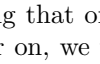
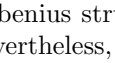
Categories and Quantum Informatics: Complementarity

Chris Heunen

Spring 2018

This chapter studies what happens when we have *two* interacting Frobenius structures. Specifically, we are interested in when they are "maximally incompatible", or *complementary*, and give a definition that makes sense in arbitrary monoidal dagger categories in Section 6.1. We will see that it comes down to the standard notion of mutually unbiased bases from quantum information theory in the category of Hilbert spaces, and classify the complementary groupoids in the category of sets and relations. We will also characterize complementarity in terms of a canonical morphism being isometric. This is exemplified by discussing the Deutsch–Jozsa algorithm in Section 6.2, where the canonical morphism plays the role of an oracle function. Section 6.3 links complementarity to the subject of Hopf algebra. It turns out that this well-studied notion gives rise to a stronger form of complementarity that we characterize. Finally, Section 6.4 discusses how many-qubit gates can be modeled in categorical quantum mechanics using only complementary Frobenius structures, such as controlled negation, controlled phase gates, and arbitrary single qubit gates.

We have been using colours to distinguish between monoid multiplication  and comonoid comultiplication  . We have also been indicating that one is the dagger of the other by abbreviating  to just a single colour  . From this chapter on, we will deal with *two* Frobenius structures, each carrying both a multiplication and a comultiplication. When this is the case we will specialize to dagger Frobenius structures, so we can distinguish them. By drawing the operations of a single Frobenius structure in a single colour, we can speak about two dagger Frobenius structures $(A,$  $)$ and $(A,$$)$, in a way perfectly consistent with our conventions. Nevertheless, many results hold more generally without daggers.

6.1 Complementarity

Consider two measurements of a qubit: one in the basis $\{\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right), \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)\}$, and one in the basis $\{\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)/\sqrt{2}, \left(\begin{smallmatrix}1\\-1\end{smallmatrix}\right)/\sqrt{2}\}$. If we measure in the first basis, the qubit will collapse to either $\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ or $\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$; a repeated measurement in the first basis is guaranteed to repeat the same outcome. However, a measurement in the second basis could yield either outcome with equal probability. Two bases with this property are said to be unbiased. This is a simple form of Heisenberg's uncertainty principle.

Definition 6.1. For a finite-dimensional Hilbert space H, two orthogonal bases $\{a_i\}$ and $\{b_j\}$ are *complementary*, or *unbiased*, when there is some constant $c \in \mathbb{C}$ such that the following holds:

$$\langle a_i|b_j\rangle\langle b_j|a_i\rangle = c \tag{6.1}$$

In other words, the inner products have constant absolute value.

We can prove the following simple lemma about complementary bases.

Lemma 6.2. *For a pair of complementary bases $\{a_i\}$ and $\{b_j\}$, within each basis, the elements have constant norm.*

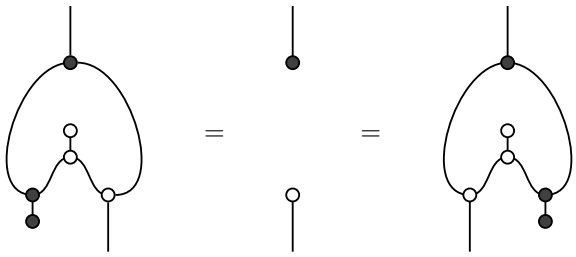
Proof. We perform the following computation:

$$\langle b_j|b_j\rangle = \sum_i \frac{\langle b_j|a_i\rangle\langle a_i|b_j\rangle}{\langle a_i|a_i\rangle} \overset{(6.1)}{=} \sum_i \frac{c}{\langle a_i|a_i\rangle}$$

In the first equality, we insert the identity as a sum over the complete family of projectors $|a_i\rangle\langle a_i|/\langle a_i|a_i\rangle$. The final expression is independent of j as required. A similar argument holds for the $\{a_i\}$ basis. □

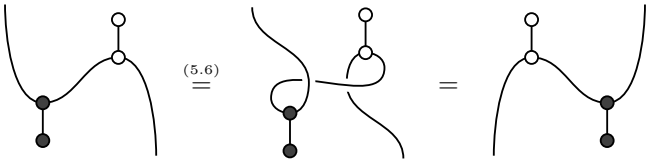
We know from Corollary 5.31 that an orthogonal basis can be represented as a commutative dagger Frobenius structure, so a natural goal is to characterize complementarity as an interaction law between two commutative dagger Frobenius structures. Following this inspiration leads to the following definition.

Definition 6.3 (Complementary Frobenius structures)**.** In a braided monoidal dagger category, two symmetric dagger Frobenius structures and on the same object are *complementary* when the following equals hold:



(6.2)

The roles of the black and white dots in the previous definition are not obviously interchangeable. However, since the Frobenius algebras are symmetric, we can make the following argument:



(6.3)

Using these equations and the dagger, we see that 'black is complementary to white' is equivalent to 'white is complementary to black'.

First properties

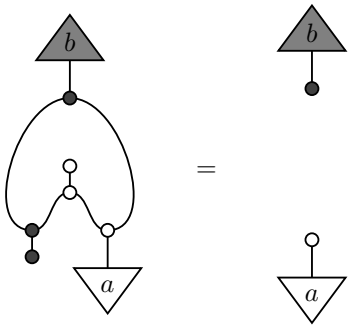
We now establish that this captures the correct notion in **FHilb**.

Proposition 6.4 (Complementarity in **FHilb**)**.** *In* **FHilb***, the following are equivalent for two commutative dagger Frobenius structures on the same object:*

- *as Frobenius structures, they are complementary;*
- *as bases, they are complementary with constant* $c = 1$*.*

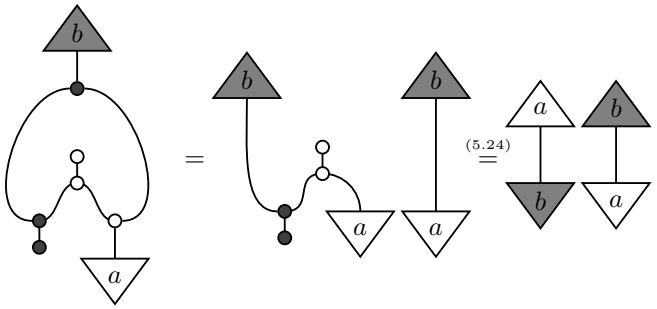
Proof. The complementarity equation (6.2) holds if and only if the following equation holds for all a in the

white basis, and b in the black basis:



(6.4)

The left-hand side can be simplified as follows:



(6.5)

The right-hand side expands to 1. □

Example 6.5 (Pauli bases)**.** Here are three bases of the Hilbert space $\mathbb{C}^2$:

$$X \text{ basis:} \quad \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\} \tag{6.6}$$

$$Y \text{ basis:} \quad \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \right\} \tag{6.7}$$

$$Z \text{ basis:} \quad \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\} \tag{6.8}$$

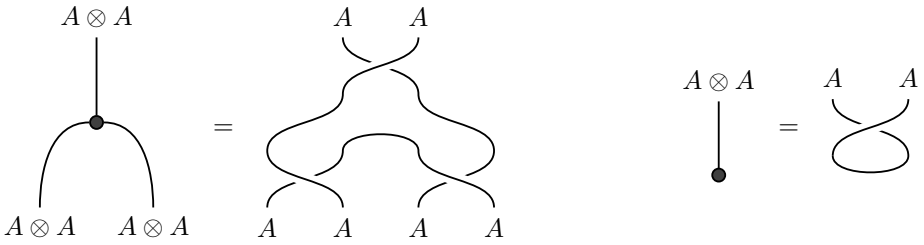
These are all mutually complementary. The terminology is explained by the fact that these bases consist of eigenvectors of the three Pauli matrices that measure spin in the X, Y and Z coordinates of a spin-$\frac{1}{2}$ particle in three-dimensional space.

It is known that this is the largest family of complementary bases that can exist in $\mathbb{C}^2$, in the sense that it is not possible to find four bases for this Hilbert space which are all mutually complementary. Establishing the maximum possible number of mutually complementary bases in a Hilbert space of a given dimension is a difficult problem, which has not been solved in general for Hilbert spaces of dimensions which are not a prime power.

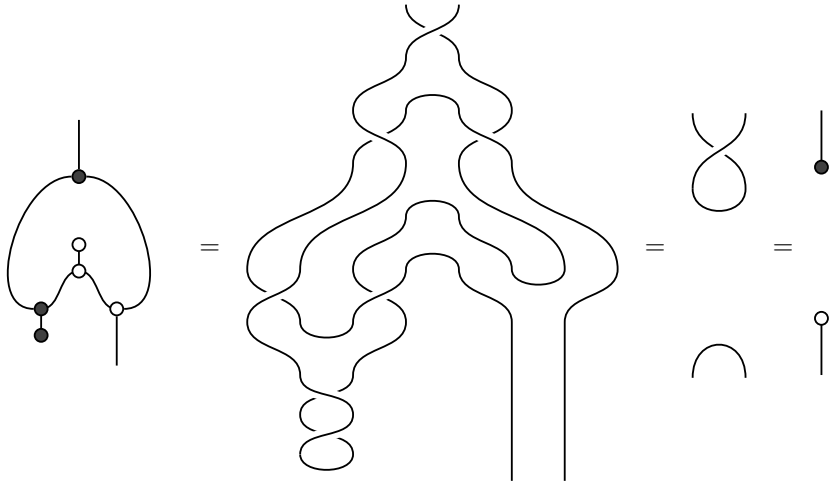
The next lemma provides a large stock of examples of complementary Frobenius structures.

Lemma 6.6. *If A is a dagger self-dual object in a braided monoidal category, then the following two Frobenius structures on $A \otimes A$ are complementary: the pair of pants from Lemma 5.9, and its transport across the braiding $\sigma_{A,A}$ as in Lemma 5.17.*

Proof. Denote the pair of pants Frobenius structure from Lemma 5.9 by white dots, and its transport across the braiding, the 'twisted knickers', by black dots:



Then straightforward diagrammatic calculation shows:



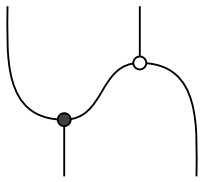
The other identity in (6.2) follows similarly. □

Combined with Theorem 5.15, the previous lemma says that any dagger Frobenius structure on A gives rise to a complementary pair of Frobenius structures on $A \otimes A$ in any symmetric monoidal dagger category.

Dagger complementarity

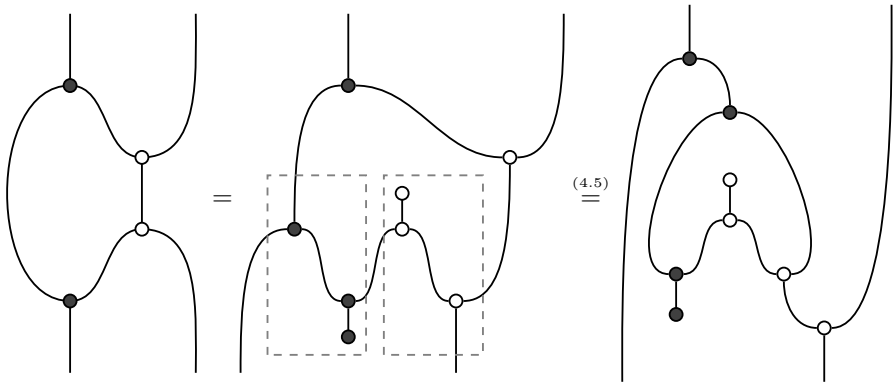
Complementarity is an equality of morphisms built from the (co)multiplication and (co)unit of a Frobenius structure. We can also characterize complementarity in terms of daggers, namely as some canonical morphism being unitary. This is the content of the following proposition.

Proposition 6.7. *Two symmetric dagger Frobenius structures in a braided monoidal dagger category are complementary if and only if the following endomorphism is unitary:*



(6.9)

Proof. Composing (6.9) with its adjoint, we obtain:



(6.10)

Here, the first equality follows from two applications of the noncommutative spider Theorem 5.21 to the dashed areas. Now, if complementarity (6.2) holds then (6.10) equals the identity. Conversely, if the right-hand side of (6.10) equals the identity, then composing with the white counit on the top right and the black unit on the bottom left gives back the left-hand equality of complementarity (6.2). Therefore the left identity in (6.2) holds if and only if (6.9) is an isometry. A similar argument composing (6.9) with its adjoint in the other order corresponds to the right-hand equality of complementarity (6.2). □

Complementary groupoids

Now we investigate what complementarity means in our other example category **Rel**. It turns out to be a phenomenon similar to mutual unbiasedness. The construction in the following example is a lot like that of Lemma 6.6.

Example 6.8. Let G and H be nontrivial groups. Set $A = G \times H$. Let $\mathbf{G}$ be the groupoid with objects G and homsets $\mathbf{G}(g, g) = H$ and no morphisms between distinct objects, and let $\mathbf{H}$ be the groupoid with objects H and homsets $\mathbf{H}(h, h) = G$ and no morphisms between distinct objects. Then in a natural way, $\mathbf{G}$ and $\mathbf{H}$ can be considered to have the same set of morphisms, and in fact they are complementary as Frobenius structures.

Proof. Consider the left-hand side of (6.2). It expands to

$$\{(a, b) \mid \exists x \in A \colon x \bullet a = x \circ b\},$$

where we write $\bullet$ for the composition in $\mathbf{G}$, and $\circ$ for the composition in $\mathbf{H}$. This set clearly contains the right-hand side of (6.2), which is

$$\{(\mathrm{id}_g, \mathrm{id}_h) \mid g \in \mathrm{Ob}(\mathbf{G}), h \in \mathrm{Ob}(\mathbf{H}))\}.$$

Remember that we cannot compose any two morphisms in a groupoid; they have to have matching domain and codomain. Suppose $x \bullet a = x \circ b$. Then the $\circ$-inverse of x is $\circ$-composable with $x \bullet a$. That is, $\mathrm{cod}_\circ(x) = \mathrm{cod}_\circ(x \bullet a)$. But by construction that means a must be a $\bullet$-identity. Similarly, b must be a $\circ$-identity. So the left-hand and right-hand sides of (6.2) are equal, and $\mathbf{G}$ and $\mathbf{H}$ are complementary. □

The previous example suggests a certain balance between two complementary groupoids. The following proposition makes this precise: the fewer objects one groupoid has, the more a complementary one must have.

Proposition 6.9 (Complementarity in **Rel**)**.** *The following are equivalent for groupoids* $\mathbf{G}$ *and* $\mathbf{H}$ *with the same set* A *of morphisms:*

- *their Frobenius structures are complementary;*
- *the map* $A \longrightarrow \mathrm{Ob}(\mathbf{G}) \times \mathrm{Ob}(\mathbf{H})$ *given by* $a \mapsto \big(\mathrm{cod}_{\mathbf{G}}(a), \mathrm{cod}_{\mathbf{H}}(a)\big)$ *is bijective.*

Proof. Write $\bullet$ for the multiplication in $\mathbf{G}$, and $\circ$ for that in $\mathbf{H}$. By Proposition 6.7, complementarity is equivalent to unitarity of the morphism (6.9). Unitaries in **Rel** are exactly the bijective functions (see Exercise **??**). Unfolding this, we see that complementarity is equivalent to:

$$\forall a, b \in A\ \exists! c, d \in A\ \exists e \in A\colon b = e \bullet d,\ c = a \circ e.$$

Because we're in a groupoid, when a, b, c, d are fixed, there is only one possible e fitting the bill, so we can reformulate this as:

$$\forall a, b \in A\ \exists! c, d, e \in A\colon d = e^{-1} \bullet b,\ c = a \circ e,$$

where the inverse is taken in $\mathbf{G}$. This just means that all $a, b \in A$ allow a unique $e \in A$ making $e^{-1} \bullet b$ and $a \circ e$ well-defined. But this happens precisely when e and b have the same codomain in $\mathbf{G}$, and $\mathrm{cod}(e) = \mathrm{dom}(a)$ in $\mathbf{H}$. Thus complementarity holds if and only if all objects g of $\mathbf{G}$ and h of $\mathbf{H}$ allow unique $e \in A$ with $\mathbf{G}$-codomain g and $\mathbf{H}$-codomain h. □

In particular: if two classical structures in **Rel** corresponding to abelian groupoids $\mathbf{G}$ and $\mathbf{H}$ are complementary, then $\mathbf{G}(g, g) \simeq \mathrm{Ob}(\mathbf{H})$ and $\mathbf{H}(h, h) \simeq \mathrm{Ob}(\mathbf{G})$ for each object g of $\mathbf{G}$ and h of the $\mathbf{H}$.

In **FHilb**, it so happens any classical structure allows a complementary one, that is, every orthonormal basis has a mutually unbiased one. The following corollary shows that this is not always the case in **Rel**, where dagger Frobenius structures need to be 'homogeneous' in the sense that the groupoid looks the same under any 'translation' from one object to another.

Proposition 6.10. *A Frobenius structure in* **Rel** *corresponding to a groupoid* $\mathbf{G}$ *allows a complementary one exactly when the cardinality of the set of all morphisms into an object* g *is independent of* g*.*

Proof. One direction is obvious after the previous proposition. We will prove the other, by constructing a complementary groupoid $\mathbf{H}$. We may assume that $\mathbf{G}$ is not empty without loss of generality. Pick some object g_0. Observe that the set of A morphisms of $\mathbf{G}$ decomposes as $\bigcup_{g' \in \mathrm{Ob}(\mathbf{G})} \Big(\bigcup_{g \in \mathrm{Ob}(\mathbf{G})} \mathbf{G}(g, g') \Big)$. We will define $\mathbf{H}$ by carving up the set of morphisms of $\mathbf{G}$ the other way around. Set $\mathrm{Ob}(\mathbf{H}) = \bigcup_{g \in \mathrm{Ob}(\mathbf{G})} \mathbf{G}(g, g_0)$. By assumption, there are bijections $\varphi_{g'}\colon \mathrm{Ob}(\mathbf{H}) \to \bigcup_{g \in \mathrm{Ob}(\mathbf{G})} \mathbf{G}(g, g')$. Define $\mathbf{H}(h, h') = \emptyset$ for distinct h, h', and set $\mathbf{H}(h, h) = \{\varphi_g(h) \mid g \in \mathrm{Ob}(\mathbf{G})\}$. Then $\mathbf{H}$ has the same set of morphisms as $\mathbf{G}$, and if $a \in \mathbf{G}(g, g')$, then $a = \varphi'_g(h)$ for a unique $h \in \mathrm{Ob}(\mathbf{H})$, namely $h = \mathrm{cod}_{\mathbf{H}}(a)$. This construction makes the map $A \longrightarrow \mathrm{Ob}(\mathbf{G}) \times \mathrm{Ob}(\mathbf{H})$ given by $a \mapsto (\mathrm{cod}_{\mathbf{G}}(a), \mathrm{cod}_{\mathbf{H}}(a))$ into a bijection.

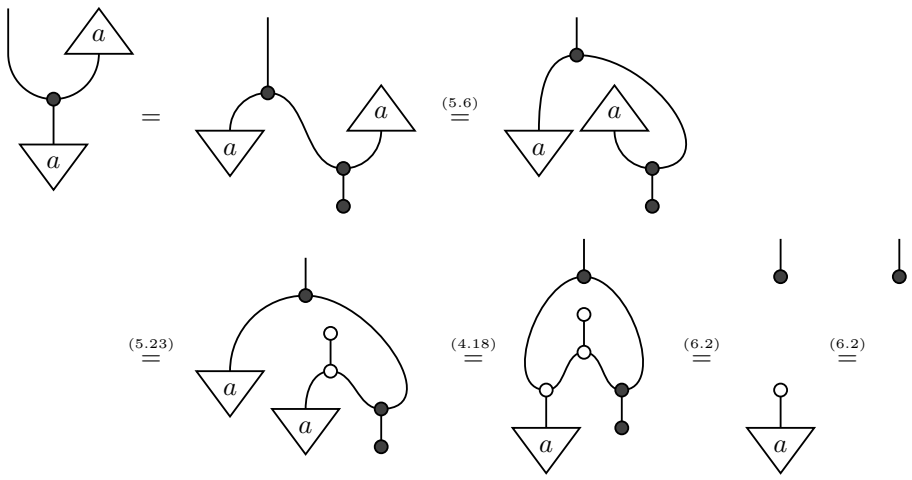
By the previous proposition, all that is left to do is to make $\mathbf{H}$ a well-defined groupoid in some way. For this it suffices to make $\mathrm{Ob}(\mathbf{G})$ into a group. If $\mathrm{Ob}(\mathbf{G})$ is finite, you can use the multiplication of $\mathbb{Z}_n$. If $\mathrm{Ob}(\mathbf{G})$ is infinite, then it is isomorphic to the set of its finite subsets, which form a group under the symmetric difference $U \cdot V = (U \cup V) \setminus (U \cap V)$ as multiplication. □

Unbiased states

One way to understand complementary bases is to recognize that copyable states for one basis will be *unbiased* for a complementary basis. In other words, if you write out one basis element using column vector notation defined by the other basis, then up to an overall scalar factor, each entry will be unitary. We captured this abstractly with the notion of a *phase* for a Frobenius structure, introduced in Definition 5.40. In other words, a state is unbiased for a dagger Frobenius structure when its phase shift is unitary.

Proposition 6.11. *Let* $(A, \curlywedge, \curlyvee)$ *and* $(A, \curlywedge, \bullet)$ *be complementary symmetric dagger Frobenius structures in a braided monoidal dagger category. If a state is self-conjugate, copyable and deletable for* $(\curlywedge, \curlyvee)$*, then it is a phase for* $(\curlywedge, \bullet)$*.*

Proof. Using the graphical calculus:



These equalities used, in order: the noncommutative spider theorem, symmetry, self-conjugateness, copyability, complementarity, and deletability. The symmetric requirement of (5.25) is analogous. □

6.2 The Deutsch–Jozsa algorithm

The Deutsch–Jozsa algorithm solves a certain problem faster in the quantum case than is possible in the classical case. It is typical of quantum algorithms that decide on a solution without relying on approximation. The Deutsch–Jozsa algorithm solve a slightly artificial problem, but other algorithms in this family include Shor's factoring algorithm, Grover's search algorithm, and the more general hidden subgroup problem. The 'all or nothing' nature of these algorithms make them amenable to categorical models, where we can see the difference between no information flow and maximum information flow. This section discusses the algorithm and proves its correctness categorically.

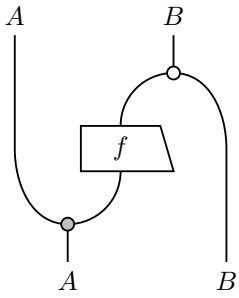
The Deutsch–Jozsa algorithm addresses the following problem. Suppose we have a 2-valued function $A \xrightarrow{f} \{0,1\}$ on a finite set A. If the function f takes just a single value on every element of A, it is called *constant*. Another possibility is that the function takes the value 0 on exactly half the elements of A, and takes the value 1 on the other half; in this case it is called *balanced*. Most functions are neither balanced or constant, but we will restrict to those that are. The Deutsch–Jozsa problem, given a function $A \xrightarrow{f} \{0,1\}$ promised to be either balanced or constant, is to determine which of the two is the case.

The best classical strategy is rather simple. We have no knowledge of the structure of the function f in general, so we must simply proceed to sample the function on elements of A. If we find two elements which have different values, then f cannot be constant, so we conclude that f is balanced and we are done. However, in the worst case we might have to sample $\frac{1}{2}|A| + 1$ elements until we find two elements with different values. If we sample this many elements and we find that f returns the same value for each one, then we can conclude that f is constant.

Oracles

The quantum Deutsch–Jozsa algorithm decides between the constant and balanced cases with just a *single* use of the function f. However, we have to be more precise about how to access the function f. A quantum computation only allows unitary gates; so we have to linearize the function $A \xrightarrow{f} \{0,1\}$ to a unitary map, called an *oracle*.

Definition 6.12. In a monoidal dagger category, given Frobenius structures (A, δ, ι) and (B, δ, ι), an *oracle* is a morphism $A \xrightarrow{f} B$ such that the following morphism is unitary:



(6.11)

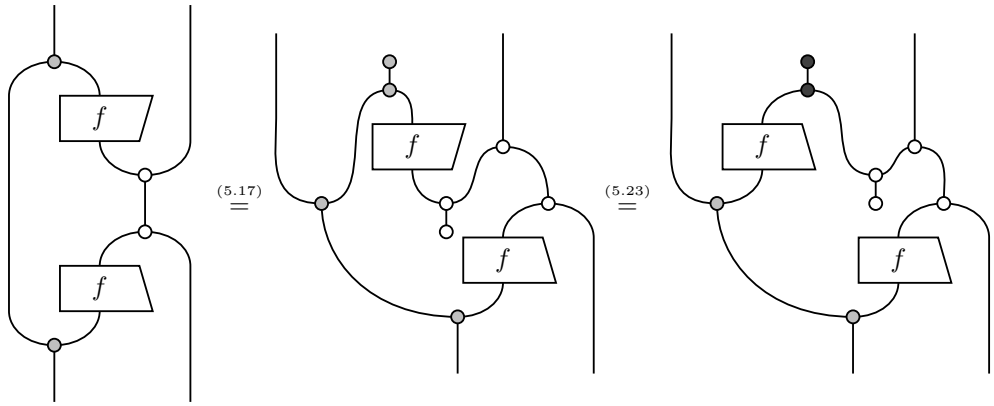
Example 6.13. Let $A \xrightarrow{f} B$ be a morphism of **FSet**. Write H and K for the free Hilbert spaces on A and B respectively. The function f induces a morphism $H \longrightarrow K$ in **FHilb** that extends the function $a \mapsto f(a)$.

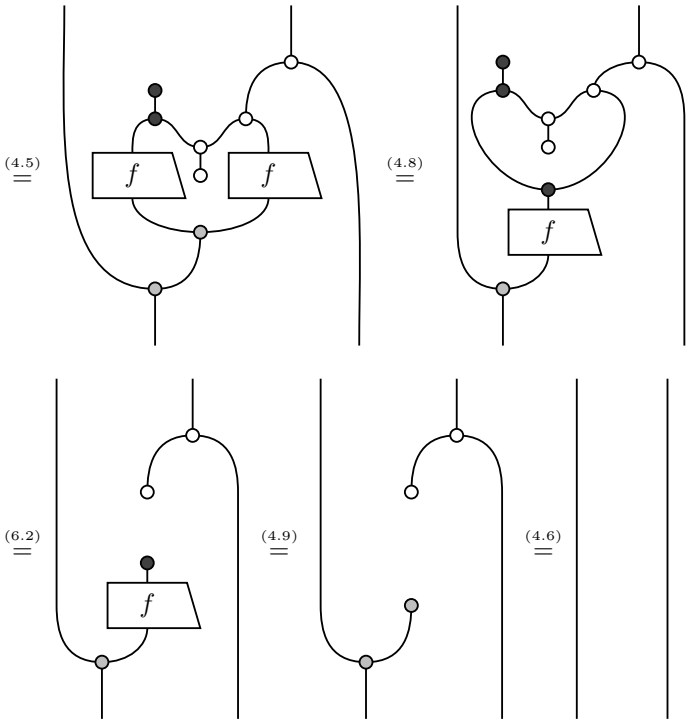
Now choose an orthogonal basis $\{e_i\}$ for K that is mutually unbiased to B, with length $\|e_i\|^2 = \dim(K)$. With this basis as the white Frobenius structure, the map (6.11) sends $a \otimes e_i$ to $\langle e_i | f(a) \rangle a \otimes e_i$, where the coefficients have amplitude $|\langle e_i | f(a) \rangle|^2 = \|e_i\|^2 \|f(a)\|^2 / \dim(K) = 1$ by (**??**). Hence (6.11) is unitary, and the morphism $H \longrightarrow K$ is an oracle. Because it extends the function f, we say it is an *oracle for* f.

The previous example is typical: we now prove that any oracle extends a function between bases. Recall from Corollary 5.34 that functions between bases are comonoid homomorphisms between classical structures, and from Lemma 5.35 that the latter are always self-conjugate.

Proposition 6.14. *Let* (A, δ, ι), (B, δ, ι) *and* (B, δ, ι) *be symmetric dagger Frobenius structures in a braided monoidal dagger category. A self-conjugate comonoid homomorphism* $(A, \delta, \iota) \xrightarrow{f} (B, \delta, \iota)$ *is an oracle* $(A, \delta, \iota) \longrightarrow (B, \delta, \iota)$ *if and only if* ι *is complementary to* ι.

Proof. Suppose ι and ι are complementary, and compose (6.11) with its adjoint:





These equalities used the noncommutative spider theorem, self-conjugacy of f, (co)associativity, the fact that f preserves comultiplication, complementarity, the fact that f preserves the counit, and the unit and counit laws. The composition of (6.11) and its adjoint in the other order similarly gives the identity. Thus f is an oracle.

Conversely, if f is an oracle, composing the above computation with a white unit on the bottom right and a gray counit on the top left shows the left equation of (6.2). A similar argument to the composition of (6.11) with its adjoint in the other order gives the other equation, showing that and are complementary. □

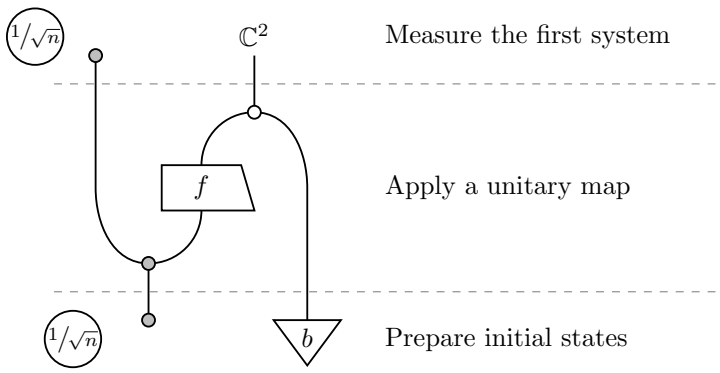
Notice that the previous proposition resembles Proposition 6.7, just with a morphism f 'in the middle'.

The algorithm

We can now state the procedure of the Deutsch–Jozsa algorithm itself.

Definition 6.15 (The Deutsch–Jozsa algorithm)**.** Say that A has n elements, and let $A \xrightarrow{f} \{0,1\}$ be the given function. Extend it to an oracle $H \longrightarrow \mathbb{C}^2$ as in Example 6.13; the two complementary bases on $\mathbb{C}^2$ are the computational basis and the X basis from Example 6.5 scaled by $\sqrt{2}$. Write b for the state $\begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix}$ of

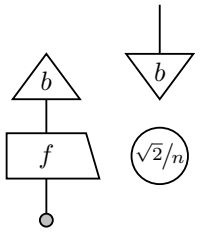
$\mathbb{C}^2$. The *Deutsch–Jozsa algorithm* is the following morphism in **FHilb**:



(6.12)

The dashed horizontal lines separate the different stages of the procedure. In the language of states and effects of Sections 1.3 and **??**: first prepare two systems in initial states, one in the maximally mixed state according to the gray classical structure, the other in state b; then apply a unitary gate; finally postselect on the first system being measured in the maximally mixed effect for the gray classical structure. The diagram (6.12) describes a particular quantum history, and taking the square of the norm of the state it represents gives the probability this history will occur.

Lemma 6.16. *The Deutsch–Jozsa algorithm* (6.12) *simplifies to:*



(6.13)

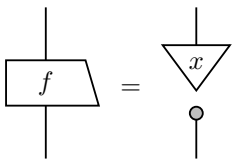
Proof. Duplicate the copyable state $\sqrt{2}b$ through the white dot in (6.12), and apply the noncommutative Spider Theorem 5.21 to the cluster of gray dots. □

Correctness

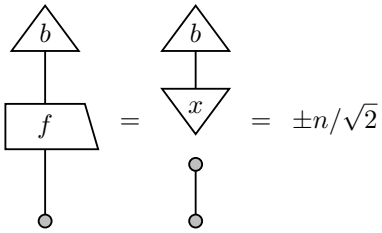
We now set out to prove correctness of the Deutsch–Jozsa algorithm.

Lemma 6.17 (The constant case)**.** *If the function $A \xrightarrow{f} \{0,1\}$ is constant, then the history described in diagram* (6.12) *is certain.*

Proof. Suppose $f(a) = x$ for all $a \in A$. Then the oracle $H \xrightarrow{f} \mathbb{C}^2$ decomposes as:



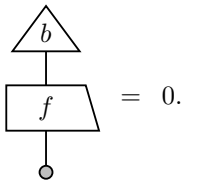
Thus the amplitude of the main component of the quantum history (6.13) is:



Hence the norm of (6.13) is 1. □

Lemma 6.18 (The balanced case)**.** *If the function* $A \xrightarrow{f} \{0,1\}$ *is balanced, then the history described in diagram* (6.12) *is impossible.*

Proof. Suppose f takes each value of the set $\{0,1\}$ on an equal number of elements of A. To test whether a particular f is balanced, we could perform a sum indexed by $a \in A$, with summand given by $+1$ if $f(a) = 0$, and by -1 if $f(a) = 1$; the function f would be balanced exactly when this sum gives 0. Given the definition of the state b, we could equivalently test the equality $\sum_{a \in A} b^\dagger(f(a)) = 0$, with the following graphical representation:



Hence the norm of (6.13) is 0. □

Theorem 6.19 (Deutsch–Jozsa is correct)**.** *The Deutsch–Jozsa algorithm* (6.12) *correctly identifies constant functions* $A \xrightarrow{f} \{0,1\}$.

Proof. The squared norm of the state (6.13) is the probability of the history occurring. The previous two lemmas show that the history (6.12) is a perfect test for discriminating constant and balanced functions. □

6.3 Bialgebras

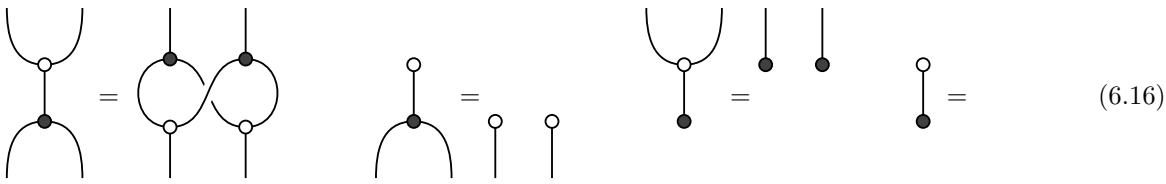
As we saw in Proposition 6.4, complementary classical structures **FHilb** are mutually unbiased bases. One common way to construct mutually unbiased bases is the following. Let G be a finite group, and consider the Hilbert space for which $\{g \in G\}$ is an orthonormal basis. Defining

$$\curlyvee : g \mapsto g \otimes g \qquad \text{⚲} : g \mapsto 1 \tag{6.14}$$

$$\curlywedge : g \otimes h \mapsto gh \qquad \bullet : 1 \mapsto 1_G \tag{6.15}$$

gives complementary dagger Frobenius structures; see Examples 4.2 and 5.2. This construction additionally satisfies $\curlyvee \circ \curlywedge : g \otimes h \mapsto gh \otimes gh$, which is captured abstractly as follows.

Definition 6.20 (Bialgebra, dagger bialgebra)**.** A *bialgebra* in a braided monoidal category consists of a monoid ($\curlywedge$,$\bullet$) and a comonoid ($\curlyvee$,⚲) on the same object, satisfying the following *bialgebra laws*:



(6.16)

The last equation is not missing a picture, because we are drawing id_I as the empty picture (1.6). A bialgebra is *commutative* when the underlying monoid and comonoid are commutative. In a braided monoidal dagger category, a *dagger bialgebra* is a bialgebra for which  =  .

Example 6.21. There are many interesting examples of bialgebras.

- Any monoid M is a bialgebra in **Set**, by choosing

   : $m \mapsto (m, m)$  : $m \mapsto \bullet$  : $(m, n) \mapsto mn$  : $\bullet \mapsto 1_M$.

- Any monoid M in **FSet** induces a bialgebra in **FHilb** as follows. Let $(A, \text{}, \text{})$ be the group algebra; see Example 5.2. Define

   : $m \mapsto m \otimes m$: $m \mapsto 1$

  When M is a group, $(A, \text{  }, \text{  })$ can also be made into a Frobenius structure as in Example 5.2, but with different  and . In Section **??** we will see a converse: bialgebras in **FSet** satisfying some additional properties always arise from groups like this.

  Any monoid in **Set** induces a bialgebra in **Rel** in a similar way.

- The space of complex polynomials in one variable $\mathbb{C}[x]$ gives rise to a commutative dagger bialgebra in **Hilb**. The Hilbert space in question, also called *Fock space* has $\{1, x, x^2, x^3, \ldots\}$ as an orthonormal basis, and multiplication  : $\mathbb{C}[x] \otimes \mathbb{C}[x] \longrightarrow \mathbb{C}[x]$ is defined by

  $$x^n \otimes x^m \mapsto \sqrt{\frac{(m+n)!}{m!\, n!}}\, x^{m+n}.$$

  This is a heuristic idea, since the resulting linear map $\mathbb{C}[x] \otimes \mathbb{C}[x] \longrightarrow \mathbb{C}[x]$ is unbounded, and hence not technically a morphism in **Hilb**.

The following concise formulation is a good way to remember the bialgebra laws; compare **??**.

Lemma 6.22. *The following are equivalent in a braided monoidal category:*

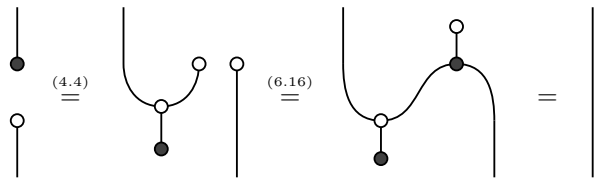
- *a comonoid* $(A, \text{  }, \text{  })$ *and monoid* $(A, \text{  }, \text{  })$ *form a bialgebra;*
- *and* *are comonoid homomorphisms;*
-  *and*  *are monoid homomorphisms.*

Proof. The canonical comonoid structure on $A \otimes A$ is that of Lemma 4.8. Unfolding what it means for  to be a comonoid homomorphism: comultiplication preservation gives the first of the bialgebra laws (6.16); counit preservation gives the second; and the last two come from requiring that  is a comonoid homomorphism. The case of monoid homomorphisms is analogous. □

As far as interaction between monoids and comonoids is concerned, Frobenius structures and bialgebras are opposite extremes. The following theorem shows that both cannot happen simultaneously, except in the trivial case. What leads to the degeneracy is the fact that the Frobenius law (5.1) equates *connected* diagrams, whereas the bialgebra laws (6.16) equate connected diagrams with *disconnected* ones.

Theorem 6.23 (Frobenius bialgebras are trivial)**.** *If a monoid* $(A, \text{  }, \text{  })$ *and comonoid* $(A, \text{  }, \text{  })$ *form both a Frobenius structure and a bialgebra in a braided monoidal category, then* $A \simeq I$.

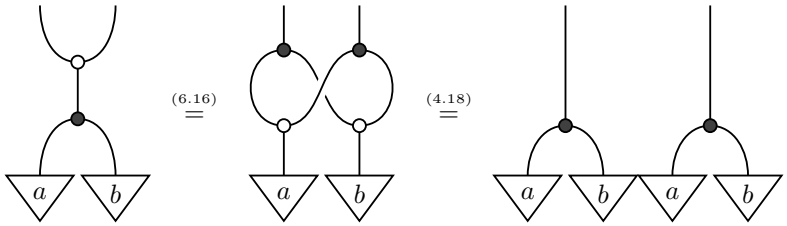
Proof. We will show that and are inverse morphisms. The bialgebra laws (6.16) already require $= \mathrm{id}_I$. For the other composite:



The first equality is counitality, the second equality is the second bialgebra law, and the last equality follows from Theorem 5.15. □

Lemma 6.24. *Let $(A,$ $,$ $,$ $,$ $)$ be a bialgebra in a braided monoidal category. The states that are copyable by and deletable by form a monoid under with unit .*

Proof. Associativity (4.5) is immediate. Unitality (4.6) comes down to the third and fourht bialgebra laws (6.16): is copyable by and deletable by . What has to be proven is that if we multiply two -copyable states using , we get another -copyable state:



Similarly using the second bialgebra law (6.16) shows that multiplying two -deletable states with gives another -deletable state. □

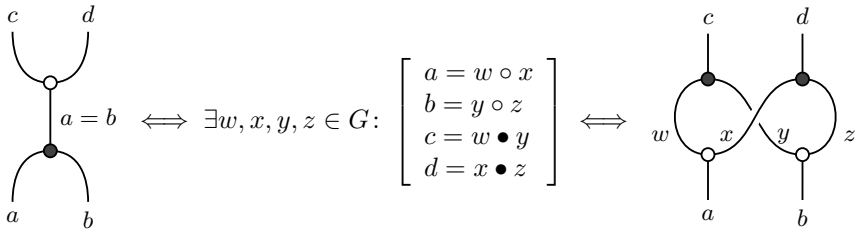
Strong complementarity

We now investigate the relationship between complementarity and bialgebras.

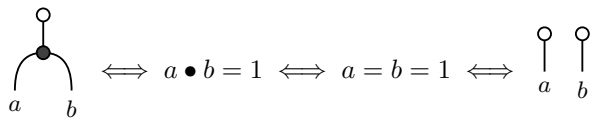
Lemma 6.25. *The special dagger Frobenius structures in* **Rel** *induced by a group and a discrete groupoid on the same set of morphisms form a bialgebra.*

The bialgebra structure is between the monoid part of one structure and the comonoid part of the other. This must be the case, since we saw that Frobenius bialgebras are trivial in Theorem 6.23.

Proof. Let $(G, \circ, 1)$ be a group and $(G, \bullet)$ a discrete groupoid. Then:



because for $c = w \bullet y$ to make sense we must have $c = w = y$. Similarly:



The final two bialgebra laws hold similarly by Proposition 6.9. □

It is not true that any two complementary groupoids form a bialgebra in **Rel**, as the following counterexample demonstrates.

Example 6.26. The following two groupoids are complementary, but do not form a bialgebra in **Rel**.

$b^2 = a = \mathrm{id}_0$ $\qquad$ $d^2 = a = \mathrm{id}_0$

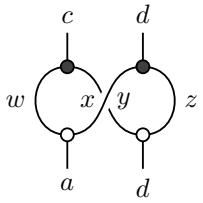
$d^2 = c = \mathrm{id}_1$ $\qquad$ $b^2 = c = \mathrm{id}_1$

Proof. Both groupoids have $G = \{a, b, c, d\}$ as set of morphisms, and $\{a, c\}$ as set of identities. Write $\circ$ for the composition in the left groupoid, and $\bullet$ for the right one. The function $G \longrightarrow \{0, 1\}^2$ given by $g \mapsto (\mathrm{cod}_\circ(g), \mathrm{cod}_\bullet(g))$ is bijective:

$$a \mapsto (0, 0) \qquad b \mapsto (0, 1) \qquad c \mapsto (1, 1) \qquad d \mapsto (1, 0)$$

Hence the two groupoids are complementary by Proposition 6.9.

Notice that $a \bullet d = d = c \circ d$. Hence $(a, d) \sim (c, d)$ in the left-hand side of the first bialgebra law (6.16). Suppose it held in the right-hand side too:



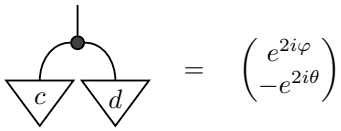
Then $w \bullet y = c$, so either $w = y = c$, or $w = y = b$. But also $y \circ z = d$, so either $y = c$ and $z = d$, or $y = d$ and $z = c$. Therefore $w = y = c$ and $z = d$. But that contradicts $w \circ x = a$, so the two groupoids do not form a bialgebra. □

The same situation occurs in **FHilb**: complementary Frobenius structures often do not form a bialgebra.

Example 6.27. Consider the object $\mathbb{C}^2$ in **FHilb**. The computational basis $\{\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right), \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)\}$ gives it a dagger Frobenius structure  for any angles $\varphi, \theta \in \mathbb{R}$. The orthogonal basis $\{\left(\begin{smallmatrix}e^{i\varphi}\\e^{i\theta}\end{smallmatrix}\right), \left(\begin{smallmatrix}e^{i\varphi}\\-e^{i\theta}\end{smallmatrix}\right)\}$ gives it a dagger Frobenius structure  . These two Frobenius structures are complementary, but they can only form a bialgebra when the angles φ and θ are integer multiples of 2π.

Proof. Write $\{a, b\}$ for the computational basis, and $\{c, d\}$ for the other one. The two bases are complementary because $\langle a|c\rangle\langle c|a\rangle = \langle a|d\rangle\langle d|a\rangle = \langle b|c\rangle\langle c|b\rangle = \langle b|d\rangle\langle d|b\rangle = 1$. Plugging in $c \otimes d$, the

first bialgebra law (6.16) holds if and only if the state



is copyable for ; that is, when φ and θ are zero modulo 2π. □

Let us name pairs of symmetric dagger Frobenius structures that satisfy both properties of being complementary and forming a bialgebra.

Definition 6.28 (Strong complementarity)**.** In a braided monoidal dagger category, two symmetric dagger Frobenius structures are *strongly complementary* when they are complementary, and also form a bialgebra.

Example 6.26 and Example 6.27 showed that strong complementarity is strictly stronger than complementarity. Strongly complementary pairs of Frobenius algebras enjoy extra properties. Note the resemblance of the following theorem to the phase group (5.27).

Theorem 6.29. *Let* (, ,) *and* (, ,) *be strongly complementary symmetric dagger Frobenius structures in a braided monoidal dagger category. The states that are self-conjugate, copyable and deletable for* (,) *form a group under* .

Proof. By Lemma 6.24 these states form a monoid, and by Proposition 6.11 every element of this monoid has a left and right inverse. □

When one of the Frobenius structures is commutative, strong complementarity lets us classify strongly complementary pairs in **FHilb**. The following theorem shows that the group algebra of Example 5.2, and (6.14) and (6.15), are in fact the only way to generate strongly complementary pairs in **FHilb**.

Theorem 6.30. *Pairs of strongly complementary symmetric dagger Frobenius structures in* **FHilb***, one of which is commutative, correspond to finite groups via* (6.14) *and* (6.15)*.*

Proof. We already saw that (6.14) and (6.15) give symmetric dagger Frobenius structures that form a strongly complementary pair, and that one of them is commutative.

Conversely, suppose symmetric dagger Frobenius structures and form a strongly complementary pair on H in **FHilb**, and that is commutative. By Theorem 6.29 the states which are self-conjugate, copyable and deletable for (,) form a group for . But by the classification theorem for commutative dagger Frobenius structures, there is an entire basis of such states for . So must be the group algebra of Example 5.2. □

Contrast the previous theorem with the open problem of classifying (non-strongly) complementary pairs of commutative Frobenius structures – mutually unbiased bases – on Hilbert spaces whose dimension is not a prime power.

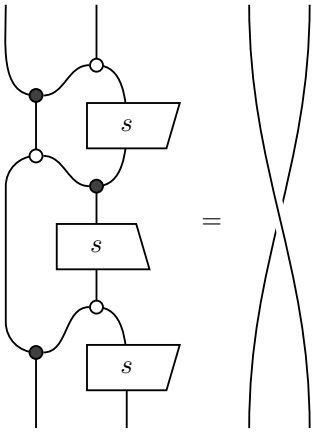
6.4 Many-qubit gates

The graphical calculus can be used to describe various quantum computing gates, and to prove that they have good properties. Before specializing to qubits in Hilbert spaces, we first show that a basic property of quantum computation really holds more generally, and only depends on (strong) complementarity: namely, a swap gate can be built using three CNOT gates.

Controlled negation

The following theorem proves that the first bialgebra law is equivalent to the property that the swap map can be built from three CNOT gates.

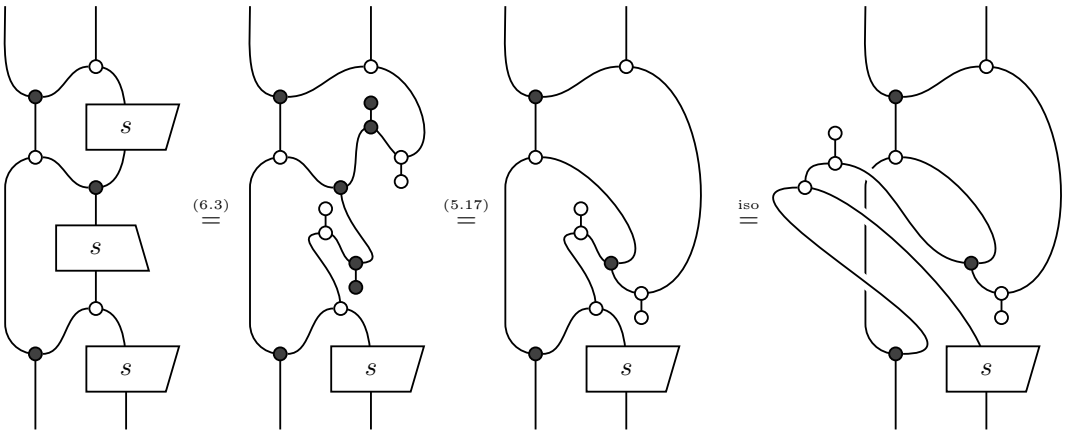
Theorem 6.31 (Swap via three CNOTs)**.** *Let* (Δ, ε) *and* (∇, η) *be complementary classical structures in a braided monoidal dagger category. If they are strongly complementary, then the following equation holds, where* s *is the morphism* (6.3)*:*

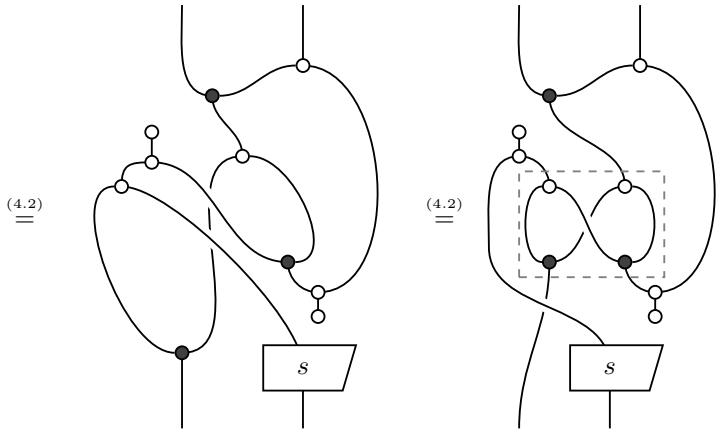


(6.17)

In fact, equation (6.17) *holds if and only if the first equation of* (6.16) *does.*

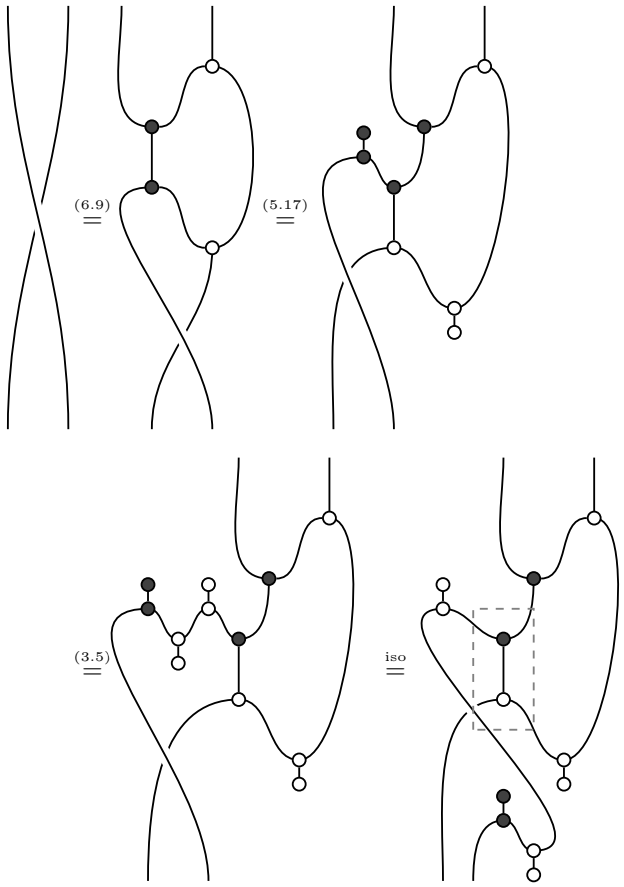
Proof. First, rewrite the left-hand side of (6.17):





The second equality uses the (noncommutative) black spider Theorem 5.21, the fourth uses cocommmutativity of  , and fifth uses the (commutative) white spider Theorem 5.22.

Rewrite the right-hand side similarly:



The first equality comes from Proposition 6.7.

Now, using strong complementarity on the marked parts turns the left-hand side into the right-hand side. Conversely, if the left-hand side equals the right-hand side, we can use snake equations to 'undo' everything but the marked bits to see that the bialgebra law must hold. □

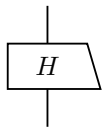
Why may we think of the left-hand side of (6.17) as a generalization of 'three CNOT gates'? It is clearly a composition of six unitary maps, namely three unitaries of the form (6.9), and three of the form (6.3).

Example 6.32. In the category **FHilb**, fix A to be the qubit $\mathbb{C}^2$. Let $(\Delta, \bullet)$ be defined by the computational basis $\{|0\rangle, |1\rangle\}$, and $(\Delta, \circ)$ by the X basis from Example 6.5. Then the three antipodes (6.3) become identities.

Furthermore, the three unitaries of the form (6.9) indeed reduce to three CNOT gates. This gate performs a NOT operation on the second qubit if the first (control) qubit is $|1\rangle$, and does nothing if the first qubit is $|0\rangle$.

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{6.18}$$

We will fix these two classical structures for the rest of this chapter. The relationship between them is $|+\rangle = |0\rangle + |1\rangle$, and $|-\rangle = |0\rangle - |1\rangle$. Hence they are transported into each other by the *Hadamard gate* (see also Lemma 5.17).

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

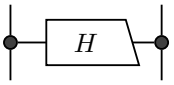
(6.19)

Controlled phases

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

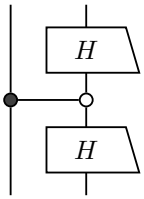
In the following lemma, we will draw dots loosely, as in Section 5.5. This is allowed, because we are dealing with classical structures.

Lemma 6.33. *The CZ gate in* **FHilb** *can be defined as follows.*

$CZ :=$ 

(6.20)

Proof. We can rewrite equation (6.20) as follows.

CZ $\overset{(5.12)}{=}$ 

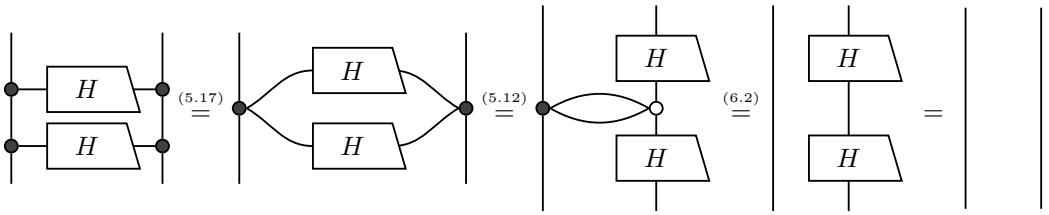
Hence

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

This is indeed the controlled Z gate. □

Proposition 6.34 (CZ has order two)**.** *If* (A, Δ) *and* (A, Δ) *are complementary classical structures in a braided monoidal dagger category, and* $A \xrightarrow{H} A$ *satisfies* $H \circ H = \mathrm{id}_A$*, then* (6.20) *makes sense and satisfies* $CZ \circ CZ = \mathrm{id}$.

Proof. Easy graphical manipulation:

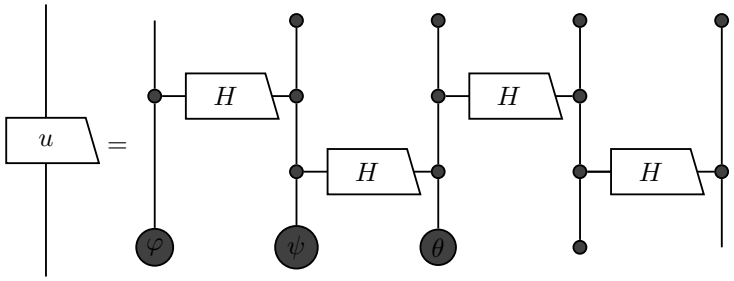


The third equality uses Proposition 6.7. □

Single qubit gates

Finally, qubits have the nice property that any unitary on them can be implemented via its *Euler angles*. More precisely: for any unitary $\mathbb{C}^2 \xrightarrow{u} \mathbb{C}^2$, there exist phases $\varphi, \psi, \theta \in \mathbb{C}$ such that $u = Z_\theta \circ X_\psi \circ Z_\varphi$, where Z_θ is the unitary rotation in the Z basis over angle θ, and X_φ in the X basis over angle φ. Therefore we can implement such unitaries abstractly using just CZ-gates and Hadamard gates.

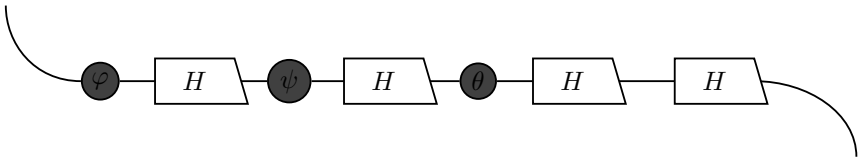
Theorem 6.35. *If a unitary $\mathbb{C}^2 \xrightarrow{u} \mathbb{C}^2$ in* **FHilb** *has Euler angles φ, ψ, θ, then:*



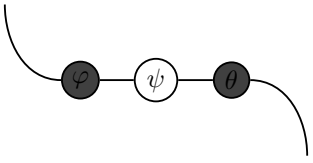
(6.21)

The phased spider notation here is that of Corollary 5.46.

Proof. By using the Phased spider Corollary 5.46 equation (6.21) reduces to



But by Lemma 5.17, this is just:



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