Dynamic Determinacy Analysis

Soundness Proof

Max Schäfer[1], Manu Sridharan[2], Julian Dolby[2], and Frank Tip[3]

[1]Nanyang Technological University, Singapore
[2]IBM T. J. Watson Research Center, Yorktown Heights, NY, USA
[2]University of Waterloo, Waterloo, Ontario, Canada

1 Soundness of Dynamic Determinacy Analysis

This section gives a detailed proof of the soundness theorem.

To make the presentation self-contained, we repeat Figures 1, 2 and 3 presenting the syntax and concrete semantics of μJS, and Figures 4 and 5 presenting the instrumented semantics.

A basic property needed for much of the proof is *well-formedness*:

Definition 1. *A value, record, environment or trace is well-formed with respect to a heap if every address appearing in it belongs to the domain of the heap. A heap h is well-formed if every record in its codomain is well-formed with respect to h.*

Clearly, evaluation preserves well-formedness:

Lemma 1. *If h is well-formed, ρ is well-formed with respect to h,and $\langle h, \rho, s\rangle \downarrow \langle h', \rho', t\rangle$, then h' is well-formed, and ρ' and t are well-formed with respect to h'.*

Proof. Straightforward induction. □

A key fact about the modeling relation between values well-formed with respect to some heap h is that it remains valid if we replace μ by some μ' that agrees with μ on $\mathrm{dom}(h)$

Lemma 2. *If $\hat{h} \models_\mu h$ and h is well-formed, then for any μ' that agrees with μ on* $\mathrm{dom}(h)$ *we also have $\hat{h} \models_{\mu'} h$, and similar for values, records, and environments.*

Proof. We prove this by mutual induction.

1. First, consider the case of values; we need to show: if $\hat{v} \models_\mu v$, then also $\hat{v} \models_{\mu'} v$ for any μ' that agrees with μ on $\mathrm{dom}(h)$.

$$\begin{array}{lcll}
l \in \text{Literal} & ::= & pv & \text{primitive value} \\
 & | & \textbf{fun}(x)\ \{ & \text{function value} \\
 & & \quad \textbf{var}\ \overline{y};\ \overline{s};\ \textbf{return}\ z; & \\
 & & \} & \\
 & | & \{\} & \text{empty record} \\
 & & & \\
s \in \text{Stmt} & ::= & x = l & \text{literal load} \\
 & | & x = y & \text{variable copy} \\
 & | & x = y[z] & \text{property load} \\
 & | & x[y] = z & \text{property store} \\
 & | & x = y \diamond z & \text{primitive operator} \\
 & | & x = f(y) & \text{function call} \\
 & | & \textbf{if}(x)\{\overline{s}\} & \text{conditional} \\
 & | & \textbf{while}(x)\{\overline{s}\} & \text{loop}
\end{array}$$

$$\begin{array}{lcl}
\multicolumn{3}{l}{x, y, z, f \in \text{Name};\ \diamond \in \text{PrimOp};\ pv \in \text{PrimVal}; a \in \text{Address}} \\
v \in \text{Value} & ::= & pv \mid a \mid (\textbf{fun}(x)\ \{b\}, \rho) \\
r \in \text{Rec} & ::= & \{\overline{x\colon v}\} \\
\rho \in \text{Env} & := & \text{Name} \rightharpoonup \text{Value} \\
h \in \text{Heap} & := & \text{Address} \rightharpoonup \text{Rec}
\end{array}$$

Figure 1: Syntax and semantic domains of μJS; b abbreviates function bodies

$$\begin{array}{lcll}
e \in \text{Event} & ::= & x = v & \text{variable write} \\
 & | & a[x] = v & \text{heap write} \\
 & | & \textbf{if}(v)\{t\} & \text{conditional} \\
 & | & \textbf{fun}(v)\{t\}_\rho & \text{function call} \\
t \in \text{Trace} & := & \overline{e} &
\end{array}$$

Figure 2: Concrete execution traces

$$(\textsc{LdLit})\ \frac{x \in \mathrm{dom}(\rho)}{\langle h, \rho, x = pv\rangle \downarrow \langle h, \rho[x \mapsto pv], x = pv\rangle}$$

$$(\textsc{LdClos})\ \frac{F \equiv \mathbf{fun}(y)\ \{\ \mathbf{var}\ \overline{y};\ \overline{s};\ \mathbf{return}\ z;\ \} \quad x \in \mathrm{dom}(\rho)}{\langle h, \rho, x = F\rangle \downarrow \langle h, \rho[x \mapsto (F, \rho)], x = (F, \rho)\rangle}$$

$$(\textsc{LdRec})\ \frac{x \in \mathrm{dom}(\rho) \quad a \notin \mathrm{dom}(\rho)}{\langle h, \rho, x = \{\}\rangle \downarrow \langle h[a \mapsto \{\}], \rho[x \mapsto a], x = a\rangle}$$

$$(\textsc{Assign})\ \frac{x \in \mathrm{dom}(\rho) \quad \rho(y) = v}{\langle h, \rho, x = y\rangle \downarrow \langle h, \rho[x \mapsto v], x = v\rangle}$$

$$(\textsc{Ld})\ \frac{x \in \mathrm{dom}(\rho) \quad \rho(y) = a \quad \rho(z) = z' \quad h(a) = r \quad r(z') = v}{\langle h, \rho, x = y[z]\rangle \downarrow \langle h, \rho[x \mapsto v], x = v\rangle}$$

$$(\textsc{Sto})\ \frac{\rho(x) = a \quad \rho(y) = y' \quad h(a) = r \quad \rho(z) = v}{\langle h, \rho, x[y] = z\rangle \downarrow \langle h[a \mapsto r[y' \mapsto v]], \rho, a[y'] = v\rangle}$$

$$(\textsc{PrimOp})\ \frac{x \in \mathrm{dom}(\rho)\ \rho(y) = pv_1\ \rho(z) = pv_2\ pv_1[\![\diamond]\!]pv_2 = pv_3}{\langle h, \rho, x = y \diamond z\rangle \downarrow \langle h, \rho[x \mapsto pv_3], x = pv_3\rangle}$$

$$(\textsc{Inv})\ \frac{\begin{array}{c} x \in \mathrm{dom}(\rho) \quad \rho(f) = (\mathbf{fun}(z)\ \{\mathbf{var}\ \overline{x'}; \overline{s};\ \mathbf{return}\ y'; \}, \rho') \quad \rho(y) = v \\ \langle h, \rho'[z \mapsto v, \overline{x' \mapsto \mathbf{undefined}}], \overline{s}\rangle\, \overline{\downarrow} \langle h', \rho'', t\rangle \quad \rho''(y') = v' \end{array}}{\langle h, \rho, x = f(y)\rangle \downarrow \langle h', \rho[x \mapsto v'], (\mathbf{fun}(v)\{t\}_{\rho'}; x = v')\rangle}$$

$$(\textsc{If}_1)\ \frac{\rho(x) = v \quad v = \mathbf{true} \quad \langle h, \rho, \overline{s}\rangle\, \overline{\downarrow} \langle h', \rho', t\rangle}{\langle h, \rho, \mathbf{if}(x)\{\overline{s}\}\rangle \downarrow \langle h', \rho', \mathbf{if}(v)\{t\}\rangle}$$

$$(\textsc{If}_2)\ \frac{\rho(x) = v \quad v = \mathbf{false}}{\langle h, \rho, \mathbf{if}(x)\{\overline{s}\}\rangle \downarrow \langle h, \rho, \mathbf{if}(v)\{\}\rangle}$$

$$(\textsc{While})\ \frac{\langle h, \rho, \mathbf{if}(x)\{\overline{s};\ \mathbf{while}(x)\{\overline{s}\}\}\rangle \downarrow \langle h', \rho', t\rangle}{\langle h, \rho, \mathbf{while}(x)\{\overline{s}\}\rangle \downarrow \langle h', \rho', t\rangle}$$

$$(\textsc{Seq})\ \frac{\langle h_i, \rho_i, s_i\rangle \downarrow \langle h_{i+1}, \rho_{i+1}, e_i\rangle}{\langle h_0, \rho_0, \overline{s}\rangle\, \overline{\downarrow} \langle h_n, \rho_n, \overline{e}\rangle}$$

Figure 3: Concrete semantics of μJS

$$\begin{array}{lcl}
d \in D & := & \{!, ?\} \\
\hat{v} \in \widehat{\text{Value}} & ::= & pv^d \mid a^d \mid (\textbf{fun}(x)\ \{b\}, \hat{\rho})^d \\
\hat{r} \in \widehat{\text{Rec}} & ::= & \{\overline{x\colon \hat{v}}\} \mid \{\overline{x\colon \hat{v}}, \ldots\} \\
\hat{h} \in \widehat{\text{Heap}} & := & \text{Address} \rightharpoonup \widehat{\text{Rec}} \\
\hat{\rho} \in \widehat{\text{Env}} & := & \text{Name} \rightharpoonup \widehat{\text{Value}} \\
\hat{e} \in \widehat{\text{Event}} & ::= & x = \hat{v} \mid a^d[x^{d'}] = \hat{v} \mid \textbf{if}(\hat{v})\{\hat{t}\} \\
 & \mid & (\textbf{fun}(\hat{v})\{\hat{t}\})^d_{\hat{\rho}} \\
\hat{t} \in \widehat{\text{Trace}} & := & \overline{\hat{e}}
\end{array}$$

Figure 4: Instrumented semantic domains and traces

If $\hat{v}$ is indeterminate, then clearly $\hat{v} \models_{\mu'} v$ without any assumptions on μ'. If $\hat{v} = pv^!$, then v must be pv, and again $pv^! \models_{\mu'} pv$ for arbitrary μ'. If $\hat{v} = \mu(a)^!$ and $v = a$, then note that $\mu'(a) = \mu(a)$, hence $\mu'(a)^! \models_{\mu'} a$.

Finally, if $\hat{v}$ is $(\textbf{fun}(y)\ \{b\}, \hat{\rho})^!$ and v is $(\textbf{fun}(y)\ \{b\}, \rho)$ where $\hat{\rho} \models_{\mu} \rho$, we note that by induction hypothesis $\hat{\rho} \models_{\mu'} \rho$ since ρ must be well-formed; this gives us $\hat{v} \models_{\mu'} v$.

2. For records, we need to show: if $\hat{r} \models_{\mu} r$, then also $\hat{r} \models_{\mu'} r$ for any μ' that agrees with μ on $\text{dom}(h)$.

   So consider some name x. If $\hat{r}$ does not have a field x, then $\hat{r}(x)$ is either $\textbf{undefined}^!$ if r is closed, or $\textbf{undefined}^?$ if it is open. In the former case, we must have $r(x) = \textbf{undefined}$, so $\hat{r}(x) \models_{\mu'} r(x)$; in the latter case, $\hat{r}(x) \models_{\mu'} r(x)$ trivially.

3. For environments, we need to show: if $\hat{\rho} \models_{\mu} \rho$, then also $\hat{\rho} \models_{\mu'} \rho$ for any μ' that agrees with μ on $\text{dom}(h)$.

   Consider some $x \in \text{dom}(\rho)$, for which by assumption we have $\hat{\rho}(x) \models_{\mu} \rho(x)$. Since $\rho(x)$ must be well-formed, we can apply the induction hypothesis to get $\hat{\rho}(x) \models_{\mu'} \rho(x)$. Since this holds for arbitrary $x \in \text{dom}(\rho)$, we get $\hat{\rho} \models_{\mu'} \rho$.

4. For heaps, we need to show: if $\hat{h} \models_{\mu} h$, then also $\hat{h} \models_{\mu'}$ for any μ' that agrees with μ on $\text{dom}(h)$.

   Consider any $a \in \text{dom}(h)$, for which by assumption we have $\hat{h}(\mu(a)) \models_{\mu} h(a)$. Since $h(a)$ must be well-formed, we can apply the induction hypothesis to get $\hat{h}(\mu(a)) \models_{\mu'} h(a)$; but clearly $\mu'(a) = \mu(a)$, so $\hat{h}(\mu'(a)) \models_{\mu'} h(a)$, and, since a was arbitrary, $\hat{h} \models_{\mu'} h$.

□

The variable and property domains of a trace are defined in Figure 6. The main text mentions a simple result establishing the correctness of these definitions that we prove in a bit more detail here.

$$(\widehat{\textsc{LdLit}})\ \frac{x \in \mathrm{dom}(\hat{\rho})}{\langle \hat{h}, \hat{\rho}, x = pv \rangle \hat{\downarrow}^{n} \langle \hat{h}, \hat{\rho}[x \mapsto pv^{!}], x = pv^{!} \rangle}$$

$$(\widehat{\textsc{LdClos}})\ \frac{F \equiv \mathbf{fun}(y)\ \{\ \mathbf{var}\ \overline{y};\ \overline{s};\ \mathbf{return}\ z;\ \} \quad x \in \mathrm{dom}(\hat{\rho})}{\langle \hat{h}, \hat{\rho}, x = F \rangle \hat{\downarrow}^{n} \langle \hat{h}, \hat{\rho}[x \mapsto F, \hat{\rho})^{!}], x = (F, \hat{\rho})^{!} \rangle}$$

$$(\widehat{\textsc{LdRec}})\ \frac{x \in \mathrm{dom}(\hat{\rho}) \quad a \notin \mathrm{dom}(\hat{h})}{\langle \hat{h}, \hat{\rho}, x = \{\} \rangle \hat{\downarrow}^{n} \langle \hat{h}[a \mapsto \{\}], \hat{\rho}[x \mapsto a^{!}], x = a^{!} \rangle}$$

$$(\widehat{\textsc{Assign}})\ \frac{x \in \mathrm{dom}(\hat{\rho}) \quad \hat{\rho}(y) = \hat{v}}{\langle \hat{h}, \hat{\rho}, x = y \rangle \hat{\downarrow}^{n} \langle \hat{h}, \hat{\rho}[x \mapsto \hat{v}], x = \hat{v} \rangle}$$

$$(\widehat{\textsc{Ld}})\ \frac{x \in \mathrm{dom}(\hat{\rho}) \quad \hat{\rho}(y) = a^{d} \quad \hat{\rho}(z) = {z'}^{d'} \quad \hat{h}(a) = \hat{r} \quad \hat{r}(z') = \hat{v}}{\langle \hat{h}, \hat{\rho}, x = y[z] \rangle \hat{\downarrow}^{n} \langle \hat{h}, \hat{\rho}[x \mapsto (\hat{v}^{d})^{d'}], x = (\hat{v}^{d})^{d'} \rangle}$$

$$(\widehat{\textsc{Sto}})\ \frac{\hat{\rho}(x) = a^{d} \quad \hat{\rho}(y) = {y'}^{d'} \quad \hat{h}(a) = \hat{r} \quad \hat{\rho}(z) = \hat{v}}{\langle \hat{h}, \hat{\rho}, x[y] = z \rangle \hat{\downarrow}^{n} \langle (\hat{h}[a \mapsto (\hat{r}[y' \mapsto \hat{v}])^{d'}])^{d}, \hat{\rho}, a^{d}[y'^{d'}] = \hat{v} \rangle}$$

$$(\widehat{\textsc{PrimOp}})\ \frac{x \in \mathrm{dom}(\hat{\rho}) \quad \hat{\rho}(y) = pv_1^{d_1} \quad \hat{\rho}(z) = pv_2^{d_2} \quad pv_1 [\![\diamond]\!] pv_2 = pv_3}{\langle \hat{h}, \hat{\rho}, x = y \diamond z \rangle \downarrow \langle \hat{h}, \hat{\rho}[x \mapsto (pv_3^{d_1})^{d_2}], x = (pv_3^{d_1})^{d_2} \rangle}$$

$$(\widehat{\textsc{Inv}})\ \frac{\begin{array}{c} x \in \mathrm{dom}(\hat{\rho}) \quad \hat{\rho}(f) = (\mathbf{fun}(z)\ \{\mathbf{var}\ \overline{x'};\ \overline{s};\ \mathbf{return}\ z';\}, \hat{\rho}')^{d} \quad \hat{\rho}(y) = \hat{v} \\ \langle \hat{h}, \hat{\rho}'[z \mapsto \hat{v}, \overline{x' \mapsto \mathbf{undefined}^{!}}], \overline{s} \rangle \overline{\hat{\downarrow}^{n}} \langle \hat{h}', \hat{\rho}'', \hat{t} \rangle \quad \hat{\rho}''(z') = \hat{v}' \end{array}}{\langle \hat{h}, \hat{\rho}, x = f(y) \rangle \hat{\downarrow}^{n} \langle \hat{h}'^{d}, \hat{\rho}[x \mapsto \hat{v}'^{d}], (\mathbf{fun}(\hat{v})\ \{\hat{t}\}^{d}_{\hat{\rho}'}; x = \hat{v}'^{d}) \rangle}$$

$$(\widehat{\textsc{If}_1})\ \frac{\hat{\rho}(x) = v^{d} \quad v = \mathbf{true} \quad \langle \hat{h}, \hat{\rho}, \overline{s} \rangle \overline{\hat{\downarrow}^{n}} \langle \hat{h}', \hat{\rho}', \hat{t} \rangle}{\langle \hat{h}, \hat{\rho}, \mathbf{if}(x)\{\overline{s}\} \rangle \hat{\downarrow}^{n} \langle \hat{h}'[\mathrm{pd}(\hat{t}) := \hat{h}'^{d}], \hat{\rho}'[\mathrm{vd}(\hat{t}) := \hat{\rho}'^{d}], \mathbf{if}(v^{d})\{\hat{t}\} \rangle}$$

$$(\widehat{\textsc{If}_2\text{-}\textsc{Det}})\ \frac{\hat{\rho}(x) = v^{!} \quad v = \mathbf{false}}{\langle \hat{h}, \hat{\rho}, \mathbf{if}(x)\{\overline{s}\} \rangle \downarrow \langle \hat{h}, \hat{\rho}, \mathbf{if}(v^{!})\{\} \rangle}$$

$$(\widehat{\textsc{Cntr}})\ \frac{\hat{\rho}(x) = v^{?} \quad v = \mathbf{false} \quad n < k \quad \langle \hat{h}, \hat{\rho}, \overline{s} \rangle \overline{\hat{\downarrow}^{n+1}} \langle \hat{h}', \hat{\rho}', \hat{t} \rangle}{\langle \hat{h}, \hat{\rho}, \mathbf{if}(x)\{\overline{s}\} \rangle \hat{\downarrow}^{n} \langle \hat{h}'[\mathrm{pd}(\hat{t}) := \hat{h}^{?}], \hat{\rho}'[\mathrm{vd}(\hat{t}) := \hat{\rho}^{?}], \mathbf{if}(v^{?})\{\hat{t}\} \rangle}$$

$$(\widehat{\textsc{CntrAbort}})\ \frac{\hat{\rho}(x) = v^{?} \quad v = \mathbf{false} \quad n \geq k}{\langle \hat{h}, \hat{\rho}, \mathbf{if}(x)\{\overline{s}\} \rangle \hat{\downarrow}^{n} \langle \hat{h}^{?}, \hat{\rho}[\mathrm{vd}(\overline{s}) := \hat{\rho}^{?}], \mathbf{if}(v^{?})\{\} \rangle}$$

$$(\widehat{\textsc{While}})\ \frac{\langle \hat{h}, \hat{\rho}, \mathbf{if}(x)\{\overline{s};\ \mathbf{while}(x)\{\overline{s}\}\}\ \mathbf{else}\ \{\} \rangle \hat{\downarrow}^{n} \langle \hat{h}', \hat{\rho}', \hat{t} \rangle}{\langle \hat{h}, \hat{\rho}, \mathbf{while}(x)\{\overline{s}\} \rangle \hat{\downarrow}^{n} \langle \hat{h}', \hat{\rho}', \hat{t} \rangle}$$

$$(\widehat{\textsc{Seq}})\ \frac{\langle \hat{h}_0, \hat{\rho}_0, s_1 \rangle \hat{\downarrow}^{n} \langle \hat{h}_1, \hat{\rho}_1, \hat{e}_1 \rangle \ldots \langle \hat{h}_{n-1}, \hat{\rho}_{n-1}, s_s \rangle \hat{\downarrow}^{n} \langle \hat{h}_n, \hat{\rho}_n, \hat{e}_n \rangle}{\langle \hat{h}_0, \hat{\rho}_0, \overline{s} \rangle \overline{\hat{\downarrow}^{n}} \langle \hat{h}_n, \hat{\rho}_n, \overline{\hat{e}} \rangle}$$

Figure 5: Instrumented semantics for determinacy analysis.

$$
\begin{array}{lcl}
\multicolumn{3}{l}{\mathrm{vd}\colon \mathrm{Event} \to \mathcal{P}(\mathrm{Name})} \\
\mathrm{vd}(x = v) & = & \{x\} \\
\mathrm{vd}(a[x] = v) & = & \emptyset \\
\mathrm{vd}(\mathbf{if}(v)\ \{\overline{e}\}) & = & \bigcup_i \mathrm{vd}(e_i) \\
\mathrm{vd}(\mathbf{fun}(v)\ \{\overline{e}\})_\rho & = & \emptyset \\
\\
\multicolumn{3}{l}{\mathrm{pd}\colon \mathrm{Event} \to \mathcal{P}(\mathrm{Address} \times \mathrm{Name})} \\
\mathrm{pd}(x = v) & = & \emptyset \\
\mathrm{pd}(a[x] = v) & = & \{(a, p)\} \\
\mathrm{pd}(\mathbf{if}(v)\ \{\overline{e}\}) & = & \bigcup_i \mathrm{pd}(e_i) \\
\mathrm{pd}(\mathbf{fun}(v)\ \{\overline{e}\})_\rho & = & \bigcup_i \mathrm{pd}(e_i)
\end{array}
$$

Figure 6: Variable and property domains

$$
\begin{array}{lcl}
\multicolumn{3}{l}{\mathrm{vd}\colon \mathrm{Stmt} \to \mathcal{P}(\mathrm{Name})} \\
\mathrm{vd}(x = l) & = & \{x\} \\
\mathrm{vd}(x = y) & = & \{x\} \\
\mathrm{vd}(x = y[z]) & = & \{x\} \\
\mathrm{vd}(x[y] = z) & = & \emptyset \\
\mathrm{vd}(x = y \diamond z) & = & \{x\} \\
\mathrm{vd}(x = f(y)) & = & \{x\} \\
\mathrm{vd}(\mathbf{if}(x)\{\overline{s}\}) & = & \bigcup_i \mathrm{vd}(s_i) \\
\mathrm{vd}(\mathbf{while}(x)\{\overline{s}\}) & = & \bigcup_i \mathrm{vd}(s_i)
\end{array}
$$

Figure 7: Syntactic variable domain

Lemma 3. *If $\langle h, \rho, s\rangle \downarrow \langle h', \rho', t\rangle$, then for any $(a, p) \notin \mathrm{pd}(t)$ we have $h'(a)(p) = h(a)(p)$, and for any $x \notin \mathrm{vd}(t)$ we have $\rho'(x) = \rho(x)$.*

Proof. To establish the result for pd we only need to consider rules (LdRec) and (Sto): the other rules either do not change the heap, or the result follows directly from the induction hypothesis. However, for (LdRec) no property is actually updated, so the result holds vacuously. For (Sto), the updated property $a[y']$ appears in the trace, so $(a, y') \in \mathrm{pd}(t)$.

For vd, simple inspection of the rules shows that whenever x is updated in the resulting environment, it also appears in the trace, and hence in vd. □

We can overapproximate $\mathrm{vd}(t)$ by textually scanning the executed code s for all variables it writes (Figure 7). This is sound:

Lemma 4. *If $\langle h, \rho, s\rangle \downarrow \langle h', \rho', t\rangle$, then $\mathrm{vd}(t) \subseteq \mathrm{vd}(s)$.*

Proof. Easily seen by inspection of the rules for concrete derivations. □

When extending environments, we can extend the modeling relation along with it:

Lemma 5. *If $\hat{\rho} \models_\mu \rho$ and $\hat{v} \models_\mu v$, then $\hat{\rho}[x \mapsto \hat{v}] \models_\mu \rho[x \mapsto v]$.*

Proof. Consider any $y \in \mathrm{dom}(\rho[x \mapsto v])$. If $y = x$, then $\rho[x \mapsto v](y) = v$ and $\hat{\rho}[x \mapsto \hat{v}] = \hat{v}$, but by assumption $\hat{v} \models_\mu v$. Otherwise, $\hat{\rho}[x \mapsto \hat{v}](x) = \hat{\rho}(x) \models_\mu \rho(x) = \rho[x \mapsto v](x)$. □

The same result holds for records; for heaps we need injectivity:

Lemma 6. *If $\hat{h} \models_\mu h$ and μ is injective on $\mathrm{dom}(h) \cup \{a\}$, then $\hat{h}[\mu(a) \mapsto \hat{r}] \models_\mu h[a \mapsto r]$, whenever $\hat{r} \models_\mu r$.*

Proof. Consider any $a' \in \mathrm{dom}(h[a \mapsto r])$. If $a' = a$, then $\hat{h}[\mu(a) \mapsto \hat{r}](\mu(a')) = \hat{r} \models_\mu r = h[a \mapsto r](a')$. If $a' \neq a$, then by the assumption about injectivity $\mu(a') \neq \mu(a)$, so $\hat{h}[\mu(a) \mapsto \hat{r}](\mu(a')) = \hat{h}(\mu(a')) \models_\mu h(a') = h[a \mapsto r](a')$. □

If we already know that $\hat{h}$ models h, then flushing and resetting some properties in $\hat{h}$ will not change this fact:

Lemma 7. *If $\hat{h}' \models_\mu h$, then $\hat{h}'[A := \hat{h}^?] \models_\mu h$ as well, and likewise for environments.*

Proof. We first prove the result for environments.

Let $\hat{\rho}', \hat{\rho}$ be instrumented environments, ρ a concrete environment such that $\hat{\rho}' \models_\mu \rho$, and V a set of names. We show $\hat{\rho}'[V := \hat{\rho}^?] \models_\mu \rho$.

Consider some name $x \in \mathrm{dom}(\rho)$. If $x \in \mathrm{dom}(\hat{\rho}) \cap V$, then $\hat{\rho}'[V := \hat{\rho}^?] = \hat{\rho}(x)^? \models_\mu \rho(x)$ trivially; otherwise x must still be in $\mathrm{dom}(\hat{\rho}')$ by assumption, so $\hat{\rho}'[V := \hat{\rho}^?] = \hat{\rho}'(x) \models_\mu \rho(x)$ also by assumption.

The result extends to records.

Now consider instrumented heaps $\hat{h}, \hat{h}'$ and a concrete heap h such that $\hat{h}' \models_\mu h$, and let $A \subseteq \text{Address} \times \text{Name}$ be a set of address-property name pairs. We show $\hat{h}'[A := \hat{h}^?] \models_\mu h$.

So consider $a \in \mathrm{dom}(h)$. By assumption $a \in \mathrm{dom}(\hat{h}')$. If also $a \in \mathrm{dom}(\hat{h})$, we have $\hat{h}'[A := \hat{h}^?](a) = \hat{h}'(a)[A_a := \hat{h}(a)^?]$, and by the result for records $\hat{h}'(a)[A_a := \hat{h}(a)^?] \models_\mu h(a)$ since $\hat{h}'(a) \models_\mu h(a)$, which is what we need. Otherwise $\hat{h}'[A := \hat{h}^?](a) = \hat{h}'(a) \models_\mu h(a)$ immediately. □

With these technical results out of the way, we can prove our main theorem.

Theorem 1. *If $\langle \hat{h}, \hat{\rho}, s\rangle \mathrel{\hat{\downarrow}^n} \langle \hat{h}', \hat{\rho}', \hat{t}\rangle$ and $\langle h, \rho, s\rangle \downarrow \langle h', \rho', t\rangle$ where $\hat{h} \models_\mu h$, $\hat{\rho} \models_\mu \rho$, h is well-formed, ρ is well-formed with respect to h, and μ is injective on $\mathrm{dom}(d)$; then $\hat{h}' \models_{\mu'} h'$, $\hat{\rho}' \models_{\mu'} \rho'$ and $\hat{t} \models_{\mu'} t$ for some μ' such that $\forall a \in \mathrm{dom}(h). \mu(a) = \mu'(a)$ and μ' is injective on $\mathrm{dom}(h')$.*

Proof. The proof proceeds by induction on the derivation of $\langle \hat{h}, \hat{\rho}, s\rangle \mathrel{\hat{\downarrow}^n} \langle \hat{h}', \hat{\rho}', \hat{t}\rangle$, with a case distinction on the last rule used in the derivation.

1. Case $(\widehat{\textsc{LdLit}})$:

   The instrumented derivation must be of the form

$$\frac{x \in \mathrm{dom}(\hat{\rho})}{\langle \hat{h}, \hat{\rho}, x = pv\rangle \,\hat{\downarrow}^{n}\, \langle \hat{h}, \hat{\rho}[x \mapsto pv^{!}], x = pv^{!}\rangle}$$

The concrete derivation must be of the form

$$\frac{x \in \mathrm{dom}(\rho)}{\langle h, \rho, x = pv\rangle \downarrow \langle h, \rho[x \mapsto pv], x = pv\rangle}$$

We choose $\mu' := \mu$, which is injective on $\mathrm{dom}(h') = \mathrm{dom}(h)$. By assumption, $\hat{h} \models_{\mu} h$ and $\hat{\rho} \models_{\mu} \rho$. This immediately gives $\hat{h} \models_{\mu'} h$. Since $pv^{!} \models_{\mu'} pv$ we also have $\hat{\rho}[x \mapsto pv^{!}] \models_{\mu'} \rho[x \mapsto pv]$ (by Lemma 5) and $x = pv^{!} \models_{\mu'} x = pv$, as required.

2. Case ($\widehat{\text{LdClos}}$):

   The instrumented derivation must be of the form

$$\frac{x \in \mathrm{dom}(\hat{\rho})}{\langle \hat{h}, \hat{\rho}, x = \mathbf{fun}(y)\ \{b\}\rangle \,\hat{\downarrow}^{n}\, \langle \hat{h}, \hat{\rho}[x \mapsto (\mathbf{fun}(y)\ \{b\}, \hat{\rho})^{!}], x = (\mathbf{fun}(y)\ \{b\}, \hat{\rho})^{!}\rangle}$$

   and the concrete derivation is

$$\frac{x \in \mathrm{dom}(\rho)}{\langle h, \rho, x = \mathbf{fun}(y)\ \{b\}\rangle \downarrow \langle h, \rho[x \mapsto (\mathbf{fun}(y)\ \{b\}, \rho)], x = (\mathbf{fun}(y)\ \{b\}, \rho)\rangle}$$

   We again choose $\mu' := \mu$ and argue as in the previous case, noting that $(\mathbf{fun}(y)\ \{b\}, \hat{\rho})^{!} \models_{\mu'} (\mathbf{fun}(y)\ \{b\}, \rho)$ since $\hat{\rho} \models_{\mu'} \rho$ by assumption.

3. Case ($\widehat{\text{LdRec}}$):

   The instrumented derivation must be of the form

$$(\widehat{\text{LdRec}})\ \frac{x \in \mathrm{dom}(\hat{\rho}) \qquad a' \notin \mathrm{dom}(h)}{\langle \hat{h}, \hat{\rho}, x = \{\}\rangle \,\hat{\downarrow}^{n}\, \langle \hat{h}[a' \mapsto \{\}], \hat{\rho}[x \mapsto a'^{!}], x = a'^{!}\rangle}$$

   and the concrete derivation must be of the form

$$(\text{LdRec})\ \frac{x \in \mathrm{dom}(\rho) \qquad a \notin \mathrm{dom}(h)}{\langle h, \rho, x = \{\}\rangle \downarrow \langle h[a \mapsto \{\}], \rho[x \mapsto a], x = a\rangle}$$

   We choose $\mu' := \mu[a \mapsto a']$, which agrees with μ on $\mathrm{dom}(h)$ as required (since $a \notin \mathrm{dom}(h)$), and is injective on $\mathrm{dom}(h') = \mathrm{dom}(h) \cup \{a\}$ (since there cannot be an $a_0 \in \mathrm{dom}(h)$ with $\mu(a_0) = a'$).

   By Lemma 2, we have $\hat{h} \models_{\mu'} h$ and $\hat{\rho} \models_{\mu'} \rho$, from which the result follows by Lemmas 5 and 6, since $a'^{!} = \mu'(a)^{!} \models_{\mu'} a$ and trivially $\{\} \models_{\mu'} \{\}$.

4. Case ($\widehat{\textsc{Assign}}$):

   The instrumented derivation must be of the form

$$(\widehat{\textsc{Assign}})\ \frac{x \in \mathrm{dom}(\hat{\rho}) \qquad \hat{\rho}(y) = \hat{v}}{\langle \hat{h}, \hat{\rho}, x = y\rangle \mathrel{\hat{\downarrow}^{n}} \langle \hat{h}, \hat{\rho}[x \mapsto \hat{v}], x = \hat{v}\rangle}$$

   and the concrete derivation must be of the form

$$(\textsc{Assign})\ \frac{x \in \mathrm{dom}(\rho) \qquad \rho(y) = v}{\langle h, \rho, x = y\rangle \downarrow \langle h, \rho[x \mapsto v], x = v\rangle}$$

   We choose $\mu' := \mu$. The result follows by Lemma 5, since $\hat{v} \models_{\mu} v$.

5. Case ($\widehat{\textsc{Ld}}$):

   The instrumented derivation must be of the form

$$(\widehat{\textsc{Ld}})\ \frac{x \in \mathrm{dom}(\hat{\rho}) \quad \hat{\rho}(y) = a'^{d_1} \quad \hat{\rho}(z) = p'^{d_2} \quad \hat{h}(a') = \hat{r} \quad \hat{r}(p') = \hat{v}}{\langle \hat{h}, \hat{\rho}, x = y[z]\rangle \mathrel{\hat{\downarrow}^{n}} \langle \hat{h}, \hat{\rho}[x \mapsto (\hat{v}^{d_1})^{d_2}], x = (\hat{v}^{d_1})^{d_2}\rangle}$$

   and the concrete derivation must be of the form

$$(\textsc{Ld})\ \frac{x \in \mathrm{dom}(\rho) \quad \rho(y) = a \quad \rho(z) = p \quad h(a) = r \quad r(p) = v}{\langle h, \rho, x = y[z]\rangle \downarrow \langle h, \rho[x \mapsto v], x = v\rangle}$$

   We choose $\mu' := \mu$ and note that $\mathrm{dom}(h') = \mathrm{dom}(h)$; all we need to show is $(\hat{v}^{d_1})^{d_2} \models_{\mu} v$. If either $d_1 =?$ or $d_2 =?$, this is immediate; so let us consider the case where $d_1 = d_2 =!$.

   Then we must have $a' = \mu(a)$ since $\hat{\rho} \models_{\mu} \rho$ by assumption, which gives us $\hat{r} \models_{\mu} r$ since $\hat{h} \models_{\mu} h$ by assumption. But then we note that also $p' = p$ (again by $\hat{\rho} \models_{\mu} \rho$), so $\hat{v} \models_{\mu} v$, which is what we need.

6. Case ($\widehat{\textsc{Sto}}$):

   The instrumented derivation must be of the form

$$(\widehat{\textsc{Sto}})\ \frac{\hat{\rho}(x) = a'^{d_1} \quad \hat{\rho}(y) = p'^{d_2} \quad \hat{h}(a') = \hat{r} \quad \hat{\rho}(z) = \hat{v}}{\langle \hat{h}, \hat{\rho}, x[y] = z\rangle \mathrel{\hat{\downarrow}^{n}} \langle (\hat{h}[a' \mapsto (\hat{r}[p' \mapsto \hat{v}])^{d_2}])^{d_1}, \hat{\rho}, a'^{d_1}[p'^{d_2}] = \hat{v}\rangle}$$

   and the concrete derivation must be of the form

$$(\textsc{Sto})\ \frac{\rho(x) = a \quad \rho(y) = p \quad h(a) = r \quad \rho(z) = v}{\langle h, \rho, x[y] = z\rangle \downarrow \langle h[a \mapsto r[p \mapsto v]], \rho, a[p] = v\rangle}$$

We choose $\mu' := \mu$ and note that $\mathrm{dom}(h') = \mathrm{dom}(h)$. Clearly, $a'^{d_1} \models_\mu a$, $p'^{d_2} \models p$ and $\hat{v} \models_\mu v$ by the assumption that $\hat{\rho} \models_\mu \rho$, so $a'^{d_1}[p'^{d_2}] = \hat{v} \models_\mu a'[p'] = v$.

It remains to show that $(\hat{h}[a' \mapsto (\hat{r}[p' \mapsto \hat{v}])^{d_2}])^{d_1} \models_\mu h[a \mapsto r[p \mapsto v]]$.

Let us first consider the case where $d_1 =!$. Then $a' = \mu(a)$, and we can apply Lemma 6, which gives the result if we can show that

$$(\hat{r}[p' \mapsto \hat{v}])^{d_2} \models_{\mu'} r[p \mapsto v]$$

This is clearly true if $d_2 =?$. If $d_2 =!$, we note that $p' = p$ and $\hat{v} \models_\mu v$, so it is also true.

Now consider $d_1 =?$; then every record in the heap is made indeterminate, which also gives the result.

7. Case $(\widehat{\textsc{PrimOp}})$:

   The instrumented derivation must be of the form

$$(\widehat{\textsc{PrimOp}})\ \frac{x \in \mathrm{dom}(\hat{\rho}) \quad \hat{\rho}(y) = {pv'}_1^{d_1} \quad \hat{\rho}(z) = {pv'}_2^{d_2} \quad {pv'}_1[\![\circ]\!]{pv'}_2 = {pv'}_3}{\langle \hat{h}, \hat{\rho}, x = y \circ z\rangle \downarrow \langle \hat{h}, \hat{\rho}[x \mapsto ({pv'}_3^{d_1})^{d_2}], x = ({pv'}_3^{d_1})^{d_2}\rangle}$$

   and the concrete derivation must be of the form

$$(\textsc{PrimOp})\ \frac{x \in \mathrm{dom}(\rho) \quad \rho(y) = pv_1 \quad \rho(z) = pv_2 \quad pv_1[\![\circ]\!]pv_2 = pv_3}{\langle h, \rho, x = y \circ z\rangle \downarrow \langle h, \rho[x \mapsto pv_3], x = pv_3\rangle}$$

   We choose $\mu' := \mu$. All that remains to show is $({pv'}_3^{d_1})^{d_2} \models_\mu pv_3$. This is easy if $d_1 =?$ or $d_2 =?$; if $d_1 = d_2 =!$, then ${pv'}_i = pv_i$ for $i \in \{1, 2\}$, so also ${pv'}_3 = pv_3$, which is what we want.

8. Case $(\widehat{\textsc{Inv}})$:

   The instrumented derivation must be of the form

$$(\widehat{\textsc{Inv}})\ \frac{\begin{array}{c} x \in \mathrm{dom}(\rho) \quad \hat{\rho}(f) = (\mathbf{fun}(z')\ \{\mathbf{var}\ \overline{l'};\ \overline{s'};\ \mathbf{return}\ u';\}, \hat{\rho}')^d \quad \hat{\rho}(y) = \hat{v} \\ \langle \hat{h}, \hat{\rho}'[\overline{z' \mapsto \hat{v}}, \overline{l' \mapsto \mathbf{undefined}^{!}}], \overline{s'}\rangle \overline{\hat{\downarrow}^{n}} \langle \hat{h}', \hat{\rho}'', \hat{t}\rangle \quad \hat{\rho}''(u') = \hat{v}' \end{array}}{\langle \hat{h}, \hat{\rho}, x = f(y)\rangle \hat{\downarrow}^{n} \langle \hat{h}'^{d}, \hat{\rho}[x \mapsto \hat{v}'^{d}], (\mathbf{fun}(\overline{\hat{v}})\ \{\hat{t}\}^{d}_{\hat{\rho}'}; x = \hat{v}'^{d})\rangle}$$

   and the concrete derivation must be of the form

$$(\textsc{Inv})\ \frac{\begin{array}{c} x \in \mathrm{dom}(\rho) \quad \rho(f) = (\mathbf{fun}(z)\ \{\mathbf{var}\ \overline{l}; \overline{s};\ \mathbf{return}\ u;\}, \rho') \quad \rho(y) = v \\ \langle h, \rho'[\overline{z \mapsto v}, \overline{l \mapsto \mathbf{undefined}}], \overline{s}\rangle \overline{\downarrow}\langle h', \rho'', t\rangle \quad \rho''(u) = v' \end{array}}{\langle h, \rho, x = f(y)\rangle \downarrow \langle h', \rho[x \mapsto v'], (\mathbf{fun}(\overline{v})\{t\}_{\rho'}; x = v')\rangle}$$

If $d =?$, we choose μ' to be an injective extension of μ that maps addresses in $\mathrm{dom}(h') \setminus \mathrm{dom}(h)$ to arbitrary addresses not in $\mathrm{dom}(h)$. The result is then obvious.

If $d =!$, we infer that $z' = z$, $l' = l$, $\overline{s'} = \overline{s}$, $u' = u$, $\hat{\rho}' \models_\mu \rho'$, and also $\hat{v} \models_\mu v$. Applying the induction hypothesis, we get μ' such that $\hat{h}' \models_{\mu'} h'$, $\hat{\rho}'' \models_{\mu'} \rho''$, and $\hat{t} \models_{\mu'} t$. This means that $\hat{v}' \models_{\mu'} v'$, so we are done.

9. Case $(\widehat{\textsc{If}_1})$:

   The instrumented derivation must be of the form

$$(\widehat{\textsc{If}_1})\ \frac{\hat{\rho}(x) = v'^d \quad v' = \mathbf{true} \quad \langle \hat{h}, \hat{\rho}, \overline{s}\rangle \,\overline{\hat{\downarrow}}^{n} \langle \hat{h}', \hat{\rho}', \hat{t}\rangle}{\langle \hat{h}, \hat{\rho}, \mathbf{if}(x)\{\overline{s}\}\rangle \,\hat{\downarrow}^{n} \langle \hat{h}'[\mathrm{pd}(\hat{t}) := \hat{h}'^d], \hat{\rho}'[\mathrm{vd}(\hat{t}) := \hat{\rho}'^d], \mathbf{if}(v'^d)\{\hat{t}\}\rangle}$$

   In general, the concrete execution may either use $(\textsc{If}_1)$ or $(\textsc{If}_2)$. In the former case, it is of the form

$$(\textsc{If}_1)\ \frac{\rho(x) = v \quad v = \mathbf{true} \quad \langle h, \rho, \overline{s}\rangle \,\overline{\downarrow} \langle h', \rho', t\rangle}{\langle h, \rho, \mathbf{if}(x)\{\overline{s}\}\rangle \downarrow \langle h', \rho', \mathbf{if}(v)\{t\}\rangle}$$

   Applying the induction hypothesis, we get μ' such that $\hat{h}' \models_{\mu'} h'$, $\hat{\rho}' \models_{\mu'} \rho'$ and $\hat{t} \models_{\mu'} t$, and this μ' agrees with μ on $\mathrm{dom}(h)$. By assumption we have $v'^d \models_\mu v$, and hence by Lemma 2 also $v'^d \models_{\mu'} v$. By Lemma 7 we get $\hat{h}'[pd(\hat{t}) := \hat{h}'^d] \models_{\mu'} h'$ and $\hat{\rho}'[vd(\hat{t}) := \hat{\rho}'^d] \models_{\mu'} \rho'$, and so finally the result.

   If the concrete execution uses $(\textsc{If}_2)$, it is of the form

$$(\textsc{If}_2)\ \frac{\rho(x) = v \quad v = \mathbf{false}}{\langle h, \rho, \mathbf{if}(x)\{\overline{s}\}\rangle \downarrow \langle h, \rho, \mathbf{if}(v)\{\}\rangle}$$

   Since $v'^d \models_\mu v$ and v' and v have different "truthiness", this can only happen if $d =?$.

   We choose $\mu' := \mu$, so all that remains to show is that $\hat{h}'[pd(\hat{t}) := \hat{h}'^?] \models_{\mu'} h$ and $\hat{\rho}'[vd(\hat{t}) := \hat{\rho}'^?] \models_{\mu'} \rho$.

   For the former, consider some $a \in \mathrm{dom}(h)$; we need to show that $\forall p. \hat{h}'[pd(\hat{t}) := \hat{h}'^?](\mu'(a))(p) \models_{\mu'} h(a)(p)$. If $(\mu'(a), p) \in pd(\hat{t})$, then the left hand side is indeterminate, so we are done. Otherwise, we know by Lemma 3 that $\hat{h}'[pd(\hat{t}) := \hat{h}'^?](\mu'(a))(p) = \hat{h}'(\mu'(a))(p) = \hat{h}(\mu'(a))(p)$, and since μ' must agree with μ on a, we get the result.

   The result for the environment follows by a similar appeal to Lemma 3.

10. Case $(\widehat{\textsc{If}_2\text{-}\textsc{Det}})$:

    The instrumented derivation must be of the form

$$(\widehat{\textsc{If}_2\text{-}\textsc{Det}})\ \dfrac{\hat{\rho}(x) = v'^{!} \quad v' = \mathbf{false}}{\langle \hat{h}, \hat{\rho}, \mathbf{if}(x)\{\overline{s}\}\rangle \downarrow \langle \hat{h}, \hat{\rho}, \mathbf{if}(v'^{!})\{\}\rangle}$$

and the concrete derivation must be of the form

$$(\textsc{If}_2)\ \dfrac{\rho(x) = v \quad v = \mathbf{false}}{\langle h, \rho, \mathbf{if}(x)\{\overline{s}\}\rangle \downarrow \langle h, \rho, \mathbf{if}(v)\{\}\rangle}$$

Choosing $\mu' := \mu$, the result is obvious.

11. Case $(\widehat{\textsc{Cntr}})$:

The instrumented derivation must be of the form

$$(\widehat{\textsc{Cntr}})\ \dfrac{\hat{\rho}(x) = v'^{?} \quad v' = \mathbf{false} \quad n < k \quad \langle \hat{h}, \hat{\rho}, \overline{s}\rangle \overline{\hat{\downarrow}^{n+1}} \langle \hat{h}', \hat{\rho}', \hat{t}\rangle}{\langle \hat{h}, \hat{\rho}, \mathbf{if}(x)\{\overline{s}\}\rangle \hat{\downarrow}^{n} \langle \hat{h}'[\mathrm{pd}(\hat{t}) := \hat{h}^{?}], \hat{\rho}'[\mathrm{vd}(\hat{t}) := \hat{\rho}^{?}], \mathbf{if}(v'^{?})\{\hat{t}\}\rangle}$$

The concrete derivation can proceed either by $(\textsc{If}_1)$ or $(\textsc{If}_2)$.

In the former case, it must be of the form

$$(\textsc{If}_1)\ \dfrac{\rho(x) = v \quad v = \mathbf{true} \quad \langle h, \rho, \overline{s}\rangle \overline{\downarrow} \langle h', \rho', t\rangle}{\langle h, \rho, \mathbf{if}(x)\{\overline{s}\}\rangle \downarrow \langle h', \rho', \mathbf{if}(v)\{t\}\rangle}$$

We apply the induction hypothesis to obtain μ' agreeing with μ on $\mathrm{dom}(h)$ such that $\hat{h}' \models_{\mu'} h$, $\hat{\rho}' \models_{\mu'} \rho'$ and $\hat{t} \models_{\mu'} t$. By Lemma 7 also $\hat{h}'[\mathrm{pd}(\hat{t}) := \hat{h}^{?}] \models h'$ and $\hat{\rho}'[\mathrm{vd}(\hat{t}) := \hat{\rho}^{?}] \models \rho'$, and we are done.

In the latter case, it must be of the form

$$(\textsc{If}_2)\ \dfrac{\rho(x) = v \quad v = \mathbf{false}}{\langle h, \rho, \mathbf{if}(x)\{\overline{s}\}\rangle \downarrow \langle h, \rho, \mathbf{if}(v)\{\}\rangle}$$

Choosing $\mu' := \mu$, we observe that by Lemma 3 $\hat{h}'$ must agree with $\hat{h}$ on all $(a, p) \notin \mathrm{pd}(\hat{t})$; but the latter are made indeterminate in the resulting heap, so $\hat{h}'[\mathrm{pd}(\hat{t}) := \hat{h}^{?}] \models_{\mu'} h$. Similar reasoning shows $\hat{\rho}'[\mathrm{vd}(\hat{t}) := \hat{\rho}^{?}] \models_{\mu'} \rho$, which is what we need.

12. Case $(\widehat{\textsc{CntrAbort}})$:

The instrumented derivation must be of the form

$$(\widehat{\textsc{CntrAbort}})\ \dfrac{\hat{\rho}(x) = v'^{?} \quad v' = \mathbf{false} \quad n > k}{\langle \hat{h}, \hat{\rho}, \mathbf{if}(x)\{\overline{s}\}\rangle \hat{\downarrow}^{n} \langle \hat{h}^{?}, \hat{\rho}[\mathrm{vd}(\overline{s}) := \hat{\rho}^{?}], \mathbf{if}(v'^{?})\{\}\rangle}$$

The concrete derivation may either use ($\textsc{If}_1$) or ($\textsc{If}_2$) as its last rule.

In the former case, it must be of the form

$$(\textsc{If}_1)\ \frac{\rho(x) = v \quad v = \textbf{true} \quad \langle h, \rho, \overline{s}\rangle \,\overline{\downarrow}\, \langle h', \rho', t\rangle}{\langle h, \rho, \textbf{if}(x)\{\overline{s}\}\rangle \downarrow \langle h', \rho', \textbf{if}(v)\{t\}\rangle}$$

For μ', we choose an injective extension of μ that maps addresses in $\mathrm{dom}(h') \setminus \mathrm{dom}(h)$ to arbitrary addresses not in $\mathrm{dom}(\hat{h})$.

Then clearly $\hat{h}^? \models_{\mu'} h'$. To see $\hat{\rho}[\mathrm{vd}(\overline{s}) := \hat{\rho}^?] \models_{\mu'} \rho'$, consider some name $x \in \mathrm{dom}(\rho')$. If $x \in \mathrm{vd}(\overline{s})$, then obviously $\hat{\rho}[\mathrm{vd}(\overline{s}) := \hat{\rho}^?](x) \models_{\mu'} \rho'(x)$; otherwise, $\rho'(x) = \rho(x)$ by Lemma 4 and Lemma 3, so $\hat{\rho}[\mathrm{vd}(\overline{s}) := \hat{\rho}^?](x) = \hat{\rho}(x) \models_{\mu'} \rho(x) = \rho'(x)$.

If the concrete derivation uses ($\textsc{If}_2$), it must be of the form

$$(\textsc{If}_2)\ \frac{\rho(x) = v \quad v = \textbf{false}}{\langle h, \rho, \textbf{if}(x)\{\overline{s}\}\rangle \downarrow \langle h, \rho, \textbf{if}(v)\{\}\rangle}$$

and the result follows immediately, choosing $\mu' := \mu$.

13. Case ($\widehat{\textsc{While}}$):

    Direct appeal to induction hypothesis.

14. Case ($\widehat{\textsc{Seq}}$):

    Appeal to induction hypothesis; note that the μ' of the ith subderivation can be used as the μ of the $i + 1$th subderivation.

□