$\mathcal{Q}$WIRE: A Core Language for Quantum Circuits

Jennifer Paykin Robert Rand Steve Zdancewic
University of Pennsylvania
jpaykin@seas.upenn.edu, rrand@seas.upenn.edu, stevez@cis.upenn.edu

Appendix A Type safety and normalization

Theorem 6 (Preservation). *Suppose $\longrightarrow_{\text{H}}$ satisfies preservation.*

1. *If $\vdash t : A$ and $t \longrightarrow t'$, then $\vdash t' : A$.*
2. *If $\cdot; \mathcal{Q} \vdash C : W$ and $C \Longrightarrow C'$, then $\cdot; \mathcal{Q} \vdash C' : W$.*

Proof.

1. If t steps via $\longrightarrow_{\text{H}}$ then the result is immediate by the assumption that $\longrightarrow_{\text{H}}$ satisfies preservation. Otherwise, suppose $t \longrightarrow_b t'$. It must be the case that $A = \mathsf{Circ}(W_1, W_2)$ and $t = \mathsf{box}\ p \Rightarrow C$ where $\Omega \Rightarrow p : W_1$ and $\cdot; \Omega \vdash C : W_2$. If t steps via the structural rule with $C \Longrightarrow C'$, then $t' = \mathsf{box}\ p \Rightarrow C'$, and by the inductive hypothesis, $\cdot; \Omega \vdash C' : W_2$ and so $\cdot \vdash \mathsf{box}\ p \Rightarrow C' : \mathsf{Circ}(W_1, W_2)$.

If t steps instead by an η rule, then $t' = \mathsf{box}\ p' \Rightarrow C\ \{p'/p\}$ where p' is concrete for W_1. By Lemma 5 there is some $\mathcal{Q}$ such that $\mathcal{Q} \Rightarrow p' : W_1$, so by the substitution lemma (Lemma 4), we have $\cdot; \mathcal{Q} \vdash C\ \{p'/p\} : W_2$, and thus $\cdot \vdash t' : \mathsf{Circ}(W_1, W_2)$.

2. By induction on $C \Longrightarrow C'$.

(a) If $C = \mathsf{unbox}\ t\ p$ then we have

$$\cdot \vdash t : \mathsf{Circ}(W_1, W) \qquad \text{and} \qquad \mathcal{Q} \Rightarrow p : W_1.$$

If C steps by a structural rule with $t \longrightarrow t'$, then by the inductive hypothesis we have $\cdot \vdash t' : \mathsf{Circ}(W_1, W)$, and so $\cdot; \mathcal{Q} \vdash \mathsf{unbox}\ t'\ p : W$. If it steps via the β rule, then $t = \mathsf{box}\ p' \Rightarrow N$, and so by inversion we know there is some $\mathcal{Q}' \Rightarrow p' : W_1$ such that $\cdot; \mathcal{Q}' \vdash N : W_2$. By the substitution lemma (Lemma 4), we have that $\cdot; \mathcal{Q} \vdash N\ \{p/p'\} : W$ as expected.

(b) Suppose C is $p_2 \leftarrow \mathsf{gate}\ g\ p_1; C_0$, where $\mathcal{Q} = \mathcal{Q}_1, \mathcal{Q}_0$ and

$$\mathcal{Q}_1 \Rightarrow p_1 : W_1 \qquad \Omega_2 \Rightarrow p_2 : W_2 \qquad \cdot; \Omega_2, \mathcal{Q}_0 \vdash C_0 : W.$$

If C steps via a structural rule on C_0, the result is straightforward from the induction hypothesis. Otherwise, it steps via an η-expansion:

$$p_2 \leftarrow \mathsf{gate}\ g\ p_1; C_0 \Longrightarrow p_2' \leftarrow \mathsf{gate}\ g\ p_1; C_0\ \{p_2'/p_2\}$$

where $\mathcal{Q}_2 \Rightarrow p_2' : W_1$. By Lemma 4 we know $\cdot; \mathcal{Q}_2, \mathcal{Q} \vdash C_0\ \{p_2'/p_2\} : W$, and so $\cdot; \mathcal{Q}_1, \mathcal{Q} \vdash p_2' \leftarrow \mathsf{gate}\ g\ p_2; C_0\ \{p_2'/p_2\} : W$.

(c) Finally, suppose $C = p \leftarrow C_1; C_2$, where $\mathcal{Q} = \mathcal{Q}_1, \mathcal{Q}_2$ and

$$\cdot; \mathcal{Q}_1 \vdash C_1 : W' \qquad \Omega \Rightarrow p : W' \qquad \cdot; \Omega, \mathcal{Q}_2 \vdash C_2 : W$$

If C steps via a structural rule, the result is immediate. If it steps via a β-rule, then $C_1 = \mathsf{output}\ p'$, and by inversion, $\mathcal{Q}_1 \Rightarrow p' : W$. By Lemma 4, we have $\cdot; \mathcal{Q}_1, \mathcal{Q}_2 \vdash C'\ \{p'/p\} : W'$.

If $C_1 = p_2 \leftarrow \mathsf{gate}\ g\ p_1; C_0$ such that

$$p \leftarrow C_1; C_2 \Longrightarrow p_2 \leftarrow \mathsf{gate}\ g\ p_1; p \leftarrow C_0; C_2$$

by a commuting conversion, then by inversion we have $\mathcal{Q}_1 = \mathcal{Q}_1', \mathcal{Q}_0$ where $g \in \mathcal{G}(W_1, W_2)$, $\mathcal{Q}_1' \Rightarrow p_1 : W_1$, $\Omega_2' \Rightarrow p_2 : W_2$, and $\cdot; \Omega_2', \mathcal{Q}_0 \vdash C_0 : W'$. Then $\cdot; \Omega_2', \mathcal{Q}_0, \mathcal{Q}_2 \vdash p \leftarrow C_0; C_2 : W$ and so

$$\cdot; \mathcal{Q}_1', \mathcal{Q}_0, \mathcal{Q}_2 \vdash p_2 \leftarrow \mathsf{gate}\ g\ p_1; p \leftarrow C_0; C_2 : W.$$

If $C_1 = x \Leftarrow \mathsf{lift}\ p'; C_0$ such that

$$p \leftarrow C_1; C_2 \Longrightarrow x \Leftarrow \mathsf{lift}\ p'; p \leftarrow C_0; C_2$$

by a commuting conversion, then by inversion we have $\mathcal{Q}_1 = \mathcal{Q}_0, \mathcal{Q}'$ such that $\mathcal{Q}_0 \Rightarrow p' : W_0$ and $x : |W_0|; \mathcal{Q}' \vdash C_0 : W'$. In that case, $x : |W_0|; \mathcal{Q}', \mathcal{Q}_2 \vdash p \leftarrow C_0; C_2 : W$ and so $\cdot; \mathcal{Q}_0, \mathcal{Q}', \mathcal{Q}_2 \vdash x \Leftarrow \mathsf{lift}\ p'; p \leftarrow C_0; C_2 : W$.

□

Theorem 7 (Progress). *Suppose $\longrightarrow_{\text{H}}$ satisfies progress with respect to the values v^{H}.*

1. *If $\cdot \vdash t : A$ then either t is a value v^{C} or there is some t' such that $t \longrightarrow t'$.*
2. *If $\cdot; \mathcal{Q} \vdash C : W$ then either C is normal or there is some C' such that $C \Longrightarrow C'$.*

Proof.

1. By the progress hypothesis for $\longrightarrow_{\text{H}}$, either $t = v^{\text{H}}$ for some v^{H} or there exists some t' such that $t \longrightarrow_{\text{H}} t'$ (in which case $t \longrightarrow t'$ as well). In first case however, t is either a value in the original host language (v), or $t = \mathsf{box}\ p \Rightarrow C$, where

$$\frac{\Omega \Rightarrow p : W_1 \quad \cdot; \Omega \vdash C : W_2}{\cdot \vdash \mathsf{box}\ p \Rightarrow C : \mathsf{Circ}(W_1, W_2)}$$

If p is not concrete for W_1, then $\mathsf{box}\ p \Rightarrow C$ can step via the η rule. If p is concrete, then by the inductive hypothesis, C is either normal already (in which case so is $\mathsf{box}\ p \Rightarrow C$), or there is some C' such that $C \Longrightarrow C'$. In that case, $\mathsf{box}\ p \Rightarrow C \longrightarrow_b \mathsf{box}\ p \Rightarrow C'$.

2. By induction on the typing judgment of C.

(a) If the last rule in the derivation is

$$\frac{\cdot \vdash t : \mathsf{Circ}(W_1, W_2) \quad \mathcal{Q} \Rightarrow p : W_1}{\cdot; \mathcal{Q} \vdash \mathsf{unbox}\ t\ p : W_2}$$

then by the inductive hypothesis, either t can take a step to some t', or t is a value of the form $\mathsf{box}\ p' \Rightarrow N$. In the first case, $\mathsf{unbox}\ t\ p \Longrightarrow \mathsf{unbox}\ t'\ p$, and in the second case, $\mathsf{unbox}\ t\ p \Longrightarrow N\ \{p'/p\}$.

(b) Next, suppose the last rule in the derivation is

$$\frac{g \in \mathcal{G}(W_1, W_2) \quad \mathcal{Q}_1 \Rightarrow p_1 : W_1 \quad \Omega_2 \Rightarrow p_2 : W_2 \quad \cdot; \Omega_2, \mathcal{Q} \vdash C : W}{\cdot; \mathcal{Q}_1, \mathcal{Q} \vdash p_2 \leftarrow \mathsf{gate}\ g\ p_1; C : W}$$

If C is not concrete, then $p_2 \leftarrow \mathsf{gate}\ g\ p_1; C$ can step via an η rule. Otherwise, C is either normal, in which case $p_2 \leftarrow \mathsf{gate}\ g\ p_1; C$ is also normal, or C can take a step, in which case so can $p_2 \leftarrow \mathsf{gate}\ g\ p_1; C$ by the structural rule.

(c) Suppose the circuit is

$$\frac{\cdot; \mathcal{Q}_1 \vdash C : W \quad \Omega_0 \Rightarrow p : W \quad \cdot; \Omega_0, \mathcal{Q}_2 \vdash C' : W'}{\cdot; \mathcal{Q}_1, \mathcal{Q}_2 \vdash p \leftarrow C; C' : W'}$$

By the inductive hypothesis, either C can take a step, in which case so can $p \leftarrow C; C'$, or C is normal. The following chart covers these remaining cases: if C is the normal circuit in the first column, then $p \leftarrow C; C'$ steps to the circuit in the second column.

$\mathsf{output}\ p'$	$C'\ \{p'/p\}$
$p_2 \leftarrow \mathsf{gate}\ g\ p_1; C_0$	$p_2 \leftarrow \mathsf{gate}\ g\ p_1; p \leftarrow C_0; C'$
$x \Leftarrow \mathsf{lift}\ p_0; C_0$	$x \Leftarrow \mathsf{lift}\ p_0; p \leftarrow C_0; C'$

□

Theorem 8 (Normalization)**.** *Suppose that $\longrightarrow_{\mathrm{H}}$ is strongly normalizing with respect to v^{H}.*

1. *If $\cdot \vdash t : A$, there exists some value v^{C} such that $t \longrightarrow^* v^{\mathrm{C}}$.*
2. *If $\cdot; \mathcal{Q} \vdash C : W$, there exists some normal circuit N such that $C \Longrightarrow^* N$.*

Proof. By induction on the number of constructors in the term and circuit.

1. By the normalization property for $\longrightarrow_{\mathrm{H}}$, there is some value v^{C} such that $t \longrightarrow_{\mathrm{H}}^* v^{\mathrm{C}}$. This value v^{C} is either a regular host language value v, in which case we are done, or it is some uninterpreted boxed circuit $\mathsf{box}\ (p : W) \Rightarrow C$. If p is concrete with respect to W, then by the inductive hypothesis, there is some N such that $C \Longrightarrow^* N$, and so $\mathsf{box}\ p \Rightarrow C \longrightarrow^* \mathsf{box}\ p \Rightarrow N$.

If p is not concrete, then by an η-expansion, there is some p' that is concrete for W and $\mathsf{box}\ p \Rightarrow C \longrightarrow_b \mathsf{box}\ p' \Rightarrow C\ \{p'/p\}$. By induction we know that $C\ \{p'/p\}$ normalizes (since the number of constructors in $C\ \{p'/p\}$ is the same as the number in C), and thus so does $\mathsf{box}\ p \Rightarrow C$.

2. If C is an output or lifting circuit then it is already normal. If C is an unboxing operator of the form

$$\frac{\cdot \vdash t : \mathsf{Circ}(W_1, W_2) \quad \mathcal{Q} \Rightarrow p : W_1}{\cdot; \mathcal{Q} \vdash \mathsf{unbox}\ t\ p : W_2}$$

then by the inductive hypothesis, there is some $\mathsf{box}\ p' \Rightarrow N$ such that $t \longrightarrow^* \mathsf{box}\ p' \Rightarrow N$, so $\mathsf{unbox}\ t\ p \longrightarrow^* N\ \{p/p'\}$, which is also normal.

Next, consider a gate application:

$$\frac{g \in \mathcal{G}(W_1, W_2) \quad \mathcal{Q}_1 \Rightarrow p_1 : W_1 \quad \Omega_2 \Rightarrow p_2 : W_2 \quad \cdot; \Omega_2, \mathcal{Q} \vdash C : W}{\cdot; \mathcal{Q}_1, \mathcal{Q} \vdash p_2 \leftarrow \mathsf{gate}\ g\ p_1; C : W}$$

Again, if C is concrete, it normalizes by the inductive hypothesis; otherwise there is some $\mathcal{Q}_2 \Rightarrow p_2' : W_2$ where $C\ \{p_2'/p_2\}$ normalizes to some N, in which case $p_2 \leftarrow \mathsf{gate}\ g\ p_1; C \Longrightarrow^* p_2' \leftarrow \mathsf{gate}\ g\ p_1; N$.

Finally, consider a composition operator:

$$\frac{\cdot; \mathcal{Q}_1 \vdash C : W \quad \Omega_0 \Rightarrow p : W \quad \cdot; \Omega_0, \mathcal{Q}_2 \vdash C' : W'}{\cdot; \mathcal{Q}_1, \mathcal{Q}_2 \vdash p \leftarrow C; C' : W'}$$

By the inductive hypothesis, there is some N such that $C \Longrightarrow^* N$. If $N = \mathsf{output}\ p'$, then $p \leftarrow C; C' \Longrightarrow^* C'\ \{p'/p\}$, which normalizes by the inductive hypothesis for C'. If $N = p_2 \leftarrow \mathsf{gate}\ g\ p_1; C_0$, then $p \leftarrow C_0; C'$ normalizes to some N' by the inductive hypothesis, and so

$$p \leftarrow C; C' \Longrightarrow^* p_2 \leftarrow \mathsf{gate}\ g\ p_1; N'.$$

Finally, if $N = x \Leftarrow \mathsf{lift}\ p'; C_0$, then

$$p \leftarrow C; C' \Longrightarrow x \Leftarrow \mathsf{lift}\ p'; p \leftarrow C_0; C',$$

which is immediately normal.

□

Appendix B Soundness of denotational semantics

Theorem 11 (Soundness)**.** *If $\cdot; \mathcal{Q} \vdash C : W$ and $C \Longrightarrow C'$, then*

$$[\![\mathcal{Q} \vdash C : W]\!] = [\![\mathcal{Q} \vdash C' : W]\!].$$

Proof. By induction on the typing judgment.

If C is

$$\frac{\cdot; \mathcal{Q}' \vdash C : W \quad \pi : \mathcal{Q} \equiv \mathcal{Q}'}{\cdot; \mathcal{Q} \vdash C : W}$$

and $C \Longrightarrow C'$, then by the inductive hypothesis,

$$\begin{aligned}[\![\mathcal{Q} \vdash C : W]\!] &= [\![\mathcal{Q}' \vdash C : W]\!] \circ [\pi]^* \\ &= [\![\mathcal{Q}' \vdash C' : W]\!] \circ [\pi]^* = [\![\mathcal{Q} \vdash C' : W]\!]\end{aligned}$$

If

$$\frac{\cdot \vdash t : \mathsf{Circ}(W_1, W_2) \quad \mathcal{Q} \Rightarrow p : W_1}{\cdot; \mathcal{Q} \vdash \mathsf{unbox}\ t\ p : W_2}$$

and the circuit steps by a structural rule with $t \longrightarrow t'$, then, assuming HOST is strongly normalizing we have some $\mathsf{box}\ p' \Rightarrow N$ such that $t, t' \longrightarrow^* \mathsf{box}\ p' \Rightarrow N$. Then

$$[\![\mathcal{Q} \vdash \mathsf{unbox}\ t\ p : W_2]\!] = [\![\mathcal{Q} \vdash \mathsf{unbox}\ t'\ p : W_2]\!] = [\![\mathcal{Q}' \vdash N : W_2]\!]$$

Suppose

$$\frac{g \in \mathcal{G}(W_1, W_2) \quad \mathcal{Q}_1 \Rightarrow p_1 : W_1 \quad \Omega_2 \Rightarrow p_2 : W_2 \quad \cdot; \Omega_2, \mathcal{Q} \vdash C : W}{\cdot; \mathcal{Q}_1, \mathcal{Q} \vdash p_2 \leftarrow \mathsf{gate}\ g\ p_1; C : W}$$

If the circuit steps via a structural rule, the result is immediate. If it steps via an η rule to $p_2' \leftarrow \mathsf{gate}\ g\ p_1; C\ \{p_2'/p_2\}$, then the result follows from the fact that $[\![C\ \{p_2'/p_2\}]\!] = [\![C]\!]$ (Lemma 10).

Next, consider

$$\frac{\cdot; \mathcal{Q}_1 \vdash C_1 : W \qquad \Omega_0 \Rightarrow p : W \qquad \cdot; \Omega_0, \mathcal{Q}_2 \vdash C_2 : W'}{\cdot; \mathcal{Q}_1, \mathcal{Q}_2 \vdash p \leftarrow C_1; C_2 : W'}$$

If the circuit steps via a structural rule, the result follows immediately. Otherwise, we know C_1 is normal, and the circuit stepped via a β or commuting conversion rule. We proceed by a further case analysis on the typing judgment of C_1.

For a permutation rule $\pi : \mathcal{Q}_1 \equiv \mathcal{Q}_1'$, by induction we know that

$$[\![\mathcal{Q}_1', \mathcal{Q}_2 \vdash p \leftarrow C_1; C_2 : W']\!] = [\![\mathcal{Q}_1', \mathcal{Q}_2 \vdash C' : W']\!]$$

But then

$$\begin{aligned}&[\![\mathcal{Q}_1, \mathcal{Q}_2 \vdash p \leftarrow C_1; C_2 : W']\!] \\ &= [\![\Omega_0, \mathcal{Q}_2 \vdash C_2 : W']\!] \circ ([\![\mathcal{Q}_1 \vdash C_1 : W]\!] \otimes \mathbf{I}^*) \\ &= [\![\Omega_0, \mathcal{Q}_2 \vdash C_2 : W']\!] \circ \big(([\![\mathcal{Q}_1' \vdash C_1 : W]\!] \circ [\pi]^*) \otimes \mathbf{I}^*\big) \\ &= [\![\Omega_0, \mathcal{Q}_2 \vdash C_2 : W']\!] \circ \big([\![\mathcal{Q}_1' \vdash C_1 : W]\!] \otimes \mathbf{I}^*\big) \circ ([\pi] \otimes \mathbf{I})^* \\ &= [\![\mathcal{Q}_1', \mathcal{Q}_2 \vdash p \leftarrow C_1; C_2 : W']\!] \circ ([\pi] \otimes \mathbf{I})^* \\ &= [\![\mathcal{Q}_1, \mathcal{Q}_2 \vdash p \leftarrow C_1; C_2 : W']\!]\end{aligned}$$

For $C_1 = \mathsf{output}\ p'$ with $\mathcal{Q}_1 \Rightarrow p' : W$, where

$$p \leftarrow C_1; C_2 \Longrightarrow C_2\,\{p'/p\},$$

we know

$$\begin{aligned}
&[\![\mathcal{Q}_1, \mathcal{Q}_2 \vdash p \leftarrow \mathsf{output}\ p'; C_2 : W']\!]\\
&= [\![\Omega_0, \mathcal{Q}_2 \vdash C_2 : W']\!] \circ \left([\![\mathcal{Q}_1 \vdash \mathsf{output}\ p' : W]\!] \otimes \mathbf{I}^*\right)\\
&= [\![\Omega_0, \mathcal{Q}_2 \vdash C_2 : W']\!] \circ (\mathbf{I}^* \otimes \mathbf{I}^*)\\
&= [\![\Omega_0, \mathcal{Q}_2 \vdash C_2 : W']\!] = [\![\mathcal{Q}_1, \mathcal{Q}_2 \vdash C_2\,\{p'/p\} : W']\!]
\end{aligned}$$

by Lemma 10.

If C_1 is

$$\frac{\mathcal{Q}_1' \Rightarrow p_1 : W_1 \qquad \Omega_2 \Rightarrow p_2 : W_2 \qquad \overset{g \in \mathcal{G}(W_1, W_2)}{\cdot; \Omega_2, \mathcal{Q}' \vdash C_0 : W}}{\cdot; \mathcal{Q}_1', \mathcal{Q}' \vdash p_2 \leftarrow \mathsf{gate}\ g\ p_1; C_0 : W}$$

and steps via a commuting conversion

$$p \leftarrow C_1; C_2 \Longrightarrow p_2 \leftarrow \mathsf{gate}\ g\ p_1; p \leftarrow C_0; C_2$$

then

$$\begin{aligned}
&[\![\mathcal{Q}_1', \mathcal{Q}', \mathcal{Q}_2 \vdash p \leftarrow (p_2 \leftarrow \mathsf{gate}\ g\ p_1; C_0); C_2 : W']\!]\\
&= [\![\Omega_0, \mathcal{Q}_2 \vdash C_2 : W']\!] \circ \left([\![\mathcal{Q}_1', \mathcal{Q}' \vdash p_2 \leftarrow \mathsf{gate}\ g\ p_1; C_0 : W]\!] \otimes \mathbf{I}^*\right)\\
&= [\![\Omega_0, \mathcal{Q}_2 \vdash C_2 : W']\!] \circ \left(\left([\![\Omega_2, \mathcal{Q}' \vdash C_0 : W]\!] \circ ([\![g]\!] \otimes \mathbf{I}^*)\right) \otimes \mathbf{I}^*\right)\\
&= [\![\Omega_0, \mathcal{Q}_2 \vdash C_2 : W']\!] \circ \left([\![\Omega_2, \mathcal{Q}' \vdash C_0 : W]\!] \otimes \mathbf{I}^*\right) \circ \left([\![g]\!] \otimes \mathbf{I}^* \otimes \mathbf{I}^*\right)\\
&= [\![\Omega_2, \mathcal{Q}', \mathcal{Q}_2 \vdash p \leftarrow C_0; C_2 : W']\!] \circ ([\![g]\!] \otimes \mathbf{I}^*)\\
&= [\![\mathcal{Q}_1', \mathcal{Q}', \mathcal{Q}_2 \vdash p_2 \leftarrow \mathsf{gate}\ g\ p_1; p \leftarrow C_0; C_2 : W']\!]
\end{aligned}$$

Finally, if C_1 is

$$\frac{\mathcal{Q}_0 \Rightarrow p_0 : W_0 \qquad x : |W_0|; \mathcal{Q}' \vdash C_0 : W}{\cdot; \mathcal{Q}_0, \mathcal{Q}' \vdash x \Leftarrow \mathsf{lift}\ p_0; C_0 : W}$$

and steps via a commuting conversion

$$p \leftarrow C_1; C_2 \Longrightarrow x \Leftarrow \mathsf{lift}\ p_0; p \leftarrow C_0; C_2$$

then

$$\begin{aligned}
&[\![\mathcal{Q}_0, \mathcal{Q}', \mathcal{Q}_2 \vdash p \leftarrow (x \Leftarrow \mathsf{lift}\ p_0; C_0); C_2 : W']\!]\\
&= [\![\Omega_0, \mathcal{Q}_2 \vdash C_2 : W']\!] \circ \left([\![\mathcal{Q}_0, \mathcal{Q}' \vdash x \Leftarrow \mathsf{lift}\ p_0; C_0 : W]\!] \otimes \mathbf{I}^*\right)\\
&= [\![C_2]\!] \circ \left(\left(\sum_{\vdash v : |W_0|} [\![\mathcal{Q}' \vdash C_0\{v/x\} : W]\!] \circ ([v : |W_0|]^\dagger \otimes \mathbf{I})^*\right) \otimes \mathbf{I}^*\right)\\
&= [\![C_2]\!] \circ \sum_{\vdash v : |W_0|} \left(\left([\![\mathcal{Q}' \vdash C_0\{v/x\} : W]\!] \circ ([v : |W_0|]^\dagger \otimes \mathbf{I})^*\right) \otimes \mathbf{I}^*\right)\\
&= [\![C_2]\!] \circ \sum_{\vdash v : |W_0|} ([\![C_0\{v/x\}]\!] \otimes \mathbf{I}^*) \circ \left([v : |W_0|]^\dagger \otimes \mathbf{I}^* \otimes \mathbf{I}^*\right)\\
&= \sum_{\vdash v : |W_0|} [\![C_2]\!] \circ ([\![C_0\{v/x\}]\!] \otimes \mathbf{I}^*) \circ \left([v : |W_0|]^\dagger \otimes \mathbf{I}^*\right)\\
&= \sum_{\vdash v : |W_0|} [\![p \leftarrow C_0\{v/x\}; C_2]\!] \circ \left([v : |W_0|]^\dagger \otimes \mathbf{I}^*\right)\\
&= [\![x \Leftarrow \mathsf{lift}\ p_0; p \leftarrow C_0; C_2]\!]
\end{aligned}$$

□

Appendix C Correctness of circuit case analysis

Theorem 12. *For all terms* `t` *of type* `ICirc W1 W2` *and* `c` *of type* $\mathsf{Circ}(W_1, W_2)$*, we have:*

$$\texttt{toICirc (fromICirc t)} = \texttt{t}$$
$$\texttt{fromICirc (toICirc c)} = \texttt{c}$$

Proof.

1. Start with case analysis on `t : ICirc W1 W2`. If `t` = `Output p`, then

```
toICirc (fromICirc (Output p))
= toICirc (box w => output (unpat p w))
= Output (pat w => unpat p w)
```

When `p=pat p1 => p2`, then we have

```
(pat w => unpat p w) = (pat p1 => unpat p p1)
= pat p1 => p2 = p
```

as expected.

If `t` = `Output p g c` then

```
toICirc (fromICirc (Gate p g c))
= toICirc (box (unpat (reverse-pat p) (w1,w0)) =>
         w2 <- gate g w1; unbox c (w2,w0))
= Gate (pat (unpat (reverse-pat p) (w1,w0)) => (w1,w0))
       g (box (w2,w0) => unbox c (w2,w0))
```

By η expansion it is clear that

`box (w2,w0) => unbox c (w2,w0)` = `c`,

and furthermore we have

`pat (unpat (reverse-pat p) (w1,w0)) => (w1,w0)` = `p` :

Suppose `p = pat p1 => (p1',p0)`. In general, notice that $\mathsf{pat}\ p_0 \Rightarrow p_0' = \mathsf{pat}\ p_0\{p'/p\} \Rightarrow p_0'\{p'/p\}$ for any compatible substitution. Then

```
pat (unpat (reverse-pat p) (w1,w0)) => (w1,w0)
= pat (unpat (reverse-pat p) (p1',p0)) => (p1',p0)
= (pat p1 => (p1',p0)) = p
```

as expected.

Next, suppose `t` = `Lift p f`. Then

```
toICirc (fromICirc (Lift p f))
= toICirc (box (unpat (reverse-pat p) (w,w')) =>
    x <= lift w; unbox (f x) w')
= Lift (pat (unpat (reverse-pat p) (w,w')) => (w,w'))
       (fun x => box w' => unbox (f x) w')
```

As we saw in the case for `Gate`'s,

`(pat (unpat (reverse-pat p) (w,w')) => (w,w'))` = `p`,

and by η-expansion,

```
fun x => (box w' => unbox (f x ) w')
= (fun x => f x) = f
```

2. Next, by case analysis on `N` where `c` = `box p => N`.

If `N` = `output p'` for some pattern `p'`, then

```
fromICirc (toICirc (box p => output p'))
= fromICirc (Output (pat p => p'))
= box w => output (unpat (pat p => p') w)
= box p => output (unpat (pat p => p') p)
= box p => p'.
```

If `N = p2 <- gate g p1; N'`, then let `p0` be the pattern corresponding to the intermediate context Ω_0. Then

```
fromICirc (toICirc (box p => (p2 <- gate g p1; N')))
= fromICirc (Gate (pat p => (p1,p0)) g (box (p2,p0) => N'))
= box (unpat (reverse-pat (pat p => (p1,p0))) (w1,w0)) =>
    w2 <- gate g w1; unbox (box (p2,p0) => N') (w2,w0)
= box (unpat (pat (p1,p0) => p) (p1,p0)) =>
    p2 <- gate g p1; unbox (box (p2,p0) => N') (p2,p0)
= box p => (p2 <- gate g p1; N')
```

Finally, if `N = (x <= lift p'; N')`, then let `p0` be the pattern corresponding to the intermediate context Ω_0. Then

```
fromICirc (toICirc (box p => (x <= lift p'; N')))
= fromICirc (Lift (pat p => (p',p0)) (fun x => box p0 => N'))
= box (unpat (reverse-pat (pat p => (p',p0))) (w',w0)) =>
    x <= lift w'; unbox ((fun x => box p0 => N') x) w0
= box (unpat (pat (p',p0) => p) (p',p0)) =>
    x <= lift p'; unbox (box p0 => N') p0
```

```
  = box p => (x <= lift p'; N')
```

□

Appendix D Correctness of Circuit Reversal

To prove the circuit reversal operation `reverse` c is semantically correct, we assume that the `reverse_gate` operation is also correct; in other words, assume that `reverse_gate` $g =$ `Some` g' implies $[\![g]\!] \circ [\![g']\!] = \mathbf{I}^* = [\![g']\!] \circ [\![g]\!]$. Then we can prove the following theorem:

Theorem 13. *If* `reverse c` $=$ `Some c'` *then*

$$[\![c]\!] \circ [\![c']\!] = \mathbf{I}^* \quad \textit{and} \quad [\![c']\!] \circ [\![c]\!] = \mathbf{I}^*.$$

Proof. Notice that $[\![\texttt{inSeq}\ c\ c']\!] = [\![c']\!] \circ [\![c]\!]$.

If $c = \mathsf{box}\ p \Rightarrow \mathsf{output}\ p'$ then it must be the case that $c' = \mathsf{box}\ p' \Rightarrow \mathsf{output}\ p$. In that case we have $[\![c]\!] = [\![c']\!] = \mathbf{I}^*$.

Otherwise, it must be the case that $c = \mathsf{box}\ p \Rightarrow p_2 \leftarrow \mathsf{gate}\ g\ p_1; N$; we can assume that `reverse` $(\mathsf{box}\,(p_2, p_0) \Rightarrow N) =$ `Some` c'' and `reverse_gate g` $=$ `Some g'`. Then

```
c' = box w => (p2,w') <- unbox c'' w;
              p1     <- gate g' p2;
              output (p1,w')
```

In this case, $[\![c]\!] = [\![N]\!] \circ ([\![g]\!] \otimes \mathbf{I}^*)$ and

$$\begin{aligned} [\![c']\!] &= [\![\mathsf{output}\ (p_1, w')]\!] \circ \left([\![g']\!] \otimes \mathbf{I}^*\right) \circ [\![c'']\!] \\ &= \left([\![g']\!] \otimes \mathbf{I}^*\right) \circ [\![c'']\!] \end{aligned}$$

Therefore

$$\begin{aligned} [\![c]\!] \circ [\![c']\!] &= [\![N]\!] \circ ([\![g]\!] \otimes \mathbf{I}^*) \circ \left([\![g']\!] \otimes \mathbf{I}^*\right) \circ [\![c'']\!] \\ &= [\![N]\!] \circ [\![c'']\!] = \mathbf{I}^* \end{aligned}$$

by the inductive hypothesis, and similarly for the other direction. □

As a corollary, we have

Corollary. *If* `reverse` $c_1 =$ `Some` c_1' *and* `reverse` $c_2 =$ `Some` c_2' *then* $[\![c_1']\!] = [\![c_2']\!]$.

We assert that syntactic version of this corollary is also true, namely that c_1' is operationally equivalent to c_2', but we leave its proof to future work.