

# 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:

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

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

$$\begin{array}{c} \uparrow \\ \text{---} \\ \uparrow \end{array} = \begin{array}{c} \uparrow \\ | \\ \uparrow \end{array} \qquad \begin{array}{c} \downarrow \\ \text{---} \\ \downarrow \end{array} = \begin{array}{c} \downarrow \\ | \\ \downarrow \end{array} \quad (3.5)$$

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

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

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

- The monoidal category **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:

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

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

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

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

- Infinite-dimensional Hilbert spaces do not have duals. For an infinite-dimensional Hilbert space, the definitions of  $\eta$  and  $\varepsilon$  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:

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

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

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

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

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:

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

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:

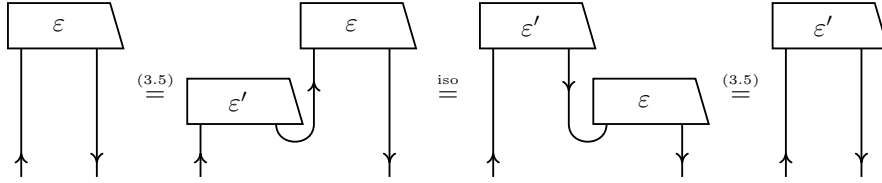
$$(3.14)$$

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. □

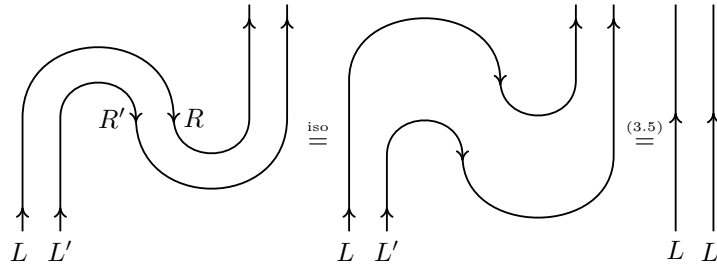
The following lemmas show that dual objects interact well with the monoidal structure.

**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:

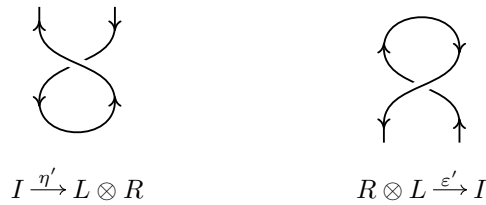


The other snake equation follows similarly. □

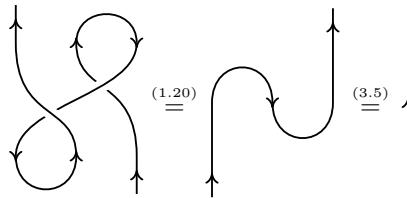
If the monoidal category has a braiding then a duality  $L \dashv R$  gives rise to a duality  $R \dashv L$ , as the next lemma investigates.

**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  $\eta$  and  $\varepsilon$ :



The other snake equation can be proved in a similar way.  $\square$

### 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:

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

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.  $\square$

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  $A \xrightarrow{f} B$ :*

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

*Proof.* Direct from writing out the definitions of the components involved.  $\square$

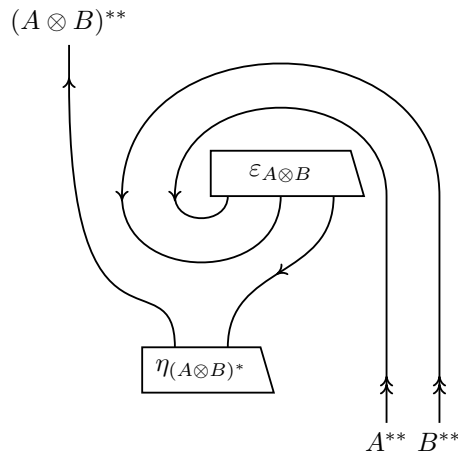
**Example 3.13.** Let's see how the right duals functor acts for our example categories, with chosen right duals as given by Example 3.2.

- 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,  $A^{**} \otimes B^{**} \simeq (A \otimes B)^{**}$ .

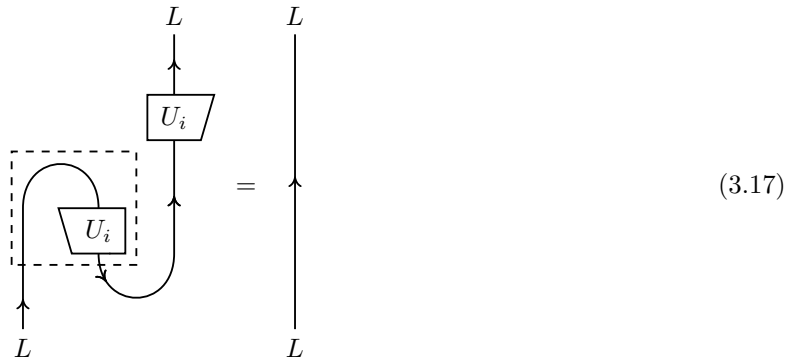
*Proof.* The isomorphism  $A^{**} \otimes B^{**} \simeq (A \otimes B)^{**}$  looks like this:



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.



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

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

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

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**,  $\mathbf{Mat}_{\mathbb{C}}$ , **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  $\varepsilon$  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  $\eta'$  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:

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

*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:

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

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

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<sub>C</sub>** and **Rel** are all compact dagger categories.

- On **FHilb**, the conjugation functor gives the conjugate of a linear map.
- On **Mat<sub>C</sub>**, 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)

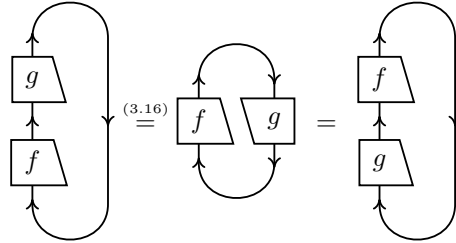
It is denoted by  $\text{Tr}(f)$ , or sometimes  $\text{Tr}_A(f)$  to emphasize  $A$ . (Don't confuse it with the partial trace of quantum theory.)

**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.

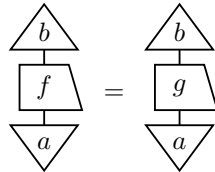
**Corollary 3.34.** *Infinite-dimensional Hilbert spaces do not have duals.*

*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  $\dim(H) \in \mathbb{C}$ .  $\square$

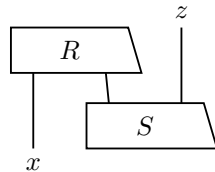
This argument would not apply in **Rel**, since we have  $\text{id}_1 + \text{id}_1 = \text{id}_1$  in that category. And indeed, as we have seen at the beginning of this chapter, both finite and infinite sets are self-dual in this category, despite the fact that sets  $S$  of infinite cardinality can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

### 3.3 Information flow

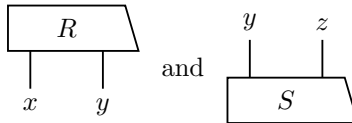
In a monoidal dagger category, we may think of the wires in the graphical calculus carrying information flow as follows. If the category is well-pointed, two morphisms  $A \xrightarrow{f,g} B$  are equal if and only if for all points  $I \xrightarrow{a} A$  and  $I \xrightarrow{b} B$  the following two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



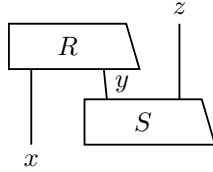
So we could verify an equation by computing the ‘matrix entries’ of both sides. In the category **Rel** is convenient to do this by decorating the wires with elements. For example, the scalar



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  $\eta$  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  $\text{id}_L$  and  $\text{id}_R$  factor through the monoidal unit object  $I$ .*

*Proof.* Suppose that  $\eta$  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  $\text{id}_R$ . □

Interpreting a graphical diagram as a history of events that have taken place, as we do, the fact that  $\text{id}_L$  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  $\eta$  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  $\eta$  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  $\pi^{-1}$  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**.