Introduction to Quantum Programming and Semantics: tutorial solutions

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 comparison.

Observe that the following equation holds because of naturality of ρ:

$$\rho_A \circ (u \otimes \mathrm{id}_I) = u \circ \rho_I$$

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

$$\rho_A \circ (u \otimes \mathrm{id}_I) = u \circ \rho_I = u \circ \lambda_I$$

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

$$\lambda_A \circ (\mathrm{id}_I \otimes u') = u' \circ \lambda_I = u' \circ \rho_I$$

We have:

$$\begin{aligned}
& m \circ (\mathrm{id}_A \otimes u') = \rho_A \\
\Longrightarrow\ & m \circ (\mathrm{id}_A \otimes u') \circ (u \otimes \mathrm{id}_I) = \rho_A \circ (u \otimes \mathrm{id}_I) && \text{(compose on right)} \\
\Longrightarrow\ & m \circ (\mathrm{id}_A \otimes u') \circ (u \otimes \mathrm{id}_I) = u \circ \lambda_I && \text{(above equation)} \\
\Longrightarrow\ & m \circ (u \otimes u') = u \circ \lambda_I && \text{(interchange law)} \\
\Longrightarrow\ & m \circ (u \otimes \mathrm{id}_A) \circ (\mathrm{id}_I \otimes u') = u \circ \lambda_I && \text{(interchange law)} \\
\Longrightarrow\ & \lambda_A \circ (\mathrm{id}_I \otimes u') = u \circ \lambda_I && \text{(monoid axiom)} \\
\Longrightarrow\ & u' \circ \lambda_I = u \circ \lambda_I && \text{(above equation)} \\
\Longrightarrow\ & u' = u && (\lambda_I \text{ is invertible})
\end{aligned}$$

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

Exercise 4.3

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

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

$$
\begin{aligned}
m_1 \circ (m_2 \otimes m_2) \circ (u_2 \otimes u_1 \otimes u_1 \otimes u_2) &= m_2 \circ (m_1 \otimes m_1) \circ (\mathrm{id}_A \circ \sigma \circ \mathrm{id}_A) \circ \\
&\quad (u_2 \otimes u_1 \otimes u_1 \otimes u_2) \\
&\Longrightarrow \\
m_1 \circ (\lambda_A \circ (\mathrm{id}_I \otimes u_1)) \otimes (\rho_A \circ (u_1 \otimes \mathrm{id}_I)) &= m_2 \circ (m_1 \otimes m_1) \circ (u_2 \otimes u_1 \otimes u_1 \otimes u_2) \\
&\Longrightarrow \\
m_1 \circ ((u_1 \circ \lambda_I) \otimes (u_1 \circ \rho_I)) &= m_2 \circ ((\rho_A \circ (u_2 \otimes \mathrm{id}_I)) \otimes (\lambda_A \circ (\mathrm{id}_I \otimes u_2))) \\
&\Longrightarrow \\
m_1 \circ (u_1 \otimes u_1) \circ (\lambda_I \otimes \rho_I)) &= m_2 \circ ((u_2 \circ \rho_I) \otimes (u_2 \circ \lambda_I)) \\
&\Longrightarrow \\
\lambda_A \circ (\mathrm{id}_I \otimes u_1) \circ (\lambda_I \otimes \rho_I)) &= m_2 \circ (u_2 \otimes u_2) \circ (\rho_I \otimes \lambda_I) \\
&\Longrightarrow \\
\lambda_A \circ (\mathrm{id}_I \otimes u_1) &= m_2 \circ (u_2 \otimes u_2) \\
&\Longrightarrow \\
\lambda_A \circ (\mathrm{id}_I \otimes u_1) &= \lambda_A \circ (\mathrm{id}_I \otimes u_2) \\
&\Longrightarrow \\
u_1 \circ \lambda_I &= u_2 \circ \lambda_I \\
&\Longrightarrow \\
u_1 &= u_2
\end{aligned}
$$

(b) From now on we will write $u = u_1 = u_2$.

Plugging in the map $(\mathrm{id}_A \otimes u \otimes u \otimes \mathrm{id}_A)$ to both sides of the equation yields the desired result.

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

(c) We will write $m = m_1 = m_2$.

This time, the trick is to plug in the map $(u \otimes \mathrm{id}_A \otimes \mathrm{id}_A \otimes u)$ to both sides of the equation. We get:

$$
\begin{aligned}
m \circ (m \otimes m) \circ (u \otimes \mathrm{id}_A \otimes \mathrm{id}_A \otimes u) &= m \circ (m \otimes m) \circ (\mathrm{id}_A \circ \sigma \circ \mathrm{id}_A) \circ \\
&\quad (u \otimes \mathrm{id}_A \otimes \mathrm{id}_A \otimes u) \\
&\Longrightarrow \\
m \circ (\lambda_A \otimes \rho_A) &= m \circ (m \otimes m) \circ (u \otimes \mathrm{id}_A \otimes \mathrm{id}_A \otimes u) \circ \\
&\quad (\mathrm{id}_I \circ \sigma \circ \mathrm{id}_I) \\
&\Longrightarrow \\
m \circ (\lambda_A \otimes \rho_A) &= m \circ (\lambda_A \otimes \rho_A) \circ (\mathrm{id}_I \circ \sigma \circ \mathrm{id}_I) \\
&\Longrightarrow \\
m \circ (\lambda_A \otimes \rho_A) &= m \circ \sigma \circ (\lambda_A \otimes \rho_A) \\
&\Longrightarrow \\
m &= m \circ \sigma
\end{aligned}
$$

Exercise 4.4

(Note: This is ghastly without graphical calculus.)

Let A and B be arbitrary objects in our category. Set $B^A = B \otimes A^*$. We define the evaluation map $\mathrm{ev} : (B \otimes A^*) \otimes A \to B$ by $\mathrm{ev} = \rho_B \circ (\mathrm{id}_B \otimes \varepsilon_A) \circ \alpha^{-1}_{B,A^*,A}$. For a given $f : X \otimes A \to B$, define $g : X \to B \otimes A^*$ by $g = (f \otimes \mathrm{id}_{A^*}) \circ \alpha^{-1}_{X,A,A^*} \circ (\mathrm{id}_X \otimes \eta_A) \circ \rho_X^{-1}$. From the snake equations it follows that $f = \mathrm{ev} \circ (g \otimes \mathrm{id}_A)$. To show g is unique, assume $f = \mathrm{ev} \circ (g' \otimes \mathrm{id}_A)$. Then we can precompose both sides with $\alpha^{-1}_{X,A,A^*} \circ (\mathrm{id}_X \otimes \eta_A) \circ \rho_X^{-1}$ and tensor with id_{A^*} on the right to get $(f \otimes \mathrm{id}_{A^*}) \circ \alpha^{-1}_{X,A,A^*} \circ (\mathrm{id}_X \otimes \eta_A) \circ \rho_X^{-1} = (\mathrm{ev} \otimes \mathrm{id}_A) \circ ((g' \otimes \mathrm{id}_{A^*}) \otimes \mathrm{id}_A) \circ \alpha^{-1}_{X,A,A^*} \circ (\mathrm{id}_X \otimes \eta_A) \circ \rho_X^{-1}$, or $g = g'$ (where the LHS is transformed according to the snake equations).

Exercise 4.5

Let $(A, \cdot, 1)$ be a monoid in $(\mathbf{Set}, \times, 1)$ that is partially ordered in a way that $a \cdot c \leq b \cdot c$ and $c \cdot a \leq c \cdot b$ when $a \leq b$.

Consider a monoidal category $\mathcal{C}$, with objects $a \in A$. In $\mathcal{C}$, there is a unique morphism $a \to b$ between two objects iff $a \leq b$. Thus, any homset in $\mathcal{C}$ is either empty or contains exactly one morphism.

The tensor product on objects a and b in $\mathcal{C}$ is given by:

$$a \otimes b = a \cdot b$$

and on morphisms $f : a \to b$, $g : c \to d$ as:

$$f \otimes g = a \cdot c \to b \cdot d$$

which is well-defined because of the way the partial order on A is given.

The tensor unit in $\mathcal{C}$ is 1. Note, that $1 \otimes a = a = a \otimes 1$. Thus, the left and right unitors (λ_a, ρ_a) are just the identity morphisms. Similarly, $(a \otimes b) \otimes c = a \otimes (b \otimes c)$ due to associativity in the monoid, so the associator α is also just the identity.

We will prove that an object of this monoidal category has a dual if and only if it has an inverse in A.

(LHS $\Longrightarrow$ RHS)

Suppose $l \in A$ has a dual $r \in A$. Thus $l \vdash r$ and $r \vdash l$. From the first duality, we get that the unit and counit morphisms exist which means

$$1 \leq r \cdot l$$
$$l \cdot r \leq 1$$

Similarly, from the second duality, we get:

$$1 \leq l \cdot r$$
$$r \cdot l \leq 1$$

By combining these four inequalities, we get:

$$1 \leq r \cdot l \leq 1$$
$$1 \leq l \cdot r \leq 1$$

Thus, $r \cdot l = 1 = l \cdot r$, which means that r is the inverse of l and vice-versa.

(RHS $\Longrightarrow$ LHS)

Assume that an object $l \in A$ has an inverse $l^{-1} \in A$. We clearly have $1 \leq l \cdot l^{-1} \leq 1$ and $1 \leq l^{-1} \cdot l \leq 1$ which means the unit and count morphisms exist for both dualities ($l \vdash r$ and $r \vdash l$). The snake equations are then satisfied trivially. Therefore, l has a dual, namely l^{-1}.

An ordered *abelian* group induces a strict symmetry on the category, i.e. the symmetry is an identity: $ab = ba$. Furthermore, note that the dual of the dual of an object a is a itself. Therefore, because cups and caps are trivial, the conditions of a compact category are satisfied.

For the final part, if we have daggers, then

$$a \leq b \Longrightarrow b \leq a \Longrightarrow a = b$$

Thus, the category is discrete (only has identity morphisms).