Categories and Quantum Informatics: Frobenius structures

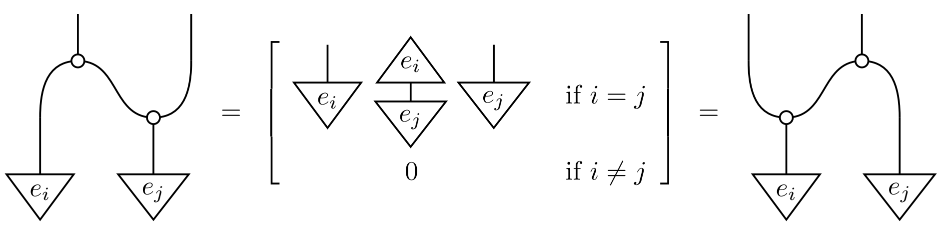
Chris Heunen

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.

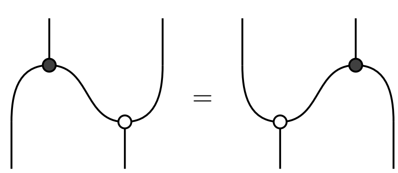
5.1 Frobenius structures

If $\{e_i\}$ is an orthogonal basis for a finite-dimensional Hilbert space H, then the copying map : $e_i \mapsto e_i \otimes e_i$ is the comultiplication of a comonoid; see Example 4.2. The adjoint multiplication is the comparison map given by $e_i \otimes e_i \mapsto \langle e_i | e_i \rangle e_i$ 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 $(A, ,)$ and a monoid $(A, ,)$ 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 : $A \otimes A \longrightarrow A$ by linearly extending $g \otimes h \mapsto gh$, and define : $\mathbb{C} \longrightarrow A$ by $z \mapsto z \cdot 1_G$. This monoid is called the *group algebra*. Its adjoint is given by

$$
\begin{aligned}
&: A \longrightarrow A \otimes A \qquad && g \mapsto \sum_{h \in G} gh^{-1} \otimes h = \sum_{h \in G} h \otimes h^{-1} g \\
&: A \longrightarrow I \qquad && g \mapsto \begin{bmatrix} 1 & \text{if } g = 1_G \\ 0 & \text{if } g \neq 1_G \end{bmatrix}
\end{aligned}
$$

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 $g \otimes h$.

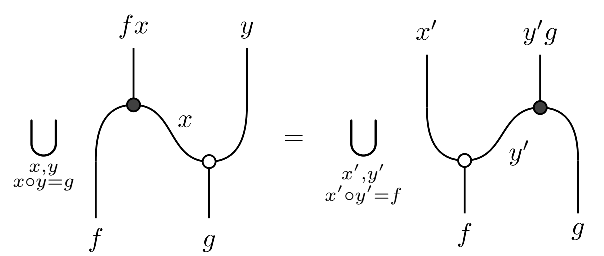
Example 5.3 (Groupoid Frobenius structure)**.** Any group G also induces a Frobenius structure in **Rel**:

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

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

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

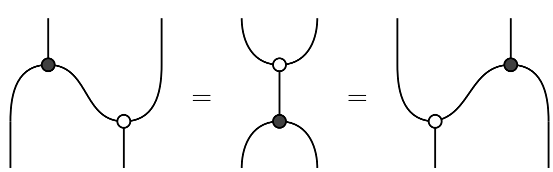
where again is the converse relation of , and that of . To see that this satisfies the Frobenius law (5.1), evaluate it on arbitrary input (f, g) in the decorated notation of Section 3.3:



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.

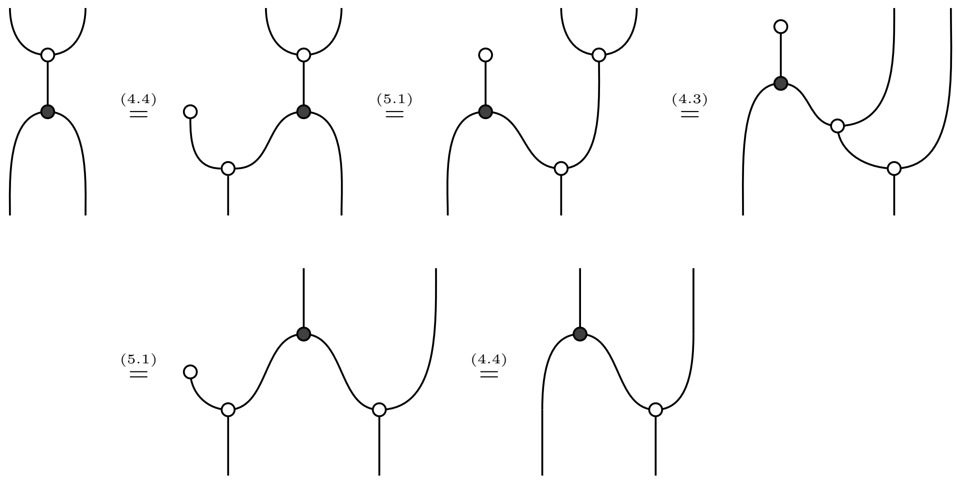
Frobenius structures automatically satisfy a further equality.

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



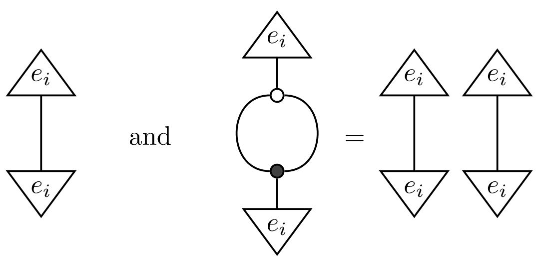
(5.4)

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



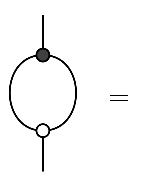
These equations use, respectively: counitality, the Frobenius law, coassociativity, the Frobenius law, and counitality. □

Consider again the Frobenius structure in **FHilb** induced by copying an orthogonal basis $\{e_i\}$. As we saw in Section 2.2, 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 $(A, \ , \ )$ and a comonoid $(A, \ , \ )$ is *special* when is a left inverse of :

 (5.5)

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

Symmetry and commutativity

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

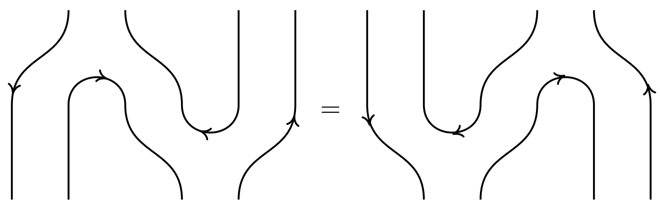
Definition 5.7 (Dagger Frobenius structure)**.** A Frobenius structure (A, , , ,) in a monoidal dagger category is a *dagger Frobenius structure* when = and = .

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

Example 5.8. The Frobenius structure in **FHilb** induced by a choice of orthogonal basis is a 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. $\square$

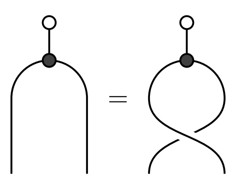
By Example 4.12, the algebra $\mathbb{M}_n$ of n-by-n complex matrices is therefore a dagger Frobenius structure in **FHilb**. We will also specifically be interested in commutative Frobenius structures. For example, the Frobenius structure induced by copying an orthonormal basis is commutative. As it allows us to copy and delete information, we think of this as *classical structure*. Rather than a negative statement about *quantum* objects like in Chapter 4 ("you *cannot* copy them uniformly", 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:



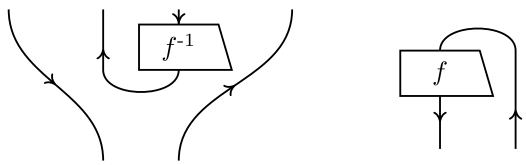
(5.6)

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: $\mathrm{Tr}(ab) = \mathrm{Tr}(ba)$.
- 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 $g \circ h = \mathrm{id}_B$ for some object B. The right-hand side contains $(g, h) \sim \bullet$ when $h \circ g = \mathrm{id}_A$ for some object A. Both mean that $h = g^{-1}$.

Example 5.14. Here is 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 $\mathrm{id}_{A^*} \otimes f^* \neq f \otimes \mathrm{id}_A$. Consider the pair of pants monoid of Lemma 4.11, take the coname $\llcorner f \lrcorner \colon A^* \otimes A \to I$ of f as counit, and $\mathrm{id}_{A^*} \otimes \ulcorner f^{-1} \urcorner \otimes \mathrm{id}_A$ as comultiplication.

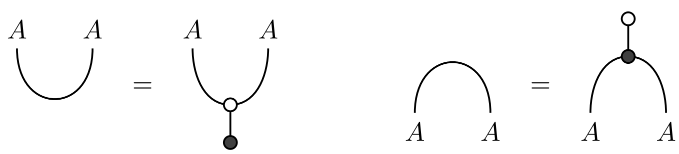


Proof. The comonoid laws follow just as in Lemma 4.11, and the Frobenius law follows similarly. The left-hand side of (5.6) becomes $\mathrm{id}_{A^*} \otimes f^*$, but the right-hand side becomes $f \otimes \mathrm{id}_A$. This contradicts the assumption, so this Frobenius structure is not symmetric.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

Self-duality and nondegenerate forms

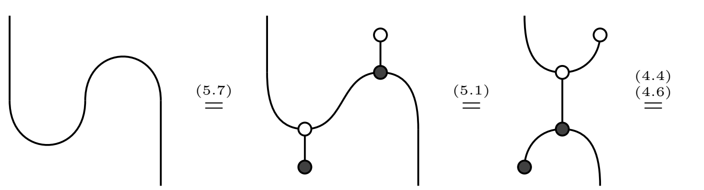
Let's now consider some properties of general Frobenius structures. First of all, they are closely related to dual objects.

Theorem 5.15 (Frobenius structures have duals)**.** *If $(A, , , ,)$ 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:*



(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:



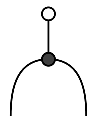
The other snake equation is proved similarly. □

It follows from the previous theorem that, if we chose a Frobenius structure on every object in a given monoidal category, then that category would have duals. 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* $(A, \cdot, \cdot)$ *in a monoidal category there is a bijective correspondence between:*

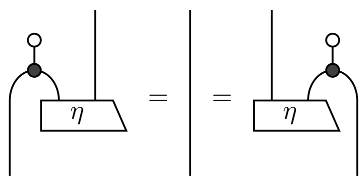
- *comonoids* $(A, \cdot, \cdot)$ *making the pair into a Frobenius structure;*
- *morphisms* $\cdot\colon A \to I$ *making the composite*



(5.8)

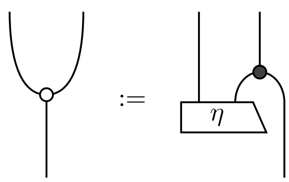
the cap of a self-duality $A \dashv A$*. Such maps are called* nondegenerate forms*.*

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 $(A, \cdot, \cdot)$ and a nondegenerate form $\cdot\colon A \to I$. That is, there exists a morphism $I \xrightarrow{\eta} A \otimes A$ satisfying the following equations:



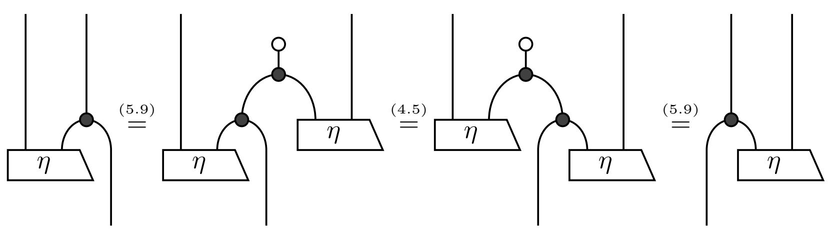
(5.9)

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



(5.10)

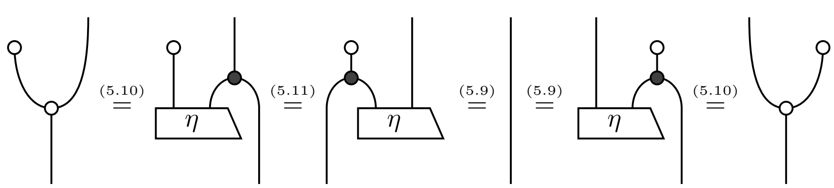
The following computation shows that we could have defined the comultiplication with the η on the left or the right, using the nondegeneracy property, associativity, and the nondegeneracy property again:



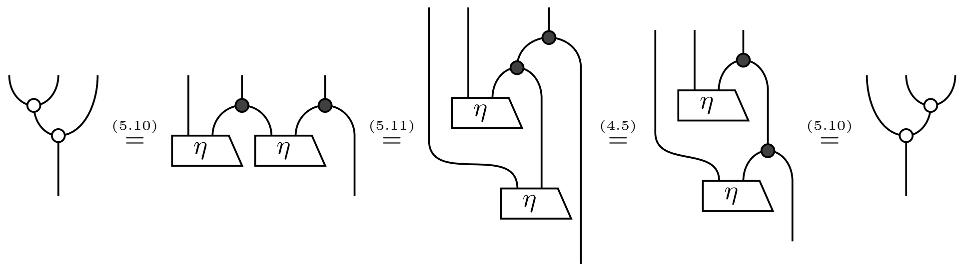
(5.11)

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

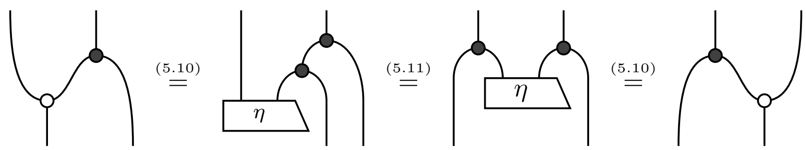
Counitality is the easiest property to demonstrate, using the definition of the comultiplication, symmetry of the comultiplication, nondegeneracy twice, and definition of the comultiplication:



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:



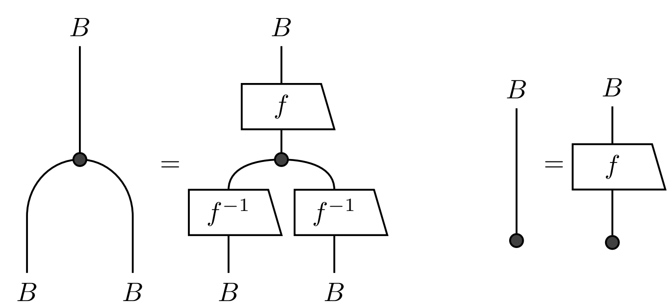
This completes the description of the correspondence.

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. □

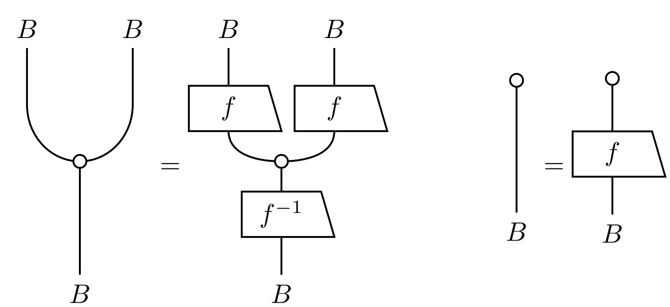
Homomorphisms

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

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



(5.12)



(5.13)

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

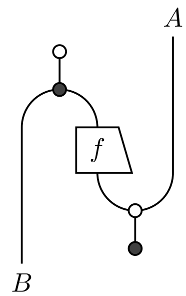
Proof. Straightforward graphical manipulation. □

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.

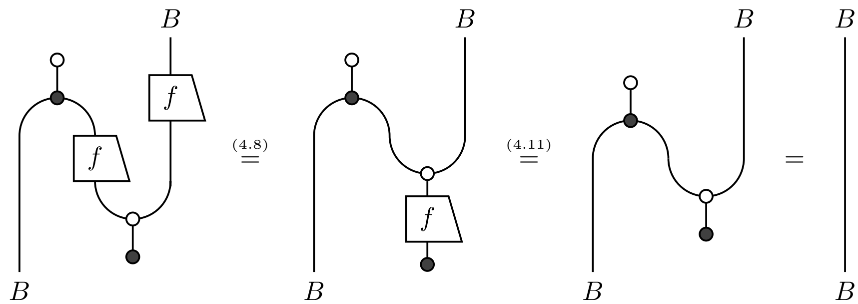
Lemma 5.19. *In a monoidal category, a homomorphism of Frobenius structures is invertible, and the inverse is again a homomorphism of Frobenius structures.*

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:



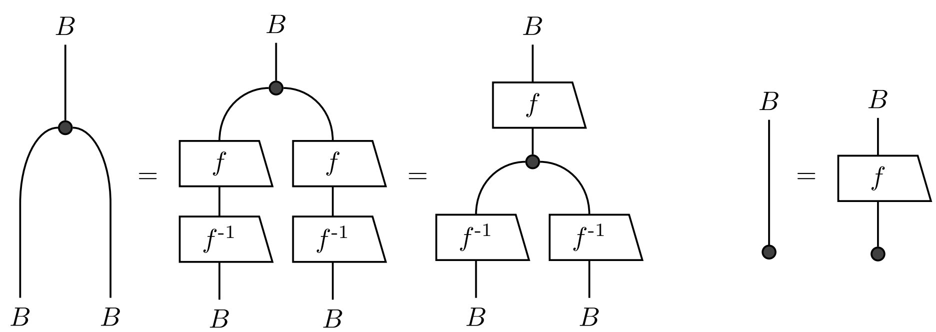
(5.14)

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

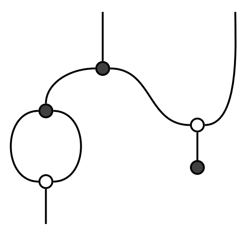
In general there are two ways to think about the graphical calculus:

- a diagram represents a morphism: it is just a shorthand to write down a linear map, for example, in the category **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), discard (using), fuse (using) and create (using) information. In fact, in symmetric monoidal categories, there is only one, but the situation is more subtle in braided monoidal categories.

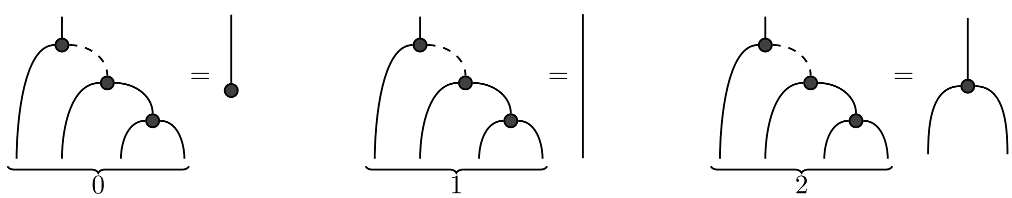
Normal forms for Frobenius structures

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



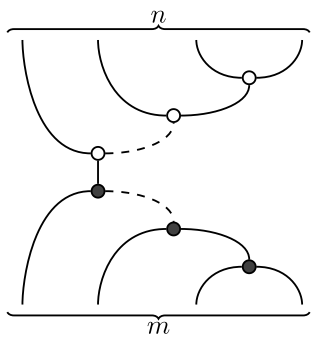
We can think of it as a graph: the wires are edges, and each dot $\circ$ or $\bullet$ is a vertex, as is the end of each input or output wire. Such a morphism is *connected* when it has a graphical representation which has a path between any two vertices.

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



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

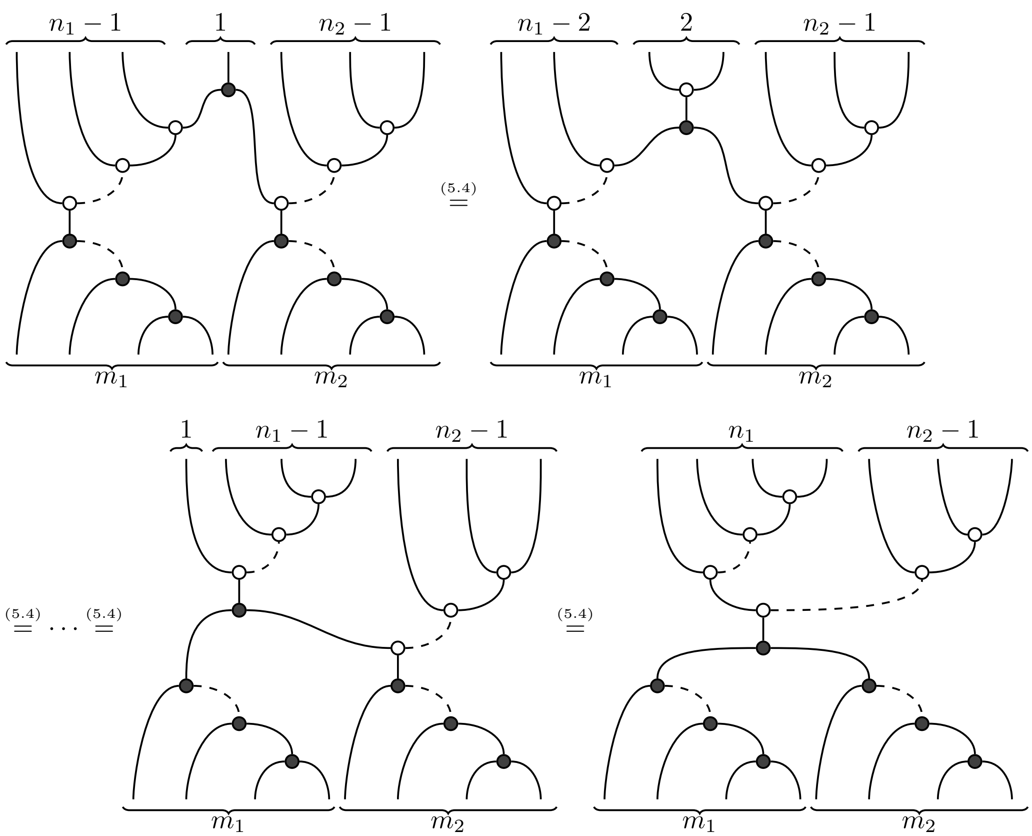
, *and* id*, using* $\circ$ *and* $\otimes$*, equals:*



(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 , , , . 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 , 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 , associativity (4.5) finishes the proof. It cannot be a because the diagram was assumed connected. That leaves the case of a . We distinguish whether the part of the diagram below the is connected or not.

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



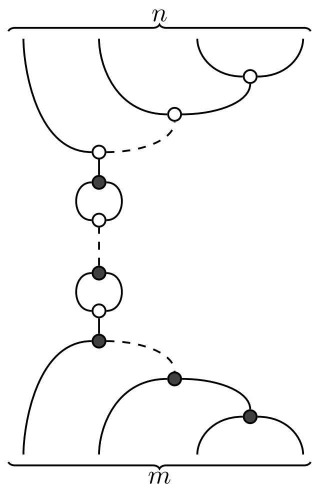
(5.16)

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

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

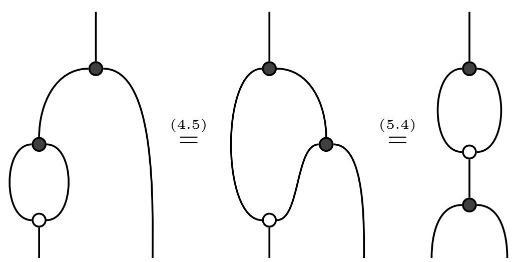
Normal form results for Frobenius structures such as the previous lemma are called Spider Theorems because (5.15) looks a bit like an $(m+n)$–legged spider. It extends to the nonspecial case as well.

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



(5.17)

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



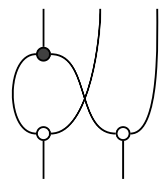
(5.18)

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

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

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

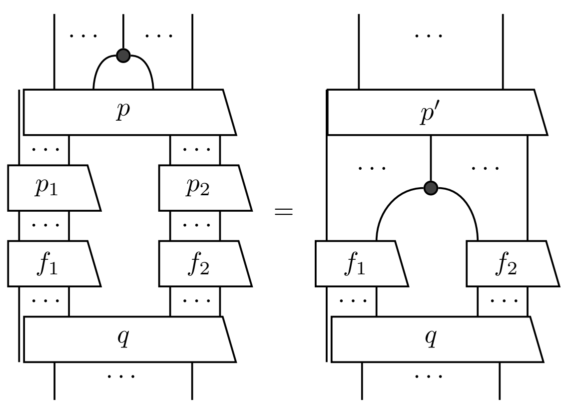


We will call a morphism $A^{\otimes n} \xrightarrow{p} A^{\otimes n}$ built from pieces id and using $\circ$ and $\otimes$ *permutations*. They correspond to bijections $\{1, \ldots, n\} \to \{1, \ldots, n\}$, and we may write things like $p^{-1}(2)$ for the (unique) input wire that p connects to the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

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

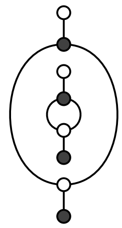
Proof. Again use the same strategy as in Lemma 5.20. Without loss of generality we may assume there are no above the topmost dot, because they will vanish by coassociativity (4.3) and cocommutativity (4.2) once we have rewritten the lower subdiagram in a normal form (5.17). So again the proof reduces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

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



Now the subdiagram consisting of f_i and the topmost is of the form (5.16), 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). $\square$

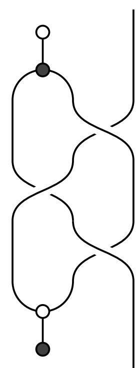
For a (co)commutative Frobenius structure in a symmetric monoidal category, any morphism built from the basic ingredients by finite means, connected or not, equals $p \circ (f_1 \otimes \cdots \otimes f_n) \circ q$ for some permutations p, q and morphisms $f_1, \ldots, f_n$ of the form (5.17); the permutations 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 $A \longrightarrow A$. □

5.3 Justifying the Frobenius law

Morphisms $A \longrightarrow A$ 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'.

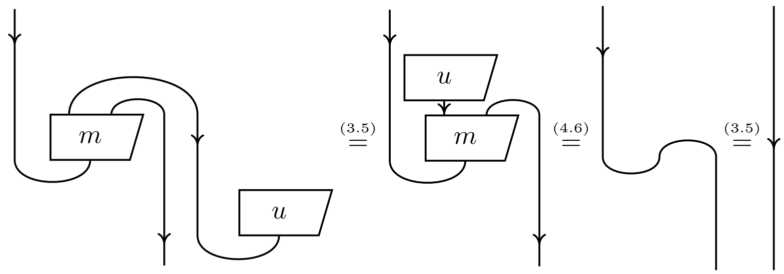
Involutive monoids

Any morphism $H \xrightarrow{f} K$ in a monoidal dagger category gives rise to another morphism $K \xrightarrow{f^\dagger} H$. The name $\ulcorner f \urcorner \colon I \longrightarrow H^* \otimes K$ 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 $A \longrightarrow A^*$. 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 $H \longrightarrow H$, which also has an involution $A \longrightarrow A^*$ 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.

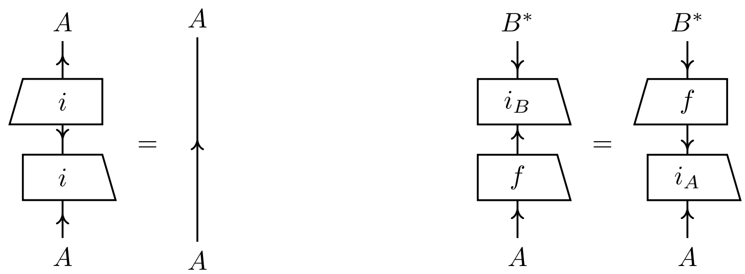
Lemma 5.24 (The opposite monoid)**.** *If (A, m, u) is a monoid in a monoidal dagger category* **C***, and $A \dashv A^*$ is a dagger dual object, then (A^*, m_*, u_*) is a monoid too.*

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



Associativity of m_* similarly follows from associativity of m. $\square$

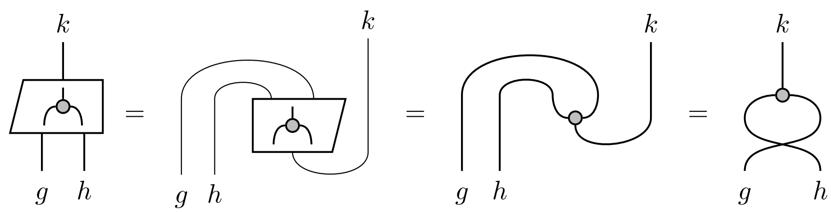
Definition 5.25 (Involutive monoid)**.** A monoid $(A, ,)$ on an object with a dagger dual is an *involutive monoid* when it comes equipped with an *involution*: a morphism of monoids $A \xrightarrow{i} A^*$ satisfying $i_* \circ i = \mathrm{id}_A$. A *morphism of involutive monoids* is a monoid homomorphism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



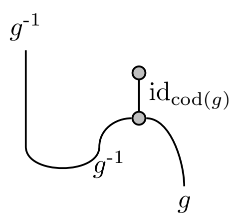
(5.19)

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

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

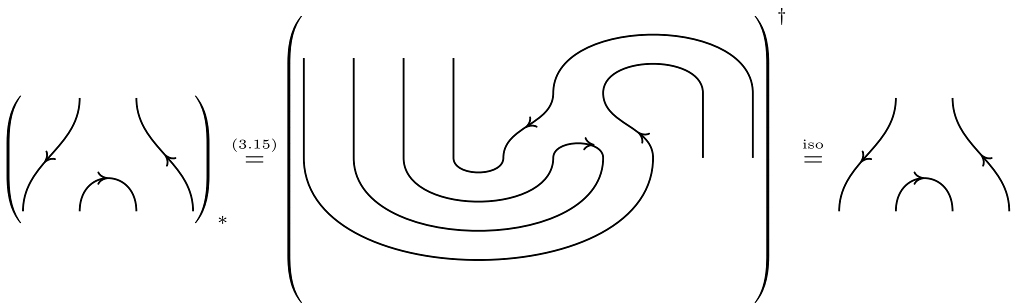


(The opposite multiplication is not simply itself, even though $G^* = G$ in **Rel**; it might only look that way because the picture is left-right symmetric.) There is a canonical involution $G \to G^*$ given by $g \sim g^{-1}$:



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:

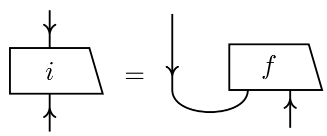


However, two abstract identifications hide the concrete algebra. Consider $A = \mathbb{C}^n$ in **FHilb**, so the pair of pants monoid $A^* \otimes A$ becomes the matrix algebra $\mathbb{M}_n$ as in Example 4.12. First, since the dual space A^* in **FHilb** consists of functions $A \longrightarrow I$, 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 $\mathbb{M}_n \longrightarrow \mathbb{M}_n^*$ 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 $(A, ,)$ on an object object A has an involution i in terms of a map $A \otimes A \xrightarrow{f} I$:

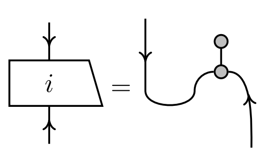


A canonical choice for such a map would be : $A \otimes A \longrightarrow I$. For a pair of pants monoid as in Example 5.27, this would give $i = \mathrm{id}_{H^* \otimes H}$. Compare also Proposition 5.16.

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

(a) $(A, , , ,)$ is a dagger Frobenius structure;

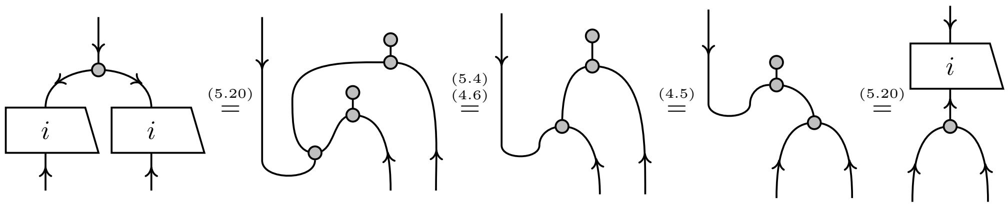
(b) the following map makes $(A, ,)$ into an involutive monoid:



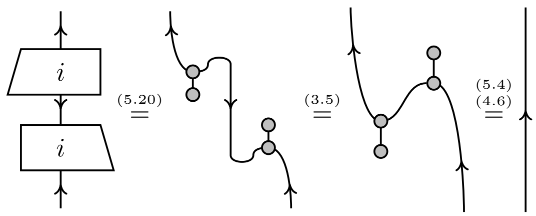
(5.20)

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.

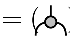
Proof. Assuming (a), we prove that i respects multiplication as in equation (4.10):

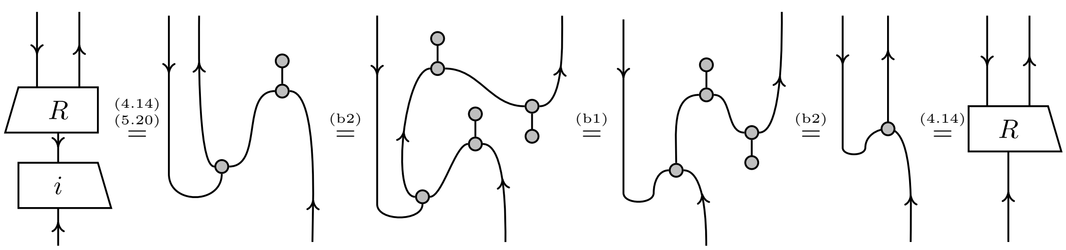


The second equation uses Lemma 5.4 and unitality, the third associativity. That i preserves units is trivial. Finally, i is indeed involutive:

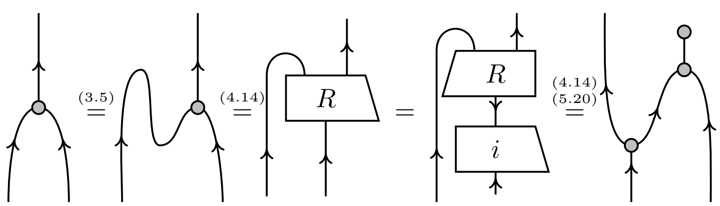


The second equation is the snake identity, and last equation uses the Frobenius law and unitality. Thus the monoid is involutive, and (b) holds.

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

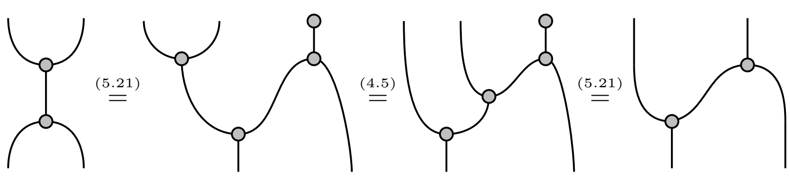


So:



(5.21)

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*:

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

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.* □

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* $n, k_1, \ldots, k_n$. □

Thus any dagger Frobenius structure $(A,)$ 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 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:*

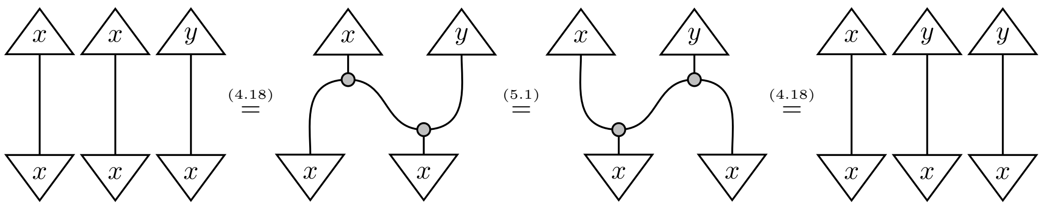
- *orthogonal bases and commutative dagger Frobenius structures;*
- *orthonormal bases and classical structures.* □

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:



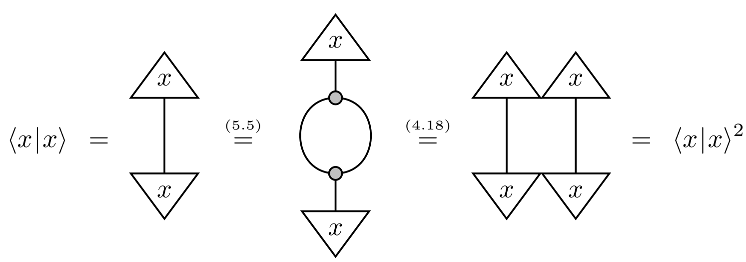
In other words, $\langle x|x\rangle\langle x|x\rangle\langle y|x\rangle = \langle x|x\rangle\langle y|x\rangle\langle y|x\rangle$. Since $x \neq 0$ also $\langle x|x\rangle \neq 0$. So we can divide to get $\langle x|x\rangle = \langle x|y\rangle$. Similarly we can find $\langle y|x\rangle = \langle y|y\rangle$. 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:



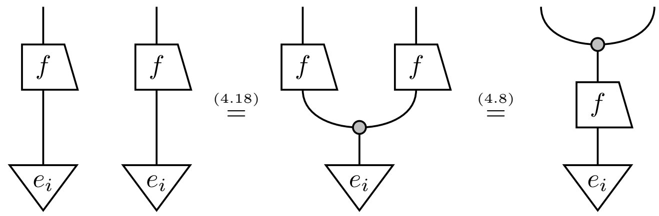
If x is nonzero then $\langle x|x\rangle$ must be nonzero, so dividing by it shows that $\|x\| = 1$. □

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.*

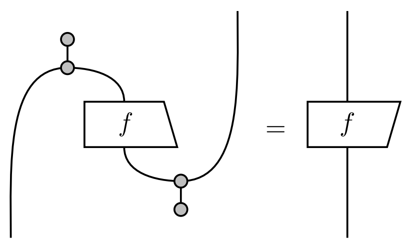
Proof. By linear extension, the comonoid homomorphism condition (4.8) will hold if and only if it holds on a basis of copyable states $\{e_i\}$ of the first classical structure, which must exist by Corollary 5.31. This gives the following equation:



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. □

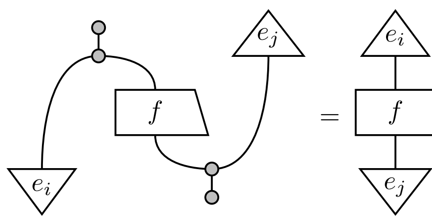
Because comonoid homomorphisms between classical structures in **FHilb** behave like functions, if we write them in matrix form using the bases of the associated classical structures, the result will be a matrix of zeroes and ones, with a single entry one in each column. These matrices are of course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

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



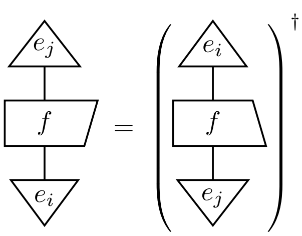
(5.23)

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



$$= \begin{bmatrix} 1 & \text{if } e_i = f(e_j) \\ 0 & \text{if } e_i \neq f(e_j) \end{bmatrix}$$

On the right we can do this calculation:



$$= \begin{bmatrix} 1 & \text{if } e_i = f(e_j) \\ 0 & \text{if } e_i \neq f(e_j) \end{bmatrix}^\dagger = \begin{bmatrix} 1 & \text{if } e_i = f(e_j) \\ 0 & \text{if } e_i \neq f(e_j) \end{bmatrix}$$

Thus (5.23) holds. □

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

(5.24)

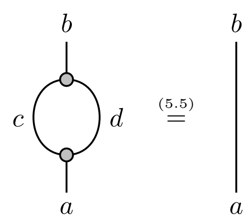
Proof. A copyable state $a : I \longrightarrow A$ can be thought of as a function from the unique copyable state on the trivial classical structure on I, to the chosen copyable state, and therefore gives a comonoid homomorphism. By Lemma 5.35, the result follows. □

Groupoids

We now investigate what special dagger Frobenius structures look like in **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 **Rel** by Example 5.3 and Example 5.11. It turns out that these examples are the only ones.

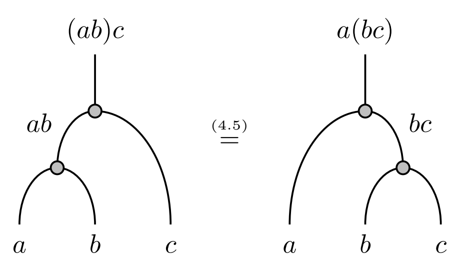
Theorem 5.37. *Special dagger Frobenius structures in* **Rel** *correspond exactly to groupoids.*

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 **Rel** with multiplication $M\colon A \times A \longrightarrow A$ and unit $U \subseteq A$. Suppose that $b\,(M \circ M^\dagger)\,a$ for $a, b \in A$. Then by the definition of relational composition, there must be some $c, d \in A$ such that $b\,M\,(c, d)$ and $(c, d)\,M^\dagger\,a$. To understand the consequence of the dagger speciality condition (5.5), we use the decorated notation of Section 3.3:



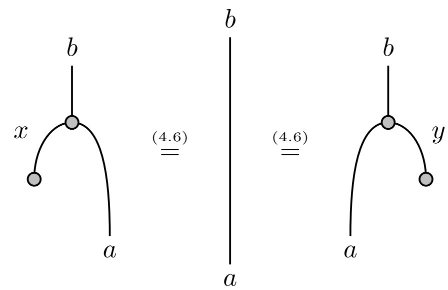
On the right-hand side, two elements $a, b \in A$ are only related by the identity relation if they are equal. So the same must be true on the left-hand side. Thus: if two elements $c, d \in A$ multiply to give two elements $a, b \in A$ — that is, both $b\,M\,(c, d)$ and $a\,M\,(c, d)$ hold — it must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

Next, consider associativity:



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

Finally, unitality:

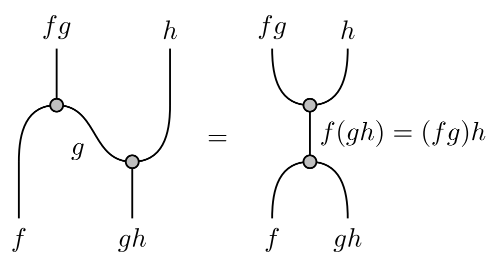


Here $x, y \in U \subseteq A$ are units, determined by the unit $1 \xrightarrow{U} A$ of the monoid. The first equality says that all a, b allow some $x \in U$ with $xa = b$ if and only if $a = b$. The second equality says that $ay = b$ for some $y \in U$ if and only $a = b$. Put differently: multiplying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

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

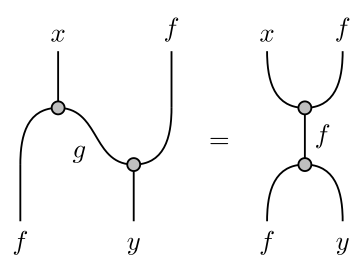
Lastly, can an element $a \in A$ have two left identities — is it possible for distinct $x, x' \in U$ to satisfy $xa = a = x'a$? This would imply $a = xa = x(x'a) = (xx')a$, which is undefined, as we have seen. So every element has a unique left identity, and similarly every element has a unique right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

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



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

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



The properties of left and right units make the right-hand side decoration valid. Hence there must be $g \in A$ with which to decorate the left-hand side. But such a g is precisely an arrow with $fg = y$ and $gf = x$, which is an inverse for f. □

Note also that the nondegenerate form of Proposition 5.16 is the coname of the function $g \mapsto g^{-1}$; see also Example 5.26.

Classifying the pair of pants Frobenius structures of Lemma 4.11 and Lemma 5.9 leads 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* **Rel** *are precisely* indiscrete groupoids, *i.e. groupoids where there is precisely one morphism between each two objects.*

Proof. Let A be a set. By definition, $(A^* \otimes A, ,)$ corresponds to a groupoid $\mathbf{G}$ whose set of morphisms is $A \times A$, and whose composition is given by

$$(b_2, b_1) \circ (a_2, a_1) = \begin{cases} (b_2, a_1) & \text{if } b_1 = a_2, \\ \text{undefined} & \text{otherwise.} \end{cases}$$

We deduce that the identity morphisms of $\mathbf{G}$ are the pairs (a_2, a_1) with $a_2 = a_1$. So objects of $\mathbf{G}$ just correspond to elements of A. Similarly, we find that the morphism (a_2, a_1) has domain a_1 and codomain a_2. Hence (a_2, a_1) is the unique morphism $a_1 \longrightarrow a_2$ in $\mathbf{G}$. □

Classifying classical structures in **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.

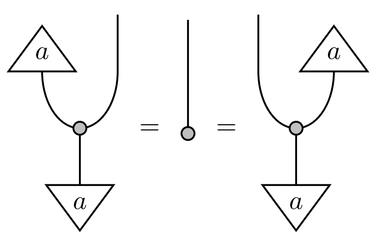
Corollary 5.39. *In* **Rel**, *classical structures exactly correspond to abelian groupoids.*

Proof. An immediate consequence of Theorem 5.37. □

5.5 Phases

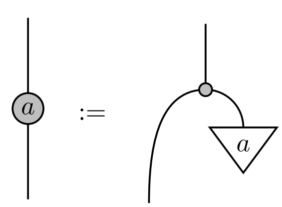
In quantum information theory, an interesting family of maps are *phase gates*: diagonal matrices whose diagonal entries are complex numbers of norm 1. For a particular Hilbert space equipped with a basis, these form a group under composition, which we will call the *phase group*. This turns out to work fully abstractly: any Frobenius structure in any monoidal dagger category gives rise to a phase group.

Definition 5.40 (Phase)**.** Let $(A, ,)$ be a Frobenius structure in a monoidal dagger category. A state $I \xrightarrow{a} A$ is called a *phase* when:



(5.25)

Its *(right) phase shift* is the following morphism $A \longrightarrow A$:

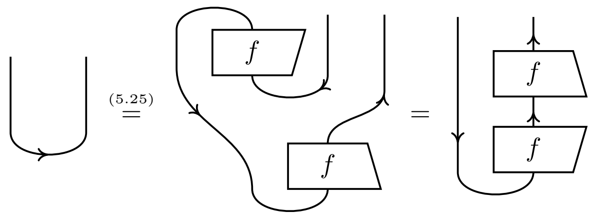


(5.26)

For the classical structure copying an orthonormal basis $\{e_i\}$ in **FHilb**, a vector $a = a_1 e_1 + \cdots a_n e_n$ is a phase precisely when each scalar a_i lies on the unit circle: $|a_i|^2 = 1$. For another example, the unit 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* $(A^* \otimes A, \ , \ , \ )$ *are the names of unitary operators* $A \longrightarrow A$.

Proof. The name of an operator $A \xrightarrow{f} A$ is a phase when:



But this precisely means $f \circ f^\dagger = \mathrm{id}_A$ by the snake equations (3.5). The other, symmetric, equation defining phases similarly comes down to $f^\dagger \circ f = \mathrm{id}_A$. $\square$

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 $\{e_1, \ldots, e_n\}$. The phases are elements of $U(1) \times \cdots \times U(1)$; that is, phases a are vectors of the form $e^{i\phi_1} e_1 + \cdots + e^{i\phi_n} e_n$ for real numbers $\phi_1, \ldots, \phi_n$. The accompanying phase shift $\mathbb{C}^n \longrightarrow \mathbb{C}^n$ 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

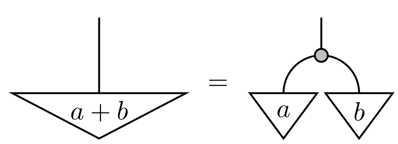
$$\{g^{-1}h \mid g, h \in a\} = \{1_G\} = \{hg^{-1} \mid g, h \in a\}.$$

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.

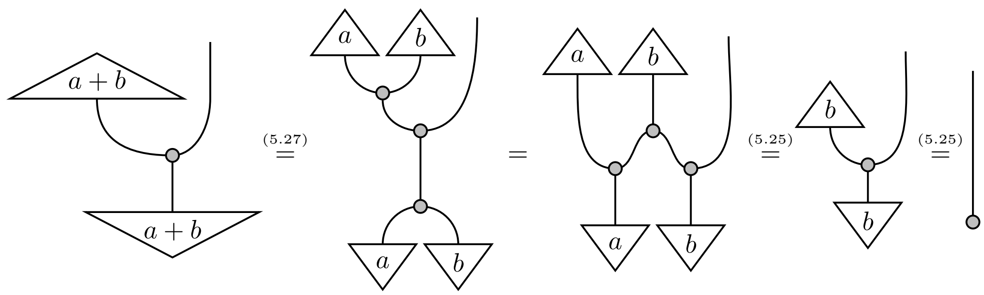
Proposition 5.44 (Phase group)**.** *Let* $(A, \ , \ )$ *be a dagger Frobenius structure in a monoidal dagger category. Its phases form a group with unit under the following addition:*



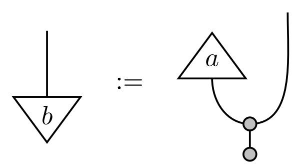
(5.27)

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.

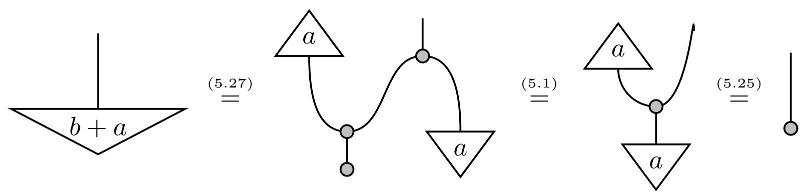
Proof. First we show that (5.27) is again a well-defined phase:



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:

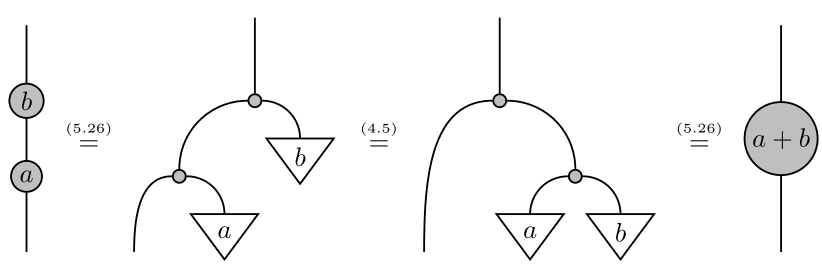


Then b is a left-inverse of a:



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 be 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:

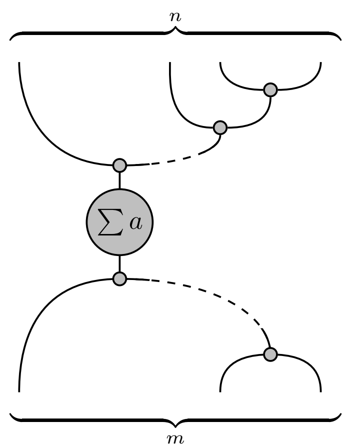
- The group operation on the phases of the pair of pants Frobenius structure of Lemma 5.41, which are names of unitary morphisms $A \xrightarrow{f} A$, is simply taking the name of composition of operators.

- 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 $(A, \ , \ )$ be a classical structure in a symmetric monoidal dagger category. Any connected morphism $A^{\otimes m} \longrightarrow A^{\otimes n}$ built out of finitely many , , id, and phases using $\circ$, $\otimes$, and $\dagger$, equals*



(5.28)

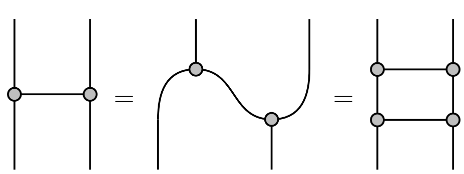
where a ranges over all the phases used in the diagram.

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 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.

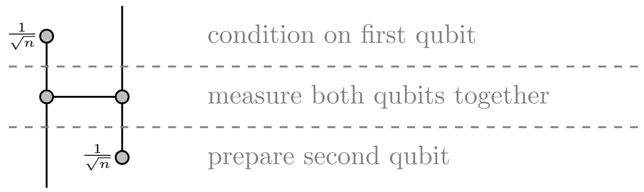
By virtue of the spider theorem, we can be quite lax when drawing wires connected by classical structures. They are all the same morphism anyway. For example:



(5.29)

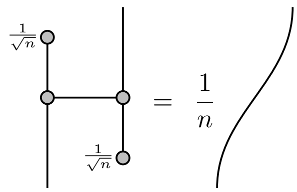
is a projection $H \otimes H \longrightarrow H \otimes H$.

Define the procedure for state transfer graphically by the following diagram:



(5.30)

We can easily simplify this diagram using the spider theorem:



(5.31)

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.