Categories and Quantum Informatics exercise sheet 1: Categorical semantics

Exercise 0.1. Let $(P, \leq)$ be a partially ordered set. Show that the following is a category: the objects are the elements x of P, and there is a unique morphism $x \to y$ if and only if $x \leq y$.

Exercise 0.2. Let M be a *monoid*: a set M together with an associative binary "multiplication" operation $M \times M \to M$ written as $(m, n) \mapsto mn$ and an element $1 \in M$ such that $1m = m = m1$. Show that the following is a category: there is a single object $*$, the morphisms $* \to *$ are elements of M, and composition is multiplication. Conversely, show that any category with a single object comes from a monoid in this way.

Exercise 0.3. Let $G = (V, E)$ be a directed graph. Show that the following is a category: objects are vertices $v \in V$, morphisms $v \to w$ are paths $v \xrightarrow{e_1} \cdots \xrightarrow{e_n} w$ with $e_i \in E$, and composition is concatenation of paths. Choose $n \geq 5$, and draw a graph with n edges whose category has more than n morphisms.

Exercise 0.4. (a) If P and Q are partially ordered sets regarded as categories, show that functors $P \to Q$ are functions $f \colon P \to Q$ that are monotone: if $x \leq y$ then $f(x) \leq f(y)$.

(b) If M and N are monoids regarded as categories, show that functors $M \to N$ are functions $f \colon P \to Q$ that are homomorphisms: $f(1) = 1$ and $f(mn) = f(m)f(n)$.

(c) If G and H are graphs regarded as categories, what are functors $G \to H$?

Exercise 0.5. (a) Show that partially ordered sets and monotone functions form a category.

(b) Show that monoids and homomorphisms form a category.

Exercise 0.6. (a) Show that in **Set**, the isomorphisms are exactly the bijections.

(b) Show that in the category of monoids and homomorphisms, the isomorphisms are exactly the bijective morphisms.

(c) Show that in the category of partially ordered sets and monotone functions, the isomorphisms are not the same as the bijective morphisms.

Exercise 0.7. Consider the following isomorphisms of categories and determine which hold.

(a) $\mathbf{Rel} \simeq \mathbf{Rel}^{\mathrm{op}}$

(b) $\mathbf{Set} \simeq \mathbf{Set}^{\mathrm{op}}$

(c) For a fixed set X with powerset $P(X)$ regarded as a category, $P(X) \simeq P(X)^{\mathrm{op}}$

Exercise 0.8. Let $(P, \leq)$ be a partially ordered set, and regard it as a category.

(a) Show that a product of x and y is a greatest lower bound: an element $x \wedge y$ such that $x \wedge y \leq x$ and $x \wedge y \leq y$, and if any other element satisfies $z \leq x$ and $z \leq y$ then $z \leq x \wedge y$.

(b) Show that a coproduct of x and y is a least upper bound.

Exercise 0.9. In any category with binary products, show that $A \times (B \times C) \simeq (A \times B) \times C$.

Categories and Quantum Informatics exercise sheet 1 answers: Categorical semantics

Exercise 0.1. Composition arises from transitivity: if $x \leq y$ and $y \leq z$ then $x \leq z$. This is automatically associative. Identities arise from reflexivity: $x \leq x$. (We don't actually need anti-symmetry, pre-orders also induce categories this way.)

Exercise 0.2. Associativity of the composition of the category is precisely associativity of the monoid multiplication.

Note: pre-orders and monoids are two 'extreme' types of categories. Pre-orders have lots of objects and as few morphisms as possible. Monoids have as few objects as possible and lots of morphisms. In a sense any category is a mixture of these two extremes.

Exercise 0.3. Concatenating paths is associative. Identities arise from paths $v \longrightarrow v$ of length 0.

Exercise 0.4.

(a) A functor $P \longrightarrow Q$ by definition consists of a function $f \colon P \longrightarrow Q$ (on objects) that maps morphisms to morphisms. This means precisely that if $x \leq y$ is a morphism in P, then there must be a morphism $f(x) \leq f(y)$ in Q.

(b) A functor $M \longrightarrow N$ by definition consists of a function $\{*\} \longrightarrow \{*\}$ (on objects), and a function $f \colon M \longrightarrow N$ (on morphisms). The latter has to preserve composition ($f(mn) = f(m)f(n)$) and identities ($f(1) = 1$).

(c) Functors $G \longrightarrow H$ by definition consist of a function $f \colon \text{Vertices}(G) \longrightarrow \text{Vertices}(H)$ (on objects), and a function $g \colon \text{Edges}(G) \longrightarrow \text{Paths}(H)$. The latter induces a function $\text{Paths}(G) \longrightarrow \text{Paths}(H)$ that respects associativity of composition and identities by definition of composition and identities in the category G.

Exercise 0.5.

(a) Composition of monotone functions is monotone, and the identity is a monotone function.

(b) Composition of homomorphisms is a homomorphism, and the identity is a homomorphism.

Exercise 0.6.

(a) Isomorphisms are clearly bijections. Conversely, suppose $f \colon A \longrightarrow B$ is a bijection. Then there exists a function $f^{-1} \colon B \longrightarrow A$ with $f(f^{-1}(b)) = b$ and $f(f^{-1}(a)) = a$. So f is an isomorphism.

(b) Isomorphisms are clearly bijective morphisms. Conversely, suppose $f \colon M \longrightarrow N$ is a bijective morphism. Then there exists a function $f^{-1} \colon N \longrightarrow M$ that inverts it. We have to show that f^{-1} is a homomorphism. Clearly $f^{-1}(1) = f^{-1}(f(f^{-1}(1))) = f^{-1}(f(1)) = 1$. Similarly $f^{-1}(xy) = f^{-1}(f(f^{-1}(x))f(f^{-1}(y))) = f^{-1}(f(f^{-1}(x)f^{-1}(y))) = f^{-1}(x)f^{-1}(y)$.

(c) Let P be the partially ordered set $\{0, 1\}$ where 0 and 1 are incomparable: $0 \not\leq_P 1$ nor $1 \not\leq_P 0$. Let Q be the set $\{0, 1\}$ partially ordered by $0 \leq_Q 1$ (but not $1 \leq_Q 0$). Let $f \colon P \longrightarrow Q$ be the function $f(0) = 0$ and $f(1) = 1$. Then f is bijective and monotone. Its inverse would have to be the set-theoretic function $Q \longrightarrow P$ given by $0 \mapsto 0$ and $1 \mapsto 1$, but that function is not monotone.

Exercise 0.7.

(a) True: the functor that sends a set A to itself, and a relation $R \subseteq A \times B$ to $\{(b, a) \mid (a, b) \in R\} \subseteq B \times A$, is its own inverse.

(b) False: if there were an isomorphism, then $\mathbf{Set}(A, B) \simeq \mathbf{Set}(B, A)$ for any sets A, B. But for e.g.

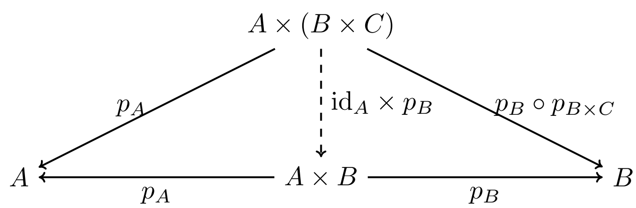
$A = \{*\}$ and $B = \{0, 1\}$ these two (hom)sets have different cardinality.

(c) True: the assignment on objects that sends $U \in P(X)$ to its complement $X \setminus U \in P(X)$ is functorial, and its own inverse.

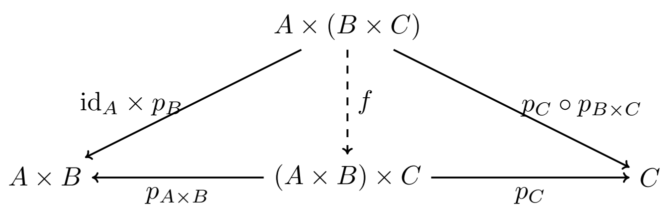
Exercise 0.8. (a) A product of x and y is by definition an object $x \wedge y$ such that $x \geq x \wedge y \leq y$. It has to satisfy the universal property: if there is another object z with $x \geq z \leq y$, then there is a (unique) morphism $z \leq x \wedge y$.

(b) Reverse all the inequality signs.

Exercise 0.9. The universal property of $A \times B$ provides a morphism that we'll call $\mathrm{id}_A \times p_B$:



The universal property of $(A \times B) \times C$ now provides a morphism $f \colon A \times (B \times C) \longrightarrow (A \times B) \times C$:



Similarly we find a morphism $g \colon (A \times B) \times C \longrightarrow A \times (B \times C)$.
Now $p_A \circ (g \circ f) = p_A \circ \mathrm{id}_{A\times(B\times C)}$ and $p_{B\times C} \circ (g \circ f) = p_{B\times C} \circ \mathrm{id}_{A\times(B\times C)}$. But the universal property of $A \times (B \times C)$ says there is only one morphisms that can satisfy this, so we must have $g \circ f = \mathrm{id}$. Similarly $f \circ g = \mathrm{id}$.

Categories and Quantum Informatics exercise sheet 2: Hilbert spaces, monoidal categories

Exercise 1.1. Show that in **FHilb**, the isomorphisms are precisely the bijective morphisms.

Exercise 1.2. Prove that direct sums form products and coproducts in **FHilb**.

Exercise 1.3. Show that the Kronecker product of matrices f, g, and h, satisfies $(f \otimes g) \otimes h = f \otimes (g \otimes h)$.

Exercise 1.4. Let A, B, C, D be objects in a monoidal category. Construct a morphism

$$(((A \otimes I) \otimes B) \otimes C) \otimes D \longrightarrow A \otimes (B \otimes (C \otimes (I \otimes D))).$$

Can you find another?

Exercise 1.5. Convert the following algebraic equations into graphical language. Which would you expect to be true in any symmetric monoidal category?

(a) $(g \otimes \mathrm{id}) \circ \sigma \circ (f \otimes \mathrm{id}) = (f \otimes \mathrm{id}) \circ \sigma \circ (g \otimes \mathrm{id})$ for $A \xrightarrow{f,g} A$.

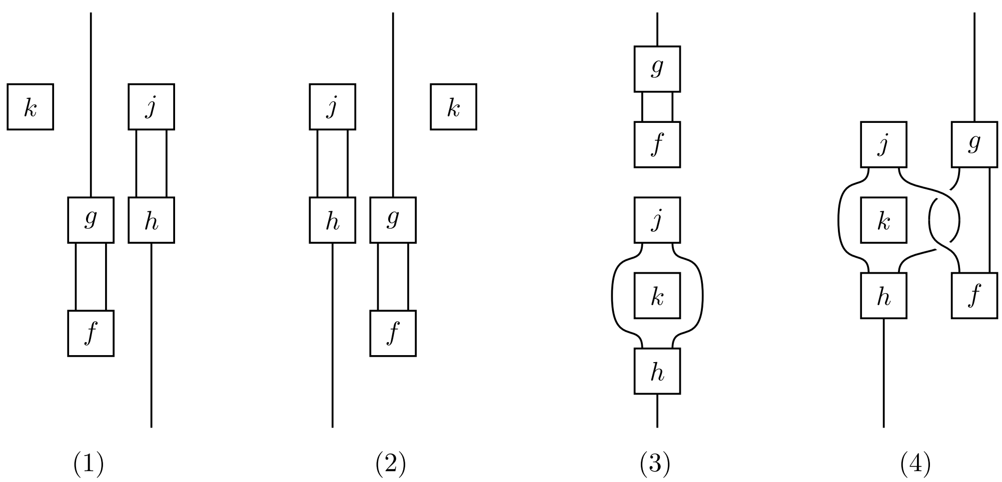
(b) $(f \otimes (g \circ h)) \circ k = (\mathrm{id} \otimes f) \circ ((g \otimes h) \circ k)$, for $A \xrightarrow{k} B \otimes C$, $C \xrightarrow{h} B$ and $B \xrightarrow{f,g} B$.

(c) $(\mathrm{id} \otimes h) \circ g \circ (f \otimes \mathrm{id}) = (\mathrm{id} \otimes f) \circ g \circ (h \otimes \mathrm{id})$, for $A \xrightarrow{f,h} A$ and $A \otimes A \xrightarrow{g} A \otimes A$.

(d) $h \circ (\mathrm{id} \otimes \lambda) \circ (\mathrm{id} \otimes (f \otimes \mathrm{id})) \circ (\mathrm{id} \otimes \lambda^{-1}) \circ g = h \circ g \circ \lambda \circ (f \otimes \mathrm{id}) \circ \lambda^{-1}$, for $A \xrightarrow{g} B \otimes C$, $I \xrightarrow{f} I$ and $B \otimes C \xrightarrow{h} D$.

(e) $\rho_C \circ (\mathrm{id} \otimes f) \circ \alpha_{C,A,B} \circ (\sigma_{A,C} \otimes \mathrm{id}_B) = \lambda_C \circ (f \otimes \mathrm{id}) \circ \alpha^{-1}_{A,B,C} \circ (\mathrm{id} \otimes \sigma_{C,B}) \circ \alpha_{A,C,B}$ for $A \otimes B \xrightarrow{f} I$.

Exercise 1.6. Consider the following diagrams in the graphical calculus:

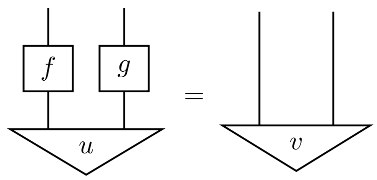


(a) Which of the diagrams (1), (2) and (3) are equal as morphisms in a monoidal category?

(b) Which of the diagrams (1), (2), (3) and (4) are equal as morphisms in a braided monoidal category?

(c) Which of the diagrams (1), (2), (3) and (4) are equal as morphisms in a symmetric monoidal category?

Exercise 1.7. We say that two joint states $I \xrightarrow{u,v} A \otimes B$ are *locally equivalent*, written $u \sim v$, if there exist invertible maps $A \xrightarrow{f} A$, $B \xrightarrow{g} B$ such that



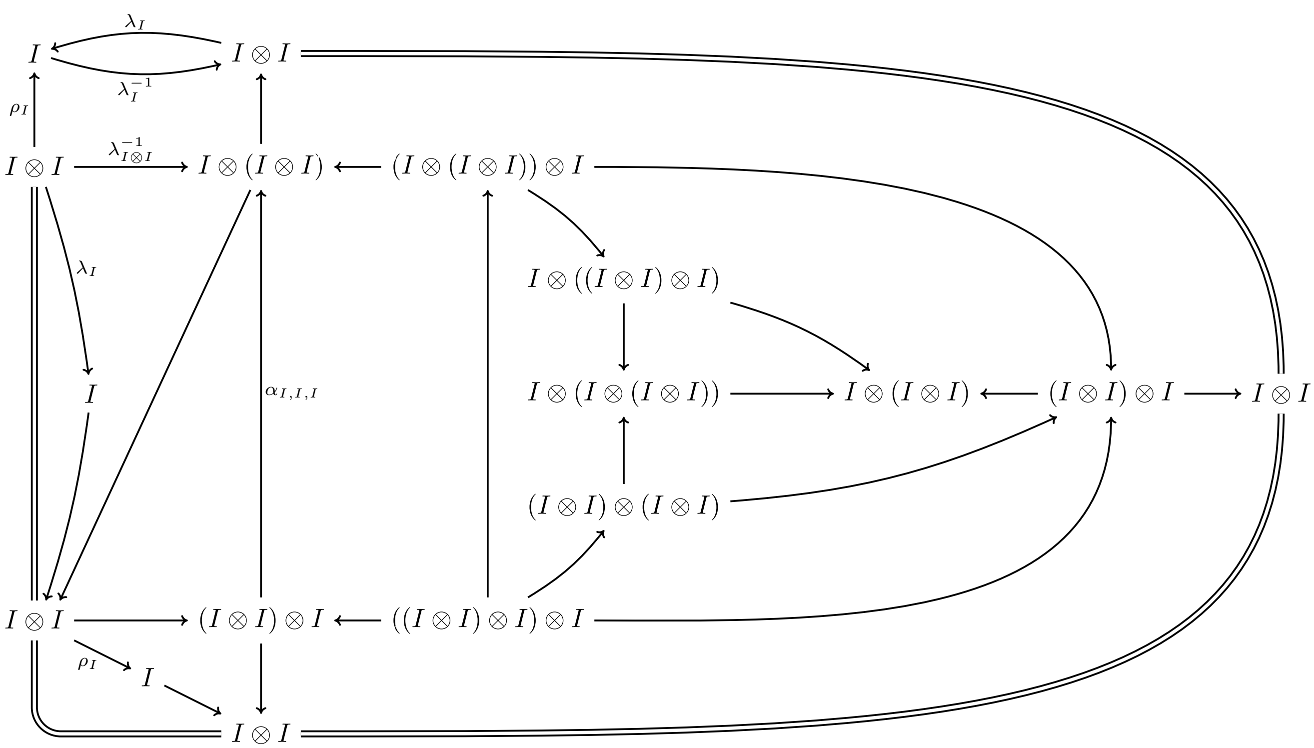
(a) Show that $\sim$ is an equivalence relation.

(b) Find all isomorphisms $\{0,1\} \longrightarrow \{0,1\}$ in **Rel**.

(c) Write out all 16 states of the object $\{0,1\} \times \{0,1\}$ in **Rel**.

(d) Use your answer to (b) to group the states of (c) into locally equivalent families. How many families are there? Which of these are entangled?

Exercise 1.8. Complete the following proof that $\rho_I = \lambda_I$ in a monoidal category, by labelling every arrow, and indicating for each region whether it follows from the triangle equation, the pentagon equation, naturality, or invertibility. Head-to-tail arrows are always inverse pairs.



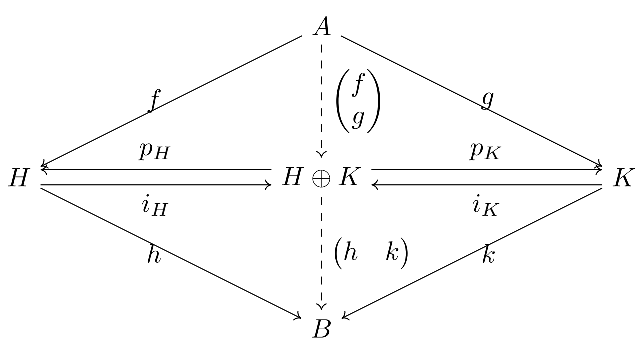
Categories and Quantum Informatics exercise sheet 2 answers: Hilbert spaces, monoidal categories

Exercise 1.1. Clearly isomorphisms are bijective morphisms. Any bijective morphism $f\colon H \longrightarrow K$ has a set-theoretical inverse $f^{-1}\colon K \longrightarrow H$; we have to prove that it is a morphism. It is additive: $f^{-1}(x+y) = f^{-1}(f(f^{-1}(x))+f(f^{-1}(y))) = f^{-1}(f(f^{-1}(x)+f^{-1}(y))) = f^{-1}(x)+f^{-1}(y)$. It respects scalar multiplication: $f^{-1}(sx) = f^{-1}(sf(f^{-1}(x))) = f^{-1}(f(sf^{-1}(x))) = sf^{-1}(x)$. (And it is automatically bounded as H and K are finite-dimensional.)

Exercise 1.2. The projections and injections are given by

$$
\begin{aligned}
p_H &\colon H \oplus K \longrightarrow H & p_H(x,y) &= x \\
p_K &\colon H \oplus K \longrightarrow H & p_K(x,y) &= y \\
i_H &\colon H \longrightarrow H \oplus K & i_H(x) &= (x,0) \\
i_K &\colon H \longrightarrow H \oplus K & i_K(y) &= (0,y)
\end{aligned}
$$

and the universal properties



are given by

$$
\begin{pmatrix} f \\ g \end{pmatrix} \colon a \mapsto (f(a), g(a))
$$
$$
\begin{pmatrix} h & k \end{pmatrix} \colon (x,y) \mapsto f(x) + g(y).
$$

Exercise 1.3. Both $(f \otimes g) \otimes h$ and $f \otimes (g \otimes h)$ expand to

$$
\begin{pmatrix}
f_{11}g_{11}h_{11} & f_{11}g_{11}h_{12} & f_{11}g_{12}h_{11} & f_{11}g_{12}h_{12} & f_{12}g_{11}h_{11} & f_{12}g_{11}h_{12} & f_{12}g_{12}h_{11} & f_{12}g_{12}h_{12} \\
f_{11}g_{11}h_{21} & f_{11}g_{11}h_{22} & f_{11}g_{12}h_{21} & f_{11}g_{12}h_{22} & f_{12}g_{11}h_{21} & f_{12}g_{11}h_{22} & f_{12}g_{12}h_{21} & f_{12}g_{12}h_{22} \\
f_{11}g_{21}h_{11} & f_{11}g_{21}h_{12} & f_{11}g_{22}h_{11} & f_{11}g_{22}h_{12} & f_{12}g_{21}h_{11} & f_{12}g_{21}h_{12} & f_{12}g_{22}h_{11} & f_{12}g_{22}h_{12} \\
f_{11}g_{21}h_{21} & f_{11}g_{21}h_{22} & f_{11}g_{22}h_{21} & f_{11}g_{22}h_{22} & f_{12}g_{21}h_{21} & f_{12}g_{21}h_{22} & f_{12}g_{22}h_{21} & f_{12}g_{22}h_{22} \\
f_{21}g_{11}h_{11} & f_{21}g_{11}h_{12} & f_{21}g_{12}h_{11} & f_{21}g_{12}h_{12} & f_{22}g_{11}h_{11} & f_{22}g_{11}h_{12} & f_{22}g_{12}h_{11} & f_{22}g_{12}h_{12} \\
f_{21}g_{11}h_{21} & f_{21}g_{11}h_{22} & f_{21}g_{12}h_{21} & f_{21}g_{12}h_{22} & f_{22}g_{11}h_{21} & f_{22}g_{11}h_{22} & f_{22}g_{12}h_{21} & f_{22}g_{12}h_{22} \\
f_{21}g_{21}h_{11} & f_{21}g_{21}h_{12} & f_{21}g_{22}h_{11} & f_{21}g_{22}h_{12} & f_{22}g_{21}h_{11} & f_{22}g_{21}h_{12} & f_{22}g_{22}h_{11} & f_{22}g_{22}h_{12} \\
f_{21}g_{21}h_{21} & f_{21}g_{21}h_{22} & f_{21}g_{22}h_{21} & f_{21}g_{22}h_{22} & f_{22}g_{21}h_{21} & f_{22}g_{21}h_{22} & f_{22}g_{22}h_{21} & f_{22}g_{22}h_{22}
\end{pmatrix}.
$$

Note: we might try to take cardinal numbers $\mu, \nu, \ldots$ as objects in $\mathbf{Mat}_{\mathbb{C}}$, and μ-by-ν matrices of complex numbers such that each row and column is square summable as morphisms $\mu \to \nu$. That is a fine category. But it is not monoidal in the same way as above. Taking $\mu\nu$ as tensor product of objects is fine. The issue is with tensor products of morphisms. To write down the Kronecker product of a μ-by-ν matrix f and a κ-by-λ matrix g, you need functions $\varphi_\mu \colon \mu \times \kappa \to \mu$ and $\psi_\kappa \colon \mu \times \kappa \to \kappa$ to say $(f \otimes g)_{ij} = f_{\varphi_\kappa(i), \varphi_\lambda(j)} g_{\varphi_\kappa(i)\psi_\lambda(j)}$. In the finite case, we took $\varphi_m(i) = \lfloor i/m \rfloor$ and $\psi_m(i) = i \mod m$ (so that $i = m \cdot \varphi_m(i) + \psi_m(i)$). But it seems unlikely that functions φ_μ and ψ_μ exist for all cardinals μ that satisfy this associativity.

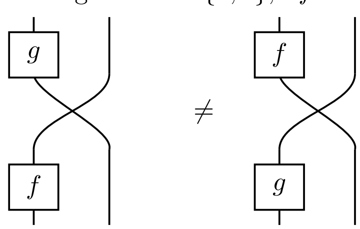
Exercise 1.4. For example:

$$
\begin{aligned}
(((A \otimes I) \otimes B) \otimes C) \otimes D &\xrightarrow{((\rho_A \otimes \mathrm{id}_B) \otimes \mathrm{id}_C) \otimes \mathrm{id}_D} ((A \otimes B) \otimes C) \otimes D \\
&\xrightarrow{\alpha_{A,B,C} \otimes \mathrm{id}_D} (A \otimes (B \otimes C)) \otimes D \\
&\xrightarrow{\alpha_{A,B \otimes C,D}} A \otimes ((B \otimes C) \otimes D) \\
&\xrightarrow{\mathrm{id}_A \otimes \alpha_{B,C,D}} A \otimes (B \otimes (C \otimes D)) \\
&\xrightarrow{\mathrm{id}_A \otimes (\mathrm{id}_B \otimes (\mathrm{id}_C \otimes \lambda_D^{-1}))} A \otimes (B \otimes (C \otimes (I \otimes D)))
\end{aligned}
$$

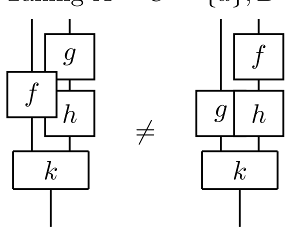
Because of coherence, this is the only morphism of this type built from the data of a monoidal category. So unless we have more information about the category than just that it's monoidal, we cannot find another morphism with the same domain and codomain.

Exercise 1.5. Recall that the swap map is natural.

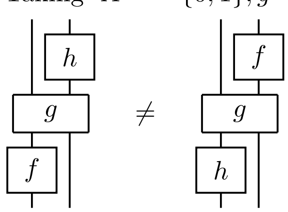
(a) Taking $A = \{0, 1\}$, $f = \mathrm{id}_A$ and $g(0) = 1$ and $g(1) = 0$ in $(\mathbf{Set}, \times)$ shows that



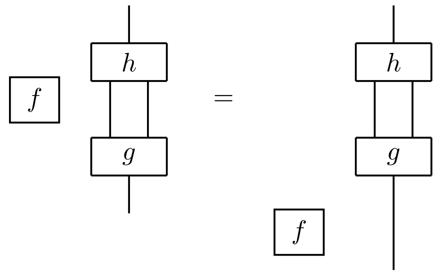
(b) Taking $A = C = \{a\}, B = \{0, 1\}, k(a) = (0, a), f = \mathrm{id}_B$ and $g(0) = 1,\ g(1) = 0$ in $(\mathbf{Set}, \times)$ shows that



(c) Taking $A = \{0, 1\}, g = \mathrm{id}_{A \times A}, f = \mathrm{id}_A$ and $h(0) = 1,\ h(1) = 0$ in $(\mathbf{Set}, \times)$ shows that

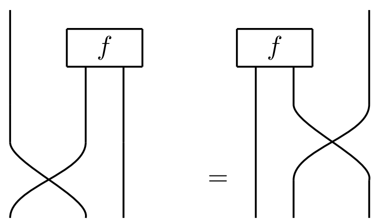


(d) The equation presented below:



is clearly true in the graphical calculus for monoidal categories.

(e) The equation presented below:



is clearly true in the graphical calculus for symmetric monoidal categories.

Exercise 1.6. (a) In monoidal categories, equalities of the diagrams hold iff they can be continously deformed into each other using 2-dimensional isotopy. Diagram (1) can be continously deformed into diagram (2), so they are equal. In diagram (3), the scalar k is stuck between the wires of j and h, so it is not equal to (1) and (2).

(b) In braided monoidal categories, equalities of the diagrams hold iff they can be continously deformed into each other using 3-dimensional isotopy. From (a) we have (1) = (2). Using 3-dimensional isotopy, we can show (1) = (2) = (3) by taking the scalar k out in the third dimension and then moving it over the enclosing wires.
However, we can't show that (4) is equal to the other three diagrams using the axioms of a braided monoidal category. We can still move the scalar k out of the enclosing wires, but we can't uncross the wires themselves. Note, that removing the crossing of the wires in (4) requires that $\sigma_{B,A} \circ \sigma_{A,B} = \mathrm{id}_{A\otimes B}$ which is always true for symmetric monoidal categories, but not necessarily for braided monoidal categories.

(c) So, in (c) all diagrams are equal, but in (b) (1) = (2) = (3) $\neq$ (4).

Exercise 1.7. Two joint states are locally equivalent when then can be transformed into one another using only uncorrelated local operations. So if two joint states possess a different 'amount of correlation', they will not be locally equivalent.

(a) Taking $f = g = \mathrm{id}$ shows that $u \sim u$. If $u \sim v$ because $v = (f \otimes g) \circ u$, then also $(f^{-1} \otimes g^{-1}) \circ v = u$, whence $v \sim u$. Finally, if $u \sim v$ and $v \sim w$ because $v = (f \otimes g) \circ u$ and $w = (k \otimes h) \circ v$, then $w = ((k \circ f) \otimes (h \circ g)) \circ u$ by the interchance law, so that $u \sim w$.

(b) Isomorphisms in **Rel** are the graphs of bijections: $\{(0,0),(1,1)\}$ and $\{(0,1),(1,0)\}$ are the only isomorphisms $\{0,1\} \longrightarrow \{0,1\}$.

(c) States of $\{0,1\} \times \{0,1\}$ are its subsets.

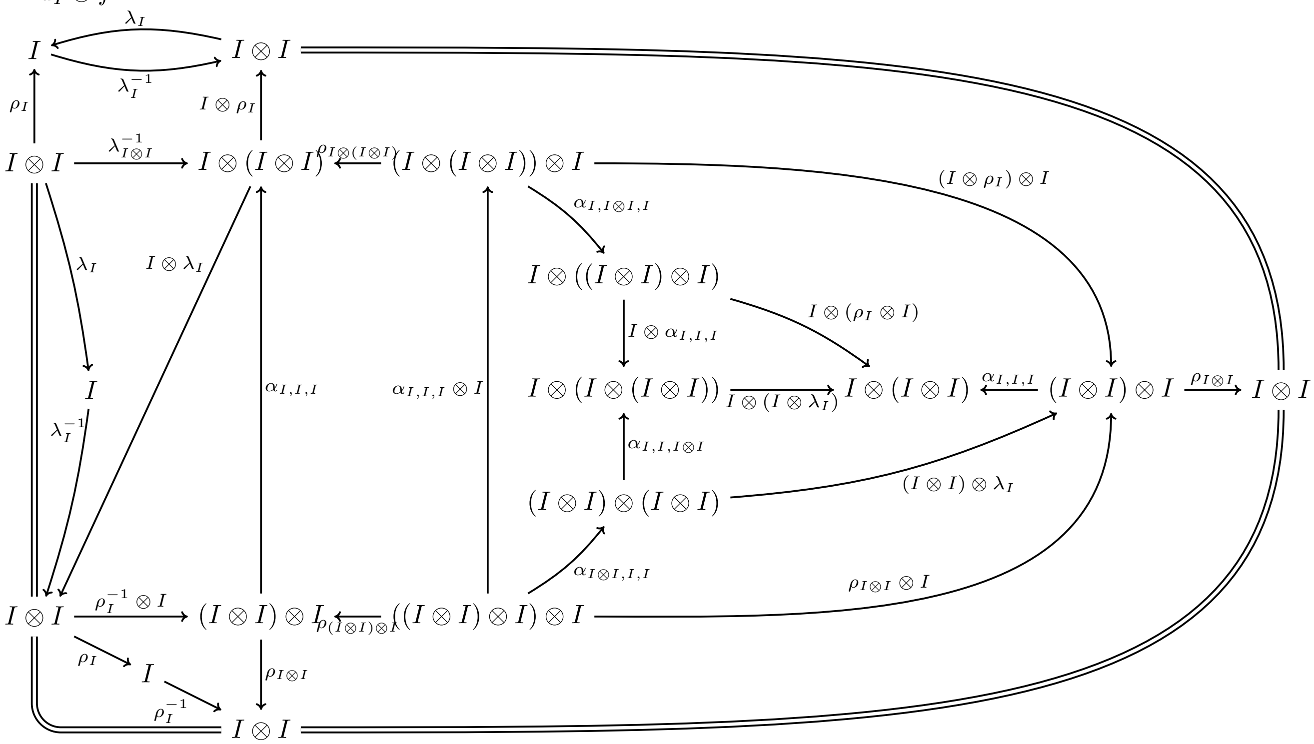
(d) Simply starting with one state we haven't classified yet, and generating all possible locally equivalent ones by pre- and/or postcomposing with all bijections, we find the following 7 local equivalence classes.

$$\emptyset$$
$$\{(0,0)\} \sim \{(0,1\} \sim \{(1,0)\} \sim \{(1,1)\}$$
$$\{(0,0),(0,1)\} \sim \{(1,0),(1,1)\}$$

$\{(0,0),(1,0)\} \sim \{(0,1),(1,1)\}$
$\{(0,0),(1,1)\} \sim \{(0,1),(1,0)\}$
$\{(0,0),(0,1),(1,0)\} \sim \{(0,0),(0,1),(1,1)\} \sim \{(0,0),(1,0),(1,1)\} \sim \{(0,1),(1,0),(1,1)\}$
$\{(0,0),(0,1),(1,0),(1,1)\}$

Notice that local equivalence respects cardinality (but states of the same cardinality need not be locally equivalent).

Exercise 1.8. The axiom applying to each region can be deduced from its number of non-identity sides: 2 for invertibility, 3 for triangle, 4 for naturality, and 5 for pentagon. To save space below we write $I \otimes f$ for $\mathrm{id}_I \otimes f$.



Categories and Quantum Informatics exercise sheet 3: Scalars

Exercise 2.1. Show that the following defines a dagger category:

- *objects* (A, p) are finite sets A equipped with *prior probability distributions*, functions $p : A \to \mathbb{R}^+$ such that $\sum_{a \in A} p(a) = 1$;
- *morphisms* $(A, p) \xrightarrow{f} (B, q)$ are *conditional probability distributions*, functions $f : A \times B \to \mathbb{R}^{\geq 0}$ such that for all $a \in A$ we have $\sum_{b \in B} f(a, b) = 1$, and for all $b \in B$ we have $q(b) = \sum_{a \in A} p(a) f(a, b)$;
- *composition* is composition of probability distributions as matrices of real numbers;
- the *dagger* is the *Bayesian converse*, acting on $f : A \times B \to \mathbb{R}^{\geq 0}$ to give $f^\dagger : B \times A \to \mathbb{R}^{\geq 0}$, defined as $f^\dagger(b, a) = f(a, b) p(a)/q(b)$.

Note that the Bayesian converse is always well-defined since we require our prior probability distributions to be nonzero at every point.

Exercise 2.2. Show that all joint states are product states when $A \otimes B$ is a product of A and B and I is a terminal object. Conclude that monoidal categories modeling nonlocal correlation such as entanglement must have a tensor product that is not a (categorical) product.

Exercise 2.3. Let $A \xrightarrow{R} B$ be a morphism in the dagger category **Rel**.

(a) Show that R is unitary if and only if it is (the graph of) a bijection;

(b) Show that R is self-adjoint if and only if it is symmetric;

(c) Show that R is positive if and only if R is symmetric and $a\,R\,b \Rightarrow a\,R\,a$.

(d) Is every isometry $A \to A$ in **Rel** unitary?

Exercise 2.4. Is $\mathbf{Mat}_{\mathbb{C}}$ a monoidal dagger category?

Exercise 2.5. Fuglede's theorem is the following statement for morphisms $f, g \colon A \to A$ in **Hilb**: if $f \circ f^\dagger = f^\dagger \circ f$ and $f \circ g = g \circ f$, then also $f^\dagger \circ g = g \circ f^\dagger$. Show that this does not hold in **Rel**.

Exercise 2.6. Recall the notion of local equivalence from Exercise Sheet 2. In **Hilb**, we can write a state $\mathbb{C} \xrightarrow{\phi} \mathbb{C}^2 \otimes \mathbb{C}^2$ as a column vector

$$\phi = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix},$$

or as a matrix

$$M_\phi := \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

(a) Show that ϕ is an entangled state if and only if M_ϕ is invertible. (Hint: a matrix is invertible if and only if it has nonzero determinant.)

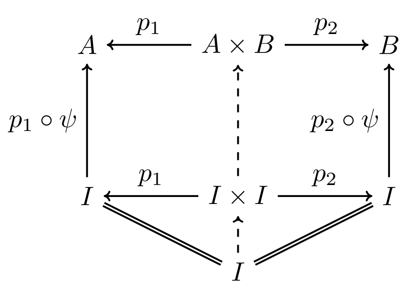
(b) Show that $M_{(\mathrm{id}_{\mathbb{C}^2} \otimes f) \circ \phi} = M_\phi \circ f^{\mathrm{T}}$, where $\mathbb{C}^2 \xrightarrow{f} \mathbb{C}^2$ is any linear map and f^{T} is the transpose of f in the canonical basis of $\mathbb{C}^2$.

(c) Use this to show that there are three families of locally equivalent joint states of $\mathbb{C}^2 \otimes \mathbb{C}^2$.

Categories and Quantum Informatics exercise sheet 3: Scalars

Exercise 2.1. The composition of two morphisms is a well-defined morphisms. The dagger is well-defined and involutive, and respects composition.

Exercise 2.2. We will show that we can write any state $\psi : I \to A \otimes B$ as the product state $\psi = (p_1 \circ \psi \otimes p_1 \circ \psi) \circ \lambda_I^{-1}$. Since the tensor product is a categorical product, $\psi : I \to A \times B$ makes the diagram below comute. The map $< p_1 \circ \psi, p_2 \circ \psi > \circ \lambda^{-1}$ makes the diagram commute as well for the following reason: Since $I \cong I \times I$ and I is the terminal object, $I \times I$ is the terminal object; hence, there is one unique arrow $I \to I \times I$, so λ^{-1} makes the lower triangle commute. By definition of the product, $< p_1 \circ \psi, p_2 \circ \psi >$ makes the upper square commute. It follows from the universal property of products that $\psi =< p_1 \circ \psi, p_2 \circ \psi > \circ \lambda^{-1}$.



Exercise 2.3. (a) First, $R^\dagger \circ R = \mathrm{id}_A$ implies that R relates every element a of A to some element of B. If it was related to two elements of B, that would violate $R \circ R^\dagger = \mathrm{id}_B$. Finally, $R \circ R^\dagger = \mathrm{id}_B$ means that every element of B is related to some element of A. So all in all, R relates each element of A to precisely one element of B, and vice versa.

(b) By definition, R being self-adjoint means that aRb if and only if $aR^\dagger b$, which in turns holds if and only if bRa.

(c) If R is symmetric and satisfies $a\,R\,b \Rightarrow a\,R\,a$, setting

$$S = \{(a, (x, y)) \mid a \in A, (x, y) \in R, a = x \text{ or } a = y\}$$

gives $R = S^\dagger \circ S$.

(d) No; $R = \{(\bullet, 0), (\bullet, 1)\} \colon \{\bullet\} \longrightarrow \{0, 1\}$ satisfies $R^\dagger \circ R = \mathrm{id}_{\{\bullet\}}$, but is not (the graph of) a subset inclusion.

Exercise 2.4. Transposition gives a dagger, and the Kronecker product of matrices respects transposition.

Exercise 2.5. Take $A = \{0, 1\}$, $R = \{(0, 0), (1, 0), (1, 1)\}$, and $S = \{(1, 0)\}$. Then $R^\dagger \circ R = R \circ R^\dagger$ and $R \circ S = S \circ R$, but not $R^\dagger \circ S = S \circ R^\dagger$.

Exercise 2.6. (a) Notice that ϕ is the product state of $\mathbb{C} \xrightarrow{\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)} \mathbb{C}^2$ and $\mathbb{C} \xrightarrow{\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)} \mathbb{C}^2$ precisely when

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} ux \\ uy \\ vx \\ vy \end{pmatrix}.$$

In this case, $\det(M_\phi) = ad - bc = uxvy - uyvx = 0$, so ϕ is invertible.
Conversely, suppose $ad - bc = 0$. If $a \neq 0$, then we may take $u = 1$, $v = ca^{-1}$, $x = a$, and $y = b$ to show that ϕ is a product state. Similar choices work when one of b,c or d is nonzero. Finally, if $a = b = c = d = 0$, we may take $u = v = x = y = 0$.

(b) Compute

$$M_\phi \circ f^{\mathrm{T}} = \begin{pmatrix} au + bv & ax + by \\ cu + dv & cx + dy \end{pmatrix},$$

and

$$(\mathrm{id}_{\mathbb{C}^2} \otimes f) \circ \phi = \begin{pmatrix} u & v & 0 & 0 \\ x & y & 0 & 0 \\ 0 & 0 & u & v \\ 0 & 0 & x & y \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} au + bv \\ ax + by \\ cu + dv \\ cx + dy \end{pmatrix}.$$

(c) First, we show that all entangled states ϕ are locally equivalent to $\psi = \left(\begin{smallmatrix} 1 \\ 0 \\ 0 \\ 1 \end{smallmatrix}\right)$. Indeed, if M_ϕ is invertible, then $M_\psi = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = M_\phi \circ (((M_\phi)^{-1})^{\mathrm{T}})^{\mathrm{T}} = M_{(\mathrm{id}_{\mathbb{C}^2} \otimes (M_\phi^{-1})^{\mathrm{T}}) \circ \phi}$, so $\psi = (\mathrm{id}_{\mathbb{C}^2} \otimes (M_\phi^{-1})^{\mathrm{T}} \circ \phi$. Also, product states can never be locally equivalent to entangled states, so all entangled states form one equivalence class.
Second, the zero state $\left(\begin{smallmatrix} 0 \\ 0 \\ 0 \\ 0 \end{smallmatrix}\right)$ is an equivalence class of its own: if any state is locally equivalent to the zero state, then it must have been the zero state to begin with.
Third, we show that all nonzero product states are locally equivalent. Indeed, if states $\left(\begin{smallmatrix} a_1 \\ a_2 \\ b_1 \\ b_2 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} c_1 \\ c_2 \\ d_1 \\ d_2 \end{smallmatrix}\right)$ are nonzero, there exist invertible maps taking $\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ to $\begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$, and $\begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$ to $\begin{pmatrix} d_1 \\ d_2 \end{pmatrix}$.

Categories and Quantum Informatics exercise sheet 4: Dual objects

Exercise 3.1. Pick a basis $\{e_i\}$ for a finite-dimensional vector space V, and define $\mathbb{C} \xrightarrow{\eta} V \otimes V$ and $V \otimes V \xrightarrow{\varepsilon} \mathbb{C}$ by $\eta(1) = \sum_i e_i \otimes e_i$ and $\varepsilon(e_i \otimes e_i) = 1$, and $\varepsilon(e_i \otimes e_j) = 0$ when $i \neq j$.

(a) Show that this satisfies the snake equations, and hence that V is dual to itself in the category **FVect**.

(b) Show that f^* is given by the transpose of the matrix of the morphism $V \xrightarrow{f} V$ (where the matrix is written with respect to the basis $\{e_i\}$).

(c) Suppose that $\{e_i\}$ and $\{e'_i\}$ are both bases for V, giving rise to two units η, η' and two counits $\varepsilon, \varepsilon'$. Let $V \xrightarrow{f} V$ be the 'change-of-base' isomorphism $e_i \mapsto e'_i$. Show that $\eta = \eta'$ and $\varepsilon = \varepsilon'$ if and only if f is *(complex) orthogonal*, i.e. $f^{-1} = f^*$.

Exercise 3.2. Let $L \dashv R$ in **FVect**, with unit η and counit ε. Pick a basis $\{r_i\}$ for R.

(a) Show that there are unique $l_i \in L$ satisfying $\eta(1) = \sum_i r_i \otimes l_i$.

(b) Show that every $l \in L$ can be written as a linear combination of the l_i, and hence that the map $R \xrightarrow{f} L$, defined by $f(r_i) = l_i$, is surjective.

(c) Show that f is an isomorphism, and hence that $\{l_i\}$ must be a basis for L.

(d) Conclude that any duality $L \dashv R$ in **FVect** is of the following *standard form* for a basis $\{l_i\}$ of L and a basis $\{r_i\}$ of R:

$$\eta(1) = \sum_i r_i \otimes l_i, \qquad \varepsilon(l_i \otimes r_j) = \delta_{ij}. \tag{1}$$

Exercise 3.3. Let $L \dashv R$ be dagger dual objects in **FHilb**, with unit η and counit ε.

(a) Use the previous exercise to show that there are an orthonormal basis $\{r_i\}$ of R and a basis $\{l_i\}$ of L such that $\eta(1) = \sum_i r_i \otimes l_i$ and $\varepsilon(l_i \otimes r_j) = \delta_{ij}$.

(b) Show that $\varepsilon(l_i \otimes r_j) = \langle l_j | l_i \rangle$. Conclude that $\{l_i\}$ is also an orthonormal basis, and hence that every dagger duality $L \dashv R$ in **FHilb** has the standard form (1) for *orthonormal* bases $\{l_i\}$ of L and $\{r_i\}$ of R.

Exercise 3.4. Show that any duality $L \dashv R$ in **Rel** is of the following *standard form* for an isomorphism $R \xrightarrow{f} L$:

$$\eta = \{(\bullet, (r, f(r))) \mid r \in R\}, \qquad \varepsilon = \{((l, f^{-1}(l)), \bullet) \mid l \in L\}.$$

Conclude that specifying a duality $L \dashv R$ in **Rel** is the same as choosing an isomorphism $R \longrightarrow L$, and that dual objects in **Rel** are automatically dagger dual objects.

Exercise 3.5. A *terminal object* is an object 1 such that there is a unique morphism $A \longrightarrow 1$ for any object A. In a monoidal category with a terminal object, show that: if $L \dashv R$, then $R \otimes 1 \simeq 1 \simeq 1 \otimes L$.

Exercise 3.6. Show that the trace in **Rel** shows whether a relation has a fixed point.

Exercise 3.7. Let **C** be a compact dagger category.

(a) Show that $\mathrm{Tr}(f)$ is positive when $A \xrightarrow{f} A$ is a positive morphism.

(b) Show that f^* is positive when $A \xrightarrow{f} A$ is a positive morphism.

(c) Show that $\mathrm{Tr}_{A^*}(f^*) = \mathrm{Tr}_A(f)$ for any morphism $A \xrightarrow{f} A$.

(d) Show that $\mathrm{Tr}(g \circ f)$ is positive when $A \xrightarrow{f,g} A$ are positive morphisms.

Exercise 3.8. Show that if $L \dashv R$ are dagger dual objects, then $\dim(L)^\dagger = \dim(R)$.

Categories and Quantum Informatics exercise sheet 4: Dual objects

Exercise 3.1. (a) Evaluating the snake equation on each e_k gives

$$\begin{aligned}(\mathrm{id}_V \otimes \varepsilon) \circ (\eta \otimes \mathrm{id}_V)(e_k) &= (\mathrm{id}_V \otimes \varepsilon)(\sum_i e_i \otimes e_i \otimes e_k) \\ &= \sum_i e_i \otimes \varepsilon(e_i \otimes e_k) \\ &= e_k,\end{aligned}$$

so indeed $(\mathrm{id}_V \otimes \varepsilon) \circ (\eta \otimes \mathrm{id}_V) = \mathrm{id}_V$; the other snake equation is verified similarly.

(b) Let $(f_{i,j})$ be the matrix of f. So $e_i \xrightarrow{f} \sum_j f_{j,i} e_j$ and $e_i \xrightarrow{f^T} \sum_j f_{i,j} e_j$.
When we evaluate on each e_k we get

$$\begin{aligned}f^*(e_k) &= (\mathrm{id}_V \otimes \varepsilon) \circ (\mathrm{id}_V \otimes f \otimes \mathrm{id}_V) \circ (\eta \otimes \mathrm{id}_V)(e_k) \\ &= (\mathrm{id}_V \otimes \varepsilon) \circ (\mathrm{id}_V \otimes f \otimes \mathrm{id}_V)(\sum_i e_i \otimes e_i \otimes e_k) \\ &= \sum_i (\mathrm{id}_V \otimes \varepsilon)(e_i \otimes f(e_i) \otimes e_k) \\ &= \sum_{ij} e_i \otimes f_{ij} \varepsilon(e_j \otimes e_k) \\ &= \sum_i f_{ik} e_i \\ &= f^{\mathrm{T}}(e_k),\end{aligned}$$

and so $f^* = f^{\mathrm{T}}$.

(c) By Lemma 3.5 we may focus on $\eta = \eta'$ and forget about $\varepsilon = \varepsilon'$. Because $e'_i = \sum_j f_{ij} e_j$, we get

$$\eta'(1) = \sum_i e'_i \otimes e'_i = \sum_{i,j,k} f_{ij} f_{ik} e_j \otimes e_k.$$

This equals $\eta(1) = \sum_i e_i \otimes e_i$ precisely when $\sum_i f_{ij} f_{ik} = \delta_{jk}$ for all j, k. But this happens precisely when $f^{\mathrm{T}} \circ f = \mathrm{id}_V$, since

$$f^T \circ f = \begin{pmatrix} f_{1,1} & \cdots & f_{n,1} \\ \vdots & \ddots & \vdots \\ f_{1,n} & \cdots & f_{n,n} \end{pmatrix} \begin{pmatrix} f_{1,1} & \cdots & f_{1,n} \\ \vdots & \ddots & \vdots \\ f_{n,1} & \cdots & f_{n,n} \end{pmatrix} = \begin{pmatrix} \sum_i f_{i,1} f_{1,i} & \cdots & \sum_i f_{i,1} f_{i,n} \\ \vdots & \ddots & \vdots \\ \sum_i f_{i,n} f_{i,1} & \cdots & \sum_i f_{i,n} f_{i,n} \end{pmatrix}$$

Because f is invertible, this means $f^{\mathrm{T}} = f^{-1}$.

Exercise 3.2. Like any vector in $R \otimes L$, we can write $\eta(1)$ as $\sum_{j=1}^m z_j x_j \otimes y_j$ for $z_j \in \mathbb{C}$, $x_j \in R$, and $y_j \in L$, where m is some finite number. Developing each x_j on the basis $\{r_i\}$ and using bilinearity of the tensor product, we see that we can also write it as $\sum_{i=1}^n r_i \otimes l_i$ for $n = \dim(V)$ and $l_i \in L$. If we could also write it as $\sum_{i=1}^n r_i \otimes l'_i$, then we would have $0 = \sum_{i=1}^n r_i \otimes (l_i - l'_i)$. Because r_i forms a basis, it would follow that $l_i = l'_i$ for each i. Hence the l_i are unique.

(a) Use the snake equation:

$$\begin{aligned} l &= \mathrm{id}_L(l) \\ &= (\varepsilon \otimes \mathrm{id}_L) \circ (\mathrm{id}_L \otimes \eta)(l) \\ &= (\varepsilon \otimes \mathrm{id}_L)(\sum_i l \otimes r_i \otimes l_i) \\ &= \sum_i \varepsilon(l \otimes r_i) l_i. \end{aligned}$$

(b) Similarly, it follows from the snake equation that $r_i = \sum_k \varepsilon(l_k \otimes r_i) r_k$. Suppose that $l_i = l_j$. Because $\{r_k\}$ are linearly independent, then $\varepsilon(l_i \otimes r_i) = 1$, and $\varepsilon(l_k \otimes r_i) = 0$ for $k \neq i$. Hence $\varepsilon(l_j \otimes r_i) = 1$, and it follows that $i = j$, and so $r_i = r_j$. So f is injective.

(c) First notice that the standard form unit and counit indeed satisfy the snake equation. For the converse, combine the previous parts with **??**.

Exercise 3.3. (a) A Hilbert space is in particular a vector space. In the previous exercise, we may start by choosing $\{r_i\}$ to be orthonormal.

(b) First, compute that $\eta^\dagger(r_i \otimes l_j) = \langle l_i | l_j \rangle$:

$$\begin{aligned} \langle \eta(1) | r_i \otimes l_j \rangle &= \sum_k \langle r_k | r_i \rangle \langle l_k | l_j \rangle \\ &= \langle l_i | l_j \rangle \\ &= \langle 1 | \eta^\dagger (r_i \otimes l_j) \rangle. \end{aligned}$$

Hence dagger duality shows that $\varepsilon(l_i \otimes r_j) = \eta^\dagger \circ \sigma(l_i \otimes r_j) = \eta^\dagger(r_j \otimes l_i) = \langle l_j | l_i \rangle$. But part (a) shows that also $\varepsilon(l_i \otimes r_j) = \delta_{ij}$. Hence $\langle l_i | l_j \rangle = \delta_{ij}$, making $\{l_i\}$ orthonormal.

Exercise 3.4. First notice that the standard form indeed satisfies the snake equations.
Second, if η and ε witness $L \dashv R$, then for each $r \in R$ there exists $l \in L$ such that $(\bullet, (r, l)) \in \eta$ by one snake equation. But there can be at most one such l because of the other snake equation. Thus $f(r) = l$ defines an isomorphism $R \xrightarrow{f} L$ that makes η of the standard form. By **??**, also ε must be of the standard form.
Third, observe that if $f \neq f'$, then $\eta \neq \eta'$. Hence different choices of isomorphism $R \simeq L$ yield different (co)unit maps.
Finally, notice that any isomorphism is a unitary.

Exercise 3.5. We will prove that $L \otimes 0$ is the initial object; that is: for every object X, there exists a unique morphism $L \otimes 0 \to Z$. The isomorphism $L \otimes 0 \cong 0$ follows the from uniqueness of the initial object. The isomorphism $0 \dashv 0 \otimes R$ is done analogously.

Exercise 3.6. Let $X \xrightarrow{R} X$. Compute:

$$\begin{aligned} \mathrm{Tr}(R) &= \varepsilon \circ (R \otimes \mathrm{id}_X) \circ \sigma_{X,X} \circ \eta \\ &= \{((x,x), \bullet) \mid x \in X\} \circ (R \otimes \mathrm{id}_X) \circ \{((x,y),(y,x)) \mid x, y \in X\} \circ \{(\bullet, (x,x)) \mid x \in X\} \\ &= \{((x,x), \bullet) \mid x \in X\} \circ (R \otimes \mathrm{id}_X) \circ \{(\bullet, (x,x)) \mid x \in X\} \\ &= \{((x,x), \bullet) \mid x \in X\} \circ \{(\bullet, (y,x)) \mid (x,y) \in R\} \\ &= \{(\bullet, \bullet) \mid \exists x \in X \colon xRx\}. \end{aligned}$$

So $\mathrm{Tr}(R) = 1$ when R has a fixed point, and $\mathrm{Tr}(R) = 0$ otherwise.

Exercise 3.7. (a) Say $f = g^\dagger \circ g$ for $A \xrightarrow{g} B$. Now use dagger duality:

$$\begin{aligned}
\mathrm{Tr}_A(f) &= \varepsilon_A \circ (g^\dagger \otimes \mathrm{id}_{A^*}) \circ (g \otimes \mathrm{id}_{A^*}) \circ \sigma_{A^*,A} \circ \eta_A \\
&= \varepsilon_A \circ (g^\dagger \otimes \mathrm{id}_{A^*}) \circ \sigma_{A^*,B} \circ (\mathrm{id}_{A^*} \otimes g) \circ \eta_A \\
&= \eta_A^\dagger \circ \sigma_{A,A^*} \circ (g^\dagger \otimes \mathrm{id}_{A^*}) \circ \sigma_{A^*,B} \circ (\mathrm{id}_{A^*} \otimes g) \circ \eta_A \\
&= \eta_A^\dagger \circ (\mathrm{id}_{A^*} \otimes g^\dagger) \circ (\mathrm{id}_{A^*} \otimes g) \circ \eta_A.
\end{aligned}$$

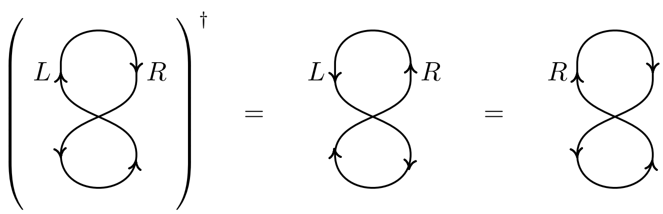
(b) If $f = g^\dagger \circ g$, then $f^* = g^* \circ (g^\dagger)^* = (g^*) \circ (g^*)^\dagger$.
(c)

$$\begin{aligned}
\mathrm{Tr}_{A^*}(f^*) &= \varepsilon_{A^*} \circ (f^* \otimes \mathrm{id}_A) \circ \sigma_{A,A^*} \circ \eta_{A^*} \\
&= \varepsilon_{A^*} \circ (\mathrm{id}_{A^*} \otimes f) \circ \sigma_{A,A^*} \circ \eta_{A^*} \\
&= \varepsilon_A \circ \sigma_{A,A^*} \circ (\mathrm{id}_{A^*} \otimes f) \otimes \sigma_{A,A^*} \circ \sigma_{A^*,A} \circ \eta_A \\
&= \mathrm{Tr}_A(f).
\end{aligned}$$

(d) This is graphically immediately clear.
(e) Suppose $f = a^\dagger \circ a$ and $g = b^\dagger \circ b$; use the cyclic property to see $\mathrm{Tr}(g \circ f) = \mathrm{Tr}((b^\dagger \circ a)^\dagger \circ (b^\dagger \circ a))$, and then use part (a) to see that this scalar is positive.

Exercise 3.8. Graphically:

$\dim(L)^\dagger =$



$= \dim(R).$

Categories and Quantum Informatics exercise sheet 5: Monoids and comonoids

Exercise 4.1. Let (A, d, e) be a comonoid in a monoidal category. Show that a comonoid homomorphism $I \xrightarrow{a} A$ is a copyable state. Conversely, show that if a state $I \xrightarrow{a} A$ is copyable and satisfies $e \circ a = \mathrm{id}_I$, then it is a comonoid homomorphism.

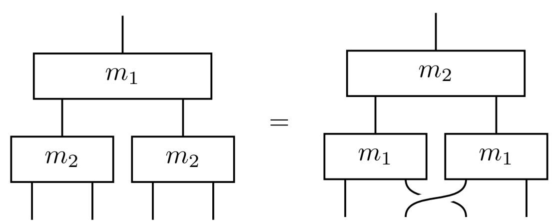
Exercise 4.2. This exercise is about *property* versus *structure*; the latter is something you have to choose, the former is something that exists uniquely (if at all).

(a) Show that if a monoid (A, m, u) in a monoidal category has a map $I \xrightarrow{u'} A$ satisfying $m \circ (\mathrm{id}_A \otimes u') = \rho_A$ and $\lambda_A = m \circ (u' \otimes \mathrm{id}_A)$, then $u' = u$. Conclude that unitality is a property.

(b) Show that in categories with binary products and a terminal object, every object has a unique comonoid structure under the monoidal structure induced by the categorical product.

(c) If $(\mathbf{C}, \otimes, I)$ is a symmetric monoidal category, denote by $\mathbf{cMon}(\mathbf{C})$ the category of commutative monoids in $\mathbf{C}$ with monoid homomorphisms as morphisms. Show that the forgetful functor $\mathbf{cMon}(\mathbf{C}) \longrightarrow \mathbf{C}$ is an isomorphism of categories if and only if $\otimes$ is a coproduct and I is an initial object.

Exercise 4.3. This exercise is about the *Eckmann–Hilton argument*, concerning interacting monoid structures on a single object in a braided monoidal category. Suppose you have morphisms $A \otimes A \xrightarrow{m_1, m_2} A$ and $I \xrightarrow{u_1, u_2} A$, such that (A, m_1, u_1) and (A, m_2, u_2) are both monoids, and the following diagram commutes:



(a) Show that $u_1 = u_2$.

(b) Show that $m_1 = m_2$.

(c) Show that m_1 is commutative.

Categories and Quantum Informatics exercise sheet 5: Monoids and comonoids

Exercise 4.1. The comonoid structure on I is given by $(I, \lambda_I^{-1}, \mathrm{id}_I)$. The definition of copyability and the first part of the definition of comonoid homomorphism are both described by the same equation in this case, namely:

$$d \circ a = (a \otimes a) \circ \lambda_I^{-1}$$

This means that a state a is copyable iff a satisfies the first equation in the definition of comonoid homomorphism. Note that in general, a copyable state a does not satisfy the other condition, namely deletion. A counter example is taking a zero state.

Exercise 4.2. (a) The graphical proof for this part is very simple (simply plug in both u and u' into m), but we present a symbolic one for comparisson.
Observe that the following equation holds because of naturality of ρ:

$$\rho_A \circ (u \otimes id_I) = u \circ \rho_I$$

Since $\lambda_I = \rho_I$, we have:

$$\rho_A \circ (u \otimes id_I) = u \circ \rho_I = u \circ \lambda_I$$

Using the same argument, but for λ and u' we get:

$$\lambda_A \circ (id_I \otimes u') = u' \circ \lambda_I = u' \circ \rho_I$$

We have:

$$\begin{aligned}
& m \circ (id_A \otimes u') = \rho_A \\
\implies\ & m \circ (id_A \otimes u') \circ (u \otimes id_I) = \rho_A \circ (u \otimes id_I) && \text{(compose on right)} \\
\implies\ & m \circ (id_A \otimes u') \circ (u \otimes id_I) = u \circ \lambda_I && \text{(above equation)} \\
\implies\ & m \circ (u \otimes u') = u \circ \lambda_I && \text{(interchange law)} \\
\implies\ & m \circ (u \otimes id_A) \circ (id_I \otimes u') = u \circ \lambda_I && \text{(interchange law)} \\
\implies\ & \lambda_A \circ (id_I \otimes u') = u \circ \lambda_I && \text{(monoid axiom)} \\
\implies\ & u' \circ \lambda_I = u \circ \lambda_I && \text{(above equation)} \\
\implies\ & u' = u && (\lambda_I \text{ is invertible})
\end{aligned}$$

Note, that we have used only one of the equations for u'.

(b) We will write the product of $f : X \longrightarrow A$ and $g : X \longrightarrow B$ as $\langle f, g \rangle : X \longrightarrow A \times B$ and the associated projections will be written as $\pi_1^{A \times B}$ and $\pi_2^{A \times B}$.
Recall, that

$$\pi_1^{A\times B} \circ \langle f, g \rangle = f$$
$$\pi_2^{A\times B} \circ \langle f, g \rangle = g$$

$$\langle f, g\rangle \circ h = \langle f \circ h, g \circ h\rangle$$

First, we need to express the monoidal structure induced by the product. It is given in the following way:
For objects, A and B

$$A \otimes B := A \times B$$

For morphisms $f : A \longrightarrow B$ and $g : C \longrightarrow D$

$$f \otimes g := \langle f \circ \pi_1^{A\times C}, g \circ \pi_2^{A\times C}\rangle$$

The monoidal unit I is the terminal object 1 of the category. Then,

$$\lambda_A := \pi_2^{1\times A}$$

$$\rho_A := \pi_1^{A\times 1}$$

$$\alpha_{A,B,C} := \langle \pi_1^{A\times B} \circ \pi_1^{(A\times B)\times C}, \langle \pi_2^{A\times B} \circ \pi_1^{(A\times B)\times C}, \pi_2^{(A\times B)\times C}\rangle\rangle$$

Next, we need to show that every object in the category has a comonoid structure. Let A be an arbitrary object. We can assign it a comonoid structure (A, d, e) by defining:

$$d := \langle id_A, id_A\rangle : A \longrightarrow A \times A$$

$$e := 1_A : A \longrightarrow 1$$

where 1_A is the unique morphism going from A to the terminal object 1. We have to verify that the axioms for a comonoid are satisfied.

$$\begin{aligned}
\rho_A \circ (id_A \otimes e) \circ d &= \pi_1^{A\times 1} \circ \langle id_A \circ \pi_1^{A\times A}, 1_A \circ \pi_2^{A\times A}\rangle \circ \langle id_A, id_A\rangle \\
&= id_A \circ \pi_1^{A\times A} \circ \langle id_A, id_A\rangle \\
&= id_A
\end{aligned}$$

as required. Next,

$$\begin{aligned}
\lambda_A \circ (e \otimes id_A) \circ d &= \pi_2^{1\times A} \circ \langle 1_A \circ \pi_1^{A\times A}, id_A \circ \pi_2^{A\times A}\rangle \circ \langle id_A, id_A\rangle \\
&= id_A \circ \pi_2^{A\times A} \circ \langle id_A, id_A\rangle \\
&= id_A
\end{aligned}$$

as required. Next, we show coassociativity:

$$\begin{aligned}
\alpha_{A,A,A} \circ (d \otimes id_A) \circ d &= \alpha_{A,A,A} \circ \langle d \circ \pi_1^{A\times A}, id_A \circ \pi_2^{A\times A}\rangle \circ d \\
&= \alpha_{A,A,A} \circ \langle d \circ \pi_1^{A\times A} \circ d, \pi_2^{A\times A} \circ d\rangle \\
&= \alpha_{A,A,A} \circ \langle d \circ id_A, id_A\rangle \\
&= \langle \pi_1^{A\times A} \circ \pi_1^{(A\times A)\times A}, \langle \pi_2^{A\times A} \circ \pi_1^{(A\times A)\times A}, \pi_2^{(A\times A)\times A}\rangle\rangle \circ \langle d, id_A\rangle \\
&= \langle \pi_1^{A\times A} \circ \pi_1^{(A\times A)\times A} \circ \langle d, id_A\rangle, \langle \pi_2^{A\times A} \circ \pi_1^{(A\times A)\times A}, \pi_2^{(A\times A)\times A}\rangle \circ \langle d, id_A\rangle\rangle \\
&= \langle \pi_1^{A\times A} \circ d, \langle \pi_2^{A\times A} \circ \pi_1^{(A\times A)\times A} \circ \langle d, id_A\rangle, \pi_2^{(A\times A)\times A} \circ \langle d, id_A\rangle\rangle\rangle \\
&= \langle id_A, \langle \pi_2^{A\times A} \circ d, id_A\rangle\rangle \\
&= \langle id_A, \langle id_A, id_A\rangle\rangle
\end{aligned}$$

Also,

$$\begin{aligned}(id_A \otimes d) \circ d &= \langle id_A \circ \pi_1^{A\times A}, d \circ \pi_2^{A\times A}\rangle \circ d \\ &= \langle \pi_1^{A\times A} \circ d, d \circ \pi_2^{A\times A} \circ d\rangle \\ &= \langle id_A, d \circ id_A\rangle \\ &= \langle id_A, d\rangle \\ &= \langle id_A, \langle id_A, id_A\rangle\rangle\end{aligned}$$

Therefore, coassociativity holds and (A, d, e) is indeed a comonoid.
Next, we have to show that the construction is unique. That is, for any other comonoid (A, d', e') that $d = d'$ and $e = e'$.
Since 1 is a terminal object, then it must be the case that $e = e' : A \longrightarrow 1$. From counitlaity of $(A, d', e' = e)$ we have:

$$\begin{aligned}id_A &= \rho_A \circ (id_A \otimes e) \circ d' \\ &= \pi_1^{A\times 1} \circ \langle id_A \circ \pi_1^{A\times A}, 1_A \circ \pi_2^{A\times A}\rangle \circ d' \\ &= id_A \circ \pi_1^{A\times A} \circ d' \\ &= \pi_1^{A\times A} \circ d'\end{aligned}$$

and also,

$$\begin{aligned}id_A &= \lambda_A \circ (e \otimes id_A) \circ d' \\ &= \pi_2^{1\times A} \circ \langle 1_A \circ \pi_1^{A\times A}, id_A \circ \pi_2^{A\times A}\rangle \circ d' \\ &= id_A \circ \pi_2^{A\times A} \circ d' \\ &= \pi_2^{A\times A} \circ d'\end{aligned}$$

Because of these two equalities and from the universal property of categorical products, it then follows that d' must be the unique morphism

$$d' = \langle id_A, id_A\rangle = d$$

which completes the proof.

(c) **RHS $\Rightarrow$ LHS:** Since $\otimes$ is a coproduct, we can simply use the dualized statement of (b) to conclude that every object A has a unique monoid structure (A, m_A, u_A).
First, note that the tensor product on two morphisms $f : A \longrightarrow B$ and $g : C \longrightarrow D$ is given by:

$$f \otimes g := \left[i_1^{B\oplus D} \circ f, i_2^{B\oplus D} \circ g\right] : A \oplus C \longrightarrow B \oplus D$$

and braiding is given by:

$$\sigma_{A,B} := [i_2^{B\oplus A}, i_1^{B\oplus A}] : A \oplus B \longrightarrow B \oplus A$$

The monoidal structure on A is defined by:

$$m_A := [id_A, id_A] : A \oplus A \longrightarrow A$$

$$u_A := 1_A : I \to A$$

where 1_A is unique morphism from the initial object to A. Also, recall that:

$$\begin{aligned}
[f,g] \circ i_1^{B \oplus D} &= f \\
[f,g] \circ i_2^{B \oplus D} &= g \\
h \circ [f,g] &= [h \circ f, h \circ g]
\end{aligned}$$

We show that every monoid (A, m_A, u_A) is commutative:

$$\begin{aligned}
m_A \circ \sigma_{A,A} &= [id_A, id_A] \circ [i_2^{B \oplus A}, i_1^{B \oplus A}] && \text{(definition)} \\
&= [[id_A, id_A] \circ i_2^{B \oplus A}, [id_A, id_A] \circ i_1^{B \oplus A}] && \text{(coproduct)} \\
&= [id_A, id_A] && \text{(coproduct)} \\
&= m_A && \text{(definition)}
\end{aligned}$$

We can definie an isomorphism $F : \mathbf{C} \to \mathbf{cMon(C)}$ in the following way:

$$\begin{aligned}
F(A) &:= (A, m_A, u_A) \\
F(f) &:= f
\end{aligned}$$

It's clear that this functor is an isomorphism, if it is well-defined. We have already shown it is well-defined on objects. We just have to show that every morphism in $\mathbf{C}$ is a monoid homomorphism. Let $f : A \to B$ be an arbitrary morphism. Now, consider the monoidal structures of the two objects (A, m_A, u_A), (B, m_B, u_B). We have:

$$\begin{gathered}
u_B = f \circ u_A \\
\iff \\
1_B = f \circ 1_A
\end{gathered}$$

which is clearly true, since $I = 1$ is an initial object.

$$\begin{aligned}
& f \circ m_A = m_B \circ (f \otimes f) \\
\iff & f \circ [id_A, id_A] = [id_B, id_B] \circ [i_1^{B \oplus B} \circ f, i_2^{B \oplus D} \circ f] \\
\iff & [f, f] = [[id_B, id_B] \circ i_1^{B \oplus B} \circ f, [id_B, id_B] \circ i_2^{B \oplus D} \circ f] \\
\iff & [f, f] = [id_B \circ f, id_B \circ f] \\
\iff & [f, f] = [f, f]
\end{aligned}$$

Therefore, f is a monoid homomorphism and thus F is an isomorphism. Showing that the functor F is a monoidal functor is straightforward with all of the definitions we have provided.

LHS $\Rightarrow$ RHS: cMon(C) is monoidally isomorphic to $\mathbf{C}$ therefore every object A has a unique monoid structure which we will denote as (A, m_A, u_A). Consider objects A, B, C and $A \otimes B$ and morphisms $f_1 : A \to C$, $f_2 : B \to C$. Since the categories are isomorphic, this implies that f_1 and f_2 are monoid homomorphisms.

First, we define morphisms $i_1^{A \otimes B} : A \to A \otimes B$, $i_2^{A \otimes B} : B \to A \otimes B$ given by:

$$i_1 := (id_A \otimes u_B) \circ \rho_A^{-1}$$

$$i_2 := (u_A \otimes id_B) \circ \lambda_B^{-1}$$

Define,

$$[f_1, f_2] := m_C \circ (f_1 \otimes f_2)$$

We claim that $([f_1, f_2], i_1, i_2)$ is the coproduct of the morphisms f_1 and f_2. First, we verify:

$$\begin{aligned}
[f_1, f_2] \circ i_1 &= m_C \circ (f_1 \otimes f_2) \circ (id_A \otimes u_B) \circ \rho_A^{-1} && \text{(definition)} \\
&= m_C \circ (f_1 \otimes (f_2 \circ u_B)) \circ \rho_A^{-1} && \text{(interchange)} \\
&= m_C \circ (f_1 \otimes u_C) \circ \rho_A^{-1} && \text{(monoid homomorphism)} \\
&= m_C \circ (id_C \otimes u_C) \circ (f_1 \otimes id_I) \circ \rho_A^{-1} && \text{(interchange)} \\
&= \rho_C \circ (f_1 \otimes id_I) \circ \rho_A^{-1} && \text{(monoid unitality for C)} \\
&= f_1 \circ \rho_A \circ \rho_A^{-1} && \text{(naturality of } \rho\text{)} \\
&= f_1
\end{aligned}$$

In a similar way, we can show that

$$[f_1, f_2] \circ i_2 = f_2$$

Finally, we have to show that the construction is universal. That is, if there exists a morphism $h : A \otimes B \longrightarrow C$ with $h \circ i_1 = f_1$ and $h \circ i_2 = f_2$ then $h = [f_1, f_2]$.
Consider:

$$\begin{aligned}
[f_1, f_2] &= m_C \circ (f_1 \otimes f_2) && \text{(definition)} \\
&= m_C \circ ((h \circ i_1) \otimes (h_2 \circ i_2)) && \text{(assumption)} \\
&= m_C \circ (h \otimes h) \circ (i_1 \otimes i_2) && \text{(interchange)} \\
&= h \circ m_{A \otimes B} \circ (i_1 \otimes i_2) && (h - \text{homomorphism}) \\
&= h \circ (m_A \otimes m_B) \circ (id_A \circ \sigma_{B,A} \circ id_B) \circ \\
&\circ (id_A \otimes u_B \otimes u_A \otimes id_B) \circ (\rho_A^{-1} \otimes \lambda_B^{-1}) && \text{(def+interchange)} \\
&= h \circ (m_A \otimes m_B) \circ (id_A \circ u_A \circ u_B \circ id_B) \circ (\rho_A^{-1} \otimes \lambda_B^{-1}) && \text{(interchange)} \\
&= h \circ (\rho_A \otimes \lambda_B) \circ (\rho_A^{-1} \otimes \lambda_B^{-1}) && \text{(unitality} \times 2\text{)} \\
&= h && \text{(interchange)}
\end{aligned}$$

We have shown that coproducts exist for any pair of objects A and B. However, we still need to show that there is an initial object. The initial object is, of course, the tensor unit I. Consider an arbitrary object A. Since A is a monoid, then there must be a map $u_A : I \longrightarrow A$. Moreover, if there is another morphism $x : I \longrightarrow A$, then it must be a monoid homomorphism. Therefore,

$$u_A = x \circ u_I = x \circ id_I = x$$

since (I, λ_I, id_I) is the unique monoid on I.
Therefore, I is an initial object, which completes the proof.

Exercise 4.3. For the whole exercise, the graphical proof is very simple and straightforward. However, for comparisson, we show a symbolic solution instead.

(a) The trick is to plug in the state $(u_2 \otimes u_1 \otimes u_1 \otimes u_2)$.

$$
\begin{aligned}
m_1 \circ (m_2 \otimes m_2) \circ (u_2 \otimes u_1 \otimes u_1 \otimes u_2) &= m_2 \circ (m_1 \otimes m_1) \circ (id_A \circ \sigma \circ id_A) \circ (u_2 \otimes u_1 \otimes u_1 \otimes u_2) \\
&\Longrightarrow \\
m_1 \circ (\lambda_A \circ (id_I \otimes u_1)) \otimes (\rho_A \circ (u_1 \otimes id_I)) &= m_2 \circ (m_1 \otimes m_1) \circ (u_2 \otimes u_1 \otimes u_1 \otimes u_2) \\
&\Longrightarrow \\
m_1 \circ ((u_1 \circ \lambda_I) \otimes (u_1 \circ \rho_I)) &= m_2 \circ ((\rho_A \circ (u_2 \otimes id_I)) \otimes (\lambda_A \circ (id_I \otimes u_2))) \\
&\Longrightarrow \\
m_1 \circ (u_1 \otimes u_1) \circ (\lambda_I \otimes \rho_I)) &= m_2 \circ ((u_2 \circ \rho_I) \otimes (u_2 \circ \lambda_I)) \\
&\Longrightarrow \\
\lambda_A \circ (id_I \otimes u_1) \circ (\lambda_I \otimes \rho_I)) &= m_2 \circ (u_2 \otimes u_2) \circ (\rho_I \otimes \lambda_I) \\
&\Longrightarrow \\
\lambda_A \circ (id_I \otimes u_1) &= m_2 \circ (u_2 \otimes u_2) \\
&\Longrightarrow \\
\lambda_A \circ (id_I \otimes u_1) &= \lambda_A \circ (id_I \otimes u_2) \\
&\Longrightarrow \\
u_1 \circ \lambda_I &= u_2 \circ \lambda_I \\
&\Longrightarrow \\
u_1 &= u_2
\end{aligned}
$$

(b) From now on we will write $u := u_1 = u_2$.
Plugging in the map $(id_A \otimes u \otimes u \otimes id_A)$ to both sides of the equation yields the desired result.

$$
\begin{aligned}
m_1 \circ (m_2 \otimes m_2) \circ (id_A \otimes u \otimes u \otimes id_A) &= m_2 \circ (m_1 \otimes m_1) \circ (id_A \circ \sigma \circ id_A) \circ (id_A \otimes u \otimes u \otimes id_A) \\
&\Longrightarrow \\
m_1 \circ (m_2 \otimes m_2) \circ (id_A \otimes u \otimes u \otimes id_A) &= m_2 \circ (m_1 \otimes m_1) \circ (id_A \otimes u \otimes u \otimes id_A) \\
&\Longrightarrow \\
m_1 \circ (\rho_A \otimes \lambda_A) &= m_2 \circ (\rho_A \otimes \lambda_A) \\
&\Longrightarrow \\
m_1 &= m_2
\end{aligned}
$$

(c) We will write $m := m_1 = m_2$.
This time, the trick is to plug in the map $(u \otimes id_A \otimes id_A \otimes u)$ to both sides of the equation. We get:

$$
\begin{aligned}
m \circ (m \otimes m) \circ (u \otimes id_A \otimes id_A \otimes u) &= m \circ (m \otimes m) \circ (id_A \circ \sigma \circ id_A) \circ (u \otimes id_A \otimes id_A \otimes u) \\
&\Longrightarrow \\
m \circ (\lambda_A \otimes \rho_A) &= m \circ (m \otimes m) \circ (u \otimes id_A \otimes id_A \otimes u) \circ (id_I \circ \sigma \circ id_I) \\
&\Longrightarrow \\
m \circ (\lambda_A \otimes \rho_A) &= m \circ (\lambda_A \otimes \rho_A) \circ (id_I \circ \sigma \circ id_I) \\
&\Longrightarrow \\
m \circ (\lambda_A \otimes \rho_A) &= m \circ \sigma \circ (\lambda_A \otimes \rho_A) \\
&\Longrightarrow \\
m &= m \circ \sigma
\end{aligned}
$$

Categories and Quantum Informatics exercise sheet 6: Frobenius structures

Exercise 5.1. Recall that in a braided monoidal category, the tensor product of monoids is again a monoid.

(a) Show that, in a braided monoidal category, the tensor product of Frobenius structures is again a Frobenius structure.
(b) Show that, in a symmetric monoidal category, the tensor product of symmetric Frobenius structures is again a symmetric Frobenius structure.
(c) Show that, in a symmetric monoidal dagger category, the tensor product of classical structures is again a classical structure.

Exercise 5.2. This exercise is about the interdependencies of the defining properties of Frobenius structures in a braided monoidal dagger categories. Recall the Frobenius law (5.1).

(a) Show that for any maps $A \xrightarrow{d} A \otimes A$ and $A \otimes A \xrightarrow{m} A$, speciality ($m \circ d = \mathrm{id}$) and equation (5.4) together imply associativity for m.
(b) Suppose $A \xrightarrow{d} A \otimes A$ and $A \otimes A \xrightarrow{m} A$ satisfy equation (5.4), speciality, and commutativity (4.7). Given a dual object $A \dashv A^*$, construct a map $I \xrightarrow{u} A$ such that unitality (4.6) holds.

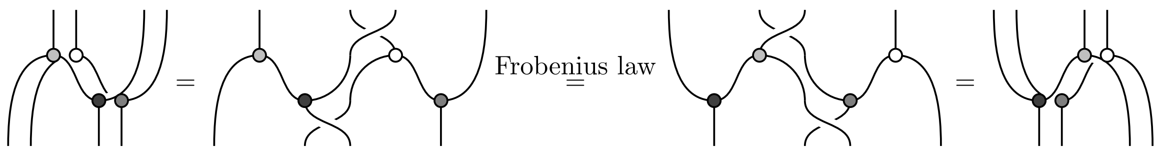
Exercise 5.3. Recall that a set $\{x_0, \ldots, x_n\}$ of vectors in a vector space is *linearly independent* when $\sum_{i=0}^{n} z_i x_i = 0$ for $z_i \in \mathbb{C}$ implies $z_0 = \ldots = z_n = 0$. Show that the nonzero copyable states of a comonoid in **FHilb** are linearly independent. (Hint: consider a minimal linearly dependent set.)

Exercise 5.4. This exercise is about the phase group of a Frobenius structure in **Rel** induced by a groupoid.

(a) Show that a phase of **G** corresponds to a subset of the arrows of **G** that contains exactly one arrow out of each object and exactly one arrow into each object.
(b) A *cycle* in a category is a series of morphisms $A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} A_3 \cdots A_n \xrightarrow{f_n} A_1$. For finite **G**, show that a phase corresponds to a union of cycles that cover all objects of **G**. Find a phase on the indiscrete category on $\mathbb{Z}$ that is not a union of cycles.
(c) A groupoid is *totally disconnected* when all morphisms are endomorphisms. Show that for such groupoids **G**, the phase group is **G** itself, regarded as a group: $\prod_{x \in \mathrm{Ob}(\mathbf{G})} \mathbf{G}(x, x)$. Conclude that this holds in particular for classical structures.

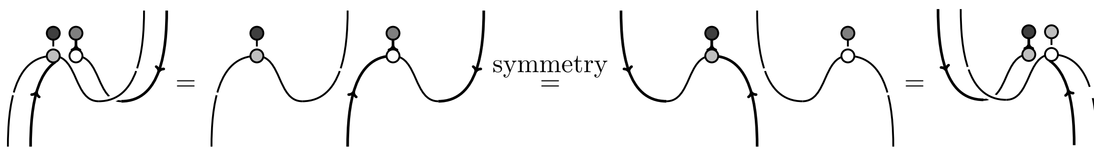
Categories and Quantum Informatics exercise sheet 6: Frobenius structures

Exercise 5.1. (a) We have seen before that the tensor product of a monoid is again a monoid. The same holds for comonoids. It is left to verify the Frobenius law:



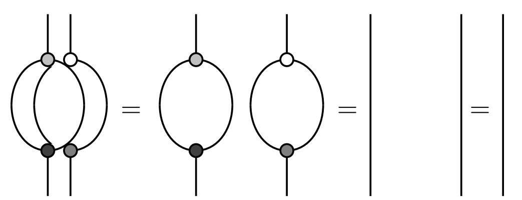
(1)

(b) We will use the fact that the tensor product $A \otimes B$ of two spaces A, B that have duals A^*, B^*, is dual to the tensor product $A^* \otimes B^*$. We use the alternative definition of symmetric Frobenius algebras in symmetric monoidal categories; however, it can also be shown directly.



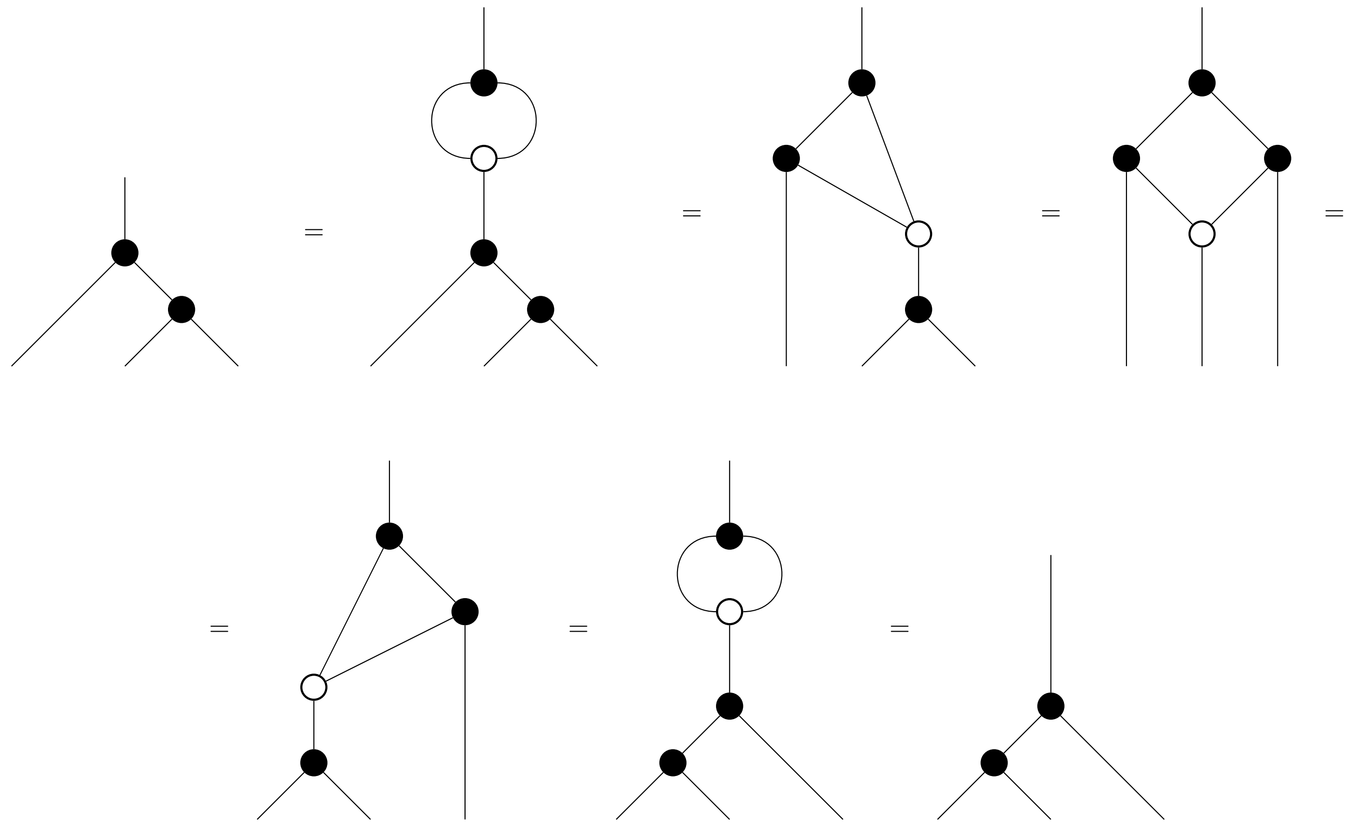
(2)

(c) The tensor product of commutative frobenius structures is again a commutative frobenius structure by (a) and an argument similar to (b). It is left to show that the tensor product of special dagger Frobenius algebras is special.

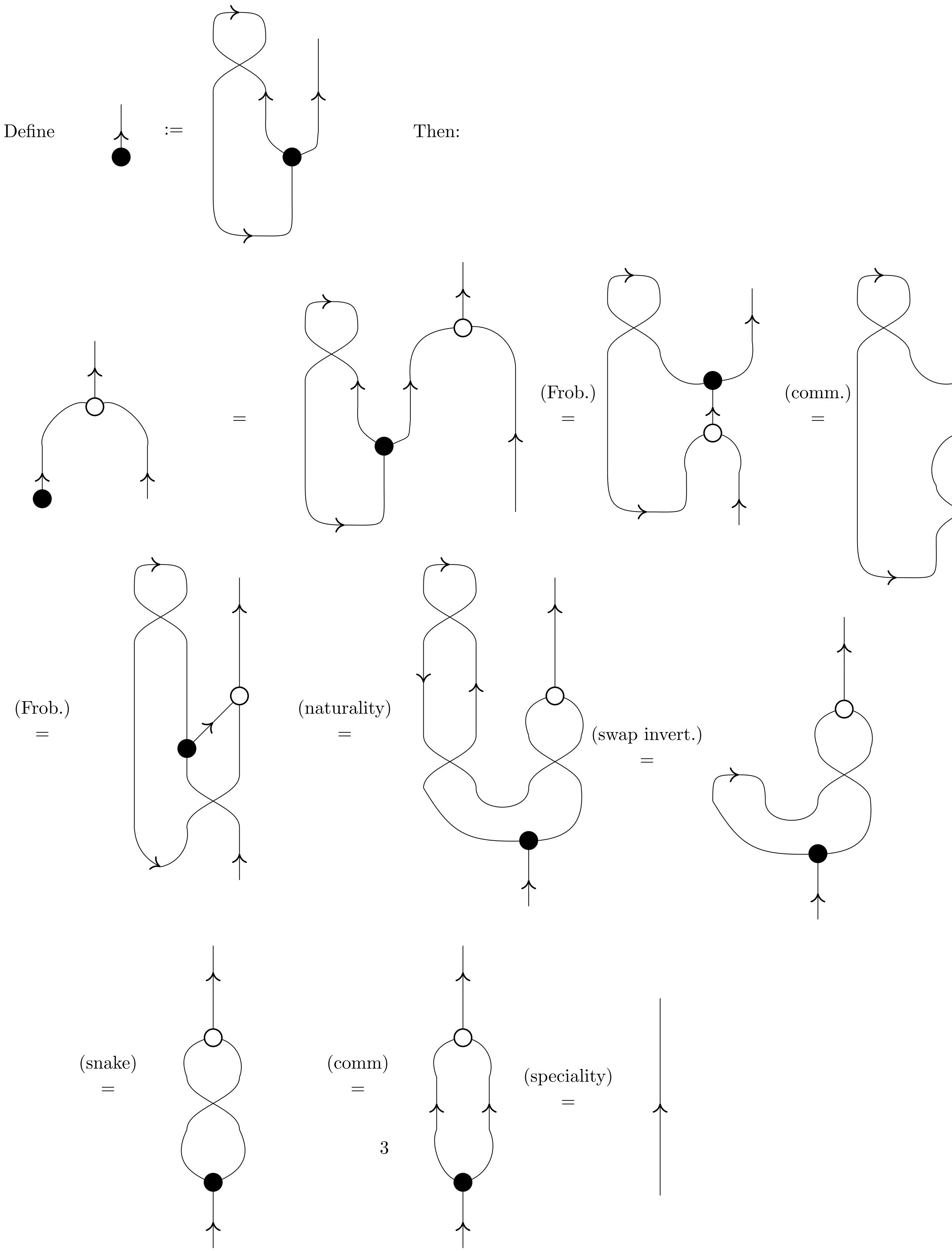


(3)

Exercise 5.2. (a)



(b)


Define
:=
Then:
=
(Frob.)
=
(comm.)
=
(Frob.)
=
(naturality)
=
(swap invert.)
=
(snake)
=
(comm)
=
(speciality)
=

Exercise 5.3. Suppose $\{x_0, \ldots, x_n\}$ is a minimal nonempty linearly dependent set of nonzero copyable states. Then $x_0 = \sum_{i=1}^n z_i x_i$ for suitable coefficients $z_i \in \mathbb{C}$. So

$$\begin{aligned}\sum_{i=1}^n z_i(x_i \otimes x_i) &= \sum_{i=1}^n z_i d(x_i) \\ &= d(x_0) \\ &= (\sum_{i=1}^n z_i x_i) \otimes (\sum_{j=1}^n z_j x_j) \\ &= \sum_{i,j=1}^n z_i z_j (x_i \otimes x_j).\end{aligned}$$

By minimality, $\{x_1, \ldots, x_n\}$ is linearly independent. Hence $z_i^2 = z_i$ for all i, and $z_i z_j = 0$ for $i \neq j$. So $z_i = 0$ or $z_i = 1$ for all i. If $z_j = 1$, then $z_i = 0$ for all $i \neq j$, so $x_0 = x_j$. By minimality, then $j = 1$ and $\{x_0, x_j\} = \{x_0\}$, which is impossible. So we must have $z_i = 0$ for all i. But then $x_0 = 0$, which is likewise a contradiction.

Exercise 5.4. (a) The defining equation for phases gives

$$\{g^{-1} \circ h \mid g, h \in a\} = \{\mathrm{id}_x \mid x \in \mathrm{Ob}(\mathbf{G})\}\{g \circ h^{-1} \mid g, h \in a\}.$$

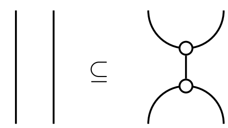
The inclusion $L \subseteq M$ means: $\forall g, h \in a\colon \mathrm{cod}(g) = \mathrm{cod}(h) \implies g = h$. The inclusion $M \supseteq R$ means: $\forall g, h \in a\colon \mathrm{dom}(g) = \mathrm{dom}(h) \implies g = h$. In other words: there can be at most one arrow in a out of each object of $\mathbf{G}$, and at most one arrow of a into each object of $\mathbf{G}$. Given this, the remaining inclusions $L \supseteq M \subseteq R$ mean: $\forall x \in \mathrm{Ob}(\mathbf{G}) \exists g, h \in a\colon \mathrm{dom}(g) = x = \mathrm{cod}(h)$. That is: a contains arrows into and out of each object.

(b) Pick an object x; the phase a contains exactly one arrow $x \to y$. If $y = x$, we have a 1-cycle. Otherwise, a contains exactly one arrow $y \to z$, etc. This process has to end, because the groupoid is finite. Delete all the objects involved in the cycle, and repeat.
For the indiscrete groupoid on $\mathbb{Z}$, there is a phase $\{n \xrightarrow{!} n+1 \mid n \in \mathbb{Z}\}$

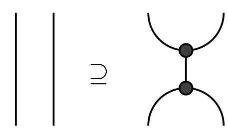
Categories and Quantum Informatics exercise sheet 7: Complementarity

Exercise 5.1. Let $(G, \circ)$ and $(G, \bullet)$ be two complementary groupoids (see Proposition 6.9).

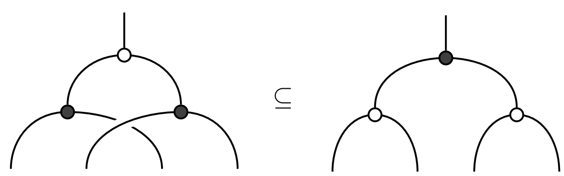
(a) Assume that $(G, \circ)$ is a group. Show that:



(b) Assume that $(G, \circ)$ is a group. Show that:



(c) Assume that $(G, \circ)$ is a group and that the corresponding Frobenius structures in **Rel** form a bialgebra. Show that:



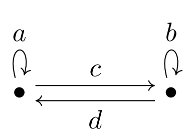
Exercise 5.2. Let A be a set with a prime number of elements. Show that pairs of complementary Frobenius structures on A in **Rel** correspond to groups whose underlying set is A.

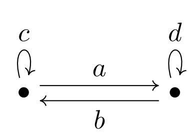
Exercise 5.3. Consider a special dagger Frobenius structure in **Rel** corresponding to a groupoid $\mathbf{G}$.

(a) Show that nonzero copyable states correspond to endohomsets $\mathbf{G}(A, A)$ of $\mathbf{G}$ that are isolated in the sense that $\mathbf{G}(A, B) = \emptyset$ for each object B in $\mathbf{G}$ different from A.

(b) Show that unbiased states of $\mathbf{G}$ correspond to sets containing exactly one morphism into each object of $\mathbf{G}$ and exactly one morphism out of each object of $\mathbf{G}$.

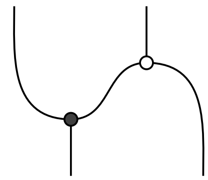
(c) Consider the following two groupoids on the morphism set $\{a, b, c, d\}$.





Show that copyable states for one are unbiased for the other, but that they are not complementary. Conclude that the converse of Proposition 6.11 is false.

Exercise 5.4. A *Latin square* is an n-by-n matrix L with entries from $\{1, \dots, n\}$, with each $i = 1, \dots, n$ appearing exactly once in each row and each column. Choose an orthonormal basis $\{e_1, \dots, e_n\}$ for $\mathbb{C}^n$. Define : $\mathbb{C}^n \to \mathbb{C}^n \otimes \mathbb{C}^n$ by $e_i \mapsto e_i \otimes e_i$, and : $\mathbb{C}^n \otimes \mathbb{C}^n \to \mathbb{C}^n$ by $e_i \otimes e_j \mapsto e_{L_{ij}}$. Show that the composite



is unitary. Note that  need not be associative or unital.

Exercise 5.5. This exercise is about *property* versus *structure*. Suppose that a category **C** has products. Show that any monoid in **C** has a unique bialgebra structure.

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:

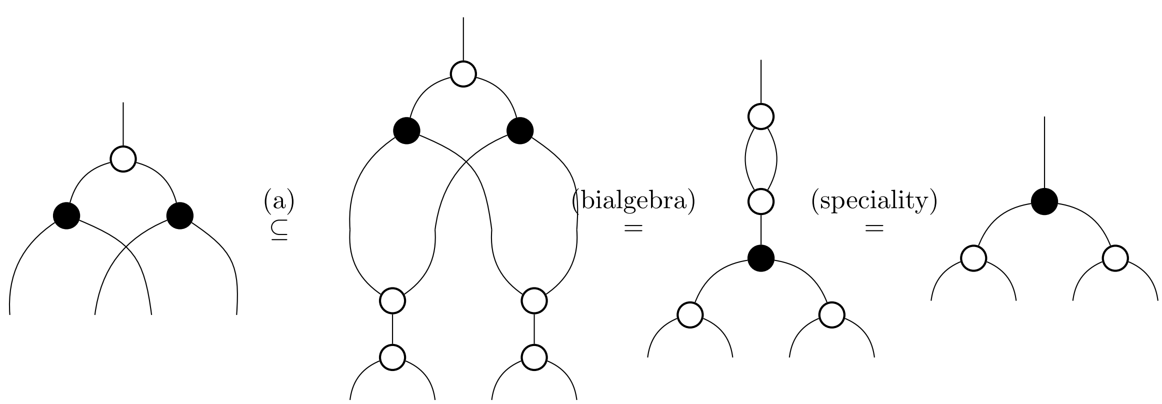
$$\begin{aligned} Arr(G_1) &\to Ob(G_1) \times Ob(G_2) \\ a &\mapsto (dom_1(a), dom_2(a)) \end{aligned}$$

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:

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

From basic set theory, we get that this means:

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

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 $f \in U$.
$f \in U \implies f \circ f \in U \implies dom(f) = cod(f) = A$, for some object $A \in Ob(G)$. In other words, f must be a self-loop (or endomorphism).
If $g \in U \implies f \circ g \in U$ and $g \circ f \in U \implies dom(g) = cod(g) = A$. In other words, all morphisms in U are endomorphisms on the object A. Therefore, $U \subseteq G(A, A)$.
$f \circ id_A = f \in U \implies id_A \in U$. So, the identity on A must be in U.
$\forall h : A \longrightarrow A$ we have $h \circ h^{-1} = id_A \in U \implies h \in U$. 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 $h \circ h^{-1} = id_A \in U \implies h \in U \implies A = B$, 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 $\mu_\circ : \mathbb{C}^n \otimes \mathbb{C}^n \to \mathbb{C}^n$, 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 $\mu_\bullet$ 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:

$$\delta_\bullet(\mu_\circ(i \otimes j)) = (\mu_\circ(i, j) \otimes \mu_\circ(i, j)), \tag{1}$$

as $\mu_\circ(i, j)$ defines a basis element,so a copyable states of $\delta_\bullet$.
On the other hand,

$$\mu_\circ\mu_\circ) \circ (\delta_\bullet \otimes \delta_\bullet)(i \otimes j) = (\mu_\circ\mu_\circ)(i \otimes j \otimes i \otimes j) = (\mu_\circ(i, j) \otimes \mu_\circ(i, j)). \tag{2}$$

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:

$$\begin{aligned} \epsilon_\circ \circ \mu_\bullet(a \otimes b) &= \epsilon_\circ c \\ &= 1 \end{aligned} \tag{3}$$

The left-hand-side give us:

$$\epsilon_\circ\epsilon_\circ(a \otimes b) = 1 \cdot 1 = 1 \tag{4}$$

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 $\eta_\circ : I \to \mathbb{C}^n$ as $\eta_\circ(1) = |1\rangle$. Using this map as the unit for $\mu_\circ$, the last two bialgebra equations hold as well.
Now we will show that $(\mathrm{id} \otimes \mu_\circ) \circ ((\delta_\bullet \otimes \mathrm{id})$ 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.

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

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

Simultaneously we have

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

Exercise 5.5. Assume that the monoidal structure in **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 **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 $(\alpha_{A,B,C}, \lambda_A, \rho_A)$.