Appendix A  Type safety and normalization

Theorem 6 (Preservation). Suppose $\rightarrow_{\mathcal{H}}$ satisfies preservation.

1. If $\vdash t : A$ and $t \rightarrow t'$, then $\vdash t' : A$.
2. If $\vdash Q \vdash C : W$ and $C \rightarrow C'$, then $\vdash Q \vdash C' : W$.

Proof.

1. If $t$ steps via $\rightarrow_{\mathcal{H}}$ then the result is immediate by the assumption that $\rightarrow_{\mathcal{H}}$ satisfies preservation. Otherwise, suppose $t \rightarrow_{\eta} t'$. It must be the case that $A = \text{Circ}(W_1, W_2)$ and $t = \text{box } p \Rightarrow C$ where $\Omega \Rightarrow p : W_1$ and $:\Omega \vdash C : W_2$. If $t$ steps via the structural rule with $C \Rightarrow C'$, then $t' = \text{box } p \Rightarrow C'$, and by the inductive hypothesis we have $\vdash Q \vdash C : W$, and by a commuting conversion, then by inversion we have $\vdash Q \vdash C' : W$.

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

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

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

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

(b) Suppose $C = p_2 \leftarrow \text{gate } g p_1; C_0$, where $Q = Q_1, Q_0$ and $Q_1 \vdash p_1 : W_1$ and $Q_2 \vdash p_2 : W_2$ and $Q_0 \vdash C_0 : W$.

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

$p_2 \leftarrow \text{gate } g p_1; C_0 \Rightarrow p_2' \leftarrow \text{gate } g p_1; C_0 \{p_2/p_2\}$

where $Q_2 \Rightarrow p_2' : W_1$. By Lemma 4 we know $\vdash Q_2, Q \vdash C_0 \{p_2/p_2\} : W$, and so $\vdash Q_1, Q \vdash p_2' \leftarrow \text{gate } g p_2; C_0 \{p_2/p_2\} : W$.

(c) Finally, suppose $C = p \leftarrow C_1; C_2$, where $Q = Q_1, Q_2$ and $\vdash Q_1 \vdash C_1 : W$ and $\vdash Q_2 \vdash C_2 : W$.

If $C$ steps via a structural rule, the result is immediate. If it steps via a $\beta$-rule, then $C_1 = \text{output } p'$, and by inversion, $Q_1 \Rightarrow p' : W$. By Lemma 4, we have $\vdash Q_1, Q_2 \vdash C' \{p'/p\} : W'$.

If $C_1 = p_2 \leftarrow \text{gate } g p_1; C_0$ such that $p \vdash C_1; C_2 \Rightarrow p_2 \leftarrow \text{gate } g p_1; p \vdash C_0; C_2$

by a commuting conversion, then by inversion we have $Q_1 = Q_0, \eta$ such that $Q_0 \Rightarrow p' : W_0$ and $\Omega \Rightarrow p_2 : W_2$ and $\Omega \vdash C_0 : W'$. Then $\vdash \Omega_2, Q_0, Q_2 \vdash p \Rightarrow C_0; C_2 : W$ and so $\vdash Q_1, Q_0, Q_2 \leftarrow p_2 \leftarrow \text{gate } g p_1; p \vdash C_0; C_2 : W$.

If $C_1 = x \leftarrow \text{lft } p'$, $C_0$ such that $p \vdash C_1; C_2 \Rightarrow x \leftarrow \text{lft } p'; p \vdash C_0; C_2$

by a commuting conversion, then by inversion we have $Q_1 = Q_0, \eta$ such that $Q_0 \Rightarrow p' : W_0$ and $\Omega \Rightarrow p_2 : W_2$ and $\Omega \vdash C_0 : W'$. In that case, $x : \{W_0\}, Q_0, Q_2 \vdash p \Rightarrow C_0; C_2 : W$ and so $\vdash Q_0, Q_2 : x \leftarrow \text{lft } p'; p \vdash C_0; C_2 : W$.

\[ \square \]

Theorem 7 (Progress). Suppose $\rightarrow_{\mathcal{H}}$ satisfies progress with respect to the values $v^n$.

1. If $\vdash t : A$ then either $t$ is a value $v^n$ or there is some $t'$ such that $t \rightarrow t'$.
2. If $\vdash Q \vdash C : W$ then either $C$ is normal or there is some $C'$ such that $C \Rightarrow C'$.

Proof.

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

$\Omega \Rightarrow p : W_1$ and $\Omega \vdash C : W_2$

\[ \vdash \text{box } p \Rightarrow C : \text{Circ}(W_1, W_2) \]

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

2. By induction on the typing judgment of $C$.

(a) If the last rule in the derivation is

$\vdash t : \text{Circ}(W_1, W_2)$

$\vdash Q \vdash \text{unbox } t p : W_2$

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

\[ \square \]
Next, suppose the last rule in the derivation is
\[ g \in G(W_1, W_2) \]
\[ \Omega_1 \Rightarrow p_1 : W_1 \quad \Omega_2 \Rightarrow p_2 : W_2 \quad \Omega_2, Q \vdash C : W \]
\[ ; \Omega_1, Q \vdash p_2 \leftarrow \text{gate } g \ p_1; C : W \]
If \( C \) is not concrete, then \( p_2 \leftarrow \text{gate } g \ p_1; C \) can step via an \( \eta \) rule. Otherwise, \( C \) is either normal, in which case \( p_2 \leftarrow \text{gate } g \ p_1; C \) is also normal, or \( C \) can take a step, in which case so can \( p_2 \leftarrow \text{gate } g \ p_1; C \) by the structural rule.

(c) Suppose the circuit is
\[ ; \Omega_1 \vdash C : W \quad \Omega_0 \Rightarrow p : W \quad \Omega_0, \Omega_2 \vdash C' : W' \]
\[ ; \Omega_1, Q \vdash p \leftarrow C; C' : W' \]
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.

\[
\begin{array}{c}
\text{output } p' \\
\text{or lift } p_0; C_0 \\
x \leftarrow \text{lift } p_0; C_0
\end{array}
\]
\[
\begin{array}{c}
C' \{p' / p\} \\
p_2 \leftarrow \text{gate } g \ p_1; C_0 \\
x \leftarrow \text{lift } p_0; p_0 \leftarrow C_0; C'
\end{array}
\]

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

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

2. If \( C \) is not concrete, then by an \( \eta \)-expansion, there is some \( p' \) that is concrete for \( W \) and box \( p \Rightarrow C \rightarrow^* \text{box } p' \Rightarrow C \{p' / p\} \). 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 box \( p \Rightarrow C \).

If \( C \) is an output or lifting circuit then it is already normal. If \( C \) is an unboxing operator of the form
\[ \vdash t: \text{Circ}(W_1, W_2) \quad Q \Rightarrow p : W_1 \]
\[ ; Q \vdash \text{unbox } t \ p : W_2 \]
then by the inductive hypothesis, there is some box \( p' \Rightarrow N \) such that \( t \rightarrow^* \text{box } p' \Rightarrow N \), so unbox \( t \ p \rightarrow^* N \ \{p/ p'\} \), which is also normal.

Next, consider a gate application:
\[ g \in G(W_1, W_2) \]
\[ \Omega_1 \Rightarrow p_1 : W_1 \quad \Omega_2 \Rightarrow p_2 : W_2 \quad \Omega_2, Q \vdash C : W \]
\[ ; \Omega_1, Q \vdash p_2 \leftarrow \text{gate } g \ p_1; C : W \]
Again, if \( C \) is concrete, it normalizes by the inductive hypothesis; otherwise there is some \( Q \Rightarrow p_2 : W_2 \) where \( C \{p_2/p_1\} \) normalizes to some \( N \), in which case \( p_2 \leftarrow \text{gate } g \ p_1; C \Rightarrow^* p_2 \leftarrow \text{gate } g \ p_1; N \).

By the inductive hypothesis, there is some \( N \) such that \( C \Rightarrow^* N \). If \( N = \text{output } p', \) then \( p \leftarrow C; C' \Rightarrow^* C' \{p' / p\} \), which normalizes by the inductive hypothesis for \( C' \). If \( N = p_2 \leftarrow \text{gate } g \ p_1; C_0, \) then \( p \leftarrow C_0; C' \) normalizes to some \( N' \) by the inductive hypothesis, and so
\[ p \leftarrow C; C' \Rightarrow^* p_2 \leftarrow \text{gate } g \ p_1; N'. \]
Finally, if \( N = x \leftarrow \text{lift } p; C_0, \) then
\[ p \leftarrow C; C' \Rightarrow x \leftarrow \text{lift } p; p \leftarrow C_0; C', \]
which is immediately normal.

### Appendix B: Soundness of denotational semantics

#### Theorem 11 (Soundness)
If \( Q \vdash C : W \) and \( C \Rightarrow C' \), then
\[ [Q \vdash C : W] = [Q \vdash C' : W] \]

**Proof.** By induction on the typing judgment.

If \( C \) is
\[ ; Q' \vdash C : W \quad \pi : Q \equiv Q' \]
\[ ; Q \vdash C : W \]
and \( C \Rightarrow C' \), then by the inductive hypothesis,
\[ [Q \vdash C : W] = [Q \vdash C' : W] \]
\[ [Q \vdash C : W] \circ [\pi]^* = [Q \vdash C' : W] \]

If \( C \Rightarrow C' \), then by the structural rule with \( t \rightarrow t' \), then, assuming \( \text{HOST} \) is strongly normalizing we have some box \( p' \Rightarrow N \) such that \( t, t' \rightarrow^* \text{box } p' \Rightarrow N \).

Suppose
\[ g \in G(W_1, W_2) \]
\[ \Omega_1 \Rightarrow p_1 : W_1 \quad \Omega_2 \Rightarrow p_2 : W_2 \quad \Omega_2, Q \vdash C : W \]
\[ ; \Omega_1, Q \vdash p_2 \leftarrow \text{gate } g \ p_1; C : W \]
If the circuit steps via a structural rule, the result is immediate. If it steps via an \( \eta \) rule to \( p_2 \leftarrow \text{gate } g \ p_1; C \{p_2 / p_1\} \), then the result follows from the fact that \( [C \{p_2 / p_1\}] = [C] \) (Lemma 10).

Next, consider
\[ ; Q_1 \vdash C : W \quad \Omega_0 \Rightarrow p : W \quad \Omega_0, Q_2 \vdash C_2 : W' \]
\[ ; Q_1, Q_2 \vdash p \leftarrow C_1; C_2 : W' \]
If the circuit steps via a structural rule, the result follows immediately. Otherwise, we know \( C_2 \) is normal, and the circuit stepped via a \( \beta \) or commuting conversion rule. We proceed by a further case analysis on the typing judgment of \( C_1 \).

For a permutation rule \( \pi : Q_1 \equiv Q_1' \), by induction we know that
\[ [Q_1', Q_2 \vdash p \leftarrow C_1; C_2 : W'] = [Q_1', Q_2 \vdash C' : W'] \]
But then
\[ [Q_1, Q_2 \vdash p \leftarrow C_1; C_2 : W'] \]
\[ = [\Omega_0, Q_2 \vdash C_2 : W'] \circ ([Q_1 \vdash C_1 : W] \circ \Gamma') \]
\[ = [\Omega_0, Q_2 \vdash C_2 : W'] \circ ([Q_1' \vdash C_1 : W] \circ \pi^* \circ \Gamma') \]
\[ = [\Omega_0, Q_2 \vdash C_2 : W'] \circ ([Q_1' \vdash C_1 : W] \circ \Gamma^*) \]
\[ = [Q_1', Q_2 \vdash p \leftarrow C_1; C_2 : W'] \circ ([\pi] \circ \Gamma)^* \]
\[ = [Q_1, Q_2 \vdash p \leftarrow C_1; C_2 : W'] \]

\( \square \)
For $C_1 = \text{output } p'$ with $Q_1 \Rightarrow p' : W$, where $p \leftarrow C_1; C_2 \implies C_2 \{p'/p\}$,
we know
\[
\begin{align*}
&[Q_1, Q_2 \vdash p \leftarrow \text{output } p' ; C_2 : W'] \\
&= [Q_0, Q_2 \vdash C_2 : W'] \circ ([Q_1 \vdash \text{output } p' : W] \otimes I^*) \\
&= [Q_0, Q_2 \vdash C_2 : W] \circ (I^* \otimes I^*) \\
&= [Q_0, Q_2 \vdash C_2 : W'] = [Q_1, Q_2 \vdash C_2 \{p'/p\} : W']
\end{align*}
\]
by Lemma 10.

If $C_1$ is
\[
Q'_1 \Rightarrow p_1 : W_1 \\
\text{and } \vdash \omega_1 \Rightarrow p_2 : W_2 \\
\vdash \omega'_2, Q' \vdash C_0 : W
\]
and steps via a commuting conversion
\[
p \leftarrow C_1; C_2 \implies p_2 \leftarrow \text{gate } g p_1; p \leftarrow C_0; C_2
\]
then
\[
\begin{align*}
&[Q'_1, Q', Q_2 \vdash p \leftarrow (p_2 \leftarrow \text{gate } g p_1; C_0); C_2 : W'] \\
&= [Q_0, Q_2 \vdash C_2 : W'] \circ ([Q'_1, Q' \vdash p_2 \leftarrow \text{gate } g p_1; C_0 : W] \otimes I^*) \\
&= [Q_0, Q_2 \vdash C_2 : W] \circ (([Q'_2, Q' : C_0 : W] \otimes I^* \otimes I^*) \circ I^*) \\
&= [Q_0, Q_2 \vdash C_2 : W'] \circ ([Q'_2, Q' \vdash C_0 : W] \otimes I^* \otimes I^*) \\
&= [Q'_1, Q', Q_2 \vdash p_2 \leftarrow \text{gate } g p_1; p \leftarrow C_0; C_2 : W']
\end{align*}
\]
Finally, if $C_1$ is
\[
Q_0 \Rightarrow p_0 : W_0 \quad x ; W_0; Q' \vdash C_0 : W
\]
and steps via a commuting conversion
\[
p \leftarrow C_1; C_2 \implies x \leftarrow \text{lift } p_0; p \leftarrow C_0; C_2
\]
then
\[
\begin{align*}
&[Q_0, Q_1, Q_2 \vdash p \leftarrow (x \leftarrow \text{lift } p_0; C_0); C_2 : W'] \\
&= [Q_0, Q_2 \vdash C_2 : W'] \circ ([Q_0, Q_2 : W] \otimes I^*) \\
&= [Q_2] \circ \left( \sum_{v \in W_0} [Q_0 \vdash \text{output } v : x ; W_0] \otimes (I^* \otimes I^*) \right) \\
&= [C_2] \circ \left( \sum_{v \in W_0} (\text{Circ } v \otimes x) \otimes (I^* \otimes I^*) \right) \\
&= [C_2] \circ \left( \sum_{v \in W_0} (\text{Circ } v \otimes x) \otimes (I^* \otimes I^*) \right) \\
&= \sum_{v \in W_0} [C_2] \circ \left( \text{Circ } v \otimes x \otimes (I^* \otimes I^*) \right)
\end{align*}
\]

Appendix C Correctness of circuit case analysis

Theorem 12. For all terms $t$ of type $\text{ICirc } W_1 \rightarrow W_2$ and $c$ of type $\text{Circ}(W_1, W_2)$, we have:
\[
\begin{align*}
&\text{toICirc } (\text{fromICirc } t) = t \\
&\text{fromICirc } (\text{toICirc } c) = c
\end{align*}
\]
Proof.
Appendix D  Correctness of Circuit Reversal

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

**Theorem 13.** If \( \text{reverse} \ c = \text{Some} \ c' \) then

\[
[c] \circ [c'] = I^* \quad \text{and} \quad [c'] \circ [c] = I^*.
\]

**Proof.** Notice that \([\text{inSeq} \ c \ c'] = [c'] \circ [c]\).

If \( c = \text{box} \ p \Rightarrow \text{output} \ p' \) then it must be the case that \( c' = \text{box} \ p' \Rightarrow \text{output} \ p \). In that case we have \([c] = [c'] = I^*\).

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

\[ p_1 \leftarrow \text{gate} \ g' \ p_2; \text{output} \ (p_1, w') \]

In this case, \([c] = [N] \circ ([g] \otimes I^*)\) and

\[
[c'] = [\text{output} \ (p_1, w')] \circ ([g'] \otimes I^*) \circ [c'']
\]

\[
= ([g'] \otimes I^*) \circ [c'']
\]

Therefore

\[
[c] \circ [c'] = [N] \circ ([g] \otimes I^*) \circ ([g'] \otimes I^*) \circ [c'']
\]

\[
= [N] \circ [c''] = I^*
\]

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

As a corollary, we have

**Corollary.** If \( \text{reverse} \ c_1 = \text{Some} \ c'_1 \) and \( \text{reverse} \ c_2 = \text{Some} \ c'_2 \) 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.