A symbolic execution semantics for TopHat

Appendices

Nico Naus
Information and Computing Sciences
Utrecht University
Utrecht, The Netherlands
n.naus@uu.nl

Tim Steenvoorden
Software Science
Radboud University
Nijmegen, The Netherlands
tim@cs.ru.nl

Markus Klinik
Software Science
Radboud University
Nijmegen, The Netherlands
m.klinik@cs.ru.nl

ACM Reference Format:
Nico Naus, Tim Steenvoorden, and Markus Klinik. 2020. A symbolic execution semantics for TopHat: Appendices. In *Proceedings of International Symposium on Implementation and Application of Functional Languages (IFL'19).* ACM, New York, NY, USA, 20 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

IFL'19, September 2019, Singapore
2020. ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

A COMPLETE SYMBOLIC SEMANTICS

A.1 Symbolic evaluation rules

$$\boxed{e, \sigma \downarrow \overline{v, \sigma', \varphi}}$$

SE-Value
$$\frac{}{v, \sigma \downarrow v, \sigma, \mathsf{True}}$$

SE-Pair
$$\frac{e_1, \sigma \downarrow \overline{v_1, \sigma', \varphi_1} \qquad e_2, \sigma' \downarrow \overline{v_2, \sigma'', \varphi_2}}{\langle e_1, e_2 \rangle, \sigma \downarrow \overline{\langle v_1, v_2 \rangle, \sigma'', \varphi_1 \wedge \varphi_2}}$$

SE-First
$$\frac{e_1, \sigma \downarrow \overline{v_1, \sigma', \varphi}}{\mathsf{fst}\langle e_1, e_2 \rangle, \sigma \downarrow \overline{v_1, \sigma', \varphi}}$$

SE-Second
$$\frac{e_2, \sigma \downarrow \overline{v_2, \sigma', \varphi}}{\mathsf{snd}\langle e_1, e_2 \rangle, \sigma \downarrow \overline{v_2, \sigma', \varphi}}$$

SE-Cons
$$\frac{e_1, \sigma \downarrow \overline{v_1, \sigma', \varphi_1} \qquad e_2, \sigma' \downarrow \overline{v_2, \sigma'', \varphi_2}}{e_1 :: e_2, \sigma \downarrow \overline{v_1 :: v_2, \sigma'', \varphi_1 \wedge \varphi_2}}$$

SE-Head
$$\frac{e, \sigma \downarrow \overline{v_1 :: v_2, \sigma', \varphi}}{\mathsf{head}\, e, \sigma \downarrow \overline{v_1, \sigma', \varphi}}$$

SE-Tail
$$\frac{e, \sigma \downarrow \overline{v_1 :: v_2, \sigma', \varphi}}{\mathsf{tail}\, e, \sigma \downarrow \overline{v_2, \sigma', \varphi}}$$

SE-App
$$\frac{e_1, \sigma \downarrow \overline{\lambda x : \tau . e_1', \sigma', \varphi_1} \qquad e_2, \sigma' \downarrow \overline{v_2, \sigma'', \varphi_2} \qquad e_1'[x \mapsto v_2], \sigma'' \downarrow \overline{v_1, \sigma''', \varphi_3}}{e_1 e_2, \sigma \downarrow \overline{v_1, \sigma''', \varphi_1 \wedge \varphi_2 \wedge \varphi_3}}$$

SE-If
$$\frac{e_1, \sigma \downarrow \overline{v_1, \sigma', \varphi_1} \qquad e_2, \sigma' \downarrow \overline{v_2, \sigma'', \varphi_2} \qquad e_3, \sigma' \downarrow \overline{v_3, \sigma''', \varphi_3}}{\mathbf{if}\, e_1\, \mathbf{then}\, e_2\, \mathbf{else}\, e_3, \sigma \downarrow \overline{v_2, \sigma'', \varphi_1 \wedge \varphi_2 \wedge v_1} \cup \overline{v_3, \sigma''', \varphi_1 \wedge \varphi_3 \wedge \neg v_1}}$$

SE-Ref
$$\frac{e, \sigma \downarrow \overline{v, \sigma', \varphi} \qquad l \notin Dom(\sigma')}{\mathbf{ref}\, e, \sigma \downarrow \overline{l, \sigma'[l \mapsto v], \varphi}}$$

SE-Deref
$$\frac{e, \sigma \downarrow \overline{l, \sigma', \varphi}}{!e, \sigma \downarrow \overline{\sigma'(l), \sigma', \varphi}}$$

SE-Assign
$$\frac{e_1, \sigma \downarrow \overline{l, \sigma', \varphi_1} \qquad e_2, \sigma' \downarrow \overline{v_2, \sigma'', \varphi_2}}{e_1 := e_2, \sigma \downarrow \overline{\langle\rangle, \sigma''[l \mapsto v_2], \varphi_1 \wedge \varphi_2}}$$

SE-Edit
$$\frac{e, \sigma \downarrow \overline{v, \sigma', \varphi}}{\Box\, e, \sigma \downarrow \overline{\Box\, v, \sigma', \varphi}}$$

SE-Enter
$$\frac{}{\boxtimes\, \tau, \sigma \downarrow \boxtimes\, \tau, \sigma, \mathsf{True}}$$

SE-Update
$$\frac{e, \sigma \downarrow \overline{l, \sigma', \varphi}}{\blacksquare\, e, \sigma \downarrow \overline{\blacksquare\, l, \sigma', \varphi}}$$

SE-Then
$$\frac{e_1, \sigma \downarrow \overline{t_1, \sigma', \varphi}}{e_1 \blacktriangleright e_2, \sigma \downarrow \overline{t_1 \blacktriangleright e_2, \sigma', \varphi}}$$

SE-Next
$$\frac{e_1, \sigma \downarrow \overline{t_1, \sigma', \varphi}}{e_1 \triangleright e_2, \sigma \downarrow \overline{t_1 \triangleright e_2, \sigma', \varphi}}$$

SE-And
$$\frac{e_1, \sigma \downarrow \overline{t_1, \sigma', \varphi_1} \qquad e_2, \sigma' \downarrow \overline{t_2, \sigma'', \varphi_2}}{e_1 \bowtie e_2, \sigma \downarrow \overline{t_1 \bowtie t_2, \sigma'', \varphi_1 \wedge \varphi_2}}$$

SE-Or
$$\frac{e_1, \sigma \downarrow \overline{t_1, \sigma', \varphi_1} \qquad e_2, \sigma' \downarrow \overline{t_2, \sigma'', \varphi_2}}{e_1 \blacklozenge e_2, \sigma \downarrow \overline{t_1 \blacklozenge t_2, \sigma'', \varphi_1 \wedge \varphi_2}}$$

SE-Xor
$$\frac{}{e_1 \lozenge e_2, \sigma \downarrow e_1 \lozenge e_2, \sigma, \mathsf{True}}$$

SE-Fail
$$\frac{}{\lightning, \sigma \downarrow \lightning, \sigma, \mathsf{True}}$$

A.2 Symbolic striding rules

$$\boxed{t, \sigma \rightsquigarrow \overline{t', \sigma', \varphi}}$$

$$\textsc{SS-ThenStay}\quad \frac{t_1, \sigma \rightsquigarrow \overline{t_1', \sigma', \varphi}}{t_1 \blacktriangleright e_2, \sigma \rightsquigarrow \overline{t_1' \blacktriangleright e_2, \sigma', \varphi}}\ \mathcal{V}(t_1', \sigma') = \bot$$

$$\textsc{SS-ThenFail}\quad \frac{t_1, \sigma \rightsquigarrow \overline{t_1', \sigma', \varphi} \qquad e_2\ v_1, \sigma' \downarrow \overline{t_2, \sigma'', \_}}{t_1 \blacktriangleright e_2, \sigma \rightsquigarrow \overline{t_1' \blacktriangleright e_2, \sigma', \varphi}}\ \mathcal{V}(t_1', \sigma') = v_1 \wedge \mathcal{F}(t_2, \sigma'')$$

$$\textsc{SS-ThenCont}\quad \frac{t_1, \sigma \rightsquigarrow \overline{t_1', \sigma', \varphi_1} \qquad e_2\ v_1, \sigma' \downarrow \overline{t_2, \sigma'', \varphi_2}}{t_1 \blacktriangleright e_2, \sigma \rightsquigarrow \overline{t_2, \sigma'', \varphi_1 \wedge \varphi_2}}\ \mathcal{V}(t_1', \sigma') = v_1 \wedge \neg\mathcal{F}(t_2, \sigma'')$$

$$\textsc{SS-OrLeft}\quad \frac{t_1, \sigma \rightsquigarrow \overline{t_1', \sigma', \varphi}}{t_1 \blacklozenge t_2, \sigma \rightsquigarrow \overline{t_1', \sigma', \varphi}}\ \mathcal{V}(t_1', \sigma') = v_1$$

$$\textsc{SS-OrRight}\quad \frac{t_1, \sigma \rightsquigarrow \overline{t_1', \sigma', \varphi_1} \qquad t_2, \sigma' \rightsquigarrow \overline{t_2', \sigma'', \varphi_2}}{t_1 \blacklozenge t_2, \sigma \rightsquigarrow \overline{t_2', \sigma'', \varphi_1 \wedge \varphi_2}}\ \mathcal{V}(t_1', \sigma') = \bot \wedge \mathcal{V}(t_2', \sigma'') = v_2$$

$$\textsc{SS-OrNone}\quad \frac{t_1, \sigma \rightsquigarrow \overline{t_1', \sigma', \varphi_1} \qquad t_2, \sigma' \rightsquigarrow \overline{t_2', \sigma'', \varphi_2}}{t_1 \blacklozenge t_2, \sigma \rightsquigarrow \overline{t_1' \blacklozenge t_2', \sigma'', \varphi_1 \wedge \varphi_2}}\ \mathcal{V}(t_1', \sigma') = \bot \wedge \mathcal{V}(t_2', \sigma'') = \bot$$

$$\textsc{SS-Edit}\quad \frac{}{\square\, v, \sigma \rightsquigarrow \square\, v, \sigma, \mathsf{True}} \qquad \textsc{SS-Fill}\quad \frac{}{\boxtimes\, \tau, \sigma \rightsquigarrow \boxtimes\, \tau, \sigma, \mathsf{True}} \qquad \textsc{SS-Update}\quad \frac{}{\blacksquare\, l, \sigma \rightsquigarrow \blacksquare\, l, \sigma, \mathsf{True}} \qquad \textsc{SS-Fail}\quad \frac{}{\lightning, \sigma \rightsquigarrow \lightning, \sigma, \mathsf{True}}$$

$$\textsc{SS-Xor}\quad \frac{}{e_1 \Diamond e_2, \sigma \rightsquigarrow e_1 \Diamond e_2, \sigma, \mathsf{True}} \qquad \textsc{SS-Next}\quad \frac{t_1, \sigma \rightsquigarrow \overline{t_1', \sigma', \varphi}}{t_1 \rhd e_2, \sigma \rightsquigarrow \overline{t_1' \rhd e_2, \sigma', \varphi}}$$

$$\textsc{SS-And}\quad \frac{t_1, \sigma \rightsquigarrow \overline{t_1', \sigma', \varphi_1} \qquad t_2, \sigma' \rightsquigarrow \overline{t_2', \sigma'', \varphi_2}}{t_1 \bowtie t_2, \sigma \rightsquigarrow \overline{t_1' \bowtie t_2', \sigma'', \varphi_1 \wedge \varphi_2}}$$

A.3 Symbolic normalisation rules

$$\boxed{e, \sigma \Downarrow \overline{t, \sigma', \varphi}}$$

$$\textsc{SN-Done}\quad \frac{e, \sigma \downarrow \overline{t, \sigma', \varphi_1} \qquad t, \sigma' \rightsquigarrow \overline{t', \sigma'', \varphi_2}}{e, \sigma \Downarrow \overline{t, \sigma', \varphi_1}}\ \sigma' = \sigma'' \wedge t = t'$$

$$\textsc{SN-Repeat}\quad \frac{\begin{array}{c} e, \sigma \downarrow \overline{t, \sigma', \varphi_1} \\ t, \sigma' \rightsquigarrow \overline{t', \sigma'', \varphi_2}\ t', \sigma'' \Downarrow \overline{t'', \sigma''', \varphi_3} \end{array}}{e, \sigma \Downarrow \overline{t'', \sigma''', \varphi_1 \wedge \varphi_2 \wedge \varphi_3}}\ \sigma' \neq \sigma'' \vee t \neq t'$$

A.4 Symbolic handling rules

$$\boxed{t, \sigma \longrightarrow \overline{t', \sigma', i, \varphi}}$$

SH-Change
$$\frac{\text{fresh } s}{\square\, v, \sigma \longrightarrow \square\, s, \sigma, s, \mathsf{True}}\ v, s : \tau$$

SH-Fill
$$\frac{\text{fresh } s}{\boxtimes\, \tau, \sigma \longrightarrow \square\, s, \sigma, s, \mathsf{True}}\ s : \tau$$

SH-Update
$$\frac{\text{fresh } s}{\blacksquare\, l, \sigma \longrightarrow \blacksquare\, l, \sigma[l \mapsto s], s, \mathsf{True}}\ \sigma(l), s : \tau$$

SH-PassNext
$$\frac{t_1, \sigma \longrightarrow \overline{t_1', \sigma', i, \varphi}}{t_1 \rhd e_2, \sigma \longrightarrow \overline{t_1' \rhd e_2, \sigma', i, \varphi}}\ \mathcal{V}(t_1, \sigma) = \bot$$

SH-PassNextFail
$$\frac{t_1, \sigma \longrightarrow \overline{t_1', \sigma_1', i, \varphi} \qquad e_2\, v_1, \sigma \Downarrow \overline{t_2, \sigma_2', \_}}{t_1 \rhd e_2, \sigma \longrightarrow \overline{t_1' \rhd e_2, \sigma_1', i, \varphi}}\ \mathcal{V}(t_1, \sigma) = v_1 \wedge \mathcal{F}(t_2, \sigma_2')$$

SH-Next
$$\frac{t_1, \sigma \longrightarrow \overline{t_1', \sigma_1', i_1, \varphi_1} \qquad e_2\, v_1, \sigma \Downarrow \overline{t_2, \sigma_2', \varphi_2}}{t_1 \rhd e_2, \sigma \longrightarrow \overline{\overline{t_1' \rhd e_2, \sigma_1', i_1, \varphi_1} \cup \overline{t_2, \sigma_2', \mathsf{C}, \varphi_2}}}\ \mathcal{V}(t_1, \sigma) = v_1 \wedge \neg\mathcal{F}(t_2, \sigma')$$

SH-PassThen
$$\frac{t_1, \sigma \longrightarrow \overline{t_1', \sigma', i, \varphi}}{t_1 \blacktriangleright e_2, \sigma \longrightarrow \overline{t_1' \blacktriangleright e_2, \sigma', i, \varphi}}$$

SH-Pick
$$\frac{e_1, \sigma \Downarrow \overline{t_1, \sigma_1, \varphi_1} \qquad e_2, \sigma \Downarrow \overline{t_2, \sigma_2, \varphi_2}}{e_1 \Diamond e_2, \sigma \longrightarrow \overline{\overline{t_1, \sigma_1, \mathsf{L}, \varphi_1} \cup \overline{t_2, \sigma_2, \mathsf{R}, \varphi_2}}}\ \neg\mathcal{F}(t_1, \sigma_1) \wedge \neg\mathcal{F}(t_2, \sigma_2)$$

SH-PickLeft
$$\frac{e_1, \sigma \Downarrow \overline{t_1, \sigma_1, \varphi_1} \qquad e_2, \sigma \Downarrow \overline{t_2, \sigma_2, \varphi_2}}{e_1 \Diamond e_2, \sigma \longrightarrow t_1, \sigma_1, \mathsf{L}, \varphi_1}\ \neg\mathcal{F}(t_1, \sigma_1) \wedge \mathcal{F}(t_2, \sigma_2)$$

SH-PickRight
$$\frac{e_1, \sigma \Downarrow \overline{t_1, \sigma_1, \varphi_1} \qquad e_2, \sigma \Downarrow \overline{t_2, \sigma_2, \varphi_2}}{e_1 \Diamond e_2, \sigma \longrightarrow t_2, \sigma_2, \mathsf{R}, \varphi_2}\ \mathcal{F}(t_1, \sigma_1) \wedge \neg\mathcal{F}(t_2, \sigma_2)$$

SH-And
$$\frac{t_1, \sigma \longrightarrow \overline{t_1', \sigma_1', i_1, \varphi_1} \qquad t_2, \sigma \longrightarrow \overline{t_2', \sigma_2', i_2, \varphi_2}}{t_1 \bowtie t_2, \sigma \longrightarrow \overline{\overline{t_1' \bowtie t_2, \sigma_1', \mathsf{F}\, i_1, \varphi_1} \cup \overline{t_1 \bowtie t_2', \sigma_2'', \mathsf{S}\, i_2, \varphi_2}}}$$

SH-Or
$$\frac{t_1, \sigma \longrightarrow \overline{t_1', \sigma_1', i_1, \varphi_1} \qquad t_2, \sigma \longrightarrow \overline{t_2', \sigma_2', i_2, \varphi_2}}{t_1 \blacklozenge t_2, \sigma \longrightarrow \overline{\overline{t_1' \blacklozenge t_2, \sigma_1', \mathsf{F}\, i_1, \varphi_1} \cup \overline{t_1 \blacklozenge t_2', \sigma_2', \mathsf{S}\, i_2, \varphi_2}}}$$

A.5 Symbolic driving rules

$$\boxed{t, \sigma \Longrightarrow \overline{t', \sigma', i, \varphi}}$$

SI-Handle
$$\frac{t, \sigma \longrightarrow \overline{t', \sigma', i, \varphi_1} \qquad t', \sigma' \Downarrow \overline{t'', \sigma'', \varphi_2}}{t, \sigma \Longrightarrow \overline{t'', \sigma'', i, \varphi_1 \wedge \varphi_2}}$$

B $\widehat{\text{TOP}}$ SEMANTICS

B.1 Typing rules

$$\boxed{\Gamma, \Sigma \vdash e : \tau}$$

$$\textsc{T-ConstBool}\ \frac{c \in B}{\Gamma, \Sigma \vdash c : \textsc{Bool}} \qquad \textsc{T-ConstInt}\ \frac{c \in I}{\Gamma, \Sigma \vdash c : \textsc{Int}} \qquad \textsc{T-ConstString}\ \frac{c \in S}{\Gamma, \Sigma \vdash c : \textsc{String}}$$

$$\textsc{T-Unit}\ \frac{}{\Gamma, \Sigma \vdash \langle\rangle : \textsc{Unit}} \qquad \textsc{T-Var}\ \frac{x : \tau \in \Gamma}{\Gamma, \Sigma \vdash x : \tau} \qquad \textsc{T-Loc}\ \frac{\Sigma(l) = \beta}{\Gamma, \Sigma \vdash l : \textsc{Ref}\,\beta}$$

$$\textsc{T-Pair}\ \frac{\Gamma, \Sigma \vdash e_1 : \tau_1 \qquad \Gamma, \Sigma \vdash e_2 : \tau_2}{\Gamma, \Sigma \vdash \langle e_1, e_2\rangle : \tau_1 \times \tau_2} \qquad \textsc{T-First}\ \frac{\Gamma, \Sigma \vdash e : \tau_1 \times \tau_2}{\Gamma, \Sigma \vdash \mathsf{fst}\, e : \tau_1} \qquad \textsc{T-Second}\ \frac{\Gamma, \Sigma \vdash e : \tau_1 \times \tau_2}{\Gamma, \Sigma \vdash \mathsf{snd}\, e : \tau_2}$$

$$\textsc{T-ListEmpty}\ \frac{}{\Gamma, \Sigma \vdash [\,]_\beta : \textsc{List}\,\beta} \qquad \textsc{T-ListCons}\ \frac{\Gamma, \Sigma \vdash e_1 : \beta \qquad \Gamma, \Sigma \vdash e_2 : \textsc{List}\,\beta}{\Gamma, \Sigma \vdash e_1 :: e_2 : \textsc{List}\,\beta}$$

$$\textsc{T-ListHead}\ \frac{\Gamma, \Sigma \vdash e : \textsc{List}\,\beta}{\Gamma, \Sigma \vdash \mathsf{head}\, e : \beta} \qquad \textsc{T-ListTail}\ \frac{\Gamma, \Sigma \vdash e : \textsc{List}\,\beta}{\Gamma, \Sigma \vdash \mathsf{tail}\, e : \textsc{List}\,\beta} \qquad \textsc{T-Abs}\ \frac{\Gamma[x : \tau_1], \Sigma \vdash e : \tau_2}{\Gamma, \Sigma \vdash \lambda x : \tau_1 . e : \tau_1 \to \tau_2}$$

$$\textsc{T-App}\ \frac{\Gamma, \Sigma \vdash e_1 : \tau_1 \to \tau_2 \qquad \Gamma, \Sigma \vdash e_2 : \tau_1}{\Gamma, \Sigma \vdash e_1 e_2 : \tau_2}$$

$$\textsc{T-If}\ \frac{\Gamma, \Sigma \vdash e_1 : \textsc{Bool} \qquad \Gamma, \Sigma \vdash e_2 : \tau \qquad \Gamma, \Sigma \vdash e_3 : \tau}{\Gamma, \Sigma \vdash \textbf{if}\, e_1\, \textbf{then}\, e_2\, \textbf{else}\, e_3 : \tau} \qquad \textsc{T-Ref}\ \frac{\Gamma, \Sigma \vdash e : \beta}{\Gamma, \Sigma \vdash \textbf{ref}\, e : \textsc{Ref}\,\beta}$$

$$\textsc{T-Deref}\ \frac{\Gamma, \Sigma \vdash e : \textsc{Ref}\,\beta}{\Gamma, \Sigma \vdash\, !e : \beta} \qquad \textsc{T-Assign}\ \frac{\Gamma, \Sigma \vdash e_1 : \textsc{Ref}\,\beta \qquad \Gamma, \Sigma \vdash e_2 : \beta}{\Gamma, \Sigma \vdash e_1 := e_2 : \textsc{Unit}}$$

$$\textsc{T-Edit}\ \frac{\Gamma, \Sigma \vdash e : \tau}{\Gamma, \Sigma \vdash \square\, e : \textsc{Task}\,\tau} \qquad \textsc{T-Enter}\ \frac{}{\Gamma, \Sigma \vdash \boxtimes\, \tau : \textsc{Task}\,\tau} \qquad \textsc{T-Update}\ \frac{\Gamma, \Sigma \vdash e : \textsc{Ref}\,\beta}{\Gamma, \Sigma \vdash \blacksquare\, e : \textsc{Task}\,\beta} \qquad \textsc{T-Fail}\ \frac{}{\Gamma, \Sigma \vdash \lightning : \textsc{Task}\,\tau}$$

$$\textsc{T-Then}\ \frac{\Gamma, \Sigma \vdash e_1 : \textsc{Task}\,\tau_1 \qquad \Gamma, \Sigma \vdash e_2 : \tau_1 \to \textsc{Task}\,\tau_2}{\Gamma, \Sigma \vdash e_1 \blacktriangleright e_2 : \textsc{Task}\,\tau_2} \qquad \textsc{T-Next}\ \frac{\Gamma, \Sigma \vdash e_1 : \textsc{Task}\,\tau_1 \qquad \Gamma, \Sigma \vdash e_2 : \tau_1 \to \textsc{Task}\,\tau_2}{\Gamma, \Sigma \vdash e_1 \triangleright e_2 : \textsc{Task}\,\tau_2}$$

$$\textsc{T-And}\ \frac{\Gamma, \Sigma \vdash e_1 : \textsc{Task}\,\tau_1 \qquad \Gamma, \Sigma \vdash e_2 : \textsc{Task}\,\tau_2}{\Gamma, \Sigma \vdash e_1 \bowtie e_2 : \textsc{Task}\,(\tau_1 \times \tau_2)}$$

$$\textsc{T-Or}\ \frac{\Gamma, \Sigma \vdash e_1 : \textsc{Task}\,\tau \qquad \Gamma, \Sigma \vdash e_2 : \textsc{Task}\,\tau}{\Gamma, \Sigma \vdash e_1 \blacklozenge e_2 : \textsc{Task}\,\tau} \qquad \textsc{T-Xor}\ \frac{\Gamma, \Sigma \vdash e_1 : \textsc{Task}\,\tau \qquad \Gamma, \Sigma \vdash e_2 : \textsc{Task}\,\tau}{\Gamma, \Sigma \vdash e_1 \lozenge e_2 : \textsc{Task}\,\tau}$$

B.2 Evaluation rules

$$\boxed{e, \hat{\sigma} \hat{\downarrow} \hat{v}, \hat{\sigma}'}$$

$$\textsc{E-App}\ \frac{e_1, \hat{\sigma} \hat{\downarrow} \lambda x : \tau . \hat{e_1}', \hat{\sigma}' \qquad e_2, \hat{\sigma}' \hat{\downarrow} \hat{v}_2, \hat{\sigma}'' \qquad e_1'[x \mapsto v_2], \hat{\sigma}'' \hat{\downarrow} \hat{v}_1, \hat{\sigma}'''}{e_1 e_2, \hat{\sigma} \hat{\downarrow} \hat{v}_1, \hat{\sigma}'''}$$

$$\textsc{E-IfTrue}\ \frac{e_1, \hat{\sigma} \hat{\downarrow} \mathsf{True}, \hat{\sigma}' \qquad e_2, \hat{\sigma}' \hat{\downarrow} \hat{v}_2, \hat{\sigma}''}{\textbf{if}\, e_1\, \textbf{then}\, e_2\, \textbf{else}\, e_3, \hat{\sigma} \hat{\downarrow} \hat{v}_2, \hat{\sigma}''} \qquad \textsc{E-Ref}\ \frac{e, \hat{\sigma} \hat{\downarrow} \hat{v}, \hat{\sigma}' \qquad l \notin Dom(\hat{\sigma}')}{\textbf{ref}\, e, \hat{\sigma} \hat{\downarrow} l, \hat{\sigma}'[l \mapsto \hat{v}]}$$

$$\textsc{E-IfFalse}\ \frac{e_1, \hat{\sigma} \hat{\downarrow} \mathsf{False}, \hat{\sigma}' \qquad e_3, \hat{\sigma}' \hat{\downarrow} \hat{v}_3, \hat{\sigma}''}{\textbf{if}\, e_1\, \textbf{then}\, e_2\, \textbf{else}\, e_3, \hat{\sigma} \hat{\downarrow} \hat{v}_3, \hat{\sigma}''} \qquad \textsc{E-Deref}\ \frac{e, \hat{\sigma} \hat{\downarrow} l, \hat{\sigma}'}{!e, \hat{\sigma} \hat{\downarrow} \hat{\sigma}'(l), \hat{\sigma}'} \qquad \textsc{E-Value}\ \frac{}{v, \hat{\sigma} \hat{\downarrow} v, \hat{\sigma}}$$

$$\textsc{E-Assign}\ \frac{e_1, \hat{\sigma} \hat{\downarrow} l, \hat{\sigma}' \qquad e_2, \hat{\sigma}' \hat{\downarrow} \hat{v}_2, \hat{\sigma}''}{e_1 := e_2, \hat{\sigma} \hat{\downarrow} \langle\rangle, \hat{\sigma}''[l \mapsto \hat{v}_2]} \qquad \textsc{E-Pair}\ \frac{e_1, \hat{\sigma} \hat{\downarrow} \hat{v}_1, \hat{\sigma}' \qquad e_2, \hat{\sigma}' \hat{\downarrow} \hat{v}_2, \hat{\sigma}''}{\langle e_1, e_2\rangle, \hat{\sigma} \hat{\downarrow} \langle \hat{v}_1, \hat{v}_2\rangle, \hat{\sigma}''}$$

$$\textsc{E-First}\ \frac{e_1, \hat{\sigma} \hat{\downarrow} \hat{v}_1, \hat{\sigma}'}{\mathsf{fst}\langle e_1, e_2\rangle, \hat{\sigma} \hat{\downarrow} \hat{v}_1, \hat{\sigma}'} \qquad \textsc{E-Second}\ \frac{e_2, \hat{\sigma} \hat{\downarrow} \hat{v}_2, \hat{\sigma}'}{\mathsf{snd}\langle e_1, e_2\rangle, \hat{\sigma} \hat{\downarrow} \hat{v}_2, \hat{\sigma}'} \qquad \textsc{E-Cons}\ \frac{e_1, \hat{\sigma} \hat{\downarrow} \hat{v}_1, \hat{\sigma}' \qquad e_2, \hat{\sigma}' \hat{\downarrow} \hat{v}_2, \hat{\sigma}''}{e_1 :: e_2, \hat{\sigma} \hat{\downarrow} \hat{v}_1 :: \hat{v}_2, \hat{\sigma}''}$$

$$\textsc{E-Head}\ \frac{e, \hat{\sigma} \hat{\downarrow} \hat{v}_1 :: \hat{v}_2, \hat{\sigma}'}{\mathsf{head}\, e, \hat{\sigma} \hat{\downarrow} \hat{v}_1, \hat{\sigma}'} \qquad \textsc{E-Tail}\ \frac{e, \hat{\sigma} \hat{\downarrow} \hat{v}_1 :: \hat{v}_2, \hat{\sigma}'}{\mathsf{tail}\, e, \hat{\sigma} \hat{\downarrow} \hat{v}_2, \hat{\sigma}'}$$

$$\textsc{E-Edit}\ \frac{e, \hat{\sigma} \hat{\downarrow} \hat{v}, \hat{\sigma}'}{\square\, e, \hat{\sigma} \hat{\downarrow} \square\, \hat{v}, \hat{\sigma}'} \qquad \textsc{E-Update}\ \frac{e, \hat{\sigma} \hat{\downarrow} l, \hat{\sigma}'}{\blacksquare\, e, \hat{\sigma} \hat{\downarrow} \blacksquare\, l, \hat{\sigma}'} \qquad \textsc{E-Then}\ \frac{e_1, \hat{\sigma} \hat{\downarrow} \hat{t}_1, \hat{\sigma}'}{e_1 \blacktriangleright e_2, \hat{\sigma} \hat{\downarrow} \hat{t}_1 \blacktriangleright e_2, \hat{\sigma}'}$$

$$\textsc{E-Next}\ \frac{e_1, \hat{\sigma} \hat{\downarrow} \hat{t}_1, \hat{\sigma}'}{e_1 \triangleright e_2, \hat{\sigma} \hat{\downarrow} \hat{t}_1 \triangleright e_2, \hat{\sigma}'} \qquad \textsc{E-And}\ \frac{e_1, \hat{\sigma} \hat{\downarrow} \hat{t}_1, \hat{\sigma}' \qquad e_2, \hat{\sigma}' \hat{\downarrow} \hat{t}_2, \hat{\sigma}''}{e_1 \bowtie e_2, \hat{\sigma} \hat{\downarrow} \hat{t}_1 \bowtie \hat{t}_2, \hat{\sigma}''}$$

$$\textsc{E-Or}\ \frac{e_1, \hat{\sigma} \hat{\downarrow} \hat{t}_1, \hat{\sigma}' \qquad e_2, \hat{\sigma}' \hat{\downarrow} \hat{t}_2, \hat{\sigma}''}{e_1 \blacklozenge e_2, \hat{\sigma} \hat{\downarrow} \hat{t}_1 \blacklozenge \hat{t}_2, \hat{\sigma}''}$$

B.3 Striding rules

$$\boxed{t, \hat\sigma \hat\rightsquigarrow \hat t', \hat\sigma'}$$

S-ThenStay
$$\frac{t_1, \hat\sigma \hat\rightsquigarrow \hat{t_1}', \hat\sigma'}{t_1 \blacktriangleright e_2, \hat\sigma \hat\rightsquigarrow \hat{t_1}' \blacktriangleright e_2, \hat\sigma'}\ \mathcal{V}(\hat{t_1}', \hat\sigma') = \bot$$

S-ThenFail
$$\frac{t_1, \hat\sigma \hat\rightsquigarrow \hat{t_1}', \hat\sigma' \qquad e_2\ \hat{v}_1, \hat\sigma' \hat\downarrow \hat{t_2}, \hat\sigma''}{t_1 \blacktriangleright e_2, \hat\sigma \hat\rightsquigarrow \hat{t_1}' \blacktriangleright e_2, \hat\sigma'}\ \mathcal{V}(\hat{t_1}', \hat\sigma') = \hat{v}_1 \wedge \mathcal{F}(\hat{t_2}, \hat\sigma'')$$

S-ThenCont
$$\frac{t_1, \hat\sigma \hat\rightsquigarrow \hat{t_1}', \hat\sigma' \qquad e_2\ \hat{v}_1, \hat\sigma' \hat\downarrow \hat{t_2}, \hat\sigma''}{t_1 \blacktriangleright e_2, \hat\sigma \hat\rightsquigarrow \hat{t_2}, \hat\sigma''}\ \mathcal{V}(\hat{t_1}', \hat\sigma') = \hat{v}_1 \wedge \neg\mathcal{F}(\hat{t_2}, \hat\sigma'')$$

S-OrLeft
$$\frac{t_1, \hat\sigma \hat\rightsquigarrow \hat{t_1}', \hat\sigma'}{t_1 \blacklozenge t_2, \hat\sigma \hat\rightsquigarrow \hat{t_1}', \hat\sigma'}\ \mathcal{V}(\hat{t_1}', \hat\sigma') = \hat{v}_1$$

S-OrRight
$$\frac{t_1, \hat\sigma \hat\rightsquigarrow \hat{t_1}', \hat\sigma' \qquad t_2, \hat\sigma' \hat\rightsquigarrow \hat{t_2}', \hat\sigma''}{t_1 \blacklozenge t_2, \hat\sigma \hat\rightsquigarrow \hat{t_2}', \hat\sigma''}\ \mathcal{V}(\hat{t_1}', \hat\sigma') = \bot \wedge \mathcal{V}(\hat{t_2}', \hat\sigma'') = \hat{v}_2$$

S-OrNone
$$\frac{t_1, \hat\sigma \hat\rightsquigarrow \hat{t_1}', \hat\sigma' \qquad t_2, \hat\sigma' \hat\rightsquigarrow \hat{t_2}', \hat\sigma''}{t_1 \blacklozenge t_2, \hat\sigma \hat\rightsquigarrow \hat{t_1}' \blacklozenge \hat{t_2}', \hat\sigma''}\ \mathcal{V}(\hat{t_1}', \hat\sigma') = \bot \wedge \mathcal{V}(\hat{t_2}', \hat\sigma'') = \bot$$

S-Edit
$$\frac{}{\square\, v, \hat\sigma \hat\rightsquigarrow \square\, v, \hat\sigma}$$

S-Fill
$$\frac{}{\boxtimes\, \tau, \hat\sigma \hat\rightsquigarrow \boxtimes\, \tau, \hat\sigma}$$

S-Update
$$\frac{}{\blacksquare\, l, \hat\sigma \hat\rightsquigarrow \blacksquare\, l, \hat\sigma}$$

S-Fail
$$\frac{}{\lightning, \hat\sigma \hat\rightsquigarrow \lightning, \hat\sigma}$$

S-Xor
$$\frac{}{e_1 \lozenge e_2, \hat\sigma \hat\rightsquigarrow e_1 \lozenge e_2, \hat\sigma}$$

S-Next
$$\frac{t_1, \hat\sigma \hat\rightsquigarrow \hat{t_1}', \hat\sigma'}{t_1 \triangleright e_2, \hat\sigma \hat\rightsquigarrow \hat{t_1}' \triangleright e_2, \hat\sigma'}$$

S-And
$$\frac{t_1, \hat\sigma \hat\rightsquigarrow \hat{t_1}', \hat\sigma' \qquad t_2, \hat\sigma' \hat\rightsquigarrow \hat{t_2}', \hat\sigma''}{t_1 \bowtie t_2, \hat\sigma \hat\rightsquigarrow \hat{t_1}' \bowtie \hat{t_2}', \hat\sigma''}$$

B.4 Normalisation rules

$$\boxed{e, \hat\sigma \hat\Downarrow \hat t, \hat\sigma'}$$

N-Done
$$\frac{e, \hat\sigma \hat\downarrow \hat t, \hat\sigma' \qquad \hat t, \hat\sigma' \hat\rightsquigarrow \hat t', \hat\sigma''}{e, \hat\sigma \hat\Downarrow \hat t, \hat\sigma'}\ \hat\sigma' = \hat\sigma'' \wedge \hat t = \hat t'$$

N-Repeat
$$\frac{e, \hat\sigma \hat\downarrow \hat t, \hat\sigma' \qquad \hat t, \hat\sigma' \hat\rightsquigarrow \hat t', \hat\sigma'' \qquad \hat t', \hat\sigma'' \hat\Downarrow \hat t'', \hat\sigma'''}{e, \hat\sigma \hat\Downarrow \hat t'', \hat\sigma'''}\ \hat\sigma' \neq \hat\sigma'' \vee \hat t \neq \hat t'$$

B.5 Handling rules

$$\boxed{t, \hat\sigma \xrightarrow{j} \hat t', \hat\sigma'}$$

H-Change
$$\frac{}{\square\, v, \hat\sigma \xrightarrow{v'} \square\, v', \hat\sigma}\ v, v' : \tau$$

H-Fill
$$\frac{}{\boxtimes\, \tau, \hat\sigma \xrightarrow{v} \square\, v, \hat\sigma}\ v : \tau$$

H-Update
$$\frac{}{\blacksquare\, l, \hat\sigma \xrightarrow{v} \blacksquare\, l, \hat\sigma[l \mapsto v]}\ \sigma(l), v : \tau$$

H-Next
$$\frac{e_2\ \hat{v}_1, \sigma \hat\Downarrow \hat{t_2}, \hat\sigma'}{t_1 \triangleright e_2, \sigma \xrightarrow{\mathsf{C}} \hat{t_2}, \hat\sigma'}\ \mathcal{V}(t_1, \sigma) = \hat{v}_1 \wedge \neg\mathcal{F}(\hat{t_2}, \hat\sigma')$$

H-PickLeft
$$\frac{e_1, \sigma \hat\Downarrow \hat{t_1}, \hat\sigma'}{e_1 \lozenge e_2, \sigma \xrightarrow{\mathsf{L}} \hat{t_1}, \hat\sigma'}\ \neg\mathcal{F}(\hat{t_1}, \hat\sigma')$$

H-PickRight
$$\frac{e_2, \sigma \hat\Downarrow \hat{t_2}, \hat\sigma'}{e_1 \lozenge e_2, \sigma \xrightarrow{\mathsf{R}} \hat{t_2}, \hat\sigma'}\ \neg\mathcal{F}(\hat{t_2}, \hat\sigma')$$

H-PassThen
$$\frac{t_1, \sigma \xrightarrow{j} \hat{t}_1', \sigma'}{t_1 \blacktriangleright e_2, \sigma \xrightarrow{j} \hat{t}_1' \blacktriangleright e_2, \sigma'}$$

H-PassNext
$$\frac{t_1, \sigma \xrightarrow{j} \hat{t}_1', \sigma'}{t_1 \triangleright e_2, \sigma \xrightarrow{j} \hat{t}_1' \triangleright e_2, \sigma'}$$

H-FirstAnd
$$\frac{t_1, \sigma \xrightarrow{j} \hat{t_1}', \hat\sigma'}{t_1 \bowtie t_2, \sigma \xrightarrow{\mathsf{F}\, j} \hat{t_1}' \bowtie t_2, \hat\sigma'}$$

H-SecondAnd
$$\frac{t_2, \sigma \xrightarrow{j} \hat{t_2}', \hat\sigma'}{t_1 \bowtie t_2, \sigma \xrightarrow{\mathsf{S}\, j} t_1 \bowtie \hat{t_2}', \hat\sigma'}$$

H-FirstOr
$$\frac{t_1, \sigma \xrightarrow{j} \hat{t_1}', \hat\sigma'}{t_1 \blacklozenge t_2, \sigma \xrightarrow{\mathsf{F}\, j} \hat{t_1}' \blacklozenge t_2, \hat\sigma'}$$

H-SecondOr
$$\frac{t_2, \sigma \xrightarrow{j} \hat{t_2}', \hat\sigma'}{t_1 \blacklozenge t_2, \sigma \xrightarrow{\mathsf{S}\, j} t_1 \blacklozenge \hat{t_2}', \hat\sigma'}$$

B.6 Driving rules

$$\boxed{\hat t, \hat\sigma \xRightarrow{j} \hat t', \hat\sigma'}$$

I-Handle
$$\frac{t, \sigma \xrightarrow{j} \hat t', \hat\sigma' \qquad \hat t', \hat\sigma' \hat\Downarrow \hat t'', \hat\sigma''}{t, \sigma \xRightarrow{j} \hat t'', \hat\sigma''}$$

C SOUNDNESS PROOFS

Proof of Lemma ??. We prove Lemma ?? by induction over e.

Case $e = v$

One rule applies, namely $\dfrac{\text{SE-Value}}{v, \sigma \downarrow v, \boxed{\sigma, \mathsf{True}}}$ Since this rule does not generate constraints, any M will do. Since neither the state, nor the expression is altered by the evaluation rule $\dfrac{\text{E-Value}}{v, \hat{\sigma} \Downarrow v, \hat{\sigma}}$, this case holds true trivially.

Case $e = \langle e_1, e_2 \rangle$

One rule applies, namely $\dfrac{e_1, \sigma \downarrow \overline{v_1, \sigma', \boxed{\varphi_1}} \quad e_2, \sigma' \downarrow \overline{v_2, \sigma'', \boxed{\varphi_2}}}{\langle e_1, e_2 \rangle, \sigma \downarrow \overline{\langle v_1, v_2 \rangle, \sigma'', \boxed{\varphi_1 \wedge \varphi_2}}}$ SE-Pair

Provided that $M\varphi_1 \wedge M\varphi_2$, we need to demonstrate that $\dfrac{e_1, \hat{\sigma} \Downarrow \hat{v_1}, \hat{\sigma}' \quad e_2, \hat{\sigma}' \Downarrow \hat{v_2}, \hat{\sigma}''}{\langle e_1, e_2 \rangle, \hat{\sigma} \Downarrow \langle \hat{v_1}, \hat{v_2} \rangle, \hat{\sigma}''}$ E-Pair with $\hat{\sigma} = M\sigma$, $M\langle v_1, v_2 \rangle \equiv \langle \hat{v_1}, \hat{v_2} \rangle$ and $M\sigma'' \equiv \hat{\sigma''}$.

From the induction hypothesis, we obtain the following.

$\forall M_1.M_1\varphi_1 \supset e_1, M_1\sigma \Downarrow \hat{v_1}, \hat{\sigma'} \wedge M_1 v_1 \equiv \hat{v_1} \wedge M_1\sigma' \equiv \hat{\sigma'}$ and $\forall M_2.M_2\varphi_2 \supset e_2, M_2\sigma' \Downarrow \hat{v_2}, \hat{\sigma''} \wedge M_2 v_2 \equiv \hat{v_2} \wedge M_2\sigma' \equiv \hat{\sigma''}$

Since M satisfies both φ_1 and φ_2, and we know that $M\sigma' \equiv \hat{\sigma'}$ we obtain that $e_1, M\sigma \Downarrow \hat{v_1}, \hat{\sigma'}$, $e_2, M\sigma' \Downarrow \hat{v_2}, \hat{\sigma''}$, $M\sigma' \equiv \hat{\sigma'}$, $Mv_1 \equiv \hat{v_1}$ and $Mv_2 \equiv \hat{v_2}$ and therefore $M\langle v_1, v_2 \rangle \equiv \langle \hat{v_1}, \hat{v_2} \rangle$. From the IH we directly obtain that $M\sigma'' \equiv \hat{\sigma''}$.

Case $e = \mathsf{fst}\, e$

One rule applies, namely $\dfrac{e_1, \sigma \downarrow \overline{v_1, \sigma', \boxed{\varphi}}}{\mathsf{fst}\langle e_1, e_2 \rangle, \sigma \downarrow \overline{v_1, \sigma', \boxed{\varphi}}}$ SE-First

Provided that $M\varphi$, we need to demonstrate that $\dfrac{e_1, \hat{\sigma} \Downarrow \hat{v_1}, \hat{\sigma}'}{\mathsf{fst}\langle e_1, e_2 \rangle, \hat{\sigma} \Downarrow \hat{v_1}, \hat{\sigma}'}$ E-First with $\hat{\sigma} = M\sigma$, $Mv_1 \equiv \hat{v_1}$ and $M\sigma' \equiv \hat{\sigma}'$.

From the induction hypothesis, we obtain the following.

$\forall M_1.M_1\varphi \supset e, M_1\sigma \Downarrow \langle \hat{v_1}, \hat{v_2} \rangle, \hat{\sigma'} \wedge M_1\langle v_1, v_2 \rangle \equiv \langle \hat{v_1}, \hat{v_2} \rangle \wedge M_1\sigma' \equiv \hat{\sigma'}$

Since M satisfies φ, we directly obtain that $\mathsf{fst}\, e, \sigma \Downarrow \hat{v_1}$, $Mv_1 \equiv \hat{v_1}$ and $M\sigma' \equiv \hat{\sigma}'$.

Case $e = \mathsf{snd}\, e$

One rule applies, namely $\dfrac{e_2, \sigma \downarrow \overline{v_2, \sigma', \boxed{\varphi}}}{\mathsf{snd}\langle e_1, e_2 \rangle, \sigma \downarrow \overline{v_2, \sigma', \boxed{\varphi}}}$ SE-Second

Provided that $M\varphi$, we need to demonstrate that $\dfrac{e_2, \hat{\sigma} \Downarrow \hat{v_2}, \hat{\sigma}'}{\mathsf{snd}\langle e_1, e_2 \rangle, \hat{\sigma} \Downarrow \hat{v_2}, \hat{\sigma}'}$ E-Second with $\hat{\sigma} = M\sigma$, $Mv_2 \equiv \hat{v_2}$ and $M\sigma' \equiv \hat{\sigma}'$.

From the induction hypothesis, we obtain the following.

$\forall M_1.M_1\varphi \supset e, M_1\sigma \Downarrow \langle \hat{v_1}, \hat{v_2} \rangle, \hat{\sigma'} \wedge M_1\langle v_1, v_2 \rangle \equiv \langle \hat{v_1}, \hat{v_2} \rangle \wedge M_1\sigma' \equiv \hat{\sigma'}$

Since M satisfies φ, we directly obtain that $\mathsf{snd}\, e, \sigma \Downarrow \hat{v_2}$, $Mv_2 \equiv \hat{v_2}$ and $M\sigma' \equiv \hat{\sigma}'$.

Case $e = e_1 :: e_2$

One rule applies, namely $\dfrac{e_1, \sigma \downarrow \overline{v_1, \sigma', \boxed{\varphi_1}} \quad e_2, \sigma' \downarrow \overline{v_2, \sigma'', \boxed{\varphi_2}}}{e_1 :: e_2, \sigma \downarrow \overline{v_1 :: v_2, \sigma'', \boxed{\varphi_1 \wedge \varphi_2}}}$ SE-Cons

Provided that $M\varphi$, we need to demonstrate that $\dfrac{e_1, \hat{\sigma} \Downarrow \hat{v_1}, \hat{\sigma}' \quad e_2, \hat{\sigma}' \Downarrow \hat{v_2}, \hat{\sigma}''}{e_1 :: e_2, \hat{\sigma} \Downarrow \hat{v_1} :: \hat{v_2}, \hat{\sigma}''}$ E-Cons with $bar\sigma = M\sigma$, $Mv_1 :: v_2 \equiv \hat{v_1} :: \hat{v_2}$ and $M\sigma'' \equiv \hat{\sigma''}$.

From the induction hypothesis, we obtain the following.

$\forall M_1.M_1\varphi_1 \supset e_1, M_1\sigma \Downarrow \hat{v_1}, \hat{\sigma'} \wedge M_1 v_1 \equiv \hat{v_1} \wedge M_1\sigma' \equiv \hat{\sigma'}$ and $\forall M_2.M_2\varphi_2 \supset e_2, M_2\sigma' \Downarrow \hat{v_2}, \hat{\sigma''} \wedge M_2 v_2 \equiv \hat{v_2} \wedge M_2\sigma' \equiv \hat{\sigma''}$

Since M satisfies both φ_1 and φ_2, and we know that $M\sigma' \equiv \hat{\sigma}'$ we obtain that $e_1, M\sigma \;\hat{\downarrow}\; \hat{v_1}, \hat{\sigma}', e_2, M\sigma' \;\hat{\downarrow}\; \hat{v_2}, \hat{\sigma}'', M\sigma' \equiv \hat{\sigma}', Mv_1 \equiv \hat{v_1}$ and $Mv_2 \equiv \hat{v_2}$ and therefore $M(v_1 :: v_2) \equiv \hat{v_1} :: \hat{v_2}$. From the IH we directly obtain that $M\sigma'' \equiv \hat{\sigma}''$.

Case $e = \mathsf{head}\, e$

One rule applies, namely $$\text{SE-Head}\;\frac{e, \sigma \;\downarrow\; \overline{v_1 :: v_2, \sigma', \boxed{\varphi}}}{\mathsf{head}\, e, \sigma \;\downarrow\; \overline{v_1, \sigma', \boxed{\varphi}}}$$

Provided that $M\varphi$, we need to demonstrate that $\text{E-Head}\;\dfrac{e, \hat{\sigma} \;\hat{\downarrow}\; \hat{v_1} :: \hat{v_2}, \hat{\sigma}'}{\mathsf{head}\, e, \hat{\sigma} \;\hat{\downarrow}\; \hat{v_1}, \hat{\sigma}'}$ with $\hat{\sigma} = M\sigma$, $Mv_1 \equiv \hat{v_1}$ and $M\sigma' \equiv \hat{\sigma}'$.

From the induction hypothesis, we obtain the following.
$\forall M_1 . M_1\varphi \supset e, M_1\sigma \;\hat{\downarrow}\; \hat{v_1} :: \hat{v_2}, \hat{\sigma}' \wedge M_1(v_1 :: v_2) \equiv \hat{v_1} :: \hat{v_2} \wedge M_1\sigma' \equiv \hat{\sigma}'$

Since M satisfies φ, we directly obtain that $\mathsf{head}\, e, \sigma \;\hat{\downarrow}\; \hat{v_1}$, $Mv_1 \equiv \hat{v_1}$ and $M\sigma' \equiv \hat{\sigma}'$.

Case $e = \mathsf{tail}\, e$

One rule applies, namely $$\text{SE-Tail}\;\frac{e, \sigma \;\downarrow\; \overline{v_1 :: v_2, \sigma', \boxed{\varphi}}}{\mathsf{tail}\, e, \sigma \;\downarrow\; \overline{v_2, \sigma', \boxed{\varphi}}}$$

Provided that $M\varphi$, we need to demonstrate that $\text{E-Tail}\;\dfrac{e, \hat{\sigma} \;\hat{\downarrow}\; \hat{v_1} :: \hat{v_2}, \hat{\sigma}'}{\mathsf{tail}\, e, \hat{\sigma} \;\hat{\downarrow}\; \hat{v_2}, \hat{\sigma}'}$ with $\hat{\sigma} = M\sigma$, $Mv_2 \equiv \hat{v_2}$ and $M\sigma' \equiv \hat{\sigma}'$.

From the induction hypothesis, we obtain the following.
$\forall M_1 . M_1\varphi \supset e, M_1\sigma \;\hat{\downarrow}\; \hat{v_1} :: \hat{v_2}, \hat{\sigma}' \wedge M_1(v_1 :: v_2) \equiv \hat{v_1} :: \hat{v_2} \wedge M_1\sigma' \equiv \hat{\sigma}'$

Since M satisfies φ, we directly obtain that $\mathsf{tail}\, e, \sigma \;\hat{\downarrow}\; \hat{v_2}$, $Mv_2 \equiv \hat{v_2}$ and $M\sigma' \equiv \hat{\sigma}'$.

Case $e = e_1 e_2$

One rule applies, namely $$\text{SE-App}\;\frac{e_1, \sigma \;\downarrow\; \overline{\lambda x : \tau . e_1', \sigma', \boxed{\varphi_1}} \qquad e_2, \sigma' \;\downarrow\; \overline{v_2, \sigma'', \boxed{\varphi_2}} \qquad e_1'[x \mapsto v_2], \sigma'' \;\downarrow\; \overline{v_1, \sigma''', \boxed{\varphi_3}}}{e_1 e_2, \sigma \;\downarrow\; \overline{v_1, \sigma''', \boxed{\varphi_1 \wedge \varphi_2 \wedge \varphi_3}}}$$

Provided that $M\varphi_1 \wedge M\varphi_2 \wedge M\varphi_3$, we need to demonstrate that $$\text{E-App}\;\frac{e_1, \hat{\sigma} \;\hat{\downarrow}\; \lambda x : \tau . \hat{e_1}', \hat{\sigma}' \qquad e_2, \hat{\sigma}' \;\hat{\downarrow}\; \hat{v_2}, \hat{\sigma}'' \qquad e_1'[x \mapsto v_2], \hat{\sigma}'' \;\hat{\downarrow}\; \hat{v_1}, \hat{\sigma}'''}{e_1 e_2, \hat{\sigma} \;\hat{\downarrow}\; \hat{v_1}, \hat{\sigma}'''}$$ with $\hat{\sigma} = M\sigma$, $Mv_1 \equiv \hat{v_1}$ and $M\sigma''' \equiv \hat{\sigma}'''$.

From the induction hypothesis, we obtain the following.
$\forall M_1 . M_1\varphi_1 \supset e_1, M_1\sigma \;\hat{\downarrow}\; \lambda x : \tau . \hat{e_1'}, \hat{\sigma}' \wedge M_1\lambda x : \tau . e_1' \equiv \lambda x : \tau . \hat{e_1'} \wedge M_1\sigma' \equiv \hat{\sigma}'$ and
$\forall M_2 . M_2\varphi_2 \supset e_2, M_2\sigma' \;\hat{\downarrow}\; \hat{v_2}, \hat{\sigma}'' \wedge M_2v_2 \equiv \hat{v_2} \wedge M_2\sigma'' \equiv \hat{\sigma}''$ and
$\forall M_3 . M_3\varphi_3 \supset \hat{e_1'}[x \mapsto \hat{v_2}], M_3\sigma'' \;\hat{\downarrow}\; \hat{v_1}, \hat{\sigma}''' \wedge M_3v_1 \equiv \hat{v_1} \wedge M_3\sigma''' \equiv \hat{\sigma}'''$.

Since M satisfies both φ_1, φ_2 and φ_3, and we know that $M\sigma' \equiv \hat{\sigma}'$ and $M\sigma'' \equiv \hat{\sigma}''$, we obtain that $e_1, M\sigma \;\hat{\downarrow}\; \lambda x : \tau . \hat{e_1'}, \hat{\sigma}', e_2, M\sigma' \;\hat{\downarrow}\; \hat{v_2}, \hat{\sigma}''$ and $\hat{e_1'}[x \mapsto \hat{v_2}], M\sigma'' \;\hat{\downarrow}\; \hat{v_1}, \hat{\sigma}'''$. We can then directly conclude that $Mv_1 \equiv \hat{v_1}$ and $M\sigma''' \equiv \hat{\sigma}'''$.

Case $e = \textbf{if}\; e_1 \;\textbf{then}\; e_2 \;\textbf{else}\; e_3$

One rule applies, namely $$\text{SE-If}\;\frac{e_1, \sigma \;\downarrow\; \overline{v_1, \sigma', \boxed{\varphi_1}} \qquad \boxed{e_2, \sigma' \;\downarrow\; \overline{v_2, \sigma'', \varphi_2}} \qquad \boxed{e_3, \sigma' \;\downarrow\; \overline{v_3, \sigma''', \varphi_3}}}{\textbf{if}\; e_1 \;\textbf{then}\; e_2 \;\textbf{else}\; e_3, \sigma \;\downarrow\; \boxed{\overline{v_2, \sigma'', \varphi_1 \wedge \varphi_2 \wedge v_1} \cup \overline{v_3, \sigma''', \varphi_1 \wedge \varphi_3 \wedge \neg v_1}}}$$

In case that $M\varphi_1 \wedge M\varphi_2 \wedge Mv_1$, we need to demonstrate that $\text{E-IfTrue}\;\dfrac{e_1, \hat{\sigma} \;\hat{\downarrow}\; \mathsf{True}, \hat{\sigma}' \qquad e_2, \hat{\sigma}' \;\hat{\downarrow}\; \hat{v_2}, \hat{\sigma}''}{\textbf{if}\; e_1 \;\textbf{then}\; e_2 \;\textbf{else}\; e_3, \hat{\sigma} \;\hat{\downarrow}\; \hat{v_2}, \hat{\sigma}''}$ with $\hat{\sigma} = M\sigma$, $Mv_2 = \hat{v_2}$ and $M\sigma'' = \hat{\sigma}''$.

From the induction hypothesis, we obtain the following.
$\forall M_1 . M_1\varphi_1 \supset e_1, M_1\sigma \;\hat{\downarrow}\; \hat{v_1}, \hat{\sigma}' \wedge M_1v_1 \equiv \hat{v_1} \wedge M_1\sigma' \equiv \hat{\sigma}'$ and
$\forall M_2 . M_2\varphi_2 \supset e_2, M_2\sigma' \;\hat{\downarrow}\; \hat{v_2}, \hat{\sigma}'' \wedge M_2v_2 \equiv \hat{v_2} \wedge M_2\sigma'' \equiv \hat{\sigma}''$.

Since M satisfies φ_1, and $Mv_1 = \mathsf{True}$, we know from the application of the induction hypothesis above, that $\hat{v_1} = \mathsf{True}$. Furthermore, M satisfies φ_2, so we directly obtain that $Mv_2 = \hat{v_2}$ and $M\sigma'' = \hat{\sigma}''$.

In case that $M\varphi_1 \wedge M\varphi_3 \wedge M\neg v_1$, we need to demonstrate that $\dfrac{e_1, \hat{\sigma} \mathrel{\hat{\downarrow}} \mathsf{False}, \hat{\sigma}' \qquad e_3, \hat{\sigma}' \mathrel{\hat{\downarrow}} \hat{v_3}, \hat{\sigma}''}{\textbf{if}\ e_1\ \textbf{then}\ e_2\ \textbf{else}\ e_3, \hat{\sigma} \mathrel{\hat{\downarrow}} \hat{v_3}, \hat{\sigma}''}$ E-IfFalse with $\hat{\sigma} = M\sigma$, $Mv_3 = \hat{v_3}$ and $M\sigma'' = \hat{\sigma''}$.

From the induction hypothesis, we obtain the following.
$\forall M_1 . M_1\varphi_1 \supset e_1, M_1\sigma \mathrel{\hat{\downarrow}} \hat{v_1}, \hat{\sigma'} \wedge M_1 v_1 \equiv \hat{v_1} \wedge M_1\sigma' \equiv \hat{\sigma'}$ and
$\forall M_3 . M_3\varphi_3 \supset e_3, M_3\sigma' \mathrel{\hat{\downarrow}} \hat{v_3}, \hat{\sigma''} \wedge M_3 v_3 \equiv \hat{v_3} \wedge M_3\sigma'' \equiv \hat{\sigma''}$.

Since M satisfies φ_1, and $Mv_1 = \mathsf{False}$, we know from the application of the induction hypothesis above, that $\hat{v_1} = \mathsf{False}$. Furthermore, M satisfies φ_3, so we directly obtain that $Mv_3 = \hat{v_3}$ and $M\sigma'' = \hat{\sigma''}$.

Case $e = \textbf{ref}\ e$

One rule applies, namely $\dfrac{e, \sigma \downarrow \overline{v, \sigma', \varphi} \qquad l \notin Dom(\sigma')}{\textbf{ref}\ e, \sigma \downarrow \overline{l, \sigma'[l \mapsto v], \varphi}}$ SE-Ref

Provided that $M\varphi$, we need to demonstrate that $\dfrac{e, \hat{\sigma} \mathrel{\hat{\downarrow}} \hat{v}, \hat{\sigma}' \qquad l \notin Dom(\hat{\sigma}')}{\textbf{ref}\ e, \hat{\sigma} \mathrel{\hat{\downarrow}} l, \hat{\sigma}'[l \mapsto \hat{v}]}$ E-Ref with $\hat{\sigma} = M\sigma$, $Ml \equiv l$ and $M\sigma'[l \mapsto v] \equiv \hat{\sigma'}[l \mapsto \hat{v}]$.

From the induction hypothesis, we obtain the following.
$\forall M_1 . M_1\varphi \supset e, M_1\sigma \mathrel{\hat{\downarrow}} \hat{v}, \hat{\sigma'} \wedge M_1 v \equiv \hat{v} \wedge M_1\sigma' \equiv \hat{\sigma'}$.

We assume that the assignment of location references happens in a deterministic manner, and that we can therefore conclude that exactly the same l is used in both cases. Since l cannot contain any symbols, $Ml \equiv l$ holds trivially.

Since M satisfies φ, we obtain that $e, M\sigma \mathrel{\hat{\downarrow}} \hat{v}, \hat{\sigma'}$ and $Mv \equiv \hat{v}$. This, together with $M\sigma' \equiv \hat{\sigma'}$ obtained from the induction hypothesis, we can conclude that $M\sigma'[l \mapsto v] \equiv \hat{\sigma'}[l \mapsto \hat{v}]$.

Case $e = !e$

One rule applies, namely $\dfrac{e, \sigma \downarrow \overline{l, \sigma', \varphi}}{!e, \sigma \downarrow \overline{\sigma'(l), \sigma', \varphi}}$ SE-Deref

Provided that $M\varphi$, we need to demonstrate that $\dfrac{e, \hat{\sigma} \mathrel{\hat{\downarrow}} l, \hat{\sigma}'}{!e, \hat{\sigma} \mathrel{\hat{\downarrow}} \hat{\sigma}'(l), \hat{\sigma}'}$ E-Deref with $\hat{\sigma} = M\sigma$, $M\sigma'(l) \equiv \hat{\sigma'}(l)$ and $M\sigma' \equiv \hat{\sigma'}$.

From the induction hypothesis, we obtain the following.
$\forall M_1 . M_1\varphi \supset e, M_1\sigma \mathrel{\hat{\downarrow}} l, \hat{\sigma'} \wedge M_1 l \equiv l \wedge M_1\sigma' \equiv \hat{\sigma'}$.

Note that since l cannot contain any symbols, $Ml \equiv l$ holds trivially.

Since M satisfies φ, we immediately obtain $e, M\sigma \mathrel{\hat{\downarrow}} l, \hat{\sigma'}$, and $M\sigma' \equiv \hat{\sigma'}$.

Case $e = e_1 := e_2$

One rule applies, namely $\dfrac{e_1, \sigma \downarrow \overline{l, \sigma', \varphi_1} \qquad e_2, \sigma' \downarrow \overline{v_2, \sigma'', \varphi_2}}{e_1 := e_2, \sigma \downarrow \overline{\langle\rangle, \sigma''[l \mapsto v_2], \varphi_1 \wedge \varphi_2}}$ SE-Assign

Provided that $M\varphi_1 \wedge M\varphi_2$, we need to demonstrate that $\dfrac{e_1, \hat{\sigma} \mathrel{\hat{\downarrow}} l, \hat{\sigma}' \qquad e_2, \hat{\sigma}' \mathrel{\hat{\downarrow}} \hat{v_2}, \hat{\sigma}''}{e_1 := e_2, \hat{\sigma} \mathrel{\hat{\downarrow}} \langle\rangle, \hat{\sigma}''[l \mapsto \hat{v_2}]}$ E-Assign with $\hat{\sigma} = M\sigma$, $M\langle\rangle \equiv \langle\rangle$, which holds true trivially, and $M\sigma''[l \mapsto v_2] \equiv \hat{\sigma''}[l \mapsto \hat{v_2}]$.

From the induction hypothesis, we obtain the following.
$\forall M_1 . M_1\varphi_1 \supset e_1, M_1\sigma \mathrel{\hat{\downarrow}} l, \hat{\sigma'} \wedge M_1 l \equiv l \wedge M_1\sigma' \equiv \hat{\sigma'}$ and
$\forall M_2 . M_2\varphi_2 \supset e_2, M_2\sigma' \mathrel{\hat{\downarrow}} \hat{v_2}, \hat{\sigma''} \wedge M_2 v_2 \equiv \hat{v_2} \wedge M_2\sigma' \equiv \hat{\sigma''}$

Since M satisfies both φ_1 and φ_2, and we know that $M\sigma' \equiv \hat{\sigma'}$, we obtain that $e_1, M\sigma \mathrel{\hat{\downarrow}} l, \hat{\sigma'}$, $e_2, M\sigma' \mathrel{\hat{\downarrow}} \hat{v_2}, \hat{\sigma''}$, $Ml \equiv l$, $Mv_2 \equiv \hat{v_2}$ and $M\sigma'' \equiv \hat{\sigma''}$ and therefore $M\sigma''[l \mapsto v_2] \equiv \hat{\sigma''}[l \mapsto \hat{v_2}]$.

Case $e = \Box\, e$

One rule applies, namely $\dfrac{e, \sigma \ \downarrow\ \overline{v, \sigma', \boxed{\varphi}}}{\Box\, e, \sigma \ \downarrow\ \overline{\overline{\Box\, v, \sigma', \boxed{\varphi}}}}$ SE-Edit

Provided that $M\varphi$, we need to demonstrate that $\dfrac{e, \hat{\sigma} \Downarrow \hat{v}, \hat{\sigma}'}{\Box\, e, \hat{\sigma} \Downarrow \Box\, \hat{v}, \hat{\sigma}'}$ E-Edit with $\hat{\sigma} = M\sigma$, $M\,\Box\, v \equiv \Box\, \hat{v}$ and $M\sigma' \equiv \hat{\sigma}'$.

From the induction hypothesis, we obtain the following.
$\forall M_1.M_1\varphi \supset e, M_1\sigma \Downarrow \hat{v}, \hat{\sigma}' \wedge M_1 v \equiv \hat{v} \wedge M_1\sigma' \equiv \hat{\sigma}'$.

Since M satisfies φ, we obtain that $e, M\sigma \Downarrow \hat{v}, \hat{\sigma}'$, $M\,\Box\, v \equiv \Box\, \hat{v}$. We can furthermore directly conclude that $\sigma' M \equiv \hat{\sigma}'$.

Case $e = \boxtimes\, \tau$

One rule applies, namely $\dfrac{}{\boxtimes\, \tau, \sigma \ \downarrow\ \boxtimes\, \tau, \sigma, \boxed{\mathsf{True}}}$ SE-Enter

Provided that $M\varphi$, we need to demonstrate that $\dfrac{}{\boxtimes\, \tau, \hat{\sigma} \Downarrow \boxtimes\, \tau, \hat{\sigma}}$ E-Enter with $\hat{\sigma} = M\sigma$, $M \boxtimes \tau \equiv \boxtimes\, \tau$, which holds trivially since types do not hold symbols, and $M\sigma \equiv \hat{\sigma}$, which also hols trivially from the premise.

Case $e = \blacksquare\, e$

One rule applies, namely $\dfrac{e, \sigma \ \downarrow\ \overline{l, \sigma', \boxed{\varphi}}}{\blacksquare\, e, \sigma \ \downarrow\ \overline{\overline{\blacksquare\, l, \sigma', \boxed{\varphi}}}}$ SE-Update

Provided that $M\varphi$, we need to demonstrate that $\dfrac{e, \hat{\sigma} \Downarrow l, \hat{\sigma}'}{\blacksquare\, e, \hat{\sigma} \Downarrow \blacksquare\, l, \hat{\sigma}'}$ E-Update with $\hat{\sigma} = M\sigma$, $M\,\blacksquare\, l \equiv \blacksquare\, l$ and $M\sigma' \equiv \hat{\sigma}'$.

From the induction hypothesis, we obtain the following.
$\forall M_1.M_1\varphi \supset e, M_1\sigma \Downarrow l, \hat{\sigma}' \wedge M_1 l \equiv l \wedge M_1\sigma' \equiv \hat{\sigma}'$.

Since M satisfies φ, we obtain that $e, M\sigma \Downarrow l, \hat{\sigma}'$, and $M\,\blacksquare\, l \equiv \blacksquare\, l$. We can furthermore directly conclude that $M\sigma' \equiv \hat{\sigma}'$.

Case $e = e_1 \blacktriangleright e_2$

One rule applies, namely $\dfrac{e_1, \sigma \ \downarrow\ \overline{t_1, \sigma', \boxed{\varphi}}}{e_1 \blacktriangleright e_2, \sigma \ \downarrow\ \overline{\overline{t_1 \blacktriangleright e_2, \sigma', \boxed{\varphi}}}}$ SE-Then

Provided that $M\varphi$, we need to demonstrate that $\dfrac{e_1, \hat{\sigma} \Downarrow \hat{t_1}, \hat{\sigma}'}{e_1 \blacktriangleright e_2, \hat{\sigma} \Downarrow \hat{t_1} \blacktriangleright e_2, \hat{\sigma}'}$ E-Then with $\hat{\sigma} = M\sigma$, $Mt_1 \blacktriangleright e_2 \equiv \hat{t_1} \blacktriangleright e_2$ and $M\sigma' \equiv \hat{\sigma}'$.

From the induction hypothesis, we obtain the following.
$\forall M_1.M_1\varphi \supset e, M_1\sigma \Downarrow \hat{t_1}, \hat{\sigma}' \quad M_1 t_1 \equiv \hat{t_1} \wedge M_1\sigma' \equiv \hat{\sigma}'$.

Since M satisfies φ, we obtain that $e, M\sigma \Downarrow \hat{t_1}, \hat{\sigma}'$ and $Mt_1 \blacktriangleright e_2 \equiv \hat{t_1} \blacktriangleright e_2$. We can furthermore directly conclude that $M\sigma' \equiv \hat{\sigma}'$.

Case $e = e_1 \rhd e_2$

One rule applies, namely $\dfrac{e_1, \sigma \ \downarrow\ \overline{t_1, \sigma', \boxed{\varphi}}}{e_1 \rhd e_2, \sigma \ \downarrow\ \overline{\overline{t_1 \rhd e_2, \sigma', \boxed{\varphi}}}}$ SE-Next

Provided that $M\varphi$, we need to demonstrate that $\dfrac{e_1, \hat{\sigma} \Downarrow \hat{t_1}, \hat{\sigma}'}{e_1 \rhd e_2, \hat{\sigma} \Downarrow \hat{t_1} \rhd e_2, \hat{\sigma}'}$ E-Next with $\hat{\sigma} = M\sigma$, $Mt_1 \rhd e_2 \equiv \hat{t_1} \blacktriangleright e_2$ and $M\sigma' \equiv \hat{\sigma}'$.

From the induction hypothesis, we obtain the following.
$\forall M_1.M_1\varphi \supset e, M_1\sigma \Downarrow \hat{t_1}, \hat{\sigma}' \wedge M_1 t_1 \equiv \hat{t_1} \wedge M_1\sigma' \equiv \hat{\sigma}'$.

Since M satisfies φ, we obtain that $e, M\sigma \Downarrow \hat{t_1}, \hat{\sigma}'$ and $Mt_1 \rhd e_2 \equiv \hat{t_1} \rhd e_2$. We can furthermore directly conclude that $M\sigma' \equiv \hat{\sigma}'$.

Case $e = e_1 \blacklozenge e_2$

One rule applies, namely $\dfrac{e_1, \sigma \downarrow \overline{t_1, \sigma', \boxed{\varphi_1}} \quad e_2, \sigma' \downarrow \overline{t_2, \sigma'', \boxed{\varphi_2}}}{e_1 \blacklozenge e_2, \sigma \downarrow \overline{t_1 \blacklozenge t_2, \sigma'', \boxed{\varphi_1 \wedge \varphi_2}}}$ SE-Or

Provided that $M\varphi_1 \wedge M\varphi_2$, we need to demonstrate that $\dfrac{e_1, \hat{\sigma} \Downarrow \hat{t_1}, \hat{\sigma}' \quad e_2, \hat{\sigma}' \Downarrow \hat{t_2}, \hat{\sigma}''}{e_1 \blacklozenge e_2, \hat{\sigma} \Downarrow \hat{t_1} \blacklozenge \hat{t_2}, \hat{\sigma}''}$ E-Or with $\hat{\sigma} = M\sigma$, $Mt_1 \blacklozenge t_2 \equiv \hat{t_1} \blacklozenge \hat{t_2}$ and $M\sigma'' \equiv \hat{\sigma''}$.

From the induction hypothesis, we obtain the following.
$\forall M_1.M_1\varphi_1 \supset e_1, M_1\sigma \Downarrow \hat{t_1}, \hat{\sigma'} \wedge M_1t_1 \equiv \hat{t_1} \wedge M_1\sigma' \equiv \hat{\sigma'}$ and
$\forall M_2.M_2\varphi_2 \supset e_2, M_2\sigma \Downarrow \hat{t_1}, \hat{\sigma'} \wedge M_2t_2 \equiv \hat{t_2} \wedge M_2\sigma' \equiv \hat{\sigma'}$

Since M satisfies both φ_1 and φ_2, and we know that $M\sigma' \equiv \hat{\sigma'}$, we obtain that $e_1, M\sigma \Downarrow \hat{t_1}, \hat{\sigma'}$, $e_2, M\sigma' \Downarrow \hat{t_2}, \hat{\sigma}$, $Mt_1 \equiv \hat{t_1}$ and $Mt_2 \equiv \hat{t_2}$ and therefore $Mt_1 \blacklozenge t_2 \equiv \hat{t_1} \blacklozenge \hat{t_2}$. From the IH we directly obtain that $M\sigma'' \equiv \hat{\sigma''}$.

Case $e = e_1 \lozenge e_2$

One rule applies, namely $\dfrac{}{e_1 \lozenge e_2, \sigma \downarrow e_1 \lozenge e_2, \sigma, \boxed{\mathsf{True}}}$ SE-Xor

Provided that $M\varphi$, we need to demonstrate that $\dfrac{}{e_1 \lozenge e_2, \hat{\sigma} \Downarrow e_1 \lozenge e_2, \hat{\sigma}}$ E-Xor with $\hat{\sigma} = M\sigma$, $Me_1 \lozenge e_2 \equiv \hat{e_1} \lozenge \hat{e_2}$, which holds trivially, and $M\sigma \equiv \hat{\sigma}$, which also holds trivially from the premise.

Case $e = \lightning$

One rule applies, namely $\dfrac{}{\lightning, \sigma \downarrow \lightning, \sigma, \boxed{\mathsf{True}}}$ SE-Fail

Provided that $M\varphi$, we need to demonstrate that $\dfrac{}{\lightning, \hat{\sigma} \Downarrow \lightning, \hat{\sigma}}$ E-Fail with $\hat{\sigma} = M\sigma$, $M \lightning \equiv \lightning$, which holds trivially since fail do not hold symbols, and $M\sigma \equiv \hat{\sigma}$, which also hols trivially from the premise.

□

Proof of Lemma **??**. We prove Lemma **??** by induction over t.

Case $t = t_1 \blacktriangleright e_2$

Three rules apply.

Case $\dfrac{t_1, \sigma \rightsquigarrow \overline{t_1', \sigma', \boxed{\varphi}}}{t_1 \blacktriangleright e_2, \sigma \rightsquigarrow \overline{t_1' \blacktriangleright e_2, \sigma', \boxed{\varphi}}}\ \mathcal{V}(t_1', \sigma') = \bot$ SS-ThenStay

Provided that $M\varphi \equiv \mathsf{True}$ we need to demonstrate that $\dfrac{t_1, \hat{\sigma} \hat{\rightsquigarrow} \hat{t_1}', \hat{\sigma}'}{t_1 \blacktriangleright e_2, \hat{\sigma} \hat{\rightsquigarrow} \hat{t_1}' \blacktriangleright e_2, \hat{\sigma}'}\ \mathcal{V}(\hat{t_1}', \hat{\sigma}') = \bot$ S-ThenStay with $\hat{\sigma} = M\sigma$, $Mt_1' \blacktriangleright e_2 \equiv \hat{t_1'} \blacktriangleright e_2$ and $M\sigma' \equiv \hat{\sigma'}$.

From the induction hypothesis, we obtain the following.
$\forall M_1.M_1\varphi \supset t_1, M_1\sigma \hat{\rightsquigarrow} \hat{t_1'}, \hat{\sigma'} \wedge M_1t_1' \equiv \hat{t_1'} \wedge M_1\sigma' \equiv \hat{\sigma'}$.

Since M satisfies φ, we know that $t_1, M\sigma \hat{\rightsquigarrow} \hat{t_1'}, \hat{\sigma'}$ and $Mt_1' \equiv \hat{t_1'}$, and therefore also $Mt_1' \blacktriangleright e_2 \equiv \hat{t_1'} \blacktriangleright e_2$, and from the induction hypothesis, we directly obtain $M\sigma' \equiv \hat{\sigma'}$.

Case $$\textsc{SS-ThenFail}\ \frac{t_1,\sigma \rightsquigarrow \overline{t_1',\sigma',\boxed{\varphi}} \qquad e_2\; v_1,\sigma' \downarrow \overline{t_2,\sigma'',\_}}{t_1 \blacktriangleright e_2,\sigma \rightsquigarrow \overline{\overline{t_1' \blacktriangleright e_2,\sigma',\boxed{\varphi}}}}\ \mathcal{V}(t_1',\sigma') = v_1 \wedge \mathcal{F}(t_2,\sigma'')$$

Provided that $M\varphi \equiv$ True we need to demonstrate that $\textsc{S-ThenFail}\ \dfrac{t_1,\hat{\sigma} \mathrel{\hat{\rightsquigarrow}} \hat{t_1}',\hat{\sigma}' \qquad e_2\; \hat{v}_1,\hat{\sigma}' \mathrel{\hat{\downarrow}} \hat{t}_2,\hat{\sigma}''}{t_1 \blacktriangleright e_2,\hat{\sigma} \mathrel{\hat{\rightsquigarrow}} \hat{t_1}' \blacktriangleright e_2,\hat{\sigma}'}\ \mathcal{V}(\hat{t_1}',\hat{\sigma}') = \hat{v}_1 \wedge \mathcal{F}(\hat{t}_2,\hat{\sigma}'')$ with $\hat{\sigma} = M\sigma$, $Mt_1' \blacktriangleright e_2 \equiv \hat{t}_1' \blacktriangleright e_2$ and $M\sigma' \equiv \hat{\sigma}'$.

From the induction hypothesis, we obtain the following.
$\forall M_1.M_1\varphi \supset t_1, M_1\sigma \mathrel{\hat{\rightsquigarrow}} \hat{t}_1',\hat{\sigma}' \wedge M_1t_1' \equiv \hat{t}_1' \wedge M_1\sigma' \equiv \hat{\sigma}'$.

Since M satisfies φ, we know that $t_1, M\sigma \mathrel{\hat{\rightsquigarrow}} \hat{t}_1',\hat{\sigma}'$ and $Mt_1' \equiv \hat{t}_1'$, and therefore also $Mt_1' \blacktriangleright e_2 \equiv \hat{t}_1' \blacktriangleright e_2$, and from the induction hypothesis, we directly obtain $M\sigma' \equiv \hat{\sigma}'$.

Case $$\textsc{SS-ThenCont}\ \frac{t_1,\sigma \rightsquigarrow \overline{t_1',\sigma',\boxed{\varphi_1}} \qquad e_2\; v_1,\sigma' \downarrow \overline{t_2,\sigma'',\boxed{\varphi_2}}}{t_1 \blacktriangleright e_2,\sigma \rightsquigarrow \overline{\overline{t_2,\sigma'',\boxed{\varphi_1 \wedge \varphi_2}}}}\ \mathcal{V}(t_1',\sigma') = v_1 \wedge \neg\mathcal{F}(t_2,\sigma'')$$

Provided that $M\varphi_1 \wedge M\varphi_2$ we need to demonstrate that $\textsc{S-ThenCont}\ \dfrac{t_1,\hat{\sigma} \mathrel{\hat{\rightsquigarrow}} \hat{t_1}',\hat{\sigma}' \qquad e_2\; \hat{v}_1,\hat{\sigma}' \mathrel{\hat{\downarrow}} \hat{t}_2,\hat{\sigma}''}{t_1 \blacktriangleright e_2,\hat{\sigma} \mathrel{\hat{\rightsquigarrow}} \hat{t}_2,\hat{\sigma}''}\ \mathcal{V}(\hat{t_1}',\hat{\sigma}') = \hat{v}_1 \wedge \neg\mathcal{F}(\hat{t}_2,\hat{\sigma}'')$ with $\hat{\sigma} = M\sigma$, $Mt_2 \equiv \hat{t}_2 \blacktriangleright e_2$ and $M\sigma'' \equiv \widehat{\sigma''}$.

From the induction hypothesis, we obtain the following.
$\forall M_1.M_1\varphi_1 \supset t_1, M_1\sigma \mathrel{\hat{\rightsquigarrow}} \hat{t}_1',\hat{\sigma}' \supset M_1t_1' \equiv \hat{t}_1' \wedge M_1\sigma' \equiv \hat{\sigma}'$.
From Lemma ?? we know that
$\forall M_2.M_2\varphi_2 \supset e_2\hat{v}_1M_2\sigma' \mathrel{\hat{\downarrow}} \hat{t}_2,\widehat{\sigma''} \quad M_2t_2 \equiv \hat{t}_2 \wedge M_2\sigma'' \equiv \widehat{\sigma''}$.

Since M satisfies both φ_1 and φ_2, we know that $t_1, M\sigma \mathrel{\hat{\rightsquigarrow}} \hat{t}_1',\hat{\sigma}'$ and $e_2\hat{v}_1M\sigma' \mathrel{\hat{\downarrow}} \hat{t}_2,\widehat{\sigma''}$, $Mt_2 \equiv \hat{t}_2$, and from the induction hypothesis, we directly obtain $M\sigma'' \equiv \widehat{\sigma''}$.

Case $t = t_1 \blacklozenge t_2$

Three rules apply.

Case $$\textsc{SS-OrLeft}\ \frac{t_1,\sigma \rightsquigarrow \overline{t_1',\sigma',\boxed{\varphi}}}{t_1 \blacklozenge t_2,\sigma \rightsquigarrow \overline{\overline{t_1',\sigma',\boxed{\varphi}}}}\ \mathcal{V}(t_1',\sigma') = v_1$$

Provided that $M\varphi \equiv$ True we need to demonstrate that $\textsc{S-OrLeft}\ \dfrac{t_1,\hat{\sigma} \mathrel{\hat{\rightsquigarrow}} \hat{t_1}',\hat{\sigma}'}{t_1 \blacklozenge t_2,\hat{\sigma} \mathrel{\hat{\rightsquigarrow}} \hat{t_1}',\hat{\sigma}'}\ \mathcal{V}(\hat{t_1}',\hat{\sigma}') = \hat{v}_1$ with $\hat{\sigma} = M\sigma$, $Mt_1' \equiv \hat{t}_1'$ and $M\sigma' \equiv \hat{\sigma}'$.

From the induction hypothesis, we obtain the following.
$\forall M_1.M_1\varphi \supset t_1, M_1\sigma \mathrel{\hat{\rightsquigarrow}} \hat{t}_1',\hat{\sigma}' \quad M_1t_1' \equiv \hat{t}_1' \wedge M_1\sigma' \equiv \hat{\sigma}'$.

Since M satisfies φ, we know that $t_1, M\sigma \mathrel{\hat{\rightsquigarrow}} \hat{t}_1',\hat{\sigma}'$, $Mt_1' \equiv \hat{t}_1'$ and $M\sigma' \equiv \hat{\sigma}'$.

Case $$\textsc{SS-OrRight}\ \frac{t_1,\sigma \rightsquigarrow \overline{t_1',\sigma',\boxed{\varphi_1}} \qquad t_2,\sigma' \rightsquigarrow \overline{t_2',\sigma'',\boxed{\varphi_2}}}{t_1 \blacklozenge t_2,\sigma \rightsquigarrow \overline{\overline{t_2',\sigma'',\boxed{\varphi_1 \wedge \varphi_2}}}}\ \mathcal{V}(t_1',\sigma') = \bot \wedge \mathcal{V}(t_2',\sigma'') = v_2$$

Provided that $M\varphi_1 \wedge M\varphi_2$ we need to deomstrate that $\textsc{S-OrRight}\ \dfrac{t_1,\hat{\sigma} \mathrel{\hat{\rightsquigarrow}} \hat{t_1}',\hat{\sigma}' \qquad t_2,\hat{\sigma}' \mathrel{\hat{\rightsquigarrow}} \hat{t_2}',\hat{\sigma}''}{t_1 \blacklozenge t_2,\hat{\sigma} \mathrel{\hat{\rightsquigarrow}} \hat{t_2}',\hat{\sigma}''}\ \mathcal{V}(\hat{t_1}',\hat{\sigma}') = \bot \wedge \mathcal{V}(\hat{t_2}',\hat{\sigma}'') = \hat{v}_2$ with $\hat{\sigma} = M\sigma$, $Mt_2' \equiv \hat{t}_2'$ and $M\sigma'' \equiv \widehat{\sigma''}$.

From the induction hypothesis, we obtain the following.
$\forall M_1.M_1\varphi_1 \supset t_1, M_1\sigma \mathrel{\hat{\rightsquigarrow}} \hat{t}_1',\hat{\sigma}' \wedge M_1t_1' \equiv \hat{t}_1' \wedge M_1\sigma' \equiv \hat{\sigma}'$ and
$\forall M_2.M_2\varphi_2 \supset t_2, M_2\sigma' \mathrel{\hat{\rightsquigarrow}} \hat{t}_2',\widehat{\sigma''} \wedge M_2t_2' \equiv \hat{t}_2' \wedge M_2\sigma'' \equiv \widehat{\sigma''}$.

Since M satisfies both φ_1 and φ_2, we know that $t_1, M\sigma \mathrel{\hat{\rightsquigarrow}} \hat{t}_1',\hat{\sigma}'$ and $t_2, M\sigma' \mathrel{\hat{\rightsquigarrow}} \hat{t}_2',\widehat{\sigma''}$, $Mt_2' \equiv \hat{t}_2'$ and $M\sigma'' \equiv \widehat{\sigma''}$.

Case $\dfrac{t_1, \sigma \rightsquigarrow \overline{t_1', \sigma', \boxed{\varphi_1}} \qquad t_2, \sigma' \rightsquigarrow \overline{t_2', \sigma'', \boxed{\varphi_2}}}{t_1 \blacklozenge t_2, \sigma \rightsquigarrow \overline{t_1' \blacklozenge t_2', \sigma'', \boxed{\varphi_1 \wedge \varphi_2}}}$ $\mathcal{V}(t_1', \sigma') = \bot \wedge \mathcal{V}(t_2', \sigma'') = \bot$ (SS-OrNone)

Provided that $M\varphi_1 \wedge M\varphi_2$ we need to demonstrate that $\dfrac{t_1, \hat{\sigma} \hat{\rightsquigarrow} \hat{t_1}', \hat{\sigma}' \qquad t_2, \hat{\sigma}' \hat{\rightsquigarrow} \hat{t_2}', \hat{\sigma}''}{t_1 \blacklozenge t_2, \hat{\sigma} \hat{\rightsquigarrow} \hat{t_1}' \blacklozenge \hat{t_2}', \hat{\sigma}''}$ $\mathcal{V}(\hat{t_1}', \hat{\sigma}') = \bot \wedge \mathcal{V}(\hat{t_2}', \hat{\sigma}'') = \bot$ (S-OrNone) with $\hat{\sigma} = M\sigma$, $Mt_1' \blacklozenge t_2' \equiv \hat{t_1'} \blacklozenge \hat{t_2'}$ and $M\sigma'' \equiv \hat{\sigma''}$.

From the induction hypothesis, we obtain the following.
$\forall M_1.M_1\varphi_1 \supset t_1, M_1\sigma \hat{\rightsquigarrow} \hat{t_1'}, \hat{\sigma'} \wedge M_1 t_1' \equiv \hat{t_1'} \wedge M_1\sigma' \equiv \hat{\sigma'}$ and
$\forall M_2.M_2\varphi_2 \supset t_2, M_2\sigma' \hat{\rightsquigarrow} \hat{t_2'}, \hat{\sigma''} \wedge M_2 t_2' \equiv \hat{t_2'} \wedge M_2\sigma'' \equiv \hat{\sigma''}$.

Since M satisfies both φ_1 and φ_2, we know that $t_1, M\sigma \hat{\rightsquigarrow} \hat{t_1'}, \hat{\sigma'}$ and $t_2, M\sigma' \hat{\rightsquigarrow} \hat{t_2'}, \hat{\sigma''}$, $Mt_1' \blacklozenge t_2' \equiv \hat{t_1'} \blacklozenge \hat{t_2'}$ and $M\sigma'' \equiv \hat{\sigma''}$.

Case $t = \square\, v$

One rule applies, namely $\dfrac{}{\square\, v, \sigma \rightsquigarrow \square\, v, \sigma, \boxed{\mathsf{True}}}$ (SS-Edit)

Provided that $M\,\mathsf{True}$, we need to demonstrate that $\dfrac{}{\square\, v, \hat{\sigma} \hat{\rightsquigarrow} \square\, v, \hat{\sigma}}$ (S-Edit) with $\hat{\sigma} = M\sigma$, $M \square\, v \equiv \square\, \hat{v}$ and $M\sigma \equiv \hat{\sigma}$. This holds trivially.

Case $t = \boxtimes\, \tau$

One rule applies, namely $\dfrac{}{\boxtimes\, \tau, \sigma \rightsquigarrow \boxtimes\, \tau, \sigma, \boxed{\mathsf{True}}}$ (SS-Fill)

Provided that $M\,\mathsf{True}$, we need to demonstrate $\dfrac{}{\boxtimes\, \tau, \hat{\sigma} \hat{\rightsquigarrow} \boxtimes\, \tau, \hat{\sigma}}$ (S-Fill) with $\hat{\sigma} = M\sigma$, $M \boxtimes\, \tau \equiv \boxtimes\, \tau$ and $M\sigma \equiv \hat{\sigma}$. This holds trivially.

Case $t = \blacksquare\, l$

One rule applies, namely $\dfrac{}{\blacksquare\, l, \sigma \rightsquigarrow \blacksquare\, l, \sigma, \boxed{\mathsf{True}}}$ (SS-Update)

Provided that $M\,\mathsf{True}$, we need to demonstrate $\dfrac{}{\blacksquare\, l, \hat{\sigma} \hat{\rightsquigarrow} \blacksquare\, l, \hat{\sigma}}$ (S-Update) with $\hat{\sigma} = M\sigma$, $M \blacksquare\, l \equiv \blacksquare\, l$ and $M\sigma \equiv \hat{\sigma}$. This holds trivially.

Case $t = ↯$

One rule applies, namely $\dfrac{}{↯, \sigma \rightsquigarrow ↯, \sigma, \boxed{\mathsf{True}}}$ (SS-Fail)

Provided that $M\,\mathsf{True}$, we need to demonstrate that $\dfrac{}{↯, \hat{\sigma} \hat{\rightsquigarrow} ↯, \hat{\sigma}}$ (S-Fail) with $\hat{\sigma} = M\sigma$, $M ↯ \equiv ↯$ and $M\sigma \equiv \hat{\sigma}$. This holds trivially.

Case $t = e_1 \lozenge e_2$

One rule applies, namely $\dfrac{}{e_1 \lozenge e_2, \sigma \rightsquigarrow e_1 \lozenge e_2, \sigma, \boxed{\mathsf{True}}}$ (SS-Xor)

Provided that $M\,\mathsf{True}$, we need to demonstrate that $\dfrac{}{e_1 \lozenge e_2, \hat{\sigma} \hat{\rightsquigarrow} e_1 \lozenge e_2, \hat{\sigma}}$ (S-Xor) with $\hat{\sigma} = M\sigma$, $Me_1 \lozenge e_2 \equiv e_1 \lozenge e_2$ and $M\sigma \equiv \hat{\sigma}$. This holds trivially.

Case $t = t_1 \rhd e_2$

One rule applies, namely $\dfrac{t_1, \sigma \rightsquigarrow \overline{t_1', \sigma', \boxed{\varphi}}}{t_1 \rhd e_2, \sigma \rightsquigarrow \overline{t_1' \rhd e_2, \sigma', \boxed{\varphi}}}$ (SS-Next)

Provided that $M\varphi$, we need to demonstrate that $\dfrac{}{e_1 \lozenge e_2, \hat{\sigma} \hat{\rightsquigarrow} e_1 \lozenge e_2, \hat{\sigma}}$ (S-Xor) with $\hat{\sigma} = M\sigma$, $Mt_1' \rhd e_2 \equiv \hat{t_1'} \rhd e_2$ and $M\sigma' \equiv \hat{\sigma}'$.

From the induction hypothesis, we obtain the following.
$\forall M_1.M_1\varphi \supset t_1, M_1\sigma \hat{\rightsquigarrow} \hat{t_1'}, \hat{\sigma'} \wedge M_1 t_1' \equiv \hat{t_1'} \wedge M_1\sigma' \equiv \hat{\sigma'}$.

Since M satisfies φ, we directly obtain $t_1, M_1\sigma \hat{\rightsquigarrow} \hat{t_1'}, \hat{\sigma'}$, $Mt_1' \rhd e_2 \equiv \hat{t_1'} \rhd e_2$ and $M\sigma' \equiv \hat{\sigma'}$.

Case $t = t_1 \bowtie t_2$

One rule applies, namely
$$\textsc{SS-And}\quad \frac{t_1, \sigma \rightsquigarrow \overline{t_1', \sigma', \boxed{\varphi_1}} \qquad t_2, \sigma' \rightsquigarrow \overline{t_2', \sigma'', \boxed{\varphi_2}}}{t_1 \bowtie t_2, \sigma \rightsquigarrow \overline{t_1' \bowtie t_2', \sigma'', \boxed{\varphi_1 \wedge \varphi_2}}}$$

Provided that $M\varphi_1 \wedge M\varphi_2$ we need to demonstrate
$$\textsc{S-And}\quad \frac{t_1, \hat{\sigma} \hat{\rightsquigarrow} \hat{t_1}', \hat{\sigma}' \qquad t_2, \hat{\sigma}' \hat{\rightsquigarrow} \hat{t_2}', \hat{\sigma}''}{t_1 \bowtie t_2, \hat{\sigma} \hat{\rightsquigarrow} \hat{t_1}' \bowtie \hat{t_2}', \hat{\sigma}''}$$
with $\hat{\sigma} = M\sigma$, $Mt_1' \bowtie t_2' \equiv \hat{t_1'} \bowtie \hat{t_2'}$ and $M\sigma'' \equiv \hat{\sigma''}$.

From the induction hypothesis, we obtain the following.
$\forall M_1.M_1\varphi_1 \supset t_1, M_1\sigma \hat{\rightsquigarrow} \hat{t_1'}, \hat{\sigma'} \quad M_1 t_1' \equiv \hat{t_1'} \wedge M_1\sigma' \equiv \hat{\sigma'}$ and
$\forall M_2.M_2\varphi_2 \supset t_2, M_2\sigma' \hat{\rightsquigarrow} \hat{t_2'}, \hat{\sigma''} \quad M_2 t_2' \equiv \hat{t_2'} \wedge M_2\sigma'' \equiv \hat{\sigma''}$.

Since M satisfies both φ_1 and φ_2, we know that $t_1, M\sigma \hat{\rightsquigarrow} \hat{t_1'}, \hat{\sigma'}$ and $t_2, M\sigma' \hat{\rightsquigarrow} \hat{t_2'}, \hat{\sigma''}$, $Mt_1' \blacklozenge t_2' \equiv \hat{t_1'} \blacklozenge \hat{t_2'}$ and $M\sigma'' \equiv \hat{\sigma''}$. ◻

Proof of Lemma ??. We prove Lemma ?? by induction over e.

The base case is when the SN-Done rule applies.
$$\textsc{SN-Done}\quad \frac{e, \sigma \downarrow \overline{t, \sigma', \boxed{\varphi_1}} \qquad t, \sigma' \rightsquigarrow \overline{t', \sigma'', \boxed{\varphi_2}}}{e, \sigma \Downarrow \overline{t, \sigma', \boxed{\varphi_1}}}\ \sigma' = \sigma'' \wedge t = t'$$

Provided that $M\varphi_1 \wedge M\varphi_2$
we need to demonstrate that
$$\textsc{N-Done}\quad \frac{e, \hat{\sigma} \hat{\downarrow} \hat{t}, \hat{\sigma}' \qquad \hat{t}, \hat{\sigma}' \hat{\rightsquigarrow} \hat{t}', \hat{\sigma}''}{e, \hat{\sigma} \hat{\Downarrow} \hat{t}, \hat{\sigma}'}\ \hat{\sigma}' = \hat{\sigma}'' \wedge \hat{t} = \hat{t}'$$
with $\hat{\sigma} = M\sigma$, $Mt \equiv \hat{t}$ and $M\sigma' \equiv \hat{\sigma'}$.

By Lemma ?? and Lemma ??, we know that
$\forall M_1.M_1\varphi_1 \supset e, M_1\sigma \hat{\downarrow} \hat{t}, \hat{\sigma'} \wedge M_1 t \equiv \hat{t} \wedge M_1\sigma' \equiv \hat{\sigma'}$ and
$\forall M_2.M_2\varphi_2 \supset t, M_2\sigma' \hat{\rightsquigarrow} \hat{t'}, \hat{\sigma''} \wedge M_2 t' \equiv \hat{t'} \wedge M_2\sigma'' \equiv \hat{\sigma''}$.

We assume M to satisfy both φ_1 and φ_2, we have $e, M\sigma \hat{\downarrow} \hat{t}, \hat{\sigma'}$ since $M\sigma \equiv \hat{\sigma}$.

The only induction step is when
$$\textsc{SN-Repeat}\quad \frac{e, \sigma \downarrow \overline{t, \sigma', \boxed{\varphi_1}} \qquad t, \sigma' \rightsquigarrow \overline{t', \sigma'', \boxed{\varphi_2}} \qquad t', \sigma'' \Downarrow \overline{t'', \sigma''', \boxed{\varphi_3}}}{e, \sigma \Downarrow \overline{t'', \sigma''', \boxed{\varphi_1 \wedge \varphi_2 \wedge \varphi_3}}}\ \sigma' \neq \sigma'' \vee t \neq t'$$
applies. In this case, where we have that $M\varphi_1 \wedge M\varphi_2 \wedge M\varphi_3$, we need to demonstrate that
$$\textsc{N-Repeat}\quad \frac{e, \hat{\sigma} \hat{\downarrow} \hat{t}, \hat{\sigma}' \qquad \hat{t}, \hat{\sigma}' \hat{\rightsquigarrow} \hat{t}', \hat{\sigma}'' \qquad \hat{t}', \hat{\sigma}'' \hat{\Downarrow} \hat{t}'', \hat{\sigma}'''}{e, \hat{\sigma} \hat{\Downarrow} \hat{t}'', \hat{\sigma}'''}\ \hat{\sigma}' \neq \hat{\sigma}'' \vee \hat{t} \neq \hat{t}'$$
with $\hat{\sigma} = M\sigma$, $Mt'' \equiv \hat{t''}$ and $M\sigma''' \equiv \hat{\sigma'''}$.

Again by Lemma ?? and Lemma ??, we know that
$\forall M_1.M_1\varphi_1 \supset e, M_1\sigma \hat{\downarrow} \hat{t}, \hat{\sigma'} \wedge M_1 t \equiv \hat{t} \wedge M_1\sigma' \equiv \hat{\sigma'}$ and
$\forall M_2.M_2\varphi_2 \supset t, M_2\sigma' \hat{\rightsquigarrow} \hat{t'}, \hat{\sigma''} \wedge M_2 t' \equiv \hat{t'} \wedge M_2\sigma'' \equiv \hat{\sigma''}$.
Furthermore, we know by applying the induction hypothesis that $\forall M_3.M_3\varphi_3 \supset t', M_3\sigma'' \hat{\Downarrow} \hat{t''}, \hat{\sigma'''} \wedge M_3 t'' \equiv \hat{t''} \wedge M_3\sigma''' \equiv \hat{\sigma'''}$.

Since M satisfies φ_1, φ_2 and φ_3, we can conclude that
$e, M\sigma \hat{\downarrow} \hat{t}, \hat{\sigma'}$, $Mt \equiv \hat{t} \wedge M\sigma' \equiv \hat{\sigma'}$ and $t, M\sigma' \hat{\rightsquigarrow} \hat{t'}, \hat{\sigma''}$ and $Mt' \equiv \hat{t'} \wedge M\sigma'' \equiv \hat{\sigma''}$. This finally gives us $t', M\sigma'' \hat{\Downarrow} \hat{t''}, \hat{\sigma'''}$ from which we can conclude that which we needed to prove, namely $Mt'' \equiv \hat{t''} \wedge M\sigma''' \equiv \hat{\sigma'''}$. ◻

Proof of Lemma ??. We prove Lemma ?? by induction over t.

Case $t = \square v$

One rule applies, namely $\overset{\textsc{SH-Change}}{\dfrac{\text{fresh } s}{\square v, \sigma \longrightarrow \square s, \sigma, s, \mathsf{True}}}\; v, s : \tau$

Provided that $M\,\mathsf{True}$ we need to demonstrate that $\overset{\textsc{H-Change}}{\dfrac{}{\square v, \hat{\sigma} \xrightarrow{v'} \square v', \hat{\sigma}}}\; v, v' : \tau$ with $\hat{\sigma} = M\sigma$ and $Ms = v'$, $M \square s \equiv \square v'$ and $M\sigma \equiv \hat{\sigma}$.

This follows trivially from the premise.

Case $t = \boxtimes \tau$

One rule applies, namely $\overset{\textsc{SH-Fill}}{\dfrac{\text{fresh } s}{\boxtimes \tau, \sigma \longrightarrow \square s, \sigma, s, \mathsf{True}}}\; s : \tau$

Provided that $M\,\mathsf{True}$ we need to demonstrate that $\overset{\textsc{H-Fill}}{\dfrac{}{\boxtimes \tau, \hat{\sigma} \xrightarrow{v} \square v, \hat{\sigma}}}\; v : \tau$ with $\hat{\sigma} = M\sigma$ and $Ms = v$, $M \square s \equiv \square v$ and $M\sigma \equiv \hat{\sigma}$.

This follows trivially from the premise.

Case $t = \blacksquare\, l$

One rule applies, namely $\overset{\textsc{SH-Update}}{\dfrac{\text{fresh } s}{\blacksquare\, l, \sigma \longrightarrow \blacksquare\, l, \sigma[l \mapsto s], s, \mathsf{True}}}\; \sigma(l), s : \tau$

Provided that $M\,\mathsf{True}$ we need to demonstrate that $\overset{\textsc{H-Update}}{\dfrac{}{\blacksquare\, l, \hat{\sigma} \xrightarrow{v} \blacksquare\, l, \hat{\sigma}[l \mapsto v]}}\; \sigma(l), v : \tau$ with $\hat{\sigma} = M\sigma$ and $Ms = v$, $M \blacksquare\, l \equiv \blacksquare\, l$ and $M\sigma[l \mapsto s] \equiv \hat{\sigma}[l \mapsto v]$.

$\overset{\textsc{H-Update}}{\dfrac{}{\blacksquare\, l, \hat{\sigma} \xrightarrow{v} \blacksquare\, l, \hat{\sigma}[l \mapsto v]}}\; \sigma(l), v : \tau$ with $\hat{\sigma} = M\sigma$ follows trivially. $M \blacksquare\, l \equiv \blacksquare\, l$ follows trivially, since locations cannot contain symbols. $M\sigma[l \mapsto s] \equiv \hat{\sigma}[l \mapsto v]$ can be concluded from the fact that $\hat{\sigma} = M\sigma$ and $Ms = v$.

Case $t = t_1 \rhd e_2$

In this case, two rules apply.

Case $\overset{\textsc{SH-Next}}{\dfrac{t_1, \sigma \longrightarrow \overline{t_1', \sigma_1', i_1, \varphi_1} \qquad e_2\, v_1, \sigma \Downarrow \overline{t_2, \sigma_2', \varphi_2}}{t_1 \rhd e_2, \sigma \longrightarrow \overline{t_1' \rhd e_2, \sigma_1', i_1, \varphi_1} \cup \overline{t_2, \sigma_2', \mathsf{C}, \varphi_2}}}\; \mathcal{V}(t_1, \sigma) = v_1 \wedge \neg \mathcal{F}(t_2, \sigma')$

In the case $M\varphi_1$, we need to demonstrate that $\overset{\textsc{H-PassNext}}{\dfrac{t_1, \sigma \xrightarrow{j} \hat{t}_1', \sigma'}{t_1 \rhd e_2, \sigma \xrightarrow{j} \hat{t}_1' \rhd e_2, \sigma'}}$ with $\hat{\sigma} = M\sigma$ and $j = Mi$, $Mt_1' \rhd e_2 \equiv \hat{t}_1' \rhd e_2$ and $M\sigma' \equiv \hat{\sigma}'$.

By the induction hypothesis we obtain the following.

$\forall M_1 . M_1 \varphi_1 \supset t_1, M_1 \sigma \xrightarrow{M_1 i} \hat{t}_1', \hat{\sigma}' \wedge M_1 t_1' \equiv \hat{t}_1' \wedge M_1 \sigma' \equiv \hat{\sigma}'$

Since M satisfies φ, we have $t_1, M\sigma \xrightarrow{Mi} \hat{t}_1', \hat{\sigma}'$, $M\sigma' \equiv \hat{\sigma}'$, which we needed to show, as well as $Mt_1' \rhd e_2 \equiv \hat{t}_1' \rhd e_2$ since this can be concluded from $Mt_1' \equiv \hat{t}_1'$.

In the case $M\varphi_2$, we need to demonstrate that $\overset{\textsc{H-Next}}{\dfrac{e_2\, \hat{v}_1, \sigma \hat{\Downarrow} \hat{t}_2, \hat{\sigma}'}{t_1 \rhd e_2, \sigma \xrightarrow{\mathsf{C}} \hat{t}_2, \hat{\sigma}'}}\; \mathcal{V}(t_1, \sigma) = \hat{v}_1 \wedge \neg \mathcal{F}(\hat{t}_2, \hat{\sigma}')$ with $\hat{\sigma} = M\sigma$, $Mt_2 \equiv \hat{t}_2$ and $M\sigma' \equiv \hat{\sigma}'$.

From Lemma **??** we obtain that $\forall M_1 . M_1 \varphi \supset e_2 v_1, M\sigma \hat{\Downarrow} \hat{t}_2, \hat{\sigma}' \wedge Mt_2 \equiv \hat{t}_2 \wedge M\sigma' \equiv \hat{\sigma}'$.

This gives us exactly what we needed to prove this case.

Case $$\frac{t_1, \sigma \;\rightarrow\; \overline{t_1', \sigma', \boxed{i, \varphi}}}{t_1 \rhd e_2, \sigma \;\rightarrow\; \overline{t_1' \rhd e_2, \sigma', \boxed{i, \varphi}}}\;\text{SH-PassNext}\;\; \mathcal{V}(t_1, \sigma) = \bot$$

Provided that $M\varphi$, we need to demonstrate that $\dfrac{t_1, \sigma \xrightarrow{j} \hat{t_1'}, \sigma'}{t_1 \rhd e_2, \sigma \xrightarrow{j} \hat{t_1'} \rhd e_2, \sigma'}\;\text{H-PassNext}$ with $\hat{\sigma} = M\sigma$ and $j = Mi$, $Mt_1' \rhd e_2 \equiv \hat{t_1'} \rhd e_2$ and $M\sigma' \equiv \hat{\sigma}'$.

By the induction hypothesis we obtain the following.
$\forall M_1.M_1\varphi_1 \supset t_1, M_1\sigma \xrightarrow{M_1 i} \hat{t_1'}, \hat{\sigma}' \wedge M_1 t_1' \equiv \hat{t_1'} \wedge M_1\sigma' \equiv \hat{\sigma}'$

Since M satisfies φ, we have $t_1, M\sigma \xrightarrow{Mi} \hat{t_1'}, \hat{\sigma}'$, $M\sigma' \equiv \hat{\sigma}'$, which we needed to show, as well as $Mt_1' \rhd e_2 \equiv \hat{t_1'} \rhd e_2$ since this can be concluded from $Mt_1' \equiv \hat{t_1'}$.

Case $t = t_1 \blacktriangleright e_2$

One rule applies, namely $$\frac{t_1, \sigma \;\rightarrow\; \overline{t_1', \sigma', \boxed{i, \varphi}}}{t_1 \blacktriangleright e_2, \sigma \;\rightarrow\; \overline{t_1' \blacktriangleright e_2, \sigma', \boxed{i, \varphi}}}\;\text{SH-PassThen}$$

Provided that $M\varphi$, we need to demonstrate that $\dfrac{t_1, \sigma \xrightarrow{j} \hat{t_1'}, \sigma'}{t_1 \blacktriangleright e_2, \sigma \xrightarrow{j} \hat{t_1'} \blacktriangleright e_2, \sigma'}\;\text{H-PassThen}$ with $\hat{\sigma} = M\sigma$ and $j = Mi$, $Mt_1' \blacktriangleright e_2 \equiv \hat{t_1'} \blacktriangleright e_2$ and $M\sigma' \equiv \hat{\sigma}'$.

By the induction hypothesis we obtain the following.
$\forall M_1.M_1\varphi_1 \supset t_1, M_1\sigma \xrightarrow{M_1 i} \hat{t_1'}, \hat{\sigma}' \wedge M_1 t_1' \equiv \hat{t_1'} \wedge M_1\sigma' \equiv \hat{\sigma}'$

Since M satisfies φ, we have $t_1, M\sigma \xrightarrow{Mi} \hat{t_1'}, \hat{\sigma}'$ and $M\sigma' \equiv \hat{\sigma}'$, which we needed to show, as well as $Mt_1' \blacktriangleright e_2 \equiv \hat{t_1'} \blacktriangleright e_2$ since this can be concluded from $Mt_1' \equiv \hat{t_1'}$.

Case $t = e_1 \lozenge e_2$

In this case, three rules apply.

Case $$\frac{e_1, \sigma \;\Downarrow\; \overline{t_1, \boxed{\sigma_1, \varphi_1}} \qquad e_2, \sigma \;\Downarrow\; \overline{t_2, \boxed{\sigma_2, \varphi_2}}}{e_1 \lozenge e_2, \sigma \;\rightarrow\; \boxed{\overline{t_1, \sigma_1, \mathsf{L}, \varphi_1} \cup \overline{t_2, \sigma_2, \mathsf{R}, \varphi_2}}}\;\text{SH-Pick}\;\; \neg\mathcal{F}(t_1, \sigma_1) \wedge \neg\mathcal{F}(t_2, \sigma_2)$$

Either we have that $M(\varphi_1 \wedge s = \mathsf{L})$ or $M(\varphi_2 \wedge s = \mathsf{R})$. In the first case, the proof is identical to the SH-PickLeft rule. In the second cse, the proof is identical to the SH-PickRight rule.

Case $$\frac{e_1, \sigma \;\Downarrow\; \overline{t_1, \boxed{\sigma_1, \varphi_1}} \qquad e_2, \sigma \;\Downarrow\; \overline{t_2, \boxed{\sigma_2, \varphi_2}}}{e_1 \lozenge e_2, \sigma \;\rightarrow\; t_1, \sigma_1, \boxed{\mathsf{L}, \varphi_1}}\;\text{SH-PickLeft}\;\; \neg\mathcal{F}(t_1, \sigma_1) \wedge \mathcal{F}(t_2, \sigma_2)$$

Provided that $M(\varphi_2 \wedge s = \mathsf{L})$, we need to demonstrate that $\dfrac{e_1, \sigma \;\Downarrow\; \hat{t_1}, \hat{\sigma}'}{e_1 \lozenge e_2, \sigma \xrightarrow{\mathsf{L}} \hat{t_1}, \hat{\sigma}'}\;\text{H-PickLeft}\;\; \neg\mathcal{F}(\hat{t_1}, \hat{\sigma}')$ with $\hat{\sigma} = M\sigma$, $Mt_1 \equiv \hat{t_1}$ and $M\sigma' \equiv \hat{\sigma}'$.

From Lemma **??** we obtain that $\forall M_1.M_1\varphi \supset e_1, M\sigma \;\hat{\Downarrow}\; \hat{t_1}, \hat{\sigma}' \wedge Mt_1 \equiv \hat{t_1} \wedge M\sigma' \equiv \hat{\sigma}'$.
Since M satisfies φ, we have $e_1, M\sigma \;\hat{\Downarrow}\; []\hat{t_1}, \hat{\sigma}'$ and $M\sigma' \equiv \hat{\sigma}'$, which we needed to show, as well as $Mt_1 \equiv \hat{t_1}$.

Case $$\frac{e_1, \sigma \;\Downarrow\; \overline{t_1, \boxed{\sigma_1, \varphi_1}} \qquad e_2, \sigma \;\Downarrow\; \overline{t_2, \boxed{\sigma_2, \varphi_2}}}{e_1 \lozenge e_2, \sigma \;\rightarrow\; t_2, \sigma_2, \boxed{\mathsf{R}, \varphi_2}}\;\text{SH-PickRight}\;\; \mathcal{F}(t_1, \sigma_1) \wedge \neg\mathcal{F}(t_2, \sigma_2)$$

Provided that $M(\varphi_2 \wedge s = \mathsf{R})$ we need to demonstrate that $\dfrac{e_2, \sigma \;\hat{\Downarrow}\; \hat{t_2}, \hat{\sigma}'}{e_1 \lozenge e_2, \sigma \xrightarrow{\mathsf{R}} \hat{t_2}, \hat{\sigma}'}\;\text{H-PickRight}\;\; \neg\mathcal{F}(\hat{t_2}, \hat{\sigma}')$ with $\hat{\sigma} = M\sigma$, $Mt_2 \equiv \hat{t_2}$ and $M\sigma' \equiv \hat{\sigma}'$.

From Lemma ?? we obtain that $\forall M_1.M_1\varphi \supset e_2, M\sigma \Downarrow \hat{t_2}, \hat{\sigma}' \wedge Mt_2 \equiv \hat{t_2} \wedge M\sigma' \equiv \hat{\sigma}'$.
Since M satisfies φ, we have $e_2, M\sigma \Downarrow []\hat{t_2}, \hat{\sigma}'$ and $M\sigma' \equiv \hat{\sigma}'$, which we needed to show, as well as $Mt_2 \equiv \hat{t_2}$.

Case $t = t_1 \bowtie t_2$

In this case, two rules apply.
Case

Provided that $M\varphi$, we need to demonstrate that $$\textsc{H-FirstAnd}\quad \dfrac{t_1, \sigma \xrightarrow{j} \hat{t_1}', \hat{\sigma}'}{t_1 \bowtie t_2, \sigma \xrightarrow{\mathsf{F}\, j} \hat{t_1}' \bowtie t_2, \hat{\sigma}'}$$ with $\hat{\sigma} = M\sigma$, $Mt_1' \bowtie t_2 \equiv \hat{t_1'} \bowtie t_2$ and $M\sigma' \equiv \hat{\sigma}'$.
By the induction hypothesis we obtain the following.
$\forall M_1.M_1\varphi_1 \supset t_1, M_1\sigma \xrightarrow{M_1 i} \hat{t_1'}, \hat{\sigma}' \wedge M_1t_1' \equiv \hat{t_1'} \wedge M_1\sigma' \equiv \hat{\sigma}'$
Since M satisfies φ, we have $t_1, M\sigma \xrightarrow{Mi} \hat{t_1'}, \hat{\sigma}'$ and $M\sigma' \equiv \hat{\sigma}'$, which we needed to show, as well as $Mt_1' \bowtie t_2 \equiv \hat{t_1'} \bowtie t_2$, which follows from $Mt_1' \equiv \hat{t_1'}$.

Case

Provided that $M\varphi$, we need to demonstrate that $$\textsc{H-SecondAnd}\quad \dfrac{t_2, \sigma \xrightarrow{j} \hat{t_2}', \hat{\sigma}'}{t_1 \bowtie t_2, \sigma \xrightarrow{\mathsf{S}\, j} t_1 \bowtie \hat{t_2}', \hat{\sigma}'}$$ with $\hat{\sigma} = M\sigma$, $Mt_1 \bowtie t_2' \equiv t_1 \bowtie \hat{t_2}$ and $M\sigma' \equiv \hat{\sigma}'$.
By the induction hypothesis we obtain the following.
$\forall M_1.M_1\varphi_1 \supset t_2, M_1\sigma \xrightarrow{M_1 i} \hat{t_2'}, \hat{\sigma}' \wedge M_1t_2' \equiv \hat{t_2'} \wedge M_1\sigma' \equiv \hat{\sigma}'$
Since M satisfies φ, we have $t_2, M\sigma \xrightarrow{Mi} \hat{t_2'}, \hat{\sigma}'$ and $M\sigma' \equiv \hat{\sigma}'$, which we needed to show, as well as $Mt_1 \bowtie t_2' \equiv t_1 \bowtie \hat{t_2'}$, which follows from $Mt_2' \equiv \hat{t_2'}$.

Case $t = e_1 \blacklozenge e_2$

One rule applies, namely $$\textsc{SH-Or}\quad \dfrac{t_1, \sigma \to \overline{t_1', \sigma_1', i_1, \varphi_1} \qquad t_2, \sigma \to \overline{t_2', \sigma_2', i_2, \varphi_2}}{t_1 \blacklozenge t_2, \sigma \to \overline{t_1' \blacklozenge t_2, \sigma_1', \mathsf{F}\, i_1, \varphi_1} \cup \overline{t_1 \blacklozenge t_2', \sigma_2', \mathsf{S}\, i_2, \varphi_2}}$$
In the case that $M\varphi_1$, we need to demonstrate that $$\textsc{H-FirstOr}\quad \dfrac{t_1, \sigma \xrightarrow{j} \hat{t_1}', \hat{\sigma}'}{t_1 \blacklozenge t_2, \sigma \xrightarrow{\mathsf{F}\, j} \hat{t_1}' \blacklozenge t_2, \hat{\sigma}'}$$ with $\hat{\sigma} = M\sigma$ and $M\,\mathsf{F}\, i = \mathsf{F}\, j$, $Mt_1' \blacklozenge t_2 \equiv \hat{t_1'} \bowtie t_2$ and $M\sigma' \equiv \hat{\sigma}'$.
By the induction hypothesis we obtain the following.
$\forall M_1.M_1\varphi_1 \supset t_1, M_1\sigma \xrightarrow{M_1 i} \hat{t_1'}, \hat{\sigma}' \wedge M_1t_1' \equiv \hat{t_1'} \wedge M_1\sigma' \equiv \hat{\sigma}'$.
Since M satisfies φ, we have $t_1, M\sigma \xrightarrow{Mi} \hat{t_1'}, \hat{\sigma}'$ and $M\sigma' \equiv \hat{\sigma}'$, which we needed to show, as well as $Mt_1' \blacklozenge t_2 \equiv \hat{t_1'} \bowtie t_2$, which follows from $Mt_1' \equiv \hat{t_1'}$.
In the case that $M\varphi_2$, we need to demonstrate that $$\textsc{H-SecondOr}\quad \dfrac{t_2, \sigma \xrightarrow{j} \hat{t_2}', \hat{\sigma}'}{t_1 \blacklozenge t_2, \sigma \xrightarrow{\mathsf{S}\, j} t_1 \blacklozenge \hat{t_2}', \hat{\sigma}'}$$ with $\hat{\sigma} = M\sigma$ and $M\,\mathsf{S}\, i = \mathsf{S}\, j$, $Mt_1 \blacklozenge t_2' \equiv t_1 \bowtie \hat{t_2}$ and $M\sigma' \equiv \hat{\sigma}'$.
By the induction hypothesis we obtain the following.
$\forall M_1.M_1\varphi_1 \supset t_2, M_1\sigma \xrightarrow{M_1 i} \hat{t_2'}, \hat{\sigma}' \wedge M_1t_2' \equiv \hat{t_2'} \wedge M_1\sigma' \equiv \hat{\sigma}'$
Since M satisfies φ, we have $t_2, M\sigma \xrightarrow{Mi} \hat{t_2'}, \hat{\sigma}'$ and $M\sigma' \equiv \hat{\sigma}'$, which we needed to show, as well as $Mt_1 \blacklozenge t_2' \equiv t_1 \bowtie \hat{t_2'}$, which follows from $Mt_2' \equiv \hat{t_2'}$.

□

Proof of Lemma ??. We prove Lemma ?? as follows. There is only one rule that applies, namely

$$\frac{t, \sigma \;\rightarrow\; \overline{t', \sigma', \boxed{i, \varphi_1}} \qquad t', \sigma' \;\Downarrow\; \overline{t'', \sigma'', \boxed{\varphi_2}}}{t, \sigma \;\Rightarrow\; \overline{t'', \sigma'', \boxed{i, \varphi_1 \wedge \varphi_2}}}\ \text{SI-Handle}\ .$$

Provided that $M\varphi_1 \wedge \varphi_2$, we need to demonstrate that

$$\frac{t, \sigma \xrightarrow{j} \hat{t}', \hat{\sigma}' \qquad \hat{t}', \hat{\sigma}' \Downarrow \hat{t}'', \hat{\sigma}''}{t, \sigma \overset{j}{\Rightarrow} \hat{t}'', \hat{\sigma}''}\ \text{I-Handle}$$

with $\hat{\sigma} = M\sigma$ and $j = Mi$, $Mt'' \equiv \hat{t''}$ and $M\sigma'' \equiv \hat{\sigma''}$.

Lemma ?? and Lemma ?? respectively give us that
$\forall M_1 . M_1\varphi_1 \supset t_1, M_1\sigma \xrightarrow{M_1 i} \hat{t'}, \hat{\sigma'} \wedge M_1 t' \equiv \hat{t'} \wedge M_1\sigma' \equiv \hat{\sigma'}$ and
$\forall M_2 . M_2\varphi_2 \supset t', M_2\sigma' \Downarrow \hat{t''}, \hat{\sigma''} \wedge M_2 t'' \equiv \hat{t''} \wedge M_2\sigma'' \equiv \hat{\sigma''}$.

Since M satisfies both φ_1 and φ_2, we obtain exactly what we needed to prove, namely $t_1, M\sigma \xrightarrow{Mi} \hat{t'}, \hat{\sigma'}$, $t', M\sigma' \Downarrow \hat{t''}, \hat{\sigma''}$, $Mt'' \equiv \hat{t''}$ and $M\sigma'' \equiv \hat{\sigma''}$.

□

D COMPLETENESS PROOFS

Proof of Lemma ??. We prove Lemma ?? by induction over t.

Case $t = \square\, v$

One rule applies in this case, namely

$$\frac{}{\square\, v, \hat{\sigma} \xrightarrow{v'} \square\, v', \hat{\sigma}}\ v, v' : \tau \quad \text{H-Change}$$

Take $i = s$ and assume $\sigma'' = \sigma$. $s \sim v'$ holds by definition. Then by the SH-Change rule, we know that a symbolic execution exists.

Case $t = \boxtimes\, \tau$

One rule applies in this case, namely

$$\frac{}{\boxtimes\, \tau, \hat{\sigma} \xrightarrow{v} \square\, v, \hat{\sigma}}\ v : \tau \quad \text{H-Fill}$$

Take $i = s$ and assume $\sigma'' = \sigma$. $s \sim v$ holds by definition. Then by the SH-Fill rule, we know that a symbolic execution exists.

Case $t = \blacksquare\, l$

One rule applies in this case, namely

$$\frac{}{\blacksquare\, l, \hat{\sigma} \xrightarrow{v} \blacksquare\, l, \hat{\sigma}[l \mapsto v]}\ \sigma(l), v : \tau \quad \text{H-Update}$$

Take $i = s$ and assume $\sigma'' = \sigma$. $s \sim v'$ holds by definition. Then by the SH-Update rule, we know that a symbolic execution exists.

Case $t = t_1 \triangleright e_2$

Two rules apply in this case

Case H-Next

$$\frac{e_2\ \hat{v_1}, \sigma \Downarrow \hat{t_2}, \hat{\sigma}'}{t_1 \triangleright e_2, \sigma \xrightarrow{\mathrm{C}} \hat{t_2}, \hat{\sigma}'}\ \mathcal{V}(t_1, \sigma) = \hat{v_1} \wedge \neg\mathcal{F}(\hat{t_2}, \hat{\sigma}')$$

Take $i = s$ and assume $\sigma'' = \sigma$. $s \sim \mathrm{C}$ holds by definition. Then by the SH-Next rule, we know that a symbolic execution exists.

Case H-PassNext

$$\frac{t_1, \sigma \xrightarrow{j} \hat{t_1'}, \sigma'}{t_1 \triangleright e_2, \sigma \xrightarrow{j} \hat{t_1'} \triangleright e_2, \sigma'}$$

By application of the induction hypothesis, we obtain the following.
For all t_1, σ, j such that $t_1, \sigma \underset{j}{\rightarrow} t_1', \sigma'$ there exists an $i \sim j$ such that $t_1'', \sigma'' \;\rightarrow\; t_1''', \sigma''', i, \varphi$.
From this we can conclude that there exists a symbolic execution $t_1 \triangleright e_2, \sigma \;\rightarrow\; t_1''' \triangleright e_2, \sigma''', i, \varphi$, and that $i \sim j$.

Case $t = t_1 \blacktriangleright e_2$

One rule applies in this case, namely

$$\frac{t_1, \sigma \xrightarrow{j} \hat{t_1'}, \sigma'}{t_1 \blacktriangleright e_2, \sigma \xrightarrow{j} \hat{t_1'} \blacktriangleright e_2, \sigma'}\ \text{H-PassThen}$$

By application of the induction hypothesis, we obtain the following.
For all t_1, σ, j such that $t_1, \sigma \underset{j}{\rightarrow} t_1', \sigma'$ there exists an $i \sim j$ such that $t_1'', \sigma'' \;\rightarrow\; t_1''', \sigma''', i, \varphi$.
From this we can conclude that there exists a symbolic execution $t_1 \blacktriangleright e_2, \sigma \;\rightarrow\; t_1''' \blacktriangleright e_2, \sigma''', i, \varphi$, and $i \sim j$.

Case $t = e_1 \Diamond e_2$

Two rules apply in this case.

Case H-PickLeft
$$\frac{e_1, \sigma \Downarrow \hat{t_1}, \hat{\sigma}' \qquad \neg\mathcal{F}(\hat{t_1}, \hat{\sigma}')}{e_1 \Diamond e_2, \sigma \xrightarrow{\mathsf{L}} \hat{t_1}, \hat{\sigma}'}$$

Take $i = s$. $s \sim \mathsf{L}$ holds by definition.
Lemma **??** gives us the following.
There exists a symbolic execution $e_1, \sigma \;\Downarrow\; t_1, \sigma_1, \varphi$.
There exists a symbolic execution $e_2, \sigma_1 \;\Downarrow\; t_2, \sigma_2, \varphi$.

We can now conclude that a symbolic execution exists. Either by the SH-PickLeft rule, in case $\mathcal{F}(t_2, \sigma_2)$, or by the SH-Pick rule in case $\neg\mathcal{F}(t_2, \sigma_2)$.

Case H-PickRight
$$\frac{e_2, \sigma \hat{\Downarrow} \hat{t_2}, \hat{\sigma}' \qquad \neg\mathcal{F}(\hat{t_2}, \hat{\sigma}')}{e_1 \Diamond e_2, \sigma \xrightarrow{\mathsf{R}} \hat{t_2}, \hat{\sigma}'}$$

Take $i = s$. $s \sim \mathsf{L}$ holds by definition.
Lemma **??** gives us the following.
There exists a symbolic execution $e_1, \sigma \;\Downarrow\; t_1, \sigma_1, \varphi$.
There exists a symbolic execution $e_2, \sigma_1 \;\Downarrow\; t_2, \sigma_2, \varphi$.

We can now conclude that a symbolic execution exists. Either by the SH-PickRight rule, in case $\mathcal{F}(t_1, \sigma_1)$, or by the SH-Pick rule in case $\neg\mathcal{F}(t_1, \sigma_1)$.

Case $t = t_1 \blacklozenge t_2$

Two rules applies in this case.

Case H-FirstOr
$$\frac{t_1, \sigma \xrightarrow{j} \hat{t_1}', \hat{\sigma}'}{t_1 \blacklozenge t_2, \sigma \xrightarrow{\mathsf{F}\, j} \hat{t_1}' \blacklozenge t_2, \hat{\sigma}'}$$

Take $i = \mathsf{F}\, i$.
By application of the induction hypothesis, we obtain the following.
For all t_1, σ, j such that $t_1, \sigma \xrightarrow{j} t_1', \sigma'$ there exists an $i \sim j$ such that $t_1'', \sigma'' \;\rightarrow\; t_1''', \sigma''', i, \varphi$.

From this, we can conclude that $\mathsf{F}\, i \sim \mathsf{F}\, j$. From SH-Or, and the conclusion of the induction hypothesis, we can conclude that there exists an i such that $t_1 \blacklozenge t_2, \sigma \;\rightarrow\; t_1' \blacklozenge t_2, \sigma', i, \varphi$.

Case H-SecondOr
$$\frac{t_2, \sigma \xrightarrow{j} \hat{t_2}', \hat{\sigma}'}{t_1 \blacklozenge t_2, \sigma \xrightarrow{\mathsf{S}\, j} t_1 \blacklozenge \hat{t_2}', \hat{\sigma}'}$$

Take $i = \mathsf{S}\, i$.
By application of the induction hypothesis, we obtain the following.
For all t_2, σ, j such that $t_2, \sigma \xrightarrow{j} t_2', \sigma'$ there exists an $i \sim j$ such that $t_2'', \sigma'' \;\rightarrow\; t_2''', \sigma''', i, \varphi$.

From this, we can conclude that $\mathsf{S}\, i \sim \mathsf{S}\, j$. From SH-Or, and the conclusion of the induction hypothesis, we can conclude that there exists an i such that $t_1 \blacklozenge t_2, \sigma \;\rightarrow\; t_1 \blacklozenge t_2', \sigma', i, \varphi$.

Case $t = t_1 \bowtie t_2$

Two rules applies in this case.

Case $$\frac{t_1, \sigma \xrightarrow{j} \hat{t_1}', \hat{\sigma}'}{t_1 \bowtie t_2, \sigma \xrightarrow{\mathsf{F}\,j} \hat{t_1}' \bowtie t_2, \hat{\sigma}'}\ \textsc{H-FirstAnd}$$

Take $i = \mathsf{F}\, i$.

By application of the induction hypothesis, we obtain the following.

For all t_1, σ, j such that $t_1, \sigma \xrightarrow{j} t_1', \sigma'$ there exists an $i \sim j$ such that $t_1'', \sigma'' \ \rightarrow\ t_1''', \sigma''', i, \varphi$.

From this, we can conclude that $\mathsf{F}\, i \sim \mathsf{F}\, j$. From SH-And, and the conclusion of the induction hypothesis, we can conclude that there exists an i such that $t_1 \bowtie t_2, \sigma \ \rightarrow\ t_1' \blacklozenge t_2, \sigma', i, \varphi$.

Case $$\frac{t_2, \sigma \xrightarrow{j} \hat{t_2}', \hat{\sigma}'}{t_1 \bowtie t_2, \sigma \xrightarrow{\mathsf{S}\,j} t_1 \bowtie \hat{t_2}', \hat{\sigma}'}\ \textsc{H-SecondAnd}$$

Take $i = \mathsf{S}\, i$.

By application of the induction hypothesis, we obtain the following.

For all t_2, σ, j such that $t_2, \sigma \xrightarrow{j} t_2', \sigma'$ there exists an $i \sim j$ such that $t_2'', \sigma'' \ \rightarrow\ t_2''', \sigma''', i, \varphi$.

From this, we can conclude that $\mathsf{F}\, i \sim \mathsf{S}\, j$. From SH-And, and the conclusion of the induction hypothesis, we can conclude that there exists an i such that $t_1 \bowtie t_2, \sigma \ \rightarrow\ t_1 \bowtie t_2', \sigma', i, \varphi$.

□

Proof of Theorem **??**. The driving semantics only consists of one rule, namely $\dfrac{t, \sigma \xrightarrow{j} \hat{t}', \hat{\sigma}' \qquad \hat{t}', \hat{\sigma}' \Downarrow \hat{t}'', \hat{\sigma}''}{t, \sigma \overset{j}{\Rightarrow} \hat{t}'', \hat{\sigma}''}\ \textsc{I-Handle}$.

By Lemma **??** we obtain the following.

$t, \sigma \underset{j}{\rightarrow} \hat{t'}, \hat{\sigma'} \supset \exists i. t, \sigma \ \rightarrow\ t', \sigma', i, \varphi \wedge i \sim j$

Then by Lemma **??** we obtain the following.

$\hat{t'}, \hat{\sigma'} \Downarrow \hat{t''}, \hat{\sigma''} \supset \hat{t'}, \hat{\sigma'} \ \Downarrow\ t'', \sigma'', \varphi'$

From the above, together with the SI-Handle rule, we can conclude that there exists a symbolic execution $t, \sigma \ \Rightarrow\ t', \sigma', i, \varphi \wedge i \sim j$.

□