Categories and Quantum Informatics exercise sheet 8: Complementarity

Exercise 5.1. (a) We have to show $L \subseteq R$. First, note that:

$$L = \{((f,g),(f,g)) \mid f,g \in Arr(G_1)\}$$

Since G_1 is a group, this means there is only one object in G_1. Therefore, all morphisms in G_1 are composable (as they are self-loops). Then, computing the relation R, we see that $((f,g),(f,g)) \in R$ for any two morphisms $f,g \in G$. Thus, $L \subseteq R$.

(b) We have to show $R \subseteq L$. Obviously, L is the same as in (a). Because the two groupoids G_1 and G_2 are complementary (and share the same morphisms), then there is a bijection:

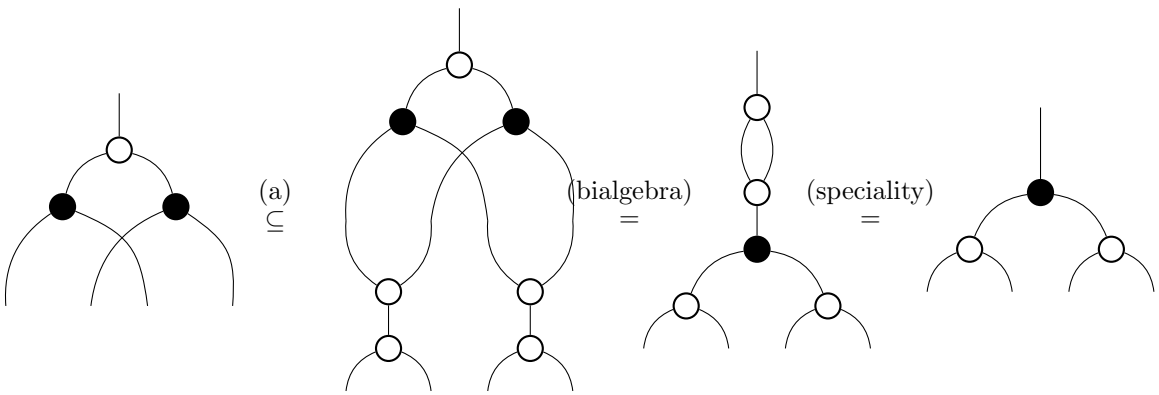
$$\begin{aligned} Arr(G_1) &\longrightarrow Ob(G_1) \times Ob(G_2) \\ a &\mapsto (dom_1(a), dom_2(a)) \end{aligned}$$

However, the groupoid G_1 has only one object and thus, this extends immidiately to a bijection between $Arr(G_1) = Arr(G_2)$ and $Ob(G_2)$. Therefore, there is a 1-1 correspondance between the arrows and objects of G_2 which means that G_2 is discrete. Thus, all arrows in G_2 are identities. Then:

$$R = \{((id_x, id_x),(id_x, id_x)) \mid x \in Ob(G_2)\}$$

so clearly $R \subseteq L$.

(c)



Note, that the last equation makes use of speciality, which is satisfied by groupoids in **Rel**.

Exercise 5.2. Let G and H be complementary groupoids. From Proposition 6.8, we have

$$|A| = |Ob(G)| \cdot |Ob(H)|$$

Because $|A|$ is prime, one of the groupoids has one object and the other has $|A|$ objects. Without loss of generality, let's assume G has one object. But then, H has as many objects as it has arrows ($|A|$) and H is therefore discrete and therefore its structure is trivial. G has one object and it is therefore a group with morphisms those of A (and G carries all of the non-trivial structure/information). Thus, the complementary pair is entirely determined by the group G.

Exercise 5.3. (a) Note, that zero states are copyable, but not of the required form.

Let $X := Arr(G)$.

An arbitrary state $u : I \longrightarrow X$ is given by:

$$u = \{(\cdot, f) \mid f \in U \subseteq X\}$$

where U is the subset of X which determines u.

Let's assume $u : I \longrightarrow X$ is copyable and non-zero. Thus, $U \neq \emptyset$. The definition of copyable state in **Rel**, then translates as:

$$\{(\cdot, (f, g)) \mid f \in U,\ g \in U\} = \{(\cdot, (f, g)) \mid cod(g) = dom(f) \Longrightarrow f \circ g \in U\}$$

From basic set theory, we get that this means:

$$f \in U,\ g \in U \ \text{ iff } (cod(g) = dom(f) \Longrightarrow f \circ g \in U)$$

for every $f, g \in X$.

By making use of this equivalence several times, we can finish the proof.

U is not empty, thus there exists some morphism $f \in U$.

$f \in U \Longrightarrow f \circ f \in U \Longrightarrow dom(f) = cod(f) = A$, for some object $A \in Ob(G)$. In other words, f must be a self-loop (or endomorphism).

If $g \in U \Longrightarrow f \circ g \in U$ and $g \circ f \in U \Longrightarrow dom(g) = cod(g) = A$. In other words, all morphisms in U are endomorphisms on the object A. Therefore, $U \subseteq G(A, A)$.

$f \circ id_A = f \in U \Longrightarrow id_A \in U$. So, the identity on A must be in U.

$\forall h : A \longrightarrow A$ we have $h \circ h^{-1} = id_A \in U \Longrightarrow h \in U$. Thus, all endomorphisms on A are in U. Therefore, $G(A, A) \subseteq U$. Combining this with the above result, we get $G(A, A) = U$.

Finally, we have to show A is disconnected. Consider an arbitrary morphism $h : A \longrightarrow B$. We have $h \circ h^{-1} = id_A \in U \Longrightarrow h \in U \Longrightarrow A = B$, which completes the proof.

(b) The right phase shift of a state $u : I \longrightarrow X$ (defined as in (a)) is given by:

$$P := \{(f, f \circ g) \mid f \in X,\ g \in U, dom(f) = cod(g)\}$$

A state is unbiased if its right phase shift is unitary. In **Rel** this means that the right phase shift is a bijection.

The fact that P is a function (not merely a relation), means that, for a given object, there can be at most one morphism in U with codomain this object.

The fact that P is defined everywhere, means that, for every object, there exists at least one morphism in U with codomain that object.

Combining these two facts, we get for every object in G, there exists exactly one morphism with codomain that object.

The fact that P is a surjection, means that, for every object, there exists at least one morphism in U with domain that object.

The fact that P is a injection, means that, for every object, there can be at most one morphism in U with domain that object (to see that, assuming two morphisms in U have the same domain, compose each of them with its inverse and then use injectivity).

Combining these two facts, we get for every object in G, there exists exactly one morphism with domain that object. This completes the proof.

(c) Proposition 6.8 shows that these two groupoids are not complementary. According to (a), non-zero copyable states do not exist in either of the groupoids and therefore the implication is trivially satisfied.

Exercise 5.4. An $n \times n$ Latin square corresponds to an n by n table with entries ranging from 1 to n, in a way that each row and each column contains each number exactly once.

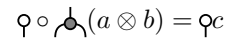
We can consider this as a multiplication table on the set $\{1, ..., n\}$ in the following sense: the product $i * j$ is given by the entry indexed by (i, j) in the table (so in the ith row and the jth column). We can extend this linearly to the map  $: \mathbb{C}^n \otimes \mathbb{C}^n \to \mathbb{C}^n$, taking $|i\rangle$ for $i = 1, .., n$ as a basis of $\mathbb{C}^n$. This is a well-defined function that maps basis elements to basis elements.
For the classical structure, we take the standard classical structure  that copies the basis elements.
We show that the first bialgebra law holds by showing that the equality holds for any choice of basis states i, j:


$$= (\quad(i, j) \otimes \quad(i, j)), \tag{1}$$

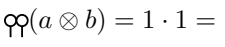
as  (i, j) defines a basis element,so a copyable states of .
On the other hand,


$$= (\quad(i, j) \otimes \quad(i, j)). \tag{2}$$

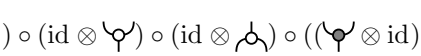
Now we will prove the second bialgebra law. Let a, b be arbitrary basis elements and let c be $a * b$. The right-hand-side gives us:


$$\begin{aligned} &= \quad c \\ &= 1 \end{aligned} \tag{3}$$

The left-hand-side give us:

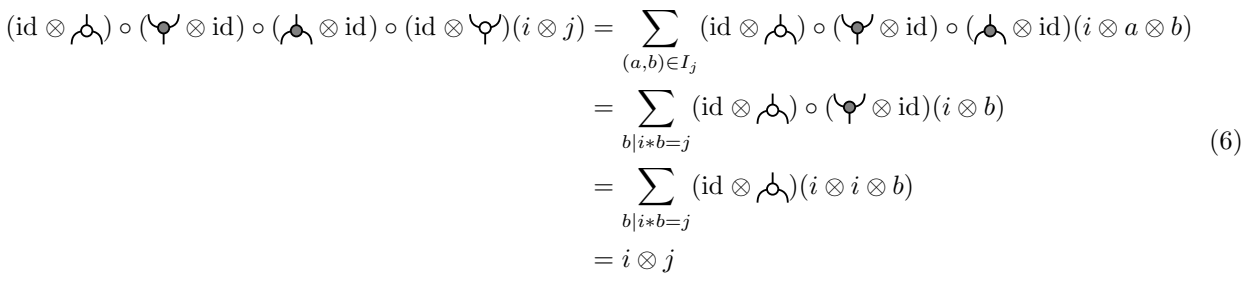

$$= 1 \cdot 1 = 1 \tag{4}$$

Consider an equivalence relation on Latin squares that allows changing the order of the rows and the columns of the latin square, and renaming the symbols. Every latin square is equivalent to one that has $1, 2, ..., n$ as its first row and as its first column. It follows that we can define a map  $: I \to \mathbb{C}^n$ as $(1) = |1\rangle$. Using this map as the unit for , the last two bialgebra equations hold as well.
Now we will show that (id $\otimes$ $) \circ ($($\otimes$ id) is unitary.
Note that the multiplication map is injective: if $i * j = i * j'$ then j must equal j', as every row contains every element exactly once. Similarly, if $i * j = i' * j$, then i must equal i'. Its dagger maps each basis element a to the sum of n tuples $\sum_{(i,j) \in I_a)} i \otimes j$ of basis elements, where I_a is the set of all indices of the entry a in the Latin square. In other words, these tuples correspond to the row and column of each entry a. Note that i and j range over $1, .., n$ and all tuples are disjoint.
Now it follows that for every two basis states $|i\rangle, |j\rangle$, where $i * j = a$ for some a.


$$\begin{aligned} &= \sum_{i=1,..,n} (\quad \otimes \mathrm{id}) \circ (\mathrm{id} \otimes \quad) \circ (\mathrm{id} \otimes \quad)(i \otimes i \otimes j) \\ &= \sum_{a=1,..,n} (\quad \otimes \mathrm{id}) \circ (\mathrm{id} \otimes \quad)(i \otimes a) \\ &= \sum_{(b,c) \in I_a} (\quad \otimes \mathrm{id})(i \otimes b \otimes c) \\ &= i \otimes j \end{aligned} \tag{5}$$

The last equality holds, because $(i \otimes b) = \delta_{b,i} i$, and furthermore, the only tuple of the form $(i, c) \in I_a$ is (i, j).

Simultaneously we have



$$
\begin{aligned}
(\mathrm{id} \otimes \mu) \circ (\eta \otimes \mathrm{id}) \circ (\mu \otimes \mathrm{id}) \circ (\mathrm{id} \otimes \eta)(i \otimes j) &= \sum_{(a,b) \in I_j} (\mathrm{id} \otimes \mu) \circ (\eta \otimes \mathrm{id}) \circ (\mu \otimes \mathrm{id})(i \otimes a \otimes b) \\
&= \sum_{b | i * b = j} (\mathrm{id} \otimes \mu) \circ (\eta \otimes \mathrm{id})(i \otimes b) \\
&= \sum_{b | i * b = j} (\mathrm{id} \otimes \mu)(i \otimes i \otimes b) \\
&= i \otimes j
\end{aligned} \tag{6}
$$

Exercise 5.5. Assume that the monoidal structure in $\mathbf{C}$ is given by the categorical product. Let (A, m, u) be a monoid. From an earlier exercise, we already know that A has a unique comonoid structure (A, d, e) given by:

$$
\begin{aligned}
d &= \langle id_A, id_A \rangle \\
e &= 1_A : A \longrightarrow 1
\end{aligned}
$$

where 1 is the terminal object of $\mathbf{C}$.
To complete the proof, we simply have to show that the bialgebra equations are satisfied. This is lengthy, but straightforward and can be done simply by expanding the definitions and using the basic algebraic properties of the categorical product. However, we have to be careful when doing this symbolically (as opposed to diagrammatically) because we also have to explicitly take into account the associator and unitors $(\alpha_{A,B,C}, \lambda_A, \rho_A)$.