3.7). Writing a morphism as a matrix on some orthonormal basis, the dagger computes its

conjugate transpose; we have already noted this is independent of the basis. The right-duals functor computes its transpose, and therefore does depend on the basis. Combining the two shows that conjugation indeed computes the entrywise conjugation of the matrix, and does depend on the basis.

In $\mathbf{FHilb_{ss}}$ every object has a canonical basis, and hence a canonical self-duality. The right-duals functor still computes transposition of matrices. Since the adjunction functor on this category computes the conjugate transpose matrix, it is clear that this will commute with the duality functor, as we expect from Lemma 3.16. The conjugation functor then computes the conjugate of a matrix.

Relations. In **Rel**, every object is its own right dual in a canonical way. The right-duals functor gives transposition of relations, as does the dagger. Hence conjugation is the identity. You might think that things like transpose and conjugation are typical notions from linear algebra. But notice from these examples that no linear structure was required to generalize these notions: it can be done purely in terms of tensor products.

3.4* Interaction with linear structure

Chapter 2 noted that linear structure does not necessarily interact well with monoidal structure. However, in the presence of duals for all objects, this good kind of interaction is guaranteed. This is quite remarkable, since dual objects are defined independently from linear structures such as superposition rules, biproducts and zero objects. This indicates that, for some fundamental reason which is not yet completely understood, linear structure is deeply related to our graphical calculus.

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

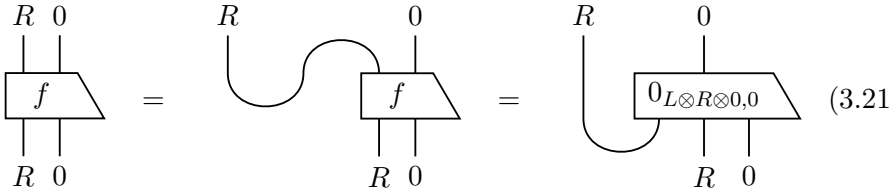
Lemma 3.18. *In a monoidal category with a zero object* 0*:*

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

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

Proof. Because $0 \otimes 0 \cong 0$ by Lemma 2.12, there are unique morphisms $I \xrightarrow{\eta} 0 \otimes 0$ and $0 \otimes 0 \xrightarrow{\varepsilon} I$. It also follows that $0 \otimes (0 \otimes 0) \cong 0$, so that both sides of the snake equation must equal the unique morphism $0 \to 0$. This establishes (a).

For (b), let $f \colon R \otimes 0 \to R \otimes 0$ be an arbitrary morphism. Then:



(3.21)

So there really is only one morphism $R \otimes 0 \to R \otimes 0$, namely the identity. Similarly, the only morphism $0 \to 0$ 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 $R \otimes 0 \cong 0$. The other claims follow similarly. □

Corollary 3.19. *Let A, B, C, D be objects in a monoidal category, and $A \xrightarrow{f} B$ a morphism. If one of A or B has either a left or a right dual, then*

$$f \otimes 0_{C,D} = 0_{A\otimes C, B\otimes D},$$
$$0_{C,D} \otimes f = 0_{C\otimes A, D\otimes B}.$$

Proof. The morphism $f \otimes 0_{C,D} \colon A \otimes C \to B \otimes D$ factors through $A \otimes 0$. But this object is isomorphic to 0 by Lemma 3.18(b). Hence $f \otimes 0_{C,D}$ must have been the zero morphism. Similarly, $0_{C,D} \otimes f$ is the zero morphism. □

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

Lemma 3.20. *Let A, B, C be objects in a monoidal category with biproducts. If A has either a left or right dual, then the following morphisms are*

each other's inverse:

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

$$A \otimes (B \oplus C) \qquad\qquad (A \otimes B) \oplus (A \otimes C)$$

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

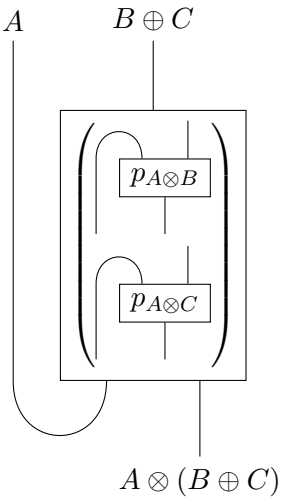
(3.22)

Proof. To begin, we use Corollary 3.19 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 has a left dual, consider the following morphism:

$g' \quad :=$



(3.23)

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 $A^* \otimes (A \otimes (B \oplus C)) \to B \oplus C$, 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 left 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 3.21. *Let A, B, C, D be objects in a monoidal category with biproducts and a zero object, and $A \xrightarrow{f} B$ and $C \xrightarrow{g,h} D$ morphisms. If A has either a left or a right dual, then*

$$(f \otimes g) + (f \otimes h) = f \otimes (g + h), \tag{3.24}$$
$$(g \otimes f) + (h \otimes f) = (g + h) \otimes f. \tag{3.25}$$

Proof. Compose the morphisms of Lemma 3.20 for $B = C$ to obtain the identity on $A \otimes (C \oplus C)$. Applying the interchange law shows that this identity equals

$$A \otimes (C \oplus C) \xrightarrow{\mathrm{id}_A \otimes \left(\begin{smallmatrix} \mathrm{id}_C & 0_{C,C} \\ 0_{C,C} & 0_{C,C} \end{smallmatrix}\right) + \mathrm{id}_A \otimes \left(\begin{smallmatrix} 0_{C,C} & 0_{C,C} \\ 0_{C,C} & \mathrm{id}_C \end{smallmatrix}\right)} A \otimes (C \oplus C). \tag{3.26}$$

Now, further applications of the matrix calculus and the interchange law,

$$f \otimes (g + h) = \left(\mathrm{id}_B \otimes \left(\mathrm{id}_D \;\; \mathrm{id}_D\right)\right) \circ \left(f \otimes \begin{pmatrix} g & 0 \\ 0 & h \end{pmatrix}\right) \circ \left(\mathrm{id}_A \otimes \begin{pmatrix} \mathrm{id}_C \\ \mathrm{id}_C \end{pmatrix}\right) \tag{3.27}$$

Inserting the identity in the form of morphism (3.26), and using the interchange law and distributivity of composition over superposition (2.8), gives

$$\begin{aligned} f \otimes \begin{pmatrix} g & 0 \\ 0 & h \end{pmatrix} &= \left(f \otimes \begin{pmatrix} g & 0 \\ 0 & h \end{pmatrix}\right) \circ \left(\mathrm{id}_A \otimes \left(\begin{smallmatrix} \mathrm{id}_C & 0_{C,C} \\ 0_{C,C} & 0_{C,C} \end{smallmatrix}\right) + \mathrm{id}_A \otimes \left(\begin{smallmatrix} 0_{C,C} & 0_{C,C} \\ 0_{C,C} & \mathrm{id}_C \end{smallmatrix}\right)\right) \\ &= \left(f \otimes \begin{pmatrix} g & 0 \\ 0 & 0 \end{pmatrix}\right) + \left(f \otimes \begin{pmatrix} 0 & 0 \\ 0 & h \end{pmatrix}\right). \end{aligned} \tag{3.28}$$

Substituting this into equation (3.27),

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

as required. The equation $(g+h) \otimes f = (g \otimes f) + (h \otimes f)$ is proved similarly. □

Finally, the next proposition proves that taking biproducts preserves dual objects.

Proposition 3.22. *If $L \dashv R$ and $L' \dashv R'$ are dual objects in a compact category with biproducts and a zero object, then $L \oplus L' \dashv R \oplus R'$.*

Proof. Let $I \xrightarrow{\eta} R \otimes L$ and $I \xrightarrow{\eta'} R' \otimes L'$ be the unit maps, and $L \otimes R \xrightarrow{\varepsilon} I$ and $L' \otimes R' \xrightarrow{\varepsilon'} I$ the counit maps. Abbreviate $L'' := L \otimes L'$ and $R'' := R \otimes R'$, and define

$$\begin{aligned} \eta'' &:= ((i_R \otimes i_L) \circ \eta) + ((i_{R'} \otimes i_{L'}) \circ \eta') \colon I \to R'' \otimes L'', \\ \varepsilon'' &:= (\varepsilon \circ (p_L \otimes p_R)) + (\varepsilon' \circ (p_{L'} \otimes p_{R'})) \colon L'' \otimes R'' \to I. \end{aligned}$$

Now Lemma (3.21) guarantees

$$\begin{aligned} \eta'' \otimes \mathrm{id}_{R''} &= ((i_R \otimes i_L \otimes \mathrm{id}_{R''}) \circ (\eta \otimes \mathrm{id}_{R''})) + ((i_{R'} \otimes i_{L'} \otimes \mathrm{id}_{R''}) \circ (\eta' \otimes \mathrm{id}_{R''})), \\ \mathrm{id}_{R''} \otimes \varepsilon'' &= ((\mathrm{id}_{R''} \otimes \varepsilon) \circ (\mathrm{id}_{R''} \otimes p_L \otimes p_R)) + ((\mathrm{id}_{R''} \otimes \varepsilon') \circ (\mathrm{id}_{R''} \otimes p_{L'} \otimes p_{R'})). \end{aligned}$$

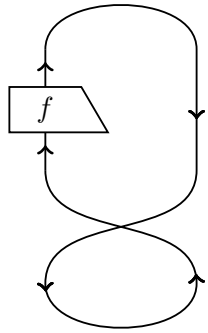
It follows that the snake morphism $\rho \circ (\mathrm{id}_{R''} \otimes \varepsilon'') \circ \alpha \circ (\eta'' \otimes \mathrm{id}_{R''}) \circ \lambda^{-1}$ is the biproduct of $\rho \circ (\mathrm{id}_R \otimes \varepsilon) \circ \alpha \circ (\eta \otimes \mathrm{id}_R) \circ \lambda^{-1}$ and $\rho \circ (\mathrm{id}_{R'} \otimes \varepsilon') \circ \alpha \circ (\eta' \otimes \mathrm{id}_{R'}) \circ \lambda^{-1}$. That is, the snake equation for η'' and ε'' follows from the snake equations for η and ε, and η' and ε'. □

3.5 Traces and dimensions

In addition to scalars, transpose, and conjugation, there are more notions from linear algebra that can be formulated purely in terms of tensor products, without the need for any linear structure. In a symmetric monoidal

category, we can use the existence of duals to define traces of morphisms and even dimensions of objects.

Definition 3.23. Let L be an object in a symmetric monoidal category that has a right dual. The *trace* of a morphism $L \xrightarrow{f} L$, denoted $\mathrm{Tr}_L(f)$, is defined as the following scalar:



(3.29)

Definition 3.24. Let L be an object in a symmetric monoidal category that has a right dual. Its *dimension* is the scalar $\dim(A) := \mathrm{Tr}_L(\mathrm{id}_L)$.

Basic properties

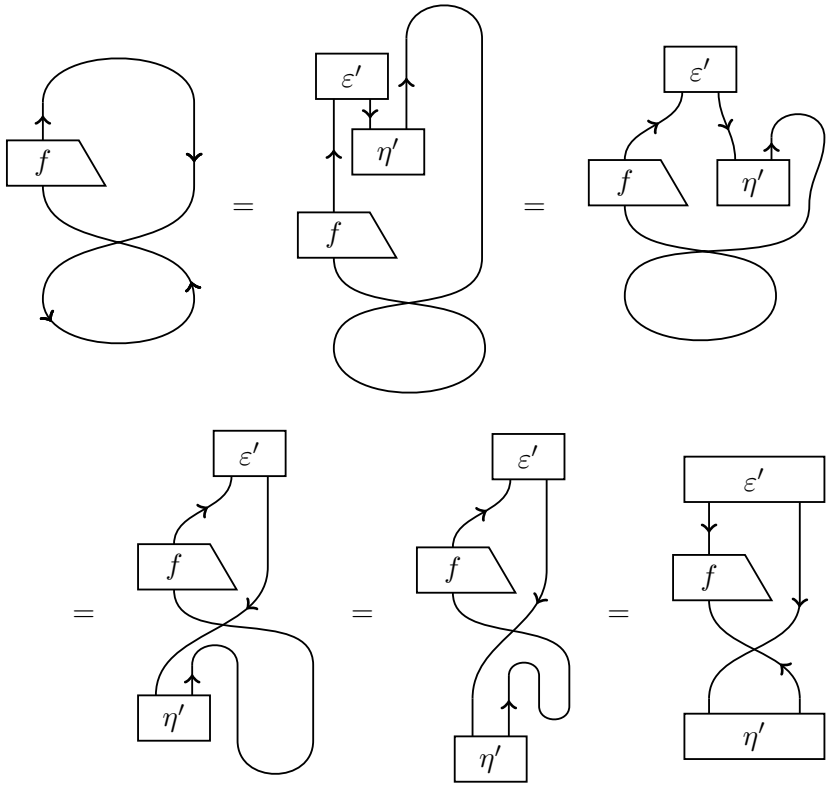
For traces and dimensions to be useful notions, we need the following lemma.

Lemma 3.25. *In a symmetric monoidal category, the trace of a morphism is well-defined.*

Proof. We must show that the value of the trace is independent of the choices of right dual object, unit and counit maps. Suppose dualities $(L, R, \eta, \varepsilon)$ and $(L, R', \eta', \varepsilon')$, draw the first duality using the conventions of equations (3.3-3.4), and draw η' and ε' as follows:

(3.30)

Then:



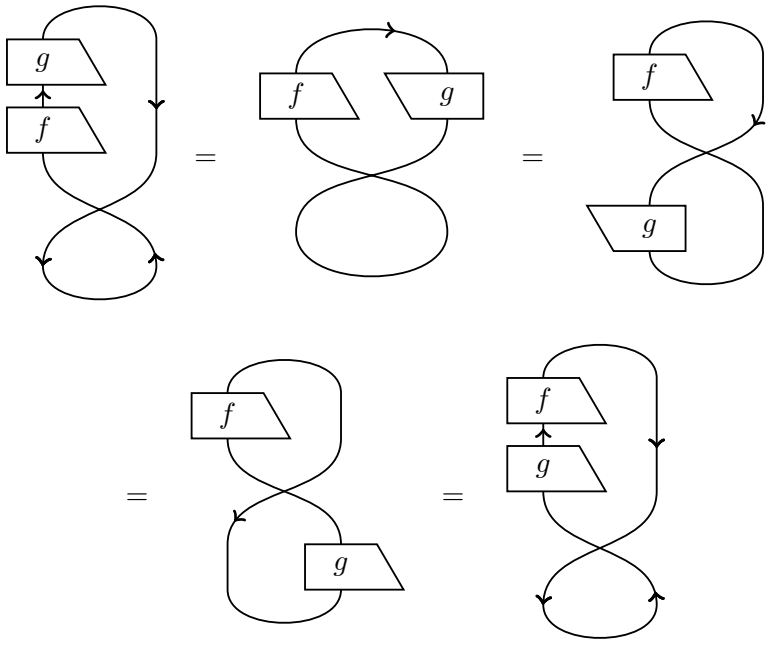
(3.31)

This shows that the trace is well-defined. □

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

Lemma 3.26. *Let* $A \xrightarrow{f} B$ *and* $B \xrightarrow{g}$ *be morphisms in a symmetric monoidal category. If* A *and* B *have a right dual, then* $\mathrm{Tr}_A(g \circ f) = \mathrm{Tr}_B(f \circ g)$.

Proof.



The second and fourth equalities use naturality of the symmetry, the other two equalities follow from properties of dual morphisms. □

Examples

To determine $\mathrm{Tr}_H(f)$ for a morphism $H \xrightarrow{f} H$ in **FHilb**, substitute equations (3.6) and (3.7) into the definition of the abstract trace (3.29). Then $\mathrm{Tr}_H(f) = \sum_i \langle e_i \mid f \mid e_i \rangle$ for an orthonormal basis $|e_i\rangle$, 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, concrete, dimension of H.

Further properties

Abstract traces satisfy many properties familiar from linear algebra, even though the category might not have any linear structure.

Lemma 3.27. *In a symmetric monoidal category, if A, B are objects with right duals, the following properties hold:*

(a) $\mathrm{Tr}_{A\otimes B}(f \otimes g) = \mathrm{Tr}_A(f) \circ \mathrm{Tr}_B(g)$ *for morphisms* $A \xrightarrow{f} A$ *and* $B \xrightarrow{g} B$*;*

(b) $\mathrm{Tr}_A(f + g) = \mathrm{Tr}_A(f) + \mathrm{Tr}_A(g)$ *for* $A \xrightarrow{f,g} B$*;*

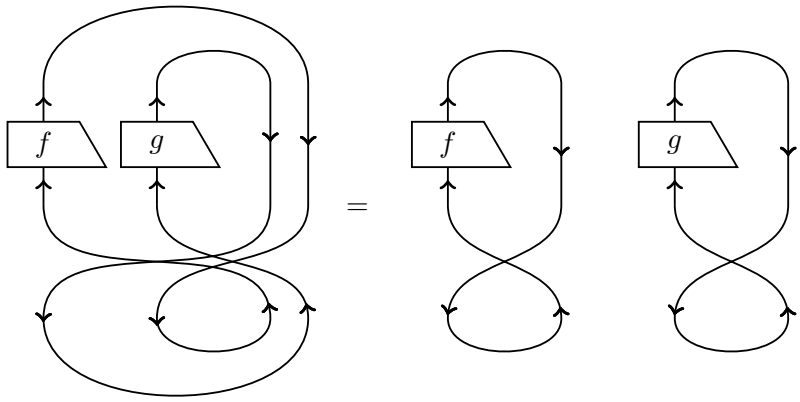
(c) $\mathrm{Tr}_{A\oplus B}\begin{pmatrix} f & g \\ h & j \end{pmatrix} = \mathrm{Tr}_A(f) + \mathrm{Tr}_B(j)$ *when the biproduct* $A \oplus B$ *exists, for morphisms* $A \xrightarrow{f} A$*,* $B \xrightarrow{g} A$*,* $A \xrightarrow{h} B$ *and* $B \xrightarrow{j} B$*;*

(d) $\mathrm{Tr}_I(s) = s$ *for a scalar* $I \xrightarrow{s} I$*;*

(e) $\mathrm{Tr}_A(0_{A,A}) = 0_{I,I}$ *for a zero morphism* $0_{A,A}$*;*

(f) $\big(\mathrm{Tr}_A(f)\big)^\dagger = \mathrm{Tr}_A(f^\dagger)$ *for a morphism* $A \xrightarrow{f} A$ *in a dagger symmetric monoidal category.*

Proof. Part (a) follows from naturality:



Part (b) follows directly from Lemma 3.21 and compatibility of addition with composition as in equation (2.8). For part (c), use the cyclic property

of Lemma 3.26:

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

Part (d) follows from $\mathrm{Tr}_I(s) = s \bullet \mathrm{id}_I = s$, which trivializes graphically. For part (e): because $0_{A,A} \otimes \mathrm{id}_{A^*} = 0_{A\otimes A^*, A\otimes A^*}$ by Corollary 3.19, also $\mathrm{Tr}_A(0_{A,A}) = \varepsilon \circ (0_{A,A} \otimes \mathrm{id}_{A^*}) \circ \sigma \circ \eta = 0_{I,I}$. Finally, (f) follows from simple graphical manipulations unfolding Definition **??**. □

This immediately yields some properties of dimensions of objects.

Lemma 3.28. *Let A, B be objects in a symmetric monoidal category that have a right dual.*

(a) $\dim(A \otimes B) = \dim(A) \circ \dim(B)$*;*

(b) $\dim(A \oplus B) = \dim(A) + \dim(B)$ *when the biproduct $A \oplus B$ exists;*

(c) $\dim(I) = \mathrm{id}_I$*;*

(d) $\dim(0) = 0_{I,I}$ *for a zero object* 0*;*

(e) $A \simeq B \Rightarrow \dim(A) = \dim(B)$.

Proof. Parts (a)–(d) are straightforward consequences of Lemma 3.27. Property (e) follows from the cyclic property of the trace demonstrated in Lemma 3.26: 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 3.29. *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 (b) and (e) of Lemma 3.28 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 $A \oplus I \cong A$, 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 **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 $S \simeq S \cup 1$.

3.6 Information flow

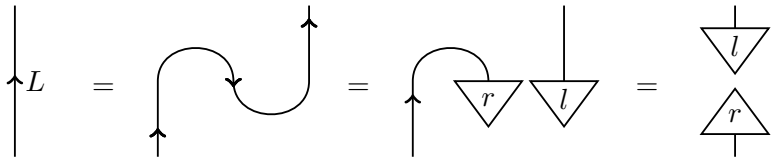
Dual objects in a monoidal category provide a categorical way to model *entanglement* of a pair of systems in an abstract way. Given dual objects $L \dashv R$, the entangled state is the unit $I \xrightarrow{\eta} R \otimes L$. The corresponding counit $L \otimes R \xrightarrow{\varepsilon} I$ gives an 'entangled effect', a way to measure whether a pair of systems are in a particular entangled state. The theory of dual objects gives rise to a natural variation between $L \otimes R$ and $R \otimes L$ for the state space of the pair of systems, which turns out to fit naturally with the structure of procedures that make use of entanglement.

We use the term 'entanglement' because, in **Hilb**, these entangled states $\mathbb{C} \xrightarrow{\eta} H \otimes H$ correspond exactly to generalized Bell states: quantum states of a pair of quantum systems of the same dimension, which are of the form $\sum_i |i\rangle \otimes |i\rangle'$ for orthonormal bases $|i\rangle$, $|i\rangle'$ of H. These states are of enormous importance in quantum theory, because they can be used to produce strong correlations between measurement results that cannot be explained classically.

The following lemma shows abstractly that η is an entangled state in a precise way.

Lemma 3.30. *Let $L \dashv R$ be dual objects in a symmetric monoidal category. If the unit $I \xrightarrow{\eta} R \otimes L$ is a product state, then id_L and id_R factor through the monoidal unit object I.*

Proof. Suppose that η is the morphism $I \xrightarrow{\lambda_i^{-1}} I \otimes I \xrightarrow{r \otimes l} R \otimes L$. Then



(3.32)

A similar argument holds for id_R. □

Interpreting a graphical diagram as a history of events that have taken place, as we do, the fact that id_L factors through I means that, in any observable history of this experiment, whatever input we give the process, the output will be independent of it. Clearly such objects L are quite degenerate. Thus η is always an entangled state, except in degenerate situations.

In **Rel**, a unit map $1 \xrightarrow{\eta} S \times S$ is of the form $\sum_s (s, \pi(s))$, where $\pi : S \to S$ is an arbitrary bijection. This is a form of nondeterministic creation of correlation. Information-theoretically, it is useful to think of it as the creation of a *one-time pad*. This is shared secret information which two agents can use to communicate a private message over a public channel. If the nondeterministic process η is implemented, and the first agent receives the secret key $s \in S = 2^N$, then she can take the elementwise exclusive-OR of this with a secret message to produce a new string, which contains no information to those with no knowledge of the secret key. This message is passed publicly to the second agent, who has received a private key $\pi(s)$. Applying the inverse bijection π^{-1} to this key, the second agent can then apply a second exclusive-OR and reconstruct the original message.

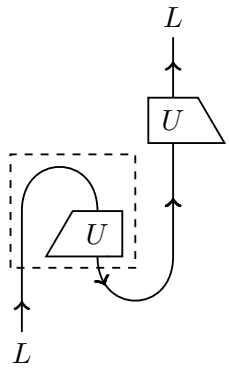
So duals for objects give us maximally entangled joint states in **Hilb**, and one-time pads in **Rel**. We will now see how the snake equations defining the dual objects allow us to account for correctness of several protocols.

Abstract teleportation

The most fundamental procedure we will cover is 'abstract teleportation', that can be defined for any dagger monoidal category. As we will see,

Hilb it reduces to quantum teleportation, and in **Rel** it models classical encrypted communication.

The basic history diagram for quantum teleportation takes the following form:



(3.33)

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. To describe this history in words:

1. Begin with a single system L.

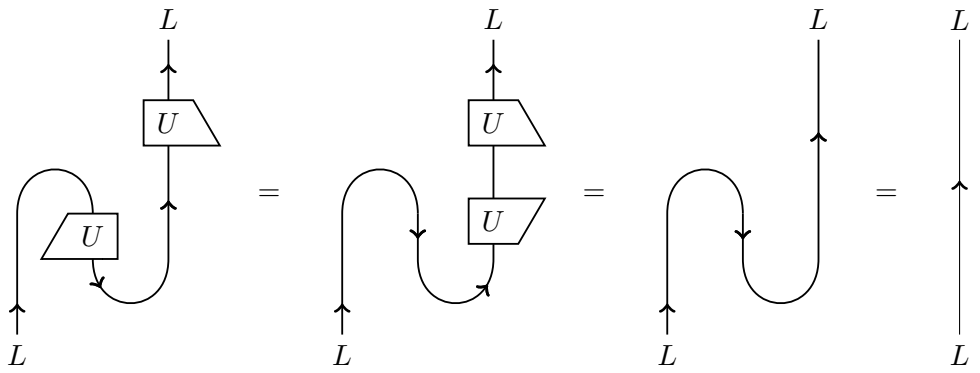
2. Independently, prepare a joint system $R \otimes L$ in the state η, resulting in a total system $L \otimes (R \otimes L)$.

3. Perform a joint measurement on the first two systems, with a result given by the effect $\varepsilon \circ (\mathrm{id}_L \otimes U_*)$.

4. Perform a unitary operation U on the remaining system.

Ignoring the dashed box, the graphical calculus simplifies the graphical

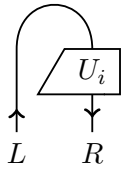
expression for this history:



(3.34)

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 that the history equals the identity. So if the events described in (3.33) come to pass, then the result is for the original system to be transmitted unaltered.

The trouble with this account is that we cannot guarantee that measuring the subsystem $L \otimes R$ gives the required result $\varepsilon \circ (\mathrm{id}_L \otimes U_*)$ as described in step 3 above. One way to get around this is to consider a complete set of effects, in the sense of Definition 2.21. We require that each element of our set of effects is of the following form, equal to the coname of the conjugate of a unitary morphism:



(3.35)

Having performed the measurement, record which effect is obtained, and apply the corresponding unitary $L \xrightarrow{U_i} L$ as a controlled operation at the next stage of the protocol. There is an important transfer of classical information that takes place here, which is not treated formally as part of the categorical setup at the minute.

Having chosen a complete family of effects, there is a corresponding family of possible histories, each of the form of (3.33) with U replaced by U_i. Each is equal to id_L, thanks to the argument of (3.34). As a result, the original system is 'teleported' successfully, regardless of the particular effect that was obtained.

Concrete examples

Hilbert spaces. 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:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{3.36}$$

The construction of (3.35) gives rise to the following family of effects:

$$\begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 & -1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & -1 & 0 \end{pmatrix} \tag{3.37}$$

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.

Relations. We can also implement the abstract teleportation procedure in **Rel**. For the simplest implementation, choose $L = R = 2 := \{0, 1\}$, and $\eta^\dagger = \varepsilon = \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}$. In **Rel** there are only two unitaries of type $2 \to 2$, as the unitaries are exactly the permutations:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{3.38}$$

Choose these as the family of unitaries U_i. This gives rise to the following family of effects:

$$\begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix} \tag{3.39}$$

These form a complete set of effects, since every element of 2×2 is related to $\bullet$ by one of the two effects. Thus we obtain a correct implementation

of the abstract teleportation procedure. In fact, this is precisely classical encrypted communication via a one-time pad.

3.7 Exercises

Exercise 3.7.1. Recall the notion of local equivalence from Exercise 1.6.6. In **Hilb**, we can write a state $\phi\colon \mathbb{C} \to \mathbb{C}^2 \otimes \mathbb{C}^2$ as a column vector

$$\phi = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix},$$

or as a matrix

$$M_\phi := \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

(a) Show that ϕ is an entangled state if and only if M_ϕ is invertible. (Hint: a matrix is invertible if and only if it has nonzero determinant.)

(b) Show that $M_{(\mathrm{id}_{\mathbb{C}^2} \otimes f) \circ \phi} = M_\phi \circ f^{\mathrm{T}}$, where $f\colon \mathbb{C}^2 \to \mathbb{C}^2$ is any linear map and f^{T} is the transpose of f in the canonical basis of $\mathbb{C}^2$.

(c) Use this to show that there are three families of locally equivalent joint states of $\mathbb{C}^2 \otimes \mathbb{C}^2$.

Exercise 3.7.2. Recall that if V is a vector space, a set $\{e_i\}$ of its elements is a *basis* when (i) every $v \in V$ can be written as a linear combination of the e_i, and (ii) if $\sum_i z_i e_i = 0$ for $z_i \in \mathbb{C}$, then each $z_i = 0$. Every vector space has at least one basis; the cardinality is independent of the chosen basis, and is called the dimension of V.
Pick a basis $\{e_i\}$ for a finite-dimensional vector space V, and define $\eta\colon \mathbb{C} \to V \otimes V$ and $\varepsilon\colon V \otimes V \to \mathbb{C}$ 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 **FVect**.

(b) Show that f^* is given by the transpose of the matrix of the morphism $V \xrightarrow{f} V$ (where the matrix is written with respect to the basis $\{e_i\}$).

(c) Suppose that $\{e_i\}$ and $\{e'_i\}$ are both bases for V, giving rise to two units η, η' and two counits $\varepsilon, \varepsilon'$. Let $V \xrightarrow{f} V$ be the 'change-of-base' isomorphism $e_i \mapsto f_i$. Show that $\eta = \eta'$ and $\varepsilon = \varepsilon'$ if and only if f is *(complex) orthogonal*, i.e. $f^{-1} = f^*$.

Exercise 3.7.3. Let $L \dashv R$ in **FVect**, with unit η and counit ε. Pick a basis $\{r_i\}$ for R.

(a) Show that there are unique $l_i \in L$ satisfying $\eta(1) = \sum_i r_i \otimes l_i$.

(b) Show that every $l \in L$ can be written as a linear combination of the l_i, and hence that the map $f\colon R \to L$, defined by $f(r_i) = l_i$, is surjective.

(c) Use the previous exercise to 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:

$$\eta(1) = \sum_i r_i \otimes l_i, \qquad \varepsilon(l_i \otimes r_j) = \delta_{ij}. \tag{3.40}$$

Exercise 3.7.4. Let $L \dashv R$ be dagger dual objects in **FHilb**, with unit η and counit ε.

(a) Use the previous exercise to show that there are an orthonormal basis $\{r_i\}$ of R and a basis $\{l_i\}$ of L such that $\eta(1) = \sum_i r_i \otimes l_i$ and $\varepsilon(l_i \otimes r_j) = \delta_{ij}$.

(b) Show that $\varepsilon(l_i \otimes r_j) = \langle l_j | l_i \rangle$. Conclude that $\{l_i\}$ is also an orthonormal basis, and hence that every dagger duality $L \dashv R$ in **FHilb** has the standard form (3.40) for *orthonormal* bases $\{l_i\}$ of L and $\{r_i\}$ of R.

Exercise 3.7.5. Show that any duality $L \dashv R$ in **Rel** is of the following *standard form* for an isomorphism $f\colon R \to L$:

$$\eta = \{(\bullet, (r, f(r)) \mid r \in R\}, \qquad \varepsilon = \{((r, f^{-1}(r)), \bullet) \mid r \in R\}. \tag{3.41}$$

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 3.7.6. In a monoidal category, show that:

(a) if an initial object $\bot$ exists and $L \dashv R$, then $L \otimes \bot \cong \bot \cong \bot \otimes R$;

(b) if a terminal $\top$ exists and $L \dashv R$, then $R \otimes \top \cong \top \cong \top \otimes L$.

Exercise 3.7.7. Show that trace in **Rel** shows whether a relation has a fixed point.

Exercise 3.7.8. Let $\mathbf{C}$ be a dagger compact 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 3.7.9. Show that if $L \dashv R$ are dagger dual objects, then $\dim(L)^\dagger = \dim(R)$.

Notes and further reading

Dual objects can be neatly formulated in terms of adjoint functors, which make sense in any (weak) 2-category [52]. Combined with the knowledge that adjoint functors preserve limits, this perspective greatly simplifies several proofs in this chapter. We have not used it because of the required machinery, and the possible confusion of adjoint functors and adjoint functions between Hilbert spaces.

Compact categories were first introduced by Kelly in 1972 as a class of examples in the context of the coherence problem [46]. They were subsequently studied first from the perspective of categorical algebra [27, 48], and later in relation to linear logic [69, 10].

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 [42]. 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: rigid, pivotal, autonomous, sovereign, spherical, ribbon, tortile, balanced, and category with conjugates [72].

Abstract traces in monoidal categories were introduced by Joyal, Street and Verity in 1996 [44]. Definition 3.23 is one instance. In fact, Hasegawa proved in 2008 that abstract traces in a compact category are unique [35]. The link between abstract traces and traces of matrices was made explicit by Abramsky and Coecke in 2005 [5]. The use of dagger compact categories in foundations of quantum mechanics was initiated in 2004 by Abramsky and Coecke [4]. This was the article that initiated the study of categorical quantum mechanics.

The graphical calculus for dagger compact categories was worked out in detail by Selinger, who proved its soundness [72]. In 2008 [73], he also proved that an equation holds in the graphical calculus of dagger compact categories if and only if it holds in every possible instantiation in **FHilb**.

The quantum teleportation protocol was discovered in 1993 by Bennett, Brassard, Crépeau, Jozsa, Peres, and Wootters [12], and has been performed experimentally many times since, over distances as large as 16 kilometers.

Monogamy of entanglement was known to quantum information theorists such as Bennett in the 1980s, but was first given a mathematical form by Coffman, Kundu and Wootters in 1999 [26].

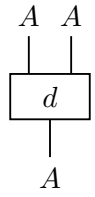
Chapter 4

Classical structures

The tensor product in **Hilb** and **Rel** is not a categorical product, so it doesn't provide an automatic way to copy information. However, in the real world, certain types of information *can* be copied. We call this classical information, and we model it in a monoidal category using a classical structure.

4.1 Monoids and comonoids

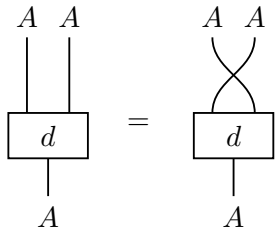
Let's start by making the notions of copying and deleting more precise in our setting of symmetric monoidal categories. Clearly, copying should be an operation of type $A \xrightarrow{d} A \otimes A$. We draw it in the following way:



(4.1)

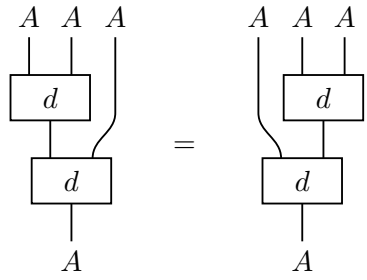
What does it mean that d 'copies' information? First, it shouldn't matter if we switch both output copies, corresponding to the requirement that

$d = \sigma_{A,A} \circ d$:



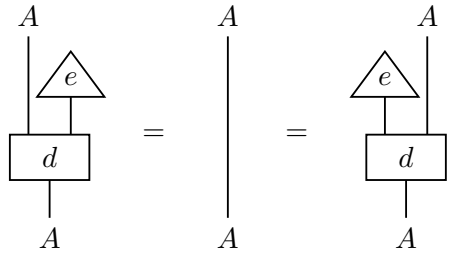
(4.2)

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 symmetric 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 (4.6) are *coassociativity* and *counitality*.

Some examples of comonoids:

- In **Set**, the tensor product is in fact a Cartesian product, so any object A carries a unique commutative 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 $1 \sim \bullet$. The comonoid is cocommutative when the group is abelian.

- In **FHilb**, any choice of basis $|i\rangle$ for a Hilbert space H provides it with comonoid structure, with comultiplication $A \xrightarrow{d} A \otimes A$ defined by $|i\rangle \mapsto |i\rangle \otimes |i\rangle$ and counit $A \xrightarrow{e} I$ defined by $|i\rangle \mapsto 1$.

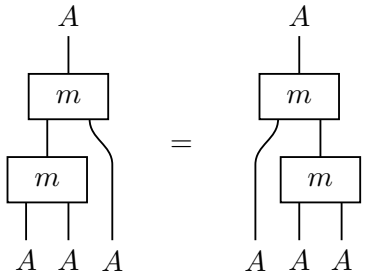
The comonoids in a monoidal category can be made into a category themselves. The morphisms in this category are morphisms in the original category satisfying the *comonoid homomorphism* property.

Definition 4.2 (Comonoid homomorphism)**.** A *comonoid homomorphism* from a monoid (A, d, e) to a monoid (A', d', e') is a morphism $A \xrightarrow{f} A'$ such that $(f \otimes f) \circ d = d' \circ f$ and $e' \circ f = e$.

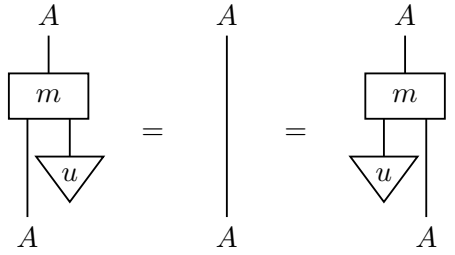
You might be growing tired of "co" before every other word. Indeed, dualizing everything gives the more well-known notion of a *monoid*. In fact, this notion is so important, that one can almost say the entire reason for defining monoidal categories is that one can define monoids in them.

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*:

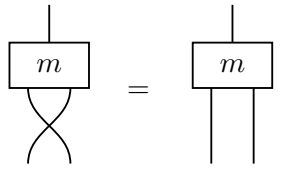


(4.5)



(4.6)

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



(4.7)

There are many examples of monoids:

- The tensor unit I in any monoidal category can be equipped with the structure of a monoid, with $d = \rho_I$ $(= \lambda_I)$ and $e = \mathrm{id}_I$.
- A monoid in **Set** gives the ordinary mathematical notion of a monoid. Any group is an example.
- A monoid **Hilb** 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 point $(1, 1, \ldots, 1)$.

The monoids in a monoidal category can be made into a category themselves. The morphisms in this category are morphisms in the original category satisfying the *monoid homomorphism* property.

Definition 4.4 (Monoid homomorphism)**.** 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 $u' = f \circ u$.

In a monoidal dagger-category, there is a duality between monoids and comonoids.

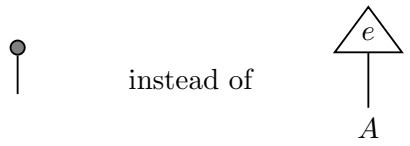
Lemma 4.5. *If (A, d, e) is a comonoid in a monoidal dagger-category, then $(A, d^\dagger, e^\dagger)$ is a monoid.*

Proof. Equations (4.5) and (4.6) are just (4.3) and (4.4) vertically reflected. □

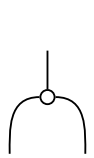
As we saw above, any group G gives a comonoid in **Rel** with $d = \{(g, (h, h^{-1}g) \mid g, h \in G\}$. The dagger-functor on **Rel** constructs converse relations, and applying this turns our example into a monoid in **Rel** with multiplication $G \times G \xrightarrow{m} G$ given by $(g, h) \sim gh$ and unit $1 \xrightarrow{u} G$ given by $\bullet \sim 1$.

For the rest of this section, we will simplify our graphical notation for monoids and comonoids in the following way:

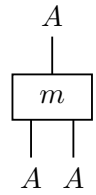
(4.8)



(4.9)

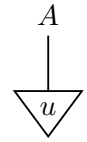


instead of



(4.10)

instead of



(4.11)

The colours we have used here are not essential. By the graphical calculus for the dagger-functor, which reflects diagrams about a horizontal axis, we can indicate the case when m and d are adjoint to each other by using the same colour dot. The same goes for e and u. Conjugation is represented by flipping a diagram about a vertical axis; a downside of our new notation is that the diagrams are symmetric about a vertical axis, so conjugation cannot be properly represented. However, we will mostly be working with *classical structures*, algebraic objects which are self-conjugate, so this ambiguity will not cause any problems.

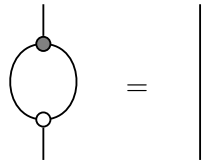
4.2 Frobenius algebras

There are various ways in which a comonoid and a monoid on the same object can interact. In this chapter we will study one such way, which are called *Frobenius algebras*. This turns out to be the right notion to capture classical information.

Our first axiom concerns the most basic way a monoid and comonoid structure can interact.

Definition 4.6. In a monoidal category, a pair consisting of a comonoid (A, d, e) and a monoid (A, m, u) is called *special* when m is a retraction of

d, which exactly gives the equation $m \circ d = \mathrm{id}_A$.

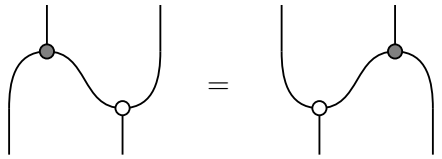


(4.12)

In a monoidal dagger-category, if $(A, m, u) = (A, m^\dagger, u^\dagger)$, we use the term *dagger-special*.

A second interaction law gives the definition of a Frobenius algebra.

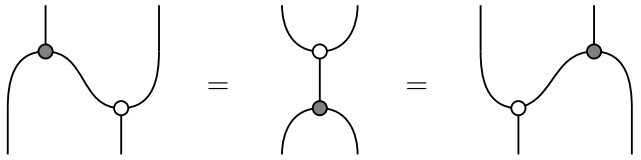
Definition 4.7 (Frobenius algebra via diagrams)**.** In a monoidal category, a *Frobenius algebra* is a comonoid (A, d, e) and a monoid (A, m, u) satisfying the following equation, called the *Frobenius law*:



(4.13)

In a monoidal dagger-category, when $m = d^\dagger$ and $u = e^\dagger$, we call this a *dagger-Frobenius algebra*.

Lemma 4.8. *For a Frobenius algebra, the following equalities hold:*



(4.14)

Proof. See Exercise Sheet 3. □

Examples 4.9. For some examples of Frobenius algebras:

- Let A be an object in the monoidal category **FHilb**. Any choice of orthogonal basis $\{|i\rangle\}_{i=1,\ldots,n}$ for A endows it with the structure of a dagger Frobenius algebra as follows. Define $A \xrightarrow{d} A \otimes A$ by linearly extending $d(|i\rangle)) = |i\rangle \otimes |i\rangle$, define $A \xrightarrow{e} \mathbb{C}$ by linearly extending $e(|i\rangle) = 1$. Then $e^\dagger(z) = z\sum_{i=1}^n |i\rangle$, $d^\dagger(|i\rangle \otimes |i\rangle) = 1$ and $d^\dagger(|i\rangle \otimes |j\rangle) = 0$ when $i \neq j$. This algebra is special when the basis is orthonormal instead of just orthogonal.

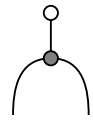
- Any finite group G induces a dagger Frobenius algebra in **FHilb**. Let $A = \mathbb{C}[G]$ be the Hilbert space of linear combinations of elements of G with its standard inner product. In other words, A has G as an orthonormal basis. Define $A \otimes A \xrightarrow{d^\dagger} A$ by linearly extending $d^\dagger(g,h) = gh$, and define $\mathbb{C} \xrightarrow{e^\dagger} A$ by $e^\dagger(z) = z \cdot 1_G$ — this gives an algebra structure called the *group algebra*. Then define $d(g) = \sum_{h\in G} gh^{-1} \otimes h = \sum_{h\in G} h \otimes h^{-1}g$.

- Any group G also induces a dagger Frobenius algebra in **Rel**. Define $d^\dagger = \{((g,h),gh) \mid g,h \in G\} \colon G \times G \to G$ and $e^\dagger = \{(*,1_G)\} \colon 1 \to G$.

  More generally, recall that a *groupoid* is a category whose every morphism is an isomorphism. Any groupoid **G** induces a dagger Frobenius algebra in **Rel** on the set G of all morphisms in **G**. Define $d^\dagger = \{((g,f), g\circ f) \mid \mathrm{dom}(g) = \mathrm{cod}(f)\}$, $e^\dagger = \{(*, \mathrm{id}_x) \mid x \in \mathrm{Ob}(\mathbf{G})\}$.

Frobenius algebras can also be defined in a different way, closer to the way in which they were originally conceived.

Definition 4.10 (Frobenius algebra via form)**.** A *Frobenius algebra* is a monoid (A, m, u) equipped with a *form* $A \xrightarrow{e} I$, such that the composite



(4.15)

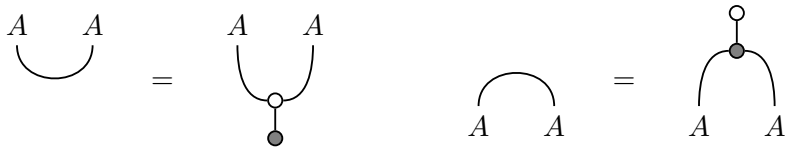
forms part of a self-duality $A \dashv A$. Such a form is sometimes called *non-degenerate*.

Lemma 4.11. *Definitions 4.7 and 4.10 are equivalent.*

Proof. See Exercise Sheet 3. □

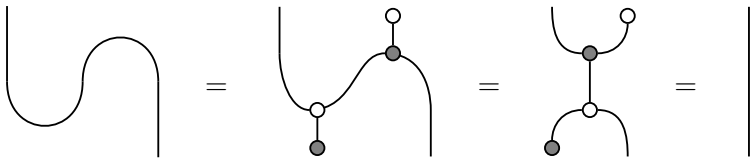
Carrying Frobenius algebra structure is essentially a finite-dimensional property. As the following theorem shows, if an object carries a Frobenius algebra, it must be dual to itself.

Theorem 4.12 (Frobenius algebras have duals)**.** *If an object (A, d, e, m, u) is a Frobenius algebra in a monoidal category, then $A = A^*$ is self-dual (in the sense of Definition 3.1) by $\eta = d \circ u$ and $\varepsilon = e \circ m$.*



(4.16)

Proof. We have to verify the snake equations (3.5).



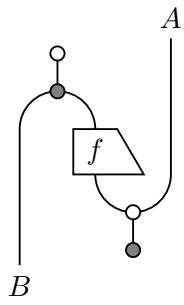
The first equality is the definition (4.16), the second equality is the Frobenius law (4.48), and the third equality follows from unitality (4.6) and counitality (4.4). Similarly, the other snake equation holds. □

Definition 4.13. A *homomorphism of Frobenius algebras* is a morphism that is simultaneously a monoid homomorphism and a comonoid homomorphism.

Lemma 4.14. *In a monoidal category, a homomorphism of Frobenius algebras is invertible.*

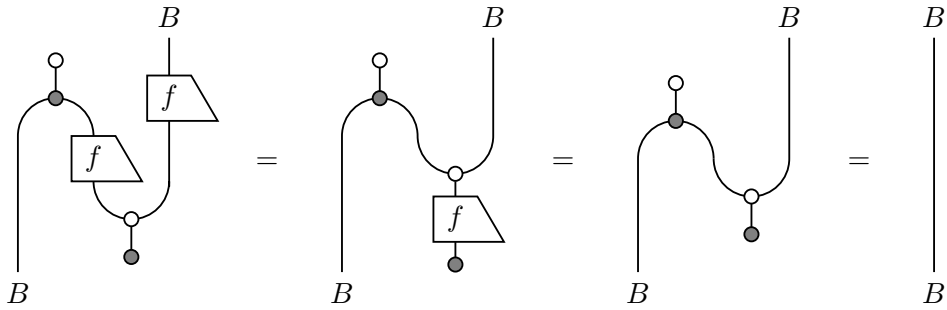
Proof. Given Frobenius algebras on objects A and B and a Frobenius

algebra homomorphism $A \xrightarrow{f} B$, we construct an inverse to f as follows:



(4.17)

We can demonstrate that the composite of this with f gives the identity in one direction:



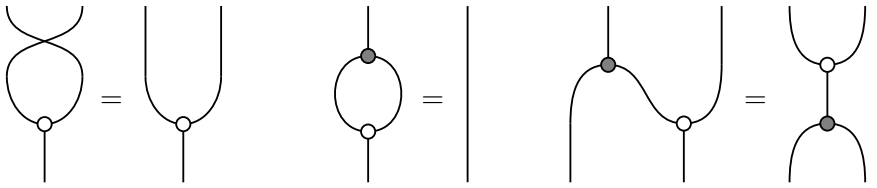
(4.18)

Here the first equality uses the comonoid homomorphism property, the second equality uses the monoid homomorphism property, and the third equality follows from Theorem 4.12. The other composite is also the identity by a similar argument. □

We will see later that in a monoidal category with duals, the no-cloning theorem prevents us from choose copying and deleting maps uniformly. But we can use this contrapositively: instead of stating something negative about *quantum* objects ("you cannot copy them uniformly"), we state something positive about *classical* objects ("you can equip them with a non-uniform copying operation").

Definition 4.15 (Classical structure)**.** A *classical structure* in a dagger–symmetric monoidal category is a commutative special dagger-Frobenius algebra.

Because of cocommutativity (4.2), we only need to require one half of counitality (4.4) and one half of the Frobenius law (4.48). In fact, we need not have mentioned (co)associativity, because it is implied by speciality (4.21) and the Frobenius law (4.48). Also, in compact categories, the Frobenius law (4.48) implies unitality (4.4). Hence to check that (A, d, e) is a classical structure, we only need to verify the following properties:

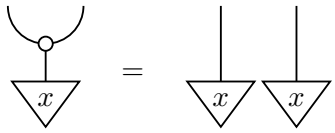


(4.2, 4.21, 4.48)

Classical structures in Hilbert spaces

As we saw in Example 4.9, any choice of orthonormal basis for a finite-dimensional Hilbert space A induces a Frobenius algebra structure on A. In fact, this makes A into a classical structure, as is easy to verify. As it turns out, every classical structure in **FHilb** is of this form. Given a classical structure (A, d, e), we retrieve an orthonormal basis for A by its set of copyable states.

Definition 4.16 (Copyable state)**.** A state $I \xrightarrow{x} A$ of a comonoid (A, d, e) is *copyable* when $(x \otimes x) \circ \rho_I^{-1} = d \circ x$.

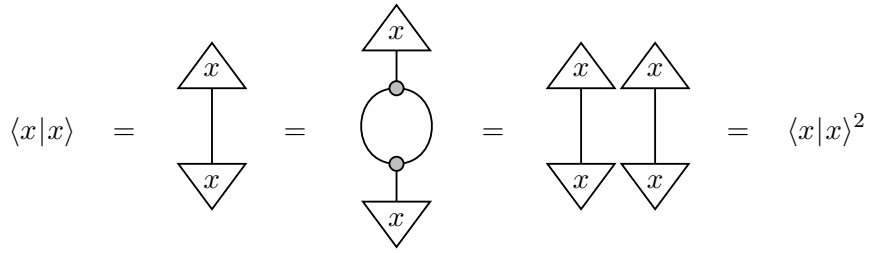


(4.19)

Lemma 4.17. *Nonzero copyable states of a classical structure in* **FHilb** *are orthonormal.*

Proof. It follows from speciality that any nonzero copyable state x has a

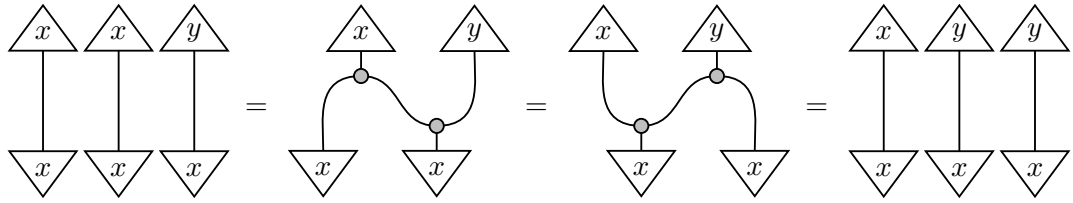
norm that squares to itself:



(4.20)

If x is nonzero then $\langle x|x\rangle$ must therefore be nonzero, a fact that holds in **Hilb**, and which can be obtained abstractly from Lemma 2.25. If scalar multiplication is cancellable, it follows that $\langle x|x\rangle = 1$.

Now 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 $x - y = 0$. □

In fact, the copyable states are not only orthonormal, they span the whole space. So we obtain an orthonormal basis. The proof of this is beyond the scope of this course, and relies on the spectral theorem for commutative C*-algebras.

Theorem 4.18. *Given a classical structure in* **FHilb**, *the copyable states form an orthonormal basis.*

Proof. See [**?**]. □

We have seen in Examples 4.9 that, given an orthonormal basis, we can build a classical structure from it. This construction is clearly inverse the process of finding the copyable states. So we have a complete classification of classical structures.

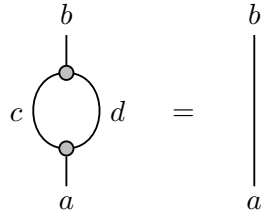
Corollary 4.19. *Classical structures in* **Hilb** *correspond to finite-dimensional Hilbert spaces equipped with a choice of orthonormal basis.*

Classical structures in sets and relations

We now investigate what classical structures look like in **Rel**. Remember that a groupoid is a category in which every morphism has an inverse.

Theorem 4.20. *Special dagger-Frobenius monoids in* **Rel** *correspond exactly to small groupoids.*

Proof. Let (A, M, U) be a dagger-special monoid in **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, we can draw a picture of the dagger-speciality condition (4.21) decorated with elements of A:

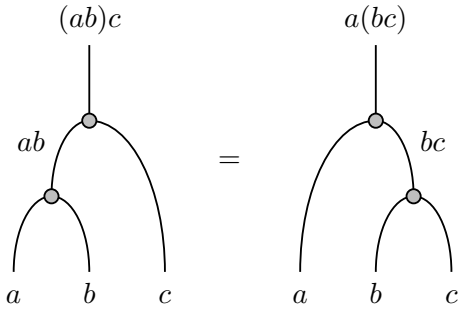


(4.21)

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, since we assume the dagger-special axiom to hold. This tells us something important: 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 — then we must have $a = b$. This says exactly that if two elements can be multiplied, then their product is unique. As a result as can simply write ab for the

product of a and b, remembering that this only makes sense if the product is defined.

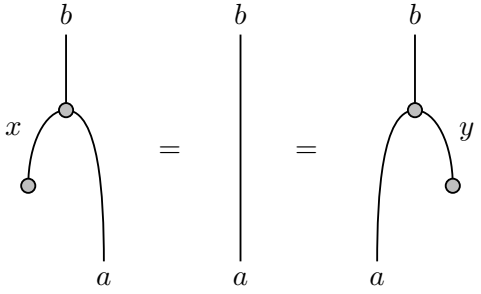
We now consider the associativity condition (4.5). Again, we decorate this with elements of our set to understand what it implies.



(4.22)

This says that ab and $(ab)c$ are both defined exactly when bc and $a(bc)$ are both defined; and furthermore, in that case $(ab)c = a(bc)$. So when a triple product is defined by one bracketing, it's defined by the other bracketing, and the products are equal.

Finally we consider the unit conditions (4.6).



(4.23)

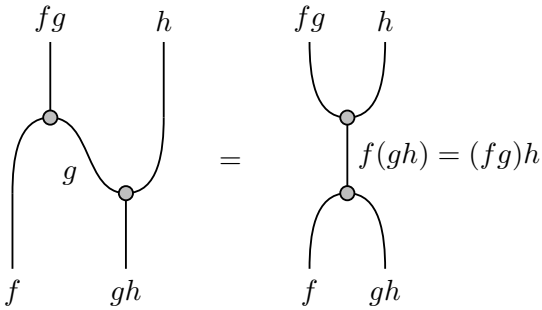
Here $x, y \in U \subseteq A$ are elements of the unit subset, determined by the unit $1 \xrightarrow{U} A$ of the monoid. The first equality says that for all a, b, there exists some $x \in U$ such that $xa = b$ if and only if $a = b$. The second equality says that there exists some $y \in u$ such that $ay = b$ 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.

But now, what happens when multiply elements from U together? Well, if we have $z \in U$ the we certainly have $z \in A$, and we saw that

this implies there exists some $x \in U$ with $xz = x$. But then this means we can multiply $z \in U \subseteq A$ on the left with x to produce x, and that implies $x = z$ by the argument of the previous paragraph! So elements of U are idempotent, and if we multiply two different elements, the result is undefined.

Lastly, for some $a \in A$, is it possible for there to exist $x, x' \in U$ such that $x \neq x'$ and $xa = a = x'a$ — that is, can an element have two distinct left inverses? This would imply that $a = xa = x(x'a) = (xx')a$, which is undefined as we have seen above. So every element has a unique left inverse, and similarly every element has a unique right inverse.

Altogether, this gives exactly the data to define a category. Let U be the set of objects, and A be the set of arrows. Suppose $f, g, h \in A$ are arrows such that fg is defined and gh is defined. Then for a category, we require that $(fg)h = f(gh)$ is also defined. To establish this, we consider the Frobenius axiom decorated with the following elements:

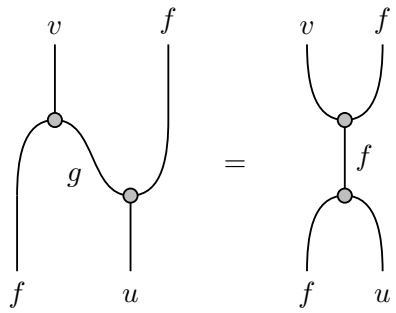


(4.24)

If fg and gh are defined then the left-hand side is defined, and hence the right hand side must also be defined.

For our category to be a groupoid, we must show that every arrow has an inverse. For this, we consider the following different decoration of the

Frobenius axiom, for any $f \in A$, with right unit u and left unit v:

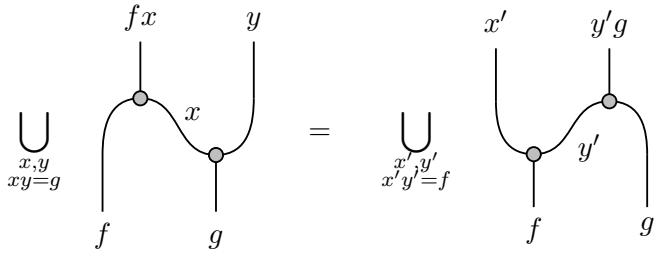


(4.25)

By the properties of left and right units, the decoration of the right-hand side gives an element of the composite relation. Hence there must be some valid $g \in A$ with which to decorate the left-hand side. But such a g is precisely an arrow with $fg = v$ and $gf = u$, which is an inverse for f.

Finally we consider the other direction of the theorem. Suppose we are given a small groupoid. Then write A for its set of arrows and U for its set of unit arrows, with a given subset inclusion $U \subseteq A$. Then we consider the triple (A, M, U) in **Rel**, where M in the partial composition operation of arrows in the category. This is single-valued when it is defined, so M satisfies the dagger-special axiom. Every arrow has a right and left unit, and morphism composition is associative when it is defined. So (A, M, U) is a partial monoid, and hence a dagger-special monoid in **Rel**.

To prove that the Frobenius axiom is satisfied, we evaluate it on an arbitrary input.



(4.26)

On the left we are left with $\cup_{x,y|xy=g}(fx, y)$, and on the right $\cup_{x',y'|x'y'=f}(x', y'g)$. Making the change of variables $x' \rightsquigarrow fx$ 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, and we have demonstrated the Frobenius axiom. □

To classify classical structures, we must understand the implications of the commutativity axiom.

Definition 4.21. An *abelian groupoid* is a groupoid for which all morphisms are endomorphisms, such that for all endomorphisms f, g of the same object, we have $fg = gf$.

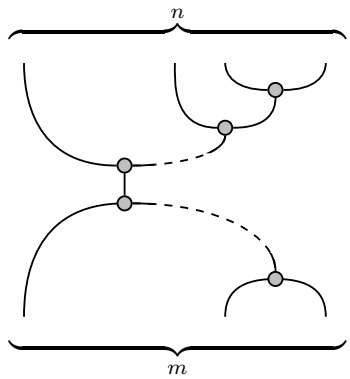
Lemma 4.22. *In* **Rel**, *classical structures exactly correspond to abelian groupoids.*

Proof. An immediate consequence of Theorem 4.20. □

4.3 Normal forms

As you might expect, there are only so many ways you can copy (using d), forget (using e), compare (using $d^\dagger$) and create (using $e^\dagger$) classical information. In fact, as long as we are talking about connected diagrams of classical information flows, there is only one! That is, we can prove the following theorem, which reminds one of the Coherence Theorem 1.2.

Theorem 4.23 (Spider theorem)**.** *Let (A, d, e) be a classical structure. Any connected morphism $A^{\otimes m} \to A^{\otimes n}$ built out of $d, e, \mathrm{id}, \sigma, \otimes$ and $\dagger$ equals the following* normal form*.*



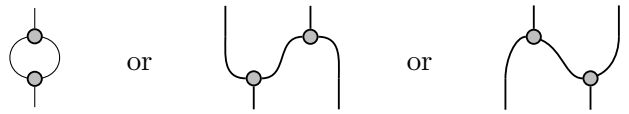
(4.27)

So any morphism built from $d, e, \mathrm{id}, \sigma, \otimes, \dagger$ can be built from normal forms with $\otimes$ and σ.

Proof. We start by ignoring the swap σ, and consider a morphism $A^{\otimes m} \to A^{\otimes n}$ built out of  , ,  ,  , and . Take one of the building blocks  . Our strategy will be to push it down, until it comes before any  . What can we meet on our way down? If we meet a  , we can use unitality (4.6), and the  vanishes. Using the Euler characteristic of the diagram (regarded as a planar graph with g inner faces), we find

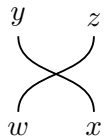
$$\#\left(\ \right) = m + g - 1 + \#\left(\ \right), \qquad \#\left(\ \right) = n + g - 1 + \#\left(\ \right).$$

In particular, there are enough copies of  to spend on getting rid of all the . We can also meet another  . In this case we can use associativity (4.5) to push our chosen one below the one we meet. Finally, we can meet a  . This can happen in three ways:



The first case vanishes by speciality, and in the second and third cases we use the Frobenius law (4.48) to push the  below the  . In the same way, we can push up all the  , getting rid of all  in the process, and end up with the desired normal form.

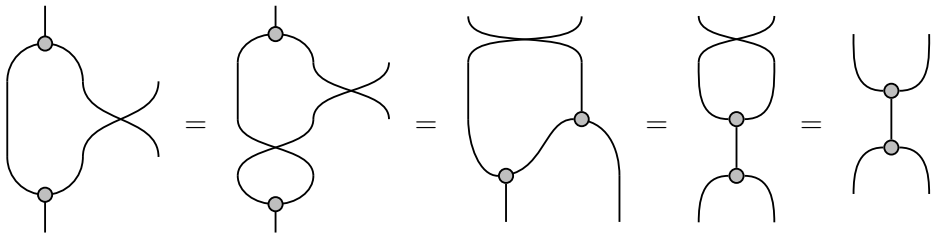
Next, consider diagrams that may involve swap maps as well. Pick one of them. By naturality, we can make sure that only pieces are parallel with our swap map:



Since the diagram is connected, some of the other regions w, x, y, z of the diagram must be connected to each other. Suppose w and x are connected to each other. Then they are connected by a diagram involving strictly

less swap maps than the original, so by induction we can assume it can be brought on normal form. But then, perhaps by using coassociativity, we can make sure that our chosen swap map comes directly above a  . So by cocommutativity, our swap map vanishes, and we are done. The same argument holds when if y and z are interconnected.

We're down to the case where w and y are connected to each other. Then each of the subdiagrams w and y contain strictly less swaps than the original, and we may assume them to be on normal form. So the direct neighbourhood of our swap map looks as follows.



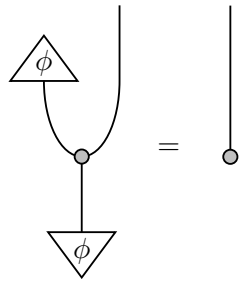
Hence we can make our swap map vanish. The first equality is cocommutativity, the second is naturality of the swap, the third is the Frobenius law, and the fourth equality is cocommutativity again. □

4.4 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 classical structure in any dagger compact category gives rise to a phase group.

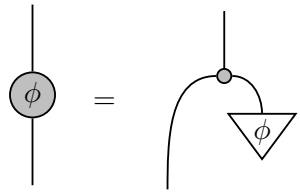
Definition 4.24 (Phase)**.** Let (A, m, u) be a classical structure. A state

$I \xrightarrow{\phi} A$ is called a *phase* when the following equation holds.



(4.28)

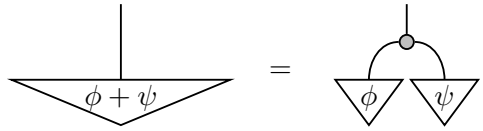
Its *phase shift* is the morphism $d \circ (\phi \otimes \mathrm{id})\colon A \to A$, which we denote as follows.



(4.29)

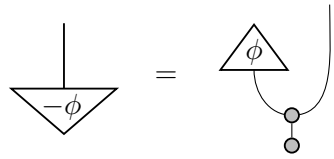
Notice that the unit  of a classical structure is always a phase.

Proposition 4.25. *Let (A, m, u) be a classical structure in a dagger symmetric monoidal category. Its phases form an abelian group under $\phi+\psi := m \circ (\phi \otimes \psi)$ with unit u.*



(4.30)

Proof. It follows from the Spider Theorem 4.23 that $\phi+\psi$ is again a phase when ϕ and ψ are phases. Since m is commutative, the phases thus form a commutative monoid. But for each phase ϕ, we can define an inverse phase $-\phi$ in the following way:



(4.31)

By definition (4.28), it is in fact an abelian group, with inverse $-\phi = (\phi \otimes \mathrm{id}) \circ \eta$. □

The group of the previous proposition is called the *phase group*. Equivalently, the phase shifts form an abelian group under composition. For example, let a classical structure on A in **FHilb** be given by an orthonormal basis $\{|i\rangle\}_{i=1,\ldots,n}$. Its phases are the vectors in A of the form

$$\begin{pmatrix} e^{i\phi_1} \\ \vdots \\ e^{i\phi_n} \end{pmatrix}$$

when written on basis $\{|i\rangle\}$, for real numbers ϕ_i. The group operations are simply

$$\begin{pmatrix} e^{i\phi_1} \\ \vdots \\ e^{i\phi_n} \end{pmatrix} + \begin{pmatrix} e^{i\psi_1} \\ \vdots \\ e^{i\psi_n} \end{pmatrix} = \begin{pmatrix} e^{i(\phi_1+\psi_1)} \\ \vdots \\ e^{i(\phi_n+\psi_n)} \end{pmatrix}, \qquad 0 = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} e^{i0} \\ \vdots \\ e^{i0} \end{pmatrix}$$

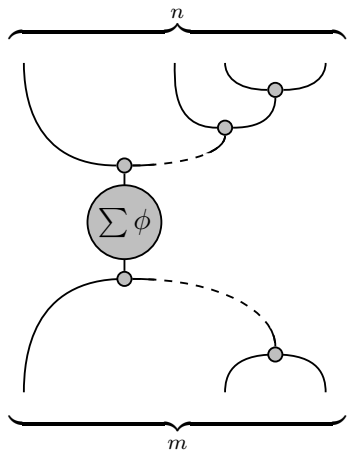
The phase shift accompanying a phase is the unitary matrix

$$\begin{pmatrix} e^{i\phi_1} & 0 & \cdots & 0 \\ 0 & e^{i\phi_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & e^{i\phi_n} \end{pmatrix}.$$

In **Rel**, the phase group of a classical structure induced by an abelian group G as in Example 4.9, is G itself. More generally, consider an abelian groupoid $\mathbf{G}$ and the classical structure in **Rel** it induces. Its phase group is the product group $\prod_{x \in \mathrm{Ob}(\mathbf{G})} \mathbf{G}(x, x)$.

Theorem 4.26 (Generalized spider theorem)**.** *Let (A, d, e) be a classical structure. Any connected morphism $A^{\otimes m} \to A^{\otimes n}$ built out of $d, e, \mathrm{id}, \sigma, \otimes, \dagger$*

and phase shifts equals



(4.32)

where ϕ ranges over all the phases used in the diagram.

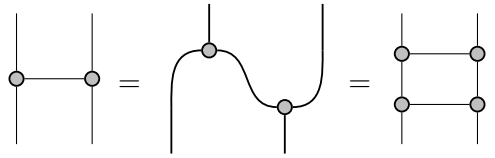
Proof. Adapting the proof of the Spider Theorem 4.23, we can get to a normal form of the form (4.27), with phases dangling at the bottom. But then we can propagate those phases upwards, by the very definition of the phase group operation (4.30). When we reach the "middle" of our diagram, all phases will have been incorporated, and we end up with the desired form (4.32). □

4.5 State transfer

Given: two qubits, one in an unknown state and one in the state $|+\rangle = |0\rangle + |1\rangle$.
Goal: transfer the unknown state from the first qubit to the second.
Extra challenge: apply a phase gate ϕ to the first qubit in the process.

We now study a protocol called state transfer. It operates by using two projections. The first is used to condition on measurement outcomes, and the second is the "measurement projection" (4.33) below. To be precise, consider the computational basis $\{|0\rangle, |1\rangle\}$ on $\mathbb{C}^2$ and the classical structure this induces. By virtue of the spider theorem, we can be quite lax when drawing wires connected by classical structures. They are all the

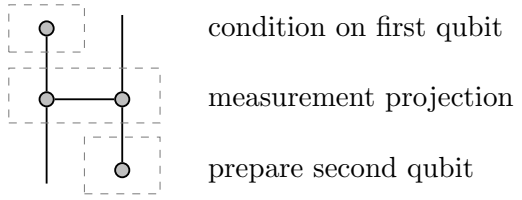
same morphism anyway. For example:



(4.33)

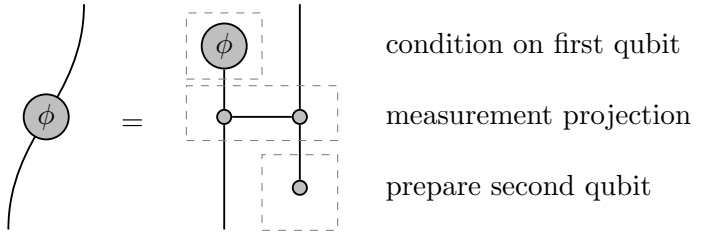
is a projection $\mathbb{C}^2 \otimes \mathbb{C}^2 \to \mathbb{C}^2 \otimes \mathbb{C}^2$.

The protocol consists of three steps. First, prepare the second qubit in $|+\rangle$. Second, apply the measurement projection to the compound system of both qubits. Third, condition on the first qubit.



By the Spider Theorem 4.23, this equals the identity! 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 generalized Spider Theorem 4.26, we can also easily achieve the extra challenge, by the following adapted protocol.



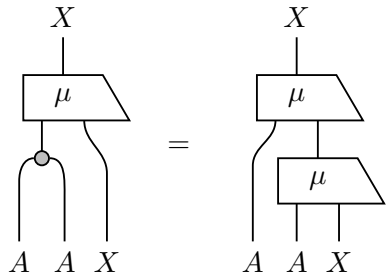
This protocol is important in *measurement-based quantum computing*.

4.6 Modules and measurement

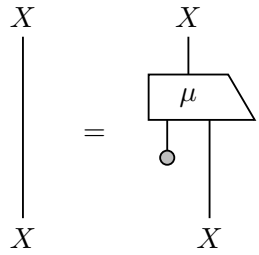
Modules

We can use classical structures to give mathematical structure to the notion of quantum measurement. To do this, we need the theory of *modules*.

Definition 4.27. For a monoid (A, m, u) in a monoidal category, a *module* is an object X equipped with a map $A \otimes X \xrightarrow{\mu} X$ satisfying the following equations:



(4.34)



(4.35)

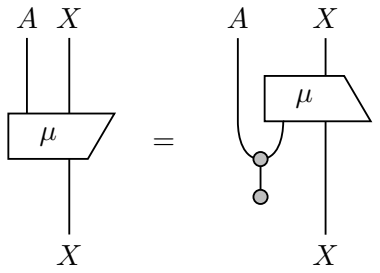
We call the morphism μ an *action* of the monoid (A, m, u) on the object X. There is an asymmetry here: we could just as easily have chosen $X \otimes A$ as the source of x, which would have led to reflected versions of axioms (4.34) and (4.35). To distinguish these, we could call the structure defined above a *left module*, and the alternative version a *right module*. We will only consider left modules in these notes, so we will just refer to them as modules.

These equations for a module look very familiar: they are almost identical to the associativity (4.5) and unit (4.6) laws from the definition of a

monoid! We can interpret a module action $A \otimes X \xrightarrow{\mu} X$ as a way modify the state of the system X in a way that depends on the state of the system A. The associativity condition (4.34) then means that if we have two copies of the system A, we could combine them using the monoid operation and use the result to modify X, or instead simply modify X twice with each copy of A in turn. The unitality condition (4.35) means that if we act on a system X with a monoid in its unit state, the state of X doesn't change.

If we have a classical structure in a monoidal dagger-category, we can define an additional axiom.

Definition 4.28. In a monoidal dagger-category, a *dagger module* for a classical structure (A, m, u) is a module action $A \otimes X \xrightarrow{\mu} X$ satisfying the following equation:



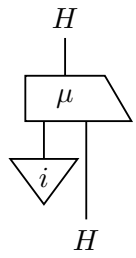
(4.36)

In **Hilb**, dagger modules are important because they correspond exactly to *measurement contexts*: Hilbert spaces H equipped with a partition into mutually-orthogonal subspaces.

Lemma 4.29. *In* **Hilb***, a dagger module for a classical structure* (A, m, u) *on a Hilbert space* H *corresponds to a decomposition of* H *into a family of* $\dim(A)$ *orthogonal subspaces.*

Proof. The module action $A \otimes H \xrightarrow{\mu} H$ is determined by the endomor-

phisms



(4.37)

for each classical point $|i\rangle \in A$ of the classical structure. We can show that these are a family of projectors, which are self-adjoint and sum to the identity, and which therefore determine an orthogonal partition of H.

$P_i P_i = P_i$ comes from the associativity axiom for a module, the fact that i is copyable, and dagger-specialness.

$P_i = P_i^\dagger$ comes from the dagger-module axiom.

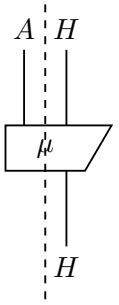
Sum to the identity comes from the definition of the unit, and the unit axiom for a module.

Conversely, suppose we have an orthogonal partition of H. Then we can define a module action $A \otimes H \xrightarrow{\mu} H$ by asserting that each composite of the form (4.37) corresponds to one of our projectors. It can then be shown directly that this satisfies the associativity, unitality and dagger-module axioms, using the same techniques as employed above. □

Every classical structure (A, m, u) gives rise to a partition of A, since it describes a basis structure. As a result, the multiplication operation $A \otimes A \xrightarrow{m} A$ itself satisfies the dagger module axioms.

Measurements and controlled operations

A *projective measurement* corresponds to the adjoint $H \xrightarrow{\mu^\dagger} A \otimes H$ of a dagger module for a classical structure (A, m, u).

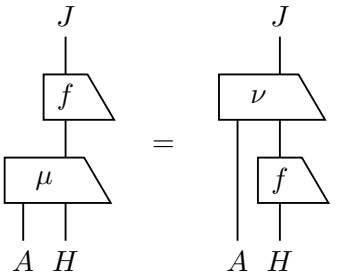


(4.38)

The system marked A encodes the result of the measurement. It represents classical information. The dashed line separates this from the total state space of the system. Mathematically, we require that the the system on the left of the dashed line is always a classical structure, and that this has a dagger module action on the system on the right of the dashed line. For each given basis element $|i\rangle \in A$ corresponding to a particular measurement outcome, the state space of the system is reduced to the support of P_i, as defined above.

Following a measurement, the only allowed quantum dynamics are the *controlled operations*. These are the unitary maps on H which do not change the result of the measurement. Mathematically, the are the *module homomorphisms* for the module action.

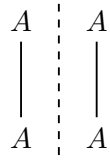
Definition 4.30. In a monoidal category, given a monoid (A, m, u) and module actions $A \otimes H \xrightarrow{\mu} H$ and $A \otimes J \xrightarrow{\nu} J$, a *module homomorphism* $\mu \xrightarrow{f} \nu$ is a morphism $H \xrightarrow{f} J$ such that the following condition holds:



(4.39)

For the morphism f to represent a physically possible operation, we also require it to be *norm preserving*, meaning that it is an isometry, satisfying $f^\dagger \circ f = \mathrm{id}$.

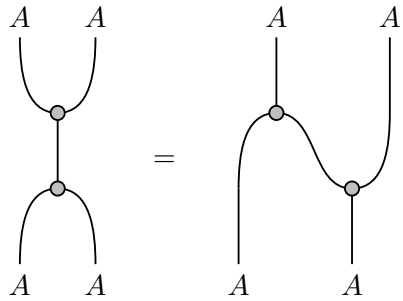
Suppose that we have a classical structure (A, m, u), and for each value of the classical information, a one-dimensional state space. Then our total state space is $A \otimes \mathbb{C} \simeq A$ on the right of the dashed line.



(4.40)

The module action in this case is given by the monoid multiplication operation. Suppose we want to find the value of the classical information. This means for each basis element $|i\rangle \in A$ defined by the classical structure, we want to create a new copy of the system A prepared in the state $|i\rangle$. The comultiplication $A \to A \otimes A$ acts as $|i\rangle \mapsto |i\rangle \otimes |i\rangle$, so it does what we want. But does it satisfy the module homomorphism property given above? It has to, as the module homomorphisms are the only physically-implementable operation. The other necessary condition, isometry, is satisfied thanks to the dagger-specialness axiom.

Verifying the module homomorphism definition 4.30 for $\mu = m$, $\nu = m \otimes \mathrm{id}_A$ and $f = m^\dagger$, we obtain the following condition:



(4.41)

For (A, m, u) a commutative monoid, this is precisely the defining equation for a dagger-Frobenius monoid! So we have yet another reason to use Frobenius algebras to describe classical information: they allow us to

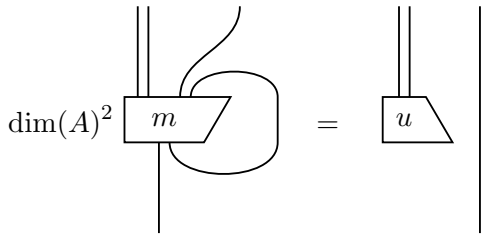
extract the value of classical information and turn it into quantum information. This also gives us a completely new definition of Frobenius algebra.

Definition 4.31 (Frobenius algebra by modules)**.** A *Frobenius algebra* is a monoid (A, m, u) and a comonoid (A, d, e) such that d is a module homomorphism for the action of A on itself given by m.

Quantum teleportation

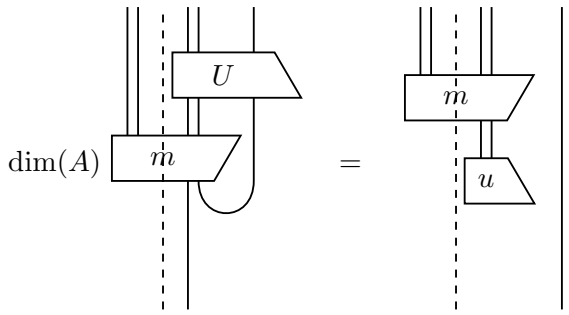
We can use this new account of quantum measurement to axiomatise quantum teleportation in an algebraic way.

Lemma 4.32. *A classical structure $(A \otimes A, m, u)$ on a product system describes the measurement operation in a teleportation protocol if and only if*



(4.42)

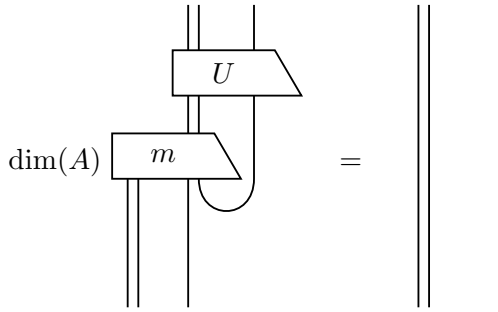
Proof. Successful execution of a quantum teleportation protocol corresponds to the following equation:



(4.43)

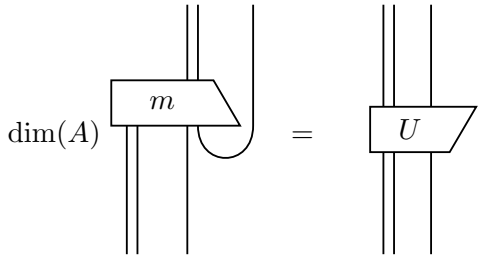
Bending down the top-left $A \otimes A$ leg using the compact structure induced

by the classical structure gives the following equivalent expression:



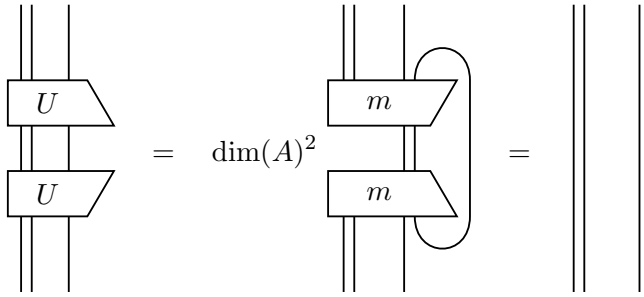
(4.44)

We neglect the vertical dashed lines from this point on, as they are only important for the interpretation and we are trying to prove a purely mathematical result. We now compose both sides with $U^\dagger$ at the top:



(4.45)

Using this definition of $U^\dagger$, we can evaluate $U \circ U^\dagger = \mathrm{id}_{(A\otimes A)\otimes A}$ as follows:



(4.46)

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 the expression (4.42) as required.

For this to make sense physically, the morphism U must be a controlled operation. Using (4.45)

Conversely, suppose we have a classical structure satisfying equation (4.42). Then we can define □

4.7 Exercises

Exercise 4.7.1. 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 $m \circ (\mathrm{id} \otimes u') = \mathrm{id} = m \circ (u' \otimes \mathrm{id})$, then $u' = u$. Conclude that unitality is a property.

(b) Show that in categories with products, every object has a unique comonoid structure under the monoidal structure induced by the categorical product.

(c) If $(\mathbf{C}, \otimes, I)$ is a monoidal category, denote by $\mathbf{cMon}(\mathbf{C})$ the category of commutative monoids in $\mathbf{C}$ with monoid homomorphisms as morphisms. Show that the categories $\mathbf{cMon}(\mathbf{C})$ and $\mathbf{C}$ are isomorphic if and only if $\otimes$ is a coproduct.

Exercise 4.7.2. This exercise is about tensor products of various structures with progressively more structure.

(a) Show that, in a symmetric monoidal category, the tensor product of monoids is again a monoid.

(b) Show that, in a symmetric monoidal category, the tensor product of Frobenius algebras is again a Frobenius algebra.

(c) Show that, in a symmetric monoidal dagger-category, the tensor product of classical structures is again a classical structure.

Exercise 4.7.3. This exercise is about monoid structures on a single object A in a symmetric monoidal category. Suppose you have morphisms $X \otimes X \xrightarrow{m_1, m_2} X$ and $I \xrightarrow{u_1, u_2} X$, such that (X, m_1, u_1) and (X, m_2, u_2)

are both monoids, and the following diagram commutes:

$$\begin{array}{ccc} A \otimes A \otimes A \otimes A & \xrightarrow{m_2 \otimes m_2} & A \otimes A \\ \downarrow{\scriptstyle \mathrm{id} \otimes \sigma \otimes \mathrm{id}} & & \\ A \otimes A \otimes A \otimes A & & \downarrow{\scriptstyle m_1} \\ \downarrow{\scriptstyle m_1 \otimes m_1} & & \\ A \otimes A & \xrightarrow{m_2} & A \end{array} \tag{4.47}$$

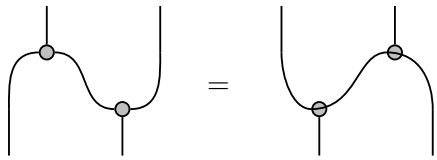
(a) Show that $u_1 = u_2$.

(b) Show that $m_1 = m_2$.

(c) Show that m_1 is commutative ($m_1 \circ \sigma = m_1$).

(d) What does diagram (4.47) mean in terms of homomorphisms? What conclusions can you draw?

Exercise 4.7.4. This exercise is about the interdependencies of the defining properties of classical structures in symmetric monoidal dagger-categories. Recall the Frobenius law:



(4.48)

(a) Show that, for any monoid (A, m, u) and comonoid (A, d, e), the Frobenius law (4.48) implies

$$d \circ m = (m \otimes \mathrm{id}) \circ (\mathrm{id} \otimes d) = (\mathrm{id} \otimes m) \circ (d \otimes \mathrm{id}) \tag{4.49}$$

(b) 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 (4.49) together imply associativity for m.

(c) Suppose $A \xrightarrow{d} A \otimes A$ and $A \otimes A \xrightarrow{m} A$ satisfy equation (4.49), 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 4.7.5. This exercise is about different definitions of Frobenius algebras. Show that the three definitions below define the same set structures. Hint: for the implication (b)⇒(a), find a way to express the comultiplication of an (a)–style Frobenius algebra just in terms of m, e and $d \circ u$.

(a) Pairs of a monoid (A, m, u) and a comonoid (A, d, e) satisfying the Frobenius law (4.48).

(b) Monoids (A, m, u) equipped with a *non-degenerate form*: a morphism $A \xrightarrow{e} I$ such that the composite $e \circ m$

forms the counit for a self-duality $A \dashv A$.

(c) Pairs of a monoid (A, m, u) and a comonoid (A, d, e) such that d is a module homomorphism from the action $A \otimes A \xrightarrow{m} A$ of A on itself, to the action $A \otimes (A \otimes A) \xrightarrow{\alpha_{A,A,A}} (A \otimes A) \otimes A \xrightarrow{m \otimes \mathrm{id}_A} I \otimes A \xrightarrow{\lambda_A} A$ of A on $A \otimes A$.

Exercise 4.7.6. This exercise is about phases for classical structures in **Rel**. Let G be an abelian group, and $G \xrightarrow{d} G \times G$ the classical structure in **Rel** it induces.

(a) Show that $d \circ u = \{(*, (x, x^{-1})) \mid x \in G\}$.

(b) Show that if $1 \xrightarrow{g} G$ is a phase, then $g = \{(*, x)\}$ for precisely one x in G.

(c) Conclude that the phase group of d is G itself.

Exercise 4.7.7. This question is on describing teleportation using Frobenius algebras.

(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 (**??**).

(b) (Hard.) 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.

Notes and further reading

The Frobenius law (4.48) is named after F. Georg Frobenius, who first studied the requirement that $A \cong A^*$ as right A-modules for a ring A in the context of group representations in 1903 [33]. The formulation with multiplication and comultiplication we use is due to Lawvere in 1967 [50], and was rediscovered by Quinn in 1995 [64] and Abrams in 1997 [1]. Dijkgraaf realized in 1989 that the category of commutative Frobenius algebras is equivalent to that of 2-dimensional topological quantum field theories [29]. For a comprehensive treatment, see the monograph by Kock [49].

Coecke and Pavlović first realized in 2007 that commutative Frobenius algebras could be used to model the flow of classical information [24]. Theorem **??**, that classical structures in **FHilb** correspond to orthonormal bases, was proved in 2009 by Coecke, Pavlović and Vicary [25]. In 2011, Abramsky and Heunen adapted Definition 4.15 to generalize this correspondence to infinite dimensions in **Hilb** [6].

Theorem **??**, that classical structures in **Rel** are groupoids, was proven by by Pavlović in 2009 [61], and generalized to the noncommutative case by Heunen, Contreras and Cattaneo in 2012 [37].

The phase group was made explicit by Coecke and Duncan in 2008 [19], and later Edwards in 2009 [31, 21]. The state transfer protocol is important in efficient measurement-based quantum computation. It is due to Perdrix in 2005 [63].

Chapter 5

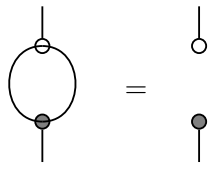
Complementarity

In this chapter we will study what happens when we have *two* interacting classical structures. Specifically, we are interested in they are 'maximally incompatible', or *complementary*. In the case of qubits, such *mutually unbiased bases* play a pivotal role in quantum information theory. We will show how this gets us Hadamard gates, and hence universal quantum computation. Graphically, we will distinguish between the two (co)units and (co)multiplications by colouring their dots differently.

5.1 Bialgebras

It turns out that complementarity can be modelled by letting the multiplication of one observable interact with the comultiplication of the other in a way that is in many ways opposite to the way the multiplication and the comultiplication of a single classical structure interact.

Definition 5.1. A pair of a comonoid (A, d, e) and a monoid (A, m, u) is called *disconnected* when $m \circ d = u \circ e$.

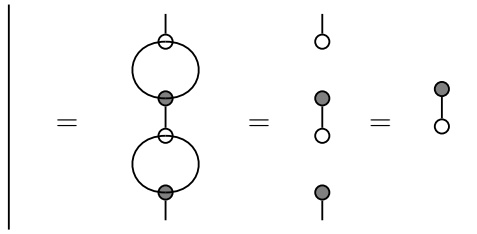


(5.1)

As far as interaction between monoids and comonoids goes, speciality and disconnectedness are opposite extremes. As the following proposition shows, both cannot happen simultaneously under reasonable conditions.

Proposition 5.2. *If a comonoid* (A, d, e) *and a monoid* (A, m, u) *are simultaneously special and disconnected, and* $(e \circ u) \bullet \mathrm{id}_A = \mathrm{id}_A$ *implies* $e \circ u = \mathrm{id}_I$*, then* $A \cong I$*.*

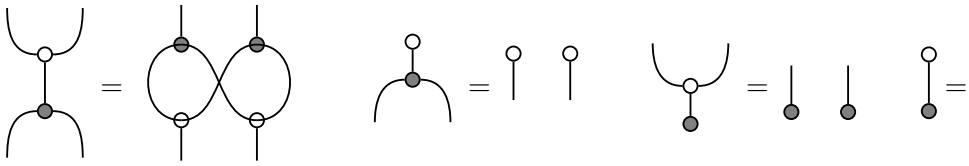
Proof. We will show that e and u are each others' inverses. Applying equation (5.1) and then equation (4.21) establishes $e \circ u = \mathrm{id}_A$. Conversely,



which by assumption implies that $e \circ u = \mathrm{id}_I$. □

There is another way in which we can compose first multiplication and then comultiplication, called the bialgebra laws.

Definition 5.3 (Bialgebra)**.** A *bialgebra* in a monoidal category consists of a monoid (A, m, u) and a comonoid (A, d, e) on the same object, satisfying the following equations, called the *bialgebra laws*.



(5.2)

The last equation $u \circ e = \mathrm{id}_I$ is not missing a picture, because we are drawing id_I as the empty picture (1.11). The following concise formulation is a good way to remember the bialgebra laws.

Lemma 5.4. *A comonoid (A, d, e) and monoid (A, m, u) form a bialgebra if and only if d and e are monoid homomorphisms.*

Proof. Just unfold the definitions. This involves showing that $A \otimes A$ carries a monoid structure when A does, which we leave as an exercise. □

Examples 5.5.

- Considering **Hilb** as a monoidal category under biproducts, any object A has a bialgebra structure given by its copying and deleting maps: $d = \begin{pmatrix} 1 \\ 1 \end{pmatrix} : A \to A \oplus A$, $e = !_A : 0 \to A$, $u = !_A : A \to 0$, $m = \begin{pmatrix} 1 & 1 \end{pmatrix} : A \oplus A \to A$.

- Any finite monoid G (in **Set**) induces a bialgebra in $(\mathbf{Hilb}, \otimes, \mathbb{C})$ as follows. Let $A = \mathbb{C}[G]$ 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 $A \otimes A \xrightarrow{m} A$ by linearly extending $m(g, h) = gh$, define $\mathbb{C} \xrightarrow{u} A$ by $u(z) = z \cdot 1_G$, and define d and e by linearly extending $d(g) = g \otimes g$ and $e(g) = 1$.

  Notice that m and u can also make A into a Frobenius algebra as in Example 4.9, but with different d and e. Indeed, by the following theorem, they *have* to be different unless G is the trivial monoid.

- Any monoid G is a bialgebra in the monoidal category **Set**, by $d(g) = (g, g)$, $e(g) = *$, $u(*) = 1_G$, $m(g, h) = gh$.

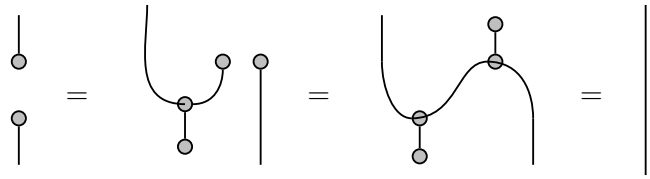
  Notice again that m and u can also make G into a Frobenius algebra in **Rel** as in Example 4.9, but again, with different d and e.

- Fock space?

As far as interaction between monoids and comonoids is concerned, Frobenius algebras and bialgebras are opposite extremes. The following theorem shows that both cannot happen simultaneously, except in the trivial case. The crux is that the Frobenius law (4.48) equates *connected* diagrams, whereas the bialgebra laws (5.2) equate connected diagrams with *disconnected* ones. As we saw with special and disconnected algebras in Proposition 5.2, the only object that is both connected and disconnected is the tensor unit.

Theorem 5.6 (Bialgebras cannot be Frobenius)**.** *If* $(A, d, e, d^\dagger, e^\dagger)$ *is both a Frobenius algebra and a bialgebra in a monoidal category, then* $A \cong I$*.*

Proof. We will show that $u = e^\dagger$ and e are each others' inverses. The bialgebra laws (5.2) already require that $e \circ u = \mathrm{id}_I$.



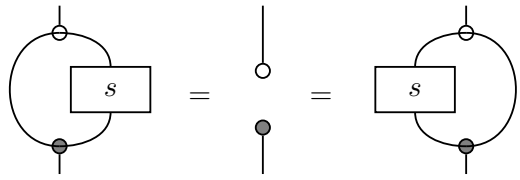
The first equality is counitality (4.4), the second equality is one of the bialgebra law (5.2), and the last equality follows from Theorem 4.12. □

The previous theorem is not all that surprising when we realize that $e \circ u$ is the dimension of A. Equation (5.2) says that A and I have the same dimension. But notice that the proof of the previous theorem holds equally well when we had merely required $e \circ u$ to be positive and invertible, instead of $e \circ u = \mathrm{id}_I$. We will in fact do this soon, but first we consider Hopf algebras.

5.2 Hopf algebras and complementarity

A property that often goes together with bialgebras is the so-called Hopf law.

Definition 5.7 (Hopf law)**.** Let (A, d, e) be a comonoid and (A, m, u) a monoid, and $A \xrightarrow{s} A$ a morphism. The *Hopf law* states $m \circ (\mathrm{id}_A \otimes s) \circ d = \mathrm{id}_A = m \circ (s \otimes \mathrm{id}_A) \circ d$. The morphism s is called the *antipode*.



(5.3)

The example we gave of a bialgebra $\mathbb{C}[G]$ induced by a finite monoid G in fact satisfies the Hopf law if and only if the monoid is a group. The antipode $\mathbb{C}[G] \xrightarrow{s} \mathbb{C}[G]$ is the linear extension of $s(g) = g^{-1}$, and the algebra is then called the *group algebra*. In this sense bialgebras satisfying the Hopf law are the quantum version of groups.

Proposition 5.8. *Bialgebras algebras in* **Set** *satisfying the Hopf law are precisely groups.*

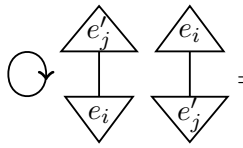
Proof. Given a bialgebra (G, d, e, m, u, s) in **Set** satisfying the Hopf law, define a multiplication on G by $gh := m(g, h)$, define inverses by $g^{-1} := s(g)$, and set $1 := u(*) \in G$. It follows from the Hopf law (5.3) that $g^{-1}g = 1 = gg^{-1}$, and hence that G is a group.

Conversely, let G be a group. Define $G \xrightarrow{d} G \times G$ by $d(g) = (g, g)$. Similarly, define $e(g) = *$, $u(*) = 1_G$, $m(g, h) = gh$, and $s(g) = g^{-1}$. It is a quick exercise to verify that these data satisfy the bialgebra laws (5.2) and the Hopf law (5.3). □

Now, suppose we have not just a pair of a monoid and a comonoid, but a pair of classical structures. In **FHilb**, this means we have chosen two bases of a single space. Then there is a canonical choice for an antipode, and the Hopf law encodes that the two bases are *mutually unbiased*.

Definition 5.9. Two bases $\{e_i\}, \{e'_i\}$ of a Hilbert space H are *mutually unbiased* when $|\langle e_i | e'_j \rangle|^2 = 1/\dim(H)$ for all i, j.

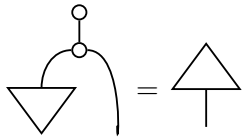
The idea is that each of the elements of one basis make maximal angles with each of the elements of the other basis. In other words, having perfect information about the system in one basis reveals nothing at all in the other basis. For example, in the case of qubits, the bases $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ are mutually unbiased. We can reformulate this graphically as follows.



$$= \tag{5.4}$$

In **FHilb**, basis vectors correspond to copyable states, and satisfy the

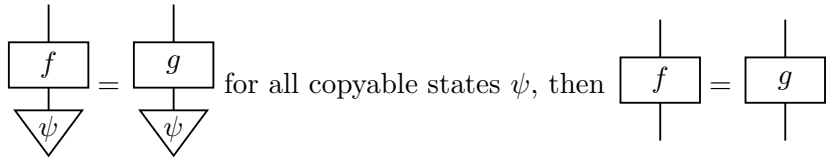
following equation.



(5.5)

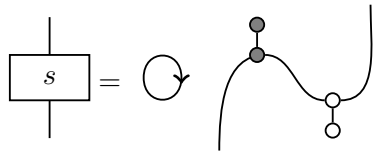
Moreover, they form a basis, which gives a stronger version of well-pointedness.

Definition 5.10. A classical structure on A has *enough copyable states* when two morphisms $A \xrightarrow{f,g} B$ are equal as soon as $f \circ \psi = g \circ \psi$ for all copyable states $I \xrightarrow{\psi} A$.



(5.6)

Definition 5.11 (Complementarity)**.** Two classical structures are called *complementary* when they satisfy the Hopf law (5.3) for the following antipode.

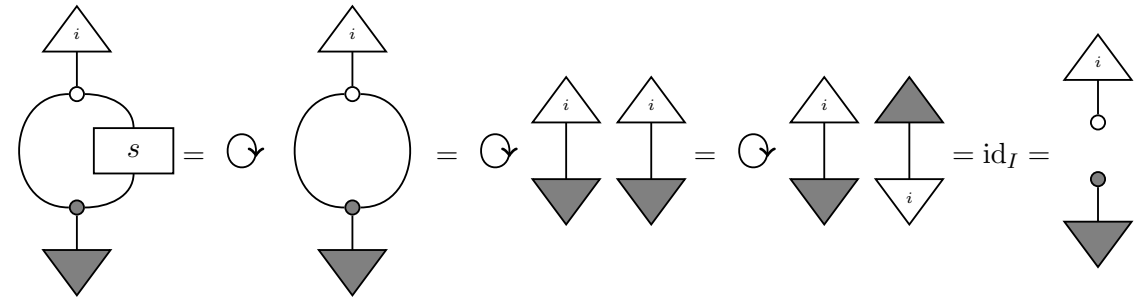


(5.7)

Proposition 5.12. *Suppose equations* (5.5) *and* (5.6) *hold. Then the Hopf law* (5.3) *is equivalent to equation* (5.4)*. Hence two orthonormal bases on a Hilbert space are mutually unbiased if and only if the classical structures they induce are complementary.*

Proof. Assume equations (5.4) and (5.5), and draw copyable states in the

same color as the classical structure that copies them. Then:

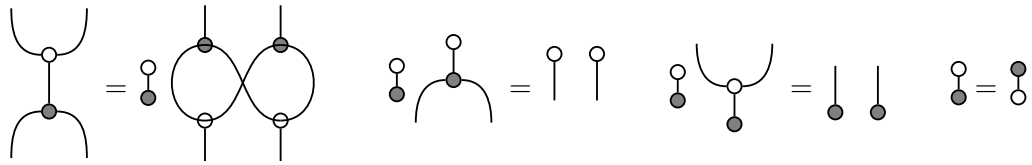


Equation (5.6) now establishes the Hopf law (5.3). The converse is similar. □

5.3 Strong complementarity

We will now investigate a strong version of complementarity, where not just the Hopf law holds, but also the bialgebra laws. In fact, the latter will imply the former. However, as we saw in Proposition 5.2 and Theorem 5.6, we will need to scale by an appropriate dimension factor. This leads to a *scaled* version of the bialgebra laws.

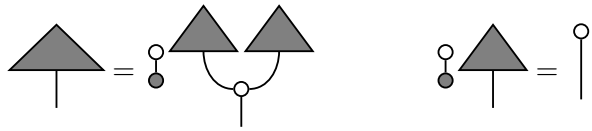
Definition 5.13 (Scaled bialgebra, strong complementarity)**.** A *scaled bialgebra* is a pair of a monoid $(A,$  $)$ and a comonoid $(A,$  $)$ satisfying the following equations.



(5.8)

Two classical structures are called *strongly complementary* when the monoid of one forms a scaled bialgebra with the comonoid of the other.

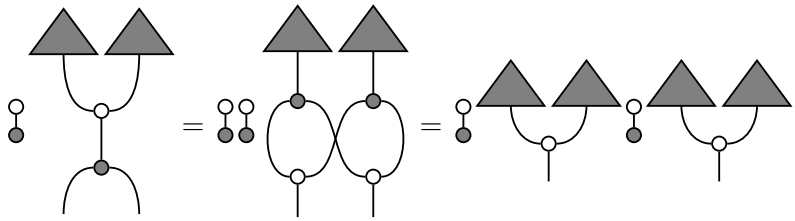
Lemma 5.14. *Suppose that the scalar*  *is invertible. For two strongly complementary classical structures, the following defines a monoid structure on the copyable states of*  .



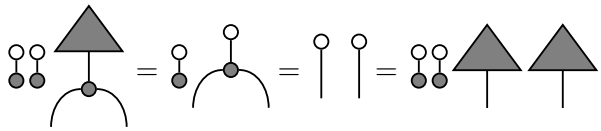
(5.9)

In fact, this defines a submonoid of the phase group for ( , ).

Proof. Associativity and unitality are clear, but we have to prove that $i \cdot j$ and 1 are again copyable states. For $i \cdot j$:

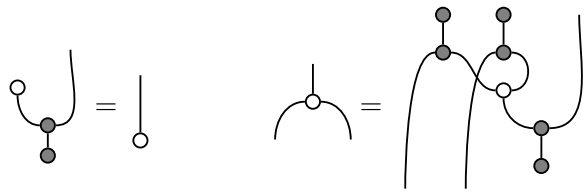


And for 1:



Since the scalar  is invertible, 1 is a copyable state. □

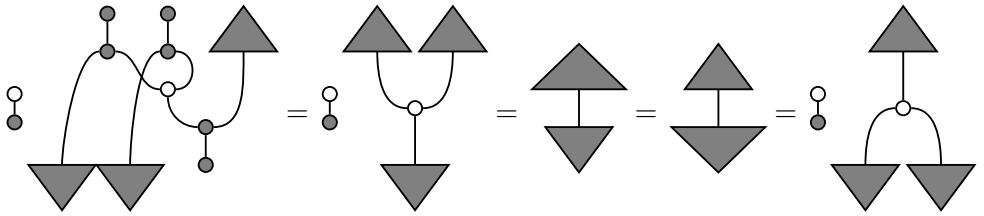
Lemma 5.15. *Suppose that the scalar*  *is invertible. If they have enough copyable states, then strongly complementary classical structures satisfy the following equation.*



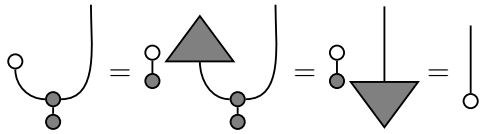
(5.10)

Hence  $= \dim(A)$.

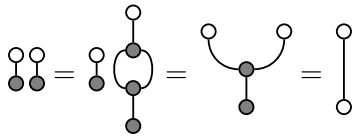
Proof. First, use Lemma 5.14:



Then, we can conclude the right equation of (5.10) from property (5.6). Similarly, for the left equation of (5.10):



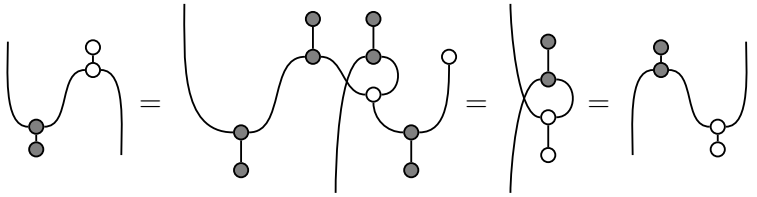
Finally:



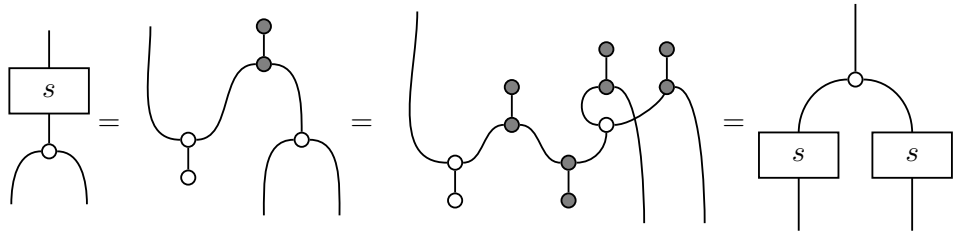
and the latter equals $\dim(A)$ by the Spider Theorem 4.23 and Theorem 4.12. □

Lemma 5.16. *Suppose that the scalar*  *is invertible. If two strongly complementary classical structures have enough copyable states, then the antipode* (5.7) *is self-adjoint, and is an automorphism for both classical structures.*

Proof. First we prove that $s = s^\dagger$ using Lemma 5.15.



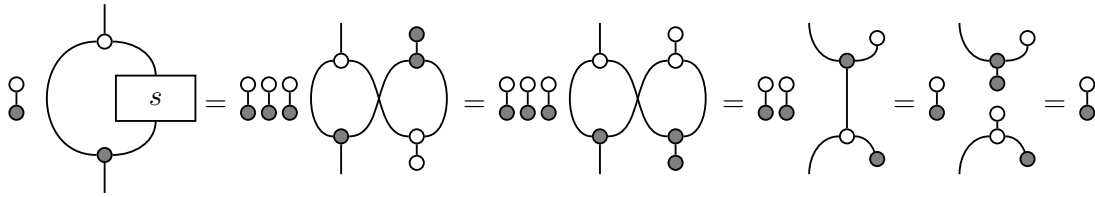
Consequently, s preserves units. Using Lemma (5.10) again:



Therefore s is a homomorphism of Frobenius algebras, and must be an isomorphism by Lemma 4.14. □

Proposition 5.17. *Suppose that the scalar*  *is invertible. If two strongly complementary classical structures have enough copyable states, then they are complementary.*

Proof.



The first equality is the definition of s, the second equality is Lemma 5.16, the third equality is the scaled bialgebra law (5.8), the fourth equation uses the Spider Theorem 4.23 and the scaled bialgebra law (5.8), and the last equation follows from Lemma 5.15. □

The classification of pairs of complementary classical structures (i.e. mutually unbiased bases) on a finite-dimensional Hilbert space is an open problem. But we can classify strong complementarity completely.

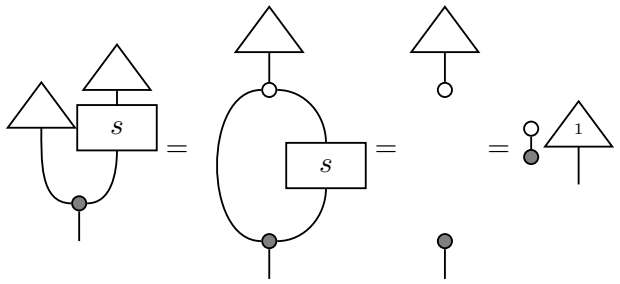
Theorem 5.18. *Pairs of strongly complementary classical structures on H in* **FHilb** *correspond to abelian groups of order* $\dim(H)$.

Proof. Let G be an abelian group of order n. Its elements form a basis $\{|g\rangle\}$ for $H = \mathbb{C}^n$. Defining

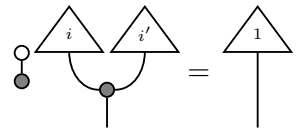
$$d\colon |g\rangle \mapsto |g\rangle \otimes |g\rangle, \qquad e\colon |g\rangle \mapsto 1$$
$$m\colon |g\rangle \otimes |h\rangle \mapsto \frac{1}{\sqrt{n}}|g+h\rangle \qquad u\colon 1 \mapsto \sum_{g\in G} |g\rangle$$

gives classical structures $(A, d, e, d^\dagger, e^\dagger)$ and $(A, m^\dagger, u^\dagger, m, u)$. Moreover, (A, d, e, m, u) is a scaled version of the group algebra, and hence forms a scaled bialgebra. Therefore these two classical structures are strongly complementary.

For the converse, let two strongly complementary classical structures be given. By Lemma 5.14 the copyable states of  form a monoid under  , and in fact a submonoid of the phase group. But the phase group is finite, and any submonoid of a finite group is a (sub)group itself. This already establishes the theorem, but let's work out what inverses look like anyway. The following equation now follows from Proposition 5.17 for any state that is copyable under  .



By Lemma 5.16 the antipode s is a homomorphism of Frobenius algebras and therefore an isomorphism by Lemma 4.14. Thus s permutes classical points. Hence the previous equation implies that each copyable state i has a copyable state i' such that:

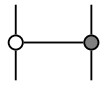


Therefore all copyable states of  have inverses, and  is isomorphic to the group algebra $\mathbb{C}[G]$ for that abelian group G. □

5.4 Applications

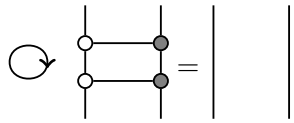
We can now consider some applications to quantum computation. We start by defining CNOT gates. This gate performs a NOT operation on the second qubit if the first (control) qubit is $|1\rangle$, and does nothing if the first qubit is $|0\rangle$. But the definition itself makes sense for arbitrary pairs of classical structures.

CNOT :=



(5.11)

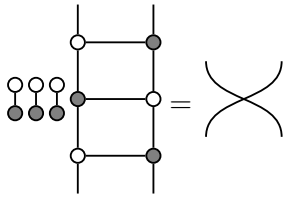
Proposition 5.19. *Two classical structures* (,) *and* (,) *are complementary if and only if the following equation holds.*



(5.12)

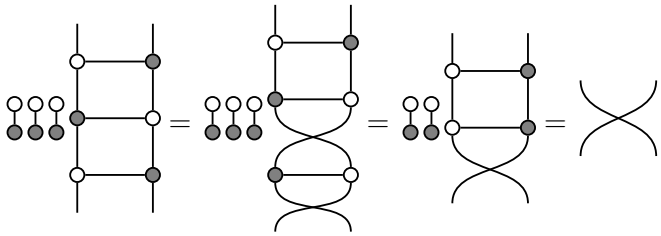
Proof. Both implications follow from one application of the Spider Theorem (4.23) and one application of the Hopf law (5.3). □

Theorem 5.20. *Two complementary classical structures* (,) *and* (,) *are strongly complementary if and only if the following equation holds.*



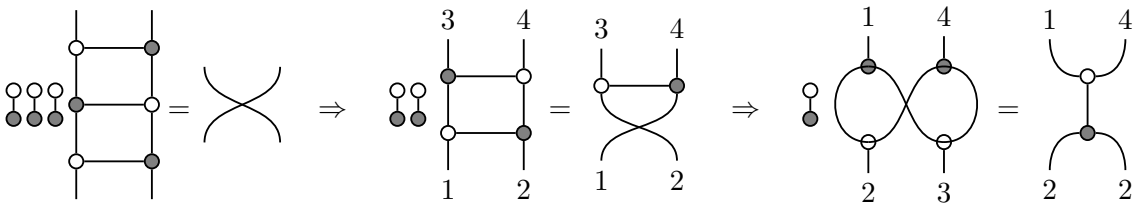
(5.13)

Proof. First, assume strong complementarity. Then:



By naturality of the swap, the scaled bialgebra law (5.8) and Proposition 5.19.

Conversely:



The first implication follows from postcomposing with CNOT and Proposition 5.19. The second implication follows from the Spider Theorem 4.23; for convenience, we have labeled the wires to make the idenfication. The other scaled bialgebra laws follow similarly. □

For the rest of this section, we work in the category **FHilb**, fix $A = \mathbb{C}^2$, let () be defined by the Z basis $\{|0\rangle, |1\rangle\}$, and define () to copy the X basis $\{|+\rangle, |-\rangle\}$.

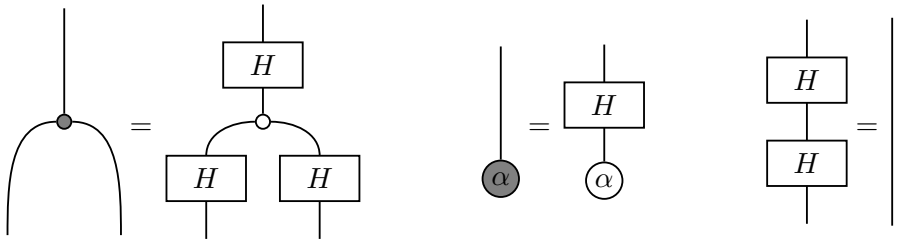
Equation (5.11) now indeed reduces to the CNOT gate.

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{5.14}$$

The relationship between the two classical structures is $|+\rangle = |0\rangle + |1\rangle$, and $|-\rangle = |0\rangle - |1\rangle$. Hence they are transformed into each other by the *Hadamard gate*.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \boxed{H} \tag{5.15}$$

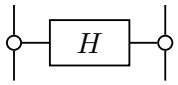
Thus the following equations are satisfied.



(5.16)

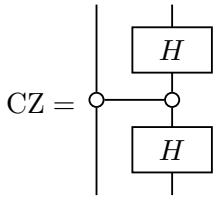
In addition to the CNOT gate, we can now also define the CZ gate abstractly. This gate performs a Z phase shift on the second qubit when the first (control) qubit is $|1\rangle$, and leaves it alone when the first qubit is $|0\rangle$.

Lemma 5.21. *The CZ gate can be defined as follows.*



(5.17)

Proof. We can rewrite equation (5.17) as follows.



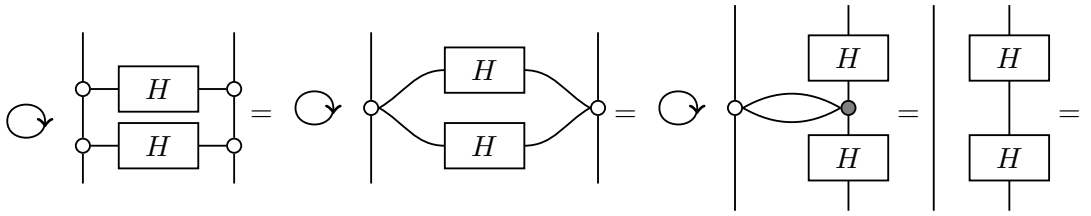
Hence

$$\mathrm{CZ} = (\mathrm{id} \otimes H) \circ \mathrm{CNOT} \circ (\mathrm{id} \otimes H) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

This is indeed the controlled Z gate. □

Proposition 5.22. $2 \bullet CZ \circ CZ = \mathrm{id}$.

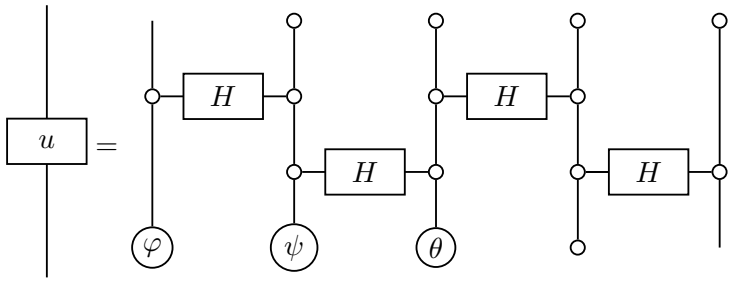
Proof.



□

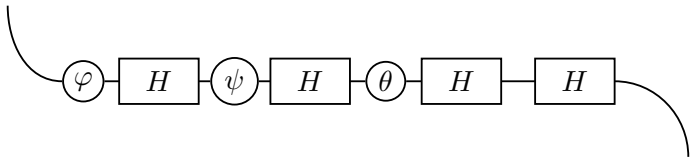
Qubits have the nice property that any unitary on them can be implemented via its *Euler angles*. More precisely: for any unitary $\mathbb{C}^2 \xrightarrow{u} \mathbb{C}^2$, there exist phases φ, ψ, θ such that $u = Z_\theta \circ X_\psi \circ Z_\varphi$. Therefore we can implement such unitaries abstractly using just CZ-gates and Hadamard gates.

Theorem 5.23. *If a unitary* $\mathbb{C}^2 \xrightarrow{u} \mathbb{C}^2$ *in* **FHilb** *has Euler angles* φ, ψ, θ*, then:*

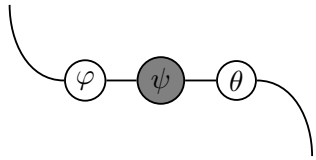


(5.18)

Proof. By using the Generalized Spider Theorem 4.26 equation (5.18) reduces to



But by equation (5.16), this is just:



which equals u, by definition of the Euler angles. □

5.5 Exercises

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 [67]. Its mathematical formulation in terms of mutually unbiased bases is due to Schwinger in 1960 [68]. The abstract formulation in terms of classical structures we used was first given by Coecke and Duncan in 2008 [19]. Strong complementarity was first discussed in that article, and the ensuing Theorem 5.18 is due to Coecke, Duncan, Kissinger and Wang in 2012 [20].

The applications in Section 5.4 are basic properties in quantum computation [58], and are especially important to measurement based quantum computing [65]. See [30] for more abstract results on Euler angles.

Bialgebras and Hopf algebras are the starting point for the theory of quantum groups [45, 75]. They have been around in algebraic form since the 1960s, when Heinz Hopf first studied them [38]. Graphical notation for them is becoming more standard now, with so-called Sweedler notation as a middle ground [15].

Chapter 6

Copying and deleting

Our running examples of compact categories involved tensor products rather than products or direct sums. This chapter shows there is a good reason for doing so: categorical products might give a perfectly good example of a monoidal category, but they cannot give examples of compact categories except in degenerate cases.

This sets "classical" categories like **Set** apart from more "quantum" categories like **Rel** and **Hilb**. To see the difference between, for example, **Set** and **Rel**, we have to think about classical and quantum information. Recall the famous *no-cloning theorem*, and its slightly less well-known sibling the *no-deleting theorem*. They show that quantum information is distinguished by the fact that it cannot be copied or deleted. Conversely, we will show that tensor products equipped with uniform copying and deleting operators are (categorical) products. But before we go into these matters, we have to review the issue of *closure*.

6.1 Closure

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 **Vect**, addition of matrices yields a new matrix.

Indeed, the monoidal category **Vect** is able to handle "higher order"

morphisms. Namely, if V and W are vector spaces, then the set

$$W^V = \{f \colon V \to W \mid f \text{ linear}\} \tag{6.1}$$

is again a vector space, with pointwise operations such as $(f+g)(x) = f(x) + g(x)$. (In fact, this is the homset $\mathbf{Vect}(V, W)$ itself!) Thus we can talk about transformations of morphisms as being just ordinary morphisms by encoding morphisms as vectors in function spaces.

The vector space W^V comes with nice property we might expect from such a function space. If we have $f \in W^V$ and $x \in V$, then there is $f(x) \in W$. Moreover, this assignment is linear in both f and x. In other words, there is a bilinear function $V \times W^V \to W$ given by $(f, x) \mapsto f(x)$. Hence, there is an *evaluation* map $\mathrm{ev} \colon V \otimes W^V \to W$. Objects that stand in such a relation to the tensor product are called *exponentials* in general.

Definition 6.1 (Exponential)**.** Let A and B be objects in a symmetric monoidal category. Their *exponential* is an object B^A together with a map $\mathrm{ev} \colon A \otimes B^A \to B$ such that every morphism $f \colon A \otimes X \to B$ allows a unique morphism $h \colon X \to B^A$ with $f = \mathrm{ev} \circ (\mathrm{id}_A \otimes h)$.

$$\begin{array}{ccc} A \otimes X & \xrightarrow{\quad f \quad} & B \\ & \searrow^{\mathrm{id}_A \otimes h} & \uparrow \mathrm{ev} \\ & & A \otimes B^A \end{array} \tag{6.2}$$

The category is called *closed* when every pair of objects has an exponential.

For the monoidal category **Hilb**, equation (6.1) does not obviously give a well-defined object: what would the inner product be? Indeed, **Hilb** is not closed. In finite dimension, however, we can take the so-called *Hilbert-Schmidt inner product* $\langle f | g \rangle = \mathrm{Tr}(f^\dagger \circ g)$. In general, objects that have duals always have exponentials!

Lemma 6.2. *If an object A in a symmetric monoidal category has a dual A^*, and B is any object, then $B^A := A^* \otimes B$ is an exponential.*

Proof. Define the evaluation map by

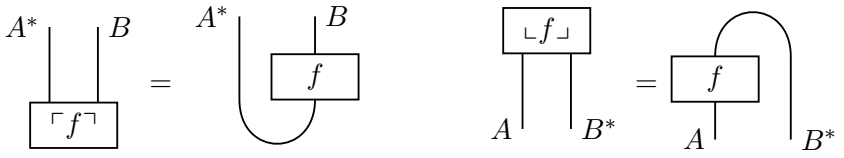
$$\mathrm{ev} = \lambda_B \circ (\eta_A \otimes \mathrm{id}_B) \circ \alpha_{A,A^*,B} \colon A \otimes (A^* \otimes B) \to B.$$

It is now trivial to check equation (6.2). □

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. According to our definitions, the previous lemma says that compact categories are always closed. Regardless, compact categories are sometimes also called compact closed categories.

Taking $B = I$ in Lemma 6.2 gives an especially nice setting. We can encode morphisms as states in this way. We repeat the definition of names and conames from Definition 3.3.

Definition 6.3 (Name, coname)**.** The *name* of a morphism $f\colon A \to B$ 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 $\llcorner f \lrcorner = \varepsilon_B \circ (f \otimes \mathrm{id}_{B^*})\colon A \otimes B^* \to I$.



(6.3)

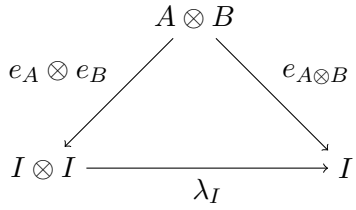
This is also called *map-state duality* or the *Choi-Jamiołkowski isomorphism*. With this preparation, we can get back to thinking about copying and deleting.

6.2 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.

Definition 6.4 (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:



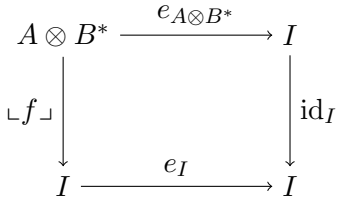
(6.4)

We now show that uniform deleting has significant effects in a compact category.

Definition 6.5 (Preorder)**.** A *preorder* is a category that has at most one morphism $A \to B$ for any pair of objects A, B.

Theorem 6.6 (Deleting collapse)**.** *If a compact category has uniform deleting, then it must be a preorder.*

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



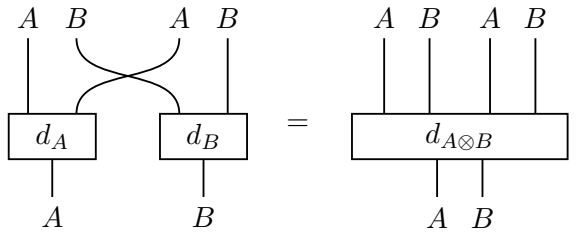
(6.5)

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 $f = g$. □

6.3 Uniform copying

We now move to uniform copying. The comultiplication $A \xrightarrow{d} A \otimes A$ of a comonoid lets us copy the information contained in one object A. What happens if we have this ability for all objects, systematically?

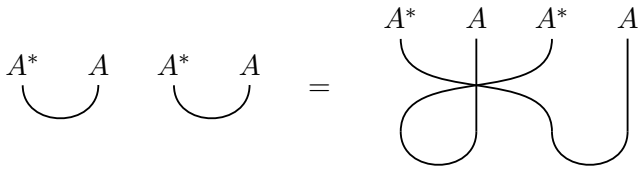
Definition 6.7 (Uniform copying)**.** A symmetric monoidal category has *uniform copying* if there is a natural transformation $A \xrightarrow{d_A} A \otimes A$ with $d_I = \rho_I$, satisfying equations (4.2) and (4.3), and making the following diagram commute for all objects A, B.



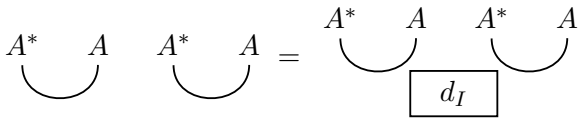
(6.6)

This turns out to be a drastic restriction on the category, as we will see in the Copying collapse theorem below. First we need some preparatory lemmas.

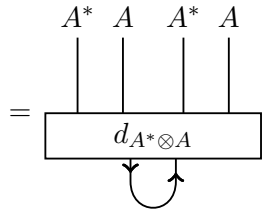
Lemma 6.8. *If a compact category has uniform copying, then*



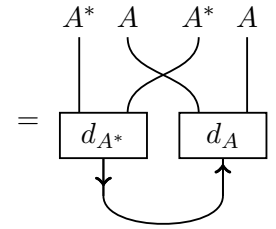
Proof. First, consider the following equalities.



(because $d_I = \rho_I$)

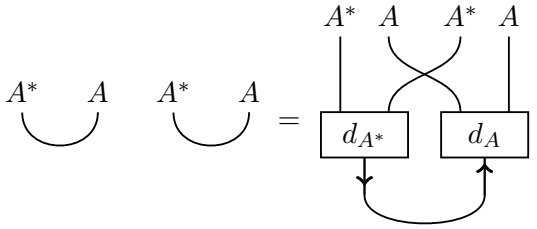


(by naturality of d)

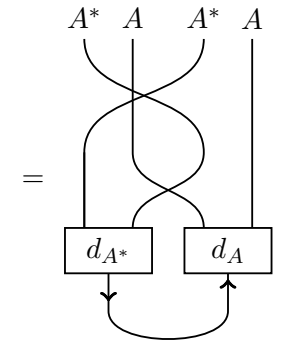


(by equation (6.6))

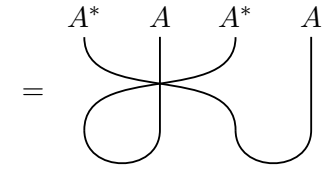
Let's temporarily call this equation $(*)$. Then:



(by equation $(*)$)



(by equation (4.2))

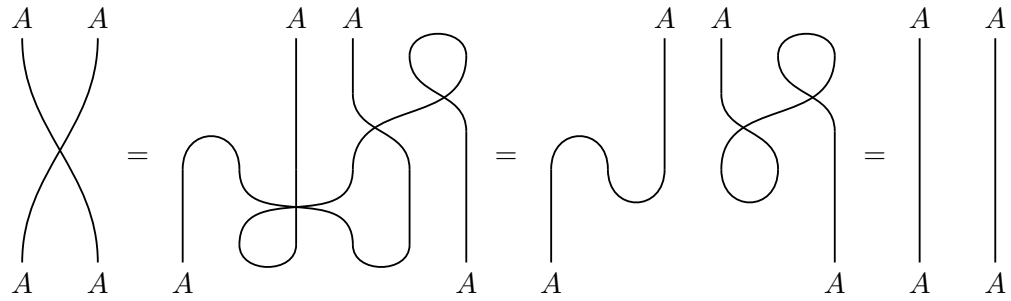


(by equation $(*)$)

□

Lemma 6.9. *If a compact category has uniform copying, then* $\sigma_{A,A} = \mathrm{id}_{A\otimes A}$.

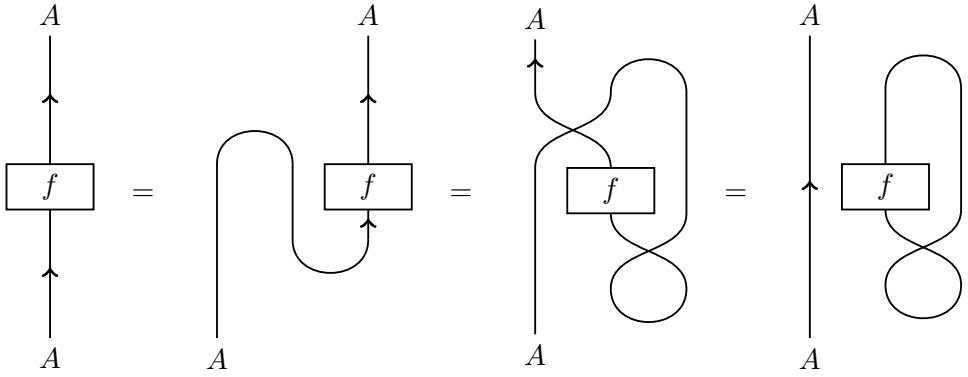
Proof.



The middle equation is Lemma 6.8, and the outer equations are standard operations in a symmetric monoidal category. □

Theorem 6.10 (Copying collapse)**.** *If a compact category has uniform copying, then every endomorphism is a scalar multiple of the identity. In fact,* $f = \mathrm{Tr}(f) \bullet \mathrm{id}_A$ *for any* $A \xrightarrow{f} A$.

Proof.



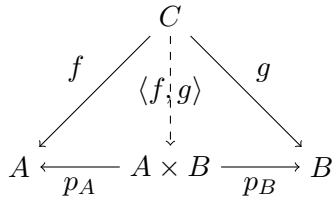
The middle equality follows from naturality of σ. The last equality uses Lemma 6.9. □

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.

6.4 Products

Let's forget about compact structure for this section. What happens when a symmetric monoidal category has 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. First recall what products are.

Definition 6.11 (Products)**.** A *product* of two objects A, B in a category 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 every diagram as below has a unique morphism $\langle f, g \rangle$ making both triangles commute.



(6.7)

An object I is *terminal* when there is a unique morphism $A \xrightarrow{!_A} I$ for every object A. A category that has a terminal object and products for all pairs of objects is called *cartesian*.

For an example, let's temporarily go back to the compact case. There, uniform deleting implies that I is terminal. But in general, I being terminal is strictly stronger than uniform deleting.

Lemma 6.12. *Let* $\mathbf{C}$ *be a monoidal category.*

1. *If the tensor unit* I *is terminal, then* $\mathbf{C}$ *has uniform deleting.*
2. *If* $\mathbf{C}$ *is compact and has uniform deleting, then its tensor unit* I *is terminal.*

Proof. If I is terminal, we can define $!_A = e_A \colon A \to I$. This will automatically satisfy naturality as well as equation (6.4). For the second part, notice that any object A has at least one morphism $A \to I$, namely e_A. By the deleting collapse theorem 6.6, this must be the only morphism of that type. □

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.

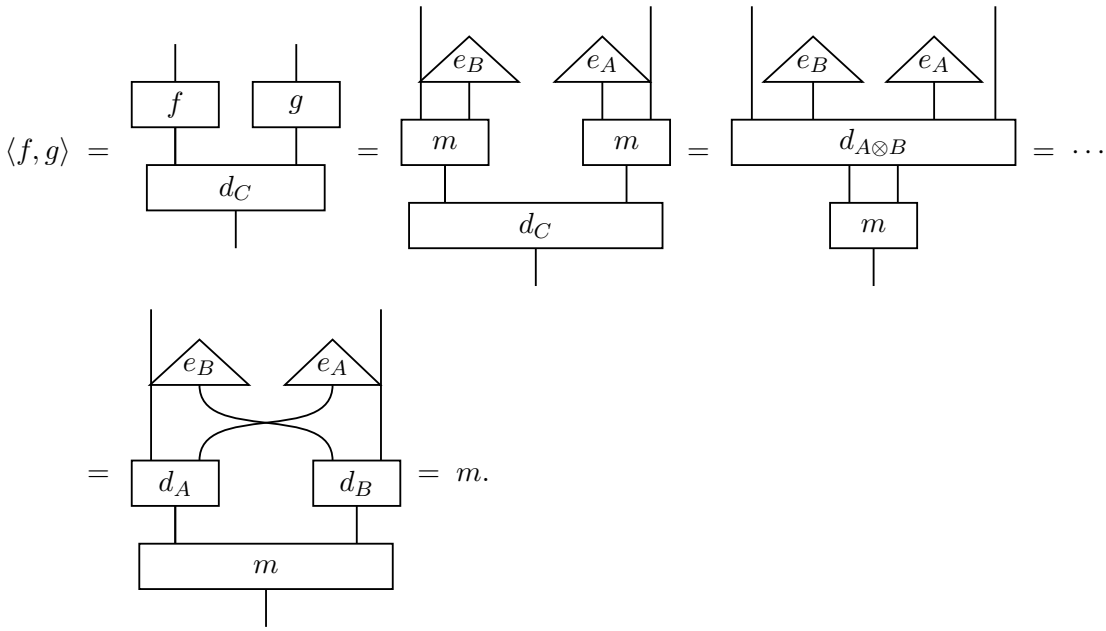
Theorem 6.13. *The following are equivalent for a symmetric monoidal category:*

- *it is Cartesian; more precisely, tensor products are products;*
- *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 $e_A = !_A$ and $d_A = \langle \mathrm{id}_A, \mathrm{id}_A \rangle$ provide uniform copying and deleting operators that moreover satisfy (4.4). Moreover, I is by definition terminal.

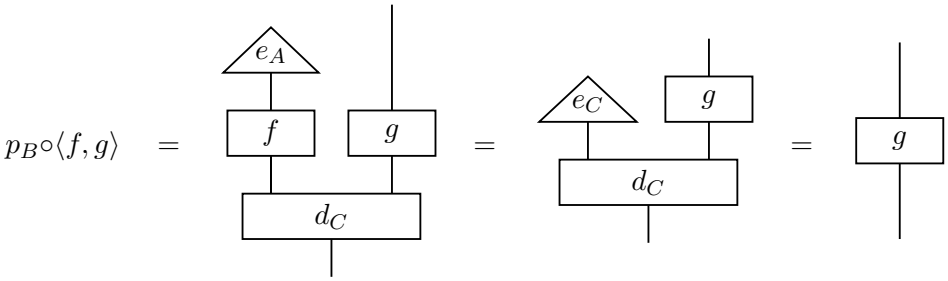
For the converse, we need to prove that $A \otimes B$ is a product of A and B. Define $p_A = \rho_A \circ (\mathrm{id}_A \otimes !_B) \colon A \otimes B \to A$ and $p_B = \lambda_B \circ (!_A \otimes \mathrm{id}_B) \colon A \otimes B \to I$. For given $C \xrightarrow{f} A$ and $C \xrightarrow{g} B$, define $\langle f, g \rangle = (f \otimes g) \circ d$.

First, suppose $C \xrightarrow{m} A \otimes B$ satisfies $p_A \circ m = f$ and $p_B \circ m = g$; we show that $m = \langle f, g \rangle$.



The second equality is our assumption, the third equality is naturality of d, the fourth equality is equation (6.6), and the last equality follows from equation (4.4). Hence mediating morphisms, if they exist, are unique: they all equal $\langle f, g \rangle$.

Finally, we show that $\langle f, g \rangle$ indeed satisfies (6.7).



The first equality holds by definition, the second equality is naturality of e, and the last equality is equation (4.4). Similarly $p_A \circ \langle f, g \rangle = f$. □

6.5 Exercises

Notes and further reading

The no-cloning theorem was proved in 1982 independently by Wootters and Zurek, and Dieks [77, 28]. The categorical version we presented here is due to Abramsky in 2010 [3]. The no-deleting theorem we presented is due to Coecke and was also published in that paper.

Theorem 6.13 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 [40]. It should be mentioned here that, in compact categories, products are automatically biproducts, which was proved by Houston in 2008 [39].

The notion of closure of monoidal categories is the starting point for a large area called *enriched* category theory [47]. Exponentials also play an important role in categorical logic, namely that of implications between logical formulae.

Chapter 7

Complete positivity

In Chapter 6 we have seen that the kind of categories we consider 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, for example, has no copying either. What really sets quantum mechanics apart is the fact that uniform broadcasting is impossible. 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. As a result, we show that broadcasting is impossible, finishing our categorical setup capturing quantum mechanics.

The key point is that in quantum mechanics, we often do not know precisely what pure state a system is in, but we do know that it is in one of several pure states with certain probability. This leads to general states being convex sums of pure states, which can conveniently be captured using *density matrices* — positive matrices with unit trace. We will not concern ourselves with the trace condition. Recall that unlike superposition, which is inherent to the physical system, these probabilities only represent our own (lack of) knowledge about the system.

7.1 Complete positivity

We have defined *states* as morphisms $I \xrightarrow{\psi} A$. Such a state is *normal* when $\psi^\dagger \circ \psi = \mathrm{id}_I$. In the category **Hilb**, normal states thus correspond to normal vectors, i.e. vectors ψ on the unit sphere, i.e. $\|\psi\| = 1$. However, in this chapter it will be more convenient to think of the rank 1 map $\psi \circ \psi^\dagger \colon A \to A$ induced by a (pure) state.

Definition 7.1 (Pure state)**.** A *pure state* of an object A is a morphism $A \to A$ of the form $\psi \circ \psi^\dagger$ for a morphism $\psi \colon I \to A$ with $\psi^\dagger \circ \psi = \mathrm{id}_I$.

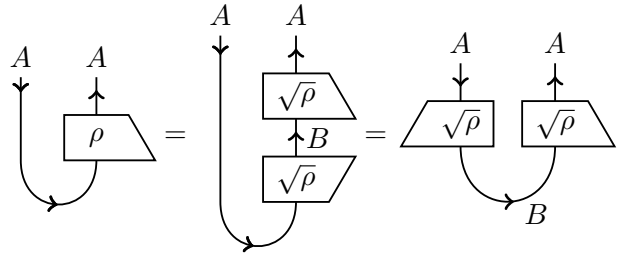
Hence pure states are by definition positive maps. Then, abstracting from the category **Hilb**, general states, also called mixed states, are convex sums of pure states.

Definition 7.2 (Mixed state)**.** A *mixed state* of an object A is a positive morphism $A \xrightarrow{\rho} A$.

When working in compact categories, instead of morphisms $A \to B$, we can equivalently work with matrices $I \to A^* \otimes B$ by taking names (see Definition 3.3).

Definition 7.3 (Positive matrix)**.** A *positive matrix* is a morphism $I \xrightarrow{\ulcorner \rho \urcorner} A^* \otimes A$ that is the name of a positive morphism $A \xrightarrow{\rho} A$.

Graphically, positive matrices are morphisms of the following form.

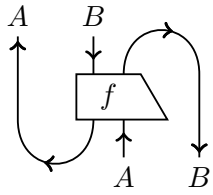


(7.1)

The morphism $\sqrt{\rho}$ and the object B are by no means unique.

Next, we of course want processes to send (mixed) states to (mixed) states. In other words, we are only interested in morphisms $A^* \otimes A \to B^* \otimes B$ that preserve positive matrices. Once again taking our cue from the situation in **FHilb**, these turn out to be the following sort of morphisms.

Definition 7.4 (Completely positive morphism)**.** A morphism $A^* \otimes A \xrightarrow{f} B^* \otimes B$ is *completely positive* when the following morphism $A \otimes B \to A \otimes B$ is positive.

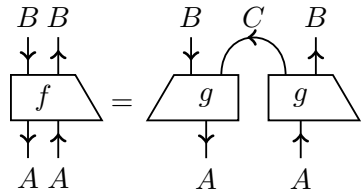


(7.2)

This definition looks fairly abstract, so let's unpack it.

Theorem 7.5 (Stinespring Dilation Theorem)**.** *The following are equivalent:*

1. $A^* \otimes A \xrightarrow{f} B^* \otimes B$ *is completely positive;*
2. *there is an object* C *and a morphism* $A \xrightarrow{g} C \otimes B$ *making the following equation true.*



(7.3)

Given a completely positive map f as in the previous theorem, the morphism g is called its *Kraus morphism*, and the object C is an *ancilla* of f. These are not unique.

7.2 The CP construction

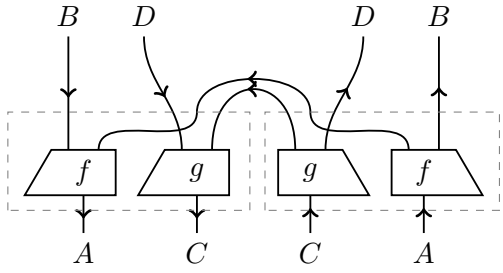
We will now see that completely positive morphisms behave well under our categorical operations, and hence form a well-behaved category in their own right. Thus we will assign to any dagger compact category $\mathbf{C}$ a new one called $\mathrm{CP}(\mathbf{C})$.

Lemma 7.6 (CP respects structure)**.** *In a dagger compact category:*

(i) the identity map $A^* \otimes A \xrightarrow{\mathrm{id}} A^* \otimes A$ *is completely positive;*

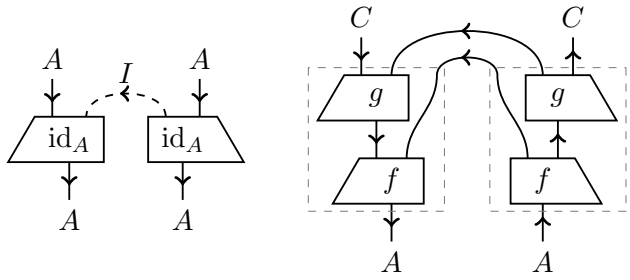
(ii) *if* $A^* \otimes A \xrightarrow{f} B^* \otimes B$ *and* $B^* \otimes B \xrightarrow{g} C^* \otimes C$ *are completely positive, then so is* $A^* \otimes A \xrightarrow{g \circ f} C^* \otimes C$*;*

(iii) *if* $A^* \otimes A \xrightarrow{f} B^* \otimes B$ *and* $C^* \otimes C \xrightarrow{g} D^* \otimes D$ *are completely positive, then so is*



(7.4)

Proof. This is obvious from the graphical calculus and Theorem 7.5.



□

Definition 7.7 (The CP construction)**.** Given a dagger compact category $\mathbf{C}$, we define a new category $\mathrm{CP}(\mathbf{C})$. Its objects are the same as those of $\mathbf{C}$. A morphism $A \to B$ in $\mathrm{CP}(\mathbf{C})$ is a completely positive morphism $A^* \otimes A \xrightarrow{f} B^* \otimes B$ in $\mathbf{C}$. Composition and identities in $\mathrm{CP}(\mathbf{C})$ are as in $\mathbf{C}$.

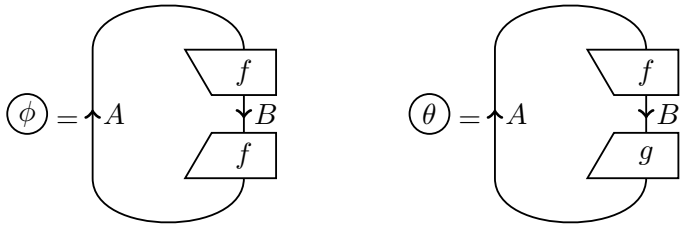
Notice that $\mathrm{CP}(\mathbf{C})$ is indeed a well-defined category by Lemma 7.6.

Lemma 7.8 (CP kills phases)**.** *Let* $\mathbf{C}$ *be a dagger compact category.*

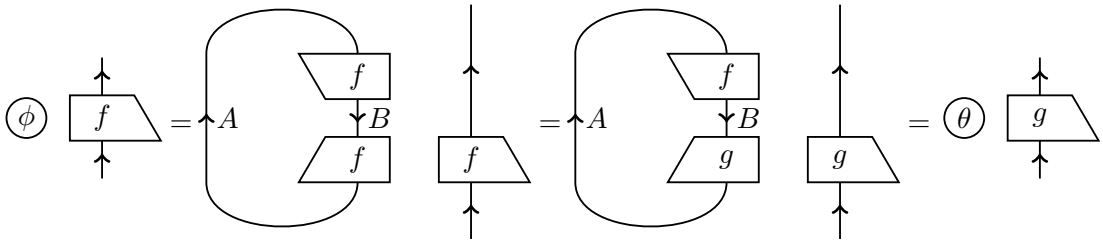
(i) *There is a functor* $F \colon \mathbf{C} \to \mathrm{CP}(\mathbf{C})$*, defined by* $F(A) = A^* \otimes A$ *and* $F(f) = f_* \otimes f$*.*

(ii) The functor F is faithful up to global phases. More precisely: if $F(f) = F(g)$ for $A \xrightarrow{f,g} B$, then there are scalars $I \xrightarrow{\phi,\theta} I$ with $\phi \bullet f = \theta \bullet g$ and $\phi^\dagger \bullet \phi = \theta^\dagger \bullet \theta$.

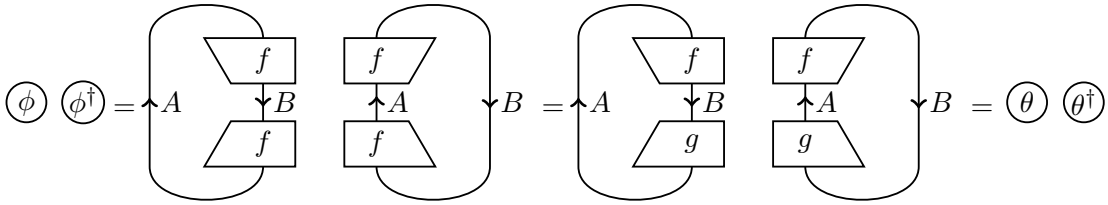
Proof. Part (i) is clear. Let f, g as in part (ii) be given. Define



Then:



And:

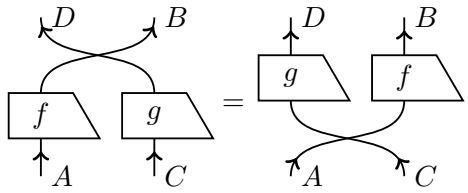


This proof is completely graphical and does not depend on anything like angles. □

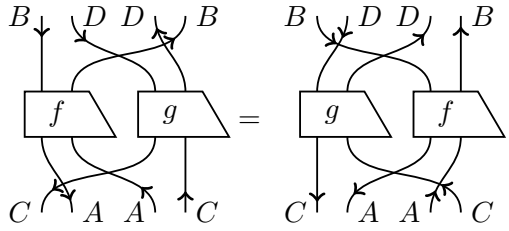
In fact, CP(**C**) is not just a category, but again a dagger compact category. The dagger in CP(**C**) can be regarded as the duality between the Heisenberg and Schrödinger pictures.

Theorem 7.9 (CP is dagger compact)**.** *If* $\mathbf{C}$ *is a dagger compact category, so is* $\mathrm{CP}(\mathbf{C})$.

Proof. The proof consists of verifying a lot of equations, but the graphical calculus makes them all easy. See Table 7.1 for a dictionary. We check one equation as an example: naturality of σ. To prove that



holds in $\mathrm{CP}(\mathbf{C})$, we must prove the following equation in $\mathbf{C}$.



But this is clearly satisfied. □

Question. What would go wrong if we insisted that morphisms in $\mathrm{CP}(\mathbf{C})$ preserve trace?

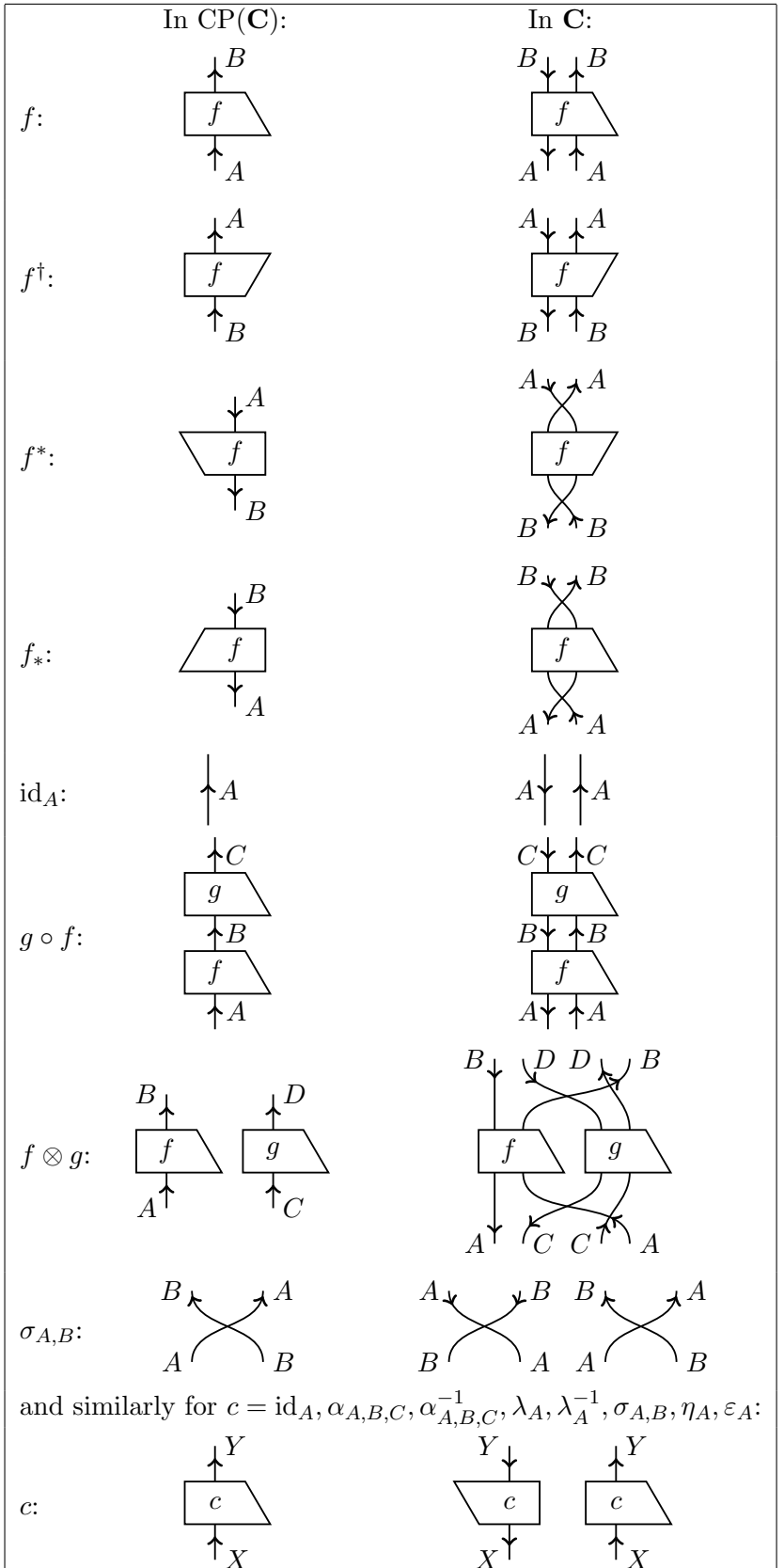
Examples

By spelling out the definition, we see that a morphism $X \times X \xrightarrow{R} Y \times Y$ in **Rel** is completely positive when the following two properties hold for all $x, x' \in X$ and $y, y' \in Y$:

$$(x', x)R(y', y) \iff (x, x')R(y, y'), \tag{7.5}$$

$$(x', x)R(y', y) \implies (x, x)R(y, y). \tag{7.6}$$

In the category **Hilb**, we can identify $(\mathbb{C}^n)^* \otimes \mathbb{C}^n$ with the Hilbert space M_n of n-by-n matrices, with inner product $\langle f | g \rangle = \mathrm{Tr}(f^\dagger g)$. By

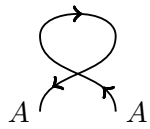

In CP(C):
In C:
f:
f†:
f*:
f*:
id_A:
g ∘ f:
f ⊗ g:
σ_{A,B}:
and similarly for c = id_A, α_{A,B,C}, α^{-1}_{A,B,C}, λ_A, λ^{-1}_A, σ_{A,B}, η_A, ε_A:
c:

Choi's theorem, completely positive morphisms $\mathbb{C}^m \to \mathbb{C}^n$ in **Hilb** are then precisely what are usually called completely positive maps: a linear map $M_m \xrightarrow{T} M_n$ is called *positive* when it preserves positive matrices, and *completely positive* when $M_m \otimes M_k \xrightarrow{T\otimes \mathrm{id}_{M_k}} M_n \otimes M_k$ is positive. The idea behind this usual definition is that not only T should send states to states, but also regarding T as a local operation on a larger system should send states to states. We can now recognize Theorem 7.5 as the Stinespring Dilation Theorem, and the CP construction of Definition 7.7 as lifting that characterization to a definition.

We can regard the ancilla system C as the "amount of probabilistic mixing" inherent in the completely positive morphism f. Indeed, morphisms in image of the functor $\mathbf{C} \to \mathrm{CP}(\mathbf{C})$ have ancilla system I, and hence no mixing at all. In the case of **Hilb**, the minimal dimension of C make this amount more precise.

7.3 Environment structures

In categories of the form $\mathrm{CP}(\mathbf{C})$, any object A allows a morphism $A \xrightarrow{\top_A} I$, namely $A^* \otimes A \xrightarrow{\sigma_{A^*,A}} A \otimes A^* \xrightarrow{\varepsilon_A} I \cong I^* \otimes I$.



(7.7)

We can think of this morphism as *tracing out* the system A: if $I \xrightarrow{\ulcorner\rho\urcorner} A^* \otimes A$ is the matrix of a map $A \xrightarrow{\rho} A$, then $\top_A \circ \ulcorner\rho\urcorner = \mathrm{Tr}(\rho)\colon I \to I$ by Definition 3.23. As it turns out, we can axiomatize whether a given abstract category is of the form $\mathrm{CP}(\mathbf{C})$ in this way.

Definition 7.10 (Environment structure)**.** An *environment structure* for a dagger compact category $\mathbf{C}$ consists of the following data:

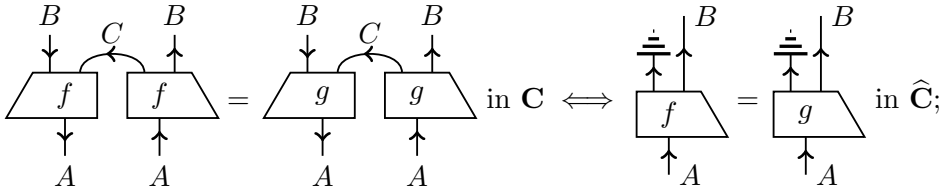
- a dagger compact category $\widehat{\mathbf{C}}$ of which $\mathbf{C}$ is a dagger compact subcategory, that satisfies $\mathrm{Ob}(\widehat{\mathbf{C}}) = \mathrm{Ob}(\mathbf{C})$;
- for each object A, a morphism $A \xrightarrow{\top_A} I$, depicted as  ;

satisfying the following properties:

(i) $\top_I = \mathrm{id}_I$ and $\top_{A\otimes B} = (\top_A \otimes \top_B) \circ \lambda_I$;

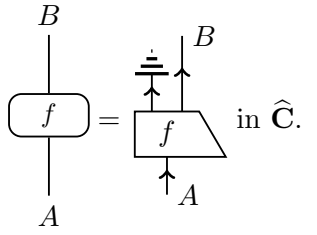
(7.8)

(ii) for all $A \xrightarrow{f,g} C \otimes B$ in $\mathbf{C}$:



(7.9)

(iii) for each $A \xrightarrow{\widehat{f}} B$ in $\widehat{\mathbf{C}}$ there is $A \xrightarrow{f} C \otimes B$ such that



(7.10)

Morphisms in $\widehat{\mathbf{C}}$ are depicted with round corners.

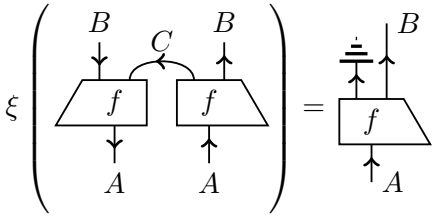
Intuitively, we think of $\mathbf{C}$ as consisting of pure states, and the supercategory $\widehat{\mathbf{C}}$ of containing mixed states. Condition (7.10) then reads that every mixed state can be regarded as a pure state in an extended system. The idea behind the ground symbol is that the ancilla system becomes the 'environment', into which our system is plugged.

Starting with a dagger compact category $\mathbf{C}$, write $\mathbf{D}$ for the image of the functor $\mathbf{C} \to \mathrm{CP}(\mathbf{C}$. Explicitly, $\mathbf{D}$ is the subcategory of $\mathrm{CP}(\mathbf{C})$ whose morphisms can be written with ancilla I. (Don't forget that $\mathbf{C} \to \mathrm{CP}(\mathbf{C})$

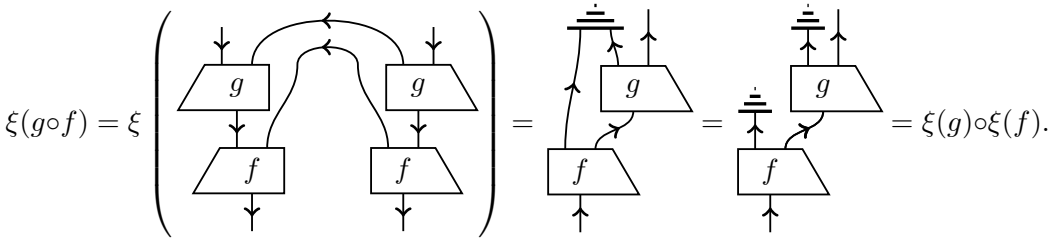
is not faithful, see Lemma 7.8!) This category $\mathbf{D}$ is clearly dagger compact again. Then $\mathbf{D}$ has an environment structure with $\widehat{\mathbf{D}} = \mathrm{CP}(\mathbf{C})$, and $\top_A$ given by (7.7). Conversely, having an environment structure is essentially the same as working with a category of completely positive morphisms, as the following theorem shows.

Theorem 7.11. *If a dagger compact category $\mathbf{C}$ comes with an environment structure, then there is an invertible functor $\xi\colon \mathrm{CP}(\mathbf{C}) \to \widehat{\mathbf{C}}$ that satisfies $\xi(A) = A$ on objects and $\xi(f \otimes g) = \xi(f) \otimes \xi(g)$ on morphisms.*

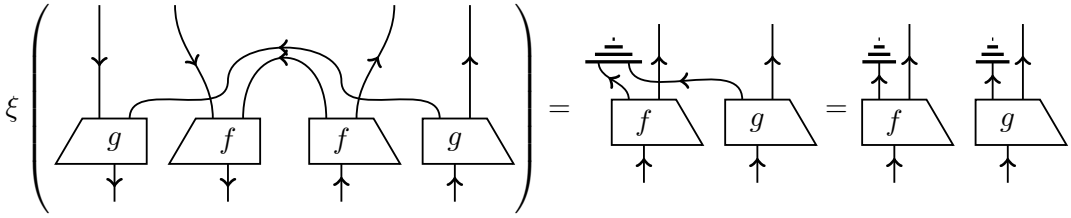
Proof. Define ξ by $\xi(A) = A$ on objects, and as follows on morphisms.



This is indeed functorial by (7.8):



It is obvious that the functor ξ is invertible: (7.9) shows that it faithful, and (7.10) shows that it is full. Finally, by (7.8):



So $\xi(f \otimes g) = \xi(f) \otimes \xi(g)$. □

Environment structures give us a convenient way to graphically handle categories of completely positive maps, because we do not have to "double" the pictures all the time.

7.4 Exercises

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 [74]. Quantum information theory could be said to have grown out of operator algebra theory, and repurposed completely positive maps. See also the textbooks [60, 13].

The CP construction is due to Selinger in 2007 [70]. 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 [22].

Environment structures are due to Coecke [17, 23].

Bibliography

[1] Lowell Abrams. *Frobenius algebra structures in topological quantum field theory and quantum cohomology.* PhD thesis, Johns Hopkins University, 1997.

[2] Samson Abramsky. Abstract scalars, loops, and free traced and strongly compact closed categories. In *Algebra and Coalgebra in Computer Science*, CALCO'05, pages 1–30. Springer, 2005.

[3] Samson Abramsky. No-cloning in categorical quantum mechanics. In Simon Gay and Ian Mackey, editors, *Semantic Techniques in Quantum Computation*, pages 1–28. Cambridge University Press, 2010.

[4] Samson Abramsky and Bob Coecke. A categorical semantics of quantum protocols. In *Logic in Computer Science 19*, pages 415–425. IEEE Computer Society, 2004.

[5] Samson Abramsky and Bob Coecke. Abstract physical traces. *Theory and Applications of Categories*, 14(6):111–124, 2005.

[6] Samson Abramsky and Chris Heunen. H*-algebras and nonunital Frobenius algebras: first steps in infinite-dimensional categorical quantum mechanics. *Clifford Lectures, AMS Proceedings of Symposia in Applied Mathematics*, 71:1–24, 2011.

[7] Steve Awodey. *Category Theory.* Oxford Logic Guides. Oxford University Press, 2006.

[8] John Baez and James Dolan. Higher-dimensional algebra and topological quantum field theory. *Journal of Mathematical Physics*, 36:6073–6105, 1995.

[9] John C Baez. *Structural Foundations of Quantum Gravity*, chapter Quantum Quandries: A Category-Theoretic Perspective, pages 240–265. Oxford University Press, 2006.

[10] Michael Barr. **-autonomous categories*, volume 752 of *Lecture Notes in Mathematics*. Springer, 1979.

[11] Jean Bénabou. Categories avec multiplication. *Comptes Rendus de l'Acadmie des Sciences. Série I. Mathmatique*, pages 1887–1890, 1963.

[12] Charles H. Bennett, Giles Brassard, Claue Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895–1899, 1993.

[13] Rejandra Bhatia. *Positive definite matrices*. Princeton University Press, 2007.

[14] Francis Borceux. *Handbook of Categorical Algebra*. Encyclopedia of Mathematics and its Applications 50–52. Cambridge University Press, 1994.

[15] Stephen U. Chase and Moss Sweedler. *Hopf algebras and Galois theory*. Number 97 in Lecture Notes in Mathematics. Springer, 1969.

[16] Bob Coecke. The logic of entanglement: An invitation. Technical report, University of Oxford, 2003. Computing Laboratory Research Report PRG-RR-03-12.

[17] Bob Coecke. De-linearizing linearity: projective quantum axiomatics from strong compact closure. In Peter Selinger, editor, *QPL 5*, volume 170 of *Electronic Notes in Theoretical Computer Science*, pages 49–72, 2007.

[18] Bob Coecke, editor. *New structures for physics*. Number 813 in Lecture Notes in Physics. Springer, 2011.

[19] Bob Coecke and Ross Duncan. Interacting quantum observables. In *International Colloquium on Automata, Languages and Programming*, volume 5126 of *Lecture Notes in Computer Science*, pages 298–310. Springer, 2008.

[20] Bob Coecke, Ross Duncan, Aleks Kissinger, and Quanlong Wang. Strong complementarity and non-locality in categorical quantum mechanics. *to appear*, 2012.

[21] Bob Coecke, Bill Edwards, and Robert W. Spekkens. Phase groups and the origin of non-locality for qubits. In Bob Coecke, Prakash Panangaden, and Peter Selinger, editors, *QPL 9*, volume 270 of *Electronic Notes in Theoretical Computer Science*, pages 15–36, 2011.

[22] Bob Coecke and Chris Heunen. Pictures of complete positivity in arbitrary dimension. *Electronic Proceedings in Theoretical Computer Science*, 95:27–35, 2011.

[23] Bob Coecke, Éric O. Paquette, and Simon Perdrix. Bases in diagrammatic quantum protocols. In *Mathematical Foundations of Programming Semantics 24*, volume 218 of *Electronic Notes in Theoretical Computer Science*, pages 131–152. Elsevier, 2008.

[24] Bob Coecke and Duško Pavlović. Quantum measurements without sums. In *Mathematics of Quantum Computing and Technology*. Taylor and Francis, 2007.

[25] Bob Coecke, Duško Pavlović, and Jamie Vicary. A new description of orthogonal bases. *Mathematical Structures in Computer Science*, 2009.

[26] Valerie Coffman, Joydip Kundu, and William K. Wootters. Distributed entanglement. *Physical Review A*, 61:052306, 2000.

[27] Brian J. Day. Note on compact closed categories. *Journal of the Australian Mathematical Society*, Series A 24(3):309–311, 1977.

[28] Dennis Dieks. Communication by EPR devices. *Physics Letters A*, 92(6):271–272, 1982.

[29] Robbert Dijkgraaf. *A geometric approach to two dimensional conformal field theory*. PhD thesis, University of Utrecht, 1989.

[30] Ross Duncan and Simon Perdrix. Graph states and the necessity of euler decomposition. In Klaus Ambos-Spies, Benedikt Löwe, and

Wolfgang Merkle, editors, *Computability in Europe*, volume 5635 of *Lecture Notes in Computer Science*, pages 167–177. Springer, 2009.

[31] Bill Edwards. *Non-locality in categorical quantum mechanics*. PhD thesis, Oxford University, 2009.

[32] Peter Freyd. *Abelian Categories: An introduction to the theory of functor*. Harper and Row, 1964.

[33] F. Georg Frobenius. Theorie der hyperkomplexen grössen. *Sitzungsberichte der Koniglich Preussischen Akademie Der Wissenschaften*, 24:504–537; 634–645, 1903.

[34] Alexandre Grothendieck. Pursuing stacks. *Documents Mathématiques, Société Mathétique de France*, 1983. Letter to Daniel Quillen.

[35] Masahito Hasegawa. On traced monoidal closed categories. *Mathematical Structures in Computer Science*, 19:217–244, 2008.

[36] Chris Heunen. An embedding theorem for Hilbert categories. *Theory and Applications of Categories*, 22(13):321–344, 2009.

[37] Chris Heunen, Ivan Contreras, and Alberto S. Cattaneo. Relative Frobenius algebras are groupoids. *Journal of Pure and Applied Algebra*, 217:114–124, 2012.

[38] Heinz Hopf. Über die Topologie der Gruppen-Mannigfaltigkeiten und ihrer Verallgemeinerungen. *Annals of Mathematics*, 42:22–52, 1941.

[39] Robin Houston. Finite products are biproducts in a compact closed category. *Journal of Pure and Applied Algebra*, 212(2):394–400, 2008.

[40] Bart Jacobs. Semantics of weakening and contraction. *Annals of Pure and Applied Logic*, 69:73–106, 1994.

[41] André Joyal and Ross Street. The geometry of tensor calculus I. *Advances in Mathematics*, 88:55–113, 1991.

[42] André Joyal and Ross Street. An introduction to Tannaka duality and quantum groups. In *Category Theory, Part II*, volume 1488 of *Lecture Notes in Mathematics*, pages 411–492. Springer, 1991.

[43] André Joyal and Ross Street. Braided tensor categories. *Advances in Mathematics*, 102:20–78, 1993.

[44] André Joyal, Ross Street, and Dominic Verity. Traced monoidal categories. *Mathematical Proceedings of the Cambridge Philosophical Society*, 3(447–468), 1996.

[45] Christian Kassel. *Quantum Groups*. Springer, 1995.

[46] G. Max Kelly. Many variable functorial calculus (I). In *Coherence in Categories*, volume 281 of *Lecture Notes in Mathematics*, pages 66–105. Springer, 1970.

[47] G. Max Kelly. *Basic Concepts of Enriched Category Theory*. Cambridge University Press, 1982.

[48] G. Max Kelly and Miguel L. Laplaza. Coherence for compact closed categories. *Journal of Pure and Applied Algebra*, 19:193–213, 1980.

[49] Joachim Kock. *Frobenius algebras and 2-D Topological Quantum Field Theories*. Number 59 in London Mathematical Society Student Texts. Cambridge University Press, 2003.

[50] F. William Lawvere. Ordinal sums and equational doctrines. In Beno Eckmann, editor, *Seminar on triples and categorical homology theory*, number 80 in Lecture Notes in Mathematics, pages 141–155, 1967.

[51] Tom Leinster. *Higher operads, higher categories*. Number 298 in London Mathematical Society Lecture Note Series. Cambridge University Press, 2004.

[52] Harald Lindner. Adjunctions in monoidal categories. *Manuscripta Mathematica*, 26:123–139, 1978.

[53] Saunders Mac Lane. Duality for groups. *Bulletin of the American Mathematical Society*, 56(6):485–516, 1950.

[54] Saunders Mac Lane. An algebra of additive relations. *Proceedings of the National Academy of Sciences*, 47:1043–1051, 1961.

[55] Saunders Mac Lane. Natural associativity and commutativity. *Rice University Studies*, 49:28–46, 1963.

[56] Saunders Mac Lane. *Categories for the Working Mathematician*. Springer, 2nd edition, 1971.

[57] Barry Mitchell. *Theory of Categories*. Academic Press, 1965.

[58] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[59] Paul H. Palmquist. Adjoint functors induced by adjoint linear transformations. *Proceedings of the American Mathematical Society*, 44(2):251–254, 1974.

[60] Vern Paulsen. *Completely bounded maps and operators algebras*. Cambridge University Press, 2002.

[61] Duško Pavlović. Quantum and classical structures in nondeterministic computation. In P. Bruza et al., editor, *Third International symposium on Quantum Interaction*, volume 5494 of *Lecture Notes in Artificial Intelligence*, pages 143–157. Springer, 2009.

[62] Roger Penrose. Applications of negative dimensional tensors. In *Combinatorial mathematics and its applications*, pages 221–244, 1971.

[63] Simon Perdrix. State transfer instead of teleportation in measurement-based quantum computation. *International journal of quantum information*, 3(1):219–223, 2005.

[64] Frank Quinn. Lectures on axiomatic topological quantum field theory. In *Geometry and quantum field theory*, pages 323–453. American Mathematical Society, 1995.

[65] Robert Raussendorf and Hans J. Briegel. A one-way quantum computer. *Physical Review Letters*, 86(22):5188, 2001.

[66] Michael Reed and Barry Simon. *Methods of Modern Mathematical Physics I: Functional Analysis*. Academic Press, 1980.

[67] Léon Rosenfeld. *Foundations of Quantum Physics II*, chapter Complementarity: Bedrock of the quantal description, pages 284–285. Number 7 in Niels Bohr, collected works. Elsevier, 1996.

[68] Julian Schwinger. Unitary operator bases. *Proceedings of the National Academy of Sciences: Physics*, 46:570–579, 1960.

[69] Robert A. G. Seely. Linear logic, $*$-autonomous categories and cofree coalgebras. In *Categories in Computer Science and Logic*, volume 92, pages 371–382. American Mathematical Society, 1989.

[70] Peter Selinger. Dagger compact closed categories and completely positive maps. In *Quantum Programming Languages*, volume 170 of *Electronic Notes in Theoretical Computer Science*, pages 139–163. Elsevier, 2007.

[71] Peter Selinger. Idempotents in dagger categories. In *Quantum Programming Languages*, volume 210 of *Electronic Notes in Theoretical Computer Science*, pages 107–122. Elsevier, 2008.

[72] Peter Selinger. A survey of graphical languages for monoidal categories. In *New Structures for Physics*, Lecture Notes in Physics. Springer, 2009.

[73] Peter Selinger. Finite dimensional Hilbert spaces are complete for dagger compact closed categories. *Logical Methods in Computer Science*, 8(3:06):1–12, 2012.

[74] W. Forrest Stinespring. Positive functions on C*-algebras. *Proceedings of the American Mathematical Society*, pages 211–216, 1955.

[75] Ross Street. *Quantum Groups: a path to current algebra*. Number 19 in Australian Mathematical Society Lecture Series. Cambridge University Press, 2007.

[76] Jamie Vicary. Completeness of †-categories and the complex numbers. *Journal of Mathematical Physics*, 52:082104, 2011.

[77] William K. Wootters and Wojciech H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

Index