Lógica Quântica
Assessment 2

2022–2023

Erratum: (12/06) Definition 6 (needed in Exercise 4) has been changed to fix a mistake.
(13/06) In Exercise 1.d, "any state" changed to "any phase".

Throughout this text, we work in a dagger symmetric monoidal category $\mathbf{C}$, that is, a symmetric monoidal category equipped with an involutive contravariant endofunctor $\dagger$. We can therefore use the graphical language of dagger symmetric monoidal categories, where the action of the dagger is represented by vertical reflection of the diagrams.

Monoids Recall the following definition of monoid in a monoidal category.

Definition 1. A *monoid* in $\mathbf{C}$ is a triple (A, m, u) consisting of an object A of $\mathbf{C}$ and two arrows

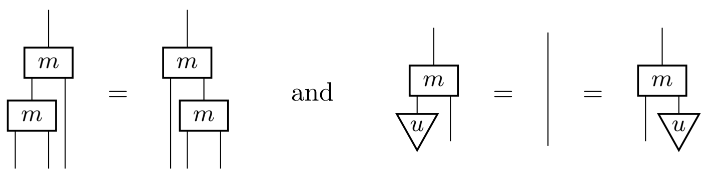
$$m \colon A \otimes A \longrightarrow A \quad \text{and} \quad u \colon I \longrightarrow A \qquad ,$$

known as *multiplication* and *unit*, satisfying the following equational properties

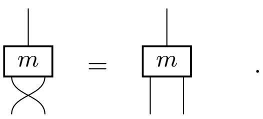
- *associativity*: $m \circ (m \otimes \mathsf{id}_A) = m \circ (id_A \otimes m)$;
- *unitality*: $m \circ (\mathsf{id}_A \otimes u) = id_A = m \circ (u \otimes \mathsf{id}_A)$.

The monoid is said to be *commutative* if $m \circ \sigma_{A,A} = m$ where $\sigma_{A,A} \colon A \otimes A \longrightarrow A \otimes A$ is the swap map.

We can write these equations using the graphical language: associativity and unitality are rendered as



while commutativity is



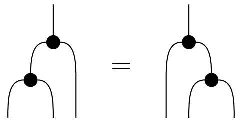
In fact, we can choose a more intuitive notation to represent m and u:

This leads to the following alternative way to present the definition of a monoid. We will use this style from now on.

Definition 2. A *monoid* in $\mathbf{C}$ is a triple (A, m, u) consisting of an object A of $\mathbf{C}$ and two arrows

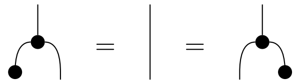
$$: A \otimes A \longrightarrow A \quad \text{and} \quad : I \longrightarrow A \quad ,$$

known as *multiplication* and *unit*, satisfying



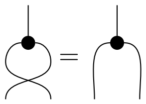
(associativity)

and



(unitality)

The monoid is said to be *commutative* if

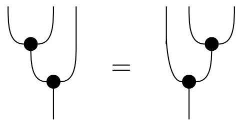


(comutativity)

Dagger monoids and comonoids As we are in a dagger category, to each monoid $(A, ,)$ corresponds a comonoid $(A, ,)$ given by *comultiplication* and *counit* maps

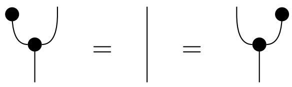
$$= ()^\dagger : A \longrightarrow A \otimes A \quad \text{and} \quad = ()^\dagger : A \longrightarrow I$$

satisfying



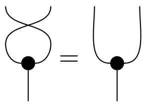
(coassociativity)

and



(counitality)

The monoid $(A, ,)$ is commutative if and only if the comonoid $(A, ,)$ is *cocommutative*:

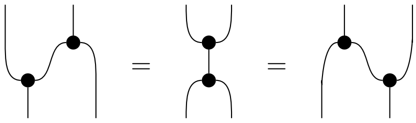


(cocommutativity)

In summary, in a dagger category, monoids and comonoids always come in pairs.

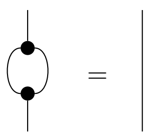
Classical structures We now consider conditions on the interaction of such monoid/comonoid pairs. These are relevant to define the concept of classical structure, which in the case of **FHilb** captures precisely the notion of orthonormal basis.

Definition 3. A *dagger Frobenius structure* in $\mathbf{C}$ is a monoid/comonoid pair satisfying the following equality known as the *Frobenius law*:



(Frobenius)

The dagger Frobenious structure is said to be *special* if it satisfies



(speciality)

Definition 4. A *classical structre* is a dagger Frobenius structure that is special and commutative.

As discussed in the lectures, classical structures in **FHilb** are in one-to-one correspondence with orthonormal bases of a Hilbert space. For example, take the Hilbert space of a qubit, $\mathbb{C}^2$. Picking a specific orthonormal basis, e.g. the computational basis

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} ,$$

determines the comultiplication map

$$= |00\rangle\langle 0| + |11\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}$$

which maps

$$:: \quad |0\rangle \longmapsto |00\rangle , \quad |1\rangle \longmapsto |11\rangle ,$$

thus *copying* the states in the computational basis. The corresponding multiplication is its adjoint

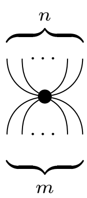
$$= |0\rangle\langle 00| + |1\rangle\langle 11| = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Moreover, the unit and counit are

$$= |0\rangle + |1\rangle = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$= \langle 0| + \langle 1| = \begin{pmatrix} 1 & 1 \end{pmatrix}$$

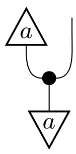
More generally, the m-to-n *spider* for this classical structure (i.e. the unique arrow $A^{\otimes m} \longrightarrow A^{\otimes n}$ representable as a (any) connected diagram built out of the (co)multiplication, (co)unit, identities, and swap by sequential and parallel composition) is



$$= \quad |0^n\rangle\langle 0^m| + |1^n\rangle\langle 1^m| \ .$$

Phases We now introduce the new notion of phase. This is the central concept explored in these questions.

Definition 5. Let (A, , ) be a classical structure. A state $a \colon I \longrightarrow A$ is a *phase* for this classical structure if it satisfies

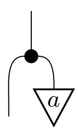


$$=$$

. (phase)

The corresponding *phase shift* is the morphism $A \longrightarrow A$ given by

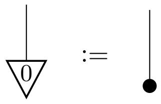
$$:=$$



. (phase shift)

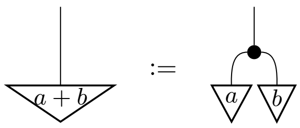
Exercise 1 (Phase group)**.** Let $(A, \;, \;)$ be a classical structure. The goal of this first question is to show that phases form a group under . Step by step:[1]

(a) Show that



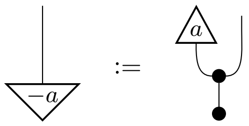
is a phase.

(b) Show that if states $a\colon I \longrightarrow A$ and $b\colon I \longrightarrow B$ are phases, then the state



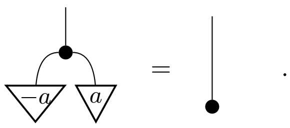
is also a phase.

(c) Show that if a is a phase, then the state



is a phase.

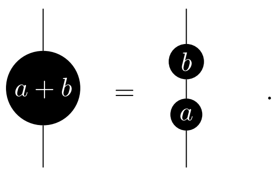
(d) Show that for any phase $a\colon I \longrightarrow A$, $(-a) + a = 0$, i.e. that



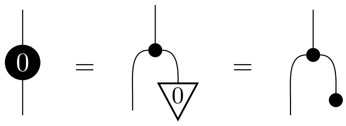
◀

Exercise 2 (Phase shift group)**.** The goal is to interpret the operations above in terms of phase shifts maps instead of phase states.

(a) Show that



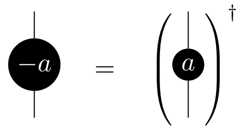
(b) What is the zero-phase shift



equal to?

[1]Note that we already know, from the fact that $(A, \;, \;)$ is a commutative monoid, that determines an operation on states that is associative, commutative, and has neutral element , i.e. it is a monoid on states. We need to show that the states that are phases are a submonoid of this, and moreover that every phase has an inverse under this operation.

(c) Observe that



and conclude that phase shifts are unitary. (Recall that an arrow $f\colon A \longrightarrow A$ is unitary if $f \circ f^\dagger = \mathsf{id}_A = f^\dagger \circ f$.)

◀

Exercise 3. In **FHilb**, consider the concrete classical structure given for $\mathbb{C}^2$ (the Hilbert space of one qubit) by the computational basis as explained above.

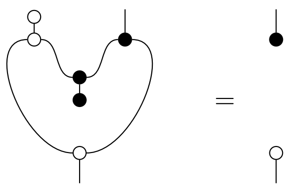
(a) What states are its phases?

(b) What is the form of the corresponding phase shifts?

◀

Complementary classical structures The notion of complementary captures the idea of bases being mutually unbiased.

Definition 6. Let A be an object equipped with two classical structures $(A, \,, \,)$ and $(A, \,, \,)$. These classical structures are said to be *complementary* if they satisfy

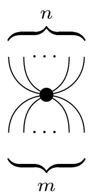


(complementarity)

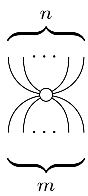
In **FHilb**, an example of two complementary classical structures on $\mathbb{C}^2$ are the classical structures defined from the computational or Z basis $\{|0\rangle, |1\rangle\}$ and from the X basis $\{|+\rangle, |-\rangle\}$, where

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \quad \text{and} \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} \quad .$$

I.e. the classical structures with spiders given by



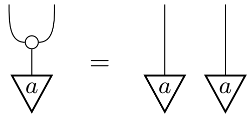
$$:= \quad |0\rangle^{\otimes n}\langle 0|^{\otimes m} + |1\rangle^{\otimes n}\langle 1|^{\otimes m} \qquad \text{and}$$



$$:= \quad |+\rangle^{\otimes n}\langle +|^{\otimes m} + |-\rangle^{\otimes n}\langle -|^{\otimes m} \qquad (\star)$$

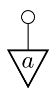
Definition 7. Let $(A, \,, \,)$ be a classical structure. With respect to the structure $(A, \,, \,)$, a state $a\colon I \longrightarrow A$ is said to be

- *copyable* if



(copyable)

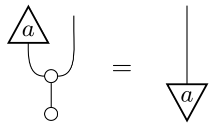
- *deletable* if [2]



(deletable)

[2]The right-hand side of the equation is blank on purpose. The empty diagram represents the arrow $\mathsf{id}_I\colon I \longrightarrow I$, the unit scalar.

- *self-conjugate* if



(self-conjugate)

In particular, the states $|0\rangle$ and $|1\rangle$ (resp. the states $|+\rangle$ and $|-\rangle$) are copyable, deletable, and self-conjugte with respect to the corresponding classical structure, denoted by black dots (resp. white dots) in Equation $(\star)$ above.

Exercise 4. Let $(A, \bullet, \bullet)$ and $(A, \circ, \circ)$ be two complementary classical structures, and let $a\colon I \longrightarrow A$ be a state. Show that if a is copyable, deletable, and self-conjugate for $(A, \circ, \circ)$, then it is a phase for $(A, \bullet, \bullet)$. ◀