

Categories and Quantum Informatics: Categorical semantics

Chris Heunen

Spring 2018

A brief introduction to categorical semantics. We focus in particular on the category **Set** of sets and functions, and the category **Rel** of sets and relations, and present a matrix calculus for relations. We introduce the idea of commuting diagrams, and define isomorphisms, groupoids, skeletal categories, opposite categories and product categories. We then define functors, equivalences and natural transformations, and also products and equalizers.

0.1 Semantics

Suppose F and G are two fragments of code, and consider the two computer programs:

$$P = (\text{if } 1 = 1 \text{ then } F \text{ else } F)$$
$$Q = (\text{if } 1 = 1 \text{ then } F \text{ else } G)$$

Are P and Q the same programs or not?

Syntactically, they are clearly different: the code fragment P is different than the code fragment Q . But do P and Q compute the same? The answer depends on how fine-grained you are willing to look. From the perspective of machine *operations*, a (nonoptimising) compiler will make P and Q into different executables, because the machine will be storing G somewhere in memory when executing Q , even though it is dead code that will never be reached, but not so when executing P . But from perspective of the user, P and Q *behave* the same. They give the same output on every input. They *denote* the same algorithm, namely F .

This little analysis we have been doing is called *semantics*. We assigned to the two syntactical fragments P and Q their meaning, in the form of some mathematical objects $\llbracket P \rrbracket$ and $\llbracket Q \rrbracket$. On the first level, *operational semantics*, that mathematical object encoded all implementation details, so that we could retain the difference between the dead code. On the second level, *denotational semantics*, that mathematical object was a set-theoretical function that transforms input into output, and we didn't care how exactly the function performed that computation.

Denotational semantics is used to show that two programs implement 'the same' algorithm. For example, there are many ways to sort an array, but as long as we don't care about how fast the implementation is they all do the same. Quicksort might be faster than bubble sort, but they both sort. In other words, denotational semantics is used to prove that programs meet their specification, that they 'do what they should do'.

The example with P and Q above was insultingly simple, but you can imagine it gets a lot more complicated when for example recursion is in play. The important thing is that the assignment $P \mapsto \llbracket P \rrbracket$ *preserves structure*. For example, if we want to prove something about *concatenating* program fragments, we should have some operation that concatenates their denotations:

$$\llbracket F; G \rrbracket = \llbracket G \rrbracket \circ \llbracket F \rrbracket$$

Similarly, recursion requires us to talk about substitution (calling subprograms with some input) in the syntax, so the semantics had better have some notion of *function space*

$$\llbracket F(X) \rrbracket = \llbracket F \rrbracket(\llbracket X \rrbracket)$$

where $\llbracket \mathbf{F} \rrbracket$ can live. For a third example, if the programming language describes concurrent computation, there should be some sort of *parallel composition* of denotations:

$$\llbracket \mathbf{F} \text{ while } \mathbf{G} \rrbracket = \llbracket \mathbf{F} \rrbracket \otimes \llbracket \mathbf{G} \rrbracket$$

The trick is to choose the mathematical object in which the denotations $\llbracket \mathbf{F} \rrbracket$ live cleverly. It should have the same structure as the programs you're analysing, but abstract away from all the unimportant details, so that powerful mathematical theorems can be used. Popular choices are λ -calculus or partially ordered sets. We will use *categories* as our semantics, which subsumes both.

There is another reason we will use categories. Above we analysed code in an actual programming language. If we consider *quantum* processes, there is no such neat description. The systems are just black boxes that we cannot look inside. But we can still see how the boxes behave; that is precisely the empirical method of physics! Analogously, in computer science, if I give you two executables instead of their source codes, can you still say whether they implement the same algorithm? No, because then you could solve the halting problem.

But you can still analyse the structure of the two computations using denotational semantics. You can see how the *information flows* from input to output and how it is recombined in the process. Categories support this kind of bookkeeping in a beautiful way. As we will see, instead of boring algebra (like in λ -calculus or partially ordered sets), we can manipulate categories graphically completely rigorously, in a way that can even be automated.

In fact, in this way category theory itself becomes a programming language of sorts, where we can click together subroutines in various ways to compose larger programs. In fact, it is unclear what a quantum programming language should look like: if you cannot copy or delete information, you cannot push and pop things on the stack, how do you handle recursion, or even if-then-else statements? Therefore, investigating the categorical semantics first is in a sense the only way to inform the design of a good *quantum programming language*.

0.2 Categories

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

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

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

Here is the definition of a category.

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

- a collection $\text{Ob}(\mathbf{C})$ of *objects*;

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

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

- *associativity*:

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

- *identity*:

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

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

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

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

0.3 The category **Set**

The most basic relationships between sets are given by functions.

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

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

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

Definition 0.3 (Set, FSet). The category **Set** of sets and functions is defined as follows:

- **objects** are sets A, B, C, \dots ;
- **morphisms** are functions f, g, h, \dots ;
- **composition** of $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$ is the function $g \circ f: a \mapsto g(f(a))$; this is the reason the standard notation $g \circ f$ is not in the other order, even though that would be more natural in some equations such as (5);
- **the identity morphism** on A is the function $\text{id}_A: a \mapsto a$.

Define the category **FSet** to be the restriction of **Set** to finite sets.

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



0.4 The category Rel

Relations give a more general notion of process between sets.

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

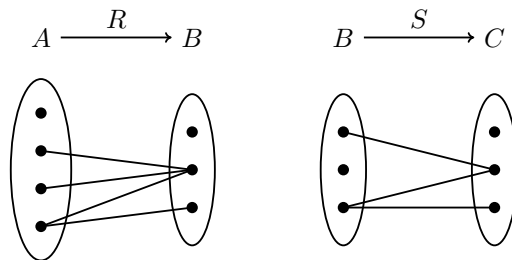
If elements $a \in A$ and $b \in B$ are such that $(a, b) \in R$, then we often indicate this by writing $a R b$, or even $a \sim b$ when R is clear. Since a subset can be defined by giving its elements, we can define our relations by listing the related elements, in the form $a_1 R b_1, a_2 R b_2, a_3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

We can think of a relation $A \xrightarrow{R} B$ in a dynamical way, generalizing (3):

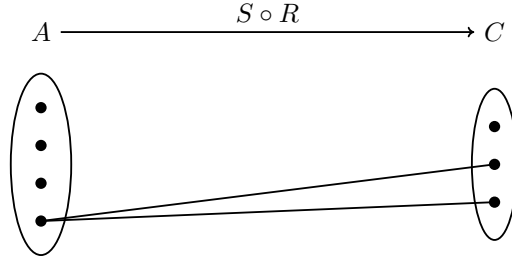


The difference with functions is that this indicates interpreting a relation as a kind of nondeterministic classical process: each element of A can evolve into any element of B to which it is related. Nondeterminism enters here because an element of A can be related to more than one element of B , so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

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



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



This definition of relational composition has the following algebraic form:

$$S \circ R := \{(a, c) \mid \exists b \in B: aRb \text{ and } bSc\} \subseteq A \times C \quad (5)$$

We can write this differently as

$$a(S \circ R)c \Leftrightarrow \bigvee_b (bSc \wedge aRb), \quad (6)$$

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

$$(g \circ f)_{ij} = \sum_k g_{ik} f_{kj} \quad (7)$$

This suggests another way to interpret a relation: as a matrix of truth values. For the example relation (4), this gives the following matrix, where we write 0 for false and 1 for true:

$$A \xrightarrow{R} B \quad \rightsquigarrow \quad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (8)$$

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

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

The intuition we have developed leads to the following definition of the category **Rel**.

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

- **objects** are sets A, B, C, \dots ;
- **morphisms** are relations $R \subseteq A \times B$;

- **composition** of $A \xrightarrow{R} B$ and $B \xrightarrow{S} C$ is the relation

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

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

Define the category **FRel** to be the restriction of **Rel** to finite sets.

While **Set** is a setting for classical physics, and **Hilb** (to be introduced later) is a setting for quantum physics, **Rel** 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.

0.5 Morphisms

It often helps to draw diagrams of morphisms, indicating a way they can be composed. Here is an example:

$$\begin{array}{ccccc}
 A & \xrightarrow{f} & B & \xrightarrow{g} & C \\
 \downarrow h & & \downarrow i & \nearrow j & \\
 D & \xrightarrow{k} & E & &
 \end{array} \tag{9}$$

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

The following terms are very useful when discussing morphisms.

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

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

$$f^{-1} \circ f = \text{id}_A \qquad f \circ f^{-1} = \text{id}_B \tag{10}$$

We then say that A and B are *isomorphic*, and write $A \simeq B$. If only the left equation of (10) holds, f is called *left-invertible*.

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

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

$$g \stackrel{(2)}{=} g \circ \text{id} \stackrel{(10)}{=} g \circ (f \circ g') \stackrel{(1)}{=} (g \circ f) \circ g' \stackrel{(10)}{=} \text{id} \circ g' \stackrel{(2)}{=} g'. \quad \square$$

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

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

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

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

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

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

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

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

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

0.6 Graphical notation

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

$$A \quad \left| \quad \right. \quad (11)$$

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

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

$$\begin{array}{c} B \\ | \\ \boxed{f} \\ | \\ A \end{array} \quad (12)$$

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

$$\begin{array}{c} C \\ | \\ \boxed{g} \\ B \\ | \\ \boxed{f} \\ A \end{array} \quad (13)$$

The identity law $f \circ \text{id}_A = f = \text{id}_B \circ f$ and the associativity law $(h \circ g) \circ f = h \circ (g \circ f)$ then look like:

$$\begin{array}{c}
 B \\
 | \\
 \boxed{f} \\
 | \\
 A \\
 | \\
 \boxed{\text{id}_A} \\
 | \\
 A
 \end{array}
 =
 \begin{array}{c}
 B \\
 | \\
 \boxed{f} \\
 | \\
 A
 \end{array}
 =
 \begin{array}{c}
 B \\
 | \\
 \boxed{\text{id}_B} \\
 | \\
 B \\
 | \\
 \boxed{f} \\
 | \\
 A
 \end{array}
 \qquad
 \begin{array}{c}
 D \\
 | \\
 \boxed{h} \\
 | \\
 C \\
 | \\
 \boxed{g} \\
 | \\
 B \\
 | \\
 \boxed{f} \\
 | \\
 A
 \end{array}
 =
 \begin{array}{c}
 D \\
 | \\
 \boxed{h} \\
 | \\
 C \\
 | \\
 \boxed{g} \\
 | \\
 B \\
 | \\
 \boxed{f} \\
 | \\
 A
 \end{array}
 \tag{14}$$

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

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

0.7 Functors and natural transformations

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

Definition 0.14 (Functor, covariance, contravariance). Given categories \mathbf{C} and \mathbf{D} , a *functor* $F: \mathbf{C} \rightarrow \mathbf{D}$ is defined by the following data:

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

This data must satisfy the following properties:

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

Functors are implicitly *covariant*. There are also *contravariant* versions reversing the direction of morphisms: $F(g \circ f) = F(f) \circ F(g)$. We will only use the above definition, and model the contravariant version $\mathbf{C} \rightarrow \mathbf{D}$ as (contravariant) functors $\mathbf{C}^{\text{op}} \rightarrow \mathbf{D}$.

A functor between groups is also called a *group homomorphism*; of course this coincides with the usual notion.

Example 0.15. There is a functor $G: \mathbf{Set} \rightarrow \mathbf{Rel}$ defined by $G(A) = A$ and $G(A \xrightarrow{f} B) = \{(a, f(a) \mid a \in A\}$. It leaves objects alone, and turns functions into (the relation representing) their graph. There is also a functor $P: \mathbf{Rel} \rightarrow \mathbf{Set}$ in the other direction. On objects, $P(A)$ is the powerset of A , and a morphism $A \xrightarrow{R} B$ is turned into the function $P(R): P(A) \rightarrow P(B)$ given by $X \mapsto \{b \in B \mid \exists a \in X: aRb\}$.

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

Definition 0.16. A functor $F: \mathbf{C} \rightarrow \mathbf{D}$ is an *equivalence* when it is:

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

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

Definition 0.17 (Natural transformation, natural isomorphism). Given functors $F: \mathbf{C} \rightarrow \mathbf{D}$ and $G: \mathbf{C} \rightarrow \mathbf{D}$, a *natural transformation* $\zeta: F \Rightarrow G$ is an assignment to every object A in \mathbf{C} of a morphism $F(A) \xrightarrow{\zeta_A} G(A)$ in \mathbf{D} , such that the following diagram commutes for every morphism $A \xrightarrow{f} B$ in \mathbf{C} .

$$\begin{array}{ccc}
 F(A) & \xrightarrow{\zeta_A} & G(A) \\
 F(f) \downarrow & & \downarrow G(f) \\
 F(B) & \xrightarrow{\zeta_B} & G(B)
 \end{array} \tag{15}$$

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

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

Proposition 0.18 (Equivalence by natural isomorphism). *A functor $F: \mathbf{C} \rightarrow \mathbf{D}$ is an equivalence if and only if there exists a functor $G: \mathbf{D} \rightarrow \mathbf{C}$ and natural isomorphisms $G \circ F \simeq \text{id}_{\mathbf{C}}$ and $\text{id}_{\mathbf{D}} \simeq F \circ G$.*

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

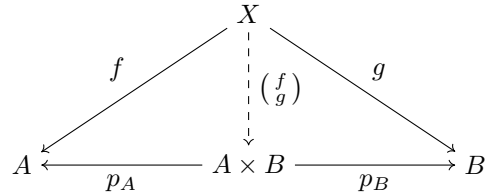
0.8 Products and equalizers

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

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

Definition 0.19 (Product, coproduct). Given objects A and B , a *product* is an object $A \times B$ together with morphisms $A \times B \xrightarrow{p_A} A$ and $A \times B \xrightarrow{p_B} B$, such that any two morphisms $X \xrightarrow{f} A$ and $X \xrightarrow{g} B$ allow a unique morphism $\begin{pmatrix} f \\ g \end{pmatrix}: X \rightarrow A \times B$ with $p_A \circ \begin{pmatrix} f \\ g \end{pmatrix} = f$ and $p_B \circ \begin{pmatrix} f \\ g \end{pmatrix} = g$. We can summarize these relationships

with the following diagram:



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

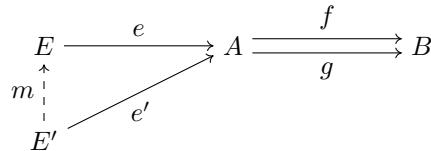
A category may or may not have products or coproducts (but if they exist they are unique up to isomorphism). In our main example categories they do exist, as we now examine.

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

- in **Set**, products are given by the Cartesian product, and coproducts by the disjoint union;
- in **Rel**, products and coproducts are both given by the disjoint union;

Given a pair of functions $S \xrightarrow{f,g} T$, it is interesting to ask on which elements of S they take the same value. Category theory dictates that we shouldn't ask about elements, but use morphisms to get the same information using a universal property.

Definition 0.21. For morphisms $A \xrightarrow{f,g} B$, their *equalizer* is a morphism $E \xrightarrow{e} A$ satisfying $f \circ e = g \circ e$, such that any morphism $E' \xrightarrow{e'} A$ satisfying $f \circ e' = g \circ e'$ allows a unique $E' \xrightarrow{m} E$ with $e' = e \circ m$:



We may think of an equalizer as the largest part of A on which f and g agree. In **Set**, it is given by $\{a \in A \mid f(a) = g(a)\}$. Again, equalizers may or may not exist in a particular category.

Example 0.22. Let's see what equalizers look like in our example categories.

- The category **Set** has equalizers for all pairs of parallel morphisms. An equalizer for $A \xrightarrow{f,g} B$ is the set $E = \{a \in A \mid f(a) = g(a)\}$, equipped with its embedding $E \xrightarrow{e} A$.
- The category **Rel** does not have all equalizers. For example, consider the relation $R = \{(y, z) \in \mathbb{R}^2 \mid y < z \in \mathbb{R}\} : \mathbb{R} \rightarrow \mathbb{R}$. Suppose $E : X \rightarrow \mathbb{R}$ were an equalizer of R and $\text{id}_{\mathbb{R}}$. Then $R \circ R = \text{id}_{\mathbb{R}} \circ R$, so there is a relation $M : \mathbb{R} \rightarrow X$ with $R = E \circ M$. Now $E \circ (M \circ E) = (E \circ M) \circ E = R \circ E = \text{id}_{\mathbb{R}} \circ E = E$, and since $S = \text{id}_X$ is the unique morphism satisfying $E \circ S = E$, we must have $M \circ E = \text{id}_X$. But then xEy and yMx for some $x \in X$ and $y \in \mathbb{R}$. It follows that $y(E \circ M)y$, that is, $y < y$, which is a contradiction.

Categories and Quantum Informatics: Hilbert spaces

Chris Heunen

Spring 2018

We introduce our main example category **Hilb** by recalling in some detail the mathematical formalism that underlies quantum theory: (complex) vector spaces, inner products, orthonormal bases, linear maps, matrices, dimensions, and dual spaces. We then introduce the adjoint of a linear map between Hilbert spaces, and define the terms unitary, isometry, partial isometry, and positive. We also define the tensor product of Hilbert spaces, and introduce the Kronecker product of matrices.

0.9 Vector spaces

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

Definition 0.1 (Vector space). A *vector space*, is a set V with a chosen element $0 \in V$, an addition operation $+: V \times V \rightarrow V$, and a scalar multiplication operation $\cdot: \mathbb{C} \times V \rightarrow V$, satisfying the following properties for all $u, v, w \in V$ and $a, b \in \mathbb{C}$:

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

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

Definition 0.2 (Linear map, antilinear map). A *linear map* is a function $f: V \rightarrow W$ between vector spaces, with the following properties, for all $u, v \in V$ and $a \in \mathbb{C}$:

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

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

An *anti-linear map* is a function that also satisfies (16), but instead of (17), has the additional property

$$f(a \cdot v) = a^* \cdot f(v), \tag{18}$$

where the star denotes complex conjugation.

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

Definition 0.3 (Vect, FVect). The category **Vect** of vector spaces and linear maps is defined as follows:

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

We define the category **FVect** to be the restriction of **Vect** to those vector spaces that are isomorphic to \mathbb{C}^n for some natural number n ; these are also called *finite-dimensional*, see Definition 0.5 below.

A *kernel* of a morphism $A \xrightarrow{f} B$ in a category is an equaliser of f and the *zero morphism* $A \xrightarrow{0} B$. Any morphism $f: V \rightarrow W$ in **Vect** has a kernel, namely the inclusion of $\ker(f) = \{v \in V \mid f(v) = 0\}$ into V . Hence kernels in the categorical sense coincide precisely with kernels in the sense of linear algebra.

Definition 0.4. The *direct sum* of vector spaces V and W is the vector space $V \oplus W$, whose elements are pairs (v, w) of elements $v \in V$ and $w \in W$, with entrywise addition and scalar multiplication.

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

0.10 Bases and matrices

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

Definition 0.5. For a vector space V , a family of elements $\{e_i\}$ is *linearly independent* when every element $a \in V$ can be expressed as a finite linear combination $a = \sum_i a_i e_i$ with *coefficients* $a_i \in \mathbb{C}$ in at most one way. It is a *basis* if additionally any $a \in V$ can be expressed as such a finite linear combination.

Every vector space admits a basis, and any two bases for the same vector space have the same cardinality. This is not clear, but quite nontrivial to show.

Definition 0.6. The *dimension* of a vector space V , written $\dim(V)$, is the cardinality of any basis. A vector space is *finite-dimensional* when it has a finite basis.

If vector spaces V and W have bases $\{d_i\}$ and $\{e_j\}$, and we fix some order on the bases, we can represent a linear map $V \xrightarrow{f} W$ as the matrix with $\dim(W)$ rows and $\dim(V)$ columns, whose entry at row i and column j is the coefficient $f(v_j)_i$. Composition of linear maps then corresponds to matrix multiplication (7). This directly leads to a category.

Definition 0.7. The skeletal category **Mat $_{\mathbb{C}}$** is defined as follows:

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

This theory of matrices is ‘just as good’ as the theory of finite-dimensional vector spaces. This can be made precise using the category theory we have developed.

Proposition 0.8. *There is an equivalence of categories $\text{Mat}_{\mathbb{C}} \rightarrow \mathbf{FVect}$, sending $n \mapsto \mathbb{C}^n$, and a matrix to its associated linear map.*

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

For a square matrix, the trace is an important operation.

Definition 0.9. For a square matrix with entries m_{ij} , its *trace* is the number $\sum_i m_{ii}$ given by the sum of the entries on the main diagonal.

0.11 Hilbert spaces

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

Definition 0.10. An *inner product* on a complex vector space V is a function $\langle - | - \rangle : V \times V \rightarrow \mathbb{C}$ that is:

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

$$\langle v | w \rangle = \langle w | v \rangle^*, \quad (19)$$

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

$$\langle v | a \cdot w \rangle = a \cdot \langle v | w \rangle, \quad (20)$$

$$\langle u | v + w \rangle = \langle u | v \rangle + \langle u | w \rangle; \quad (21)$$

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

$$\langle v | v \rangle \geq 0, \quad (22)$$

$$\langle v | v \rangle = 0 \Rightarrow v = 0. \quad (23)$$

Definition 0.11. For a vector space with inner product, the *norm* of an element v is $\|v\| := \sqrt{\langle v | v \rangle}$, a nonnegative real number.

The complex numbers carry a canonical inner-product structure given by

$$\langle a | b \rangle := a^* b, \quad (24)$$

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

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

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

Definition 0.12. 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, \dots of vectors satisfies $\sum_{i=1}^{\infty} \|v_i\| < \infty$, then there is a vector v such that $\|v - \sum_{i=1}^n v_i\|$ tends to zero.

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

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

Definition 0.13 (Bounded linear map). A linear map $f: H \rightarrow K$ between Hilbert spaces is *bounded* when there exists a number $b \in \mathbb{R}$ such that $\|f(v)\| \leq b \cdot \|v\|$ for all $v \in H$.

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

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

Definition 0.14 (**Hilb**, **FHilb**). The category **Hilb** of Hilbert spaces and bounded linear maps is defined as follows:

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

We define the category **FHilb** to be the restriction of **Hilb** to finite-dimensional Hilbert spaces.

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

Hilbert spaces have a more discerning notion of basis.

Definition 0.15 (Basis, orthogonal basis, orthonormal basis). For a Hilbert space H , an *orthogonal basis* is a family of elements $\{e_i\}$ with the following properties:

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

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

Any orthogonal family of elements is automatically linearly independent. For finite-dimensional Hilbert spaces, the ordinary notion of basis as a vector space is still useful, as given by Definition 0.5. Hence once we fix (ordered) bases on finite-dimensional Hilbert spaces, linear maps between them correspond to matrices, just as with vector spaces. For infinite-dimensional Hilbert spaces, however, having a basis for the underlying vector space is rarely mathematically useful.

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

Definition 0.16. The *direct sum* of Hilbert spaces H and K is the vector space $H \oplus K$, made into a Hilbert space by the inner product $\langle (v_1, w_1) | (v_2, w_2) \rangle = \langle v_1 | v_2 \rangle + \langle w_1 | w_2 \rangle$.

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

0.12 Adjoints

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

Definition 0.17. For a bounded linear map $f: H \rightarrow K$, its *adjoint* $f^\dagger: K \rightarrow H$ is the unique linear map with the following property, for all $u \in H$ and $v \in K$:

$$\langle f(u)|v \rangle = \langle u|f^\dagger(v) \rangle. \quad (25)$$

The existence of the adjoint follows from the Riesz representation theorem for Hilbert spaces, which we do not cover here. It follows immediately from (25) by uniqueness of adjoints that they also satisfy the following properties:

$$(f^\dagger)^\dagger = f, \quad (26)$$

$$(g \circ f)^\dagger = f^\dagger \circ g^\dagger, \quad (27)$$

$$\text{id}_H^\dagger = \text{id}_H. \quad (28)$$

Taking adjoints is an *anti-linear* operation.

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

Definition 0.18. A bounded linear map $H \xrightarrow{f} K$ between Hilbert spaces is:

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

The following notation is standard in the physics literature.

Definition 0.19 (Bra, ket). Given an element $v \in H$ of a Hilbert space, its *ket* $\mathbb{C} \xrightarrow{|v\rangle} H$ is the linear map $a \mapsto av$. Its *bra* $H \xrightarrow{\langle v|} \mathbb{C}$ is the linear map $w \mapsto \langle v|w \rangle$.

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

$$\left(\mathbb{C} \xrightarrow{|v\rangle} H \xrightarrow{\langle w|} \mathbb{C} \right) = \left(\mathbb{C} \xrightarrow{\langle w|\circ|v\rangle} \mathbb{C} \right) = \left(\mathbb{C} \xrightarrow{\langle w|v\rangle} \mathbb{C} \right) \quad (29)$$

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

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

Definition 0.20. For a Hilbert space H , its *dual Hilbert space* H^* is the vector space $\mathbf{Hilb}(H, \mathbb{C})$.

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

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

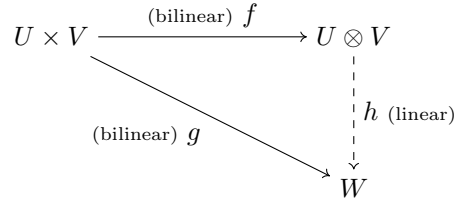
Definition 0.21 (Trace, trace class). When it converges, the *trace* of a positive linear map $f: H \rightarrow H$ is given by $\text{Tr}(f) := \sum \langle e_i|f(e_i) \rangle$ for any orthonormal basis $\{e_i\}$, in which case the map is called *trace class*.

If the sum converges for one orthonormal bases, then with some effort one can prove that it converges for all orthonormal bases, and that the trace is independent of the chosen basis. Also, in the finite-dimensional case, the trace defined in this way agrees with the matrix trace of Definition 0.9.

0.13 Tensor products

The tensor product is a way to make a new vector space out of two given ones. With some work the tensor product can be constructed explicitly, but it is only important for us that it exists, and is defined up to isomorphism by a universal property. If U , V and W are vector spaces, a function $f: U \times V \rightarrow W$ 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 0.22. The *tensor product of vector spaces* U and V is a vector space $U \otimes V$ together with a bilinear function $f: U \times V \rightarrow U \otimes V$ such that for every bilinear function $g: U \times V \rightarrow W$ there exists a unique linear function $h: U \otimes V \rightarrow W$ such that $g = h \circ f$.



The function f usually stays anonymous and is written as $(u, v) \mapsto u \otimes v$. It follows that 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 $f_1: U_1 \rightarrow V_1$ and $f_2: U_2 \rightarrow V_2$ are linear maps, there is a unique linear map $f_1 \otimes f_2: U_1 \otimes U_2 \rightarrow V_1 \otimes V_2$ 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 $\otimes: \mathbf{Vect} \times \mathbf{Vect} \rightarrow \mathbf{Vect}$.

Definition 0.23. The *tensor product of Hilbert spaces* H and K is the following Hilbert space $H \otimes K$: take the tensor product of vector spaces; give it the inner product $\langle u_1 \otimes v_1 | u_2 \otimes v_2 \rangle = \langle u_1 | u_2 \rangle_H \cdot \langle v_1 | v_2 \rangle_K$; complete it. If $H \xrightarrow{f} H'$ and $K \xrightarrow{g} K'$ are bounded linear maps, then so is the continuous extension of the tensor product of linear maps to a function that we again call $f \otimes g: H \otimes K \rightarrow H' \otimes K'$. This gives a functor $\otimes: \mathbf{Hilb} \times \mathbf{Hilb} \rightarrow \mathbf{Hilb}$.

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

Definition 0.24 (Kronecker product). When finite-dimensional Hilbert spaces H_1, H_2, K_1, K_2 are equipped with fixed ordered orthonormal bases, linear maps $H_1 \xrightarrow{f} K_1$ and $H_2 \xrightarrow{g} K_2$ can be written as matrices. Their tensor product $H_1 \otimes H_2 \xrightarrow{f \otimes g} K_1 \otimes K_2$ corresponds to the following block matrix, called their *Kronecker product*:

$$(f \otimes g) := \begin{pmatrix} (f_{11}g) & (f_{12}g) & \cdots & (f_{1n}g) \\ (f_{21}g) & (f_{22}g) & \cdots & (f_{2n}g) \\ \vdots & \vdots & \ddots & \vdots \\ (f_{m1}g) & (f_{m2}g) & \cdots & (f_{mn}g) \end{pmatrix}. \tag{30}$$

Categories and Quantum Informatics: Monoidal categories

Chris Heunen

Spring 2018

A monoidal category is a category equipped with extra data, describing how objects and morphisms can be combined ‘in parallel’. This chapter introduces the theory of monoidal categories, and shows how our example categories **Hilb**, **Set** and **Rel** can be given a monoidal structure. We also introduce a visual notation called the graphical calculus, which provides an intuitive and powerful way to work with them.

1.1 Monoidal structure

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

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

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

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

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

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

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

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

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

$$\begin{array}{ccc}
 (A \otimes B) \otimes C & \xrightarrow{\alpha_{A,B,C}} & A \otimes (B \otimes C) \\
 \downarrow (f \otimes g) \otimes h & & \downarrow f \otimes (g \otimes h) \\
 (A' \otimes B') \otimes C' & \xrightarrow{\alpha_{A',B',C'}} & A' \otimes (B' \otimes C')
 \end{array}
 \qquad
 \begin{array}{ccccc}
 I \otimes A & \xrightarrow{\lambda_A} & A & \xleftarrow{\rho_A} & A \otimes I \\
 \downarrow I \otimes f & & \downarrow f & & \downarrow f \otimes I \\
 I \otimes B & \xrightarrow{\lambda_B} & B & \xleftarrow{\rho_B} & B \otimes I
 \end{array} \tag{1.3}$$

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

The triangle and pentagon equations each say that two particular ways of ‘reorganizing’ a system are equal. Surprisingly, this implies that *any* two ‘reorganizations’ are equal; this is the content of the Coherence Theorem.

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

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

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

Our first example of a monoidal structure is on the category **Hilb**.

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

- the tensor product $\otimes: \mathbf{Hilb} \times \mathbf{Hilb} \rightarrow \mathbf{Hilb}$ is the tensor product of Hilbert space;
- the unit object I is the one-dimensional Hilbert space \mathbb{C} ;
- associators $(H \otimes J) \otimes K \xrightarrow{\alpha_{H,J,K}} H \otimes (J \otimes K)$ are the unique linear maps satisfying $(u \otimes v) \otimes w \mapsto u \otimes (v \otimes w)$ for all $u \in H$, $v \in J$ and $w \in K$;
- left unitors $\mathbb{C} \otimes H \xrightarrow{\lambda_H} H$ are the unique linear maps satisfying $1 \otimes u \mapsto u$ for all $u \in H$;
- right unitors $H \otimes \mathbb{C} \xrightarrow{\rho_H} H$ are the unique linear maps satisfying $u \otimes 1 \mapsto u$ for all $u \in H$.

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

While \mathbf{Hilb} is relevant for quantum computation, the monoidal category \mathbf{Set} is an important setting for classical computation.

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

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

The Cartesian product in \mathbf{Set} is a categorical product. This is an example of a general phenomenon: if a category has products, then these can be used to give a monoidal structure on the category. The same is true for coproducts, which in \mathbf{Set} are given by disjoint union.

This highlights an important difference between the standard tensor products on \mathbf{Hilb} and \mathbf{Set} : while the tensor product on \mathbf{Set} comes from a categorical product, the tensor product on \mathbf{Hilb} does not. We will discover many more differences between \mathbf{Hilb} and \mathbf{Set} , which provide insight into the differences between quantum and classical information.

There is a canonical monoidal structure on the category \mathbf{Rel} .

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

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

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

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

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

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

$$(g \circ f) \otimes (j \circ h) = (g \otimes j) \circ (f \otimes h) \quad (1.4)$$

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

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

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

1.2 Graphical calculus

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

$$\begin{array}{ccc} B & | & D \\ & \square & \\ f & & g \\ & \square & \\ A & | & C \end{array} \quad (1.5)$$

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

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

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

$$(1.6)$$

The left unitor $I \otimes A \xrightarrow{\lambda_A} A$, the right unitor $A \otimes I \xrightarrow{\rho_A} A$ and the associator $(A \otimes B) \otimes C \xrightarrow{\alpha_{A,B,C}} A \otimes (B \otimes C)$

are also simply not depicted:

$$\begin{array}{ccc}
 \begin{array}{c} | \\ A \\ | \\ \lambda_A \end{array} &
 \begin{array}{c} | \\ A \\ | \\ \rho_A \end{array} &
 \begin{array}{ccc} | & | & | \\ A & B & C \\ | & | & | \\ \alpha_{A,B,C} & & \end{array}
 \end{array} \tag{1.7}$$

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

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

$$\left(\begin{array}{c} | \\ C \\ | \\ \boxed{g} \\ | \\ B \\ | \\ \boxed{f} \\ | \\ A \end{array} \right) \left(\begin{array}{c} | \\ F \\ | \\ \boxed{j} \\ | \\ E \\ | \\ \boxed{h} \\ | \\ D \end{array} \right) = \begin{array}{ccc} \overbrace{C} & & \overbrace{F} \\ | & & | \\ \boxed{g} & & \boxed{j} \\ | & & | \\ \underbrace{B} & & \underbrace{E} \\ | & & | \\ \boxed{f} & & \boxed{h} \\ | & & | \\ \underbrace{A} & & \underbrace{D} \end{array} \tag{1.8}$$

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

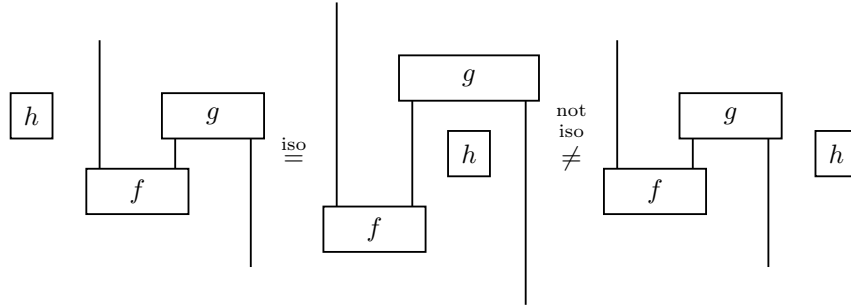
The point of the graphical calculus is that all the superficially complex aspects of the algebraic definition of monoidal categories—the unit law, the associativity law, associators, left unitors, right unitors, the triangle equation, the pentagon equation, the interchange law—melt away, allowing us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

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

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

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

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



As we have done here, we will often allow the heights of the diagrams to change, and allow input and output wires to slide horizontally along their respective boundaries, although they must never change order. The third diagram here is not isotopic to the first two, since for the h box to move to the right-hand side, it would have to “pass through” one of the wires, which is not allowed. The box cannot pass “over” or “under” the wire, since the diagrams are confined to the plane—that is what is meant by *planar* isotopy. You should imagine that the components of the diagram are trapped between two pieces of glass.

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

- $P(f, g)$: ‘under the axioms of a monoidal category, $f = g$ ’;
- $Q(f, g)$: ‘the graphical representations of f and g are planar isotopic’.

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

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

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

The notation $\stackrel{\text{iso}}{=}$ to denote isotopic diagrams, whose interpretations as morphisms in a monoidal category are therefore equal, will be used throughout this book, to indicate an application of the correctness property of the graphical calculus.

1.3 States and effects

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

Definition 1.10. In a monoidal category, a *state* of an object A is a morphism $I \rightarrow A$. States are sometimes also called *points*.

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

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

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

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

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

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

$$\begin{array}{c}
 A \\
 \downarrow \\
 \triangleleft a
 \end{array}
 \tag{1.9}$$

1.4 Product states and entangled states

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

$$\begin{array}{c}
 A \quad B \\
 \downarrow \quad \downarrow \\
 \triangleleft c
 \end{array}
 \tag{1.10}$$

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

$$\begin{array}{c}
 A \quad B \\
 \downarrow \quad \downarrow \\
 \triangleleft c
 \end{array}
 =
 \begin{array}{c}
 A \quad B \\
 \downarrow \quad \downarrow \\
 \triangleleft a \quad \triangleleft b
 \end{array}
 \tag{1.11}$$

Definition 1.14. A joint state is *entangled* when it is not a product state.

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

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

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

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

1.5 Effects

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

Definition 1.16. In a monoidal category, an *effect* or *costate* for an object A is a morphism $A \rightarrow I$.

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



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

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

Example 1.17. These statements are at a very general level. To say more, we must take account of the particular theory of processes described by the monoidal category in which we are working.

- In quantum theory, as encoded by **Hilb**, we require a , f and x to be partial isometries. The rules of quantum mechanics then dictate that the probability for this history to take place is given by the square norm of the resulting state. So in particular, the history described by this composite is impossible exactly when the overall state is zero.
- In nondeterministic classical physics, as described by **Rel**, we need put no particular requirements on a , f and x — they may be arbitrary relations of the correct types. The overall composite relation then describes the possible ways in which A can be prepared as a result of this history. If the overall composite is empty, that means this particular sequence of a state preparation, a dynamics step, and a measurement result cannot occur.
- Things are very different in **Set**. The monoidal unit object is *terminal* in that category, meaning $\mathbf{Set}(A, I)$ has only a single element for any object A . So every object has a *unique* effect, and there is no nontrivial notion of ‘measurement’.

1.6 Braiding and symmetry

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

We first consider braided monoidal categories.

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

$$A \otimes B \xrightarrow{\sigma_{A,B}} B \otimes A \quad (1.13)$$

satisfying the following *hexagon equations*:

$$\begin{array}{ccc}
 A \otimes (B \otimes C) & \xrightarrow{\sigma_{A,B \otimes C}} & (B \otimes C) \otimes A \\
 \alpha_{A,B,C}^{-1} \swarrow & & \nwarrow \alpha_{B,C,A}^{-1} \\
 (A \otimes B) \otimes C & & B \otimes (C \otimes A) \\
 \sigma_{A,B} \otimes \text{id}_C \searrow & & \nearrow \text{id}_B \otimes \sigma_{A,C} \\
 (B \otimes A) \otimes C & \xrightarrow{\alpha_{B,A,C}} & B \otimes (A \otimes C)
 \end{array} \quad (1.14)$$

$$\begin{array}{ccc}
 (A \otimes B) \otimes C & \xrightarrow{\sigma_{A \otimes B, C}} & C \otimes (A \otimes B) \\
 \alpha_{A,B,C} \swarrow & & \nwarrow \alpha_{C,A,B} \\
 A \otimes (B \otimes C) & & (C \otimes A) \otimes B \\
 \text{id}_A \otimes \sigma_{B,C} \searrow & & \nearrow \sigma_{A,C} \otimes \text{id}_B \\
 A \otimes (C \otimes B) & \xrightarrow{\alpha_{A,C,B}^{-1}} & (A \otimes C) \otimes B
 \end{array} \quad (1.15)$$

We include the braiding in the graphical notation like this:

$$\begin{array}{ccc}
 \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \end{array} & & \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} \\
 A \otimes B \xrightarrow{\sigma_{A,B}} B \otimes A & & B \otimes A \xrightarrow{\sigma_{A,B}^{-1}} A \otimes B
 \end{array} \tag{1.16}$$

Invertibility then takes the following graphical form:

$$\begin{array}{ccc}
 \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \end{array} & = & \begin{array}{c} | \\ | \\ | \end{array} \\
 \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} & = & \begin{array}{c} | \\ | \\ | \end{array}
 \end{array} \tag{1.17}$$

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

$$\begin{array}{ccc}
 \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \boxed{f} \quad \boxed{g} \\ \text{---} \end{array} & = & \begin{array}{c} \boxed{g} \quad \boxed{f} \\ \diagdown \quad \diagup \\ \text{---} \end{array} \\
 \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \boxed{f} \quad \boxed{g} \\ \text{---} \end{array} & = & \begin{array}{c} \boxed{g} \quad \boxed{f} \\ \diagdown \quad \diagup \\ \text{---} \end{array}
 \end{array} \tag{1.18}$$

The hexagon equations have the following graphical representations:

$$\begin{array}{ccc}
 \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \end{array} & = & \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \end{array} \\
 \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array} & = & \begin{array}{c} \text{---} \\ \diagup \quad \diagdown \\ \text{---} \end{array}
 \end{array} \tag{1.19}$$

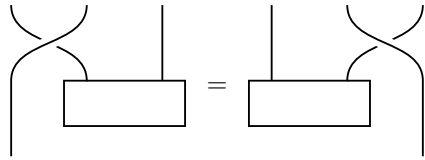
Each of these equations has two strands close to each other on the left-hand side, to indicate that we are treating them as a single composite object for the purposes of the braiding. We see that the hexagon equations are saying something quite straightforward: to braid with a tensor product of two strands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

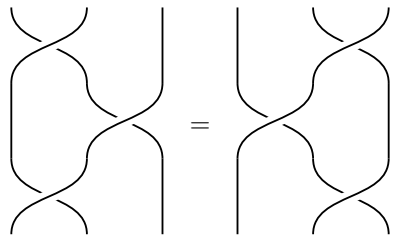
Since the strands of a braiding cross over each other, they are not lying on the plane; they live in three-dimensional space. So while categories have a one-dimensional or linear notation, and monoidal categories have a two-dimensional or planar graphical notation, braided monoidal categories have a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

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

Theorem 1.19 (Correctness of graphical calculus for braided monoidal categories). *A well-typed equation between morphisms in a braided monoidal category follows from the axioms if and only if it holds in the graphical language up to spatial isotopy.*

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


(1.20)


(1.21)

Equation (1.21) is called the *Yang–Baxter equation*, which plays an important role in the mathematical theory of knots.

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

Definition 1.20. Our example categories **Hilb**, **Set** and **Rel** can all be equipped with a canonical braiding:

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

In fact these are all symmetric monoidal structures, which we explore in Section 1.7.

1.7 Symmetric monoidal categories

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

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

$$\sigma_{B,A} \circ \sigma_{A,B} = \text{id}_{A \otimes B} \tag{1.22}$$

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

Graphically, condition (1.22) has the following representation.


(1.23)

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

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

$$\begin{array}{c} \diagup \\ \diagdown \end{array} = \begin{array}{c} \diagdown \\ \diagup \end{array} \tag{1.24}$$

Proof. Combine (1.17) and (1.23). □

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

$$\begin{array}{c} \diagup \\ \diagdown \end{array} \tag{1.25}$$

for the single type of crossing.

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

Suppose we imagine our diagrams as curves embedded in four-dimensional space. Then we can smoothly deform one crossing into the other, in the manner of equation (1.24), by making use of the extra dimension. In this sense, symmetric monoidal categories have a four-dimensional graphical notation. The following correctness theorem therefore uses the four-dimensional version of isotopy.

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

Categories and Quantum Informatics: Scalars

Chris Heunen

Spring 2018

Many aspects of linear algebra can be described using categorical structures. This chapter examines abstractions of the base field, and inner products.

2.1 Scalars

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

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

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

A *monoid* is a set A equipped with a multiplication operation, which we write as juxtaposition of elements of A , and a chosen unit element $1 \in A$, satisfying for all $u, v, w \in A$ an associativity law $u(vw) = (uv)w$ and a unit law $1v = v = v1$. We will study monoids closely from a categorical perspective later, but for now we note that it is easy to show from the axioms of a category that the scalars form a monoid under composition.

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

- In **Hilb**, scalars $\mathbb{C} \xrightarrow{f} \mathbb{C}$ correspond to complex numbers $f(1) \in \mathbb{C}$ as discussed above. Composition of scalars $\mathbb{C} \xrightarrow{f,g} \mathbb{C}$ corresponds to multiplication of complex numbers, as $(g \circ f)(1) = g(f(1)) = f(1) \cdot g(1)$. Hence the scalars in **Hilb** are the complex numbers under multiplication.
- In **Set**, scalars are functions $\{\bullet\} \xrightarrow{f} \{\bullet\}$. There is only one unique such function, namely $\text{id}_{\{\bullet\}} : \bullet \mapsto \bullet$, which we will also simply write as 1. Hence the scalars in **Set** form the trivial one-element monoid.
- In **Rel**, scalars are relations $\{\bullet\} \xrightarrow{R} \{\bullet\}$. There are two such relations: $F = \emptyset$ and $T = \{(\bullet, \bullet)\}$. Working out the composition in **Rel** gives the following multiplication table:

	F	T
F	F	F
T	F	T

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

Commutativity

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

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

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

$$\begin{array}{ccccc}
 I & \xrightarrow{a} & I & & I \\
 \downarrow \lambda_I^{-1} & \searrow b & \downarrow \lambda_I^{-1} & \xrightarrow{a} & \downarrow \lambda_I^{-1} \\
 I & & I & \xrightarrow{a} & I \\
 \downarrow \rho_I^{-1} & & \downarrow \rho_I^{-1} & & \downarrow \rho_I^{-1} \\
 I \otimes I & \xrightarrow{\lambda_I} & I \otimes I & \xrightarrow{a \otimes \text{id}_I} & I \otimes I \\
 \downarrow \text{id}_I \otimes b & \uparrow \rho_I & \downarrow \text{id}_I \otimes b & \xrightarrow{\rho_I} & \downarrow \text{id}_I \otimes b \\
 I \otimes I & & I \otimes I & \xrightarrow{a \otimes \text{id}_I} & I \otimes I \\
 & & & & \uparrow \lambda_I \\
 & & & & I
 \end{array} \tag{2.1}$$

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. Hence we have $ab = ba$. Note the importance of coherence here, as we rely on the fact that $\rho_I = \lambda_I$. \square

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

- In **Hilb**: multiplication of complex numbers is commutative.
- In **Set**: $1 \circ 1 = 1 \circ 1$ is trivially commutative.
- In **Rel**: let a, b be Boolean values; then $(a \text{ and } b)$ is true precisely when $(b \text{ and } a)$ is true.

Graphical calculus

We draw scalars as circles:

$$\textcircled{a} \tag{2.2}$$

Commutativity of scalars then has the following graphical representation:

$$\begin{array}{ccc}
 \textcircled{b} & & \textcircled{a} \\
 & = & \\
 \textcircled{a} & & \textcircled{b}
 \end{array} \tag{2.3}$$

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

Scalar multiplication

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

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

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

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

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

- (a) $\text{id}_I \bullet f = f$;
- (b) $a \bullet b = a \circ b$;
- (c) $a \bullet (b \bullet f) = (a \bullet b) \bullet f$;
- (d) $(b \bullet g) \circ (a \bullet f) = (b \circ a) \bullet (g \circ f)$.

Proof. These statements all follow straightforwardly from the graphical calculus, thanks to the correctness theorem. We also give the direct algebraic proofs. 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:

$$\begin{array}{ccccccc}
 A & \xrightarrow{\text{id}_A} & A & \xrightarrow{a \bullet (b \bullet f)} & B & \xrightarrow{\text{id}_B} & B \\
 \lambda_A^{-1} \downarrow & & \lambda_A^{-1} \downarrow & & \lambda_B \uparrow & & \lambda_B \uparrow \\
 I \otimes A & \xrightarrow{\text{id}_{I \otimes A}} & I \otimes A & \xrightarrow{a \otimes (b \bullet f)} & I \otimes B & \xrightarrow{\text{id}_{I \otimes B}} & I \otimes B \\
 & \searrow \lambda_I^{-1} \otimes \text{id}_A & \downarrow \text{id}_I \otimes \lambda_A^{-1} & & \uparrow \text{id}_I \otimes \lambda_B & & \uparrow \lambda_I \otimes \text{id}_B \\
 & & I \otimes (I \otimes A) & \xrightarrow{a \otimes (b \otimes f)} & I \otimes (I \otimes B) & & \\
 & & \downarrow \alpha_{I,I,A}^{-1} & & \uparrow \alpha_{I,I,B} & & \\
 & & (I \otimes I) \otimes A & \xrightarrow{(a \otimes b) \otimes f} & (I \otimes I) \otimes B & &
 \end{array}$$

Part (d) follows from the interchange law. □

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

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

2.2 Daggers

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

Dagger categories

To describe inner products abstractly, begin by thinking about *adjoints*. Any bounded linear map $H \xrightarrow{f} K$ between Hilbert spaces has a unique adjoint, which is another bounded linear map $K \xrightarrow{f^\dagger} H$. We can encode this action as a functor.

Definition 2.8. On \mathbf{Hilb} , the functor *taking adjoints* $\dagger: \mathbf{Hilb} \rightarrow \mathbf{Hilb}$ is the contravariant functor that takes objects to themselves, and morphisms to their adjoints as bounded linear maps.

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

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

$$\begin{aligned} (\mathbb{C} \xrightarrow{w} H \xrightarrow{v^\dagger} \mathbb{C}) &\equiv v^\dagger(w(1)) \\ &= \langle 1|v^\dagger(w(1)) \rangle \\ &= \langle v|w \rangle \end{aligned} \tag{2.5}$$

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

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

Definition 2.9 (Dagger functor, dagger category). A *dagger functor* on a category \mathbf{C} is an involutive contravariant functor $\dagger: \mathbf{C} \rightarrow \mathbf{C}$ that is the identity on objects. A *dagger category* is a category equipped with a dagger functor.

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

$$(g \circ f)^\dagger = f^\dagger \circ g^\dagger \tag{2.6}$$

$$\text{id}_H^\dagger = \text{id}_H \tag{2.7}$$

$$(f^\dagger)^\dagger = f \tag{2.8}$$

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

The canonical dagger functor on \mathbf{Hilb} is the functor taking adjoints. \mathbf{Rel} also has a canonical dagger functor.

Definition 2.10. The dagger structure on \mathbf{Rel} is given by relational converse: for $S \xrightarrow{R} T$, define $T \xrightarrow{R^\dagger} S$ by setting $t R^\dagger s$ if and only if $s R t$.

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

Another important non-example is **Vect**, the category of complex vector spaces and linear maps. For an infinite-dimensional complex vector space V , the set $\mathbf{Vect}(\mathbb{C}, V)$ has a strictly smaller cardinality than the set $\mathbf{Vect}(V, \mathbb{C})$, so no dagger functor is possible. The category **FVect** containing only finite-dimensional objects *can* be equipped with a dagger functor: one way to do this is by assigning an inner product to every object, and then constructing the associated adjoints. However, it does not come with a *canonical* dagger functor.

A one-object dagger category is also called an *involutive monoid*. It consists of a set M together with an element $1 \in M$ and functions $M \times M \rightarrow M$ and $M \overset{\dagger}{\rightarrow} M$ satisfying $1m = m = m1$, $m(no) = (mn)o$, and $(m^\dagger)^\dagger = m$ for all $m, n, o \in M$.

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

Definition 2.11. A morphism $A \xrightarrow{f} B$ in a dagger category is:

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

If a category carries an important structure, it is often fruitful to require that the constructions one makes are compatible with that structure. The dagger functor is an important structure for us, and for most of this book we will require compatibility with it. In the search for good definitions, it is useful to see this as a sort of guiding principle, which we summarize as the *way of the dagger*.

Monoidal dagger categories

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

Definition 2.12 (Monoidal dagger category, braided, symmetric). A *monoidal dagger category* is a dagger category that is also monoidal, such that $(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger$ for all morphisms f and g , and such that all components of the natural isomorphisms α , λ and ρ are unitary. A *braided monoidal dagger category* is a monoidal dagger category equipped with a unitary braiding. A *symmetric monoidal dagger category* is a braided monoidal dagger category for which the braiding is a symmetry.

Example 2.13. Both **Hilb** and **Rel** are symmetric monoidal dagger categories.

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

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

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

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

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

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

$$\begin{array}{c} B \\ | \\ \boxed{f} \\ | \\ A \end{array} \mapsto \begin{array}{c} A \\ | \\ \boxed{f^\dagger} \\ | \\ B \end{array} \quad (2.9)$$

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

$$\begin{array}{c} B \\ | \\ \boxed{f} \text{ (wedge)} \\ | \\ A \end{array} \mapsto \begin{array}{c} A \\ | \\ \boxed{f} \text{ (wedge)} \\ | \\ B \end{array} \quad (2.10)$$

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

For example, the graphical representation unitarity (see Definition 2.11) is:

$$\begin{array}{c} | \\ \boxed{f} \text{ (wedge)} \\ | \\ \boxed{f} \text{ (wedge)} \\ | \end{array} = \left| \right. \quad \begin{array}{c} | \\ \boxed{f} \text{ (wedge)} \\ | \\ \boxed{f} \text{ (wedge)} \\ | \end{array} = \left| \right. \quad (2.11)$$

In particular, in a monoidal dagger category, we can use this notation for morphisms $I \xrightarrow{v} A$ representing

a state. This gives a representation of the adjoint morphism $A \xrightarrow{v^\dagger} I$ as follows.

$$\begin{array}{ccc}
 \begin{array}{c} A \\ \downarrow \\ \triangle v \end{array} & \mapsto & \begin{array}{c} \triangle v \\ \uparrow \\ A \end{array}
 \end{array}
 \tag{2.12}$$

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

Equation (2.5) demonstrated how to recover inner products from the ability to take daggers of states. Applying this argument graphically yields the following expression for the inner product $\langle v|w \rangle$ of two states $I \xrightarrow{v,w} H$.

$$\langle v|w \rangle = \begin{array}{c} \triangle v \\ \updownarrow \\ \triangle w \end{array} = \begin{array}{c} \diamond v \\ \diamond w \end{array}
 \tag{2.13}$$

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

Probabilities

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

Definition 2.14 (Probability). If $I \xrightarrow{v} A$ is a state, and $A \xrightarrow{x} I$ an effect, in a monoidal dagger category, set

$$\text{Prob}(x, v) = v^\dagger \circ x^\dagger \circ x \circ v : I \rightarrow I.
 \tag{2.14}$$

Example 2.15. In our example categories, probabilities match with our interpretation.

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

Categories and Quantum Informatics: Dual objects

Chris Heunen

Spring 2018

Dualizability is a property of an object that means the wire representing it in the graphical calculus can bend. In terms of linear algebra, it is a categorical model for entangled states.

3.1 Dual objects

Definition 3.1 (Dual object). In a monoidal category, an object L is *left-dual* to an object R , and R is *right-dual* to L , written $L \dashv R$, when there exist a unit morphism $I \xrightarrow{\eta} R \otimes L$ and a counit morphism $L \otimes R \xrightarrow{\varepsilon} I$ making the following diagrams commute:

$$\begin{array}{ccccc}
 L & \xrightarrow{\rho_L^{-1}} & L \otimes I & \xrightarrow{\text{id}_L \otimes \eta} & L \otimes (R \otimes L) \\
 \text{id}_L \downarrow & & & & \downarrow \alpha_{L,R,L}^{-1} \\
 L & \xleftarrow{\lambda_L} & I \otimes L & \xleftarrow{\varepsilon \otimes \text{id}_L} & (L \otimes R) \otimes L
 \end{array} \tag{3.1}$$

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

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

We draw an object L as a wire with an upward-pointing arrow, and a right dual R as a wire with a downward-pointing arrow.

$$\begin{array}{ccc}
 \begin{array}{c} \uparrow \\ L \end{array} & & \begin{array}{c} \downarrow \\ R \end{array}
 \end{array} \tag{3.3}$$

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

$$\begin{array}{ccc}
 \begin{array}{c} R \quad L \\ \downarrow \quad \uparrow \\ \text{U-shaped wire} \end{array} & & \begin{array}{c} \text{Arched wire} \\ \uparrow \quad \downarrow \\ L \quad R \end{array}
 \end{array} \tag{3.4}$$

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

$$\begin{array}{c} \uparrow \\ \curvearrowright \\ \uparrow \end{array} = \uparrow \qquad \begin{array}{c} \downarrow \\ \curvearrowleft \\ \downarrow \end{array} = \downarrow \qquad (3.5)$$

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

These equations add *orientation* to the graphical calculus. Physically, η represents a state of $R \otimes L$; a way for these two systems to be brought into being. We will see later that it represents a full-rank entangled state of $R \otimes L$. The fact that entanglement is modelled so naturally using monoidal categories is a key reason for interest in the categorical approach to quantum information.

Example 3.2. We now see what dual objects look like in our example categories.

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

$$\varepsilon : |\phi\rangle \otimes \langle\psi| \mapsto \langle\psi|\phi\rangle \qquad (3.6)$$

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

$$\eta : 1 \mapsto \sum_i \langle i| \otimes |i\rangle \qquad (3.7)$$

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

- Infinite-dimensional Hilbert spaces do not have duals. For an infinite-dimensional Hilbert space, the definitions of η and ε given above are no good, as they do not give bounded linear maps. Later in this chapter we will see that a Hilbert space has a dual if and only if it is finite-dimensional.
- In **Rel**, every object is its own dual, even sets of infinite cardinality. For a set S , the relations $1 \xrightarrow{\eta} S \times S$ and $S \times S \xrightarrow{\varepsilon} 1$ are defined in the following way, where we write \bullet for the unique element of the 1-element set:

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

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

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

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

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

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

$$\begin{array}{c} A^* \quad B \\ \downarrow \quad \uparrow \\ \text{---} \boxed{f} \text{---} \\ \uparrow \quad \downarrow \\ A \quad B^* \end{array} \qquad (3.11)$$

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

$$(3.12)$$

In **Set**, the monoidal unit object 1 is terminal, and so all conames $A \otimes B^* \xrightarrow{\perp f \dashv} 1$ must be equal. If the set B has a dual, this would imply that for all sets A , all functions $A \xrightarrow{f} B$ are equal, which is only the case for $B = \emptyset$ (the empty set), or $B = 1$. It is easy to see that \emptyset does not have a dual, because there is no function $1 \rightarrow \emptyset \times \emptyset^*$ for any value of \emptyset^* . The 1-element set does have a dual since it is the monoidal unit, as established by Lemma 3.7 below.

Basic properties

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

Lemma 3.4. *In a monoidal category with $L \dashv R$, then $L \dashv R'$ if and only if $R \simeq R'$. Similarly, if $L \dashv R$, then $L' \dashv R$ if and only if $L \simeq L'$.*

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

$$(3.13)$$

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

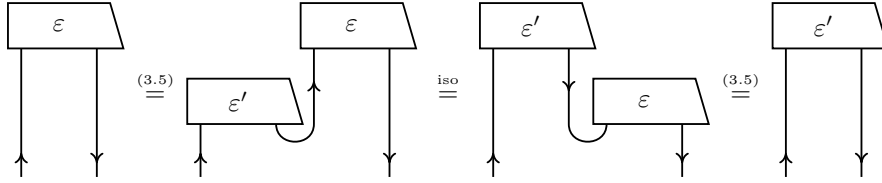
$$(3.14)$$

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

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

Lemma 3.5. *In a monoidal category, if $(L, R, \eta, \varepsilon)$ and $(L, R, \eta, \varepsilon')$ both exhibit a duality, then $\varepsilon = \varepsilon'$. Similarly, if $(L, R, \eta, \varepsilon)$ and $(L, R, \eta', \varepsilon)$ both exhibit a duality, then $\eta = \eta'$.*

Proof. For the first case, we use the following graphical argument.



The second case is similar. □

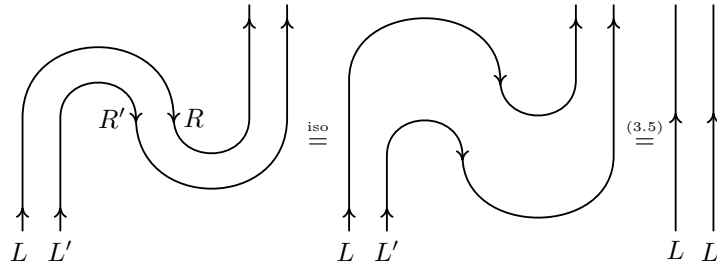
The following lemmas show that dual objects interact well with the monoidal structure.

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

Proof. Take $\eta = \lambda_I^{-1}: I \rightarrow I \otimes I$ and $\varepsilon = \lambda_I: I \otimes I \rightarrow I$ shows that $I \dashv I$. The snake equations follow directly from the coherence theorem. □

Lemma 3.7. *In a monoidal category, $L \dashv R$ and $L' \dashv R'$ implies $L \otimes L' \dashv R' \otimes R$.*

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

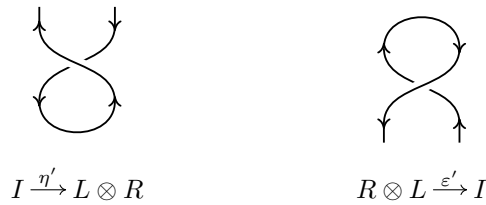


The other snake equation follows similarly. □

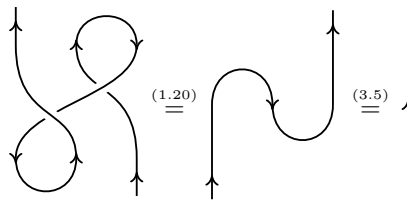
If the monoidal category has a braiding then a duality $L \dashv R$ gives rise to a duality $R \dashv L$, as the next lemma investigates.

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

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



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



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

The duality functor

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

Definition 3.9. 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:

$$\begin{array}{c} A^* \\ \downarrow \\ \boxed{f^*} \\ \downarrow \\ B^* \end{array} := \begin{array}{c} A^* \\ \downarrow \\ \boxed{f} \\ \downarrow \\ B^* \end{array} \stackrel{(3.15)}{=} \begin{array}{c} A^* \\ \downarrow \\ \boxed{f} \\ \downarrow \\ B^* \end{array}$$
(3.15)

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

Definition 3.10 (Right dual functor). In a monoidal category \mathbf{C} in which every object X has a chosen right dual X^* , the *right dual functor* $(-)^* : \mathbf{C} \rightarrow \mathbf{C}^{\text{op}}$ is defined on objects as $(X)^* := X^*$ and on morphisms as $(f)^* = f^*$.

Lemma 3.11. *The right-duals functor satisfies the functor axioms.*

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

$$\begin{array}{c} A^* \\ \downarrow \\ \boxed{(g \circ f)^*} \\ \downarrow \\ C^* \end{array} \stackrel{(3.15)}{=} \begin{array}{c} A^* \\ \downarrow \\ \boxed{g} \\ \uparrow \\ \boxed{f} \\ \downarrow \\ C^* \end{array} \stackrel{(3.5)}{=} \begin{array}{c} A^* \\ \downarrow \\ \boxed{f} \\ \uparrow \\ \boxed{g} \\ \downarrow \\ C^* \end{array} \stackrel{(3.15)}{=} \begin{array}{c} A^* \\ \downarrow \\ \boxed{f^*} \\ \downarrow \\ \boxed{g^*} \\ \downarrow \\ C^* \end{array}$$

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

The dual of a morphism can ‘slide’ along the cups and the caps.

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

$$\begin{array}{c} \uparrow \\ \boxed{f} \\ \downarrow \end{array} = \begin{array}{c} \uparrow \\ \boxed{f} \\ \downarrow \end{array} \quad \begin{array}{c} \downarrow \\ \boxed{f} \\ \uparrow \end{array} = \begin{array}{c} \downarrow \\ \boxed{f} \\ \uparrow \end{array}$$
(3.16)

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

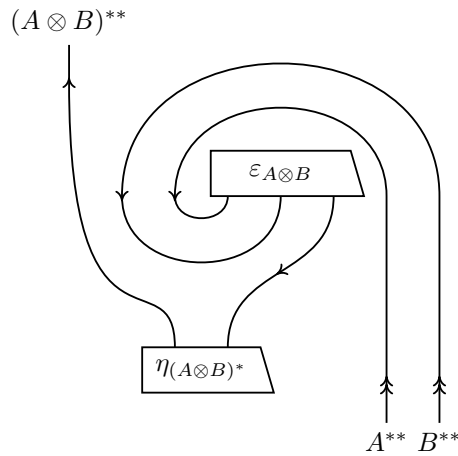
Example 3.13. Let's see how the right duals functor acts for our example categories, with chosen right duals as given by Example 3.2.

- In **FVect** and **FHilb**, the right dual of a morphism $V \xrightarrow{f} W$ is $W^* \xrightarrow{f^*} V^*$, acting as $f^*(e) := e \circ f$, where $W \xrightarrow{e} \mathbb{C}$ is an arbitrary element of W^* .
- In **Mat $_{\mathbb{C}}$** , the dual of a matrix is its transpose.
- In **Rel**, the dual of a relation is its converse. So the right duals functor and the dagger functor have the same action: $R^* = R^\dagger$ for all relations R .

The right-duals functor is involutive: applying it twice is naturally isomorphic to the identity.

Lemma 3.14. For a monoidal category with chosen right duals for objects, $A^{**} \otimes B^{**} \simeq (A \otimes B)^{**}$.

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



This finishes the proof. □

Abstract teleportation

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

(3.17)

It makes use of a duality $L \dashv R$ witnessed by morphisms $I \xrightarrow{\eta} R \otimes L$ and $L \otimes R \xrightarrow{\epsilon} I$, and a unitary morphism $L \xrightarrow{U} L$. The dashed box around part of the diagram indicates that we will treat it as a single effect. Let's describe this history in words:

1. Begin with a single system L .
2. Independently, prepare a joint system $R \otimes L$ in the state η , resulting in a total system $L \otimes (R \otimes L)$.
3. Perform a joint measurement on the first two systems, with a result given by the effect $\varepsilon \circ (\text{id}_L \otimes U^*)$.
4. Perform a unitary operation U on the remaining system.

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

$$(3.18)$$

By rotating the box U along the path of the wire, using the unitary property of U , and then using a snake equation to straighten out the wire, we see the history equals the identity. So if the events described in (3.17) come to pass, then the result is for the original system to be transmitted unaltered.

For us to be sure that the state of the system is transmitted correctly, we require that some history of this form necessarily takes place.

Example 3.15. Let's instantiate abstract teleportation in our running example categories.

- We now consider implementing this abstract teleportation in **Hilb**. Choose $L = R = \mathbb{C}^2$ and $\eta^\dagger = \varepsilon = \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}$, and choose the following family of unitaries U_i :

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad (3.19)$$

This gives rise to the following family of effects:

$$\begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & -1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & -1 & 0 \end{pmatrix} \quad (3.20)$$

This is a complete set of effects, since it forms a basis for the vector space $\mathbf{Hilb}(\mathbb{C}^2 \otimes \mathbb{C}^2, \mathbb{C})$. As a result, thanks to the categorical argument, we can implement a teleportation scheme which is guaranteed to be successful whatever result is obtained at the measurement step. This scheme is precisely conventional qubit teleportation.

- We can also implement the abstract teleportation procedure in **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 $2 \rightarrow 2$, as the unitaries are exactly the permutations:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (3.21)$$

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

$$\begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix} \quad (3.22)$$

These form a complete set of effects, since they partition the set. Thus we obtain a correct implementation of the abstract teleportation procedure. This procedure is usually known as *encrypted communication via a one-time pad*.

Compact categories

We will be interested in symmetric monoidal categories with duals.

Definition 3.16. A *compact category* is a symmetric monoidal category where every object has dual.

Example 3.17. Since they are symmetric monoidal categories with duals, our main example categories **FHilb**, **FVect**, **Mat_C**, **Rel** can all be considered compact categories.

When using the graphical calculus, there is now an extra *orientation* on the wires. Lemma 3.8 shows that we need not be careful with loops on a single strand. Here is the correctness theorem making this precise.

Theorem 3.18 (Correctness of the graphical calculus for compact categories). *A well-formed equation between morphisms in a ribbon category follows from the axioms if and only if it holds in the graphical language up to oriented isotopy in four dimensions.*

We could have got by with a bit weaker structure than symmetric monoidal with chosen duals for this theorem. Framed isotopy is the name for the version of isotopy where the strands are thought of as ribbons, rather than just wires. To get a feeling for framed isotopy, find some ribbons, or make some by cutting long, thin strips from a piece of paper. Use them to verify the following equation:

(3.23)

Dagger duality

Lemma 3.19. In a monoidal dagger category, $L \dashv R \Leftrightarrow R \dashv L$.

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

Definition 3.20. In a dagger category that is also a compact category, a *dagger dual* is a duality $A \dashv A^*$ witnessed by morphisms $I \xrightarrow{\eta} A^* \otimes A$ and $A \otimes A^* \xrightarrow{\varepsilon} I$, satisfying the following condition:

(3.24)

A *compact dagger category* is a symmetric monoidal dagger category whose every object has a dagger dual.

Definition 3.21. In a compact dagger category, a *maximally entangled state* is a bipartite state satisfying the following equations:

(3.25)

Lemma 3.22. *In a compact dagger category, a bipartite state is maximally entangled if and only if it is part of a dagger duality.*

Proof. Use the dagger dual condition (3.24) to verify the first equation of (3.25):

(3.26)

The central isotopy here is a bit hard to see; the box ε makes a full rotation. The other equation, and the reverse implication, can be proved in a similar way. \square

Lemma 3.23. *In a compact dagger category, dagger duals are unique up to unique unitary isomorphism.*

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

(3.27)

The following calculation establishes that this is a co-isometry:

As with the previous proof, the central isotopy here is a bit tricky to see; the η' morphism performs a full anticlockwise rotation. Similarly, it can be shown that equation (3.27) is also an isometry, and hence unitary. Uniqueness is straightforward. \square

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

Theorem 3.24. In a compact dagger category, for any two maximally entangled states $I \xrightarrow{\eta, \eta'} A \otimes B$ there is a unique unitary $A \xrightarrow{f} A$ satisfying the following equation:

$$\begin{array}{c} \text{---} \\ | \\ \boxed{f} \\ | \\ \boxed{\eta} \end{array} = \begin{array}{c} \text{---} \\ | \\ \boxed{\eta'} \\ | \\ \text{---} \end{array} \quad (3.28)$$

Proof. This follows from Lemmas 3.22 and 3.23. □

Lemma 3.25. In a pivotal dagger category, every morphism f satisfies the following equation:

$$(f^*)^\dagger = (f^\dagger)^* \quad (3.29)$$

Proof. Compute both sides:

$$\begin{array}{c} \downarrow \\ \boxed{(f^*)^\dagger} \\ \downarrow \end{array} = \left(\begin{array}{c} \downarrow \\ \boxed{f} \\ \downarrow \end{array} \right)^\dagger = \begin{array}{c} \downarrow \\ \boxed{f} \\ \downarrow \end{array} \quad (3.30)$$

$$\begin{array}{c} \downarrow \\ \boxed{(f^\dagger)^*} \\ \downarrow \end{array} = \begin{array}{c} \downarrow \\ \boxed{f} \\ \downarrow \end{array} \quad (3.31)$$

These are isotopic, and hence equal by the correctness theorem. □

Definition 3.26. On a pivotal dagger category, *conjugation* $(-)_*$ is defined as the composite of the dagger functor and the right-duals functor:

$$(-)_* := (-)^*\dagger = (-)^\dagger* \quad (3.32)$$

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

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

$$\begin{array}{c} \downarrow \\ \boxed{f} \\ \downarrow \end{array} := \begin{array}{c} \downarrow \\ \boxed{f_*} \\ \downarrow \end{array} \quad (3.33)$$

Example 3.27. Our examples **FHilb**, **Mat_C** and **Rel** are all compact dagger categories.

- On **FHilb**, the conjugation functor gives the conjugate of a linear map.
- On **Mat_C**, the conjugation functor gives the conjugate of a matrix, with each matrix entry replaced by its conjugate as a complex number.
- On **Rel**, the conjugation functor is the identity.

3.2 Traces and dimensions

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

Definition 3.28 (Trace). In a compact dagger category, the *trace* of a morphism $A \xrightarrow{f} A$ is the following scalar:


(3.34)

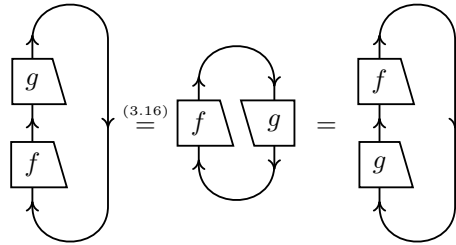
It is denoted by $\text{Tr}(f)$, or sometimes $\text{Tr}_A(f)$ to emphasize A . (Don't confuse it with the partial trace of quantum theory.)

Definition 3.29. In a compact dagger category, the *dimension* of an object A is the scalar $\dim(A) := \text{Tr}(\text{id}_A)$.

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

Lemma 3.30. In a compact dagger category, morphisms $A \xrightarrow{f} B$ and $B \xrightarrow{g} A$ satisfy $\text{Tr}_A(g \circ f) = \text{Tr}_B(f \circ g)$.

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


(3.35)

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

Example 3.31. To determine $\text{Tr}(f)$ for a morphism $H \xrightarrow{f} H$ in \mathbf{FHilb} , substitute equations (3.7) and (3.6) into the definition of the abstract trace (3.34). Then $\text{Tr}(f) = \sum_i \langle i | f | i \rangle$, so the abstract trace of f is in fact the usual trace of f from linear algebra. Therefore, for an object H of \mathbf{FHilb} , also $\dim(H) = \text{Tr}(\text{id}_H)$ equals the usual dimension of H .

Abstract traces satisfy many properties familiar from linear algebra.

Lemma 3.32. In a compact dagger category, the trace has the following properties:

- (a) $\text{Tr}_I(s) = s$;
- (b) $\text{Tr}_{A \otimes B}(f \otimes g) = \text{Tr}_A(f) \circ \text{Tr}_B(g)$ in a braided pivotal category;
- (c) $(\text{Tr}_A(f))^\dagger = \text{Tr}_A(f^\dagger)$ in a dagger pivotal category.

Proof. Property (a) follows from $\text{Tr}_I(s) = s \bullet \text{id}_I = s$, which trivializes graphically. Property (b) follows because the traces over A and B can separate in a braided monoidal category; the inner one is not trapped by the outer one. Finally, property (c) follows from correctness of the graphical language for dagger pivotal categories. □

This immediately yields some properties of dimensions of objects.

Lemma 3.33. *In a compact dagger category, the following properties hold:*

- (a) $\dim(I) = \text{id}_I$;
- (b) $\dim(A \otimes B) = \dim(A) \circ \dim(B)$.
- (c) $A \simeq B \Rightarrow \dim(A) = \dim(B)$;

Proof. Properties (a) and (b) are straightforward consequences of Lemma 3.32. Property (c) follows from the cyclic property of the trace demonstrated in Lemma 3.30: if $A \xrightarrow{k} B$ is an isomorphism, then $\dim(A) = \text{Tr}_A(k^{-1} \circ k) = \text{Tr}_B(k \circ k^{-1}) = \dim(B)$. \square

In a similar way, we can prove that if a category had coinciding products and coproducts (like the direct sum of Hilbert spaces), then $\text{Tr}_{A \oplus B} \begin{pmatrix} f & g \\ h & j \end{pmatrix} = \text{Tr}_A(f) + \text{Tr}_B(j)$. This gives a simple argument that infinite-dimensional Hilbert spaces cannot have duals.

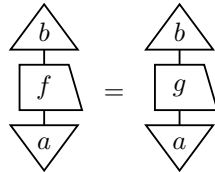
Corollary 3.34. *Infinite-dimensional Hilbert spaces do not have duals.*

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 this would imply $\dim(H) + 1 = \dim(H)$, which has no solutions for $\dim(H) \in \mathbb{C}$. \square

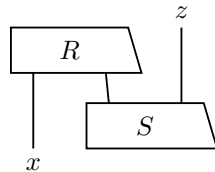
This argument would not apply in **Rel**, since we have $\text{id}_1 + \text{id}_1 = \text{id}_1$ in that category. And indeed, as we have seen at the beginning of this chapter, both finite and infinite sets are self-dual in this category, despite the fact that sets S of infinite cardinality can be equipped with isomorphisms $S \simeq S \cup 1$.

3.3 Information flow

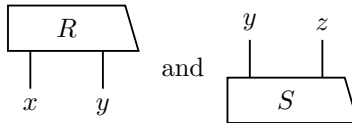
In a monoidal dagger category, we may think of the wires in the graphical calculus carrying information flow as follows. If the category is well-pointed, two morphisms $A \xrightarrow{f,g} B$ are equal if and only if for all points $I \xrightarrow{a} A$ and $I \xrightarrow{b} B$ the following two scalars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



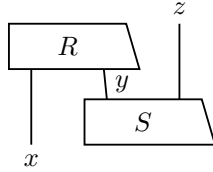
So we could verify an equation by computing the ‘matrix entries’ of both sides. In the category **Rel** is convenient to do this by decorating the wires with elements. For example, the scalar



is 1 if and only if there exists an element y such that both the scalars



are 1; remember that the scalars in **Rel** are Boolean truth values $\{0, 1\}$. Thus we can decorate



to signify that if element x is connected to z by this composite morphism, then it must ‘flow’ through some element y in the middle. In the category **FHilb**, however, this intuition runs into (destructive) interference. For example, if $g = \begin{pmatrix} -1 & -1 \\ 1 & 1 \end{pmatrix}$, $f = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, and $x = z = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, the scalar

$$\begin{array}{c} z \\ \downarrow \\ \boxed{g} \\ \downarrow \\ \boxed{f} \\ \downarrow \\ x \end{array} = \begin{array}{c} (1 \ 0) \\ \downarrow \\ \boxed{g} \\ \downarrow \\ x \end{array} \begin{array}{c} z \\ \downarrow \\ \boxed{f} \\ \downarrow \\ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{array} + \begin{array}{c} (0 \ 1) \\ \downarrow \\ \boxed{g} \\ \downarrow \\ x \end{array} \begin{array}{c} z \\ \downarrow \\ \boxed{f} \\ \downarrow \\ \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{array} = -4 + 4 = 0$$

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

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 3.35. *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

$$\begin{array}{c} \uparrow \\ | \\ \uparrow L \end{array} = \begin{array}{c} \uparrow \\ \curvearrowright \\ \uparrow \end{array} = \begin{array}{c} \uparrow \\ \curvearrowright \\ \downarrow \\ \triangleleft r \end{array} \begin{array}{c} \downarrow \\ \triangleleft l \end{array} = \begin{array}{c} \triangleleft l \\ \downarrow \\ \triangleleft r \end{array}$$

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 $\pi : S \rightarrow S$ 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 dual objects give us maximally entangled joint states in **Hilb**, and one-time pads in **Rel**.

Categories and Quantum Informatics: Monoids and comonoids

Chris Heunen

Spring 2018

The tensor product of a monoidal category allows us to consider multiplications on its objects, leading to the notion of a monoid. In fact, this notion is so important, that one can almost say the entire reason for defining monoidal categories is that one can define monoids in them. We investigate such structures in Section 4.1, and their relation to dual objects. We also consider comonoids, whose operation is something like copying. Classical information can be copied and deleted, whereas quantum information cannot. This leads to big differences between classical and quantum information; we think of a classical system as a quantum one equipped with special morphisms that copy and delete the information it carries. We prove categorical no-deleting and no-cloning theorems in Sections 4.1 and 4.2, showing that if these structures are able to copy and delete every state of the system, then the category collapses. Finally, we characterize when a tensor product is a categorical product in Section 4.3.

4.1 Monoids and comonoids

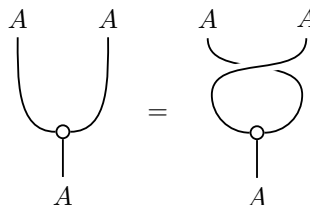
Let's start by making the notions of copying and deleting more precise in our setting of monoidal categories.

Comonoids

Clearly, copying should be an operation of type $A \xrightarrow{d} A \otimes A$. As we will be using this morphism a lot, we will draw it as follows rather than with a generic box:

(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)

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

Secondly, if we make a third copy, it shouldn't matter if we start from the first or the second copy. We can formulate this as $\alpha_{A,A,A} \circ (d \otimes \text{id}_A) \circ d = (\text{id}_A \otimes d) \circ d$, 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 $\rho_A \circ (\text{id}_A \otimes e) \circ d = \text{id}_A$ and $\text{id}_A = \lambda_A \circ (e \otimes \text{id}_A) \circ d$. Graphically:

(4.4)

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

Definition 4.1 (Comonoid). A *comonoid* in a monoidal category is a triple (A, φ, ρ) of an object A and morphisms $\varphi: A \rightarrow A \otimes A$ and $\rho: A \rightarrow I$ satisfying equations (4.3) and (4.4). If the monoidal category is braided and equation (4.2) holds, the comonoid is called *cocommutative*.

The morphism φ is called the *comultiplication*, and ρ is called the *counit*. Properties (4.3) and (4.4) are *coassociativity* and *counitality*.

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

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

- In **Rel**, any group G forms a comonoid with comultiplication $g \sim (h, h^{-1}g)$ for all $g, h \in G$, and counit $1 \sim \bullet$. To see counitality, for example, notice that the left-hand side of (4.4) is the relation $g \sim h$ where $h^{-1}g = 1$, and the right-hand side is $g \sim 1^{-1}g$; that is, both equal the identity $g \sim g$.

The comonoid is cocommutative when the group is abelian. The left-hand side of (4.2) is $g \sim (h, h^{-1}g)$ for all $h \in G$, whereas the right-hand side is $g \sim (k, k^{-1}g)$ for all $k \in G$. But if $k = h^{-1}g$, then $k^{-1}g = g^{-1}hg = h$ when G is abelian, so that left and right-hand sides are equal.

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

Monoids

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

Definition 4.3 (Monoid). A *monoid* in a monoidal category is a triple $(A, \blacktriangleright, \bullet)$ of an object A , a morphism $\blacktriangleright: A \otimes A \rightarrow A$, and a state $\bullet: I \rightarrow A$, satisfying the following two equations called *associativity* and *unitarity*:

(4.5)

(4.6)

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

(4.7)

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

Example 4.4. There are many examples of monoids:

- The tensor unit I in any monoidal category can be equipped with the structure of a monoid, with $m = \rho_I (= \lambda_I)$ and $u = \text{id}_I$.
- A monoid in **Set** gives the ordinary mathematical notion of a monoid. Any group is an example.
- A monoid in **Vect** is called an *algebra*. The multiplication is a linear function $A \otimes A \xrightarrow{m} A$, corresponding to a bilinear function $A \times A \rightarrow A$. Hence an algebra is a set where we can not only add vectors and multiply vectors with scalars, but also multiply vectors with each other in a bilinear way. For example, \mathbb{C}^n forms an algebra under pointwise multiplication; the unit is the vector $(1, 1, \dots, 1)$. For another example, the vector space of complex n -by- n matrices \mathbb{M}_n forms an algebra under matrix multiplication.

We have used a black dot for the comonoid structures and a white dot for the monoid structures, but that is not essential: we will just make sure to use different colours to differentiate structures as the need arises. Later on we will use monoids and comonoids for which the multiplication is the adjoint of the comultiplication, and the unit is the adjoint of the counit, and in that case we will use the same colour dots for all of these structures.

Combining monoids

Given a monoidal category, we can build a new category whose objects are comonoids, with the following morphisms.

Definition 4.5. A *comonoid homomorphism* from a comonoid (A, d, e) to a comonoid (A', d', e') is a morphism $A \xrightarrow{f} A'$ such that $(f \otimes f) \circ d = d' \circ f$ and $e' \circ f = e$. These equations have the following graphical representations:

(4.8)

(4.9)

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

Example 4.6. Consider again the comonoids of Example 4.2.

- In **Set**, any function $f: A \rightarrow B$ is a comonoid homomorphism: by definition $(f \times f)(a, a) = (f(a), f(a))$, and $A \xrightarrow{f} B \rightarrow I$ equals the unique function $A \rightarrow I$.
- In **Rel**, any surjective homomorphism $f: G \rightarrow H$ of groups is a comonoid homomorphism. The left-hand side of (4.8) is the relation $g \sim (h, h^{-1}f(g))$ for $h \in H$, and the right-hand side is $g \sim (f(g'), f(g')^{-1}f(g))$. Since f is surjective, any $h \in H$ is of the form $f(g')$ for some $g' \in G$, making both sides equal. Similarly, both sides of (4.9) come down to the relation $1 \sim f(1) = 1$.
- In **FHilb**, any function $f: \{d_i\} \rightarrow \{e_j\}$ between bases extends linearly to a comonoid homomorphism between the Hilbert spaces they span. Almost by definition $d(f(d_i)) = f(d_i) \otimes f(d_i)$ and $e(f(d_j)) = 1 = e(d_j)$.

We can define a monoid homomorphism in a similar way.

Definition 4.7 (Monoid homomorphism). In a monoidal category, a *monoid homomorphism* from a monoid (A, m, u) to a monoid (A', m', u') is a morphism $A \xrightarrow{f} A'$ such that $f \circ m = m' \circ (f \otimes f)$ and $u' = f \circ u$. These equations have the following graphical representations:

(4.10)

$$\begin{array}{c} | \\ \boxed{f} \\ | \\ \bullet \end{array} = \begin{array}{c} | \\ \bullet \end{array} \quad (4.11)$$

Again we can use this notion to form a category, whose objects are monoids and whose morphisms are monoid homomorphisms.

In a braided monoidal category we can combine two comonoids to give a single comonoid on the tensor product object, as the following lemma shows.

Lemma 4.8 (Product comonoid). *In a braided monoidal category, given a pair of comonoids, we can produce a new comonoid with the following multiplication and counit:*

$$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \bullet \quad \circ \\ | \quad | \end{array} = \begin{array}{c} \bullet \quad \circ \\ | \quad | \end{array} \quad (4.12)$$

Proof. The two comonoid structures are just sitting on top of each other, and the coassociativity and counitality properties of the original comonoids are inherited by the new composite structure. \square

In the case that the braiding is a symmetry, this gives the actual categorical product of comonoids in the category of cocommutative comonoids and comonoid homomorphisms.

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

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

- The product comonoid on sets A and B in **Set** is simply the unique comonoid on $A \times B$.
- The product comonoid of groups G and H in **Rel** is the comonoid of the product group $G \times H$ with multiplication $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$.
- The product of comonoids on Hilbert spaces H and K in **FHilb** that copy orthonormal bases $\{d_i\}$ and $\{e_j\}$ is the comonoid that copies the orthonormal basis $\{d_i \otimes e_j\}$ of $H \otimes K$.

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

Lemma 4.10. *If (A, d, e) is a comonoid in a monoidal dagger category, then $(A, d^\dagger, e^\dagger)$ is a monoid.*

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

The previous lemma shows that Examples 4.2 and 4.4 are related by taking daggers in **Rel**. Taking daggers in **Rel** constructs converse relations, and applying this to Example 4.2 turns the comultiplication $G \xrightarrow{d} G \times G$ given by $g \sim (h, h^{-1}g)$ for a group G into the multiplication $G \times G \xrightarrow{m} G$ given by $(g, h) \sim gh$.

Monoids of operators

One of the most important features of matrices is that they can be multiplied. In other words, linear maps $\mathbb{C}^n \rightarrow \mathbb{C}^n$ can be composed. Using the closure properties of the previous subsection we can *internalize* this, to see that the vector space \mathbb{M}_n of Example 4.4 is actually a monoid that lives in the same category as \mathbb{C}^n .

More generally, if an object A in a monoidal category has a dual A^* , then operators $A \xrightarrow{f} A$ correspond bijectively to states $I \xrightarrow{\ulcorner f \urcorner} A^* \otimes A$. Composition $A \xrightarrow{g \circ f} A$ of operators transfers to states $I \xrightarrow{\ulcorner g \circ f \urcorner} A^* \otimes A$:

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

Lemma 4.11. *If $A \dashv A^*$ are dual objects in a monoidal category, then $A^* \otimes A$ is a monoid, with multiplication and unit defined as follows:*

(4.13)

Proof. Straightforward graphical manipulation shows:

Hence this definition satisfies unitality and associativity. □

Example 4.12. The pair of pants algebra on the object \mathbb{C}^n in the category **FHilb** is the algebra \mathbb{M}_n of n -by- n matrices under matrix multiplication.

Proof. Fix an orthonormal basis $\{|i\rangle\}$ for $A = \mathbb{C}^n$, so that an orthonormal basis of $A^* \otimes A$ is given by $\{|j\rangle \otimes |i\rangle\}$. Define a linear function $A^* \otimes A \rightarrow \mathbb{M}_n$ by mapping $|j\rangle \otimes |i\rangle$ to the matrix e_{ij} , which has a single entry 1 on row i and column j and zeroes elsewhere. This is clearly a bijection. Furthermore, it respects multiplication; using the decorated notation from Section 3.3:

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

Pair of pants monoids are universal, in the sense that any monoid embeds into a pair of pants monoid.

Proposition 4.13. *In a monoidal category, for a monoid (A, \cdot, \circ) and a duality $A \dashv A^*$, there is a monoid homomorphism $R : (A, \cdot, \circ) \rightarrow (A^* \otimes A, \cdot, \circ)$ with a retraction.*

(4.14)

Proof. The morphism R preserves units:

It also preserves multiplication:

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

This finishes the proof. □

4.2 Uniform deleting and copying

Uniform deleting

The counit $A \xrightarrow{e} I$ of a comonoid A tells us we can ‘forget’ about A if we want to. In other words, we can delete the information contained in A . It is perfectly possible to delete individual systems like this. The no-deleting theorem only prohibits a systematic way of deleting arbitrary systems.

What happens when *every* object in our category can be deleted *systematically*? In our setting, deleting systematically means that the deleting operations respect the categorical structure. This means that deleting is *uniform*, in the sense that it doesn’t matter if we delete something right away, or first process it for a while and then delete the result. In that case, we can say something quite dramatic. Let us first make uniform deleting precise.

Definition 4.14 (Uniform deleting). A category has *uniform deleting* if there is a natural transformation $A \xrightarrow{e_A} I$ with $e_I = \text{id}_I$.

Naturality of e_A here means that $e_B \circ f = e_A$ for any morphism $A \xrightarrow{f} B$. This is already strong enough to imply that any monoidal category whose tensor unit I is terminal, such as **Set**, has uniform deleting.

Proposition 4.15. *A category \mathbf{C} has uniform deleting if and only if I is terminal.*

Proof. Uniform deleting gives a morphism $A \xrightarrow{e_A} I$ for each object A . Naturality and $e_I = \text{id}_I$ then imply that any morphism $A \xrightarrow{f} I$ must equal e_A :

$$\begin{array}{ccc} A & \xrightarrow{e_A} & I \\ f \downarrow & & \downarrow \text{id}_I \\ I & \xrightarrow{e_I = \text{id}_I} & I \end{array}$$

Conversely, if I is terminal, we can define $A \xrightarrow{e_A} I$ as the unique morphism of that type. This will automatically satisfy naturality as well as $e_I = \text{id}_I$. \square

To further justify calling the notion of Definition 4.14 deleting, we now observe that it deletes states.

Definition 4.16 (Deletable state). A state $I \xrightarrow{u} A$ of an object A in a monoidal category with a deleting map $A \xrightarrow{e_A} I$ is *deletable* when:

$$\begin{array}{c} \boxed{e_A} \\ \downarrow \\ \nabla u \end{array} = \quad (4.15)$$

Corollary 4.17. *Consider a monoidal category with maps $A \xrightarrow{e_A} I$ for each object A . If the maps e_A provide uniform deleting, then any state is deletable. The converse holds when the category is well-pointed.*

Proof. If there is uniform deleting, then $e_A \circ u = \text{id}_I$ for each state $I \xrightarrow{u} A$ by Proposition 4.15.

Now suppose that the category is well-pointed, and let $A \xrightarrow{f} I$ and $A \xrightarrow{g} I$ be morphisms. By Proposition 4.15 it suffices to show that $f \circ u = g \circ u$ for any state $I \xrightarrow{u} A$. Both are states of I , so $e_I \circ f \circ u = \text{id}_I = e_I \circ g \circ u$. That is, both scalars $f \circ u$ and $g \circ u$ are inverse to the scalar e_I , and hence must be equal: $f \circ u = g \circ u \circ e_I \circ f \circ u = g \circ u$. \square

The no-deleting theorem below will show that uniform deleting has significant effects in a compact category. Namely, the category must collapse, in the following sense.

Definition 4.18 (Preorder). A *preorder* is a category that has at most one morphism $A \rightarrow B$ for any pair of objects A, B .

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

Theorem 4.19 (No deleting). *If a compact category has uniform deleting, then it must be a preorder.*

Proof. By Proposition 4.15, the tensor unit I is terminal. So any two parallel morphisms $A \xrightarrow{f, g} B$ must have the same coname $\lrcorner f \lrcorner = \lrcorner g \lrcorner$, whence $f = g$. \square

Uniform copying

We now move to uniform copying. The comultiplication $A \xrightarrow{d} A \otimes A$ of a comonoid lets us copy the information contained in one object A . What happens if we have this ability for all objects, systematically? In this section we will prove a categorical no-cloning theorem, showing that compact categories with uniform copying must degenerate.

Uniform deleting meant deleting something straight away is the same as processing it for a while first and then deleting the result. We want a similar definition to say that a copying procedure is uniform. It shouldn't matter whether we copy something first and then process both copies, or process the original first and then copy the result. This amounts to naturality of the comultiplication: it must respect composition.

Moreover, we want these copying maps to respect the tensor product: copying a compound object should be the same as copying both constituents. The following definition makes this precise, using Lemma 4.8 for compound objects.

Definition 4.20 (Uniform copying). A braided monoidal category has *uniform copying* if there is a natural transformation $A \xrightarrow{d_A} A \otimes A$ with $d_I = \rho_I^{-1}$, satisfying equations (4.2) and (4.3), and making the following diagram commute for all objects A, B .

$$(4.16)$$

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

$$(4.17)$$

Example 4.21. The monoidal category **Set** has uniform copying. The copying maps $A \xrightarrow{d_A} A \times A$ given by $a \mapsto (a, a)$ fit the bill: $d_1(\bullet) = (\bullet, \bullet) = \rho_1(\bullet)$, and both sides of (4.16) are the function $A \times B \rightarrow A \times B \times A \times B$ given by $(a, b) \mapsto (a, b, a, b)$.

Here are some more examples.

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

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

Example 4.23. A braided monoidal category that is discrete generally cannot have uniform copying: unless $A \otimes A = A$, there is no morphism $A \rightarrow A \otimes A$ whatsoever. A braided monoidal category that is indiscrete always has uniform copying: any equation between well-typed morphisms holds because there is only a single morphism of that type, and the copying map d_A can simply be taken to be the unique morphism $A \rightarrow A \otimes A$.

To justify calling the notion of Definition 4.20 copying, we now observe that it actually copies states.

Definition 4.24 (Copyable state). A state $I \xrightarrow{u} A$ of an object A in a braided monoidal category with a copying map $A \xrightarrow{d_A} A \otimes A$ is *copyable* when:

$$(4.18)$$

Proposition 4.25. Consider a braided monoidal category equipped with maps $A \xrightarrow{d_A} A \otimes A$ for each object A . If the maps d_A provide uniform copying, then any state is copyable. The converse holds when the category is monoidally well-pointed.

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

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

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

because any state $I \xrightarrow{v} A$ is copyable. Finally, we have to verify equation (4.16). This is where we need monoidal well-pointedness, rather than mere well-pointedness:

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

Hence our definition of uniform copying coincides with the usual one in monoidally well-pointed categories such as **Set**, **Rel**, and **Hilb**. Definition 4.20 is more general and makes sense for non-well-pointed categories, too.

No-cloning

You might have expected Example 4.21: in classical physics, as modeled in **Set**, you *can* uniformly copy states. The no-cloning theorem says something about quantum physics, which we have modeled by compact categories, which **Set** is not. Uniform copying on a compact category turns out to be a drastic restriction. It means that the category degenerates: it must have trivial dynamics, in the sense that up to scalars there is only one operator $A \rightarrow A$ on each object A . To prove this categorical no-cloning theorem, we start with a preparatory lemma.

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

$$\begin{array}{c} A^* \quad A \\ \frown \\ \end{array} \quad \begin{array}{c} A^* \quad A \\ \frown \\ \end{array} = \begin{array}{c} A^* \quad A \quad A^* \quad A \\ | \quad | \quad | \quad | \\ \quad \text{loop} \quad \\ | \quad | \quad | \quad | \end{array} \quad (4.19)$$

Proof. First, consider the following equalities:

$$\begin{array}{c} A^* \quad A \\ \frown \\ \end{array} \quad \begin{array}{c} A^* \quad A \\ \frown \\ \end{array} \stackrel{(4.17)}{=} \begin{array}{c} A^* \quad A \\ \frown \\ \end{array} \quad \begin{array}{c} A^* \quad A \\ \frown \\ \end{array} \stackrel{(4.17)}{=} \begin{array}{c} A^* \quad A \quad A^* \quad A \\ | \quad | \quad | \quad | \\ \text{trapezoid } d_{A^* \otimes A} \\ | \quad | \end{array} \stackrel{(4.16)}{=} \begin{array}{c} A^* \quad A \quad A^* \quad A \\ | \quad | \quad | \quad | \\ \text{trapezoid } d_{A^*} \quad \text{trapezoid } d_A \\ | \quad | \end{array} \quad (4.20)$$

Then we can use this as follows:

$$\begin{array}{c} A^* \quad A \\ \frown \\ \end{array} \quad \begin{array}{c} A^* \quad A \\ \frown \\ \end{array} \stackrel{(4.20)}{=} \begin{array}{c} A^* \quad A \quad A^* \quad A \\ | \quad | \quad | \quad | \\ \text{trapezoid } d_{A^*} \quad \text{trapezoid } d_A \\ | \quad | \end{array} \stackrel{(4.2)}{=} \begin{array}{c} A^* \quad A \quad A^* \quad A \\ | \quad | \quad | \quad | \\ \text{trapezoid } d_{A^*} \quad \text{trapezoid } d_A \\ | \quad | \end{array} \stackrel{(4.20)}{=} \begin{array}{c} A^* \quad A \quad A^* \quad A \\ | \quad | \quad | \quad | \\ \text{loop} \\ | \quad | \quad | \quad | \end{array}$$

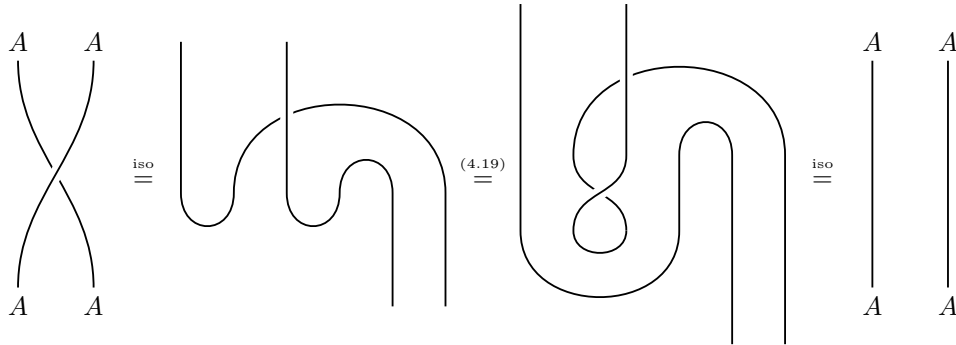
This completes the proof. □

The previous lemma already shows the core of the degeneracy, as it equates two morphisms with different connectivity. We can now prove the no-cloning theorem.

Proposition 4.27. *In a braided monoidal category with duals and uniform copying, the braiding is the identity:*

$$\begin{array}{c} A \quad A \\ \text{cross} \\ A \quad A \end{array} = \begin{array}{c} A \quad A \\ | \quad | \\ A \quad A \end{array} \quad (4.21)$$

Proof. We show this as follows:



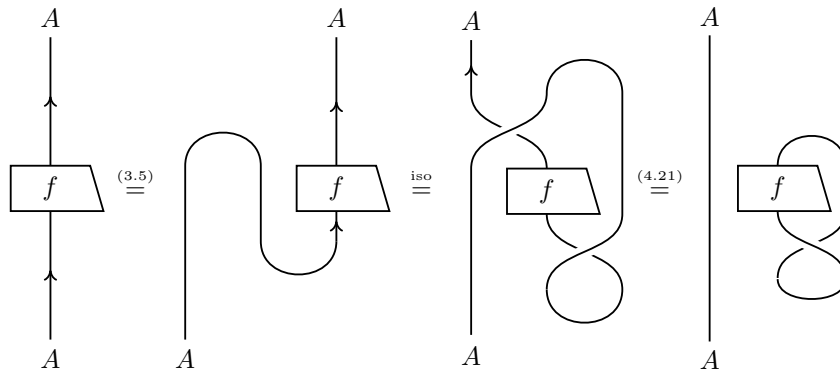
This completes the proof. □

Theorem 4.28 (No cloning). *If a braided monoidal category with duals has uniform copying, then every endomorphism is a scalar multiple of the identity:*

$$\begin{array}{c} \text{---} \\ | \\ \boxed{f} \\ | \\ \text{---} \end{array} = \left| \begin{array}{c} \text{---} \\ | \\ \boxed{f} \\ | \\ \text{---} \\ \text{---} \\ | \\ \text{---} \end{array} \right. \quad (4.22)$$

Notice that the scalar is $\text{Tr}(f)$.

Proof. Perform the following calculation:



This completes the proof. □

While highly degenerate, such categories are not necessarily trivial.

4.3 Products

Let's forget about duals for this section. What happens when a symmetric monoidal category has both uniform copying and deleting? When the copying and deletion operations form comonoids, it turns out that the tensor product is an actual categorical product.

Categories and Quantum Informatics: Frobenius structures

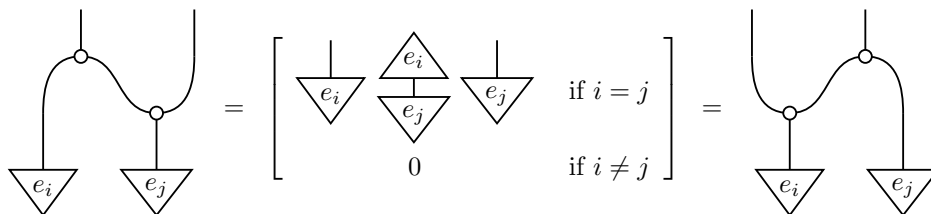
Chris Heunen

Spring 2018

In this chapter we deal with Frobenius structures: a monoid and a comonoid that interact according to the so-called Frobenius law. Section 5.1 studies its basic consequences. It turns out that the graphical calculus is very satisfying for Frobenius structures, and we prove that any diagram built up from Frobenius structures is equal to one of a very simple normal form in Section 5.2. The Frobenius law itself is justified as a coherence property between daggers and closure of a compact category in Section 5.3. We classify all Frobenius structures in **FHilb** and **Rel** in Section 5.4: in the former they come down to operator algebras, in the latter they become groupoids. Of special interest is the commutative case, as in **FHilb** this corresponds to a choice of orthonormal basis. This gives us a way to copy and delete classical information purely in terms of tensor products. Frobenius structures also allow us to discuss phase gates and the state transfer protocol in Section 5.5.

5.1 Frobenius structures

If $\{e_i\}$ is an orthogonal basis for a finite-dimensional Hilbert space H , then the copying map $\varphi: e_i \mapsto e_i \otimes e_i$ is the comultiplication of a comonoid; see Example 4.2. The adjoint multiplication ψ is the comparison map given by $e_i \otimes e_i \mapsto \langle e_i | e_i \rangle e_i$ and $e_i \otimes e_j \mapsto 0$ for $i \neq j$. These copying and comparison maps cooperate in the following way:



This type of behaviour between a monoid and a comonoid is called the *Frobenius law*. In this commutative case it means that it doesn't matter whether we compare something with a copy or with the original. We now proceed straight away with the general definition, leaving its justification to Section 5.3.

Definition 5.1 (Frobenius structure via diagrams). In a monoidal category, a *Frobenius structure* is a pair of a comonoid (A, φ, ψ) and a monoid (A, μ, ν) satisfying the following equation, called the *Frobenius law*:

(5.1)

We already saw that any choice of orthogonal basis induces a Frobenius structure in **FHilb**, but there are many other examples.

Example 5.2 (Group algebra). Any finite group G induces a Frobenius structure in **FHilb**. Let A be the Hilbert space of linear combinations of elements of G with its standard inner product. In other words, A has G as an orthonormal basis. Define $\blacktriangleright: A \otimes A \rightarrow A$ by linearly extending $g \otimes h \mapsto gh$, and define $\blacktriangleleft: \mathbb{C} \rightarrow A$ by $z \mapsto z \cdot 1_G$. This monoid is called the *group algebra*. Its adjoint is given by

$$\begin{aligned} \blacktriangleright: A \otimes A &\rightarrow A & g &\mapsto \sum_{h \in G} gh^{-1} \otimes h = \sum_{h \in G} h \otimes h^{-1}g \\ \blacktriangleleft: A &\rightarrow \mathbb{C} & g &\mapsto \begin{cases} 1 & \text{if } g = 1_G \\ 0 & \text{if } g \neq 1_G \end{cases} \end{aligned}$$

This gives a Frobenius structure, because both sides of the Frobenius law (5.1) compute to $\sum_{k \in G} gk^{-1} \otimes kh$ on input $g \otimes h$.

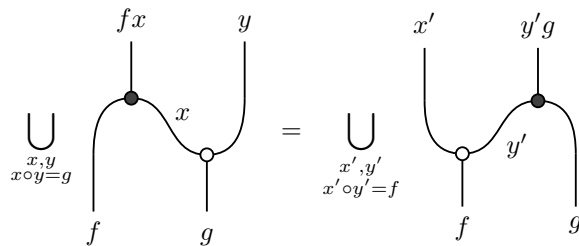
Example 5.3 (Groupoid Frobenius structure). Any group G also induces a Frobenius structure in **Rel**:

$$\begin{aligned} \blacktriangleright &= \{((g, h), gh) \mid g, h \in G\}: G \times G \rightarrow G, \\ \blacktriangleleft &= \{(\bullet, 1_G)\}: 1 \rightarrow G, \end{aligned} \tag{5.2}$$

where \blacktriangleleft is the converse relation of \blacktriangleright , and \blacktriangleleft that of \blacktriangleleft . More generally, any *groupoid* \mathbf{G} induces a Frobenius structure in **Rel** on the set G of all morphisms in \mathbf{G} :

$$\begin{aligned} \blacktriangleright &= \{((g, f), g \circ f) \mid \text{dom}(g) = \text{cod}(f)\}, \\ \blacktriangleleft &= \{(\bullet, \text{id}_x) \mid x \in \text{Ob}(\mathbf{G})\}. \end{aligned} \tag{5.3}$$

where again \blacktriangleleft is the converse relation of \blacktriangleright , and \blacktriangleleft that of \blacktriangleleft . To see that this satisfies the Frobenius law (5.1), evaluate it on arbitrary input (f, g) in the decorated notation of Section 3.3:



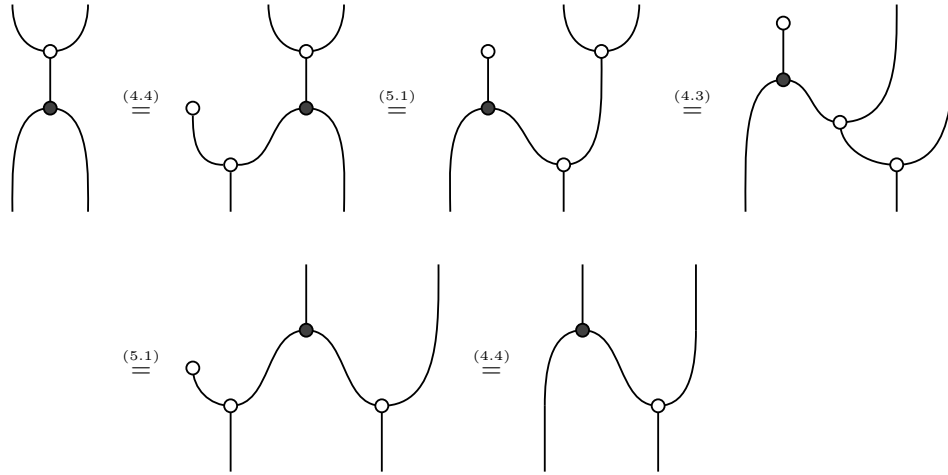
On the left we obtain output $\cup_{x,y \mid x \circ y = g} (f \circ x, y)$, on the right $\cup_{x',y' \mid x' \circ y' = f} (x', y' \circ g)$. Making the change of variables $x' = f \circ x$ and $y' = y \circ g^{-1}$, the condition $x' \circ y' = f$ becomes $f \circ x \circ y \circ g^{-1} = f$, which is equivalent to $x \circ y = g$. So the two composites above are indeed equal, establishing the Frobenius law.

Frobenius structures automatically satisfy a further equality.

Lemma 5.4. *Any Frobenius structure satisfies the following equalities:*

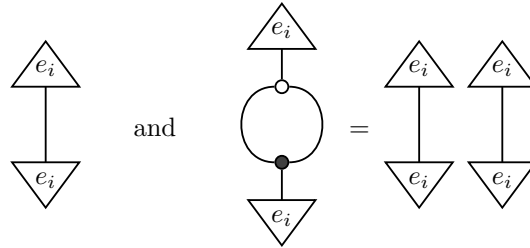
$$\tag{5.4}$$

Proof. We prove one half graphically; the other then follows from the Frobenius law.



These equations use, respectively: counitality, the Frobenius law, coassociativity, the Frobenius law, and counitality. \square

Consider again the Frobenius structure in **FHilb** induced by copying an orthogonal basis $\{e_i\}$. As we saw in Section 2.2, we can measure the squared norm of e_i and its square as:



Thus we can characterize when the orthogonal basis is orthonormal in terms of the Frobenius structure as follows. This extra property, and the Frobenius law, are the only two canonical ways in which a single multiplication and comultiplication can interact.

Definition 5.5. In a monoidal category, a pair consisting of a monoid (A, μ, η) and a comonoid (A, ν, ϵ) is *special* when $\mu \circ \nu$ is a left inverse of $\nu \circ \mu$:

$$\text{Diagram} = \text{Vertical Line} \quad (5.5)$$

Example 5.6. The group algebra of Example 5.2 is only special for the trivial group. The groupoid Frobenius structure of Example 5.3 is always special.

Symmetry and commutativity

In all the examples of Frobenius structures we have seen so far, the comultiplication is the dagger of the multiplication. We will mostly be interested in this compatibility.

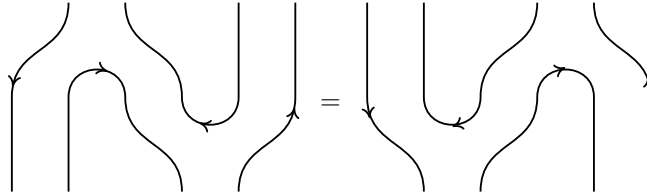
Definition 5.7 (Dagger Frobenius structure). A Frobenius structure $(A, \mu, \nu, \mu', \nu')$ in a monoidal dagger category is a *dagger Frobenius structure* when $\mu = \mu'$ and $\nu = \nu'$.

We call a Frobenius structure *commutative* when its monoid is commutative and its comonoid is cocommutative. For dagger Frobenius structures, this is equivalent to commutativity of the monoid.

Example 5.8. The Frobenius structure in **FHilb** induced by a choice of orthogonal basis is a dagger Frobenius structure. So are the Frobenius structures from Examples 5.2 and 5.3.

Lemma 5.9. *If $A \dashv A^*$ are dagger dual objects in a monoidal dagger category, the pair of pants monoid of Lemma 4.11 is a dagger Frobenius structure.*

Proof. The comultiplication and counit are the upside-down versions of the multiplication and unit. The Frobenius law



is readily verified. □

By Example 4.12, the algebra M_n of n -by- n complex matrices is therefore a dagger Frobenius structure in **FHilb**. We will also specifically be interested in commutative Frobenius structures. For example, the Frobenius structure induced by copying an orthonormal basis is commutative. As it allows us to copy and delete information, we think of this as *classical structure*. Rather than a negative statement about *quantum* objects like in Chapter 4 (“you *cannot* copy them uniformly”, we think of this as a positive statement about *classical* objects (“you *can* copy their classical states”).

Definition 5.10 (Classical structure). A *classical structure* is a dagger Frobenius structure in a braided monoidal dagger category that is special and commutative.

Example 5.11. The groupoid Frobenius structure of Example 5.3 is a classical structure when the groupoid is *abelian*, in the sense that all morphisms are endomorphisms and $f \circ g = g \circ f$ for all endomorphisms f, g of the same object. An abelian groupoid is essentially a list of abelian groups. Notice that abelian groupoids are skeletal.

The pair of pants Frobenius structures from Lemma 5.9 are hardly ever commutative. However, they do satisfy a similar property called *symmetry*.

Definition 5.12 (Symmetric Frobenius structure). In a braided monoidal category, a Frobenius structure is *symmetric* when:

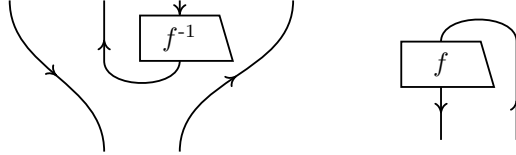
$$\begin{array}{c} \circ \\ | \\ \text{---} \\ | \\ \circ \end{array} = \begin{array}{c} \circ \\ | \\ \text{---} \\ | \\ \circ \end{array} \quad (5.6)$$

Example 5.13. We have already seen examples of symmetric Frobenius structures:

- Pair of pants algebras are always symmetric. In the category **FHilb** this comes down to the fact that the trace of matrices is cyclic: $\text{Tr}(ab) = \text{Tr}(ba)$.
- The group algebra of Example 5.2 is always symmetric. The left-hand side of equation (5.6) sends $g \otimes h$ to 1 if $gh = 1$ and to 0 otherwise. The right-hand side sends $g \otimes h$ to 1 if $hg = 1$ and to 0 otherwise. So this comes down to the fact that inverses in groups are two-sided inverses.

- The groupoid Frobenius structure of Example 5.3 is always symmetric for a similar reason. The left-hand side of (5.6) contains $(g, h) \sim \bullet$ precisely when $g \circ h = \text{id}_B$ for some object B . The right-hand side contains $(g, h) \sim \bullet$ when $h \circ g = \text{id}_A$ for some object A . Both mean that $h = g^{-1}$.

Example 5.14. Here is an example of a Frobenius structure that is not symmetric. Let $A \dashv A^*$ be dual objects in a monoidal category, and let $A^* \xrightarrow{f} A^*$ be an isomorphism such that $\text{id}_{A^*} \otimes f^* \neq f \otimes \text{id}_A$. Consider the pair of pants monoid of Lemma 4.11, take the coname $\lrcorner f \lrcorner : A^* \otimes A \rightarrow I$ of f as counit, and $\text{id}_{A^*} \otimes \lrcorner f^{-1} \lrcorner \otimes \text{id}_A$ as comultiplication.



Proof. The comonoid laws follow just as in Lemma 4.11, and the Frobenius law follows similarly. The left-hand side of (5.6) becomes $\text{id}_{A^*} \otimes f^*$, but the right-hand side becomes $f \otimes \text{id}_A$. This contradicts the assumption, so this Frobenius structure is not symmetric. For example, the condition on f is fulfilled as soon as $\dim(A) \bullet f \neq \text{Tr}(f) \bullet \text{id}_{A^*}$. \square

Self-duality and nondegenerate forms

Let's now consider some properties of general Frobenius structures. First of all, they are closely related to dual objects.

Theorem 5.15 (Frobenius structures have duals). *If $(A, \lrcorner, \lrcorner, \bullet, \bullet)$ is a Frobenius structure in a monoidal category, then $A \dashv A$ is self-dual (in the sense of Definition 3.1) with the following cap and cup:*

$$\begin{array}{c} A & A \\ \cup & \\ \bullet & \end{array} = \begin{array}{c} A & A \\ \cup & \\ \circ & \\ | & \\ \bullet & \end{array} \quad \begin{array}{c} A & A \\ \cap & \\ \circ & \\ | & \\ \bullet & \end{array} = \begin{array}{c} \circ \\ | \\ \bullet \\ \cap & \\ A & A \end{array} \tag{5.7}$$

Proof. We prove the first snake equation (3.5) using the definitions of the cups and caps, the Frobenius law, and unitality and counitality:

$$\begin{array}{c} \text{Snake diagram} \\ \cong \tag{5.7} \\ \text{Diagram with cup and cap} \\ \cong \tag{5.1} \\ \text{Diagram with Frobenius law} \\ \cong \tag{(4.4), (4.6)} \\ \text{Diagram with Frobenius law} \end{array}$$

The other snake equation is proved similarly. \square

It follows from the previous theorem that, if we chose a Frobenius structure on every object in a given monoidal category, then that category would have duals. However, by the no-deleting and no-cloning theorems, we cannot hope to choose this Frobenius structure in a uniform way. But we can use this obstruction contrapositively to motivate Definition 5.10 once more: classical structures are objects that do support copying and deleting.

It also follows from the previous theorem that we could have left out the demand for duals in Definition 5.12. The converse to the previous theorem can be used to characterize Frobenius structures, as in the following lemma.

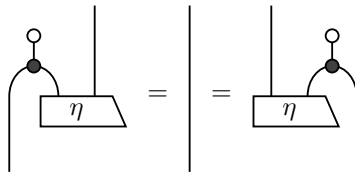
Proposition 5.16 (Frobenius structures by nondegenerate form). *For a monoid $(A, \bullet, \blacktriangleright)$ in a monoidal category there is a bijective correspondence between:*

- comonoids (A, φ', φ) making the pair into a Frobenius structure;
- morphisms $\varphi: A \rightarrow I$ making the composite


(5.8)

the cap of a self-duality $A \dashv A$. Such maps are called nondegenerate forms.

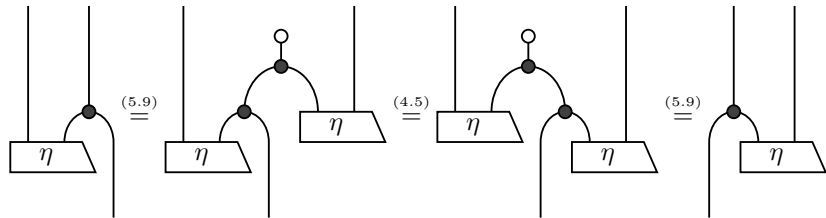
Proof. One direction follows immediately from Theorem 5.15, by taking the counit for the nondegenerate form. For the other direction, suppose we have a monoid $(A, \bullet, \blacktriangleright)$ and a nondegenerate form $\varphi: A \rightarrow I$. That is, there exists a morphism $I \xrightarrow{\eta} A \otimes A$ satisfying the following equations:


(5.9)

Use the map η to define a comultiplication in the following way:

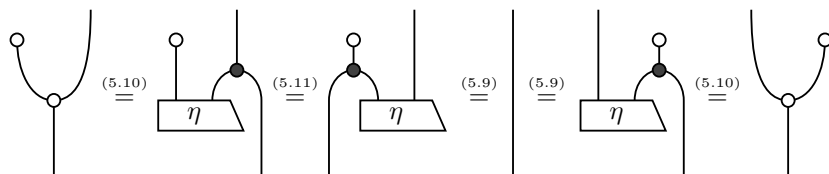

(5.10)

The following computation shows that we could have defined the comultiplication with the η on the left or the right, using the nondegeneracy property, associativity, and the nondegeneracy property again:

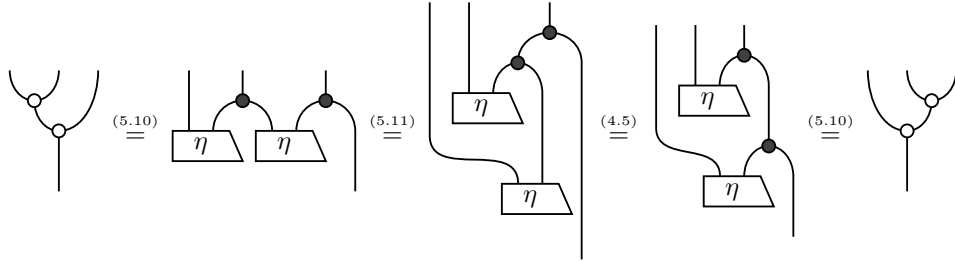

(5.11)

We must show that our new comultiplication satisfies coassociativity and counitality, and the Frobenius law (5.1). For the counit, choose the nondegenerate form.

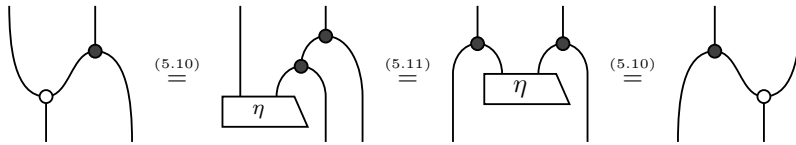
Counitality is the easiest property to demonstrate, using the definition of the comultiplication, symmetry of the comultiplication, nondegeneracy twice, and definition of the comultiplication:



To see coassociativity, we use the definition of the comultiplication, symmetry of the comultiplication, associativity, and the definition of the comultiplication:



Finally, the Frobenius law. Use the definition of the comultiplication, symmetry of the comultiplication, and the definition of the comultiplication again:



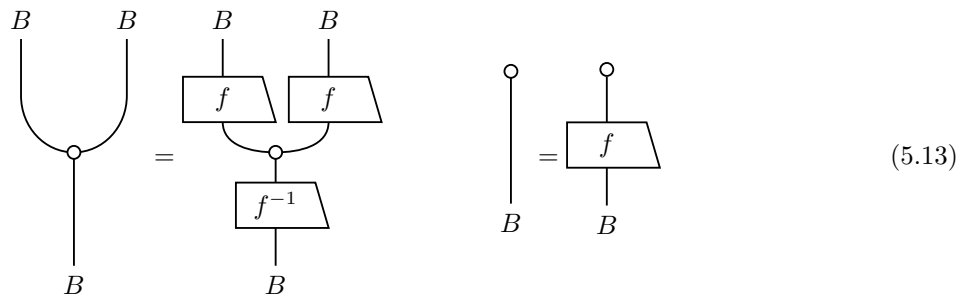
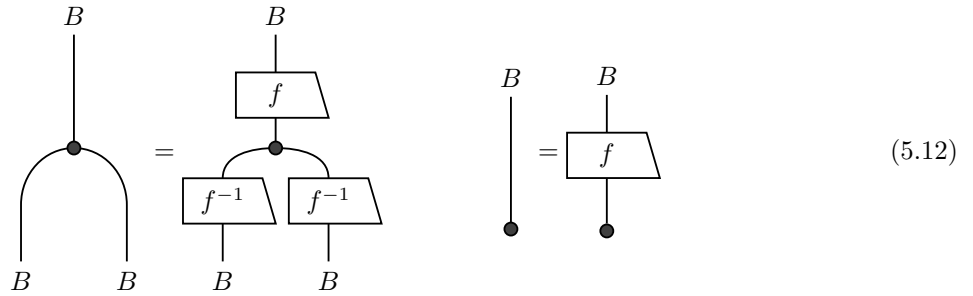
This completes the description of the correspondence.

Finally, this correspondence is bijective. Starting with a nondegenerate form, turning it into a comonoid, and then taking the counit, ends with the same nondegenerate form. Starting with a comonoid ends with the same counit but comultiplication (5.10). However, Lemma 3.5 guarantees that η must be as in Theorem 5.15, and then the Frobenius law guarantees that this comultiplication in fact equals the original one. \square

Homomorphisms

We now investigate properties of a map that preserves Frobenius structure.

Lemma 5.17 (Frobenius algebras transport across isomorphisms). *Let*
(A, μ, ν, η, ϵ) be a Frobenius structure in a monoidal category, and $A \xrightarrow{f} B$ an isomorphism. The following furnishes B with Frobenius structure:



This Frobenius structure is called the *transport* across f of the given one.

Proof. Straightforward graphical manipulation. □

Dagger Frobenius structure transports along an isomorphism f only if f is unitary.

Definition 5.18. A *homomorphism of Frobenius structures* is a morphism that is simultaneously a monoid homomorphism and a comonoid homomorphism.

Lemma 5.19. In a monoidal category, a homomorphism of Frobenius structures is invertible, and the inverse is again a homomorphism of Frobenius structures.

Proof. Given Frobenius structures on objects A and B and a Frobenius structure homomorphism $A \xrightarrow{f} B$, construct an inverse to f as follows:

(5.14)

The composite with f gives the identity in one direction:

Here, the first equality uses the comonoid homomorphism property, the second equality uses the monoid homomorphism property, and the third equality follows from Theorem 5.15. The other composite equals the identity by a similar argument.

Because f is a monoid homomorphism:

Postcomposing with f^{-1} shows that f^{-1} is again a monoid homomorphism. Similarly, it is again a comonoid homomorphism. □

5.2 Normal forms

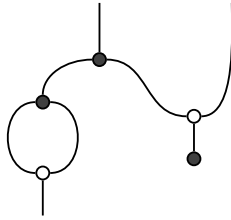
In general there are two ways to think about the graphical calculus:

- a diagram represents a morphism: it is just a shorthand to write down a linear map, for example, in the category \mathbf{FHilb} ;
- a diagram is an entity in its own right: it can be manipulated by replacing a subdiagram by one equal to it.

The first viewpoint doesn't care that many different diagrams represent the same morphism. The second viewpoint takes different representation diagrams seriously, giving a combinatorial or graph theoretic flavour. In nice cases, all diagrams representing a fixed morphism can be rewritten into a canonical diagram called a *normal form*. This should remind you of the Coherence Theorem 1.2. As you might expect, there are only so many ways you can comultiply (using \curvearrowright), discard (using \circlearrowleft), fuse (using \curvearrowleft) and create (using \bullet) information. In fact, in symmetric monoidal categories, there is only one, but the situation is more subtle in braided monoidal categories.

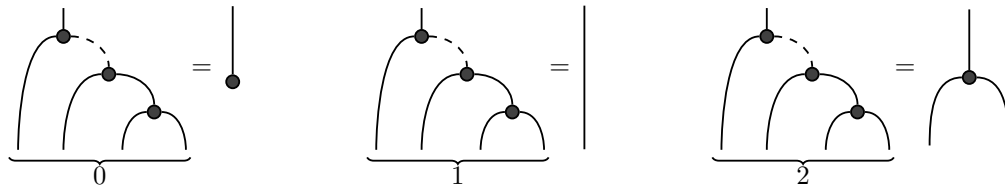
Normal forms for Frobenius structures

Consider any morphism $A^{\otimes m} \rightarrow A^{\otimes n}$ built out of the ingredients of a Frobenius structure $(A, \curvearrowright, \bullet, \circlearrowleft, \circlearrowright)$ in a monoidal category. For example, in the graphical calculus:



We can think of it as a graph: the wires are edges, and each dot \circ or \bullet is a vertex, as is the end of each input or output wire. Such a morphism is *connected* when it has a graphical representation which has a path between any two vertices.

We will use ellipses in graphical notation below, as in:



Lemma 5.20 (Special noncommutative spider theorem). *In a monoidal category, let $(A, \curvearrowright, \bullet, \circlearrowleft, \circlearrowright)$ be a special Frobenius structure. Any connected morphism $A^{\otimes m} \rightarrow A^{\otimes n}$ built out of finitely many pieces $\curvearrowright, \bullet, \circlearrowleft, \circlearrowright$,*

φ , and id , using \circ and \otimes , equals:

(5.15)

Proof. By induction on the number of dots. The base case is trivial: there are no dots and the morphism is an identity. The case of a single dot is still trivial, as the diagram must be one of \blacktriangleright , \bullet , \blacktriangleleft , φ . For the induction step, assume that all diagrams with at most n dots can be brought in normal form (5.15), and consider a diagram with $n + 1$ dots. Use naturality to write the diagram in a form where there is a topmost dot. If the topmost dot is a φ , use the induction hypothesis to bring the rest of the diagram in normal form (5.15), and use unitality (4.6) to finish the proof. If it is a \blacktriangleleft , associativity (4.5) finishes the proof. It cannot be a \bullet because the diagram was assumed connected. That leaves the case of a \blacktriangleright . We distinguish whether the part of the diagram below the \blacktriangleright is connected or not.

If the subdiagram is disconnected, use the induction hypothesis on the two connected components to bring them in normal form (5.15). The diagram is then of the form below, where we can use the Frobenius identity (5.4) repeatedly to push the topmost \blacktriangleright down and left:

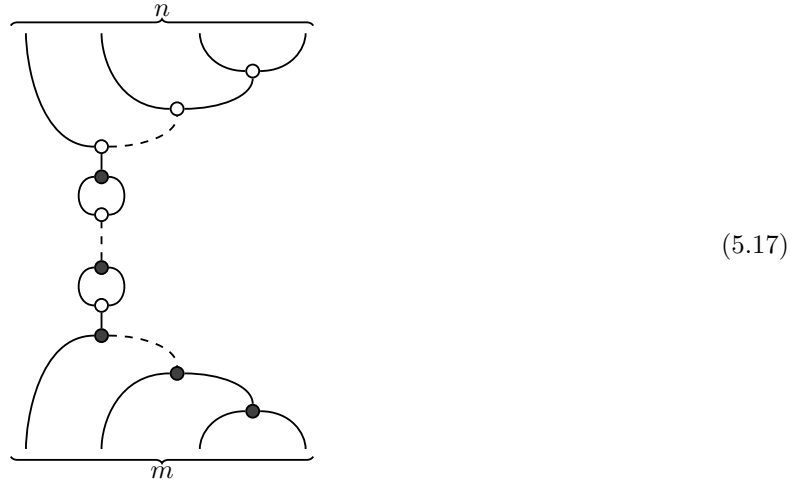
(5.16)

By (co)associativity (4.5) this is a normal form (5.15).

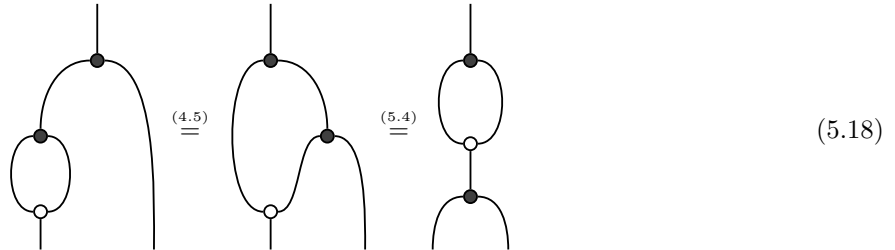
Finally, we are left with the case where the extra dot \bullet is on top of a connected subdiagram. Use the induction hypothesis to bring the subdiagram in normal form (5.15). By (co)associativity (4.5) the diagram rewrites to a normal form (5.15) with a \circ on top, which vanishes by speciality (5.5). This completes the proof. \square

Normal form results for Frobenius structures such as the previous lemma are called Spider Theorems because (5.15) looks a bit like an $(m+n)$ -legged spider. It extends to the nonspecial case as well.

Theorem 5.21 (Noncommutative spider theorem). *In a monoidal category, let $(A, \mu, \nu, \eta, \epsilon)$ be a Frobenius structure. Any connected morphism $A^{\otimes m} \rightarrow A^{\otimes n}$ built out of finitely many pieces μ, ν, η, ϵ , and id , using \circ and \otimes , equals:*



Proof. Use the same strategy as in Lemma 5.20 to reduce to a \bullet on top of a subdiagram that is connected or not. First assume the subdiagram is disconnected. Because



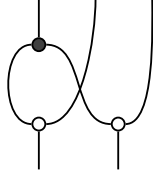
we may push arbitrarily many \circ past a \bullet . If the two subdiagrams in the first diagram of (5.16) did have \circ in the middle, these would carry over to the last diagram of (5.16) just below the topmost \bullet . Then (5.18) lets us push them above the \bullet , after which (co)associativity (4.5) finishes the proof as before, but now without assuming speciality.

Finally, assume the extra dot \bullet is on top of a connected subdiagram. As in Lemma 5.20 the diagram rewrites into a normal form (5.17) with a \circ on top. A similar argument to (5.18) lets us push the \circ down past η dots, and by (co)associativity (4.5) we end up with a normal form (5.17) again. \square

Normal forms for classical structures

Next we consider the commutative case of classical structures. We can allow symmetries as building blocks and still expect the same normal form. This introduces a subtlety in the induction step of a \bullet on top

of a disconnected subdiagram, because the subdiagram need not be a monoidal product of two connected morphisms; think for example of the following situation:

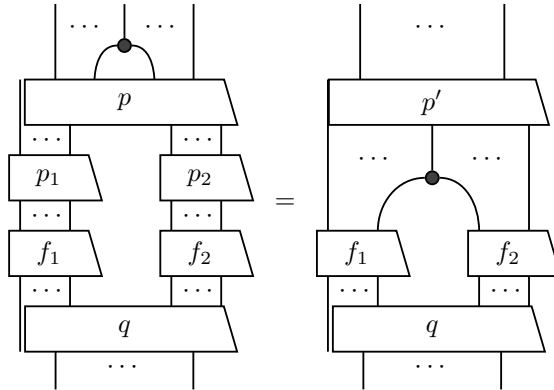


We will call a morphism $A^{\otimes n} \xrightarrow{p} A^{\otimes n}$ built from pieces id and \bowtie using \circ and \otimes *permutations*. They correspond to bijections $\{1, \dots, n\} \rightarrow \{1, \dots, n\}$, and we may write things like $p^{-1}(2)$ for the (unique) input wire that p connects to the 2nd output wire.

Theorem 5.22 (Commutative spider theorem). *Let $(A, \bullet, \circlearrowleft, \circlearrowright, \varphi)$ be a commutative Frobenius structure in a symmetric monoidal category. Any connected morphism $A^{\otimes m} \rightarrow A^{\otimes n}$ built out of finitely many pieces $\bullet, \circlearrowleft, \circlearrowright, \varphi, \text{id}$, and \bowtie , using \circ and \otimes , equals (5.17).*

Proof. Again use the same strategy as in Lemma 5.20. Without loss of generality we may assume there are no \bowtie above the topmost dot, because they will vanish by coassociativity (4.3) and cocommutativity (4.2) once we have rewritten the lower subdiagram in a normal form (5.17). So again the proof reduces to a \bullet on top of a subdiagram that is either connected or not. In the connected case, the very same strategy as in Theorem 5.21 finishes the proof.

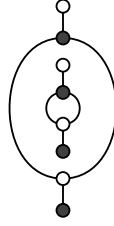
The disconnected case is more subtle. Because the whole diagram is connected, the subdiagram without the \bullet has exactly two connected components, and every input wire and every output wire belongs to one of the two. Therefore the subdiagram is of the form $p \circ (f_1 \otimes f_2) \circ q$ for permutations p, q and connected morphisms f_i . Use the induction hypothesis to bring f_i in a normal form (5.17). By cocommutativity (4.2) and coassociativity (4.3) we may freely postcompose both f_i with any permutations p_i , and precompose the \bullet with a \bowtie . For example, if $f_i: A^{\otimes m_i} \rightarrow A^{\otimes n_i}$, we may choose any permutations p_i with $p_1(n_1) = p^{-1}(k_1)$ and $p_2(1) = p^{-1}(k_2) - n_1$, where k_i is the position of the leg of the \bullet connecting to f_i . So by naturality we can write the whole diagram as follows for some permutation p' :



Now the subdiagram consisting of f_i and the topmost \bullet is of the form (5.16), and the same strategy as in Theorem 5.21 brings it in normal form (5.17), after which p' and q vanish by (co)associativity (4.5) and (co)commutativity (4.7). \square

For a (co)commutative Frobenius structure in a symmetric monoidal category, any morphism built from the basic ingredients by finite means, connected or not, equals $p \circ (f_1 \otimes \dots \otimes f_n) \circ q$ for some permutations p, q and morphisms f_1, \dots, f_n of the form (5.17); the permutations p, q are only unique up to reordering

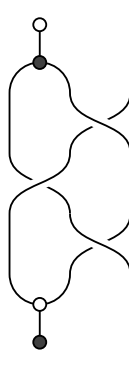
the connected components f_i . This is not true in braided monoidal categories; think for example of this morphism:



Using only planar isotopy, the ‘inner’ scalar cannot be brought alongside the ‘outer’ one by pre- and postcomposing with any permutation.

Proposition 5.23 (No braided spider theorem). *Theorem 5.22 does not hold for braided monoidal categories.*

Proof. Regard the following diagram as a piece of string on which an overhand knot is tied:



The knot cannot be untied by string deformations such as (co)associativity (4.5), (co)unitality (4.6), (co)commutativity (4.7), or the Frobenius law (5.4). Thus different knots give different morphisms $A \rightarrow A$. \square

5.3 Justifying the Frobenius law

Morphisms $A \rightarrow A$ in a category can be composed, and by map-state duality, this endows $A^* \otimes A$ with the pair of pants monoid structure, as discussed in Section 4.1. In the presence of daggers, this monoid picks up the additional structure of an involution. This section proves that the Frobenius law holds precisely when the Cayley embedding of Proposition 4.13 preserves this additional structure. Thus Frobenius structures are motivated by the ‘way of the dagger’.

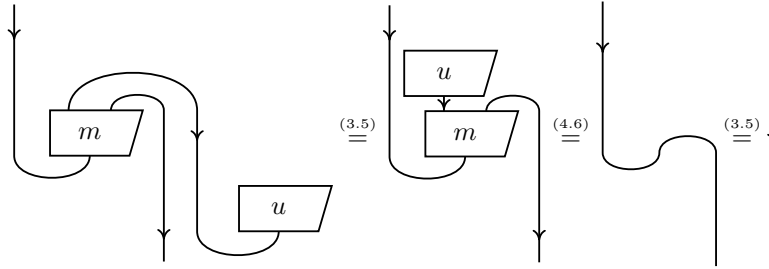
Involutive monoids

Any morphism $H \xrightarrow{f} K$ in a monoidal dagger category gives rise to another morphism $K \xrightarrow{f^\dagger} H$. The name $\ulcorner f \urcorner: I \rightarrow H^* \otimes K$ of f lands in $A = H^* \otimes K$, whereas the name $\ulcorner f^\dagger \urcorner$ of f^\dagger lives in $A^* = K^* \otimes H$. Indeed, in the category **Hilb**, taking daggers $f \mapsto f^\dagger$ is anti-linear, and so is a morphism $A \rightarrow A^*$. We will use this in particular when $H = K$. Then $A = H^* \otimes H$ becomes a pair of pants monoid under (names of) composition of morphisms $H \rightarrow H$, which also has an involution $A \rightarrow A^*$ induced by taking (names of) daggers.

The involution $f \mapsto f^\dagger$ additionally satisfies $(g \circ f)^\dagger = f^\dagger \circ g^\dagger$. Hence it is a homomorphism of monoids if we take the codomain to be the monoid with the opposite multiplication. This comes down to the following lemma and definition when we internalize the involution along map-state duality.

Lemma 5.24 (The opposite monoid). *If (A, m, u) is a monoid in a monoidal dagger category \mathbf{C} , and $A \dashv A^*$ is a dagger dual object, then (A^*, m_*, u_*) is a monoid too.*

Proof. Unitality of m_* and u_* follows directly from unitality of m and u :



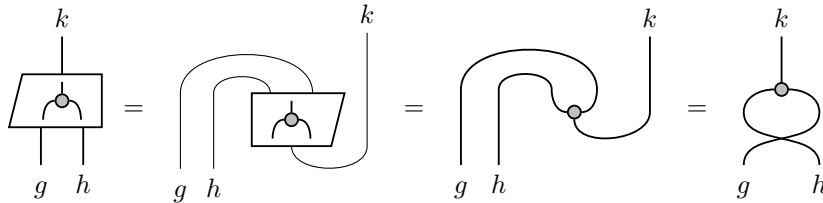
Associativity of m_* similarly follows from associativity of m . □

Definition 5.25 (Involutive monoid). A monoid (A, \circ, \circ) on an object with a dagger dual is an *involutive monoid* when it comes equipped with an *involution*: a morphism of monoids $A \xrightarrow{i} A^*$ satisfying $i_* \circ i = \text{id}_A$. A *morphism of involutive monoids* is a monoid homomorphism $A \xrightarrow{f} B$ satisfying $i_B \circ f = f_* \circ i_A$.

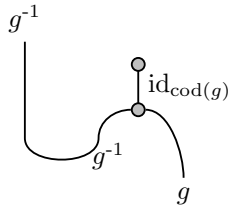
(5.19)

Note that the involution i is necessarily an isomorphism: by definition $i_* \circ i = \text{id}_A$, and because the opposite identity $i \circ i_* = \text{id}_{A^*}$ follows by applying the functor $(-)_*$.

Example 5.26. The Frobenius structure (G, \circ, \circ) in **Rel** induced by a groupoid \mathbf{G} as in Example 5.3 is involutive. First, observe that the opposite monoid G^* is induced by the opposite groupoid \mathbf{G}^{op} , since its multiplication is, in the decorated notation of Section 3.3:



(The opposite multiplication is not simply \circ itself, even though $G^* = G$ in **Rel**; it might only look that way because the picture \circ is left-right symmetric.) There is a canonical involution $G \rightarrow G^*$ given by $g \sim g^{-1}$:



Note that this is a homomorphism of monoids, that happens to be induced by a contravariant functor of groupoids.

Example 5.27. The pair of pants monoids $A^* \otimes A$ of Lemma 4.11 are involutive in any monoidal dagger category, with the identity map as involution:

However, two abstract identifications hide the concrete algebra. Consider $A = \mathbb{C}^n$ in **FHilb**, so the pair of pants monoid $A^* \otimes A$ becomes the matrix algebra \mathbb{M}_n as in Example 4.12. First, since the dual space A^* in **FHilb** consists of functions $A \rightarrow I$, the convention $B^* \otimes A^* \simeq (A \otimes B)^*$ identifies $\langle j | \otimes \langle i | \in B^* \otimes A^*$ with $|ij\rangle \in (A \otimes B)^*$. Thus, if we want to think of \mathbb{M}_n^* as being the same set of complex n -by- n matrices again rather than something abstract, it has to carry the opposite multiplication: ab in \mathbb{M}_n^* is the ordinary matrix multiplication ba in \mathbb{M}_n . Second, the canonical isomorphism $A^* \simeq A$ given by $\langle i | \mapsto |i\rangle$ is anti-linear. Hence the canonical involution $\mathbb{M}_n \rightarrow \mathbb{M}_n^*$ concretely becomes the complex conjugate transpose $f \mapsto f^\dagger$, and scalar multiplication in \mathbb{M}_n^* is the complex conjugate of scalar multiplication in \mathbb{M}_n .

Dagger closure

Proposition 4.13 showed that any monoid on a dual object is a submonoid of a pair of pants monoid. Example 5.27 showed that pair of pants monoid in monoidal dagger categories are involutive monoids. It therefore makes sense to ask when a monoid on a dagger dual object is an involutive submonoid of a pair of pants monoid. The following theorem characterizes when this is the case.

We can also phrase when a monoid (A, μ, ν) on an object object A has an involution i in terms of a map $A \otimes A \xrightarrow{f} I$:

A canonical choice for such a map would be $\mu \circ \nu : A \otimes A \rightarrow I$. For a pair of pants monoid as in Example 5.27, this would give $i = \text{id}_{H^* \otimes H}$. Compare also Proposition 5.16.

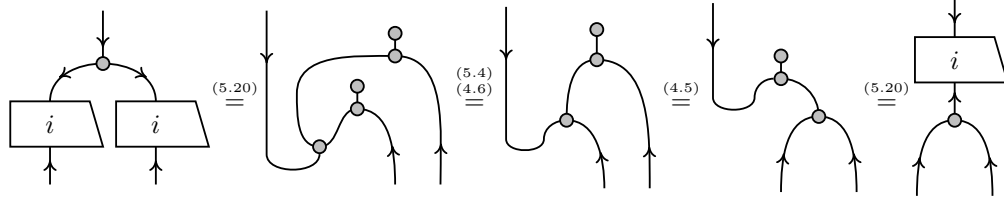
Theorem 5.28. For a monoid (A, μ, ν) on a dagger dual object $A \dashv A^*$ in a monoidal dagger category, the following are equivalent:

- (a) $(A, \mu, \nu, \mu', \nu')$ is a dagger Frobenius structure;
- (b) the following map makes (A, μ, ν) into an involutive monoid:

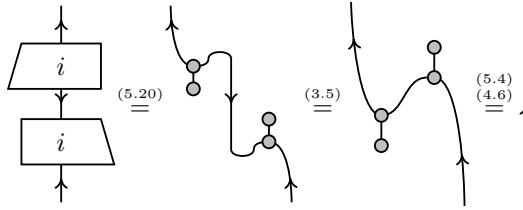
(5.20)

Recall from Example 5.27 that the identity is an involution on $A^* \otimes A$, so that property (c) says that the embedding preserves the canonical maps, $R_* \circ i_A = i_{A^* \otimes A} \circ R$, as in Definition 5.25.

Proof. Assuming (a), we prove that i respects multiplication as in equation (4.10):

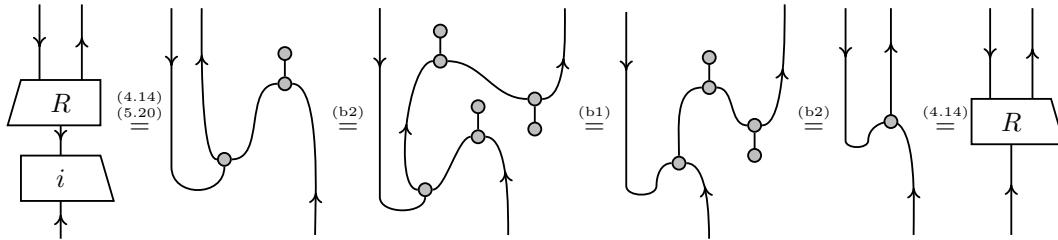


The second equation uses Lemma 5.4 and unitality, the third associativity. That i preserves units is trivial. Finally, i is indeed involutive:

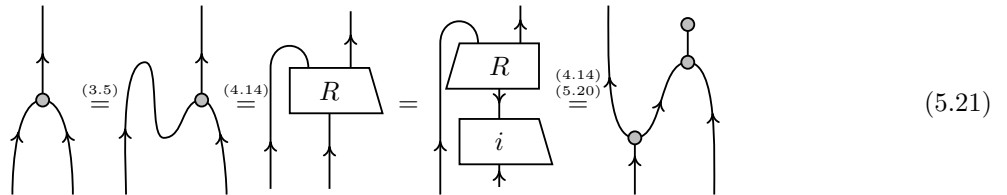


The second equation is the snake identity, and last equation uses the Frobenius law and unitality. Thus the monoid is involutive, and (b) holds.

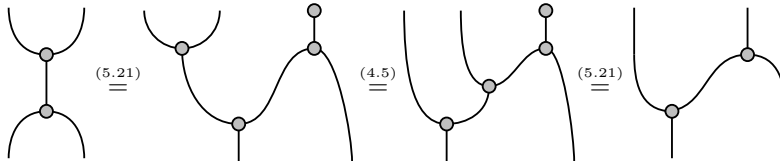
Next, assume (b); split the assumption into two as in the previous step, say (b1) for $i \circ \circlearrowleft = (\circlearrowleft)_* \circ (i \otimes i)$, and (b2) for $i_* \circ i = \text{id}_A$. Then:



So:



Hence:



The first and last step used (5.21), the middle step associativity. Because the left-hand side is self-adjoint, so is the right-hand side; that is, the Frobenius law holds, establishing (a). \square

Thus, if we want to think of endomorphisms as forming monoids via map-state duality, cooperation with daggers forces the Frobenius law on us. We may regard the Frobenius law as a coherence property between daggers and dual objects.

5.4 Classification

This section classifies the special dagger Frobenius structures in our two running examples, the category of Hilbert spaces, and the category of sets and relations. It turns out that dagger Frobenius structures in **FHilb** must be direct sums of the matrix algebras of Example 4.12; hence classical structures in **FHilb** must copy an orthonormal basis as in Section 5.1; and special dagger Frobenius structures in **Rel** must be induced by a groupoid as in Example 5.3.

Operator algebras

To classify the special dagger Frobenius structures in **FHilb**, we are going to have to use some results that are beyond the scope of this book. First, combine Theorem 5.28 and Example 4.12 to find the following: dagger Frobenius structures in **FHilb** correspond to subsets $A \subseteq \mathbb{M}_n$ that are closed under addition, scalar multiplication, matrix multiplication, matrix adjoint, and that contain the identity matrix.

The matrix algebra \mathbb{M}_n , and hence its subalgebra A , has a final piece of structure, namely a *norm*:

$$\|a\| = \min\{c \geq 0 \mid \|ax\| \leq c\|x\| \text{ for all } x \in \mathbb{C}^n\} \quad (5.22)$$

for $a \in \mathbb{M}_n$. This norm satisfies $\|a^\dagger a\| = \|a\|^2$ and $\|ab\| \leq \|a\|\|b\|$ for all matrices a and b , and is the unique one that does so.

In fact, these conditions are enough to characterize subsets $A \subseteq \mathbb{M}_n$ as above! They are called finite-dimensional *C*-algebras*. One of their basic properties is precisely what Theorem 5.28 did abstractly: any finite-dimensional C*-algebra embeds into a pair of pants algebra on some Hilbert space H . Well, there is one caveat: the embedding must not only preserve multiplication and involution, but also the norm. Tracking through Theorem 5.28, it turns out that this corresponds to the Frobenius structure being special. However, in finite dimension all norms are equivalent, and indeed we may rescale the inner product on A by the scalar $k(A)$ given by Definition 3.29. The following theorem summarizes this somewhat vague discussion without proof, by using the notion of transport of Lemma 5.17 along the rescaling isomorphism.

Theorem 5.29. *Any dagger Frobenius structure in **FHilb** is the transport of a special one, and special dagger Frobenius structures in **FHilb** are precisely finite-dimensional C*-algebras.* \square

If $A \subseteq \mathbb{M}_m$ and $B \subseteq \mathbb{M}_n$ are operator algebras, then so is their direct sum $A \oplus B \subseteq \mathbb{M}_{m+n}$. But taking direct sums of matrix algebras is the only freedom there is in finite-dimensional operator algebras, as the following theorem shows. Its proof is based on the Artin–Wedderburn theorem, which is beyond the scope of this book.

Theorem 5.30 (Artin–Wedderburn). *Any finite-dimensional C*-algebra is of the form $A \simeq \mathbb{M}_{k_1} \oplus \cdots \oplus \mathbb{M}_{k_n}$ for natural numbers n, k_1, \dots, k_n .* \square

Thus any dagger Frobenius structure (A, \mathcal{A}) in **FHilb** is (isomorphic to) one of the form $\mathbb{M}_{k_1} \oplus \cdots \oplus \mathbb{M}_{k_n}$. Via the Cayley embedding, we may think of them as algebras of matrices that are block diagonal. This restriction to block diagonal form is caused physically by *superselection rules*.

Orthonormal bases

Of course the matrix algebra \mathbb{M}_n is not commutative as soon as $n \geq 2$. In particular, if \mathcal{A} is commutative, we must have $k_1 = \cdots = k_n = 1$ and so $A \simeq \mathbb{C} \oplus \cdots \oplus \mathbb{C}$! The latter is a direct sum of Hilbert spaces, which corresponds to a choice of orthogonal basis, giving the following corollary.

Corollary 5.31. *In **FHilb**, For a finite-dimensional Hilbert space, there are exact correspondences between:*

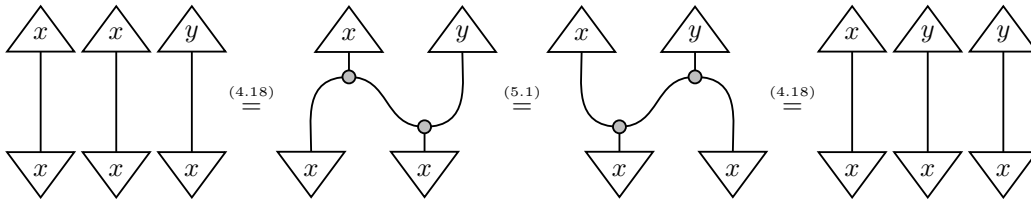
- *orthogonal bases and commutative dagger Frobenius structures;*
- *orthonormal bases and classical structures.* \square

We can now recognize the transport Lemma 5.17 as saying that the image of an orthonormal basis under a unitary map is again an orthonormal basis. Note that the map has to be unitary; if it is merely invertible then the transport is merely a Frobenius structure, and not necessarily a dagger Frobenius structure, so that the previous theorem does not apply.

Let's make all this use of high-powered machinery more concrete. We saw in Section 5.1 that copying any orthonormal basis of a finite-dimensional Hilbert space makes it into a classical structure, as is easy to verify. Corollary 5.31 is the converse: every classical structure in **FHilb** is of this form. Given a classical structure, we can retrieve an orthonormal basis by its set of copyable states, discussed in Section 4.2. The following lemmas form part of the proof of Corollary 5.31.

Lemma 5.32. *Nonzero copyable states of a dagger Frobenius structure in **FHilb** are orthogonal.*

Proof. Let x, y be nonzero copyable states and assume that $\langle x|y \rangle \neq 0$. Then:



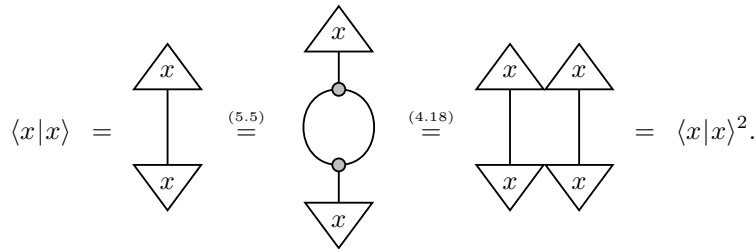
In other words, $\langle x|x \rangle \langle x|x \rangle \langle y|x \rangle = \langle x|x \rangle \langle y|x \rangle \langle y|x \rangle$. Since $x \neq 0$ also $\langle x|x \rangle \neq 0$. So we can divide to get $\langle x|x \rangle = \langle x|y \rangle$. Similarly we can find $\langle y|x \rangle = \langle y|y \rangle$. Hence these inner products are all in \mathbb{R} , and are all equal. But then

$$\langle x - y|x - y \rangle = \langle x|x \rangle - \langle x|y \rangle - \langle y|x \rangle + \langle y|y \rangle = 0,$$

so $x - y = 0$. □

Lemma 5.33. *Nonzero copyable states of a dagger special monoid-comonoid pair in **FHilb** have unit length.*

Proof. It follows from speciality that any nonzero copyable state x has a norm that squares to itself:



If x is nonzero then $\langle x|x \rangle$ must be nonzero, so dividing by it shows that $\|x\| = 1$. □

The difficult part of proving Corollary 5.31 is that the copyable states of a classical structure are not only orthonormal, they span the whole space; this is where the powerful theorems that are beyond the scope of this book come in.

Using Corollary 5.31, we can prove a converse to Example 4.6: every comonoid homomorphism between classical structures in **FHilb** is a function between the corresponding orthonormal bases.

Corollary 5.34. *In **FHilb**, a morphism between two commutative dagger Frobenius structures preserves comultiplication if and only if it sends copyable states to copyable states. It is a comonoid homomorphism if and only if it sends nonzero copyable states to nonzero copyable states.*

Proof. By linear extension, the comonoid homomorphism condition (4.8) will hold if and only if it holds on a basis of copyable states $\{e_i\}$ of the first classical structure, which must exist by Corollary 5.31. This gives the following equation:

Here the first equality expresses the fact that the state e_i is copyable, and the second equality is the comonoid homomorphism condition. Hence $f(e_i)$ is itself a copyable state. Thus (4.8) holds if and only if f sends copyable states to copyable states. The counit preservation condition (4.9) follows if and only if f sends nonzero copyable states to nonzero copyable states, because the counit of a classical structure is just the sum of its copyable states. \square

Because comonoid homomorphisms between classical structures in **FHilb** behave like functions, if we write them in matrix form using the bases of the associated classical structures, the result will be a matrix of zeroes and ones, with a single entry one in each column. These matrices are of course self-conjugate, since all the entries are real numbers. This gives a further property of comonoid homomorphisms.

Lemma 5.35. *Comonoid homomorphisms between classical structures in **FHilb** are self-conjugate:*

Proof. These linear maps will be the same if their matrix entries are the same. On the left-hand side, this gives:

On the right we can do this calculation:

$$\begin{array}{c} \triangle e_j \\ | \\ \text{box } f \\ | \\ \triangle e_i \end{array} = \left(\begin{array}{c} \triangle e_i \\ | \\ \text{box } f \\ | \\ \triangle e_j \end{array} \right)^\dagger = \begin{bmatrix} 1 & \text{if } e_i = f(e_j) \\ 0 & \text{if } e_i \neq f(e_j) \end{bmatrix}^\dagger = \begin{bmatrix} 1 & \text{if } e_i = f(e_j) \\ 0 & \text{if } e_i \neq f(e_j) \end{bmatrix}$$

Thus (5.23) holds. \square

Lemma 5.36. *In \mathbf{FHilb} , for a commutative dagger Frobenius structure, the following equations hold for any copyable state a :*

$$(5.24)$$

Proof. A copyable state $a : I \rightarrow A$ can be thought of as a function from the unique copyable state on the trivial classical structure on I , to the chosen copyable state, and therefore gives a comonoid homomorphism. By Lemma 5.35, the result follows. \square

Groupoids

We now investigate what special dagger Frobenius structures look like in \mathbf{Rel} . Recall that a groupoid is a category in which every morphism has an inverse, and that any groupoid induces a dagger Frobenius structure in \mathbf{Rel} by Example 5.3 and Example 5.11. It turns out that these examples are the only ones.

Theorem 5.37. *Special dagger Frobenius structures in \mathbf{Rel} correspond exactly to groupoids.*

Proof. Examples 5.3 and 5.6 already showed that groupoids give rise to special dagger Frobenius structures by writing A for its set of arrows, U for its subset of identities, and M for the composition relation. Conversely, let A be a special dagger monoid-comonoid pair in \mathbf{Rel} with multiplication $M : A \times A \rightarrow A$ and unit $U \subseteq A$. Suppose that $b(M \circ M^\dagger)a$ for $a, b \in A$. Then by the definition of relational composition, there must be some $c, d \in A$ such that $bM(c, d)$ and $(c, d)M^\dagger a$. To understand the consequence of the dagger speciality condition (5.5), we use the decorated notation of Section 3.3:

$$(5.5)$$

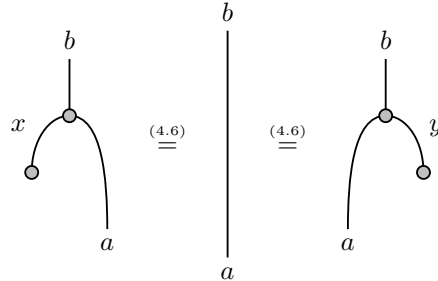
On the right-hand side, two elements $a, b \in A$ are only related by the identity relation if they are equal. So the same must be true on the left-hand side. Thus: if two elements $c, d \in A$ multiply to give two elements $a, b \in A$ — that is, both $bM(c, d)$ and $aM(c, d)$ hold — it must be the case that $a = b$. This says exactly that if two elements can be multiplied, then their product is unique. As a result we may simply write cd for the product of c and d , remembering that this only makes sense if the product is defined.

Next, consider associativity:

$$(4.5)$$

So ab and $(ab)c$ are both defined exactly when bc and $a(bc)$ are both defined, and then $(ab)c = a(bc)$. So when a triple product is defined under one bracketing, it is also defined under the other bracketing, and the products are equal.

Finally, unitality:

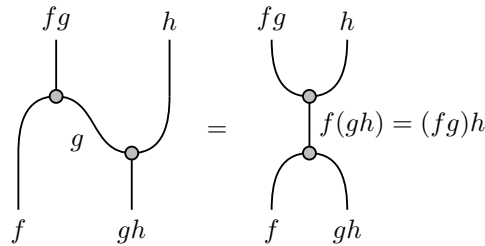


Here $x, y \in U \subseteq A$ are units, determined by the unit $1 \xrightarrow{U} A$ of the monoid. The first equality says that all a, b allow some $x \in U$ with $xa = b$ if and only if $a = b$. The second equality says that $ay = b$ for some $y \in U$ if and only if $a = b$. Put differently: multiplying on the left or the right by a element of U is either undefined, or gives back the original element.

What happens when multiplying elements from U together? Well, if $z \in U$ then certainly $z \in A$, and so $xz = x$ for some $x \in U$. But then we can multiply $z \in U \subseteq A$ on the left with x to produce x , and so $x = z$ by the previous paragraph! So elements of U are idempotent, and if we multiply two different elements, the result is undefined.

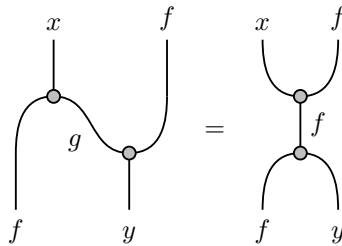
Lastly, can an element $a \in A$ have two left identities — is it possible for distinct $x, x' \in U$ to satisfy $xa = a = x'a$? This would imply $a = xa = x(x'a) = (xx')a$, which is undefined, as we have seen. So every element has a unique left identity, and similarly every element has a unique right identity.

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



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

To show that every arrow has an inverse, consider the following different decoration of the Frobenius law, for any $f \in A$, with left unit x and right unit y :



The properties of left and right units make the right-hand side decoration valid. Hence there must be $g \in A$ with which to decorate the left-hand side. But such a g is precisely an arrow with $fg = y$ and $gf = x$, which is an inverse for f . \square

Note also that the nondegenerate form \mathcal{P} of Proposition 5.16 is the coname of the function $g \mapsto g^{-1}$; see also Example 5.26.

Classifying the pair of pants Frobenius structures of Lemma 4.11 and Lemma 5.9 leads us back to the indiscrete categories of Section 4.2, as the following corollary shows.

Corollary 5.38. *Pair of pants dagger Frobenius structures in \mathbf{Rel} are precisely indiscrete groupoids, i.e. groupoids where there is precisely one morphism between each two objects.*

Proof. Let A be a set. By definition, $(A^* \otimes A, \lrcorner, \smile)$ corresponds to a groupoid \mathbf{G} whose set of morphisms is $A \times A$, and whose composition is given by

$$(b_2, b_1) \circ (a_2, a_1) = \begin{cases} (b_2, a_1) & \text{if } b_1 = a_2, \\ \text{undefined} & \text{otherwise.} \end{cases}$$

We deduce that the identity morphisms of \mathbf{G} are the pairs (a_2, a_1) with $a_2 = a_1$. So objects of \mathbf{G} just correspond to elements of A . Similarly, we find that the morphism (a_2, a_1) has domain a_1 and codomain a_2 . Hence (a_2, a_1) is the unique morphism $a_1 \rightarrow a_2$ in \mathbf{G} . \square

Classifying classical structures in \mathbf{Rel} is now easy. Recall from Example 5.11 that a groupoid is abelian when $g \circ h = h \circ g$ whenever one of the two sides is defined.

Corollary 5.39. *In \mathbf{Rel} , classical structures exactly correspond to abelian groupoids.*

Proof. An immediate consequence of Theorem 5.37. \square

5.5 Phases

In quantum information theory, an interesting family of maps are *phase gates*: diagonal matrices whose diagonal entries are complex numbers of norm 1. For a particular Hilbert space equipped with a basis, these form a group under composition, which we will call the *phase group*. This turns out to work fully abstractly: any Frobenius structure in any monoidal dagger category gives rise to a phase group.

Definition 5.40 (Phase). Let $(A, \mathcal{P}, \mathcal{M})$ be a Frobenius structure in a monoidal dagger category. A state $I \xrightarrow{a} A$ is called a *phase* when:

$$\begin{array}{c} \triangleup_a \\ | \\ \bullet \\ | \\ \triangleleft_a \end{array} = \begin{array}{c} | \\ | \\ \bullet \\ | \\ \triangleleft_a \end{array} = \begin{array}{c} | \\ | \\ \bullet \\ | \\ \triangleup_a \end{array} \quad (5.25)$$

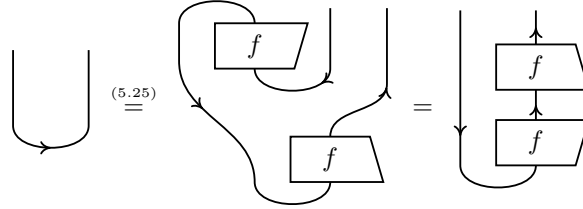
Its (right) *phase shift* is the following morphism $A \rightarrow A$:

$$\begin{array}{c} | \\ | \\ \circ_a \\ | \\ | \end{array} := \begin{array}{c} | \\ | \\ \bullet \\ | \\ \triangleleft_a \end{array} \quad (5.26)$$

For the classical structure copying an orthonormal basis $\{e_i\}$ in **FHilb**, a vector $a = a_1e_1 + \cdots a_n e_n$ is a phase precisely when each scalar a_i lies on the unit circle: $|a_i|^2 = 1$. For another example, the unit \circ of a Frobenius structure is always a phase. The following lemma gives more examples.

Lemma 5.41. *The phases of a pair of pants Frobenius structure $(A^* \otimes A, \lrcorner, \smile)$ are the names of unitary operators $A \rightarrow A$.*

Proof. The name of an operator $A \xrightarrow{f} A$ is a phase when:



But this precisely means $f \circ f^\dagger = \text{id}_A$ by the snake equations (3.5). The other, symmetric, equation defining phases similarly comes down to $f^\dagger \circ f = \text{id}_A$. \square

Example 5.42 (Phases in **FHilb**). The set of phases of the Frobenius structure \mathbb{M}_n in **FHilb** is the set $U(n)$ of n -by- n unitary matrices. Hence the phases of the Frobenius structure $\mathbb{M}_{k_1} \oplus \cdots \oplus \mathbb{M}_{k_n}$ range over $U(k_1) \times \cdots \times U(k_n)$.

Now consider the special case of a classical structure on \mathbb{C}^n that copies an orthonormal basis $\{e_1, \dots, e_n\}$. The phases are elements of $U(1) \times \cdots \times U(1)$; that is, phases a are vectors of the form $e^{i\phi_1}e_1 + \cdots + e^{i\phi_n}e_n$ for real numbers ϕ_1, \dots, ϕ_n . The accompanying phase shift $\mathbb{C}^n \rightarrow \mathbb{C}^n$ is the unitary matrix

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

Example 5.43 (Phases in **Rel**). The phases of a Frobenius structure in **Rel** induced by a group G are elements of that group G itself.

Proof. For a subset $a \subseteq G$, the equation (5.25) defining phases reads

$$\{g^{-1}h \mid g, h \in a\} = \{1_G\} = \{hg^{-1} \mid g, h \in a\}.$$

So if $g \in G$, then $a = \{g\}$ is a phase. But if a contains two distinct elements $g \neq h$ of G , then it cannot be a phase. Similarly, $a = \emptyset$ is not a phase. Hence a is a phase precisely when it is a singleton $\{g\}$. \square

Phase groups

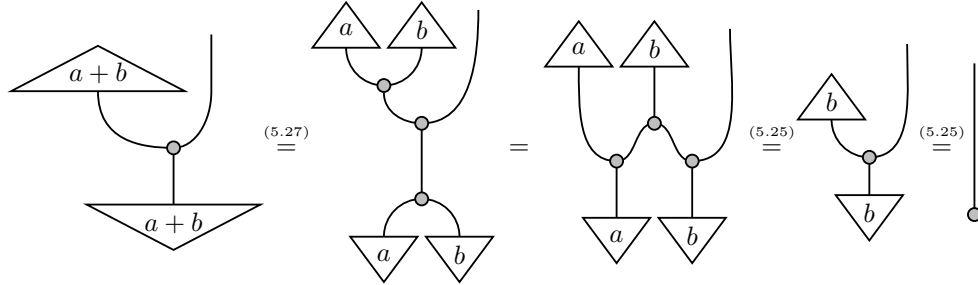
The phases in all of the previous examples can be composed: unitary matrices under matrix multiplication, group elements under group multiplication. In general, phase shifts can be composed, and hence we expect phases to form a monoid. The following proposition shows that they in fact always form a group.

Proposition 5.44 (Phase group). *Let (A, \circ, \bullet) be a dagger Frobenius structure in a monoidal dagger category. Its phases form a group with unit \circ under the following addition:*

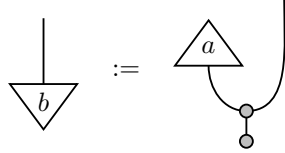
(5.27)

Equivalently, the phase shifts form a group under composition. The phases of a classical structure in a braided monoidal dagger category form an abelian group.

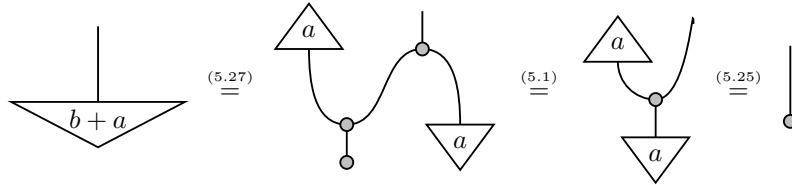
Proof. First we show that (5.27) is again a well-defined phase:



The second equality follows from the noncommutative Spider Theorem 5.21. As the other equation of (5.25) follows similarly, the set of phases form a monoid by associativity (4.5). Fix a phase a and set:

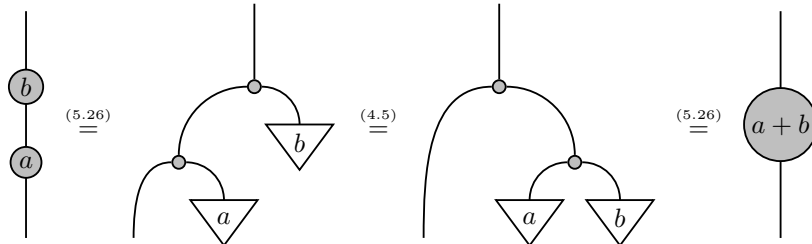


Then b is a left-inverse of a :



The reflection of b similarly gives a right-inverse c . But then actually $b = b + 0 = b + (a + c) = (b + a) + c = 0 + c = c$, so a has a unique (two-sided) inverse $-a := b = c$ making the phase monoid into a group.

Notice that (5.27) corresponds to composition when we turn phases into phase shifts:



Clearly this group is abelian when the Frobenius structure is commutative. □

The group of the previous proposition is called the *phase group*.

Example 5.45. Here are examples of phase groups for some of our standard dagger Frobenius structures:

- The group operation on the phases of the pair of pants Frobenius structure of Lemma 5.41, which are names of unitary morphisms $A \xrightarrow{f} A$, is simply taking the name of composition of operators.

- The group operation on the phases $U(k_1) \times \cdots \times U(k_n)$ of a Frobenius structure $\mathbb{M}_{k_1} \oplus \cdots \oplus \mathbb{M}_{k_n}$ in **FHilb** of Example 5.42 is simply entrywise multiplication. In particular, the group operation on a classical structure is multiplication of diagonal matrices.
- The group operation on the phases G of a Frobenius structure in **Rel** induced by a group G as in Example 5.43 is by construction (5.27) the multiplication of G itself. Hence the phase group of the Frobenius structure G in **Rel** is G itself.

Phased normal forms

The next theorem generalizes the spider theorem to take phases into account, which can be done as long as the Frobenius structure is a classical structure.

Corollary 5.46 (Phased spider theorem). *Let (A, μ, ν) be a classical structure in a symmetric monoidal dagger category. Any connected morphism $A^{\otimes m} \rightarrow A^{\otimes n}$ built out of finitely many $\mu, \nu, \text{id}, \times$ and phases using \circ, \otimes , and \dagger , equals*

$$(5.28)$$

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

Proof. Using symmetries we can first make sure all the phases dangle at the bottom right of the diagram. Next we can apply Theorem 5.22. By definition (5.27) of the phase group, the phases on the bottom right, together with the multiplications μ above them, reduce to a single phase $\sum a$ on the bottom right. Finally, another application of Theorem 5.22 turns the diagram into the desired form (5.28). \square

State transfer

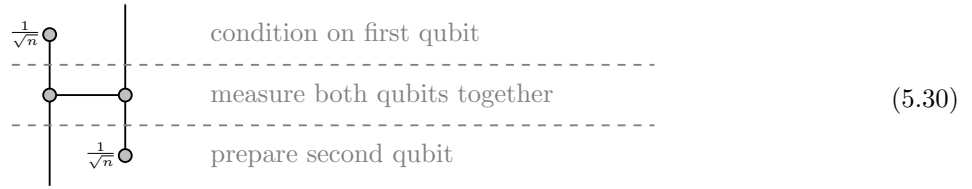
We're now going to apply our knowledge of classical structures to analyze the quantum state transfer protocol. This procedure transfers the quantum state of a Hilbert space H from one system to another, with a probability of success given by $1/\dim(H)^2$. Interest in state transfer lies in the fact that all the procedures involved are state preparations or measurements: no unitary dynamics takes place.

By virtue of the spider theorem, we can be quite lax when drawing wires connected by classical structures. They are all the same morphism anyway. For example:

$$(5.29)$$

is a projection $H \otimes H \rightarrow H \otimes H$.

Define the procedure for state transfer graphically by the following diagram:

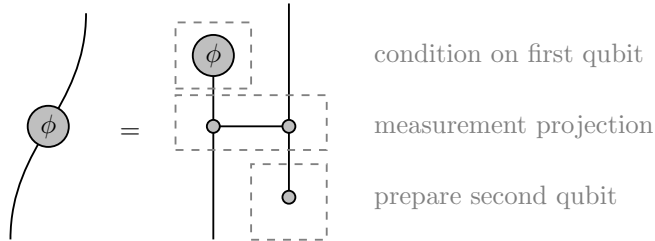


We can easily simplify this diagram using the spider theorem:



Hence this protocol indeed achieves the goal of transferring the first qubit to the second. To appreciate the power of the graphical calculus, one only needs to compute the same protocol using matrices.

By using the phased spider theorem, Corollary 5.46, we can also easily achieve the extra challenge of applying a phase gate in the process of transferring the state, by the following adapted protocol.



Categories and Quantum Informatics: Complementarity

Chris Heunen

Spring 2018

This chapter studies what happens when we have *two* interacting Frobenius structures. Specifically, we are interested in when they are “maximally incompatible”, or *complementary*, and give a definition that makes sense in arbitrary monoidal dagger categories in Section 6.1. We will see that it comes down to the standard notion of mutually unbiased bases from quantum information theory in the category of Hilbert spaces, and classify the complementary groupoids in the category of sets and relations. We will also characterize complementarity in terms of a canonical morphism being isometric. This is exemplified by discussing the Deutsch–Jozsa algorithm in Section 6.2, where the canonical morphism plays the role of an oracle function. Section 6.3 links complementarity to the subject of Hopf algebra. It turns out that this well-studied notion gives rise to a stronger form of complementarity that we characterize. Finally, Section 6.4 discusses how many-qubit gates can be modeled in categorical quantum mechanics using only complementary Frobenius structures, such as controlled negation, controlled phase gates, and arbitrary single qubit gates.

We have been using colours to distinguish between monoid multiplication \blacklozenge and comonoid comultiplication \blackcomultiplication . We have also been indicating that one is the dagger of the other by abbreviating $\blacklozenge = \blackcomultiplication$ to just a single colour \blacklozenge . From this chapter on, we will deal with *two* Frobenius structures, each carrying both a multiplication and a comultiplication. When this is the case we will specialize to dagger Frobenius structures, so we can distinguish them. By drawing the operations of a single Frobenius structure in a single colour, we can speak about two dagger Frobenius structures $(A, \blacklozenge, \blackcomultiplication, \blackcirclearrowright)$ and $(A, \blackcomultiplication, \blacklozenge, \blackcirclearrowright)$, in a way perfectly consistent with our conventions. Nevertheless, many results hold more generally without daggers.

6.1 Complementarity

Consider two measurements of a qubit: one in the basis $\{(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}), (\begin{smallmatrix} 0 \\ 1 \end{smallmatrix})\}$, and one in the basis $\{(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix})/\sqrt{2}, (\begin{smallmatrix} 1 \\ -1 \end{smallmatrix})/\sqrt{2}\}$. If we measure in the first basis, the qubit will collapse to either $(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix})$ or $(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix})$; a repeated measurement in the first basis is guaranteed to repeat the same outcome. However, a measurement in the second basis could yield either outcome with equal probability. Two bases with this property are said to be unbiased. This is a simple form of Heisenberg’s uncertainty principle.

Definition 6.1. For a finite-dimensional Hilbert space H , two orthogonal bases $\{a_i\}$ and $\{b_j\}$ are *complementary*, or *unbiased*, when there is some constant $c \in \mathbb{C}$ such that the following holds:

$$\langle a_i | b_j \rangle \langle b_j | a_i \rangle = c \tag{6.1}$$

In other words, the inner products have constant absolute value.

We can prove the following simple lemma about complementary bases.

Lemma 6.2. For a pair of complementary bases $\{a_i\}$ and $\{b_j\}$, within each basis, the elements have constant norm.

Proof. We perform the following computation:

$$\langle b_j | b_j \rangle = \sum_i \frac{\langle b_j | a_i \rangle \langle a_i | b_j \rangle}{\langle a_i | a_i \rangle} \stackrel{(6.1)}{=} \sum_i \frac{c}{\langle a_i | a_i \rangle}$$

In the first equality, we insert the identity as a sum over the complete family of projectors $|a_i\rangle\langle a_i|/\langle a_i|a_i\rangle$. The final expression is independent of j as required. A similar argument holds for the $\{a_i\}$ basis. \square

We know from Corollary 5.31 that an orthogonal basis can be represented as a commutative dagger Frobenius structure, so a natural goal is to characterize complementarity as an interaction law between two commutative dagger Frobenius structures. Following this inspiration leads to the following definition.

Definition 6.3 (Complementary Frobenius structures). In a braided monoidal dagger category, two symmetric dagger Frobenius structures \blacklozenge and \whitecirc on the same object are *complementary* when the following equals hold:

$$(6.2)$$

The roles of the black and white dots in the previous definition are not obviously interchangeable. However, since the Frobenius algebras are symmetric, we can make the following argument:

$$(6.3)$$

Using these equations and the dagger, we see that ‘black is complementary to white’ is equivalent to ‘white is complementary to black’.

First properties

We now establish that this captures the correct notion in **FHilb**.

Proposition 6.4 (Complementarity in **FHilb**). *In **FHilb**, the following are equivalent for two commutative dagger Frobenius structures on the same object:*

- as Frobenius structures, they are complementary;
- as bases, they are complementary with constant $c = 1$.

Proof. The complementarity equation (6.2) holds if and only if the following equation holds for all a in the

white basis, and b in the black basis:

$$(6.4)$$

The left-hand side can be simplified as follows:

$$(6.5)$$

The right-hand side expands to 1. □

Example 6.5 (Pauli bases). Here are three bases of the Hilbert space \mathbb{C}^2 :

$$X \text{ basis: } \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\} \quad (6.6)$$

$$Y \text{ basis: } \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \right\} \quad (6.7)$$

$$Z \text{ basis: } \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\} \quad (6.8)$$

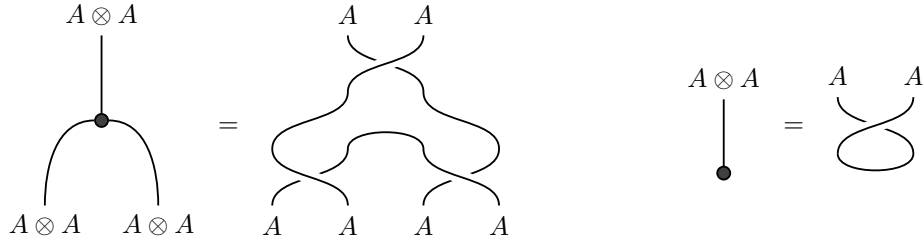
These are all mutually complementary. The terminology is explained by the fact that these bases consist of eigenvectors of the three Pauli matrices that measure spin in the X , Y and Z coordinates of a spin- $\frac{1}{2}$ particle in three-dimensional space.

It is known that this is the largest family of complementary bases that can exist in \mathbb{C}^2 , in the sense that it is not possible to find four bases for this Hilbert space which are all mutually complementary. Establishing the maximum possible number of mutually complementary bases in a Hilbert space of a given dimension is a difficult problem, which has not been solved in general for Hilbert spaces of dimensions which are not a prime power.

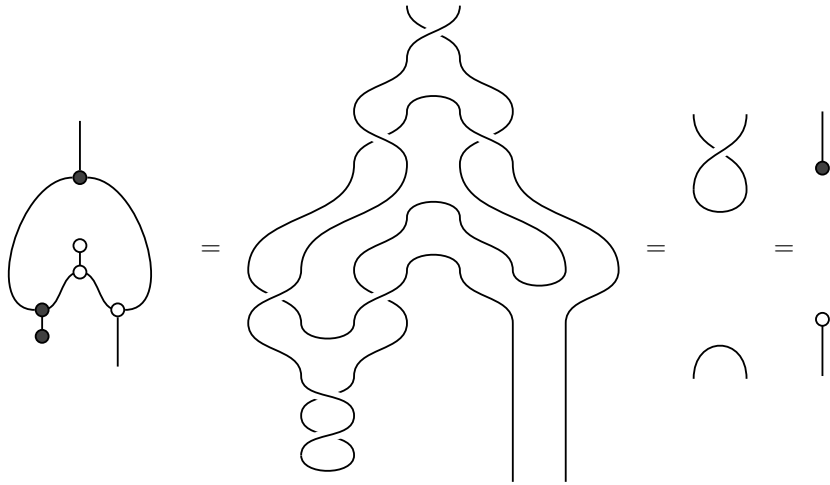
The next lemma provides a large stock of examples of complementary Frobenius structures.

Lemma 6.6. *If A is a dagger self-dual object in a braided monoidal category, then the following two Frobenius structures on $A \otimes A$ are complementary: the pair of pants from Lemma 5.9, and its transport across the braiding $\sigma_{A,A}$ as in Lemma 5.17.*

Proof. Denote the pair of pants Frobenius structure from Lemma 5.9 by white dots, and its transport across the braiding, the ‘twisted knickers’, by black dots:



Then straightforward diagrammatic calculation shows:



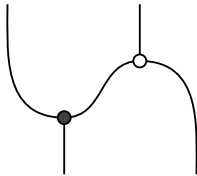
The other identity in (6.2) follows similarly. □

Combined with Theorem 5.15, the previous lemma says that any dagger Frobenius structure on A gives rise to a complementary pair of Frobenius structures on $A \otimes A$ in any symmetric monoidal dagger category.

Dagger complementarity

Complementarity is an equality of morphisms built from the (co)multiplication and (co)unit of a Frobenius structure. We can also characterize complementarity in terms of daggers, namely as some canonical morphism being unitary. This is the content of the following proposition.

Proposition 6.7. *Two symmetric dagger Frobenius structures in a braided monoidal dagger category are complementary if and only if the following endomorphism is unitary:*



(6.9)

Proof. Composing (6.9) with its adjoint, we obtain:

(6.10)

Here, the first equality follows from two applications of the noncommutative spider Theorem 5.21 to the dashed areas. Now, if complementarity (6.2) holds then (6.10) equals the identity. Conversely, if the right-hand side of (6.10) equals the identity, then composing with the white counit on the top right and the black unit on the bottom left gives back the left-hand equality of complementarity (6.2). Therefore the left identity in (6.2) holds if and only if (6.9) is an isometry. A similar argument composing (6.9) with its adjoint in the other order corresponds to the right-hand equality of complementarity (6.2). \square

Complementary groupoids

Now we investigate what complementarity means in our other example category \mathbf{Rel} . It turns out to be a phenomenon similar to mutual unbiasedness. The construction in the following example is a lot like that of Lemma 6.6.

Example 6.8. Let G and H be nontrivial groups. Set $A = G \times H$. Let \mathbf{G} be the groupoid with objects G and homsets $\mathbf{G}(g, g) = H$ and no morphisms between distinct objects, and let \mathbf{H} be the groupoid with objects H and homsets $\mathbf{H}(h, h) = G$ and no morphisms between distinct objects. Then in a natural way, \mathbf{G} and \mathbf{H} can be considered to have the same set of morphisms, and in fact they are complementary as Frobenius structures.

Proof. Consider the left-hand side of (6.2). It expands to

$$\{(a, b) \mid \exists x \in A: x \bullet a = x \circ b\},$$

where we write \bullet for the composition in \mathbf{G} , and \circ for the composition in \mathbf{H} . This set clearly contains the right-hand side of (6.2), which is

$$\{(\text{id}_g, \text{id}_h) \mid g \in \text{Ob}(\mathbf{G}), h \in \text{Ob}(\mathbf{H})\}.$$

Remember that we cannot compose any two morphisms in a groupoid; they have to have matching domain and codomain. Suppose $x \bullet a = x \circ b$. Then the \circ -inverse of x is \circ -composable with $x \bullet a$. That is, $\text{cod}_\circ(x) = \text{cod}_\circ(x \bullet a)$. But by construction that means a must be a \bullet -identity. Similarly, b must be a \circ -identity. So the left-hand and right-hand sides of (6.2) are equal, and \mathbf{G} and \mathbf{H} are complementary. \square

The previous example suggests a certain balance between two complementary groupoids. The following proposition makes this precise: the fewer objects one groupoid has, the more a complementary one must have.

Proposition 6.9 (Complementarity in \mathbf{Rel}). *The following are equivalent for groupoids \mathbf{G} and \mathbf{H} with the same set A of morphisms:*

- their Frobenius structures are complementary;
- the map $A \rightarrow \text{Ob}(\mathbf{G}) \times \text{Ob}(\mathbf{H})$ given by $a \mapsto (\text{cod}_{\mathbf{G}}(a), \text{cod}_{\mathbf{H}}(a))$ is bijective.

Proof. Write \bullet for the multiplication in \mathbf{G} , and \circ for that in \mathbf{H} . By Proposition 6.7, complementarity is equivalent to unitarity of the morphism (6.9). Unitaries in \mathbf{Rel} are exactly the bijective functions (see Exercise ??). Unfolding this, we see that complementarity is equivalent to:

$$\forall a, b \in A \exists! c, d \in A \exists e \in A: b = e \bullet d, c = a \circ e.$$

Because we're in a groupoid, when a, b, c, d are fixed, there is only one possible e fitting the bill, so we can reformulate this as:

$$\forall a, b \in A \exists! c, d, e \in A: d = e^{-1} \bullet b, c = a \circ e,$$

where the inverse is taken in \mathbf{G} . This just means that all $a, b \in A$ allow a unique $e \in A$ making $e^{-1} \bullet b$ and $a \circ e$ well-defined. But this happens precisely when e and b have the same codomain in \mathbf{G} , and $\text{cod}(e) = \text{dom}(a)$ in \mathbf{H} . Thus complementarity holds if and only if all objects g of \mathbf{G} and h of \mathbf{H} allow unique $e \in A$ with \mathbf{G} -codomain g and \mathbf{H} -codomain h . \square

In particular: if two classical structures in \mathbf{Rel} corresponding to abelian groupoids \mathbf{G} and \mathbf{H} are complementary, then $\mathbf{G}(g, g) \simeq \text{Ob}(\mathbf{H})$ and $\mathbf{H}(h, h) \simeq \text{Ob}(\mathbf{G})$ for each object g of \mathbf{G} and h of the \mathbf{H} .

In \mathbf{FHilb} , it so happens any classical structure allows a complementary one, that is, every orthonormal basis has a mutually unbiased one. The following corollary shows that this is not always the case in \mathbf{Rel} , where dagger Frobenius structures need to be 'homogeneous' in the sense that the groupoid looks the same under any 'translation' from one object to another.

Proposition 6.10. *A Frobenius structure in \mathbf{Rel} corresponding to a groupoid \mathbf{G} allows a complementary one exactly when the cardinality of the set of all morphisms into an object g is independent of g .*

Proof. One direction is obvious after the previous proposition. We will prove the other, by constructing a complementary groupoid \mathbf{H} . We may assume that \mathbf{G} is not empty without loss of generality. Pick some object g_0 . Observe that the set of A morphisms of \mathbf{G} decomposes as $\bigcup_{g' \in \text{Ob}(\mathbf{G})} \left(\bigcup_{g \in \text{Ob}(\mathbf{G})} \mathbf{G}(g, g') \right)$. We will define \mathbf{H} by carving up the set of morphisms of \mathbf{G} the other way around. Set $\text{Ob}(\mathbf{H}) = \bigcup_{g \in \text{Ob}(\mathbf{G})} \mathbf{G}(g, g_0)$. By assumption, there are bijections $\varphi_{g'}: \text{Ob}(\mathbf{H}) \rightarrow \bigcup_{g \in \text{Ob}(\mathbf{G})} \mathbf{G}(g, g')$. Define $\mathbf{H}(h, h') = \emptyset$ for distinct h, h' , and set $\mathbf{H}(h, h) = \{\varphi_g(h) \mid g \in \text{Ob}(\mathbf{G})\}$. Then \mathbf{H} has the same set of morphisms as \mathbf{G} , and if $a \in \mathbf{G}(g, g')$, then $a = \varphi'_g(h)$ for a unique $h \in \text{Ob}(\mathbf{H})$, namely $h = \text{cod}_{\mathbf{H}}(a)$. This construction makes the map $A \rightarrow \text{Ob}(\mathbf{G}) \times \text{Ob}(\mathbf{H})$ given by $a \mapsto (\text{cod}_{\mathbf{G}}(a), \text{cod}_{\mathbf{H}}(a))$ into a bijection.

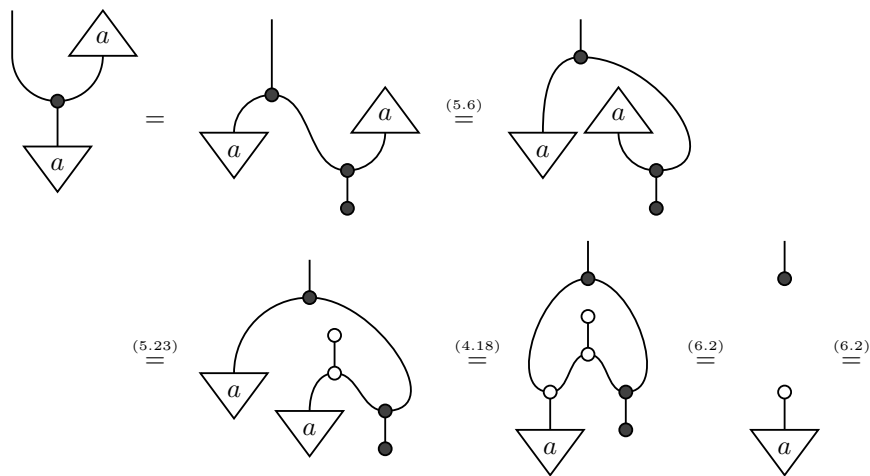
By the previous proposition, all that is left to do is to make \mathbf{H} a well-defined groupoid in some way. For this it suffices to make $\text{Ob}(\mathbf{G})$ into a group. If $\text{Ob}(\mathbf{G})$ is finite, you can use the multiplication of \mathbb{Z}_n . If $\text{Ob}(\mathbf{G})$ is infinite, then it is isomorphic to the set of its finite subsets, which form a group under the symmetric difference $U \cdot V = (U \cup V) \setminus (U \cap V)$ as multiplication. \square

Unbiased states

One way to understand complementary bases is to recognize that copyable states for one basis will be *unbiased* for a complementary basis. In other words, if you write out one basis element using column vector notation defined by the other basis, then up to an overall scalar factor, each entry will be unitary. We captured this abstractly with the notion of a *phase* for a Frobenius structure, introduced in Definition 5.40. In other words, a state is unbiased for a dagger Frobenius structure when its phase shift is unitary.

Proposition 6.11. *Let $(A, \rho_{\gamma}, \delta)$ and $(A, \rho_{\gamma}, \delta)$ be complementary symmetric dagger Frobenius structures in a braided monoidal dagger category. If a state is self-conjugate, copyable and deletable for (ρ_{γ}, δ) , then it is a phase for (ρ_{γ}, δ) .*

Proof. Using the graphical calculus:



These equalities used, in order: the noncommutative spider theorem, symmetry, self-conjugateness, copyability, complementarity, and deletability. The symmetric requirement of (5.25) is analogous. \square

6.2 The Deutsch–Jozsa algorithm

The Deutsch–Jozsa algorithm solves a certain problem faster in the quantum case than is possible in the classical case. It is typical of quantum algorithms that decide on a solution without relying on approximation. The Deutsch–Jozsa algorithm solve a slightly artificial problem, but other algorithms in this family include Shor’s factoring algorithm, Grover’s search algorithm, and the more general hidden subgroup problem. The ‘all or nothing’ nature of these algorithms make them amenable to categorical models, where we can see the difference between no information flow and maximum information flow. This section discusses the algorithm and proves its correctness categorically.

The Deutsch–Jozsa algorithm addresses the following problem. Suppose we have a 2-valued function $A \xrightarrow{f} \{0, 1\}$ on a finite set A . If the function f takes just a single value on every element of A , it is called *constant*. Another possibility is that the function takes the value 0 on exactly half the elements of A , and takes the value 1 on the other half; in this case it is called *balanced*. Most functions are neither balanced or constant, but we will restrict to those that are. The Deutsch–Jozsa problem, given a function $A \xrightarrow{f} \{0, 1\}$ promised to be either balanced or constant, is to determine which of the two is the case.

The best classical strategy is rather simple. We have no knowledge of the structure of the function f in general, so we must simply proceed to sample the function on elements of A . If we find two elements which have different values, then f cannot be constant, so we conclude that f is balanced and we are done. However, in the worst case we might have to sample $\frac{1}{2}|A| + 1$ elements until we find two elements with different values. If we sample this many elements and we find that f returns the same value for each one, then we can conclude that f is constant.

Oracles

The quantum Deutsch–Jozsa algorithm decides between the constant and balanced cases with just a *single* use of the function f . However, we have to be more precise about how to access the function f . A quantum computation only allows unitary gates; so we have to linearize the function $A \xrightarrow{f} \{0, 1\}$ to a unitary map, called an *oracle*.

Definition 6.12. In a monoidal dagger category, given Frobenius structures (A, μ, ν) and (B, μ, ν) , an *oracle* is a morphism $A \xrightarrow{f} B$ such that the following morphism is unitary:

(6.11)

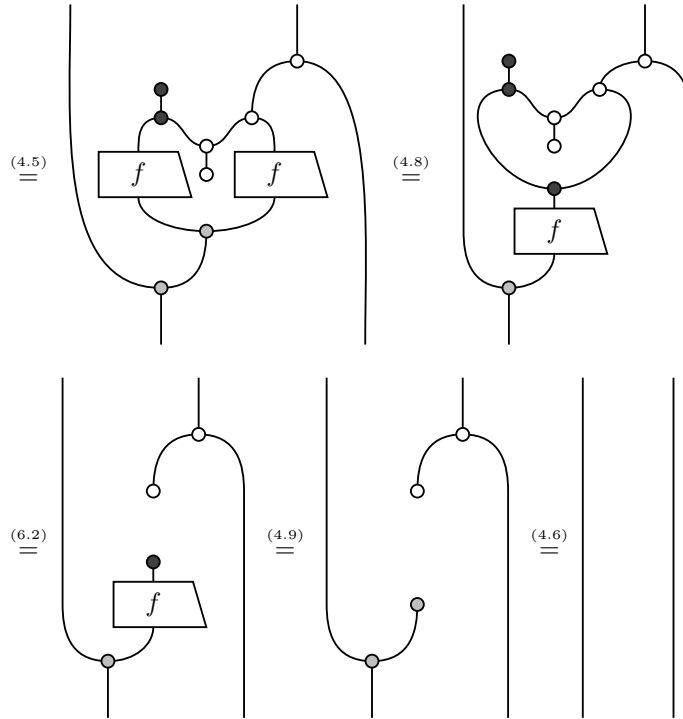
Example 6.13. Let $A \xrightarrow{f} B$ be a morphism of \mathbf{FSet} . Write H and K for the free Hilbert spaces on A and B respectively. The function f induces a morphism $H \rightarrow K$ in \mathbf{FHilb} that extends the function $a \mapsto f(a)$.

Now choose an orthogonal basis $\{e_i\}$ for K that is mutually unbiased to B , with length $\|e_i\|^2 = \dim(K)$. With this basis as the white Frobenius structure, the map (6.11) sends $a \otimes e_i$ to $\langle e_i | f(a) \rangle a \otimes e_i$, where the coefficients have amplitude $|\langle e_i | f(a) \rangle|^2 = \|e_i\|^2 \|f(a)\|^2 / \dim(K) = 1$ by (??). Hence (6.11) is unitary, and the morphism $H \rightarrow K$ is an oracle. Because it extends the function f , we say it is an *oracle for f*.

The previous example is typical: we now prove that any oracle extends a function between bases. Recall from Corollary 5.34 that functions between bases are comonoid homomorphisms between classical structures, and from Lemma 5.35 that the latter are always self-conjugate.

Proposition 6.14. Let (A, μ, ν) , (B, μ, ν) and (B, μ, ν) be symmetric dagger Frobenius structures in a braided monoidal dagger category. A self-conjugate comonoid homomorphism $(A, \mu, \nu) \xrightarrow{f} (B, \mu, \nu)$ is an oracle $(A, \mu, \nu) \rightarrow (B, \mu, \nu)$ if and only if μ is complementary to ν .

Proof. Suppose μ and ν are complementary, and compose (6.11) with its adjoint:



These equalities used the noncommutative spider theorem, self-conjugacy of f , (co)associativity, the fact that f preserves comultiplication, complementarity, the fact that f preserves the counit, and the unit and counit laws. The composition of (6.11) and its adjoint in the other order similarly gives the identity. Thus f is an oracle.

Conversely, if f is an oracle, composing the above computation with a white unit on the bottom right and a gray counit on the top left shows the left equation of (6.2). A similar argument to the composition of (6.11) with its adjoint in the other order gives the other equation, showing that $\begin{array}{c} \bullet \\ \diagdown \end{array}$ and $\begin{array}{c} \bullet \\ \diagup \end{array}$ are complementary. \square

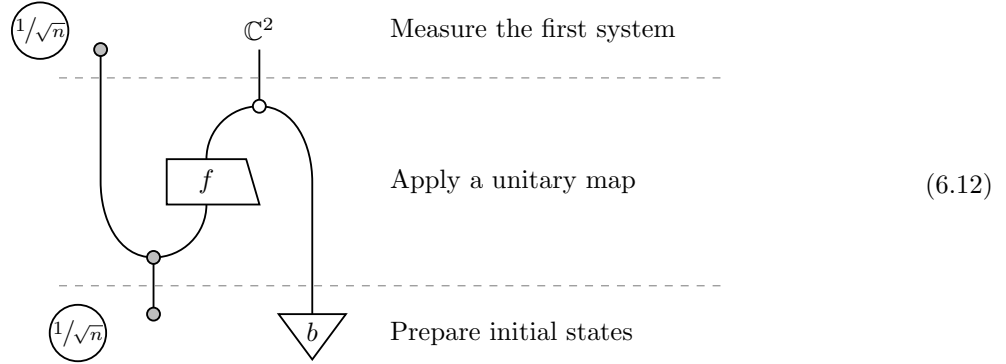
Notice that the previous proposition resembles Proposition 6.7, just with a morphism f ‘in the middle’.

The algorithm

We can now state the procedure of the Deutsch–Jozsa algorithm itself.

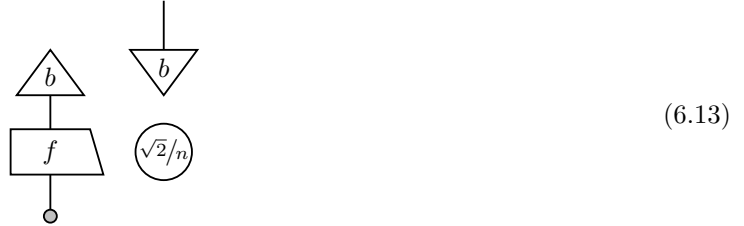
Definition 6.15 (The Deutsch–Jozsa algorithm). Say that A has n elements, and let $A \xrightarrow{f} \{0, 1\}$ be the given function. Extend it to an oracle $H \rightarrow \mathbb{C}^2$ as in Example 6.13; the two complementary bases on \mathbb{C}^2 are the computational basis and the X basis from Example 6.5 scaled by $\sqrt{2}$. Write b for the state $\begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix}$ of

\mathbb{C}^2 . The *Deutsch–Jozsa algorithm* is the following morphism in **FHilb**:



The dashed horizontal lines separate the different stages of the procedure. In the language of states and effects of Sections 1.3 and ??: first prepare two systems in initial states, one in the maximally mixed state according to the gray classical structure, the other in state b ; then apply a unitary gate; finally postselect on the first system being measured in the maximally mixed effect for the gray classical structure. The diagram (6.12) describes a particular quantum history, and taking the square of the norm of the state it represents gives the probability this history will occur.

Lemma 6.16. *The Deutsch–Jozsa algorithm (6.12) simplifies to:*



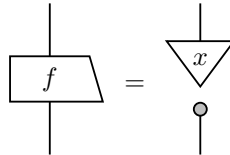
Proof. Duplicate the copyable state $\sqrt{2}b$ through the white dot in (6.12), and apply the noncommutative Spider Theorem 5.21 to the cluster of gray dots. \square

Correctness

We now set out to prove correctness of the Deutsch–Jozsa algorithm.

Lemma 6.17 (The constant case). *If the function $A \xrightarrow{f} \{0, 1\}$ is constant, then the history described in diagram (6.12) is certain.*

Proof. Suppose $f(a) = x$ for all $a \in A$. Then the oracle $H \xrightarrow{f} \mathbb{C}^2$ decomposes as:



Thus the amplitude of the main component of the quantum history (6.13) is:

$$\begin{array}{c} \triangle b \\ | \\ \text{trapezoid } f \\ | \\ \circ \end{array} = \begin{array}{c} \triangle b \\ | \\ \text{inverted trapezoid } x \\ | \\ \circ \end{array} = \pm n/\sqrt{2}$$

Hence the norm of (6.13) is 1. □

Lemma 6.18 (The balanced case). *If the function $A \xrightarrow{f} \{0,1\}$ is balanced, then the history described in diagram (6.12) is impossible.*

Proof. Suppose f takes each value of the set $\{0,1\}$ on an equal number of elements of A . To test whether a particular f is balanced, we could perform a sum indexed by $a \in A$, with summand given by $+1$ if $f(a) = 0$, and by -1 if $f(a) = 1$; the function f would be balanced exactly when this sum gives 0. Given the definition of the state b , we could equivalently test the equality $\sum_{a \in A} b^\dagger(f(a)) = 0$, with the following graphical representation:

$$\begin{array}{c} \triangle b \\ | \\ \text{trapezoid } f \\ | \\ \circ \end{array} = 0.$$

Hence the norm of (6.13) is 0. □

Theorem 6.19 (Deutsch–Jozsa is correct). *The Deutsch–Jozsa algorithm (6.12) correctly identifies constant functions $A \xrightarrow{f} \{0,1\}$.*

Proof. The squared norm of the state (6.13) is the probability of the history occurring. The previous two lemmas show that the history (6.12) is a perfect test for discriminating constant and balanced functions. □

6.3 Bialgebras

As we saw in Proposition 6.4, complementary classical structures **FHilb** are mutually unbiased bases. One common way to construct mutually unbiased bases is the following. Let G be a finite group, and consider the Hilbert space for which $\{g \in G\}$ is an orthonormal basis. Defining

$$\begin{array}{c} \curvearrowright \\ \bullet \end{array} : g \mapsto g \otimes g \qquad \begin{array}{c} \circ \\ | \\ \bullet \end{array} : g \mapsto 1 \qquad (6.14)$$

$$\begin{array}{c} \bullet \\ \curvearrowleft \end{array} : g \otimes h \mapsto gh \qquad \begin{array}{c} \bullet \\ | \\ \bullet \end{array} : 1 \mapsto 1_G \qquad (6.15)$$

gives complementary dagger Frobenius structures; see Examples 4.2 and 5.2. This construction additionally satisfies $\begin{array}{c} \curvearrowright \\ \circ \\ \bullet \end{array} \circ \begin{array}{c} \bullet \\ \curvearrowleft \end{array} : g \otimes h \mapsto gh \otimes gh$, which is captured abstractly as follows.

Definition 6.20 (Bialgebra, dagger bialgebra). A *bialgebra* in a braided monoidal category consists of a monoid $(\bullet, \curvearrowright)$ and a comonoid (\curvearrowleft, \circ) on the same object, satisfying the following *bialgebra laws*:

$$\begin{array}{c} \cup \\ \circ \\ \cap \end{array} \bullet = \begin{array}{c} \cup \\ \bullet \end{array} \begin{array}{c} \cup \\ \bullet \end{array} \qquad \begin{array}{c} \cap \\ \bullet \end{array} = \begin{array}{c} \cap \\ \bullet \end{array} \begin{array}{c} \cap \\ \bullet \end{array} \qquad \begin{array}{c} \cup \\ \bullet \end{array} = \begin{array}{c} \cup \\ \bullet \end{array} \begin{array}{c} \cup \\ \bullet \end{array} \qquad \begin{array}{c} \cap \\ \bullet \end{array} = \begin{array}{c} \cap \\ \bullet \end{array} \begin{array}{c} \cap \\ \bullet \end{array} \qquad (6.16)$$

The last equation is not missing a picture, because we are drawing id_I as the empty picture (1.6). A bialgebra is *commutative* when the underlying monoid and comonoid are commutative. In a braided monoidal dagger category, a *dagger bialgebra* is a bialgebra for which $\begin{array}{c} \bullet \\ \diagdown \quad \diagup \\ \bullet \end{array} = \begin{array}{c} \bullet \\ \diagup \quad \diagdown \\ \bullet \end{array}$.

Example 6.21. There are many interesting examples of bialgebras.

- Any monoid M is a bialgebra in **Set**, by choosing

$$\begin{array}{c} \curvearrowright \\ \bullet \end{array} : m \mapsto (m, m) \qquad \varphi : m \mapsto \bullet \qquad \begin{array}{c} \bullet \\ \diagdown \quad \diagup \\ \bullet \end{array} : (m, n) \mapsto mn \qquad \begin{array}{c} \bullet \\ \diagdown \\ \bullet \end{array} : \bullet \mapsto 1_M.$$

- Any monoid M in **FSet** induces a bialgebra in **FHilb** as follows. Let $(A, \begin{array}{c} \bullet \\ \diagdown \quad \diagup \\ \bullet \end{array}, \begin{array}{c} \bullet \\ \diagdown \\ \bullet \end{array})$ be the group algebra; see Example 5.2. Define

$$\begin{array}{c} \curvearrowright \\ \bullet \end{array} : m \mapsto m \otimes m \qquad \varphi : m \mapsto 1$$

When M is a group, $(A, \begin{array}{c} \bullet \\ \diagdown \quad \diagup \\ \bullet \end{array}, \begin{array}{c} \bullet \\ \diagdown \\ \bullet \end{array})$ can also be made into a Frobenius structure as in Example 5.2, but with different $\begin{array}{c} \curvearrowright \\ \bullet \end{array}$ and φ . In Section ?? we will see a converse: bialgebras in **FSet** satisfying some additional properties always arise from groups like this.

Any monoid in **Set** induces a bialgebra in **Rel** in a similar way.

- The space of complex polynomials in one variable $\mathbb{C}[x]$ gives rise to a commutative dagger bialgebra in **Hilb**. The Hilbert space in question, also called *Fock space* has $\{1, x, x^2, x^3, \dots\}$ as an orthonormal basis, and multiplication $\begin{array}{c} \bullet \\ \diagdown \quad \diagup \\ \bullet \end{array} : \mathbb{C}[x] \otimes \mathbb{C}[x] \rightarrow \mathbb{C}[x]$ is defined by

$$x^n \otimes x^m \mapsto \sqrt{\frac{(m+n)!}{m!n!}} x^{m+n}.$$

This is a heuristic idea, since the resulting linear map $\mathbb{C}[x] \otimes \mathbb{C}[x] \rightarrow \mathbb{C}[x]$ is unbounded, and hence not technically a morphism in **Hilb**.

The following concise formulation is a good way to remember the bialgebra laws; compare ??.

Lemma 6.22. *The following are equivalent in a braided monoidal category:*

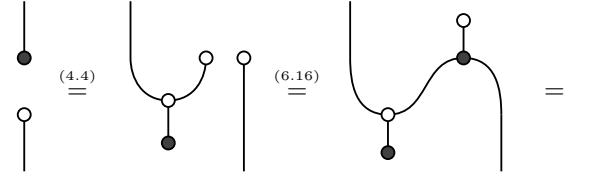
- a comonoid $(A, \begin{array}{c} \curvearrowright \\ \bullet \end{array}, \varphi)$ and monoid $(A, \begin{array}{c} \bullet \\ \diagdown \quad \diagup \\ \bullet \end{array}, \begin{array}{c} \bullet \\ \diagdown \\ \bullet \end{array})$ form a bialgebra;
- $\begin{array}{c} \bullet \\ \diagdown \quad \diagup \\ \bullet \end{array}$ and $\begin{array}{c} \bullet \\ \diagdown \\ \bullet \end{array}$ are comonoid homomorphisms;
- $\begin{array}{c} \curvearrowright \\ \bullet \end{array}$ and φ are monoid homomorphisms.

Proof. The canonical comonoid structure on $A \otimes A$ is that of Lemma 4.8. Unfolding what it means for $\begin{array}{c} \bullet \\ \diagdown \quad \diagup \\ \bullet \end{array}$ to be a comonoid homomorphism: comultiplication preservation gives the first of the bialgebra laws (6.16); counit preservation gives the second; and the last two come from requiring that $\begin{array}{c} \bullet \\ \diagdown \\ \bullet \end{array}$ is a comonoid homomorphism. The case of monoid homomorphisms is analogous. \square

As far as interaction between monoids and comonoids is concerned, Frobenius structures and bialgebras are opposite extremes. The following theorem shows that both cannot happen simultaneously, except in the trivial case. What leads to the degeneracy is the fact that the Frobenius law (5.1) equates *connected* diagrams, whereas the bialgebra laws (6.16) equate connected diagrams with *disconnected* ones.

Theorem 6.23 (Frobenius bialgebras are trivial). *If a monoid $(A, \begin{array}{c} \bullet \\ \diagdown \quad \diagup \\ \bullet \end{array}, \begin{array}{c} \bullet \\ \diagdown \\ \bullet \end{array})$ and comonoid $(A, \begin{array}{c} \curvearrowright \\ \bullet \end{array}, \varphi)$ form both a Frobenius structure and a bialgebra in a braided monoidal category, then $A \simeq I$.*

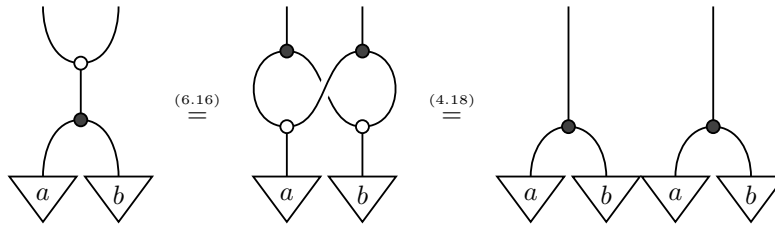
Proof. We will show that \bullet and φ are inverse morphisms. The bialgebra laws (6.16) already require $\varphi \circ \bullet = \text{id}_I$. For the other composite:



The first equality is counitality, the second equality is the second bialgebra law, and the last equality follows from Theorem 5.15. \square

Lemma 6.24. *Let $(A, \bullet, \varphi, \varphi', \varphi)$ be a bialgebra in a braided monoidal category. The states that are copyable by φ' and deletable by φ form a monoid under \bullet with unit \bullet .*

Proof. Associativity (4.5) is immediate. Unitality (4.6) comes down to the third and fourth bialgebra laws (6.16): \bullet is copyable by φ' and deletable by φ . What has to be proven is that if we multiply two φ' -copyable states using \bullet , we get another φ' -copyable state:



Similarly using the second bialgebra law (6.16) shows that multiplying two φ -deletable states with \bullet gives another φ -deletable state. \square

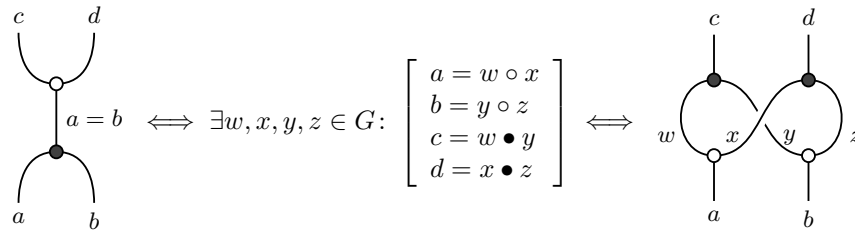
Strong complementarity

We now investigate the relationship between complementarity and bialgebras.

Lemma 6.25. *The special dagger Frobenius structures in \mathbf{Rel} induced by a group and a discrete groupoid on the same set of morphisms form a bialgebra.*

The bialgebra structure is between the monoid part of one structure and the comonoid part of the other. This must be the case, since we saw that Frobenius bialgebras are trivial in Theorem 6.23.

Proof. Let $(G, \circ, 1)$ be a group and (G, \bullet) a discrete groupoid. Then:



because for $c = w \bullet y$ to make sense we must have $c = w = y$. Similarly:

$$\begin{array}{c} \circ \\ | \\ \bullet \\ \swarrow \quad \searrow \\ a \quad b \end{array} \iff a \bullet b = 1 \iff a = b = 1 \iff \begin{array}{cc} \circ & \circ \\ | & | \\ a & b \end{array}$$

The final two bialgebra laws hold similarly by Proposition 6.9. \square

It is not true that any two complementary groupoids form a bialgebra in **Rel**, as the following counterexample demonstrates.

Example 6.26. The following two groupoids are complementary, but do not form a bialgebra in **Rel**.

$$\begin{array}{cc} a & c \\ \curvearrowright & \curvearrowright \\ 0 & 1 \\ \curvearrowleft & \curvearrowleft \\ b & d \end{array} \qquad \begin{array}{cc} a & c \\ \curvearrowright & \curvearrowright \\ 0 & 1 \\ \curvearrowleft & \curvearrowleft \\ d & b \end{array}$$

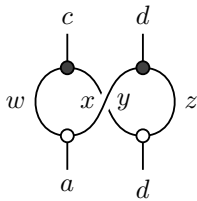
$$\begin{array}{l} b^2 = a = \text{id}_0 \\ d^2 = c = \text{id}_1 \end{array} \qquad \begin{array}{l} d^2 = a = \text{id}_0 \\ b^2 = c = \text{id}_1 \end{array}$$

Proof. Both groupoids have $G = \{a, b, c, d\}$ as set of morphisms, and $\{a, c\}$ as set of identities. Write \circ for the composition in the left groupoid, and \bullet for the right one. The function $G \rightarrow \{0, 1\}^2$ given by $g \mapsto (\text{cod}_\circ(g), \text{cod}_\bullet(g))$ is bijective:

$$a \mapsto (0, 0) \quad b \mapsto (0, 1) \quad c \mapsto (1, 1) \quad d \mapsto (1, 0)$$

Hence the two groupoids are complementary by Proposition 6.9.

Notice that $a \bullet d = d = c \circ d$. Hence $(a, d) \sim (c, d)$ in the left-hand side of the first bialgebra law (6.16). Suppose it held in the right-hand side too:



Then $w \bullet y = c$, so either $w = y = c$, or $w = y = b$. But also $y \circ z = d$, so either $y = c$ and $z = d$, or $y = d$ and $z = c$. Therefore $w = y = c$ and $z = d$. But that contradicts $w \circ x = a$, so the two groupoids do not form a bialgebra. \square

The same situation occurs in **FHilb**: complementary Frobenius structures often do not form a bialgebra.

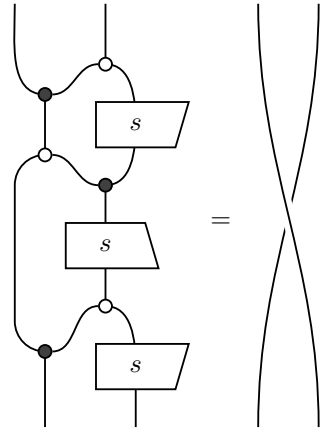
Example 6.27. Consider the object \mathbb{C}^2 in **FHilb**. The computational basis $\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ gives it a dagger Frobenius structure $\begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ \circ \end{array}$ for any angles $\varphi, \theta \in \mathbb{R}$. The orthogonal basis $\left\{ \begin{pmatrix} e^{i\varphi} \\ e^{i\theta} \end{pmatrix}, \begin{pmatrix} e^{i\varphi} \\ -e^{i\theta} \end{pmatrix} \right\}$ gives it a dagger Frobenius structure $\begin{array}{c} \circ \\ \swarrow \quad \searrow \\ \bullet \end{array}$. These two Frobenius structures are complementary, but they can only form a bialgebra when the angles φ and θ are integer multiples of 2π .

Proof. Write $\{a, b\}$ for the computational basis, and $\{c, d\}$ for the other one. The two bases are complementary because $\langle a|c\rangle\langle c|a\rangle = \langle a|d\rangle\langle d|a\rangle = \langle b|c\rangle\langle c|b\rangle = \langle b|d\rangle\langle d|b\rangle = 1$. Plugging in $c \otimes d$, the

Controlled negation

The following theorem proves that the first bialgebra law is equivalent to the property that the swap map can be built from three CNOT gates.

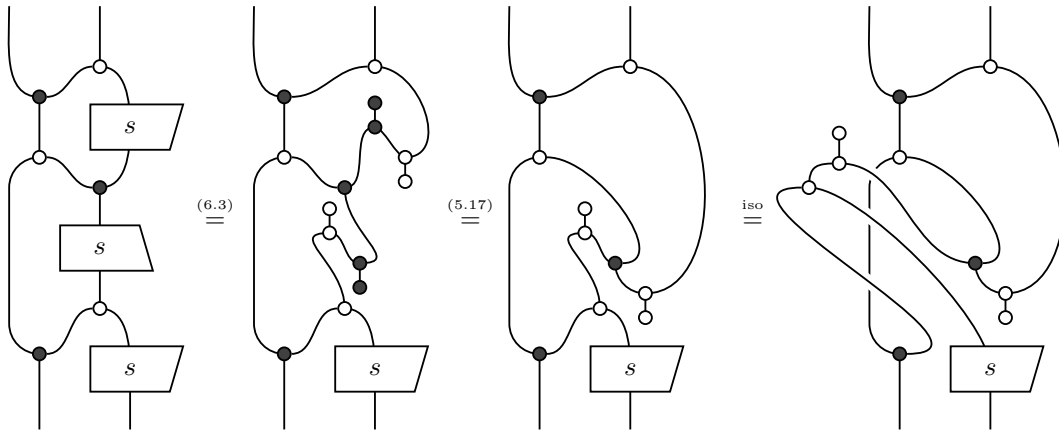
Theorem 6.31 (Swap via three CNOTs). *Let (\downarrow, \bullet) and (\uparrow, \circ) be complementary classical structures in a braided monoidal dagger category. If they are strongly complementary, then the following equation holds, where s is the morphism (6.3):*

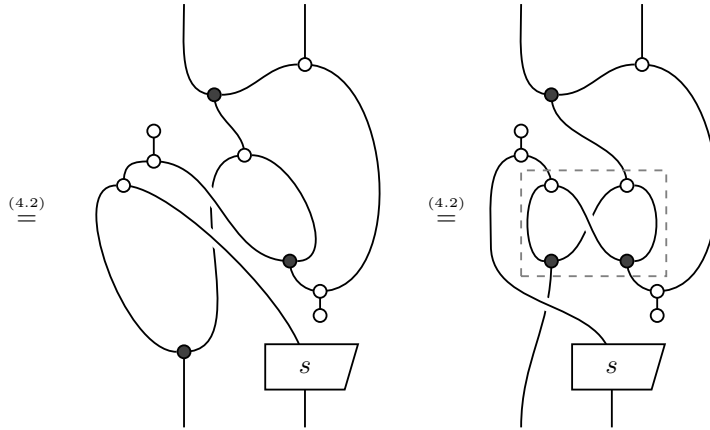


(6.17)

In fact, equation (6.17) holds if and only if the first equation of (6.16) does.

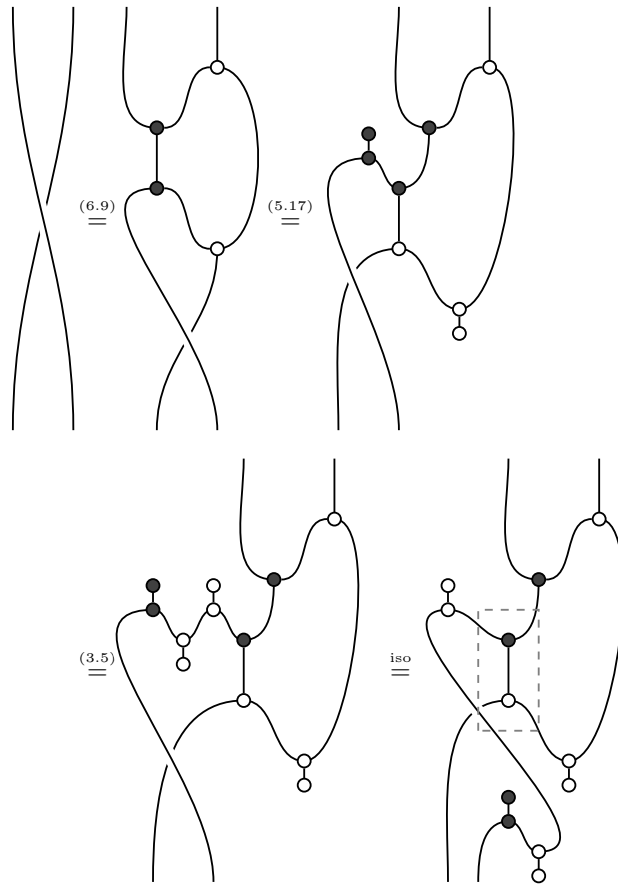
Proof. First, rewrite the left-hand side of (6.17):





The second equality uses the (noncommutative) black spider Theorem 5.21, the fourth uses cocommutativity of Ψ , and fifth uses the (commutative) white spider Theorem 5.22.

Rewrite the right-hand side similarly:



The first equality comes from Proposition 6.7.

Now, using strong complementarity on the marked parts turns the left-hand side into the right-hand side. Conversely, if the left-hand side equals the right-hand side, we can use snake equations to ‘undo’ everything but the marked bits to see that the bialgebra law must hold. \square

Why may we think of the left-hand side of (6.17) as a generalization of ‘three CNOT gates’? It is clearly a composition of six unitary maps, namely three unitaries of the form (6.9), and three of the form (6.3).

Example 6.32. In the category \mathbf{FHilb} , fix A to be the qubit \mathbb{C}^2 . Let (\downarrow, \uparrow) be defined by the computational basis $\{|0\rangle, |1\rangle\}$, and (φ', φ) by the X basis from Example 6.5. Then the three antipodes (6.3) become identities.

Furthermore, the three unitaries of the form (6.9) indeed reduce to three CNOT gates. This gate performs a NOT operation on the second qubit if the first (control) qubit is $|1\rangle$, and does nothing if the first qubit is $|0\rangle$.

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (6.18)$$

We will fix these two classical structures for the rest of this chapter. The relationship between them is $|+\rangle = |0\rangle + |1\rangle$, and $|-\rangle = |0\rangle - |1\rangle$. Hence they are transported into each other by the *Hadamard gate* (see also Lemma 5.17).

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{array}{c} | \\ \text{---} \\ \text{H} \\ \text{---} \\ | \end{array} \quad (6.19)$$

Controlled phases

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

In the following lemma, we will draw dots loosely, as in Section 5.5. This is allowed, because we are dealing with classical structures.

Lemma 6.33. *The CZ gate in \mathbf{FHilb} can be defined as follows.*

$$CZ := \begin{array}{c} | \\ \bullet \\ \text{---} \\ \text{H} \\ \text{---} \\ \bullet \\ | \end{array} \quad (6.20)$$

Proof. We can rewrite equation (6.20) as follows.

$$CZ \stackrel{(5.12)}{=} \begin{array}{c} | \\ \text{---} \\ \text{H} \\ | \\ \bullet \\ \text{---} \\ \text{H} \\ | \end{array}$$

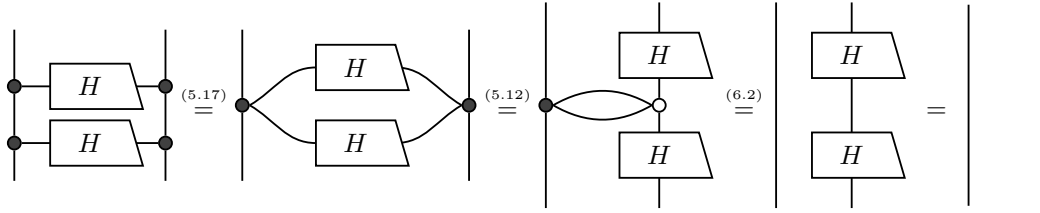
Hence

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

This is indeed the controlled Z gate. □

Proposition 6.34 (CZ has order two). *If $(A, \downarrow, \uparrow)$ and (A, φ', φ) are complementary classical structures in a braided monoidal dagger category, and $A \xrightarrow{H} A$ satisfies $H \circ H = \text{id}_A$, then (6.20) makes sense and satisfies $CZ \circ CZ = \text{id}$.*

Proof. Easy graphical manipulation:

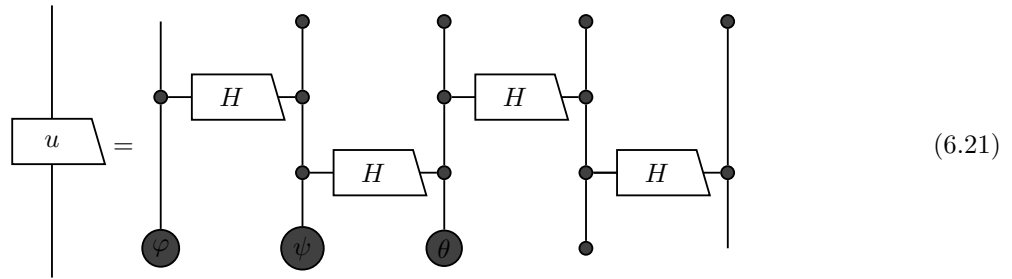


The third equality uses Proposition 6.7. □

Single qubit gates

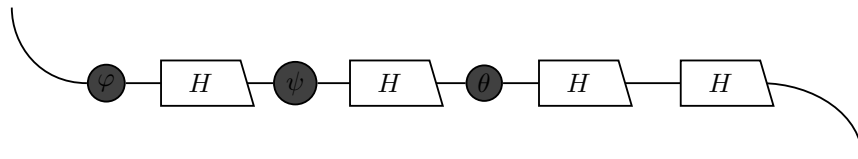
Finally, qubits have the nice property that any unitary on them can be implemented via its *Euler angles*. More precisely: for any unitary $\mathbb{C}^2 \xrightarrow{u} \mathbb{C}^2$, there exist phases $\varphi, \psi, \theta \in \mathbb{C}$ such that $u = Z_\theta \circ X_\psi \circ Z_\varphi$, where Z_θ is the unitary rotation in the Z basis over angle θ , and X_φ in the X basis over angle φ . Therefore we can implement such unitaries abstractly using just CZ-gates and Hadamard gates.

Theorem 6.35. *If a unitary $\mathbb{C}^2 \xrightarrow{u} \mathbb{C}^2$ in \mathbf{FHilb} has Euler angles φ, ψ, θ , then:*

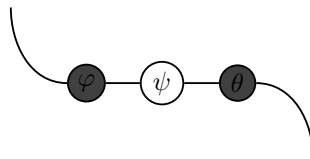


The phased spider notation here is that of Corollary 5.46.

Proof. By using the Phased spider Corollary 5.46 equation (6.21) reduces to



But by Lemma 5.17, this is just:



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