A Proof of Soundness

This Appendix is only for reviewing. If this is accepted, we will remove it, upload a preprint version with the proof to arXiv. The article will refer to the preprint version.

We prove our main theorem (Theorem 16), whose first item is Theorem 9. The proof is close to a proof of soundness of Hoare logic, with a few extra complications due to the presence of first-class functions. We first prove a few lemmas related to `LOOP` (Lemma 11), `ITER` (Lemma 12), predicate `call` (Lemmas 13 and 14), and subtyping (Lemma 15). We often use Theorem 8 implicitly.

Lemma 11. *Suppose IS satisfies*

$$S_1 \vdash \mathit{IS} \Downarrow S_2 \text{ and } \sigma : \Gamma \models S_1 : \{\Upsilon \mid \exists x{:}\mathtt{int}.\varphi \land x \neq 0\} \text{ imply } \sigma : \Gamma \models S_2 : \{x{:}\mathtt{int} \rhd \Upsilon \mid \varphi\} \tag{H.1}$$

for any S_1 and S_2. If

$$S_1 \vdash \mathtt{LOOP}\,\mathit{IS} \Downarrow S_2 \tag{H.2}$$

$$\sigma : \Gamma \models S_1 : \{x{:}\mathtt{int} \rhd \Upsilon \mid \varphi\} \tag{H.3}$$

then $\sigma : \Gamma \models S_2 : \{\Upsilon \mid \exists x{:}\mathtt{int}.\varphi \land x = 0\}$.

Proof. By induction on the derivation of (H.2). We conduct the last rule that derives (H.2), which is either (E-LoopT) or (E-LoopF).

Case (E-LoopT). We have

$$S_1 = i \rhd S \tag{H.4}$$

$$i \neq 0 \tag{H.5}$$

$$S \vdash \mathit{IS} \Downarrow S' \tag{H.6}$$

$$S' \vdash \mathtt{LOOP}\,\mathit{IS} \Downarrow S_2. \tag{H.7}$$

From (H.4), (H.5), and (H.3), we have

$$\sigma : \Gamma \models S : \{\Upsilon \mid \exists x{:}\mathtt{int}.\varphi \land x \neq 0\} \tag{H.8}$$

From (H.1), we have $\sigma : \Gamma \models S' : \{x{:}\mathtt{int} \rhd \Upsilon \mid \varphi\}$. Then, the goal from (H.7), (H.8), and IH.

Case (E-LoopF). We have $S_1 = 0 \rhd S_2$. The goal $\sigma : \Gamma \models S_2 : \{\Upsilon \mid \exists x{:}\mathtt{int}.\varphi \land x = 0\}$ follows from Lemma 10 and (H.3).

□

Lemma 12. *Suppose*

$$x_1 \notin \mathit{fvars}(\varphi) \tag{H.1}$$

$$x_2 \notin \mathit{fvars}(\varphi) \tag{H.2}$$

Suppose also that

$$\begin{aligned} &S_1' \vdash \mathit{IS} \Downarrow S_2' \text{ and } \sigma' : \Gamma, x_2{:}T\,\mathtt{list} \models S_1' : \{x_1{:}T \rhd \Upsilon \mid \exists x{:}T\,\mathtt{list}.\varphi \land x_1 :: x_2 = x\} \text{ imply} \\ &\sigma' : \Gamma, x_2{:}T\,\mathtt{list} \models S_2' : \{\Upsilon \mid \exists x{:}T\,\mathtt{list}.\varphi \land x_2 = x\} \end{aligned} \tag{H.3}$$

for any S_1', S_2', and σ'. If

$$S_1 \vdash \mathtt{ITER}\,\mathit{IS} \Downarrow S_2 \tag{H.4}$$

$$\sigma : \Gamma \models S_1 : \{x{:}T\,\mathtt{list} \rhd \Upsilon \mid \varphi\} \tag{H.5}$$

then $\sigma : \Gamma \models S_2 : \{\Upsilon \mid \exists x{:}T\,\mathtt{list}.\varphi \land x = []\}$.

Proof. By induction on the derivation of (H.4). We conduct case analysis on the last rule that derives (H.4), which is either (E-IterNil) or (E-IterCons).

Case (E-ITERNIL). We have

$$S_1 = [] \triangleright S_2. \tag{H.6}$$

The goal follows from Lemma 10 and (H.5).

Case (E-ITERCONS). We have

$$S_1 = V_1 :: V_2 \triangleright S \tag{H.7}$$

$$V_1 \triangleright S \vdash IS \Downarrow S' \tag{H.8}$$

$$V_2 \triangleright S' \vdash \texttt{ITER}\, IS \Downarrow S_2. \tag{H.9}$$

Therefore, from (H.7), (H.5), and Lemma 10, we have

$$\sigma : \Gamma \models S : \{\Upsilon \mid \exists x{:}T\,\texttt{list}.\varphi \wedge x = V_1 :: V_2\}. \tag{H.10}$$

Therefore, we have $\sigma : \Gamma \models S : \{\Upsilon \mid \exists x{:}T\,\texttt{list}, x_1{:}T, x_2{:}T\,\texttt{list}.\varphi \wedge x = x_1 :: x_2 \wedge x_1 = V_1 \wedge x_2 = V_2\}$ and hence

$$\sigma[x_2 \mapsto V_2] : \Gamma, x_2{:}T\,\texttt{list} \models V_1 \triangleright S : \{x_1{:}T \triangleright \Upsilon \mid \exists x{:}T\,\texttt{list}.\varphi \wedge x = x_1 :: x_2\} \tag{H.11}$$

From (H.3) and (H.8), we have

$$\sigma[x_2 \mapsto V_2] : \Gamma, x_2{:}T\,\texttt{list} \models S' : \{\Upsilon \mid \exists x{:}T\,\texttt{list}.\varphi \wedge x = x_2\}. \tag{H.12}$$

From Lemma 10, we have

$$\sigma : \Gamma \models V_2 \triangleright S' : \{x_2{:}T\,\texttt{list} \triangleright \Upsilon \mid \exists x{:}T\,\texttt{list}.\varphi \wedge x = x_2\}. \tag{H.13}$$

Knowing (H.2), we have

$$\sigma : \Gamma \models V_2 \triangleright S' : \{x{:}T\,\texttt{list} \triangleright \Upsilon \mid \varphi\} \tag{H.14}$$

from (H.13). Now the goal follows from IH, (H.8), and (H.14).

□

Lemma 13. *If*

$$y_1 \neq y_2 \tag{H.1}$$

$$y_1'{:}T_1, y_1{:}T_1 \vdash \varphi_1 : * \tag{H.2}$$

$$y_1'{:}T_1, y_2{:}T_2 \vdash \varphi_2 : * \tag{H.3}$$

$$\langle IS \rangle : T_1 \to T_2 \tag{H.4}$$

$$\left(\begin{array}{l} \textit{For any } V_1, V_2, \sigma, \\ \quad \textit{if } V_1 \triangleright \ddagger \vdash IS \Downarrow V_2 \triangleright \ddagger \textit{ and} \\ \qquad \sigma : y_1'{:}T_1 \models V_1 \triangleright \ddagger : \{y_1{:}T_1 \triangleright \ddagger \mid y_1' = y_1 \wedge \varphi_1\} \\ \quad \textit{then } \sigma : y_1'{:}T_1 \models V_2 \triangleright \ddagger : \{y_2{:}T_2 \triangleright \ddagger \mid \varphi_2\} \end{array}\right) \tag{H.5}$$

then $\Gamma \models \forall y_1'{:}T_1, y_1{:}T_1, y_2{:}T_2. y_1' = y_1 \wedge \varphi_1 \wedge \texttt{call}(\langle IS \rangle, y_1') = y_2 \implies \varphi_2$ *for any* Γ.

Proof. By the definition of the semantics of `call`. □

Lemma 14. *If*

$$V_1 \triangleright \ddagger \vdash IS \Downarrow V_2 \triangleright \ddagger \tag{H.1}$$

$$V_1 : T_1 \tag{H.2}$$

$$V_2 : T_2 \tag{H.3}$$

$$\langle IS \rangle : T_1 \to T_2 \tag{H.4}$$

then $\Gamma \models \texttt{call}(\langle IS \rangle, V_1) = V_2$ *for any* Γ.

— *Proof.* By the definition of the semantics of `call`. □

Lemma 15. *If*

$$\Gamma \vdash \Phi_1 <: \Phi_2 \tag{H.1}$$
$$\sigma : \Gamma \models S : \Phi_1 \tag{H.2}$$

then $\sigma : \Gamma \models S : \Phi_2$.

— *Proof.* Straightforward from Definition 4.

□

Theorem 16 (Soundness). *The following two statements hold.*

(1) If

$$\Gamma \vdash \Phi_1 \; IS \; \Phi_2 \tag{H.1}$$
$$S_1 \vdash IS \Downarrow S_2 \tag{H.2}$$
$$\sigma : \Gamma \models S_1 : \Phi_1 \tag{H.3}$$

then $\sigma : \Gamma \models S_2 : \Phi_2$.

(2) If

$$\Gamma \vdash \Phi_1 \; I \; \Phi_2 \tag{H.4}$$
$$S_1 \vdash I \Downarrow S_2 \tag{H.5}$$
$$\sigma : \Gamma \models S_1 : \Phi_1 \tag{H.6}$$

then $\sigma : \Gamma \models S_2 : \Phi_2$.

— *Proof.* The proof is done by mutual induction on the given derivation of (H.1) and (H.4).

Case (RT-NOP). We have $IS = \{\}$ and $\Phi_1 = \Phi_2$. The last rule that is used to derive (H.2) is (E-NOP). Therefore, we have $S_1 = S_2$, which is followed by (H.3).

Case (RT-SEQ). We have

$$IS = \{I'; IS'\} \tag{H.7}$$
$$\Gamma \vdash \Phi_1 \; I' \; \Phi' \tag{H.8}$$
$$\Gamma \vdash \Phi' \; IS' \; \Phi_2 \tag{H.9}$$

for some I', IS', and Φ'. The last rule that derives (H.2) is (E-SEQ). Therefore, we have

$$S_1 \vdash I' \Downarrow S' \tag{H.10}$$
$$S' \vdash IS' \Downarrow S_2 \tag{H.11}$$

for some S'. Now we have

$$\sigma : \Gamma \models S' : \Phi' \tag{H.12}$$

by applying IH to (H.8), (H.10) and (H.3). Then, the goal follows by applying IH to (H.9), (H.11) and (H.12).

Case (RT-DIP). We have

$$I = \mathtt{DIP}\, \mathit{IS} \tag{H.13}$$
$$\Phi_1 = \{x{:}T \rhd \Upsilon \mid \varphi\} \tag{H.14}$$
$$\Phi_2 = \{x{:}T \rhd \Upsilon' \mid \varphi'\} \tag{H.15}$$
$$\Gamma, x{:}T \vdash \{\Upsilon \mid \varphi\}\ \mathit{IS}\ \{\Upsilon' \mid \varphi'\} \tag{H.16}$$

for some IS, x, T, Υ, Υ', φ, and φ'. The last rule that derives (H.5) is (E-DIP). Therefore, we have

$$S_1 = V \rhd S_1' \tag{H.17}$$
$$S_2 = V \rhd S_2' \tag{H.18}$$
$$S_1' \vdash \mathit{IS} \Downarrow S_2' \tag{H.19}$$

for some V, S_1', and S_2'. By Lemma 10, we have

$$\sigma[x \mapsto V] : \Gamma, x{:}T \models S_1' : \{\Upsilon \mid \varphi\} \tag{H.20}$$

from (H.6), (H.14), and (H.17). By applying IH to (H.16), (H.19), and (H.20), we have

$$\sigma[x \mapsto V] : \Gamma, x{:}T \models S_2' : \{\Upsilon' \mid \varphi'\}. \tag{H.21}$$

Therefore, $\sigma : \Gamma \models V \rhd S_2' : \{x{:}T \rhd \Upsilon' \mid \varphi'\}$ follows from (SEM-PUSH) and (H.21).

Case (RT-DROP). We have

$$I = \mathtt{DROP} \tag{H.22}$$
$$\Phi_1 = \{x{:}T \rhd \Upsilon \mid \varphi\} \tag{H.23}$$
$$\Phi_2 = \{\Upsilon \mid \exists x{:}T.\varphi\} \tag{H.24}$$

for some x, T, Υ, and φ. The last rule that derives (H.5) is (E-DROP). Therefore, we have

$$S_1 = V \rhd S_2 \tag{H.25}$$

for some V. From (H.6), (H.25), and Lemma 10, we have $\sigma : \Gamma \models S_2 : \{\Upsilon \mid \exists x{:}T.\varphi \wedge x = V\}$ and hence $\sigma : \Gamma \models S_2 : \{\Upsilon \mid \exists x{:}T.\varphi\}$ as required.

Case (RT-DUP). We have

$$I = \mathtt{DUP} \tag{H.26}$$
$$\Phi_1 = \{x{:}T \rhd \Upsilon \mid \varphi\} \tag{H.27}$$
$$\Phi_2 = \{x'{:}T \rhd x{:}T \rhd \Upsilon \mid \varphi \wedge x' = x\} \tag{H.28}$$
$$x' \notin \mathrm{dom}(\Gamma, \widehat{x{:}T \rhd \Upsilon}) \tag{H.29}$$

for some x, x', T, Υ, and φ. The last rule that derives (H.5) is (E-DUP). Therefore, we have

$$S_1 = V \rhd S \tag{H.30}$$
$$S_2 = V \rhd V \rhd S \tag{H.31}$$

for some V and S. By (H.6), we have $\sigma[x \mapsto V] : \Gamma, x{:}T \models S : \{\Upsilon \mid \varphi\}$ and hence $\sigma[x \mapsto V][x' \mapsto V] : \Gamma, x{:}T, x'{:}T \models S : \{\Upsilon \mid \varphi\}$. Since $\sigma[x \mapsto V][x' \mapsto V] : \Gamma, x{:}T, x'{:}T \models \varphi \implies (\varphi \wedge x = x')$, we have $\sigma[x \mapsto V][x' \mapsto V] : \Gamma, x{:}T, x'{:}T \models S : \{\Upsilon \mid \varphi \wedge x = x'\}$. Therefore, we have $\sigma : \Gamma \models S_2 : \{\Upsilon \mid \varphi \wedge x = x'\}$ as required.

Case (RT-Swap). We have

$$I = \mathtt{SWAP} \tag{H.32}$$

$$\varPhi_1 = \{x{:}T \triangleright x'{:}T \triangleright \Upsilon \mid \varphi\} \tag{H.33}$$

$$\varPhi_2 = \{x'{:}T \triangleright x{:}T \triangleright \Upsilon \mid \varphi\} \tag{H.34}$$

for some x, x', T, Υ, and φ. The last rule that derives (H.5) is (E-Swap). Therefore, we have

$$S_1 = V \triangleright V' \triangleright S \tag{H.35}$$

$$S_2 = V' \triangleright V \triangleright S \tag{H.36}$$

for some V, V', and S. By (H.6), we have $\sigma[x \mapsto V][x' \mapsto V'] : \varGamma, x{:}T, x'{:}T \models S : \{\Upsilon \mid \varphi\}$. Since $x \neq x'$, we have $\sigma[x' \mapsto V'][x \mapsto V] : \varGamma, x'{:}T, x{:}T \models S : \{\Upsilon \mid \varphi\}$. Therefore, we have $\sigma : \varGamma \models S_2 : \{\Upsilon \mid \varphi\}$.

Case (RT-Push). We have

$$I = \mathtt{PUSH}\, T\, V \tag{H.37}$$

$$\varPhi_1 = \{\Upsilon \mid \varphi\} \tag{H.38}$$

$$\varPhi_2 = \{x{:}T \triangleright \Upsilon \mid \varphi \wedge x = V\} \tag{H.39}$$

$$V : T \tag{H.40}$$

$$x \notin \mathrm{dom}(\varGamma, \widehat{\Upsilon}) \tag{H.41}$$

for some x, T, Υ, φ, and V. The last rule that derives (H.6) is (E-Push). Therefore, we have

$$S_2 = V \triangleright S_1. \tag{H.42}$$

To show $\sigma : \varGamma \models S_2 : \{x{:}T \triangleright \Upsilon \mid \varphi \wedge x = V\}$, it suffices to show $\sigma[x \mapsto V] : \varGamma, x{:}T \models S_1 : \{\Upsilon \mid \varphi \wedge x = V\}$ from (Sem-Push), which follows from $\sigma : \varGamma \models S_1 : \{\Upsilon \mid \varphi\}$, (H.41), and $\sigma[x \mapsto V] : \varGamma, x{:}T \models \varphi \implies (\varphi \wedge x = V)$.

Case (RT-Not). We have

$$I = \mathtt{NOT} \tag{H.43}$$

$$\varPhi_1 = \{x{:}\mathtt{int} \triangleright \Upsilon \mid \varphi\} \tag{H.44}$$

$$\varPhi_2 = \{x'{:}\mathtt{int} \triangleright \Upsilon \mid \exists x{:}\mathtt{int}.\varphi \wedge (x \neq 0 \wedge x' = 0 \vee x = 0 \wedge x' = 1)\} \tag{H.45}$$

$$x' \notin \mathrm{dom}(\varGamma, \widehat{x{:}\mathtt{int} \triangleright \Upsilon}) \tag{H.46}$$

for some x, Υ, and φ. The last rule that derives (H.5) is either (E-NotT) or (E-NotF). We only show the case of (E-NotT); (E-NotF) is similar. In this case, we have

$$S_1 = i \triangleright S \tag{H.47}$$

$$i \neq 0 \tag{H.48}$$

$$S_2 = 0 \triangleright S. \tag{H.49}$$

for some i and S. By (H.6), we have

$$\sigma[x \mapsto i] : \varGamma, x{:}T \models S : \{\Upsilon \mid \varphi\}. \tag{H.50}$$

From Lemma 10, we have

$$\sigma : \varGamma \models S : \{\Upsilon \mid \exists x{:}T.\varphi \wedge x = i\}. \tag{H.51}$$

From $i \neq 0$, we have $\sigma : \varGamma \models S : \{\Upsilon \mid \exists x{:}T.\varphi \wedge x \neq 0\}$. From (H.46), we have $\sigma[x' \mapsto 0] : \varGamma, x'{:}T \models S : \{\Upsilon \mid \exists x{:}T.\varphi \wedge x \neq 0\}$. From $\sigma[x' \mapsto 0] : \varGamma, x'{:}T \models (\exists x{:}T.\varphi \wedge x \neq 0) \implies (\exists x{:}T.\varphi \wedge x \neq 0 \wedge x' = 0)$, we have $\sigma[x' \mapsto 0] : \varGamma, x'{:}T \models S : \{\Upsilon \mid \exists x{:}T.\varphi \wedge x \neq 0 \wedge x' = 0\}$. Therefore, we have $\sigma : \varGamma \models 0 \triangleright S : \{x'{:}T \triangleright \Upsilon \mid \exists x{:}T.\varphi \wedge x \neq 0 \wedge x' = 0\}$, which is followed by $\sigma : \varGamma \models 0 \triangleright S : \{x'{:}T \triangleright \Upsilon \mid \exists x{:}T.\varphi \wedge ((x \neq 0 \wedge x' = 0) \vee (x = 0 \wedge x' \neq 1))\}$ as required.

Case (RT-ADD). We have We have

$$I = \mathtt{ADD} \tag{H.52}$$

$$\Phi_1 = \{x_1{:}\mathtt{int} \triangleright x_2{:}\mathtt{int} \triangleright \Upsilon \mid \varphi\} \tag{H.53}$$

$$\Phi_2 = \{x_3{:}\mathtt{int} \triangleright \Upsilon \mid \exists x_1{:}\mathtt{int}, x_2{:}\mathtt{int}. \varphi \wedge x_1 + x_2 = x_3\} \tag{H.54}$$

$$x_3 \notin \mathrm{dom}(\Gamma, \widehat{x_1{:}\mathtt{int} \triangleright x_2{:}\mathtt{int} \triangleright \Upsilon}) \tag{H.55}$$

for some x_1, x_2, x_3, Υ, and φ. The last rule that derives (H.5) is (E-ADD). Therefore,

$$S_1 = i_1 \triangleright i_2 \triangleright S \tag{H.56}$$

$$S_2 = i_3 \triangleright S \tag{H.57}$$

$$i_1 + i_2 = i_3 \tag{H.58}$$

for some i_1, i_2, i_3, and S. By (H.6), we have

$$\sigma[x_1 \mapsto i_1][x_2 \mapsto i_2] : \Gamma, x_1{:}\mathtt{int}, x_2{:}\mathtt{int} \models S : \{\Upsilon \mid \varphi\}. \tag{H.59}$$

From (H.55), we have

$$\sigma[x_1 \mapsto i_1][x_2 \mapsto i_2][x_3 \mapsto i_3] : \Gamma, x_1{:}\mathtt{int}, x_2{:}\mathtt{int}, x_3{:}\mathtt{int} \models S : \{\Upsilon \mid \varphi\}. \tag{H.60}$$

From $\sigma[x_1 \mapsto i_1][x_2 \mapsto i_2][x_3 \mapsto i_3] : \Gamma, x_1{:}\mathtt{int}, x_2{:}\mathtt{int}, x_3{:}\mathtt{int} \models \varphi \implies \varphi \wedge x_1 + x_2 = x_3$, we have

$$\sigma[x_1 \mapsto i_1][x_2 \mapsto i_2][x_3 \mapsto i_3] : \Gamma, x_1{:}\mathtt{int}, x_2{:}\mathtt{int}, x_3{:}\mathtt{int} \models S : \{\Upsilon \mid \varphi \wedge x_1 + x_2 = x_3\}. \tag{H.61}$$

and therefore $\sigma[x_1 \mapsto i_1][x_2 \mapsto i_2] : \Gamma, x_1{:}\mathtt{int}, x_2{:}\mathtt{int} \models i_3 \triangleright S : \{x_3{:}\mathtt{int} \triangleright \Upsilon \mid \varphi \wedge x_1 + x_2 = x_3\}$. By Lemma 10, we have $\sigma : \Gamma \models i_3 \triangleright S : \{x_3{:}\mathtt{int} \triangleright \Upsilon \mid \exists x_1{:}\mathtt{int}, x_2{:}\mathtt{int}. \varphi \wedge x_1 + x_2 = x_3\}$ as required.

Case (RT-PAIR). Similar to the case for (RT-ADD).

Case (RT-CAR). We have

$$I = \mathtt{CAR} \tag{H.62}$$

$$\Phi_1 = \{x{:}T_1 \times T_2 \triangleright \Upsilon \mid \varphi\} \tag{H.63}$$

$$\Phi_2 = \{x_1{:}T_1 \triangleright \Upsilon \mid \exists x{:}T_1 \times T_2, x_2{:}T_2. \varphi \wedge x = (x_1, x_2)\} \tag{H.64}$$

$$x_1 \neq x_2 \tag{H.65}$$

$$x_1 \notin \mathrm{dom}(\Gamma, \widehat{x{:}T_1 \times T_2 \triangleright \Upsilon}) \tag{H.66}$$

$$x_2 \notin \mathrm{dom}(\Gamma, \widehat{x{:}T_1 \times T_2 \triangleright \Upsilon}) \tag{H.67}$$

for some x, x_1, x_2, T_1, T_2, Υ, and φ. The last rule that derives (H.5) is (E-CAR). Therefore,

$$S_1 = (V_1, V_2) \triangleright S \tag{H.68}$$

$$S_2 = V_1 \triangleright S \tag{H.69}$$

for some V_1, V_2, and S. By (H.6), we have

$$\sigma[x \mapsto (V_1, V_2)] : \Gamma, x{:}T_1 \times T_2 \models S : \{\Upsilon \mid \varphi\} \tag{H.70}$$

and hence

$$\sigma : \Gamma \models S : \{\Upsilon \mid \exists x{:}T_1 \times T_2. \varphi \wedge x = (V_1, V_2)\}. \tag{H.71}$$

$\sigma : \Gamma \models S : \{\Upsilon \mid \exists x{:}T_1 \times T_2. \varphi \wedge x = (V_1, V_2)\}$ implies $\sigma : \Gamma \models S : \{\Upsilon \mid \exists x{:}T_1 \times T_2, x_1{:}T_1, x_2{:}T_2. \varphi \wedge x = (x_1, x_2) \wedge x_1 = V_1 \wedge x_2 = V_2\}$. Therefore, $\sigma : \Gamma \models S : \{\Upsilon \mid \exists x_1{:}T_1.(\exists x{:}T_1 \times T_2, x_2{:}T_2. \varphi) \wedge x_1 = V_1\}$, which implies $\sigma : \Gamma \models V_1 \triangleright S : \{\Upsilon \mid \exists x{:}T_1 \times T_2, x_2{:}T_2. \varphi\}$ as required.

Case (RT-CDR). Similar to the case for (RT-CAR).

Case (RT-NIL). Similar to the case for (RT-PUSH).

Case (RT-CONS). Similar to the case for (RT-PAIR).

Case (RT-IF). We have

$$I = \mathtt{IF}\, IS_1\, IS_2 \tag{H.72}$$

$$\Phi_1 = \{x{:}\mathtt{int} \triangleright \Upsilon \mid \varphi\} \tag{H.73}$$

$$\Gamma \vdash \{\Upsilon \mid \exists x{:}\mathtt{int}.\varphi \wedge x \neq 0\}\; IS_1\; \Phi_2 \tag{H.74}$$

$$\Gamma \vdash \{\Upsilon \mid \exists x{:}\mathtt{int}.\varphi \wedge x = 0\}\; IS_2\; \Phi_2 \tag{H.75}$$

for some IS_1, IS_2, x, Υ, and φ. The last rule that derives (H.5) is (E-IFT) or (E-IFF). We conduct case analysis.

SCase (E-IFT). For some i and S,

$$i \neq 0 \tag{H.76}$$

$$S_1 = i \triangleright S \tag{H.77}$$

$$S \vdash IS_1 \Downarrow S_2. \tag{H.78}$$

From (H.6), (H.73), (H.77), and Lemma 10, we have

$$\sigma : \Gamma \models S : \{\Upsilon \mid \exists x{:}\mathtt{int}.\varphi \wedge x = i\}. \tag{H.79}$$

From (H.76), we have

$$\sigma : \Gamma \models S : \{\Upsilon \mid \exists x{:}\mathtt{int}.\varphi \wedge x \neq 0\}. \tag{H.80}$$

Then, the goal follows From IH and (H.74).

SCase (E-IFF). Similar to the case for (E-IFT).

Case (RT-LOOP). We have

$$I = \mathtt{LOOP}\, IS \tag{H.81}$$

$$\Phi_1 = \{x{:}\mathtt{int} \triangleright \Upsilon \mid \varphi\} \tag{H.82}$$

$$\Phi_2 = \{\Upsilon \mid \exists x{:}\mathtt{int}.\varphi \wedge x = 0\} \tag{H.83}$$

$$\Gamma \vdash \{\Upsilon \mid \exists x{:}\mathtt{int}.\varphi \wedge x \neq 0\}\; IS\; \{x{:}\mathtt{int} \triangleright \Upsilon \mid \varphi\} \tag{H.84}$$

$$S_1 = i \triangleright S \tag{H.85}$$

for some IS, x, Υ, S, and φ. By IH and (H.84), we have

$$\text{For any } S_1', S_2',\ \text{if } S_1' \vdash IS \Downarrow S_2' \text{ and } \sigma : \Gamma \models S_1' : \{\Upsilon \mid \exists x{:}\mathtt{int}.\varphi \wedge x \neq 0\}, \\ \text{then } \sigma : \Gamma \models S_2' : \{x{:}\mathtt{int} \triangleright \Upsilon \mid \varphi\}. \tag{H.86}$$

Then, the goal follows from Lemma 11, (H.5), (H.6), (H.81), (H.82) and (H.86).

Case (RT-IFCONS). Similar to the case for (RT-IF).

Case (RT-ITER). We have

$$I = \texttt{ITER}\,IS \tag{H.87}$$

$$\Phi_1 = \{x{:}T\,\texttt{list} \triangleright \Upsilon \mid \varphi\} \tag{H.88}$$

$$\Phi_2 = \{\Upsilon \mid \exists x{:}T\,\texttt{list}.\varphi \land x = []\} \tag{H.89}$$

$$\Gamma, x_2{:}T\,\texttt{list} \vdash \{x_1{:}T \triangleright \Upsilon \mid \exists x{:}T\,\texttt{list}.\varphi \land x_1 :: x_2 = x\}\; IS\; \{\Upsilon \mid \exists x{:}T\,\texttt{list}.\varphi \land x_2 = x\} \tag{H.90}$$

$$x_1 \neq x_2 \tag{H.91}$$

$$x_1 \notin \mathrm{dom}(\Gamma, x{:}\widehat{T\,\texttt{list}} \triangleright \Upsilon) \tag{H.92}$$

$$x_2 \notin \mathrm{dom}(\Gamma, x{:}\widehat{T\,\texttt{list}} \triangleright \Upsilon) \tag{H.93}$$

for some IS, x, x_1, x_2, T, Υ, and φ. From IH and (H.90), we have

$$\begin{aligned} &\text{For any } S_1', S_2', \sigma',\ \text{if } S_1' \vdash IS \Downarrow S_2' \text{ and } \sigma' : \Gamma, x_2{:}T\,\texttt{list} \models S_1' : \{x_1{:}T \triangleright \Upsilon \mid \exists x{:}T\,\texttt{list}.\varphi \land x_1 :: x_2 = x\},\\ &\qquad\qquad\text{then } \sigma' : \Gamma, x_2{:}T\,\texttt{list} \models S_2' : \{\Upsilon \mid \exists x{:}T\,\texttt{list}.\varphi \land x_2 = x\}. \end{aligned} \tag{H.94}$$

Then, the goal follows from Lemma 12. (H.93), and (H.94).

Case (RT-LAMBDA). Since the last rule that derive (H.5) is (E-LAMBDA), we have

$$I = \texttt{LAMBDA}\,T_1\,T_2\,IS \tag{H.95}$$

$$\Phi_1 = \{\Upsilon \mid \varphi\} \tag{H.96}$$

$$\Phi_2 = \{x{:}T_1 \to T_2 \triangleright \Upsilon \mid \varphi \land \forall y_1'{:}T_1, y_1{:}T_1, y_2{:}T_2.y_1' = y_1 \land \varphi_1 \land \texttt{call}(x, y_1') = y_2 \implies \varphi_2\} \tag{H.97}$$

$$y_1'{:}T_1 \vdash \{y_1{:}T_1 \triangleright \ddagger \mid y_1' = y_1 \land \varphi_1\}\; IS\; \{y_2{:}T_2 \triangleright \ddagger \mid \varphi_2\} \tag{H.98}$$

$$x \notin \mathrm{dom}(\Gamma, \widehat{\Upsilon}) \cup \{y_1, y_1', y_2\} \tag{H.99}$$

$$y_1 \neq y_1' \tag{H.100}$$

$$y_1'{:}T_1, y_1{:}T_1 \vdash \varphi_1 : * \tag{H.101}$$

$$S_2 = \langle IS \rangle \triangleright S_1 \tag{H.102}$$

for some IS, x, y_1, y_1', y_2, T_1, T_2, Υ, φ, φ_1, and φ_2. From IH and (H.98), we have

$$\begin{aligned} &\text{For any } V_1, V_2, \sigma,\ \text{if } V_1 \triangleright \ddagger \vdash IS \Downarrow V_2 \triangleright \ddagger \text{ and } \sigma : y_1'{:}T_1 \models V_1 \triangleright \ddagger : \{y_1{:}T_1 \triangleright \ddagger \mid y_1' = y_1 \land \varphi_1\},\\ &\qquad\qquad\text{then } \sigma : y_1'{:}T_1 \models V_2 \triangleright \ddagger : \{y_2{:}T_2 \triangleright \ddagger \mid \varphi_2\}. \end{aligned} \tag{H.103}$$

By Lemma 13, (H.100), (H.101), (H.103), (H.91), and (H.92), we have

$$\Gamma, \widehat{\Upsilon} \models \forall y_1'{:}T_1, y_1{:}T_1, y_2{:}T_2.y_1' = y_1 \land \varphi_1 \land \texttt{call}(\langle IS \rangle, y_1') = y_2 \implies \varphi_2 \tag{H.104}$$

and hence, from (H.6), (H.96), and (H.104), we have

$$\sigma : \Gamma \models S_1 : \{\Upsilon \mid \varphi \land \forall y_1'{:}T_1, y_1{:}T_1, y_2{:}T_2.y_1' = y_1 \land \varphi_1 \land \texttt{call}(\langle IS \rangle, y_1') = y_2 \implies \varphi_2\}. \tag{H.105}$$

By (H.99), and (H.105), we have

$$\begin{aligned} &\sigma : \Gamma \models S_1 : \{\Upsilon \mid \exists x{:}T_1 \to T_2.(\varphi \land\\ &\qquad\qquad \forall y_1'{:}T_1, y_1{:}T_1, y_2{:}T_2.y_1' = y_1 \land \varphi_1 \land \texttt{call}(x, y_1') = y_2 \implies \varphi_2) \land x = \langle IS \rangle\}. \end{aligned} \tag{H.106}$$

Therefore, from Lemma 10 and (H.106), we have

$$\begin{aligned} &\sigma : \Gamma \models \langle IS \rangle \triangleright S_1 : \{x{:}T_1 \to T_2 \triangleright \Upsilon \mid \varphi \land\\ &\qquad\qquad\qquad\qquad \forall y_1'{:}T_1, y_1{:}T_1, y_2{:}T_2.y_1' = y_1 \land \varphi_1 \land \texttt{call}(x, y_1') = y_2 \implies \varphi_2\} \end{aligned}$$

as required.

Case (RT-EXEC). We have

$$I = \texttt{EXEC} \tag{H.107}$$

$$\Phi_1 = \{x_1{:}T_1 \rhd x_2{:}T_1 \to T_2 \rhd \Upsilon \mid \varphi\} \tag{H.108}$$

$$\Phi_2 = \{x_3{:}T_2 \rhd \Upsilon \mid \exists x_1{:}T_1, x_2{:}T_1 \to T_2.\varphi \wedge \texttt{call}(x_2, x_1) = x_3\} \tag{H.109}$$

$$x_3 \notin \mathrm{dom}(\Gamma, \widehat{x_1{:}T_1 \rhd x_2{:}T_1 \to T_2 \rhd \Upsilon}) \tag{H.110}$$

for some x_1, x_2, x_3, T_1, T_2, Υ, and φ. Since the last rule that derives (H.5) is (E-EXEC), we have

$$S_1 = V_1 \rhd \langle IS \rangle \rhd S \tag{H.111}$$

$$S_2 = V_2 \rhd S \tag{H.112}$$

$$V_1 \rhd \ddagger \vdash IS \Downarrow V_2 \rhd \ddagger \tag{H.113}$$

for some V_1, V_2, IS, and S. By (H.6), (H.108), and (H.111), we have

$$\sigma : \Gamma \models S : \{\Upsilon \mid \exists x_2{:}T_1 \to T_2.(\exists x_1{:}T_1.\varphi \wedge x_1 = V_1) \wedge x_2 = \langle IS \rangle\}. \tag{H.114}$$

By Lemma 14, (H.113), (H.105), and (H.51), we have

$$\Gamma, \widehat{\Upsilon} \models \texttt{call}(\langle IS \rangle, V_1) = V_2. \tag{H.115}$$

Therefore, from (H.114), and (H.115), we have

$$\sigma : \Gamma \models S : \{\Upsilon \mid (\exists x_2{:}T_1 \to T_2.(\exists x_1{:}T_1.\varphi \wedge x_1 = V_1) \wedge x_2 = \langle IS \rangle) \wedge \texttt{call}(\langle IS \rangle, V_1) = V_2\}. \tag{H.116}$$

From (H.110) and (H.116), we have $\sigma : \Gamma \models S : \{\Upsilon \mid \exists x_3{:}T_2.(\exists x_1{:}T_1, x_2{:}T_1 \to T_2.\varphi \wedge \texttt{call}(x_2, x_1) = x_3) \wedge x_3 = V_2\}$ and hence $\sigma : \Gamma \models V_2 \rhd S : \{x_3{:}T_2 \rhd \Upsilon \mid (\exists x_1{:}T_1, x_2{:}T_1 \to T_2.\varphi \wedge \texttt{call}(x_2, x_1) = x_3)\}$ as required.

Case (RT-TRANSFERTOKENS). We have

$$I = \texttt{TRANSFER\_TOKENS}\, T \tag{H.117}$$

$$\Phi_1 = \{x_1{:}T \rhd x_2{:}\texttt{int} \rhd x_3{:}\texttt{address} \rhd \Upsilon \mid \varphi\} \tag{H.118}$$

$$\Phi_2 = \{x_4{:}\texttt{operation} \rhd \Upsilon \mid \exists x_1{:}T, x_2{:}\texttt{int}, x_3{:}\texttt{address}.\varphi \wedge x_4 = \texttt{Transfer}(x_1, x_2, x_3)\} \tag{H.119}$$

$$x_4 \notin \mathrm{dom}(\Gamma, \widehat{x_1{:}T \rhd x_2{:}\texttt{int} \rhd x_3{:}\texttt{address} \rhd \Upsilon}) \tag{H.120}$$

for some x_1, x_2, x_3, x_4, T, Υ, and φ. The last rule that derives (H.5) is (E-TRANSFERTOKENS); therefore

$$S_1 = V \rhd i \rhd a \rhd S \tag{H.121}$$

$$S_2 = \texttt{Transfer}(V, i, a) \rhd S \tag{H.122}$$

for some V, i, a, and S. By (H.6), (H.118), and (H.121), we have

$$\sigma : \Gamma \models S : \{\Upsilon \mid \exists x_3{:}\texttt{address}.(\exists x_2{:}\texttt{int}.(\exists x_1{:}T.\varphi \wedge x_1 = V) \wedge x_2 = i) \wedge x_3 = a\}. \tag{H.123}$$

By (H.120) and (H.123), we have

$$\begin{aligned} \sigma : \Gamma \models S : \{\Upsilon \mid \exists x_4{:}\texttt{operation}.(&\exists x_1{:}T, x_2{:}\texttt{int}, x_3{:}\texttt{address}.\varphi \wedge \\ &x_4 = \texttt{Transfer}(x_1, x_2, x_3)) \wedge x_4 = \texttt{Transfer}(V, i, a)\}. \end{aligned} \tag{H.124}$$

Therefore, we have

$$\begin{aligned} \sigma : \Gamma \models \texttt{Transfer}(V, i, a) \rhd S : \{x_4{:}\texttt{operation} \rhd \Upsilon \mid (&\exists x_1{:}T, x_2{:}\texttt{int}, x_3{:}\texttt{address}.\varphi \wedge \\ &x_4 = \texttt{Transfer}(x_1, x_2, x_3))\} \end{aligned}$$

as required.

$$\frac{}{[\,] \rhd V \rhd S \vdash \texttt{MAP}\,\mathit{IS} \searrow V \rhd S}\ (\text{E-MAPINIL})$$

$$\frac{V_1 \rhd S \vdash \mathit{IS} \Downarrow V_1' \rhd S' \qquad V_2 \rhd V @ [V_1'] \rhd S' \vdash \texttt{MAP}\,\mathit{IS} \searrow V' \rhd S''}{V_1 :: V_2 \rhd V \rhd S \vdash \texttt{MAP}\,\mathit{IS} \searrow V' \rhd S''}\ (\text{E-MAPICONS})$$

Fig. 14 Accumulating semantics of `MAP`

Case (RT-SUB). We have

$$\Gamma \vdash \Phi_1 <: \Phi_1' \tag{H.125}$$

$$\Gamma \vdash \Phi_2' <: \Phi_2 \tag{H.126}$$

$$\Gamma \vdash \Phi_1'\ I\ \Phi_2' \tag{H.127}$$

for some Φ_1' and Φ_2'. By Lemma 15, (H.6), and (H.125), we have

$$\sigma : \Gamma \models S_1 : \Phi_1'. \tag{H.128}$$

By IH, (H.127), (H.5), and (H.128), we have

$$\sigma : \Gamma \models S_2 : \Phi_2'. \tag{H.129}$$

Then, the goal follows from Lemma 15. □

B Soundness for `MAP`

Here, we show how to prove soundness of Mini-Michelson with `MAP` instruction. The goal of this section is to show Lemma 20, which is similar to Lemma 11 and 12. Once we prove the property, it is straightforward to modify Theorem 16.

Unfortunately, however, Lemma 20 cannot be shown similarly, called *direct way* here, to Lemma 11 or 12. The main reason is that the pre-condition of (RT-MAP) is not a loop invariant. As a result, we cannot apply an induction hypothesis during a proof in the direct way.

To solve the problem, we take an *indirect way*. Firstly, we give an alternative semantics, called *accumulating* semantics, of `MAP` as Figure 14, where a resulting list is explicitly held in the second from the top of the stack. Note that using the original semantics in the first premise is intentional, which minimizes modification on the formalization. Next, we show Lemma 18, which says that the accumulating semantics can simulate the original semantics. At the same time, we show Lemma 19, which is similar to Lemma 20 but for the accumulating semantics. The problematic condition $z' = [\,]$ is dispelled into a stack in the accumulating semantics. So, Lemma 19 can be shown similarly to Lemma 11 or 12. Finally, we can show Lemma 20 with lemmas shown.

Lemma 17 (Accumulator). *If $V \rhd V_1 \rhd S \vdash \texttt{MAP}\,\mathit{IS} \searrow V' \rhd S'$, then there exists V'' such that $V' = V_1 @ V''$ and $V \rhd V_2 \rhd S \vdash \texttt{MAP}\,\mathit{IS} \searrow V_2 @ V'' \rhd S'$ for any V_2.*

Proof. The proof is done by induction on the given derivation. □

Lemma 18 (Accumulating semantics can derive a simulation of normal semantics). *If $V \rhd S_1 \vdash \texttt{MAP}\,\mathit{IS} \Downarrow S_2$, then $V \rhd [\,] \rhd S_1 \vdash \texttt{MAP}\,\mathit{IS} \searrow S_2$.*

Proof. The proof is done by induction on the given derivation. In the induction step, we can have the goal by using Lemma 17. □

Lemma 19 (Soundness of accumulating semantics). *Suppose IS satisfies*

$$\begin{aligned}&S_1' \vdash \mathit{IS} \Downarrow S_2' \textit{ and}\\ &\sigma' : \varGamma, x_2{:}T\,\mathtt{list}, y_2{:}T\,\mathtt{list} \models S_1' : \{x_1{:}T \triangleright \varUpsilon \mid \exists z{:}T\,\mathtt{list}, z'{:}T\,\mathtt{list}.\varphi \wedge z = x_1 :: x_2 \wedge z' = y_2\} \textit{ imply}\\ &\sigma' : \varGamma, x_2{:}T\,\mathtt{list}, y_2{:}T\,\mathtt{list} \models S_2' : \{y_1{:}T \triangleright \varUpsilon \mid \exists z{:}T\,\mathtt{list}, z'{:}T\,\mathtt{list}.\varphi \wedge z = x_2 \wedge z' = y_2 @ [y_1]\}\end{aligned} \tag{H.1}$$

for any S_1', S_2', and σ'. If

$$S_1 \vdash \mathtt{MAP}\,\mathit{IS} \searrow S_2 \tag{H.2}$$

$$\sigma : \varGamma \models S_1 : \{z{:}T\,\mathtt{list} \triangleright z'{:}T\,\mathtt{list} \triangleright \varUpsilon \mid \varphi\} \tag{H.3}$$

then $\sigma : \varGamma \models S_2 : \{z'{:}T\,\mathtt{list} \triangleright \varUpsilon \mid \exists z{:}T\,\mathtt{list}.\varphi \wedge z = []\}$.

Proof. The proof is done by induction on the given derivation of (H.2). □

Lemma 20 (Soundness of MAP). *Suppose IS satisfies*

$$\begin{aligned}&S_1' \vdash \mathit{IS} \Downarrow S_2' \textit{ and}\\ &\sigma' : \varGamma, x_2{:}T\,\mathtt{list}, y_2{:}T\,\mathtt{list} \models S_1' : \{x_1{:}T \triangleright \varUpsilon \mid \exists z{:}T\,\mathtt{list}, z'{:}T\,\mathtt{list}.\varphi \wedge z = x_1 :: x_2 \wedge z' = y_2\} \textit{ imply}\\ &\sigma' : \varGamma, x_2{:}T\,\mathtt{list}, y_2{:}T\,\mathtt{list} \models S_2' : \{y_1{:}T \triangleright \varUpsilon \mid \exists z{:}T\,\mathtt{list}, z'{:}T\,\mathtt{list}.\varphi \wedge z = x_2 \wedge z' = y_2 @ [y_1]\}\end{aligned} \tag{H.1}$$

for any S_1', S_2', and σ'. If

$$S_1 \vdash \mathtt{MAP}\,\mathit{IS} \Downarrow S_2 \tag{H.2}$$

$$\sigma : \varGamma \models S_1 : \{z{:}T\,\mathtt{list} \triangleright \varUpsilon \mid \exists z'{:}T\,\mathtt{list}.\varphi \wedge z' = []\} \tag{H.3}$$

then $\sigma : \varGamma \models S_2 : \{z'{:}T\,\mathtt{list} \triangleright \varUpsilon \mid \exists z{:}T\,\mathtt{list}.\varphi \wedge z = []\}$.

Proof. By (H.2), we have

$$S_1 = V \triangleright S_1' \tag{H.4}$$

for some V and S_1'. So, we have

$$V \triangleright [] \triangleright S_1' \vdash \mathtt{MAP}\,\mathit{IS} \searrow S_2 \tag{H.5}$$

by Lemma 18. Also, (H.3) turns into

$$\sigma : \varGamma \models V \triangleright S_1' : \{z{:}T\,\mathtt{list} \triangleright \varUpsilon \mid \exists z'{:}T\,\mathtt{list}.\varphi \wedge z' = []\}, \tag{H.6}$$

and then we can have

$$\sigma : \varGamma \models V \triangleright [] \triangleright S_1' : \{z{:}T\,\mathtt{list} \triangleright z'{:}T\,\mathtt{list} \triangleright \varUpsilon \mid \varphi\}. \tag{H.7}$$

Now the goal follows from Lemma 19, given (H.1), (H.5), and (H.7). □