A Complete syntax

Expressions

$e ::=$	$\lambda x : \tau .\, e \ \mid\ e_1\, e_2 \ \mid\ x \ \mid\ c \ \mid\ \langle\rangle$	– abstraction, application, variable, constant, unit
$\mid$	$u\, e_1 \ \mid\ e_1\, o\, e_2 \ \mid\ \textbf{if}\, e_1\, \textbf{then}\, e_2\, \textbf{else}\, e_3$	– unary, binary operation, conditional
$\mid$	$\langle e_1, e_2\rangle \ \mid\ \mathsf{fst}\, e \ \mid\ \mathsf{snd}\, e \ \mid\ [\,]_\beta \ \mid\ e_1 :: e_2$	– pair, projections, nil, cons
$\mid$	$\mathsf{head}\ e \ \mid\ \mathsf{tail}\ e, p$	– first element, list tail, pretask
$\mid$	$\textbf{ref}\, e \ \mid\ !e \ \mid\ e_1 := e_2 \ \mid\ l$	– reference, dereference, assignment, location

Constants	$c ::= B \ \mid\ I \ \mid\ S$	– boolean, integer, string
Unary Operations	$u ::= \neg \ \mid\ - \ \mid\ \mathsf{len} \ \mid\ \mathsf{uniq}$	– not, negate, length, unique
Binary Operations	$o ::= < \mid \leq \mid \equiv \mid \not\equiv \mid \geq \mid >$	– equational
	$\mid\ + \ \mid\ - \ \mid\ \times \ \mid\ /$	– numerical
	$\mid\ +\!\!+ \ \mid \in$	– append, elementhood

Fig. 7: Language grammar

Pretasks

$p ::=$	$\square\, e \ \mid\ \boxtimes\, \tau \ \mid\ \blacksquare\, e \ \mid\ e_1 \blacktriangleright e_2 \ \mid\ e_1 \triangleright e_2$	– editors: valued, empty, shared, steps: internal, external
$\mid$	$e_1 \blacklozenge e_2 \ \mid\ e_1 \lozenge e_2 \ \mid\ e_1 \bowtie e_2 \ \mid\ \lightning$	– choice: internal, external, composition, fail

Fig. 8: Task grammar

Types	$\tau ::= \tau_1 \rightarrow \tau_2 \ \mid\ \beta \ \mid\ \textsc{Ref}\, \tau \ \mid\ \textsc{Task}\, \tau$	– function, basic, reference, task
Basic types	$\beta ::= \tau_1 \times \tau_2 \ \mid\ \textsc{List}\, \beta \ \mid\ \textsc{Unit}$	– product, list, unit
	$\mid\ \textsc{Bool} \ \mid\ \textsc{Int} \ \mid\ \textsc{String}$	– boolean, integer, string

Fig. 9: Type grammar

Values

$v ::=$	$\lambda x : \tau .\, e \ \mid\ \langle v_1, v_2\rangle \ \mid\ \langle\rangle \ \mid\ [\,]_\beta \ \mid\ v_1 :: v_2$	– abstraction, pair, unit, nil, cons
$\mid$	$c \ \mid\ l \ \mid\ t \ \mid\ u\, v \ \mid\ v_1\, o\, v_2$	– constant, location, task,unary/binary operation

Tasks

$t ::=$	$\square\, v \ \mid\ \boxtimes\, \tau \ \mid\ \blacksquare\, l \ \mid\ t_1 \blacktriangleright e_2 \ \mid\ t_1 \triangleright e_2$	– editors: valued, empty, shared, steps: internal, external
$\mid$	$t_1 \blacklozenge t_2 \ \mid\ e_1 \lozenge e_2 \ \mid\ t_1 \bowtie t_2 \ \mid\ \lightning$	– choice: internal, external, composition, fail

Fig. 10: Value grammar

B $\widehat{\textbf{TOP}}$ semantics

B.1 Typing rules

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

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

$$\textsc{T-Var}\ \frac{x : \tau \in \Gamma}{\Gamma, \Sigma \vdash x : \tau} \qquad \textsc{T-Loc}\ \frac{\Sigma(l) = \beta}{\Gamma, \Sigma \vdash l : \textsf{Ref}\,\beta} \qquad \textsc{T-Pair}\ \frac{\Gamma, \Sigma \vdash e_1 : \tau_1 \qquad \Gamma, \Sigma \vdash e_2 : \tau_2}{\Gamma, \Sigma \vdash \langle e_1, e_2\rangle : \tau_1 \times \tau_2}$$

$$\textsc{T-First}\ \frac{\Gamma, \Sigma \vdash e_1 : \tau}{\Gamma, \Sigma \vdash \textsf{fst}\langle e_1, e_2\rangle : \tau} \qquad \textsc{T-Second}\ \frac{\Gamma, \Sigma \vdash e_2 : \tau}{\Gamma, \Sigma \vdash \textsf{snd}\langle e_1, e_2\rangle : \tau} \qquad \textsc{T-ListEmpty}\ \frac{}{\Gamma, \Sigma \vdash [\,]_\beta : \textsf{List}\,\beta}$$

$$\textsc{T-ListCons}\ \frac{\Gamma, \Sigma \vdash e_1 : \beta \qquad \Gamma, \Sigma \vdash e_2 : \textsf{List}\,\beta}{\Gamma, \Sigma \vdash e_1 :: e_2 : \textsf{List}\,\beta} \qquad \textsc{T-ListHead}\ \frac{\Gamma, \Sigma \vdash e : \textsf{List}\,\beta}{\Gamma, \Sigma \vdash \textsf{head}\,e : \beta} \qquad \textsc{T-ListTail}\ \frac{\Gamma, \Sigma \vdash e : \textsf{List}\,\beta}{\Gamma, \Sigma \vdash \textsf{tail}\,e : \textsf{List}\,\beta}$$

$$\textsc{T-Abs}\ \frac{\Gamma[x : \tau_1], \Sigma \vdash e : \tau_2}{\Gamma, \Sigma \vdash \lambda x : \tau_1 . e : \tau_1 \to \tau_2} \qquad \textsc{T-App}\ \frac{\Gamma, \Sigma \vdash e_1 : \tau_1 \to \tau_2 \qquad \Gamma, \Sigma \vdash e_2 : \tau_1}{\Gamma, \Sigma \vdash e_1 e_2 : \tau_2}$$

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

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

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

$$\textsc{T-Fail}\ \frac{}{\Gamma, \Sigma \vdash \lightning : \textsf{Task}\,\tau} \qquad \textsc{T-Then}\ \frac{\Gamma, \Sigma \vdash e_1 : \textsf{Task}\,\tau_1 \qquad \Gamma, \Sigma \vdash e_2 : \tau_1 \to \textsf{Task}\,\tau_2}{\Gamma, \Sigma \vdash e_1 \blacktriangleright e_2 : \textsf{Task}\,\tau_2} \qquad \textsc{T-Next}\ \frac{\Gamma, \Sigma \vdash e_1 : \textsf{Task}\,\tau_1 \qquad \Gamma, \Sigma \vdash e_2 : \tau_1 \to \textsf{Task}\,\tau_2}{\Gamma, \Sigma \vdash e_1 \rhd e_2 : \textsf{Task}\,\tau_2}$$

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

B.2 Evaluation rules

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

$$\textsc{E-App}\quad \frac{e_1, \sigma \ \downarrow\ \lambda x : \tau . e_1', \sigma' \qquad e_2, \sigma' \ \downarrow\ v_2, \sigma'' \qquad e_1'[x \mapsto v_2], \sigma'' \ \downarrow\ v_1, \sigma'''}{e_1 e_2, \sigma \ \downarrow\ v_1, \sigma'''}$$

$$\textsc{E-IfTrue}\quad \frac{e_1, \sigma \downarrow \mathsf{True}, \sigma' \qquad e_2, \sigma' \downarrow v_2, \sigma''}{\textbf{if}\ e_1\ \textbf{then}\ e_2\ \textbf{else}\ e_3, \sigma \downarrow v_2, \sigma''} \qquad \textsc{E-Ref}\quad \frac{e, \sigma \downarrow v, \sigma' \qquad l \notin Dom(\sigma')}{\textbf{ref}\ e, \sigma \downarrow l, \sigma'[l \mapsto v]}$$

$$\textsc{E-IfFalse}\quad \frac{e_1, \sigma \downarrow v_1, \sigma' \qquad e_3, \sigma' \downarrow v_3, \sigma''}{\textbf{if}\ e_1\ \textbf{then}\ e_2\ \textbf{else}\ e_3, \sigma \downarrow v_3, \sigma''} \qquad \textsc{E-Deref}\quad \frac{e, \sigma \downarrow l, \sigma'}{!e, \sigma \downarrow \sigma'(l), \sigma'} \qquad \textsc{E-Value}\quad \frac{}{v, \sigma \downarrow v, \sigma}$$

$$\textsc{E-Assign}\quad \frac{e_1, \sigma \downarrow l, \sigma' \qquad e_2, \sigma' \downarrow v_2, \sigma''}{e_1 := e_2, \sigma \downarrow \langle\rangle, \sigma''[l \mapsto v_2]} \qquad \textsc{E-Pair}\quad \frac{e_1, \sigma \downarrow v_1, \sigma' \qquad e_2, \sigma' \downarrow v_2, \sigma''}{\langle e_1, e_2 \rangle, \sigma \downarrow \langle v_1, v_2 \rangle, \sigma''}$$

$$\textsc{E-First}\quad \frac{e_1, \sigma \downarrow v_1, \sigma'}{\mathsf{fst}\langle e_1, e_2 \rangle, \sigma \downarrow v_1, \sigma'} \qquad \textsc{E-Second}\quad \frac{e_2, \sigma \downarrow v_2, \sigma'}{\mathsf{snd}\langle e_1, e_2 \rangle, \sigma \downarrow v_2, \sigma'} \qquad \textsc{E-Cons}\quad \frac{e_1, \sigma \downarrow v_1, \sigma' \qquad e_2, \sigma' \downarrow v_2, \sigma''}{e_1 :: e_2, \sigma \downarrow v_1 :: v_2, \sigma''}$$

$$\textsc{E-Head}\quad \frac{e, \sigma \downarrow v_1 :: v_2, \sigma'}{\mathsf{head}\ e, \sigma \downarrow v_1, \sigma'} \qquad \textsc{E-Tail}\quad \frac{e, \sigma \downarrow v_1 :: v_2, \sigma'}{\mathsf{tail}\ e, \sigma \downarrow v_2, \sigma'} \qquad \textsc{E-Edit}\quad \frac{e, \sigma \downarrow v, \sigma'}{\square\, e, \sigma \downarrow \square\, v, \sigma'}$$

$$\textsc{E-Update}\quad \frac{e, \sigma \downarrow l, \sigma'}{\blacksquare\, e, \sigma \downarrow \blacksquare\, l, \sigma'} \qquad \textsc{E-Then}\quad \frac{e_1, \sigma \downarrow t_1, \sigma'}{e_1 \blacktriangleright e_2, \sigma \downarrow t_1 \blacktriangleright e_2, \sigma'} \qquad \textsc{E-Next}\quad \frac{e_1, \sigma \downarrow t_1, \sigma'}{e_1 \triangleright e_2, \sigma \downarrow t_1 \triangleright e_2, \sigma'}$$

$$\textsc{E-And}\quad \frac{e_1, \sigma \downarrow t_1, \sigma' \qquad e_2, \sigma' \downarrow t_2, \sigma''}{e_1 \bowtie e_2, \sigma \downarrow t_1 \bowtie t_2, \sigma''} \qquad \textsc{E-Or}\quad \frac{e_1, \sigma \downarrow t_1, \sigma' \qquad e_2, \sigma' \downarrow t_2, \sigma''}{e_1 \blacklozenge e_2, \sigma \downarrow t_1 \blacklozenge t_2, \sigma''}$$

B.3 Striding rules

$$\boxed{t, \sigma \;\mapsto\; t', \sigma'}$$

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

$$\textsc{S-ThenFail}\;\frac{t_1, \sigma \mapsto t_1', \sigma' \qquad e_2\; v_1, \sigma' \downarrow t_2, \sigma''}{t_1 \blacktriangleright e_2, \sigma \mapsto t_1' \blacktriangleright e_2, \sigma'}\;\mathcal{V}(t_1', \sigma') = v_1 \land \mathcal{F}(t_2, \sigma'')$$

$$\textsc{S-ThenCont}\;\frac{t_1, \sigma \mapsto t_1', \sigma' \qquad e_2\; v_1, \sigma' \downarrow t_2, \sigma''}{t_1 \blacktriangleright e_2, \sigma \mapsto t_2, \sigma''}\;\mathcal{V}(t_1', \sigma') = v_1 \land \neg\mathcal{F}(t_2, \sigma'')$$

$$\textsc{S-OrLeft}\;\frac{t_1, \sigma \mapsto t_1', \sigma'}{t_1 \blacklozenge t_2, \sigma \mapsto t_1', \sigma'}\;\mathcal{V}(t_1', \sigma') = v_1$$

$$\textsc{S-OrRight}\;\frac{t_1, \sigma \mapsto t_1', \sigma' \qquad t_2, \sigma' \mapsto t_2', \sigma''}{t_1 \blacklozenge t_2, \sigma \mapsto t_2', \sigma''}\;\mathcal{V}(t_1', \sigma') = \bot \land \mathcal{V}(t_2', \sigma'') = v_2$$

$$\textsc{S-OrNone}\;\frac{t_1, \sigma \mapsto t_1', \sigma' \qquad t_2, \sigma' \mapsto t_2', \sigma''}{t_1 \blacklozenge t_2, \sigma \mapsto t_1' \blacklozenge t_2', \sigma''}\;\mathcal{V}(t_1', \sigma') = \bot \land \mathcal{V}(t_2', \sigma'') = \bot$$

$$\textsc{S-Edit}\;\frac{}{\square\, v, \sigma \mapsto \square\, v, \sigma} \qquad \textsc{S-Fill}\;\frac{}{\boxtimes\, \tau, \sigma \mapsto \boxtimes\, \tau, \sigma} \qquad \textsc{S-Update}\;\frac{}{\blacksquare\, l, \sigma \mapsto \blacksquare\, l, \sigma}$$

$$\textsc{S-Fail}\;\frac{}{\lightning, \sigma \mapsto \lightning, \sigma} \qquad \textsc{S-Xor}\;\frac{}{e_1 \lozenge e_2, \sigma \mapsto e_1 \lozenge e_2, \sigma} \qquad \textsc{S-Next}\;\frac{t_1, \sigma \mapsto t_1', \sigma'}{t_1 \triangleright e_2, \sigma \mapsto t_1' \triangleright e_2, \sigma'}$$

$$\textsc{S-And}\;\frac{t_1, \sigma \mapsto t_1', \sigma' \qquad t_2, \sigma' \mapsto t_2', \sigma''}{t_1 \bowtie t_2, \sigma \mapsto t_1' \bowtie t_2', \sigma''}$$

B.4 Normalisation rules

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

$$\textsc{N-Done}\;\frac{e, \sigma \downarrow t, \sigma' \qquad t, \sigma' \mapsto t', \sigma''}{e, \sigma \Downarrow t, \sigma'}\;\sigma' = \sigma'' \land t = t'$$

$$\textsc{N-Repeat}\;\frac{e, \sigma \downarrow t, \sigma' \qquad t, \sigma' \mapsto t', \sigma'' \qquad t', \sigma'' \Downarrow t'', \sigma'''}{e, \sigma \Downarrow t'', \sigma'''}\;\sigma' \neq \sigma'' \lor t \neq t'$$

B.5 Handling rules

$$\boxed{t, \sigma \xrightarrow{i} t', \sigma'}$$

$$\text{H-CHANGE}\quad \frac{}{\Box\, v, \sigma \xrightarrow{v'} \Box\, v', \sigma}\; v, v' : \tau \qquad \text{H-FILL}\quad \frac{}{\boxtimes\, \tau, \sigma \xrightarrow{v} \Box\, v, \sigma}\; v : \tau$$

$$\text{H-UPDATE}\quad \frac{}{\blacksquare\, l, \sigma \xrightarrow{v} \blacksquare\, l, \sigma[l \mapsto v]}\; \sigma(l), v : \tau \qquad \text{H-NEXT}\quad \frac{e_2\ v_1, \sigma \Downarrow t_2, \sigma'}{t_1 \rhd e_2, \sigma \xrightarrow{\mathsf{C}} t_2, \sigma'}\; \mathcal{V}(t_1, \sigma) = v_1 \land \neg\mathcal{F}(t_2, \sigma')$$

$$\text{H-PICKLEFT}\quad \frac{e_1, \sigma \Downarrow t_1, \sigma'}{e_1 \lozenge e_2, \sigma \xrightarrow{\mathsf{L}} t_1, \sigma'}\; \neg\mathcal{F}(t_1, \sigma') \qquad \text{H-PICKRIGHT}\quad \frac{e_2, \sigma \Downarrow t_2, \sigma'}{e_1 \lozenge e_2, \sigma \xrightarrow{\mathsf{R}} t_2, \sigma'}\; \neg\mathcal{F}(t_2, \sigma')$$

$$\text{H-PASSTHEN}\quad \frac{t_1, \sigma \xrightarrow{i} t_1', \sigma'}{t_1 \blacktriangleright e_2, \sigma \xrightarrow{i} t_1' \blacktriangleright e_2, \sigma'} \qquad \text{H-PASSNEXT}\quad \frac{t_1, \sigma \xrightarrow{i} t_1', \sigma'}{t_1 \rhd e_2, \sigma \xrightarrow{i} t_1' \rhd e_2, \sigma'} \qquad \text{H-FIRSTAND}\quad \frac{t_1, \sigma \xrightarrow{i} t_1', \sigma'}{t_1 \bowtie t_2, \sigma \xrightarrow{\mathsf{F}\, i} t_1' \bowtie t_2, \sigma'}$$

$$\text{H-SECONDAND}\quad \frac{t_2, \sigma \xrightarrow{i} t_2', \sigma'}{t_1 \bowtie t_2, \sigma \xrightarrow{\mathsf{S}\, i} t_1 \bowtie t_2', \sigma'} \qquad \text{H-FIRSTOR}\quad \frac{t_1, \sigma \xrightarrow{i} t_1', \sigma'}{t_1 \blacklozenge t_2, \sigma \xrightarrow{\mathsf{F}\, i} t_1' \blacklozenge t_2, \sigma'} \qquad \text{H-SECONDOR}\quad \frac{t_2, \sigma \xrightarrow{i} t_2', \sigma'}{t_1 \blacklozenge t_2, \sigma \xrightarrow{\mathsf{S}\, i} t_1 \blacklozenge t_2', \sigma'}$$

B.6 Interacting rules

$$\boxed{t, \sigma \overset{i}{\Rightarrow} t', \sigma'}$$

$$\text{I-HANDLE}\quad \frac{t, \sigma \xrightarrow{i} t', \sigma' \qquad t', \sigma' \Downarrow t'', \sigma''}{t, \sigma \overset{i}{\Rightarrow} t'', \sigma''}$$

C Complete symbolic semantics

C.1 Symbolic evaluation rules

$$\boxed{\tilde{e}, \tilde{\sigma} \;\wr\; \overline{\tilde{v}, \tilde{\sigma}', \varphi}}$$

$$\textsc{SE-Value}\quad \frac{}{\tilde{v}, \tilde{\sigma} \;\wr\; \tilde{v}, \tilde{\sigma}, \mathsf{True}}$$

$$\textsc{SE-Pair}\quad \frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{\tilde{v}_1, \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \;\wr\; \overline{\tilde{v}_2, \tilde{\sigma}'', \varphi_2}}{\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \;\wr\; \overline{\langle \tilde{v}_1, \tilde{v}_2 \rangle, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}}$$

$$\textsc{SE-First}\quad \frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{\tilde{v}_1, \tilde{\sigma}', \varphi}}{\mathsf{fst}\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \;\wr\; \overline{\tilde{v}_1, \tilde{\sigma}', \varphi}}
\qquad
\textsc{SE-Second}\quad \frac{\tilde{e}_2, \tilde{\sigma} \;\wr\; \overline{\tilde{v}_2, \tilde{\sigma}', \varphi}}{\mathsf{snd}\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \;\wr\; \overline{\tilde{v}_2, \tilde{\sigma}', \varphi}}$$

$$\textsc{SE-Cons}\quad \frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \tilde{v}_1, \tilde{\sigma}', \varphi_1 \qquad \tilde{e}_2, \tilde{\sigma}' \;\wr\; \tilde{v}_2, \tilde{\sigma}'', \varphi_2}{\tilde{e}_1 :: \tilde{e}_2, \tilde{\sigma} \;\wr\; \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}
\qquad
\textsc{SE-Head}\quad \frac{\tilde{e}, \tilde{\sigma} \;\wr\; \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}', \varphi}{\mathsf{head}\, \tilde{e}, \tilde{\sigma} \;\wr\; \tilde{v}_1, \tilde{\sigma}', \varphi}$$

$$\textsc{SE-Tail}\quad \frac{\tilde{e}, \tilde{\sigma} \;\wr\; \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}', \varphi}{\mathsf{tail}\, \tilde{e}, \tilde{\sigma} \;\wr\; \tilde{v}_2, \tilde{\sigma}', \varphi}$$

$$\textsc{SE-App}\quad \frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{\lambda x : \tau. \tilde{e}_1', \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \;\wr\; \overline{\tilde{v}_2, \tilde{\sigma}'', \varphi_2} \qquad \tilde{e}_1'[x \mapsto \tilde{v}_2], \tilde{\sigma}'' \;\wr\; \overline{\tilde{v}_1, \tilde{\sigma}''', \varphi_3}}{\tilde{e}_1 \tilde{e}_2, \tilde{\sigma} \;\wr\; \overline{\tilde{v}_1, \tilde{\sigma}''', \varphi_1 \wedge \varphi_2 \wedge \varphi_3}}$$

$$\textsc{SE-If}\quad \frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{\tilde{v}_1, \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \;\wr\; \overline{\tilde{v}_2, \tilde{\sigma}'', \varphi_2} \qquad \tilde{e}_3, \tilde{\sigma}' \;\wr\; \overline{\tilde{v}_3, \tilde{\sigma}''', \varphi_3}}{\textbf{if}\, \tilde{e}_1 \,\textbf{then}\, \tilde{e}_2 \,\textbf{else}\, \tilde{e}_3, \tilde{\sigma} \;\wr\; \overline{\tilde{v}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2 \wedge \tilde{v}_1} \cup \overline{\tilde{v}_3, \tilde{\sigma}''', \varphi_1 \wedge \varphi_3 \wedge \neg \tilde{v}_1}}$$

$$\textsc{SE-Ref}\quad \frac{\tilde{e}, \tilde{\sigma} \;\wr\; \overline{\tilde{v}, \tilde{\sigma}', \varphi} \qquad l \notin Dom(\sigma')}{\textbf{ref}\, \tilde{e}, \tilde{\sigma} \;\wr\; \overline{l, \tilde{\sigma}'[l \mapsto \tilde{v}], \varphi}}
\qquad
\textsc{SE-Deref}\quad \frac{\tilde{e}, \tilde{\sigma} \;\wr\; \overline{l, \tilde{\sigma}', \varphi}}{!\tilde{e}, \tilde{\sigma} \;\wr\; \overline{\tilde{\sigma}'(l), \tilde{\sigma}', \varphi}}$$

$$\textsc{SE-Assign}\quad \frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{l, \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \;\wr\; \overline{\tilde{v}_2, \tilde{\sigma}'', \varphi_2}}{\tilde{e}_1 := \tilde{e}_2, \tilde{\sigma} \;\wr\; \overline{\langle\rangle, \tilde{\sigma}''[l \mapsto \tilde{v}_2], \varphi_1 \wedge \varphi_2}}
\qquad
\textsc{SE-Edit}\quad \frac{\tilde{e}, \tilde{\sigma} \;\wr\; \overline{\tilde{v}, \tilde{\sigma}', \varphi}}{\square\, \tilde{e}, \tilde{\sigma} \;\wr\; \overline{\square\, \tilde{v}, \tilde{\sigma}', \varphi}}$$

$$\textsc{SE-Enter}\quad \frac{}{\boxtimes\, \tau, \tilde{\sigma} \;\wr\; \boxtimes\, \tau, \tilde{\sigma}, \mathsf{True}}
\qquad
\textsc{SE-Update}\quad \frac{\tilde{e}, \tilde{\sigma} \;\wr\; \overline{l, \tilde{\sigma}', \varphi}}{\blacksquare\, \tilde{e}, \tilde{\sigma} \;\wr\; \overline{\blacksquare\, l, \tilde{\sigma}', \varphi}}$$

$$\textsc{SE-Then}\quad \frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1, \tilde{\sigma}', \varphi}}{\tilde{e}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi}}
\qquad
\textsc{SE-Next}\quad \frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1, \tilde{\sigma}', \varphi}}{\tilde{e}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma}', \varphi}}$$

$$\textsc{SE-And}\quad \frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1, \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \;\wr\; \overline{\tilde{t}_2, \tilde{\sigma}'', \varphi_2}}{\tilde{e}_1 \bowtie \tilde{e}_2, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}}
\qquad
\textsc{SE-Or}\quad \frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1, \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \;\wr\; \overline{\tilde{t}_2, \tilde{\sigma}'', \varphi_2}}{\tilde{e}_1 \blacklozenge \tilde{e}_2, \tilde{\sigma} \;\wr\; \overline{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}}$$

$$\textsc{SE-Xor}\quad \frac{}{\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \;\wr\; \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}, \mathsf{True}}
\qquad
\textsc{SE-Fail}\quad \frac{}{\lightning, \tilde{\sigma} \;\wr\; \lightning, \tilde{\sigma}, \mathsf{True}}$$

C.2 Symbolic striding rules

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

$$\textsc{SS-ThenStay}\quad \frac{\tilde{t}_1, \tilde{\sigma} \;\mapstochar\rightsquigarrow\; \overline{\tilde{t}_1', \tilde{\sigma}', \varphi}}{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \;\mapstochar\rightsquigarrow\; \overline{\tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi}}\ \mathcal{V}(\tilde{t}_1', \tilde{\sigma}') = \bot$$

$$\textsc{SS-ThenFail}\quad \frac{\tilde{t}_1, \tilde{\sigma} \;\mapstochar\rightsquigarrow\; \overline{\tilde{t}_1', \tilde{\sigma}', \varphi} \qquad \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma}' \;\rotatebox[origin=c]{-90}{$\rightsquigarrow$}\; \overline{\tilde{t}_2, \tilde{\sigma}'', \_}}{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \;\mapstochar\rightsquigarrow\; \overline{\tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi}}\ \mathcal{V}(\tilde{t}_1', \tilde{\sigma}') = \tilde{v}_1 \land \mathcal{F}(\tilde{t}_2, \tilde{\sigma}'')$$

$$\textsc{SS-ThenCont}\quad \frac{\tilde{t}_1, \tilde{\sigma} \;\mapstochar\rightsquigarrow\; \overline{\tilde{t}_1', \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma}' \;\rotatebox[origin=c]{-90}{$\rightsquigarrow$}\; \overline{\tilde{t}_2, \tilde{\sigma}'', \varphi_2}}{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \;\mapstochar\rightsquigarrow\; \overline{t_2, \sigma'', \varphi_1 \land \varphi_2}}\ \mathcal{V}(\tilde{t}_1', \tilde{\sigma}') = \tilde{v}_1 \land \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}'')$$

$$\textsc{SS-OrLeft}\quad \frac{\tilde{t}_1, \tilde{\sigma} \;\mapstochar\rightsquigarrow\; \overline{\tilde{t}_1', \tilde{\sigma}', \varphi}}{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \;\mapstochar\rightsquigarrow\; \overline{\tilde{t}_1', \tilde{\sigma}', \varphi}}\ \mathcal{V}(\tilde{t}_1', \tilde{\sigma}') = \tilde{v}_1$$

$$\textsc{SS-OrRight}\quad \frac{\tilde{t}_1, \tilde{\sigma} \;\mapstochar\rightsquigarrow\; \overline{\tilde{t}_1', \tilde{\sigma}', \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma}' \;\mapstochar\rightsquigarrow\; \overline{\tilde{t}_2', \tilde{\sigma}'', \varphi_2}}{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \;\mapstochar\rightsquigarrow\; \overline{\tilde{t}_2', \tilde{\sigma}'', \varphi_1 \land \varphi_2}}\ \mathcal{V}(\tilde{t}_1', \tilde{\sigma}') = \bot \land \mathcal{V}(\tilde{t}_2', \tilde{\sigma}'') = \tilde{v}_2$$

$$\textsc{SS-OrNone}\quad \frac{\tilde{t}_1, \tilde{\sigma} \;\mapstochar\rightsquigarrow\; \overline{\tilde{t}_1', \tilde{\sigma}', \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma}' \;\mapstochar\rightsquigarrow\; \overline{\tilde{t}_2', \tilde{\sigma}'', \varphi_2}}{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \;\mapstochar\rightsquigarrow\; \overline{\tilde{t}_1' \blacklozenge \tilde{t}_2', \tilde{\sigma}'', \varphi_1 \land \varphi_2}}\ \mathcal{V}(\tilde{t}_1', \tilde{\sigma}') = \bot \land \mathcal{V}(\tilde{t}_2', \tilde{\sigma}'') = \bot$$

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

$$\textsc{SS-Fail}\quad \frac{}{\lightning, \tilde{\sigma} \;\mapstochar\rightsquigarrow\; \lightning, \tilde{\sigma}, \mathsf{True}} \qquad \textsc{SS-Xor}\quad \frac{}{\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \;\mapstochar\rightsquigarrow\; \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}, \mathsf{True}}$$

$$\textsc{SS-Next}\quad \frac{\tilde{t}_1, \tilde{\sigma} \;\mapstochar\rightsquigarrow\; \overline{\tilde{t}_1', \tilde{\sigma}', \varphi}}{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \;\mapstochar\rightsquigarrow\; \overline{\tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}', \varphi}} \qquad \textsc{SS-And}\quad \frac{\tilde{t}_1, \tilde{\sigma} \;\mapstochar\rightsquigarrow\; \overline{\tilde{t}_1', \tilde{\sigma}', \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma}' \;\mapstochar\rightsquigarrow\; \overline{\tilde{t}_2', \tilde{\sigma}'', \varphi_2}}{\tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma} \;\mapstochar\rightsquigarrow\; \overline{\tilde{t}_1' \bowtie \tilde{t}_2', \tilde{\sigma}'', \varphi_1 \land \varphi_2}}$$

C.3 Symbolic normalisation rules

$$\boxed{\tilde{e}, \tilde{\sigma} \;\;\lll\;\; \overline{\tilde{t}, \tilde{\sigma}', \varphi}}$$

SN-Done

$$\frac{\tilde{e}, \tilde{\sigma} \;\wr\; \overline{\tilde{t}, \tilde{\sigma}', \varphi_1} \qquad \tilde{t}, \tilde{\sigma}' \;\looparrowright\; \overline{\tilde{t}', \tilde{\sigma}'', \varphi_2}}{\tilde{e}, \tilde{\sigma} \;\lll\; \overline{\tilde{t}, \tilde{\sigma}', \varphi_1}} \;\tilde{\sigma}' = \tilde{\sigma}'' \wedge \tilde{t} = \tilde{t}'$$

SN-Repeat

$$\frac{\tilde{e}, \tilde{\sigma} \;\wr\; \overline{\tilde{t}, \tilde{\sigma}', \varphi_1} \qquad \tilde{t}, \tilde{\sigma}' \;\looparrowright\; \overline{\tilde{t}', \tilde{\sigma}'', \varphi_2} \qquad \tilde{t}', \tilde{\sigma}'' \;\lll\; \overline{\tilde{t}'', \tilde{\sigma}''', \varphi_3}}{\tilde{e}, \tilde{\sigma} \;\lll\; \overline{\tilde{t}'', \tilde{\sigma}''', \varphi_1 \wedge \varphi_2 \wedge \varphi_3}} \;\tilde{\sigma}' \neq \tilde{\sigma}'' \vee \tilde{t} \neq \tilde{t}'$$

C.4 Symbolic driving rules

$$\boxed{\tilde{t}, \tilde{\sigma} \;\;\rightsquigarrow\!\!\!\!\!\rightsquigarrow\;\; \overline{\tilde{t}', \tilde{\sigma}', \tilde{\iota}, \varphi}}$$

SI-Handle

$$\frac{\tilde{t}, \tilde{\sigma} \;\rightsquigarrow\; \overline{\tilde{t}', \tilde{\sigma}', \tilde{\iota}, \varphi_1} \qquad \tilde{t}', \tilde{\sigma}' \;\lll\; \overline{\tilde{t}'', \tilde{\sigma}'', \varphi_2}}{\tilde{t}, \tilde{\sigma} \;\rightsquigarrow\!\!\!\!\!\rightsquigarrow\; \overline{\tilde{t}'', \tilde{\sigma}'', \tilde{\iota}, \varphi_1 \wedge \varphi_2}}$$

C.5 Symbolic handling rules

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

SH-Change

$$\frac{\text{fresh } s}{\Box\, \tilde{v}, \tilde{\sigma} \rightsquigarrow \Box\, s, \tilde{\sigma}, s, \mathsf{True}}\ \tilde{v}, s : \tau$$

SH-Fill

$$\frac{\text{fresh } \tilde{s}}{\boxtimes\, \tau, \tilde{\sigma} \rightsquigarrow \Box\, s, \tilde{\sigma}, s, \mathsf{True}}\ s : \tau$$

SH-Update

$$\frac{\text{fresh } s}{\blacksquare\, l, \tilde{\sigma} \rightsquigarrow \blacksquare\, l, \tilde{\sigma}[l \mapsto s], s, \mathsf{True}}\ \sigma(l), s : \tau$$

SH-PassNext

$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \tilde{\imath}, \varphi}}{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}', \tilde{\imath}, \varphi}}\ \mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \bot$$

SH-PassNextFail

$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}, \varphi} \qquad \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma} \mathrel{\rotatebox[origin=c]{-90}{$\rightsquigarrow$}} \overline{\tilde{t}_2, \tilde{\sigma}_2', \_}}{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}_1', \tilde{\imath}, \varphi}}\ \mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \tilde{v}_1 \wedge \mathcal{F}(\tilde{t}_2, \tilde{\sigma}_2')$$

SH-Next

$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}, \varphi_1} \qquad \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma} \mathrel{\rotatebox[origin=c]{-90}{$\rightsquigarrow$}} \overline{\tilde{t}_2, \tilde{\sigma}_2', \varphi_2}}{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \triangleright \tilde{e}_2, \tilde{\sigma}_1', \tilde{\imath}, \varphi_1} \cup \overline{\tilde{t}_2, \tilde{\sigma}_2', \mathsf{C}, \varphi_2}}\ \mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \tilde{v}_1 \wedge \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}')$$

SH-PassThen

$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \tilde{\imath}, \varphi}}{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \tilde{\imath}, \varphi}}$$

SH-Pick

$$\frac{\tilde{e}_1, \tilde{\sigma} \Downarrow \overline{\tilde{t}_1, \tilde{\sigma}_1, \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma} \Downarrow \overline{\tilde{t}_2, \tilde{\sigma}_2, \varphi_2}}{\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1, \tilde{\sigma}_1, \mathsf{L}, \varphi_1} \cup \overline{\tilde{t}_2, \tilde{\sigma}_2, \mathsf{R}, \varphi_2}}\ \neg\mathcal{F}(\tilde{t}_1, \tilde{\sigma}_1) \wedge \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}_2)$$

SH-PickLeft

$$\frac{\tilde{e}_1, \tilde{\sigma} \mathrel{\rotatebox[origin=c]{-90}{$\rightsquigarrow$}} \overline{\tilde{t}_1, \tilde{\sigma}_1, \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma} \mathrel{\rotatebox[origin=c]{-90}{$\rightsquigarrow$}} \overline{\tilde{t}_2, \tilde{\sigma}_2, \varphi_2}}{\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{t}_1, \tilde{\sigma}_1, \mathsf{L}, \varphi_1}\ \neg\mathcal{F}(\tilde{t}_1, \tilde{\sigma}_1) \wedge \mathcal{F}(\tilde{t}_2, \tilde{\sigma}_2)$$

SH-PickRight

$$\frac{\tilde{e}_1, \tilde{\sigma} \mathrel{\rotatebox[origin=c]{-90}{$\rightsquigarrow$}} \overline{\tilde{t}_1, \tilde{\sigma}_1, \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma} \mathrel{\rotatebox[origin=c]{-90}{$\rightsquigarrow$}} \overline{\tilde{t}_2, \tilde{\sigma}_2, \varphi_2}}{\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{t}_2, \tilde{\sigma}_2, \mathsf{R}, \varphi_2}\ \mathcal{F}(\tilde{t}_1, \tilde{\sigma}_1) \wedge \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}_2)$$

SH-And

$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}_1, \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_2', \tilde{\sigma}_2', \tilde{\imath}_2, \varphi_2}}{\tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \bowtie \tilde{t}_2, \tilde{\sigma}_1', \mathsf{F}\,\tilde{\imath}_1, \varphi_1} \cup \overline{\tilde{t}_1 \bowtie \tilde{t}_2', \tilde{\sigma}_2'', \mathsf{S}\,\tilde{\imath}_2, \varphi_2}}$$

SH-Or

$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}_1, \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_2', \tilde{\sigma}_2', \tilde{\imath}_2, \varphi_2}}{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \blacklozenge \tilde{t}_2, \tilde{\sigma}_1', \mathsf{F}\,\tilde{\imath}_1, \varphi_1} \cup \overline{\tilde{t}_1 \blacklozenge \tilde{t}_2', \tilde{\sigma}_2', \mathsf{S}\,\tilde{\imath}_2, \varphi_2}}$$

D Soundness proofs

Proof (Soundness of simulate). The structure of this proof is outlined in Fig. 6.

We have t and σ such that $t, \sigma \rightsquigarrow^* \overline{\tilde{v}, \tilde{I}, \Phi}$. By definition of simulation ($\rightsquigarrow^*$), we know that for each tuple $(\tilde{v}, \tilde{I}, \Phi)$, the following sequence of symbolic drive steps has occurred.

$$
\begin{array}{llll}
t, \sigma \rightsquigarrow \tilde{t}_1, \tilde{\sigma}_1, \tilde{\imath}_1, \varphi_1 & & & \\
\quad \tilde{t}_1, \tilde{\sigma}_1 \rightsquigarrow & \tilde{t}_2, \tilde{\sigma}_2, \tilde{\imath}_2, \varphi_2 & & \\
& \quad \tilde{t}_2, \tilde{\sigma}_2 \rightsquigarrow \cdots & & \\
& & \cdots & \rightsquigarrow \tilde{t}_n, \tilde{\sigma}_n, \tilde{\imath}_n, \varphi_n
\end{array}
$$

with $\mathcal{V}(\tilde{t}_n, \tilde{\sigma}_n) = \tilde{v}$ and $\mathcal{S}(\varphi_1 \wedge \cdots \wedge \varphi_n)$.

We need to show that there exits an I such that $t, \sigma \overset{I}{\Rightarrow}^* v$, which is defined similarly as follows.

$t, \sigma \overset{i_1}{\Rightarrow} t_1, \sigma_1 \overset{i_2}{\Rightarrow} t_2, \sigma_2 \overset{i_3}{\Rightarrow} \cdots \overset{i_n}{\Rightarrow} t_n, \sigma_n$ with $\mathcal{V}(t_n, \sigma_n)$.

By Lemma 3, we know that $t, \sigma \overset{i_1}{\Rightarrow} t_1, \sigma_1$ exists, since $t, \sigma \leftrightarrows_{\emptyset} t, \sigma, \mathsf{True}$. This also gives us that $\tilde{i_1} \sim i_1$, and $t_1, \sigma_1 \leftrightarrows_{[s_1 \mapsto c_1]} \tilde{t}_1, \tilde{\sigma}_1, \varphi_1$ with $SymOf(\sim_1) = s_1$ and $ValOf(i_1) = c_1$.

By repeatedly applying Lemma 3, until we arrive at $\tilde{t}_n, \sigma t_n$, we can show that there indeed exists an I such that $t, \sigma \overset{I}{\Rightarrow}^* v$ with $[s_1 \mapsto c_1, \cdots, s_n \mapsto c_n]\tilde{v} = v$ and $[s_1 \mapsto c_1, \cdots, s_n \mapsto c_n]\Phi$, namely $I = [i_1, \cdots, i_n]$.

Proof (Soundness of driving). The symbolic driving semantics consists of only one rule, SI-HANDLE. Given that $t, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\tilde{t}, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}', \tilde{\sigma}', \tilde{\imath}, \varphi_1}$, Lemma 5 gives us that for each pair $(\tilde{t}', \tilde{\sigma}', \tilde{\imath}, \varphi_1)$ there exists an input i such that $\tilde{\imath} \sim i$, $t, \sigma \overset{i}{\rightarrow} t', \sigma'$ and $t', \sigma' \leftrightarrows_{M.[s \mapsto c]} \tilde{t}', \tilde{\sigma}', \Phi \wedge \varphi_1$.

Then, by Lemma 6, given that $\tilde{t}', \tilde{\sigma}' \Downarrow \overline{\tilde{t}'', \tilde{\sigma}'', \varphi_2}$, we obtain that for each pair $(\tilde{t}'', \tilde{\sigma}'', \varphi_2)$, we have that $\mathcal{S}(\Phi \wedge \varphi_1 \wedge \varphi_2)$ implies that $t', \sigma' \Downarrow t'', \sigma''$ with $t'', \sigma'' \leftrightarrows_{M.[s \mapsto c]} \tilde{t}'', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Lemma 5 (Soundness of handling).
For all concrete tasks t, concrete states σ, symbolic tasks $\tilde{t}$, symbolic states $\tilde{\sigma}$ path conditions Φ and mappings M, we have that $t, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ implies that for all symbolic inputs $\tilde{\imath}$ such that $\tilde{t}, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}', \tilde{\sigma}', \tilde{\imath}, \varphi}$ and for all pairs $(\tilde{t}', \tilde{\sigma}', \tilde{\imath}, \varphi)$, $\mathcal{S}(\Phi \wedge \varphi)$ implies that there exists an input i such that $\tilde{\imath} \sim i$, $t, \sigma \overset{i}{\rightarrow} t', \sigma'$ and $t', \sigma' \leftrightarrows_{M.[s \mapsto c]} \tilde{t}', \tilde{\sigma}', \Phi \wedge \varphi$ where where $SymOf(\tilde{\imath}) = s$ and $ValOf(i) = c$.

Lemma 6 (Soundness of normalisation). *For all concrete expressions e, concrete states σ, symbolic expressions $\tilde{e}$, symbolic states $\tilde{\sigma}$ path conditions Φ and mappings M, we have that $e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ implies that if $\tilde{e}, \tilde{\sigma} \Downarrow \overline{\tilde{t}, \tilde{\sigma}', \varphi}$, then for all pairs $(\tilde{t}, \tilde{\sigma}', \varphi)$ it holds that $\mathcal{S}(\Phi \wedge \varphi)$ implies that $e, \sigma \Downarrow t, \sigma'$ with $t, \sigma' \leftrightarrows_M \tilde{t}, \tilde{\sigma}', \Phi \wedge \varphi$.*

Lemma 7 (Soundness of striding). *for all concrete tasks t, concrete states σ, symbolic tasks $\tilde{t}$, symbolic states $\tilde{\sigma}$ path conditions Φ and mappings M, we have that $t, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ implies that if $\tilde{t}, \tilde{\sigma} \mapsto \overline{\tilde{t}', \tilde{\sigma}', \varphi}$, then for all pairs $(\tilde{t}', \tilde{\sigma}', \varphi)$ it holds that $\mathcal{S}(\Phi \wedge \varphi)$ implies that $t, \sigma \mapsto t', \sigma'$ with $t', \sigma' \leftrightarrows_M \tilde{t}', \tilde{\sigma}', \Phi \wedge \varphi$.*

Lemma 8 (Soundness of evaluation). *For all concrete expressions e, concrete states σ, symbolic expressions $\tilde{e}$, symbolic states $\tilde{\sigma}$ path conditions Φ and mappings M, we have that $e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ implies that if $\tilde{e}, \tilde{\sigma} \wr \overline{\tilde{v}, \tilde{\sigma}', \varphi}$, then for all pairs $(\tilde{v}, \tilde{\sigma}', \varphi)$ it holds that $\mathcal{S}(\Phi \wedge \varphi)$ implies that $e, \sigma \wr v, \sigma'$ with $v, \sigma' \leftrightarrows_M \tilde{v}, \tilde{\sigma'}, \Phi \wedge \varphi$.*

Proof (Soundness of handle).
We prove Lemma 5 by induction over $\tilde{t}$.

Case $\tilde{t} = \boxtimes\, \tau$
Since we have $t, \sigma \leftrightarrows_M \boxtimes\, \tau, \tilde{\sigma}, \Phi$, we know that t must be $\boxtimes\, \tau$ too, $\tilde{t}$ contains no symbols. There exists only one symbolic execution, namely $\dfrac{\text{fresh } \tilde{s}}{\boxtimes\, \tau, \tilde{\sigma} \rightsquigarrow \Box\, s, \tilde{\sigma}, s, \mathsf{True}}\ s : \tau$ (SH-Fill).
We need to show that there exists an i such that $s \sim i$ and $\Box\, v, \sigma \xrightarrow{i} t', \sigma'$.
Any concrete value c of type τ will do. Now we have to show that we end up with $\Box\, c, \sigma \leftrightarrows_{M.[s \mapsto c]} \Box\, s, \tilde{\sigma}, \Phi \wedge \mathsf{True}$, which holds trivially.

Case $\tilde{t} = \Box\, \tilde{v}$
Since we have $t, \sigma \leftrightarrows_M \Box\, \tilde{v}, \tilde{\sigma}, \Phi$, we know that either $\tilde{v}$ is a concrete value, or M contains a mapping such that $M\tilde{v}$ becomes a concrete value c. We know therefore that t must be $\Box\, c$.
There exists only one symbolic execution, namely $\dfrac{\text{fresh } s}{\Box\, \tilde{v}, \tilde{\sigma} \rightsquigarrow \Box\, s, \tilde{\sigma}, s, \mathsf{True}}\ \tilde{v}, s : \tau$ (SH-Change).
We need to show that there exists an i such that $s \sim i$ and $\Box\, c, \sigma \xrightarrow{i} t', \sigma'$.
Any concrete value c' of the same type as c will do. Now we have to show that we end up with $\Box\, c', \sigma \leftrightarrows_{M.[s \mapsto c']} \Box\, s, \tilde{\sigma}, \Phi \wedge \mathsf{True}$, which holds trivially.

Case $\tilde{t} = \blacksquare\, l$
Since we have $t, \sigma \leftrightarrows_M \blacksquare\, l, \tilde{\sigma}, \Phi$, we know that t must be $\blacksquare\, l$ too, $\tilde{t}$ contains no symbols. There exists only one symbolic execution, namely $\dfrac{\text{fresh } s}{\blacksquare\, l, \tilde{\sigma} \rightsquigarrow \blacksquare\, l, \tilde{\sigma}[l \mapsto s], s, \mathsf{True}}\ \sigma(l), s : \tau$ (SH-Update).
We need to show that there exists an i such that $s \sim i$ and $\blacksquare\, l, \sigma \xrightarrow{i} t', \sigma'$.
Any concrete value c of the same type as l will do. Now we have to show that we end up with $\blacksquare\, l, \sigma[l \mapsto c] \leftrightarrows_{M.[s \mapsto c]} \blacksquare\, l, \tilde{\sigma}[l \mapsto s], \Phi \wedge \mathsf{True}$, which holds trivially.

Case $\tilde{t} = \tilde{t}_1 \rhd \tilde{e}_2$
Since we have $t, \sigma \leftrightarrows_M \tilde{t}_1 \rhd \tilde{e}_2, \tilde{\sigma}, \Phi$, we know that $M\tilde{t}_1 \rhd \tilde{e}_2 = t$, which comes down to $t_1 \rhd e_2$ for some concrete t_1 and e_2.
In this case, three rules apply.

Case SH-Next
$$\dfrac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}, \varphi_1} \qquad \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma} \wr\!\wr \overline{\tilde{t}_2, \tilde{\sigma}_2', \varphi_2}}{\tilde{t}_1 \rhd \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \rhd \tilde{e}_2, \tilde{\sigma}_1', \tilde{\imath}, \varphi_1} \cup \overline{\tilde{t}_2, \tilde{\sigma}_2', \mathsf{C}, \varphi_2}}\ \mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \tilde{v}_1 \wedge \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}')$$
In this case, we have two sets of symbolic executions.

For all tuples $(\tilde{t}_1' \rhd \tilde{e}_2, \tilde{\sigma}_1', \tilde{\imath}, \varphi_1)$, we know by application of the induction hypothesis that there exits an i such that $\tilde{\imath} \sim i$, $t_1, \sigma \xrightarrow{i} t_1', \sigma'$ and $t_1', \sigma' \leftrightarrows_{M.[s\mapsto c]} \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$ where $ValOf(i) = c$ and $ValOf(\tilde{\imath}) = s$. Therefore we also have $t_1' \rhd e_2, \sigma_1' \leftrightarrows_{M.[s\mapsto c]} \tilde{t}_1' \rhd \tilde{e}_2, \tilde{\sigma}_1', \Phi \wedge \varphi_1$.

For all tuples $(\tilde{t}_2, \tilde{\sigma}_2', \mathrm{C}, \varphi_2)$, we first have by Lemma 9 that $v_1, \sigma \leftrightarrows_M \tilde{v}_1, \tilde{\sigma}, \Phi$. Now, before we can apply Lemma 6, we need to establish that $e_2\ v_1, \sigma \leftrightarrows_M \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma}, \Phi$ holds. This means that we have to show that $M\tilde{e}_2\ \tilde{v}_1 = e_2\ v_1$. Since application of the mapping is distributive, it suffices to show that $M\tilde{v}_1 = v_1$, which is given, and $M\tilde{e}_2 = e_2$, which follows from the premise as well.

At this point, by application of Lemma 6, we obtain that $e_2\ v_1, \sigma \Downarrow t_2, \sigma_2'$ and $t_1, \sigma_2' \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}_2', \Phi \wedge \varphi_2$

Case SH-PassNext
$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \tilde{\imath}, \varphi}}{\tilde{t}_1 \rhd \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \rhd \tilde{e}_2, \tilde{\sigma}', \tilde{\imath}, \varphi}}\ \mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \bot$$

For all tuples $(\tilde{t}_1' \rhd \tilde{e}_2, \tilde{\sigma}_1', \tilde{\imath}, \varphi_1)$, we know by application of the induction hypothesis that there exits an i such that $\tilde{\imath} \sim i$, $t_1, \sigma \xrightarrow{i} t_1', \sigma'$ and $t_1', \sigma' \leftrightarrows_{M.[s\mapsto c]} \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$ where $ValOf(i) = c$ and $ValOf(\tilde{\imath}) = s$. Therefore we also have $t_1' \rhd e_2, \sigma_1' \leftrightarrows_{M.[s\mapsto c]} \tilde{t}_1' \rhd \tilde{e}_2, \tilde{\sigma}_1', \Phi \wedge \varphi_1$.

Case SH-PassNextFail
$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}, \varphi} \qquad \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma} \Downarrow \overline{\tilde{t}_2, \tilde{\sigma}_2', \_}}{\tilde{t}_1 \rhd \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \rhd \tilde{e}_2, \tilde{\sigma}_1', \tilde{\imath}, \varphi}}\ \mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \tilde{v}_1 \wedge \mathcal{F}(\tilde{t}_2, \tilde{\sigma}_2')$$

For all tuples $(\tilde{t}_1' \rhd \tilde{e}_2, \tilde{\sigma}_1', \tilde{\imath}, \varphi_1)$, we know by application of the induction hypothesis that there exits an i such that $\tilde{\imath} \sim i$, $t_1, \sigma \xrightarrow{i} t_1', \sigma'$ and $t_1', \sigma' \leftrightarrows_{M.[s\mapsto c]} \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$ where $ValOf(i) = c$ and $ValOf(\tilde{\imath}) = s$. Therefore we also have $t_1' \rhd e_2, \sigma_1' \leftrightarrows_{M.[s\mapsto c]} \tilde{t}_1' \rhd \tilde{e}_2, \tilde{\sigma}_1', \Phi \wedge \varphi_1$.

Case $\tilde{t} = \tilde{t}_1 \blacktriangleright \tilde{e}_2$

One rule applies, namely SH-PassThen
$$\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \tilde{\imath}, \varphi}}{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \tilde{\imath}, \varphi}}$$
For all tuples $(\tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \tilde{\imath}, \varphi)$, we know by application of the induction hypothesis that there exists an i such that $\tilde{\imath} \sim i$, $t_1, \sigma \xrightarrow{1} t_1', \sigma'$ and $t_1', \sigma' \leftrightarrows_{M.[s\mapsto c]} \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$ where $ValOf(i) = c$ and $SymOf(\tilde{\imath}) = s$. Therefore we also have $t_1' \blacktriangleright e_2, \sigma_1' \leftrightarrows_{M.[s\mapsto c]} \tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}_1', \Phi \wedge \varphi_1, M.[s \mapsto c])$.

Case $\tilde{t} = \tilde{e}_1 \lozenge \tilde{e}_2$

In this case, three rules apply.

Case SH-Pick
$$\frac{\tilde{e}_1, \tilde{\sigma} \Downarrow \overline{\tilde{t}_1, \tilde{\sigma}_1, \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma} \Downarrow \overline{\tilde{t}_2, \tilde{\sigma}_2, \varphi_2}}{\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1, \tilde{\sigma}_1, \mathsf{L}, \varphi_1} \cup \overline{\tilde{t}_2, \tilde{\sigma}_2, \mathsf{R}, \varphi_2}}\ \neg\mathcal{F}(\tilde{t}_1, \tilde{\sigma}_1) \wedge \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}_2)$$

In this case, we have two sets of symbolic executions.

For all tuples $(\tilde{t}_1, \tilde{\sigma}_1, \mathsf{L}, \varphi_1)$, we obtain from Lemma 6 that $e_1, \sigma \Downarrow t_1, \sigma_1$ with $t_1, \sigma_1 \leftrightarrows_M \tilde{t}_1, \tilde{\sigma}_1, \Phi \land \varphi_1$.

For all tuples $(\tilde{t}_2, \tilde{\sigma}_2, \mathsf{R}, \varphi_2)$, we obtain from Lemma 6 that $e_2, \sigma \Downarrow t_2, \sigma_2$ with $t_2, \sigma_2 \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}_2, \Phi \land \varphi_2$.

Case
$$\textsc{SH-PickLeft}\;\frac{\tilde{e}_1, \tilde{\sigma} \Downarrow \overline{\tilde{t}_1, \tilde{\sigma}_1, \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma} \Downarrow \overline{\tilde{t}_2, \tilde{\sigma}_2, \varphi_2}}{\tilde{e}_1 \Diamond \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{t}_1, \tilde{\sigma}_1, \mathsf{L}, \varphi_1}\; \neg\mathcal{F}(\tilde{t}_1, \tilde{\sigma}_1) \land \mathcal{F}(\tilde{t}_2, \tilde{\sigma}_2)$$

For all tuples $(\tilde{t}_1, \tilde{\sigma}_1, \mathsf{L}, \varphi_1)$, we obtain from Lemma 6 that $e_1, \sigma \Downarrow t_1, \sigma_1$ with $t_1, \sigma_1 \leftrightarrows_M \tilde{t}_1, \tilde{\sigma}_1, \Phi \land \varphi_1$.

Case
$$\textsc{SH-PickRight}\;\frac{\tilde{e}_1, \tilde{\sigma} \Downarrow \overline{\tilde{t}_1, \tilde{\sigma}_1, \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma} \Downarrow \overline{\tilde{t}_2, \tilde{\sigma}_2, \varphi_2}}{\tilde{e}_1 \Diamond \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{t}_2, \tilde{\sigma}_2, \mathsf{R}, \varphi_2}\; \mathcal{F}(\tilde{t}_1, \tilde{\sigma}_1) \land \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}_2)$$

For all tuples $(\tilde{t}_2, \tilde{\sigma}_2, \mathsf{R}, \varphi_2)$, we obtain from Lemma 6 that $e_2, \sigma \Downarrow t_2, \sigma_2$ with $t_2, \sigma_2 \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}_2, \Phi \land \varphi_2$.

Case $\tilde{t} = \tilde{t}_1 \bowtie \tilde{t}_2$

In this case, one rule applies.
$$\textsc{SH-And}\;\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_1, \tilde{\sigma}'_1, \tilde{\imath}_1, \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_2, \tilde{\sigma}'_2, \tilde{\imath}_2, \varphi_2}}{\tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\overline{\tilde{t}'_1 \bowtie \tilde{t}_2, \tilde{\sigma}'_1, \mathsf{F}\,\tilde{\imath}_1, \varphi_1} \cup \overline{\tilde{t}_1 \bowtie \tilde{t}'_2, \tilde{\sigma}''_2, \mathsf{S}\,\tilde{\imath}_2, \varphi_2}}}$$

In this case, we have two sets of symbolic executions.

For all tuples $(\tilde{t}'_1 \bowtie \tilde{t}_2, \tilde{\sigma}'_1, \mathsf{F}\,\tilde{\imath}_1, \varphi_1)$, we know by application of the induction hypothesis that there exists an i such that $\tilde{\imath}_1 \sim i$, $t_1, \sigma \xrightarrow{i} t'_1, \sigma'_1$ and $t'_1, \sigma'_1 \leftrightarrows_{M.[s \mapsto c]} \tilde{t}'_1, \tilde{\sigma}'_1, \Phi \land \varphi_1$. Then by H-FirstAnd, we know that also $t_1 \bowtie t_2, \sigma \xrightarrow{\mathsf{F}\,i} t'_1 \bowtie t_2, \sigma'_1$. It follows trivially that $t'_1 \bowtie t_2, \sigma'_1 \leftrightarrows_{M.[s \mapsto c]} \tilde{t}'_1 \bowtie \tilde{t}_2, \tilde{\sigma}'_1, \Phi \land \varphi_1$.

For all tuples $(\tilde{t}_1 \bowtie \tilde{t}'_2, \tilde{\sigma}'_2, \mathsf{S}\,\tilde{\imath}_2, \varphi_2)$, we know by application of the induction hypothesis that there exists an i such that $\tilde{\imath}_2 \sim i$, $t_2, \sigma \xrightarrow{i} t'_2, \sigma'_2$ and $t'_2, \sigma'_2 \leftrightarrows_{M.[s \mapsto c]} \tilde{t}'_2, \tilde{\sigma}'_2, \Phi \land \varphi_2$. Then by H-SecondAnd, we know that also $t_1 \bowtie t_2, \sigma \xrightarrow{\mathsf{S}\,i} t_1 \bowtie t'_2, \sigma'_2$. It follows trivially that $t_1 \bowtie t'_2, \sigma'_2 \leftrightarrows_{M.[s \mapsto c]} \tilde{t}_1 \bowtie \tilde{t}'_2, \tilde{\sigma}'_2, \Phi \land \varphi_2$.

Case $\tilde{t} = \tilde{e}_1 \blacklozenge \tilde{e}_2$

One rule applies, namely
$$\textsc{SH-Or}\;\frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_1, \tilde{\sigma}'_1, \tilde{\imath}_1, \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_2, \tilde{\sigma}'_2, \tilde{\imath}_2, \varphi_2}}{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\overline{\tilde{t}'_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}'_1, \mathsf{F}\,\tilde{\imath}_1, \varphi_1} \cup \overline{\tilde{t}_1 \blacklozenge \tilde{t}'_2, \tilde{\sigma}'_2, \mathsf{S}\,\tilde{\imath}_2, \varphi_2}}}$$

In this case, we have two sets of symbolic executions.

For all tuples $(\tilde{t}'_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}'_1, \mathsf{F}\,\tilde{\imath}_1, \varphi_1)$, we know by application of the induction hypothesis that there exists an i such that $\tilde{\imath}_1 \sim i$, $t_1, \sigma \xrightarrow{i} t'_1, \sigma'_1$ and $t'_1, \sigma'_1 \leftrightarrows_{M.[s \mapsto c]} \tilde{t}'_1, \tilde{\sigma}'_1, \Phi \land \varphi_1$. Then by H-FirstOr, we know that also $t_1 \blacklozenge t_2, \sigma \xrightarrow{\mathsf{F}\,i} t'_1 \blacklozenge t_2, \sigma'_1$. It follows trivially that $t'_1 \blacklozenge t_2, \sigma'_1 \leftrightarrows_{M.[s \mapsto c]} \tilde{t}'_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}'_1, \Phi \land \varphi_1$.

For all tuples $(\tilde{t}_1 \blacklozenge \tilde{t}'_2, \tilde{\sigma}'_2, \mathrm{S}\,\tilde{\imath}_2, \varphi_2)$, we know by application of the induction hypothesis that there exists an i such that $\tilde{\imath}_2 \sim i$, $t_2, \sigma \xrightarrow{i} t'_2, \sigma'_2$ and $t'_2, \sigma'_2 \leftrightarrows_{M.[s\mapsto c]} \tilde{t}'_2, \tilde{\sigma}'_2, \Phi \wedge \varphi_2$. Then by H-SecondOr, we know that also $t_1 \blacklozenge t_2, \sigma \xrightarrow{\mathrm{S}\,i} t_1 \blacklozenge t'_2, \sigma'_2$. It follows trivially that $t_1 \blacklozenge t'_2, \sigma'_2 \leftrightarrows_{M.[s\mapsto c]} \tilde{t}_1 \blacklozenge \tilde{t}'_2, \tilde{\sigma}'_2, \Phi \wedge \varphi_2$.

Lemma 9 ($\mathcal{V}$ preserves consistence). *For all concrete tasks t, concrete states σ, symbolic tasks $\tilde{t}$, symbolic states $\tilde{\sigma}$, path conditions Φ and mappings $M = [s_1 \mapsto c_1 \cdots s_n \mapsto c_n]$, if $t, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\mathcal{V}(t,\sigma) = v$ and $\mathcal{V}(\tilde{t}, \tilde{\sigma})$, then also $v, \sigma \leftrightarrows_M \tilde{v}, \tilde{\sigma}, \Phi$*

Proof ($\mathcal{V}$ preserves consistence).

Case $\tilde{t} = \square\, s$

If we have $t, \sigma \leftrightarrows_M \square\, s, \tilde{\sigma}, \Phi$, then we know that t must be $\square\, c$ for some concrete value of the same type as s.

Then by definition of $\mathcal{V}$, we have $\mathcal{V}(\square\, c, \sigma) = c$ and $\mathcal{V}(\square\, s, \tilde{\sigma}) = s$. Since we have $M(\square\, s) = \square\, c$ from the premise, we know that $Ms = c$, since mapping propagates. Therefore $c, \sigma \leftrightarrows_M s, \tilde{\sigma}, \Phi$.

Case $\tilde{t} = \boxtimes\, \tau$

If we have $t, \sigma \leftrightarrows_M \boxtimes\, \tau, \tilde{\sigma}, \Phi$, then we know that t is also $\boxtimes\, \tau$.

By definition of $\mathcal{V}$, $\mathcal{V}(\boxtimes\, \tau, \sigma) = \bot$ and $\mathcal{V}(\boxtimes\, \tau, \tilde{\sigma}) = \bot$, so this case holds trivially.

Case $\tilde{t} = \blacksquare\, l$

If we have $t, \sigma \leftrightarrows_M \blacksquare\, l, \tilde{\sigma}, \Phi$, then we know that t is also $\blacksquare\, l$.

By definition of $\mathcal{V}$, $\mathcal{V}(\blacksquare\, l, \sigma) = \sigma(l)$ and $\mathcal{V}(\blacksquare\, l, \tilde{\sigma}) = \tilde{\sigma}(l)$.

We now need to show that $M(\tilde{\sigma}(l)) = \sigma(l)$. From the premise we know that $M\tilde{\sigma} = \sigma$, from which this immediately follows.

Case $\tilde{t} = \lightning$

If we have $t, \sigma \leftrightarrows_M \lightning, \tilde{\sigma}, \Phi$, then we know that t is also $\lightning$.

By definition of $\mathcal{V}$, $\mathcal{V}(\lightning, \sigma) = \bot$ and $\mathcal{V}(\lightning, \tilde{\sigma}) = \bot$, so we know that this case holds trivially.

Case $\tilde{t} = \tilde{t}_1 \blacktriangleright \tilde{e}_2$

If we have $t, \sigma \leftrightarrows_M \tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}, \Phi$, then we know that t is $t_1 \blacktriangleright e_2$.

By definition of $\mathcal{V}$, $\mathcal{V}(t_1 \blacktriangleright e_2, \sigma) = \bot$ and $\mathcal{V}(\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}) = \bot$, so we know that this case holds trivially.

Case $\tilde{t} = \tilde{t}_1 \triangleright \tilde{e}_2$

If we have $t, \sigma \leftrightarrows_M \tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma}, \Phi$, then we know that t is $t_1 \triangleright e_2$.

By definition of $\mathcal{V}$, $\mathcal{V}(t_1 \triangleright e_2, \sigma) = \sigma(l)$ and $\mathcal{V}(\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma}) = \bot$, so we know that this case holds trivially.

Case $\tilde{t} = \tilde{t}_1 \bowtie \tilde{t}_2$

If we have $t, \sigma \leftrightarrows_M \tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma}, \Phi$, then we know that t is also $t_1 \bowtie t_2$.

By definition of $\mathcal{V}$, we can find ourselves in one of two cases.

If $\mathcal{V}(\tilde{t}_1, \sigma) = \tilde{v}_1$ and $\mathcal{V}(\tilde{t}_2, \sigma) = \tilde{v}_2$, then $\mathcal{V}(t_1 \bowtie t_2, \sigma) = \langle v_1, v_2\rangle$ and $\mathcal{V}(\tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma}) = \langle \tilde{v}_1, \tilde{v}_2\rangle$. This case follows from the induction hypothesis.

Otherwise, if either one of the two branches returns $\perp$, we have that $\mathcal{V}(t_1 \bowtie t_2, \sigma) = \perp$ and $\mathcal{V}(\tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma}) = \perp$, so we know that this case holds trivially

Case $\tilde{t} = \tilde{t}_1 \blacklozenge \tilde{t}_2$

If we have $t, \sigma \leftrightarrows_M \tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}, \Phi$, then we know that t is also $t_1 \blacklozenge t_2$.

By definition of $\mathcal{V}$, we find ourselves in one of three cases.

If $\mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \tilde{v}_1$, then $\mathcal{V}(\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}) = \tilde{v}_1$ and $\mathcal{V}(t_1 \blacklozenge t_2, \sigma) = v_1$. This case follows from the induction hypothesis.

Otherwise, if $\mathcal{V}(\tilde{t}_2, \tilde{\sigma}) = \tilde{v}_2$, then $\mathcal{V}(\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}) = \tilde{v}_2$ and $\mathcal{V}(t_1 \blacklozenge t_2, \sigma) = v_2$. This case follows from the induction hypothesis.

Otherwise, if either one of the two branches returns $\perp$, we have that $\mathcal{V}(t_1 \blacklozenge t_2, \sigma) = \perp$ and $\mathcal{V}(\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}) = \perp$, so we know that this case holds trivially.

Case $\tilde{t} = \tilde{t}_1 \lozenge \tilde{t}_2$

If we have $t, \sigma \leftrightarrows_M \tilde{t}_1 \lozenge \tilde{t}_2, \tilde{\sigma}, \Phi$, then we know that t is $t_1 \lozenge t_2$.

By definition of $\mathcal{V}$, $\mathcal{V}(t_1 \lozenge t_2, \sigma) = \perp$ and $\mathcal{V}(\tilde{t}_1 \lozenge \tilde{t}_2, \tilde{\sigma}) = \perp$, so we know that this case holds trivially.

Proof (Soundness of normalise). We prove Lemma 6 by induction over $\tilde{e}$.

From the premise, we can assume that $e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$. Now, given that $\tilde{e}, \sigma e \; \wr\!\wr \; \overline{\tilde{t}, \tilde{\sigma}', \varphi}$, we need to demonstrate that for all pairs $(\tilde{t}, \tilde{\sigma}', \varphi)$, $\mathcal{S}(\Phi \wedge \varphi)$ implies that $e, \sigma \Downarrow t, \sigma'$ with $t, \sigma' \leftrightarrows_M \tilde{t}, \tilde{\sigma}', \Phi \wedge \varphi$.

The base case is when the SN-Done rule applies.

$$\textsc{SN-Done}\quad \frac{\tilde{e}, \tilde{\sigma} \; \wr \; \overline{\tilde{t}, \tilde{\sigma}', \varphi_1} \qquad \tilde{t}, \tilde{\sigma}' \rightsquigarrow \overline{\tilde{t}', \tilde{\sigma}'', \varphi_2}}{\tilde{e}, \tilde{\sigma} \; \wr\!\wr \; \overline{\tilde{t}, \tilde{\sigma}', \varphi_1}} \; \tilde{\sigma}' = \tilde{\sigma}'' \wedge \tilde{t} = \tilde{t}'$$

In this case, we obtain from Lemma 8 that $e, \sigma \Downarrow t, \sigma'$ with $t, \sigma' \leftrightarrows_M \tilde{t}, \tilde{\sigma}', \Phi \wedge \varphi$, which is exactly what we needed to show.

The only induction step is when

$$\textsc{SN-Repeat}\quad \frac{\tilde{e}, \tilde{\sigma} \; \wr \; \overline{\tilde{t}, \tilde{\sigma}', \varphi_1} \qquad \tilde{t}, \tilde{\sigma}' \rightsquigarrow \overline{\tilde{t}', \tilde{\sigma}'', \varphi_2} \qquad \tilde{t}', \tilde{\sigma}'' \; \wr\!\wr \; \overline{\tilde{t}'', \tilde{\sigma}''', \varphi_3}}{\tilde{e}, \tilde{\sigma} \; \wr\!\wr \; \overline{\tilde{t}'', \tilde{\sigma}''', \varphi_1 \wedge \varphi_2 \wedge \varphi_3}} \; \tilde{\sigma}' \neq \tilde{\sigma}'' \vee \tilde{t} \neq \tilde{t}'$$

applies.

In this case, we obtain from Lemma 8 that $e, \sigma \Downarrow t, \sigma'$ with $t, \sigma' \leftrightarrows_M \tilde{t}, \tilde{\sigma}', \Phi \wedge \varphi_1$, which is exactly what we needed to show. Furthermore, by Lemma 7 we obtain that $t, \sigma' \mapsto t', \sigma''$ with $t', \sigma'' \leftrightarrows_M \tilde{t}', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. Then finally, by application of the induction hypothesis, we obtain what we needed to prove. $t', \sigma'' \Downarrow t'', \sigma'''$ with $t'', \sigma''' \leftrightarrows_M \tilde{t}'', \tilde{\sigma}''', \Phi \wedge \varphi_1 \wedge \varphi_2 \wedge \varphi_3$.

Proof (Soundness of stride).

Provided that $t, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\tilde{t}, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}', \tilde{\sigma}', \varphi}$, we want to show that for all pairs $(\tilde{t}', \tilde{\sigma}', \varphi)$, we have $\mathcal{S}(\Phi \wedge \varphi)$ implies that $t, \sigma \mapsto t', \sigma'$ We prove Lemma 7 by induction over t.

Case $\tilde{t} = \square\, \tilde{v}$

$$\frac{\text{SS-Edit}}{\square\, \tilde{v}, \tilde{\sigma} \rightsquigarrow \square\, \tilde{v}, \tilde{\sigma}, \mathsf{True}}$$

One rule applies, namely $\square\, \tilde{v}, \tilde{\sigma} \rightsquigarrow \square\, \tilde{v}, \tilde{\sigma}, \mathsf{True}$
Given that $t, \sigma \leftrightarrows_M \square\, \tilde{v}, \tilde{\sigma}, \Phi$ and $\square\, \tilde{v}, \tilde{\sigma} \rightsquigarrow \square\, \tilde{v}, \tilde{\sigma}, \mathsf{True}$, we know that $t = \square\, M\tilde{v}$, and we have $\square\, M\tilde{v}, \sigma \mapsto \square\, M\tilde{v}, \sigma$ by S-Edit and $\square\, M\tilde{v}, \sigma \leftrightarrows_M \square\, \tilde{v}, \tilde{\sigma}, \Phi$, since none of the tasks and states were altered.

Case $t = \boxtimes\, \tau$

$$\frac{\text{SS-Fill}}{\boxtimes\, \tau, \tilde{\sigma} \rightsquigarrow \boxtimes\, \tau, \tilde{\sigma}, \mathsf{True}}$$

One rule applies, namely $\boxtimes\, \tau, \tilde{\sigma} \rightsquigarrow \boxtimes\, \tau, \tilde{\sigma}, \mathsf{True}$
Given that $t, \sigma \leftrightarrows_M \boxtimes\, \tau, \tilde{\sigma}, \Phi$ and $\boxtimes\, \tau, \tilde{\sigma} \rightsquigarrow \boxtimes\, \tau, \tilde{\sigma}, \mathsf{True}$, we know that $t = \boxtimes\, \tau$, and we have $\boxtimes\, \tau, \sigma \mapsto \boxtimes\, \tau, \sigma$ by S-Fill and $\boxtimes\, \tau, \sigma \leftrightarrows_M \square\, \tilde{v}, \tilde{\sigma}, \Phi$, since none of the tasks and states were altered.

Case $t = \blacksquare\, l$

$$\frac{\text{SS-Update}}{\blacksquare\, l, \tilde{\sigma} \rightsquigarrow \blacksquare\, l, \tilde{\sigma}, \mathsf{True}}$$

One rule applies, namely $\blacksquare\, l, \tilde{\sigma} \rightsquigarrow \blacksquare\, l, \tilde{\sigma}, \mathsf{True}$
Given that $t, \sigma \leftrightarrows_M \blacksquare\, l, \tilde{\sigma}, \Phi$ and $\blacksquare\, l, \tilde{\sigma} \rightsquigarrow \blacksquare\, l, \tilde{\sigma}, \mathsf{True}$, we know that $t = \blacksquare\, l$, and we have $\blacksquare\, l, \sigma \mapsto \blacksquare\, l, \sigma$ by S-Update and $\blacksquare\, l, \sigma \leftrightarrows_M \blacksquare\, l, \tilde{\sigma}, \Phi$, since none of the tasks and states were altered.

Case $t = \lightning$

$$\frac{\text{SS-Fail}}{\lightning, \tilde{\sigma} \rightsquigarrow \lightning, \tilde{\sigma}, \mathsf{True}}$$

One rule applies, namely $\lightning, \tilde{\sigma} \rightsquigarrow \lightning, \tilde{\sigma}, \mathsf{True}$
Given that $t, \sigma \leftrightarrows_M \lightning, \tilde{\sigma}, \Phi$ and $\lightning, \tilde{\sigma} \rightsquigarrow \lightning, \tilde{\sigma}, \mathsf{True}$, we know that $t = \lightning$, and we have $\lightning, \sigma \mapsto \lightning, \sigma$ by S-Fail and $\lightning, \sigma \leftrightarrows_M \lightning, \tilde{\sigma}, \Phi$, since none of the tasks and states were altered.

Case $t = \tilde{e}_1 \lozenge \tilde{e}_2$

$$\frac{\text{SS-Xor}}{\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}, \mathsf{True}}$$

One rule applies, namely $\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}, \mathsf{True}$
Given that $t, \sigma \leftrightarrows_M \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}, \mathsf{True}$, we know that $t = M\tilde{e}_1 \lozenge M\tilde{e}_2$, and we have $M\tilde{e}_1 \lozenge M\tilde{e}_2, \sigma \mapsto M\tilde{e}_1 \lozenge M\tilde{e}_2, \sigma$ by S-Xor and $M\tilde{e}_1 \lozenge M\tilde{e}_2, \sigma \leftrightarrows_M \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}, \Phi$, since none of the tasks and states were altered.

Case $\tilde{t} = \tilde{t}_1 \blacktriangleright \tilde{e}_2$

Three rules apply.

Case
$$\text{SS-ThenStay}\ \frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \varphi}}{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi}}\ \mathcal{V}(\tilde{t}_1', \tilde{\sigma}') = \bot$$

Provided that $t, \sigma \leftrightarrows_M \tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{t}'_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi_1$, we obtain from the induction hypothesis that $t_1, \sigma \mapsto t'_1, \sigma'$ and $t'_1, \sigma' \leftrightarrows_M \tilde{t}'_1, \tilde{\sigma}', \Phi$. From this, we can directly conclude that $t_1 \blacktriangleright e_2, \sigma \mapsto t'_1 \blacktriangleright e_2, \sigma'$ and $t'_1 \blacktriangleright e_2, \sigma' \leftrightarrows_M \tilde{t}'_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \Phi$.

Case

$$\textsc{SS-ThenFail}\ \frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_1, \tilde{\sigma}', \varphi} \qquad \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma}' \wr \overline{\tilde{t}_2, \tilde{\sigma}'', \_}}{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi}}\ \mathcal{V}(\tilde{t}'_1, \tilde{\sigma}') = \tilde{v}_1 \wedge \mathcal{F}(\tilde{t}_2, \tilde{\sigma}'')$$

Provided that $t, \sigma \leftrightarrows_M \tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{t}'_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi_1$, we obtain from the induction hypothesis that $t_1, \sigma \mapsto t'_1, \sigma'$ and $t'_1, \sigma' \leftrightarrows_M \tilde{t}'_1, \tilde{\sigma}', \Phi$. From this, we can directly conclude that $t_1 \blacktriangleright e_2, \sigma \mapsto t'_1 \blacktriangleright e_2, \sigma'$ and $t'_1 \blacktriangleright e_2, \sigma' \leftrightarrows_M \tilde{t}'_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \Phi$.

Case

$$\textsc{SS-ThenCont}\ \frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_1, \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma}' \wr \overline{\tilde{t}_2, \tilde{\sigma}'', \varphi_2}}{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{t_2, \sigma'', \varphi_1 \wedge \varphi_2}}\ \mathcal{V}(\tilde{t}'_1, \tilde{\sigma}') = \tilde{v}_1 \wedge \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}'')$$

Provided that $t, \sigma \leftrightarrows_M \tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{t}_2, \tilde{\sigma}', \varphi_1 \wedge \varphi_2$ with $\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \tilde{t}'_1, \tilde{\sigma}', \varphi_1$ and $\mathcal{V}(\tilde{t}'_1, \tilde{\sigma}') = \tilde{v}_1$, we obtain from the induction hypothesis that $t_1, \sigma \mapsto t'_1, \sigma'$ and $t'_1, \sigma' \leftrightarrows_M \tilde{t}'_1, \tilde{\sigma}', \Phi$. Then from the consistence relation, we can conclude that $\mathcal{V}(t'_1, \sigma') = \mathcal{V}(Mt'_1, M\sigma') = M\tilde{v}_1$.

At this point, we have $e_2 M\tilde{v}_1, \sigma' \leftrightarrows_M \tilde{e}_2\tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$ and $\tilde{e}_2\tilde{v}_1, \tilde{\sigma}' \wr \tilde{t}_2, \tilde{sigma}'', \varphi_2$. This allows us to apply Lemma 8 to obtain $e_2(M\tilde{v}_1), \sigma' \downarrow t_2, \sigma''$ and $t_2, \sigma'' \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

From this, we can directly conclude that $t_1 \blacktriangleright e_2, \sigma \mapsto t_2, \sigma''$ and $t_2, \sigma'' \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $\tilde{t} = \tilde{t}_1 \blacklozenge \tilde{t}_2$

One of three rules applies.

Case

$$\textsc{SS-OrLeft}\ \frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_1, \tilde{\sigma}', \varphi}}{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_1, \tilde{\sigma}', \varphi}}\ \mathcal{V}(\tilde{t}'_1, \tilde{\sigma}') = \tilde{v}_1$$

Provided that $t, \sigma \leftrightarrows_M \tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}, \Phi$ and $\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \tilde{t}'_1, \tilde{\sigma}', \varphi$, we obtain from the induction hypothesis that $t_1, \sigma \mapsto t'_1, \sigma'$ and $t'_1, \sigma' \leftrightarrows_M \tilde{t}'_1, \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can directly conclude that $t_1 \blacklozenge t_2, \sigma \mapsto t'_1, \sigma'$.

Case

$$\textsc{SS-OrRight}\ \frac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_1, \tilde{\sigma}', \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma}' \rightsquigarrow \overline{\tilde{t}'_2, \tilde{\sigma}'', \varphi_2}}{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}}\ \mathcal{V}(\tilde{t}'_1, \tilde{\sigma}') = \bot \wedge \mathcal{V}(\tilde{t}'_2, \tilde{\sigma}'') = \tilde{v}_2$$

Provided that $t, \sigma \leftrightarrows_M \tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}, \Phi$ and $\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \tilde{t}'_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2$, we obtain from the induction hypothesis that $t_1, \sigma \mapsto t'_1, \sigma'$ and $t'_1, \sigma' \leftrightarrows_M \tilde{t}'_1, \tilde{\sigma}', \Phi \wedge \varphi_1$. Then by a second application of the induction hypothesis, we obtain that $t_2, \sigma' \mapsto t'_2, \sigma''$ and $t'_2, \sigma'' \leftrightarrows_M \tilde{t}'_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. This leads us to conclude $t_1 \blacklozenge t_2, \sigma \mapsto t'_2, \sigma''$.

Case
$$\text{SS-OrNone}\quad \frac{\tilde{t}_1, \tilde{\sigma} \;\mapsto\!\!\!\!\!\rightsquigarrow\; \overline{\tilde{t}'_1, \tilde{\sigma}', \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma}' \;\mapsto\!\!\!\!\!\rightsquigarrow\; \overline{\tilde{t}'_2, \tilde{\sigma}'', \varphi_2}}{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \;\mapsto\!\!\!\!\!\rightsquigarrow\; \overline{\tilde{t}'_1 \blacklozenge \tilde{t}'_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}}\ \mathcal{V}(\tilde{t}'_1, \tilde{\sigma}') = \bot \wedge \mathcal{V}(\tilde{t}'_2, \tilde{\sigma}'') = \bot$$

Provided that $t, \sigma \leftrightarrows_M \tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}, \Phi$ and $\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \;\mapsto\!\!\!\!\!\rightsquigarrow\; \tilde{t}'_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2$, we obtain from the induction hypothesis that $t_1, \sigma \;\mapsto\; t'_1, \sigma'$ and $t'_1, \sigma' \leftrightarrows_M \tilde{t}'_1, \tilde{\sigma}', \Phi \wedge \varphi_1$. Then by a second application of the induction hypothesis, we obtain that $t_2, \sigma' \;\mapsto\; t'_2, \sigma''$ and $t'_2, \sigma'' \leftrightarrows_M \tilde{t}'_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. This leads us to conclude $t_1 \blacklozenge t_2, \sigma \;\mapsto\; t'_1 \blacklozenge t'_2, \sigma''$ and $t'_1 \blacklozenge t'_2, \sigma'' \leftrightarrows_M \tilde{t}'_1 \blacklozenge \tilde{t}'_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $\tilde{t} = \tilde{t}_1 \triangleright \tilde{e}_2$

One rule applies, namely
$$\text{SS-Next}\quad \frac{\tilde{t}_1, \tilde{\sigma} \;\mapsto\!\!\!\!\!\rightsquigarrow\; \overline{\tilde{t}'_1, \tilde{\sigma}', \varphi}}{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \;\mapsto\!\!\!\!\!\rightsquigarrow\; \overline{\tilde{t}'_1 \triangleright \tilde{e}_2, \tilde{\sigma}', \varphi}}$$

Provided that $t, \sigma \leftrightarrows_M \tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \;\mapsto\!\!\!\!\!\rightsquigarrow\; \tilde{t}'_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi$, we obtain from the induction hypothesis that $t_1, \sigma \;\mapsto\; t'_1, \sigma'$ and $t'_1, \sigma' \leftrightarrows_M \tilde{t}'_1, \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can directly conclude that $t_1 \triangleright e_2, \sigma \;\mapsto\; t'_1 \triangleright e_2, \sigma'$ and $t'_1 \triangleright e_2, \sigma' \leftrightarrows_M \tilde{t}'_1 \triangleright \tilde{e}_2, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $\tilde{t} = \tilde{t}_1 \bowtie \tilde{t}_2$

One rule applies, namely
$$\text{SS-And}\quad \frac{\tilde{t}_1, \tilde{\sigma} \;\mapsto\!\!\!\!\!\rightsquigarrow\; \overline{\tilde{t}'_1, \tilde{\sigma}', \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma}' \;\mapsto\!\!\!\!\!\rightsquigarrow\; \overline{\tilde{t}'_2, \tilde{\sigma}'', \varphi_2}}{\tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma} \;\mapsto\!\!\!\!\!\rightsquigarrow\; \overline{\tilde{t}'_1 \bowtie \tilde{t}'_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}}$$

Provided that $t, \sigma \leftrightarrows_M \tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma}, \Phi$ and $\tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma} \;\mapsto\!\!\!\!\!\rightsquigarrow\; \tilde{t}'_1 \bowtie \tilde{t}'_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2$, we obtain from the induction hypothesis that $t_1, \sigma \;\mapsto\; t'_1, \sigma'$ and $t'_1, \sigma' \leftrightarrows_M \tilde{t}'_1, \tilde{\sigma}', \Phi \wedge \varphi_1$. Then by a second application of the induction hypothesis, we obtain that $t_2, \sigma' \;\mapsto\; t'_2, \sigma''$ and $t'_2, \sigma'' \leftrightarrows_M \tilde{t}'_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. This leads us to conclude $t_1 \bowtie t_2, \sigma \;\mapsto\; t'_1 \bowtie t'_2, \sigma''$ and $t'_1 \bowtie t'_2, \sigma'' \leftrightarrows_M \tilde{t}'_1 \bowtie \tilde{t}'_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Proof (Soundness of evaluate).
We prove Lemma 8 by induction over $\tilde{e}$.

Case $\tilde{e} = \tilde{v}$

One rule applies, namely
$$\text{SE-Value}\quad \frac{}{\tilde{v}, \tilde{\sigma} \;\wr\; \tilde{v}, \tilde{\sigma}, \mathsf{True}}$$

We assume $e, \sigma \leftrightarrows_M \tilde{v}, \tilde{\sigma}, \Phi$ and $\tilde{v}, \tilde{\sigma} \;\wr\; \tilde{v}, \tilde{\sigma}, \mathsf{True}$. By E-Value we have $v, \sigma \downarrow v, \sigma$, so this case holds trivially.

Case $\tilde{e} = \langle \tilde{e}_1, \tilde{e}_2 \rangle$

One rule applies, namely
$$\text{SE-Pair}\quad \frac{\tilde{e}_1, \tilde{\sigma} \;\wr\; \overline{\tilde{v}_1, \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \;\wr\; \overline{\tilde{v}_2, \tilde{\sigma}'', \varphi_2}}{\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \;\wr\; \overline{\langle \tilde{v}_1, \tilde{v}_2 \rangle, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}}$$

Provided that $e, \sigma \leftrightarrows_m \langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma}, \Phi$ and $\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \;\wr\; \langle \tilde{v}_1, \tilde{v}_2 \rangle, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2$, we obtain from the induction hypothesis that $e_1, \sigma \downarrow v_1, \sigma'$ with $v_1, \sigma' \leftrightarrows_m \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$.

Then by a second application of the induction hypothesis, we obtain that $e_2, \sigma' \downarrow v_2, \sigma''$ with $v_2, \sigma'' \leftrightarrows_m \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. From this, we can conclude that $\langle e_1, e_2 \rangle, \sigma \downarrow \langle v_1, v_2 \rangle, \sigma''$ with $\langle v_1, v_2 \rangle, \sigma'' \leftrightarrows_m \langle \tilde{v}_1, \tilde{v}_2 \rangle, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $\tilde{e} = \mathsf{fst}\langle \tilde{e}_1, \tilde{e}_2 \rangle$

One rule applies, namely
$$\textsc{SE-First}\quad \frac{\tilde{e}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{v}_1, \tilde{\sigma}', \varphi}}{\mathsf{fst}\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \rightsquigarrow \overline{\tilde{v}_1, \tilde{\sigma}', \varphi}}$$
Provided that $e, \sigma \leftrightarrows_m \mathsf{fst}\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma}, \Phi$ and $\mathsf{fst}\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \rightsquigarrow \tilde{v}_1, \tilde{\sigma}'', \varphi$, we obtain from the induction hypothesis that $e_1, \sigma \downarrow v_1, \sigma'$ with $v_1, \sigma' \leftrightarrows_m \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can conclude that $\mathsf{fst}\langle e_1, e_2 \rangle, \sigma \downarrow v_1, \sigma'$.

Case $e = \mathsf{snd}\langle \tilde{e}_1, \tilde{e}_2 \rangle$

One rule applies, namely
$$\textsc{SE-Second}\quad \frac{\tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{v}_2, \tilde{\sigma}', \varphi}}{\mathsf{snd}\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \rightsquigarrow \overline{\tilde{v}_2, \tilde{\sigma}', \varphi}}$$
Provided that $e, \sigma \leftrightarrows_m \mathsf{snd}\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma}, \Phi$ and $\mathsf{snd}\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \rightsquigarrow \tilde{v}_2, \tilde{\sigma}'', \varphi$, we obtain from the induction hypothesis that $e_1, \sigma \downarrow v_2, \sigma'$ with $v_2, \sigma' \leftrightarrows_m \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can conclude that $\mathsf{snd}\langle e_1, e_2 \rangle, \sigma \downarrow v_2, \sigma'$.

Case $\tilde{e} = \tilde{e}_1 :: \tilde{e}_2$

One rule applies, namely
$$\textsc{SE-Cons}\quad \frac{\tilde{e}_1, \tilde{\sigma} \rightsquigarrow \tilde{v}_1, \tilde{\sigma}', \varphi_1 \qquad \tilde{e}_2, \tilde{\sigma}' \rightsquigarrow \tilde{v}_2, \tilde{\sigma}'', \varphi_2}{\tilde{e}_1 :: \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}$$
Provided that $e, \sigma \leftrightarrows_m \tilde{e}_1 :: \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{e}_1 :: \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2$, we obtain from the induction hypothesis that $e_1, \sigma \downarrow v_1, \sigma'$ with $v_1, \sigma' \leftrightarrows_m \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$. Then by a second application of the induction hypothesis, we obtain that $e_2, \sigma' \downarrow v_2, \sigma''$ with $v_2, \sigma'' \leftrightarrows_m \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. From this, we can conclude that $e_1 :: e_2, \sigma \downarrow v_1 :: v_2, \sigma''$ with $v_1 :: v_2, \sigma'' \leftrightarrows_m \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

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

One rule applies, namely
$$\textsc{SE-Head}\quad \frac{\tilde{e}, \tilde{\sigma} \rightsquigarrow \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}', \varphi}{\mathsf{head}\, \tilde{e}, \tilde{\sigma} \rightsquigarrow \tilde{v}_1, \tilde{\sigma}', \varphi}$$
Provided that $e, \sigma \leftrightarrows_m \mathsf{head}\, \tilde{e}, \tilde{\sigma}, \Phi$ and $\mathsf{head}\, \tilde{e}, \tilde{\sigma} \rightsquigarrow \tilde{v}_1, \tilde{\sigma}', \varphi$, we obtain from the induction hypothesis that $e, \sigma \downarrow v_1 :: v_2, \sigma'$ with $v_1 :: v_2, \sigma' \leftrightarrows_m \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can conclude that $\mathsf{head}\, e, \sigma \downarrow v_1, \sigma'$.

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

One rule applies, namely
$$\textsc{SE-Tail}\quad \frac{\tilde{e}, \tilde{\sigma} \rightsquigarrow \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}', \varphi}{\mathsf{tail}\, \tilde{e}, \tilde{\sigma} \rightsquigarrow \tilde{v}_2, \tilde{\sigma}', \varphi}$$
Provided that $e, \sigma \leftrightarrows_m \mathsf{tail}\, \tilde{e}, \tilde{\sigma}, \Phi$ and $\mathsf{tail}\, \tilde{e}, \tilde{\sigma} \rightsquigarrow \tilde{v}_2, \tilde{\sigma}', \varphi$, we obtain from the induction hypothesis that $e, \sigma \downarrow v_1 :: v_2, \sigma'$ with $v_1 :: v_2, \sigma' \leftrightarrows_m \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can conclude that $\mathsf{tail}\, e, \sigma \downarrow v_2, \sigma'$.

Case $\tilde{e} = \tilde{e}_1 \tilde{e}_2$

One rule applies, namely

$$\textsc{SE-App}\ \dfrac{\tilde{e}_1, \tilde{\sigma} \wr \overline{\lambda x : \tau . \tilde{e}_1', \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \wr \overline{\tilde{v}_2, \tilde{\sigma}'', \varphi_2} \qquad \tilde{e}_1'[x \mapsto \tilde{v}_2], \tilde{\sigma}'' \wr \overline{\tilde{v}_1, \tilde{\sigma}''', \varphi_3}}{\tilde{e}_1 \tilde{e}_2, \tilde{\sigma} \wr \overline{\tilde{v}_1, \tilde{\sigma}''', \varphi_1 \land \varphi_2 \land \varphi_3}}$$

Provided that $e, \sigma \leftrightarrows_m \tilde{e}_1 \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{e}_1 \tilde{e}_2, \tilde{\sigma} \wr \tilde{v}_1, \tilde{\sigma}''', \varphi_1 \land \varphi_2 \land \varphi_3$, we obtain from the induction hypothesis that $e_1, \sigma \downarrow \lambda x : \tau . e_1', \sigma'$ with $\lambda x : \tau . e_1', \sigma' \leftrightarrows_m \lambda x : \tau . \tilde{e}_1', \tilde{\sigma}', \Phi \land \varphi_1$. Then by a second application of the induction hypothesis, we obtain that $e_2, \sigma' \downarrow v_2, \sigma''$ with $v_2, \sigma'' \leftrightarrows_m \tilde{v}_2, \tilde{\sigma}'', \Phi \land \varphi_1 \land \varphi_2$. A third and final application of the induction hypothesis gives us that $e_1'[x \mapsto v_2], \sigma'' \downarrow v_1, \sigma'''$ with $v_1, \sigma''' \leftrightarrows_m \tilde{v}_1, \tilde{\sigma}''', \Phi \land \varphi_1 \land \varphi_2 \land \varphi_3$. From this, we can conclude that $e_1 e_2, \sigma \downarrow v_1, \sigma'''$.

Case $\tilde{e} = \textbf{if}\ \tilde{e}_1\ \textbf{then}\ \tilde{e}_2\ \textbf{else}\ \tilde{e}_3$

One rule applies, namely

$$\textsc{SE-If}\ \dfrac{\tilde{e}_1, \tilde{\sigma} \wr \overline{\tilde{v}_1, \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \wr \overline{\tilde{v}_2, \tilde{\sigma}'', \varphi_2} \qquad \tilde{e}_3, \tilde{\sigma}' \wr \overline{\tilde{v}_3, \tilde{\sigma}''', \varphi_3}}{\textbf{if}\ \tilde{e}_1\ \textbf{then}\ \tilde{e}_2\ \textbf{else}\ \tilde{e}_3, \tilde{\sigma} \wr \overline{\tilde{v}_2, \tilde{\sigma}'', \varphi_1 \land \varphi_2 \land \tilde{v}_1} \cup \overline{\tilde{v}_3, \tilde{\sigma}''', \varphi_1 \land \varphi_3 \land \neg \tilde{v}_1}}$$

Provided that $e, \sigma \leftrightarrows_m \textbf{if}\ \tilde{e}_1\ \textbf{then}\ \tilde{e}_2\ \textbf{else}\ \tilde{e}_3, \tilde{\sigma}, \Phi$ and , we obtain from the induction hypothesis that $e_1, \sigma \downarrow v_1, \sigma'$ with $v_1, \sigma' \leftrightarrows_m \tilde{v}_1, \tilde{\sigma}', \Phi \land \varphi_1$. At this point, we have two potential branches. Applying the induction hypothesis to either of them, we obtain that $e_2, \sigma' \downarrow v_2, \sigma''$ with $v_2, \sigma'' \leftrightarrows_m \tilde{v}_2, \tilde{\sigma}'', \Phi \land \varphi_1 \land \varphi_2$ and $e_3, \sigma' \downarrow v_3, \sigma''$ with $v_3, \sigma'' \leftrightarrows_m \tilde{v}_3, \tilde{\sigma}'', \Phi \land \varphi_1 \land \varphi_3$. From this, we can conclude that $\textbf{if}\ e_1\ \textbf{then}\ e_2\ \textbf{else}\ e_3, \sigma \downarrow v_2, \sigma''$ with $v_2, \sigma'' \leftrightarrows_M \tilde{v}_2, \tilde{\sigma}'', \Phi \land \varphi_1 \land \varphi_2$ or $\textbf{if}\ e_1\ \textbf{then}\ e_2\ \textbf{else}\ e_3, \sigma \downarrow v_3, \sigma''$ with $v_3, \sigma'' \leftrightarrows_M \tilde{v}_3, \tilde{\sigma}'', \Phi \land \varphi_1 \land \varphi_3$.

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

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

Provided that $e, \sigma \leftrightarrows_m \textbf{ref}\ \tilde{e}, \tilde{\sigma}, \Phi$ and $\textbf{ref}\ \tilde{e}, \tilde{\sigma} \wr l, \tilde{\sigma}'[l \mapsto \tilde{v}], \varphi$, we obtain from the induction hypothesis that $e, \sigma \downarrow v_1, \sigma'$ with $v_1, \sigma' \leftrightarrows_m \tilde{v}_1, \tilde{\sigma}', \Phi \land \varphi$. From this, we can conclude that $\textbf{ref}\ e, \sigma \downarrow l, \sigma'[l \mapsto v]$ with $l, \sigma'[l \mapsto v] \leftrightarrows_m l, \tilde{\sigma}'[l \mapsto \tilde{v}], \Phi \land \varphi$.

Case $\tilde{e} = !\tilde{e}$

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

Provided that $e, \sigma \leftrightarrows_m !\tilde{e}, \tilde{\sigma}, \Phi$ and $!\tilde{e}, \tilde{\sigma} \wr \tilde{\sigma}'(l), \tilde{\sigma}', \varphi$, we obtain from the induction hypothesis that $e, \sigma \downarrow l, \sigma'$ with $l, \sigma' \leftrightarrows_m l, \tilde{\sigma}', \Phi \land \varphi$. From this, we can conclude that $!e, \sigma \downarrow \sigma'(l), \sigma'$ with $\sigma'(l), \sigma' \leftrightarrows_m \tilde{\sigma}'(l), \tilde{\sigma}', \Phi \land \varphi$.

Case $\tilde{e} = \tilde{e}_1 := \tilde{e}_2$

One rule applies, namely
$$\textsc{SE-Assign}\ \frac{\tilde{e}_1, \tilde{\sigma} \ \wr\ \overline{l, \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \ \wr\ \overline{\tilde{v}_2, \tilde{\sigma}'', \varphi_2}}{\tilde{e}_1 := \tilde{e}_2, \tilde{\sigma} \ \wr\ \overline{\langle\rangle, \tilde{\sigma}''[l \mapsto \tilde{v}_2], \varphi_1 \wedge \varphi_2}}$$
Provided that $e, \sigma \leftrightarrows_m \tilde{e}_1 := \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{e}_1 := \tilde{e}_2, \tilde{\sigma} \ \wr\ \langle\rangle, \tilde{\sigma}''[l \mapsto \tilde{v}_2], \varphi_1 \wedge \varphi_2$, we obtain from the induction hypothesis that $e_1, \sigma \ \downarrow\ l, \sigma'$ with $l, \sigma' \leftrightarrows_m l, \tilde{\sigma}', \Phi \wedge \varphi_1$. Then by a second application of the induction hypothesis, we obtain that $e_2, \sigma' \ \downarrow\ v_2, \sigma''$ with $v_2, \sigma'' \leftrightarrows_m \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. From this, we can conclude that $e_1 := e_2, \sigma \ \downarrow\ \langle\rangle, \sigma''[l \mapsto v_2]$ with $\langle\rangle, \sigma''[l \mapsto v_2] \leftrightarrows_m \langle\rangle, \tilde{\sigma}''[l \mapsto \tilde{v}_2], \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $\tilde{e} = \square\, \tilde{e}$

One rule applies, namely
$$\textsc{SE-Edit}\ \frac{\tilde{e}, \tilde{\sigma} \ \wr\ \overline{\tilde{v}, \tilde{\sigma}', \varphi}}{\square\, \tilde{e}, \tilde{\sigma} \ \wr\ \overline{\square\, \tilde{v}, \tilde{\sigma}', \varphi}}$$
Provided that $e, \sigma \leftrightarrows_m \square\, \tilde{e}, \tilde{\sigma}, \Phi$ and $\square\, \tilde{e}, \tilde{\sigma} \ \wr\ \square\, \tilde{v}, \tilde{\sigma}', \varphi$, we obtain from the induction hypothesis that $e, \sigma \ \downarrow\ v, \sigma'$ with $v, \sigma' \leftrightarrows_m \tilde{v}, \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can conclude that $\square\, e, \sigma \ \downarrow\ \square\, v, \sigma'$ with $\square\, v, \sigma' \leftrightarrows_m \square\, \tilde{v}, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $\tilde{e} = \boxtimes\, \tau$

One rule applies, namely
$$\textsc{SE-Enter}\ \frac{}{\boxtimes\, \tau, \tilde{\sigma} \ \wr\ \overline{\boxtimes\, \tau, \tilde{\sigma}, \mathsf{True}}}$$
We assume $e, \sigma \leftrightarrows_M \boxtimes\, \tau, \tilde{\sigma}, \Phi$ and $\boxtimes\, \tau, \tilde{\sigma} \ \wr\ \boxtimes\, \tau, \tilde{\sigma}, \mathsf{True}$. By E-Enter we have $\boxtimes\, \tau, \sigma \ \downarrow\ \boxtimes\, \tau, \sigma$, so this case holds trivially.

Case $\tilde{e} = \blacksquare\, \tilde{e}$

One rule applies, namely
$$\textsc{SE-Update}\ \frac{\tilde{e}, \tilde{\sigma} \ \wr\ \overline{l, \tilde{\sigma}', \varphi}}{\blacksquare\, \tilde{e}, \tilde{\sigma} \ \wr\ \overline{\blacksquare\, l, \tilde{\sigma}', \varphi}}$$
Provided that $e, \sigma \leftrightarrows_m \blacksquare\, \tilde{e}, \tilde{\sigma}, \Phi$ and $\blacksquare\, \tilde{e}, \tilde{\sigma} \ \wr\ \blacksquare\, l, \tilde{\sigma}', \varphi$, we obtain from the induction hypothesis that $e, \sigma \ \downarrow\ l, \sigma'$ with $l, \sigma' \leftrightarrows_m l, \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can conclude that $\blacksquare\, e, \sigma \ \downarrow\ \blacksquare\, l, \sigma'$ with $\blacksquare\, l, \sigma' \leftrightarrows_m \blacksquare\, l, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $\tilde{e} = \tilde{e}_1 \blacktriangleright \tilde{e}_2$

One rule applies, namely
$$\textsc{SE-Then}\ \frac{\tilde{e}_1, \tilde{\sigma} \ \wr\ \overline{\tilde{t}_1, \tilde{\sigma}', \varphi}}{\tilde{e}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \ \wr\ \overline{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi}}$$
Provided that $e, \sigma \leftrightarrows_m \tilde{e}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{e}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \ \wr\ \tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi$, we obtain from the induction hypothesis that $e_1, \sigma \ \downarrow\ t_1, \sigma'$ with $t_1, \sigma' \leftrightarrows_m \tilde{t}_1, \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can conclude that $e_1 \blacktriangleright e_2, \sigma \ \downarrow\ t_1 \blacktriangleright e_2, \sigma'$ with $t_1 \blacktriangleright e_2, \sigma' \leftrightarrows_m \tilde{t}_1 \blacktriangleright e_2, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $\tilde{e} = \tilde{e}_1 \rhd \tilde{e}_2$

One rule applies, namely
$$\textsc{SE-Next}\quad \frac{\tilde{e}_1, \tilde{\sigma} \ \wr\ \overline{\tilde{t}_1, \tilde{\sigma}', \varphi}}{\tilde{e}_1 \rhd \tilde{e}_2, \tilde{\sigma} \ \wr\ \overline{\tilde{t}_1 \rhd \tilde{e}_2, \tilde{\sigma}', \varphi}}$$
Provided that $e, \sigma \leftrightarrows_m \tilde{e}_1 \rhd \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{e}_1 \rhd \tilde{e}_2, \tilde{\sigma} \ \wr\ \tilde{t}_1 \rhd \tilde{e}_2, \tilde{\sigma}', \varphi$, we obtain from the induction hypothesis that $e_1, \sigma \downarrow t_1, \sigma'$ with $t_1, \sigma' \leftrightarrows_m \tilde{t}_1, \tilde{\sigma}', \Phi \wedge \varphi$. From this, we can conclude that $e_1 \rhd e_2, \sigma \downarrow t_1 \rhd e_2, \sigma'$ with $t_1 \rhd e_2, \sigma' \leftrightarrows_m \tilde{t}_1 \rhd e_2, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $\tilde{e} = \tilde{e}_1 \blacklozenge \tilde{e}_2$

One rule applies, namely
$$\textsc{SE-Or}\quad \frac{\tilde{e}_1, \tilde{\sigma} \ \wr\ \overline{\tilde{t}_1, \tilde{\sigma}', \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma}' \ \wr\ \overline{\tilde{t}_2, \tilde{\sigma}'', \varphi_2}}{\tilde{e}_1 \blacklozenge \tilde{e}_2, \tilde{\sigma} \ \wr\ \overline{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2}}$$
Provided that $e, \sigma \leftrightarrows_m \tilde{e}_1 \blacklozenge \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{e}_1 \blacklozenge \tilde{e}_2, \tilde{\sigma} \ \wr\ \tilde{v}_1 \blacklozenge \tilde{v}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2$, we obtain from the induction hypothesis that $e_1, \sigma \downarrow v_1, \sigma'$ with $v_1, \sigma' \leftrightarrows_m \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$. Then by a second application of the induction hypothesis, we obtain that $e_2, \sigma' \downarrow v_2, \sigma''$ with $v_2, \sigma'' \leftrightarrows_m \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. From this, we can conclude that $e_1 \blacklozenge e_2, \sigma \downarrow v_1 \blacklozenge v_2, \sigma''$ with $v_1 \blacklozenge v_2, \sigma'' \leftrightarrows_m \tilde{v}_1 \blacklozenge \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $\tilde{e} = \tilde{e}_1 \lozenge \tilde{e}_2$

One rule applies, namely
$$\textsc{SE-Xor}\quad \frac{}{\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \ \wr\ \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}, \mathsf{True}}$$
We assume $e, \sigma \leftrightarrows_M \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}, \Phi$ and $\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \ \wr\ \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}, \mathsf{True}$. By E-Xor we have $e_1 \lozenge e_2, \sigma \downarrow e_1 \lozenge e_2, \sigma$, so this case holds trivially.

Case $\tilde{e} = \lightning$

One rule applies, namely
$$\textsc{SE-Fail}\quad \frac{}{\lightning, \tilde{\sigma} \ \wr\ \lightning, \tilde{\sigma}, \mathsf{True}}$$
We assume $e, \sigma \leftrightarrows_M \lightning, \tilde{\sigma}, \Phi$ and $\lightning, \tilde{\sigma} \ \wr\ \lightning, \tilde{\sigma}, \mathsf{True}$. By E-Fail we have $\lightning, \sigma \downarrow \lightning, \sigma$, so this case holds trivially.

E Completeness proofs

Proof (Completeness of simulate). The structure of this proof is outlined in Fig. 6.

We have t and σ such that $t, \sigma \overset{I}{\Rightarrow}{}^{*} v$. By definition of $\overset{I}{\Rightarrow}{}^{*}$, we have the following. $t, \sigma \overset{i_1}{\Rightarrow} t_1, \sigma_1 \overset{i_2}{\Rightarrow} \cdots \overset{i_n}{\Rightarrow} t_n, \sigma_n$ with $\mathcal{V}(t_n, \sigma_n)$ and $I = [i_1, \cdots, i_n]$.
We need to show that we have $(\tilde{v}, \tilde{I}, \Phi) \in t, \sigma \Rightarrow^{*})$, which is defined as follows.

$$\begin{array}{llll}
t, \sigma \Rightarrow \tilde{t}_1, \tilde{\sigma}_1, \tilde{\imath}_1, \varphi_1 & & & \\
\quad \tilde{t}_1, \tilde{\sigma}_1 \Rightarrow & \tilde{t}_2, \tilde{\sigma}_2, \tilde{\imath}_2, \varphi_2 & & \\
 & \quad \tilde{t}_2, \tilde{\sigma}_2 \Rightarrow \cdots & & \\
 & & \cdots & \Rightarrow \tilde{t}_n, \tilde{\sigma}_n, \tilde{\imath}_n, \varphi_n
\end{array}$$

with $\mathcal{V}(\tilde{t}_n, \tilde{\sigma}_n) = \tilde{v}$ and $\mathcal{S}(\varphi_1 \wedge \cdots \wedge \varphi_n)$.

By Lemma 4, we know that $t, \sigma \Rightarrow \tilde{t}_1, \tilde{\sigma}_1, \tilde{\imath}_1, \varphi_1$ exists, since $t, \sigma, t \leftrightarrows_{\emptyset} \sigma, \mathsf{True}$. This also gives us that $\tilde{\imath}_1 \sim i_1$ and $t_1, \sigma_1 \leftrightarrows_{[s_1 \mapsto c_1]} \tilde{t}_1, \tilde{\sigma}_1, \varphi_1$ with $SymOf(\tilde{\imath}_1) = s_1$ and $ValOf(i_1) = c_1$.

By repeated application of Lemma 4, untill we arrive at t_n, σ_n, we can show that there exists a $\tilde{I}$ such that $t, \sigma \Rightarrow^{*} \tilde{t}_n, \tilde{\sigma}_n, \tilde{I}, \Phi$, namely $[\tilde{\imath}_1, \cdots, \tilde{\imath}_n]$.

Lemma 10 (Completeness of handling). *For all concrete tasks t, concrete states σ, concrete inputs i, symbolic tasks $\tilde{t}$, symbolic states $\tilde{\sigma}$ path conditions Φ and mappings M, we have that $t, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $t, \sigma \xrightarrow{i} t', \sigma'$ together with $\tilde{t}, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}', \tilde{\sigma}', \tilde{\imath}, \varphi}$, and for all pairs $(\tilde{t}', \tilde{\sigma}', \tilde{\imath}, \varphi)$ we have that $\mathcal{S}(\Phi \wedge \varphi)$ and $\imath \sim i$ implies $t', \sigma' \leftrightarrows_{M.[s \mapsto c]} \tilde{t}', \tilde{\sigma}', \Phi \wedge \varphi$ where where $SymOf(\tilde{\imath}) = s$ and $ValOf(i) = c$.*

Lemma 11 (Completeness of normalisation). *For all concrete expressions e, concrete states σ, symbolic expressions $\tilde{e}$, symbolic states $\tilde{\sigma}$ path conditions Φ and mappings M, we have that $e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and $e, \sigma \Downarrow t, \sigma'$, then $\tilde{e}, \tilde{\sigma} \wr\wr \overline{\tilde{t}, \tilde{\sigma}', \varphi}$, and for all pairs $(\tilde{t}, \tilde{\sigma}', \varphi)$ we have that $\mathcal{S}(\Phi \wedge \varphi)$ implies $t, \sigma' \leftrightarrows_M \tilde{t}, \tilde{\sigma}', \Phi \wedge \varphi$.*

Lemma 12 (Completeness of striding). *For all concrete tasks t, concrete states σ, symbolic tasks $\tilde{t}$, symbolic states $\tilde{\sigma}$ path conditions Φ and mappings M, we have that $t, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $t, \sigma \mapsto t', \sigma'$, then $\tilde{t}, \tilde{\sigma} \mapstochar\rightsquigarrow \overline{\tilde{t}', \tilde{\sigma}', \varphi}$, and for all pairs $(\tilde{t}', \tilde{\sigma}', \varphi)$ we have that $\mathcal{S}(\Phi \wedge \varphi)$ implies $t', \sigma' \leftrightarrows_M \tilde{t}', \tilde{\sigma}', \Phi \wedge \varphi$.*

Lemma 13 (Completeness of evaluate). *For all concrete expressions e, concrete states σ, symbolic expressions $\tilde{e}$, symbolic states $\tilde{\sigma}$ path conditions Φ and mappings M, we have that $e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and $e, \sigma \downarrow v, \sigma'$, then $\tilde{e}, \tilde{\sigma} \wr \overline{\tilde{v}, \tilde{\sigma}', \varphi}$, and for all pairs $(\tilde{v}, \tilde{\sigma}', \varphi)$ we have that $\mathcal{S}(\Phi \wedge \varphi)$ implies $v, \sigma' \leftrightarrows_M \tilde{v}, \tilde{\sigma}', \Phi \wedge \varphi$.*

Proof (Completeness of handle). We prove Lemma 10 by induction over t.

Case $t = \square\, v$

Provided that $\square\, v, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and
$$\textsc{H-Change}\ \frac{}{\square\, v, \sigma \xrightarrow{v'} \square\, v', \sigma}\ v, v' : \tau$$
, then $\square\, \tilde{v}, \tilde{\sigma} \rightarrow \square\, s, \tilde{\sigma}, s, \mathsf{True}$. $\mathcal{S}(\Phi \wedge \mathsf{True}) = \mathcal{S}(\Phi)$, which follows from the premise. Furthermore we have $s \sim v'$ by definition. Then finally $\square\, v', \sigma \leftrightarrows M[s \mapsto v']\, \square\, s, \tilde{\sigma}, \Phi$ since $M[s \mapsto v']s = v'$.

Case $t = \boxtimes\, \tau$

Provided that $\boxtimes\, \tau, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and
$$\textsc{H-Fill}\ \frac{}{\boxtimes\, \tau, \sigma \xrightarrow{v} \square\, v, \sigma}\ v : \tau$$
then $\boxtimes\, \tau, \tilde{\sigma} \rightarrow \square\, s, \tilde{\sigma}, s, \mathsf{True}$. $\mathcal{S}(\Phi \wedge \mathsf{True}) = \mathcal{S}(\Phi)$, which follows from the premise. Furthermore we have $s \sim v$ by definition. Then finally $\square\, v, \sigma \leftrightarrows M[s \mapsto v]\, \square\, s, \tilde{\sigma}, \Phi$ since $M[s \mapsto v]s = v$.

Case $t = \blacksquare\, l$

Provided that $\blacksquare\, l, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\dfrac{}{\blacksquare\, l, \sigma \xrightarrow{v} \blacksquare\, l, \sigma[l \mapsto v]}\ \sigma(l), v : \tau$ (H-Update), then $\blacksquare\, l, \tilde{\sigma} \rightarrow \blacksquare\, l, \tilde{\sigma}[l \mapsto s], s, \mathsf{True}$. $\mathcal{S}(\Phi \wedge \mathsf{True}) = \mathcal{S}(\Phi)$, which follows from the premise. Furthermore we have $s \sim v$ by definition. Then finally $\blacksquare\, l, \sigma[l \mapsto v] \leftrightarrows M[s \mapsto v]\ \blacksquare\, l, \tilde{\sigma}[l \mapsto s], \Phi$ since $M[s \mapsto v]s = v$.

Case $t = t_1 \triangleright e_2$

Case $i = \mathsf{C}$

Provided that $t_1 \triangleright e_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and

$$\textsc{H-Next}\ \dfrac{e_2\ v_1, \sigma \Downarrow t_2, \sigma'}{t_1 \triangleright e_2, \sigma \xrightarrow{\mathsf{C}} t_2, \sigma'}\ \mathcal{V}(t_1, \sigma) = v_1 \wedge \neg\mathcal{F}(t_2, \sigma'),$$

then

$$\textsc{SH-Next}\ \dfrac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_1, \tilde{\sigma}'_1, \tilde{\imath}, \varphi_1} \qquad \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma} \between \overline{\tilde{t}_2, \tilde{\sigma}'_2, \varphi_2}}{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_1 \triangleright \tilde{e}_2, \tilde{\sigma}'_1, \tilde{\imath}, \varphi_1} \cup \overline{\tilde{t}_2, \tilde{\sigma}'_2, \mathsf{C}, \varphi_2}}\ \mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \tilde{v}_1 \wedge \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}')$$

. The simulation step results in two sets, from which only the second adheres to the requirement that the symbolic input should simulate the concrete input. For this set, $\overline{\tilde{t}_2, \tilde{\sigma}'_2, \mathsf{C}, \varphi_2}$, we have $\mathcal{S}(\Phi \wedge \varphi_2)$ implies $t_2, \sigma'_2 \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}'_2, \Phi \wedge \varphi_2$, Which follows directly from Lemma 11.

Case $i \neq \mathsf{C}$

Provided that $t_1 \triangleright e_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and

$$\textsc{H-PassNext}\ \dfrac{t_1, \sigma \xrightarrow{i} t'_1, \sigma'}{t_1 \triangleright e_2, \sigma \xrightarrow{i} t'_1 \triangleright e_2, \sigma'}.$$

There are three symbolic rules that apply, namely

$$\textsc{SH-PassNext}\ \dfrac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_1, \tilde{\sigma}', \tilde{\imath}, \varphi}}{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_1 \triangleright \tilde{e}_2, \tilde{\sigma}', \tilde{\imath}, \varphi}}\ \mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \bot,$$

$$\textsc{SH-PassNextFail}\ \dfrac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_1, \tilde{\sigma}'_1, \tilde{\imath}, \varphi} \qquad \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma} \between \overline{\tilde{t}_2, \tilde{\sigma}'_2, \_}}{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_1 \triangleright \tilde{e}_2, \tilde{\sigma}'_1, \tilde{\imath}, \varphi}}\ \mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \tilde{v}_1 \wedge \mathcal{F}(\tilde{t}_2, \tilde{\sigma}'_2)$$

and

$$\textsc{SH-Next}\ \dfrac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_1, \tilde{\sigma}'_1, \tilde{\imath}, \varphi_1} \qquad \tilde{e}_2\ \tilde{v}_1, \tilde{\sigma} \between \overline{\tilde{t}_2, \tilde{\sigma}'_2, \varphi_2}}{\tilde{t}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}'_1 \triangleright \tilde{e}_2, \tilde{\sigma}'_1, \tilde{\imath}, \varphi_1} \cup \overline{\tilde{t}_2, \tilde{\sigma}'_2, \mathsf{C}, \varphi_2}}\ \mathcal{V}(\tilde{t}_1, \tilde{\sigma}) = \tilde{v}_1 \wedge \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}').$$

We are only interested in the runs that produce a symbolic input that simulates the concrete input i. Whichever rule applies, we deal with the same premise because of this restriction. This allows us to apply the induction hypothesis and obtain that $\mathcal{S}(\Phi \wedge \varphi_1) \supset t'_1, \sigma' \leftrightarrows_{M.[s\mapsto c]} \tilde{t}'_1, \tilde{\sigma}', \Phi \wedge \varphi_1$. From this, we can directly conclude that $t'_1 \triangleright e_2, \sigma' \leftrightarrows_{M.[s\mapsto c]} \tilde{t}'_1 \triangleright \tilde{e}_2, \tilde{\sigma}', \Phi \wedge \varphi_1$.

Case $t = t_1 \blacktriangleright e_2$

Provided that $t_1 \blacktriangleright e_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\dfrac{t_1, \sigma \xrightarrow{i} t_1', \sigma'}{t_1 \blacktriangleright e_2, \sigma \xrightarrow{i} t_1' \blacktriangleright e_2, \sigma'}$ H-PassThen,

then $\dfrac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}', \tilde{\imath}, \varphi}}{\tilde{t}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \tilde{\imath}, \varphi}}$ SH-PassThen.

By application of the induction hypothesis, we obtain $\mathcal{S}(\Phi \wedge \varphi)$ implies $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi$ from which we can conclude that $t_1' \blacktriangleright e_2, \sigma' \leftrightarrows_M \tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $t = e_1 \Diamond e_2$

Case $i = \mathsf{L}$

Provided that $e_1 \Diamond e_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\dfrac{e_1, \sigma \Downarrow t_1, \sigma' \qquad \neg\mathcal{F}(t_1, \sigma')}{e_1 \Diamond e_2, \sigma \xrightarrow{\mathsf{L}} t_1, \sigma'}$ H-PickLeft,

then $\dfrac{\tilde{e}_1, \tilde{\sigma} \Downarrow \overline{\tilde{t}_1, \tilde{\sigma}_1, \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma} \Downarrow \overline{\tilde{t}_2, \tilde{\sigma}_2, \varphi_2} \qquad \neg\mathcal{F}(\tilde{t}_1, \tilde{\sigma}_1) \wedge \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}_2)}{\tilde{e}_1 \Diamond \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1, \tilde{\sigma}_1, \mathsf{L}, \varphi_1} \cup \overline{\tilde{t}_2, \tilde{\sigma}_2, \mathsf{R}, \varphi_2}}$ SH-Pick.

By Lemma 11 we obtain $\mathcal{S}(\Phi \wedge \varphi_1)$ implies $t_1, \sigma' \leftrightarrows_M \tilde{t}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$ from which we can conclude that $t_1, \sigma' \leftrightarrows_M \tilde{t}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$.

Case $i = \mathsf{R}$

Provided that $e_1 \Diamond e_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\dfrac{e_1, \sigma \Downarrow t_1, \sigma' \qquad \neg\mathcal{F}(t_1, \sigma')}{e_1 \Diamond e_2, \sigma \xrightarrow{\mathsf{L}} t_1, \sigma'}$ H-PickLeft,

then $\dfrac{\tilde{e}_1, \tilde{\sigma} \Downarrow \overline{\tilde{t}_1, \tilde{\sigma}_1, \varphi_1} \qquad \tilde{e}_2, \tilde{\sigma} \Downarrow \overline{\tilde{t}_2, \tilde{\sigma}_2, \varphi_2} \qquad \neg\mathcal{F}(\tilde{t}_1, \tilde{\sigma}_1) \wedge \neg\mathcal{F}(\tilde{t}_2, \tilde{\sigma}_2)}{\tilde{e}_1 \Diamond \tilde{e}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1, \tilde{\sigma}_1, \mathsf{L}, \varphi_1} \cup \overline{\tilde{t}_2, \tilde{\sigma}_2, \mathsf{R}, \varphi_2}}$ SH-Pick.

By Lemma 11 we obtain $\mathcal{S}(\Phi \wedge \varphi_2)$ implies $t_2, \sigma' \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}', \Phi \wedge \varphi_2$ from which we can conclude that $t_2, \sigma' \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}', \Phi \wedge \varphi_2$.

Case $t = t_1 \blacklozenge t_2$

Two rules applies in this case.

Case $i = \mathsf{F}\, i$

Provided that $t_1 \blacklozenge t_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\dfrac{t_1, \sigma \xrightarrow{i} {t_1}', \sigma'}{t_1 \blacklozenge t_2, \sigma \xrightarrow{\mathsf{F}\, i} {t_1}' \blacklozenge t_2, \sigma'}$ H-FirstOr,

then $\dfrac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}_1, \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_2', \tilde{\sigma}_2', \tilde{\imath}_2, \varphi_2}}{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1' \blacklozenge \tilde{t}_2, \tilde{\sigma}_1', \mathsf{F}\, \tilde{\imath}_1, \varphi_1} \cup \overline{\tilde{t}_1 \blacklozenge \tilde{t}_2', \tilde{\sigma}_2', \mathsf{S}\, \tilde{\imath}_2, \varphi_2}}$ SH-Or.

By application of the induction hypothesis we obtain $\mathcal{S}(\Phi \wedge \varphi_1)$ implies $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$ from which we can conclude that $t_1' \blacklozenge t_2, \sigma' \leftrightarrows_M \tilde{t}_1' \blacklozenge \tilde{t}_2, \tilde{\sigma}', \Phi \wedge \varphi_1$.

Case $i = \mathsf{S}\, i$

Provided that $t_1 \blacklozenge t_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\dfrac{t_2, \sigma \xrightarrow{i} t_2', \sigma'}{t_1 \blacklozenge t_2, \sigma \xrightarrow{\mathsf{S}\, i} t_1 \blacklozenge t_2', \sigma'}$ H-SecondOr,

then $\dfrac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}_1, \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_2', \tilde{\sigma}_2', \tilde{\imath}_2, \varphi_2}}{\tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\overline{\tilde{t}_1' \blacklozenge \tilde{t}_2, \tilde{\sigma}_1', \mathsf{F}\, \tilde{\imath}_1, \varphi_1} \cup \overline{\tilde{t}_1 \blacklozenge \tilde{t}_2', \tilde{\sigma}_2', \mathsf{S}\, \tilde{\imath}_2, \varphi_2}}}$ SH-Or.

By application of the induction hypothesis we obtain $\mathcal{S}(\Phi \wedge \varphi_2)$ implies $t_2', \sigma' \leftrightarrows_M \tilde{t}_2', \tilde{\sigma}', \Phi \wedge \varphi_2$ from which we can conclude that $t_1 \blacklozenge t_2', \sigma' \leftrightarrows_M \tilde{t}_1 \blacklozenge \tilde{t}_2', \tilde{\sigma}', \Phi \wedge \varphi_2$.

Case $t = t_1 \bowtie t_2$

Two rules applies in this case.

Case $i = \mathsf{F}\, i$

Provided that $t_1 \bowtie t_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\dfrac{t_1, \sigma \xrightarrow{i} t_1', \sigma'}{t_1 \bowtie t_2, \sigma \xrightarrow{\mathsf{F}\, i} t_1' \bowtie t_2, \sigma'}$ H-FirstAnd,

then $\dfrac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}_1, \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_2', \tilde{\sigma}_2', \tilde{\imath}_2, \varphi_2}}{\tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\overline{\tilde{t}_1' \bowtie \tilde{t}_2, \tilde{\sigma}_1', \mathsf{F}\, \tilde{\imath}_1, \varphi_1} \cup \overline{\tilde{t}_1 \bowtie \tilde{t}_2', \tilde{\sigma}_2'', \mathsf{S}\, \tilde{\imath}_2, \varphi_2}}}$ SH-And.

By application of the induction hypothesis we obtain $\mathcal{S}(\Phi \wedge \varphi_1)$ implies $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$ from which we can conclude that $t_1' \bowtie t_2, \sigma' \leftrightarrows_M \tilde{t}_1' \bowtie \tilde{t}_2, \tilde{\sigma}', \Phi \wedge \varphi_1$.

Case $i = \mathsf{S}\, i$

Provided that $t_1 \bowtie t_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\dfrac{t_2, \sigma \xrightarrow{i} t_2', \sigma'}{t_1 \bowtie t_2, \sigma \xrightarrow{\mathsf{S}\, i} t_1 \bowtie t_2', \sigma'}$ H-SecondAnd,

then $\dfrac{\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_1', \tilde{\sigma}_1', \tilde{\imath}_1, \varphi_1} \qquad \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\tilde{t}_2', \tilde{\sigma}_2', \tilde{\imath}_2, \varphi_2}}{\tilde{t}_1 \bowtie \tilde{t}_2, \tilde{\sigma} \rightsquigarrow \overline{\overline{\tilde{t}_1' \bowtie \tilde{t}_2, \tilde{\sigma}_1', \mathsf{F}\, \tilde{\imath}_1, \varphi_1} \cup \overline{\tilde{t}_1 \bowtie \tilde{t}_2', \tilde{\sigma}_2'', \mathsf{S}\, \tilde{\imath}_2, \varphi_2}}}$ SH-And.

By application of the induction hypothesis we obtain $\mathcal{S}(\Phi \wedge \varphi_2)$ implies $t_2', \sigma' \leftrightarrows_M \tilde{t}_2', \tilde{\sigma}', \Phi \wedge \varphi_2$ from which we can conclude that $t_1 \bowtie t_2', \sigma' \leftrightarrows_M \tilde{t}_1 \bowtie \tilde{t}_2', \tilde{\sigma}', \Phi \wedge \varphi_2$.

Proof (Completeness of normalise). We prove Lemma 11 by induction over e.

From the premise, we can assume that $e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$. Now, given that $e, \sigma \Downarrow t, \sigma'$, we need to demonstrate that $\tilde{e}, \tilde{\sigma} \Downarrow \tilde{t}, \tilde{\sigma}'$ with $t, \sigma' \leftrightarrows_M \tilde{t}, \tilde{\sigma}', \Phi \wedge \varphi$.

The base case is when the N-Done rule applies.

N-Done

$$\frac{e, \sigma \downarrow t, \sigma' \qquad t, \sigma' \mapsto t', \sigma''}{e, \sigma \Downarrow t, \sigma'}\ \sigma' = \sigma'' \wedge t = t'$$

In this case, we obtain from Lemma 13 that $\tilde{e}, \tilde{\sigma} \;\;\rightsquigarrow\;\; \tilde{t}, \tilde{\sigma}'$ with $t, \sigma' \leftrightarrows_M \tilde{t}, \tilde{\sigma}', \Phi \wedge \varphi$, which is exactly what we needed to show.

The only induction step is when

$$\text{N-Repeat}\quad \frac{e, \sigma \downarrow t, \sigma' \qquad t, \sigma' \mapsto t', \sigma'' \qquad t', \sigma'' \Downarrow t'', \sigma'''}{e, \sigma \Downarrow t'', \sigma'''}\ \sigma' \neq \sigma'' \vee t \neq t'$$

applies.

In this case, we obtain from Lemma 13 that $\tilde{e}, \tilde{\sigma} \;\;\rightsquigarrow\;\; \tilde{t}, \tilde{\sigma}'$ with $t, \sigma' \leftrightarrows_M \tilde{t}, \tilde{\sigma}', \Phi \wedge \varphi$. Furthermore, by Lemma 12 we obtain that $\tilde{t}, \tilde{\sigma}' \;\; \hookrightarrow \;\; \tilde{t}', \tilde{\sigma}''$ with $t', \sigma'' \leftrightarrows_M \tilde{t}', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. Then finally, by application of the induction hypothesis, we obtain what we needed to prove. $\tilde{t}', \tilde{\sigma}'' \;\;\rightsquigarrow\;\; \tilde{t}'', \tilde{\sigma}'''$ with $t'', \sigma''' \leftrightarrows_M \tilde{t}'', \tilde{\sigma}''', \Phi \wedge \varphi_1 \wedge \varphi_2 \wedge \varphi_3$.

Proof (Completeness of stride).

Case $t = \square\, v$

Provided that $\square\, v, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\text{S-Edit}\ \dfrac{}{\square\, v, \sigma \mapsto \square\, v, \sigma}$, we can conclude that $\tilde{t} = \square\, \tilde{v}$ and then by SS-Edit, $\square\, \tilde{v}, \tilde{\sigma} \;\; \hookrightarrow \;\; \square\, \tilde{v}, \tilde{\sigma}$. Since the expressions do not change in this case, consistency holds trivially.

Case $t = \boxtimes\, \tau$

Provided that $\boxtimes\, \tau, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\text{S-Fill}\ \dfrac{}{\boxtimes\, \tau, \sigma \mapsto \boxtimes\, \tau, \sigma}$, we can conclude that $\tilde{t} = \boxtimes\, \tau$ and then by SS-Fill, $\boxtimes\, \tau, \tilde{\sigma} \;\; \hookrightarrow \;\; \boxtimes\, \tau, \tilde{\sigma}$. Since the expressions do not change in this case, consistency holds trivially.

Case $t = \blacksquare\, l$

Provided that $\blacksquare\, l, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\text{S-Update}\ \dfrac{}{\blacksquare\, l, \sigma \mapsto \blacksquare\, l, \sigma}$, we can conclude that $\tilde{t} = \blacksquare\, l$ and then by SS-Update, $\blacksquare\, l, \tilde{\sigma} \;\; \hookrightarrow \;\; \blacksquare\, l, \tilde{\sigma}$. Since the expressions do not change in this case, consistency holds trivially.

Case $t = \lightning$

Provided that $\lightning, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\text{S-Fail}\ \dfrac{}{\lightning, \sigma \mapsto \lightning, \sigma}$, we can conclude that $\tilde{t} = \lightning$ and then by SS-Fail, $\lightning, \tilde{\sigma} \;\; \hookrightarrow \;\; \lightning, \tilde{\sigma}$. Since the expressions do not change in this case, consistency holds trivially.

Case $t = e_1 \lozenge e_2$

Provided that $e_1 \lozenge e_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\text{S-Xor}\ \dfrac{}{e_1 \lozenge e_2, \sigma \mapsto e_1 \lozenge e_2, \sigma}$, we can conclude that $\tilde{t} = \tilde{e}_1 \lozenge \tilde{e}_2$ and then by SS-Xor, $\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \;\; \hookrightarrow \;\; \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}$. Since the expressions do not change in this case, consistency holds trivially.

Case $t = t_1 \blacktriangleright e_2$

Three rules apply.

Case S-ThenStay

Provided that $t_1 \blacktriangleright e_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\dfrac{t_1, \sigma \mapsto t_1{}', \sigma'}{t_1 \blacktriangleright e_2, \sigma \mapsto t_1{}' \blacktriangleright e_2, \sigma'} \mathcal{V}(t_1{}', \sigma') = \bot$ (S-ThenStay), then by the induction hypothesis, we have $\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \tilde{t}_1', \tilde{\sigma}', \varphi$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi$. Then by SS-ThenStay, we have $\tilde{t}_1 \blacktriangleright \tilde{e}_2, \sigma \rightsquigarrow \tilde{t}_1' \blacktriangleright \tilde{e}_2, \sigma', \varphi$ and $t_1' \blacktriangleright e_2, \sigma' \leftrightarrows_M \tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \Phi \wedge \varphi$.

Case S-ThenFail

Provided that $t_1 \blacktriangleright e_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and

S-ThenFail
$$\frac{t_1, \sigma \mapsto t_1{}', \sigma' \qquad e_2\ v_1, \sigma' \downarrow t_2, \sigma''}{t_1 \blacktriangleright e_2, \sigma \mapsto t_1{}' \blacktriangleright e_2, \sigma'} \mathcal{V}(t_1{}', \sigma') = v_1 \wedge \mathcal{F}(t_2, \sigma'')$$

, then by the induction hypothesis, we have $\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \tilde{t}_1', \tilde{\sigma}', \varphi$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi$. Then by SS-ThenFail, we have $\tilde{t}_1 \blacktriangleright \tilde{e}_2, \sigma \rightsquigarrow \tilde{t}_1' \blacktriangleright \tilde{e}_2, \sigma', \varphi$ and $t_1' \blacktriangleright e_2, \sigma' \leftrightarrows_M \tilde{t}_1' \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \Phi \wedge \varphi$.

Case S-ThenCont

Provided that $t_1 \blacktriangleright e_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and

S-ThenCont
$$\frac{t_1, \sigma \mapsto t_1{}', \sigma' \qquad e_2\ v_1, \sigma' \downarrow t_2, \sigma''}{t_1 \blacktriangleright e_2, \sigma \mapsto t_2, \sigma''} \mathcal{V}(t_1{}', \sigma') = v_1 \wedge \neg\mathcal{F}(t_2, \sigma'')$$

, then by the induction hypothesis, we have $\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \tilde{t}_1', \tilde{\sigma}', \varphi$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$. Lemma 13 gives us that $\tilde{e}_2 \tilde{v}_1, \tilde{\sigma}' \wr \tilde{t}_2, \tilde{\sigma}'', \varphi_2$ and $t_2, \sigma'' \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. Then by SS-ThenCont, we have $\tilde{t}_1 \blacktriangleright \tilde{e}_2, \sigma \rightsquigarrow \tilde{t}_2, \sigma'', \varphi_1 \wedge \varphi_2$ and $t_2, \sigma'' \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $t = t_1 \blacklozenge t_2$

One of three rules applies.

Case S-OrLeft

Provided that $t_1 \blacklozenge t_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\dfrac{t_1, \sigma \mapsto t_1{}', \sigma'}{t_1 \blacklozenge t_2, \sigma \mapsto t_1{}', \sigma'} \mathcal{V}(t_1{}', \sigma') = v_1$ (S-OrLeft), then by the induction hypothesis, we have $\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \tilde{t}_1', \tilde{\sigma}', \varphi$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi$. Then by SS-OrLeft, we have $\tilde{t}_1 \blacklozenge \tilde{t}_2, \sigma \rightsquigarrow \tilde{t}_1', \sigma', \varphi$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi$.

Case S-OrRight

Provided that $t_1 \blacklozenge t_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and

S-OrRight
$$\frac{t_1, \sigma \mapsto t_1{}', \sigma' \qquad t_2, \sigma' \mapsto t_2{}', \sigma''}{t_1 \blacklozenge t_2, \sigma \mapsto t_2{}', \sigma''} \mathcal{V}(t_1{}', \sigma') = \bot \wedge \mathcal{V}(t_2{}', \sigma'') = v_2$$

, then by the induction hypothesis, we have $\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \tilde{t}_1', \tilde{\sigma}', \varphi$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$. A second application of the induction hypothesis gives us that $\tilde{t}_2, \tilde{\sigma}' \wr \tilde{t}_2', \tilde{\sigma}'', \varphi_2$ and $t_2', \sigma'' \leftrightarrows_M \tilde{t}_2', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. Then by SS-OrRight, we have $\tilde{t}_1 \blacklozenge \tilde{t}_2, \sigma \rightsquigarrow \tilde{t}_2', \sigma'', \varphi_1 \wedge \varphi_2$ and $t_2', \sigma'' \leftrightarrows_M \tilde{t}_2', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case S-OrNone

Provided that $t_1 \blacklozenge t_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and

$$\textsc{S-OrRight}\ \frac{t_1, \sigma \mapsto t_1{}', \sigma' \qquad t_2, \sigma' \mapsto t_2{}', \sigma''}{t_1 \blacklozenge t_2, \sigma \mapsto t_2{}', \sigma''}\ \mathcal{V}(t_1{}', \sigma') = \bot \wedge \mathcal{V}(t_2{}', \sigma'') = v_2$$

, then by the induction hypothesis, we have $\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \tilde{t}_1', \tilde{\sigma}', \varphi$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$. A second application of the induction hypothesis gives us that $\tilde{t}_2, \tilde{\sigma}' \wr \tilde{t}_2', \tilde{\sigma}'', \varphi_2$ and $t_2', \sigma'' \leftrightarrows_M \tilde{t}_2', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. Then by SS-OrNone, we have $\tilde{t}_1 \blacklozenge \tilde{t}_2, \sigma \rightsquigarrow \tilde{t}_1' \blacklozenge \tilde{t}_2', \sigma'', \varphi_1 \wedge \varphi_2$ and $t_1' \blacklozenge t_2', \sigma'' \leftrightarrows_M \tilde{t}_1' \blacklozenge \tilde{t}_2', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $t = t_1 \rhd e_2$

Provided that $t_1 \rhd e_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\textsc{S-Next}\ \dfrac{t_1, \sigma \mapsto t_1{}', \sigma'}{t_1 \rhd e_2, \sigma \mapsto t_1{}' \rhd e_2, \sigma'}$, then by the induction hypothesis, we have $\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \tilde{t}_1', \tilde{\sigma}', \varphi$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi$. Then by SS-Next, we have $\tilde{t}_1 \rhd \tilde{e}_2, \sigma \rightsquigarrow \tilde{t}_1', \sigma', \varphi$ and $t_1' \rhd e_2, \sigma' \leftrightarrows_M \tilde{t}_1' \rhd \tilde{e}_2, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $t = t_1 \bowtie t_2$

Provided that $t_1 \bowtie t_2, \sigma \leftrightarrows_M \tilde{t}, \tilde{\sigma}, \Phi$ and $\textsc{S-And}\ \dfrac{t_1, \sigma \mapsto t_1{}', \sigma' \qquad t_2, \sigma' \mapsto t_2{}', \sigma''}{t_1 \bowtie t_2, \sigma \mapsto t_1{}' \bowtie t_2{}', \sigma''}$, then by the induction hypothesis, we have $\tilde{t}_1, \tilde{\sigma} \rightsquigarrow \tilde{t}_1', \tilde{\sigma}', \varphi$ and $t_1', \sigma' \leftrightarrows_M \tilde{t}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$. A second application of the induction hypothesis gives us that $\tilde{t}_2, \tilde{\sigma}' \wr \tilde{t}_2', \tilde{\sigma}'', \varphi_2$ and $t_2', \sigma'' \leftrightarrows_M \tilde{t}_2', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. Then by SS-And, we have $\tilde{t}_1 \bowtie \tilde{t}_2, \sigma \rightsquigarrow \tilde{t}_1' \bowtie \tilde{t}_2', \sigma'', \varphi_1 \wedge \varphi_2$ and $t_1' \bowtie t_2', \sigma'' \leftrightarrows_M \tilde{t}_1' \bowtie \tilde{t}_2', \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Proof (Completeness of evaluate). We prove Lemma 13 by induction over e.

Case $e = v$

One rule applies, namely $\textsc{E-Value}\ \dfrac{}{v, \sigma \downarrow v, \sigma}$
Since $v, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$, we know that $\tilde{e} = \tilde{v}$. By SE-Value, we have $\tilde{v}, \tilde{\sigma} \mathrel{\tilde{\downarrow}} \tilde{v}, \tilde{\sigma}, \mathsf{True}$. Since the expressions did not change, this case holds trivially.

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

Provided that $\langle e_1, e_2 \rangle, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and $\textsc{E-Pair}\ \dfrac{e_1, \sigma \downarrow v_1, \sigma' \qquad e_2, \sigma' \downarrow v_2, \sigma''}{\langle e_1, e_2 \rangle, \sigma \downarrow \langle v_1, v_2 \rangle, \sigma''}$, then by application of the induction hypothesis we obtain $\tilde{e}_1, \tilde{\sigma} \mathrel{\tilde{\downarrow}} \tilde{v}_1, \tilde{\sigma}', \varphi_1$ and $v_1, \sigma' \leftrightarrows_M \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$. A second application of the induction hypothesis gives us $\tilde{e}_2, \tilde{\sigma}' \mathrel{\tilde{\downarrow}} \tilde{v}_2, \tilde{\sigma}'', \varphi_2$ and $v_2, \sigma'' \leftrightarrows_M \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_2$. By SE-Pair, we have $\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \mathrel{\tilde{\downarrow}} \langle \tilde{v}_1, \tilde{v}_2 \rangle, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2$ and $\langle v_1, v_2 \rangle, \sigma'' \leftrightarrows_M \langle \tilde{v}_1, \tilde{v}_2 \rangle, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $e = \mathsf{fst}\langle e_1, e_2 \rangle$

Provided that $\mathsf{fst}\langle e_1, e_2 \rangle, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and $\textsc{E-First}\ \dfrac{e_1, \sigma \downarrow v_1, \sigma'}{\mathsf{fst}\langle e_1, e_2 \rangle, \sigma \downarrow v_1, \sigma'}$, then by application of the induction hypothesis we obtain $\tilde{e}_1, \tilde{\sigma} \mathrel{\tilde{\downarrow}} \tilde{v}_1, \tilde{\sigma}', \varphi$ and $v_1, \sigma' \leftrightarrows_M \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi$. By SE-First, we have $\mathsf{fst}\langle \tilde{e}_1, \tilde{e}_2 \rangle, \tilde{\sigma} \mathrel{\tilde{\downarrow}} \tilde{v}_1, \tilde{\sigma}', \varphi$.

Case $e = \mathsf{snd}\langle e_1, e_2\rangle$

Provided that $\mathsf{snd}\langle e_1, e_2\rangle, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and $\dfrac{e_2, \sigma \downarrow v_2, \sigma'}{\mathsf{snd}\langle e_1, e_2\rangle, \sigma \downarrow v_2, \sigma'}$ E-Second, then by application of the induction hypothesis we obtain $\tilde{e}_2, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_2, \tilde{\sigma}', \varphi$ and $v_2, \sigma' \leftrightarrows_M \tilde{v}_2, \tilde{\sigma}', \Phi \wedge \varphi$. By SE-Second, we have $\mathsf{snd}\langle \tilde{e}_1, \tilde{e}_2\rangle, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_2, \tilde{\sigma}', \varphi$.

Case $e = e_1 :: e_2$

Provided that $e_1 :: e_2, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and $\dfrac{e_1, \sigma \downarrow v_1, \sigma' \qquad e_2, \sigma' \downarrow v_2, \sigma''}{e_1 :: e_2, \sigma \downarrow v_1 :: v_2, \sigma''}$ E-Cons, then by application of the induction hypothesis we obtain $\tilde{e}_1, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1, \tilde{\sigma}', \varphi_1$ and $v_1, \sigma' \leftrightarrows_M \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$. A second application of the induction hypothesis gives us $\tilde{e}_2, \tilde{\sigma}' \tilde{\downarrow} \tilde{v}_2, \tilde{\sigma}'', \varphi_2$ and $v_2, \sigma'' \leftrightarrows_M \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_2$. By SE-Cons, we have $\tilde{e}_1 :: \tilde{e}_2, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2$ and $v_1 :: v_2, \sigma'' \leftrightarrows_M \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

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

Provided that $\mathsf{head}\, e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and $\dfrac{e, \sigma \downarrow v_1 :: v_2, \sigma'}{\mathsf{head}\, e, \sigma \downarrow v_1, \sigma'}$ E-Head, then by application of the induction hypothesis we obtain $\tilde{e}, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}', \varphi$ and $v_1 :: v_2, \sigma' \leftrightarrows_M \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}', \Phi \wedge \varphi$. By SE-Head, we have $\tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1, \tilde{\sigma}', \varphi$.

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

Provided that $\mathsf{tail}\, e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and $\dfrac{e, \sigma \downarrow v_1 :: v_2, \sigma'}{\mathsf{tail}\, e, \sigma \downarrow v_2, \sigma'}$ E-Tail, then by application of the induction hypothesis we obtain $\tilde{e}, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}', \varphi$ and $v_1 :: v_2, \sigma' \leftrightarrows_M \tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma}', \Phi \wedge \varphi$. By SE-Tail, we have $\tilde{v}_1 :: \tilde{v}_2, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_2, \tilde{\sigma}', \varphi$.

Case $e = e_1 e_2$

Provided that $e_1 e_2, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and

E-App
$$\dfrac{e_1, \sigma \ \downarrow\ \lambda x : \tau . e_1', \sigma' \qquad e_2, \sigma' \ \downarrow\ v_2, \sigma'' \qquad e_1'[x \mapsto v_2], \sigma'' \ \downarrow\ v_1, \sigma'''}{e_1 e_2, \sigma \ \downarrow\ v_1, \sigma'''}$$
, then by application of the induction hypothesis we obtain $\tilde{e}_1, \tilde{\sigma} \tilde{\downarrow} \lambda x : \tau . \tilde{e}_1', \tilde{\sigma}', \varphi_1$ and $\lambda x : \tau . e_1', \sigma' \leftrightarrows_M \lambda x : \tau . \tilde{e}_1', \tilde{\sigma}', \Phi \wedge \varphi_1$. A second application of the induction hypothesis gives us $\tilde{e}_2, \tilde{\sigma}' \tilde{\downarrow} \tilde{v}_2, \tilde{\sigma}'', \varphi_2$ and $v_2, \sigma'' \leftrightarrows_M \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. Then finally by a third application of the induction hypothesis, we get $\tilde{e}_1'[x \mapsto \tilde{v}_2], \tilde{\sigma}'' \tilde{\downarrow} \tilde{v}_1, \tilde{\sigma}''', \varphi_3$ and $v_1, \sigma''' \leftrightarrows_M \tilde{v}_1, \tilde{\sigma}''', \Phi \wedge \varphi_1 \wedge \varphi_2 \wedge \varphi_3$. By SE-App, we have $\tilde{e}_1 \tilde{e}_2, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1, \tilde{\sigma}''', \varphi_1 \wedge \varphi_2 \wedge \varphi_2$.

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

Case 1

Provided that $\textbf{if}\, e_1\, \textbf{then}\, e_2\, \textbf{else}\, e_3, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and E-IfTrue $\dfrac{e_1, \sigma \downarrow \mathsf{True}, \sigma' \quad e_2, \sigma' \downarrow v_2, \sigma''}{\textbf{if}\, e_1\, \textbf{then}\, e_2\, \textbf{else}\, e_3, \sigma \downarrow v_2, \sigma''}$, then by application of the induction hypothesis we obtain $\tilde{e}_1, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1, \tilde{\sigma}', \varphi_1$ and $\mathsf{True}, \sigma' \leftrightarrows_M \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$. A second application of the induction hypothesis gives us $\tilde{e}_2, \tilde{\sigma}' \tilde{\downarrow} \tilde{v}_2, \tilde{\sigma}'', \varphi_2$ and $v_2, \sigma'' \leftrightarrows_M \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. By SE-If, we have $\textbf{if}\, \tilde{e}_1\, \textbf{then}\, \tilde{e}_2\, \textbf{else}\, \tilde{e}_3, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2 \wedge \tilde{v}_1$.

Case 2

Provided that $\textbf{if}\, e_1\, \textbf{then}\, e_2\, \textbf{else}\, e_3, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and E-IfFalse $\dfrac{e_1, \sigma \downarrow v_1, \sigma' \quad e_3, \sigma' \downarrow v_3, \sigma''}{\textbf{if}\, e_1\, \textbf{then}\, e_2\, \textbf{else}\, e_3, \sigma \downarrow v_3, \sigma''}$, then by application of the induction hypothesis we obtain $\tilde{e}_1, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_1, \tilde{\sigma}', \varphi_1$ and $\mathsf{False}, \sigma' \leftrightarrows_M \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$. A second application of the induction hypothesis gives us $\tilde{e}_3, \tilde{\sigma}' \tilde{\downarrow} \tilde{v}_3, \tilde{\sigma}'', \varphi_2$ and $v_3, \sigma'' \leftrightarrows_M \tilde{v}_3, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$. By SE-If, we have $\textbf{if}\, \tilde{e}_1\, \textbf{then}\, \tilde{e}_2\, \textbf{else}\, \tilde{e}_3, \tilde{\sigma} \tilde{\downarrow} \tilde{v}_3, \tilde{\sigma}'', \varphi_1 \wedge \varphi_3 \wedge \neg\tilde{v}_1$.

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

Provided that $\textbf{ref}\, e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and E-Ref $\dfrac{e, \sigma \downarrow v, \sigma' \quad l \notin Dom(\sigma')}{\textbf{ref}\, e, \sigma \downarrow l, \sigma'[l \mapsto v]}$, then by application of the induction hypothesis we obtain $\tilde{e}, \tilde{\sigma} \tilde{\downarrow} \tilde{v}, \tilde{\sigma}', \varphi$ and $v, \sigma' \leftrightarrows_M \tilde{v}, \tilde{\sigma}', \Phi \wedge \varphi$. By SE-Ref, we have $\textbf{ref}\, \tilde{e}, \tilde{\sigma} \tilde{\downarrow} l, \tilde{\sigma}'[l \mapsto \tilde{v}], \varphi$ and $l, \sigma'[l \mapsto v] \leftrightarrows_M l, \tilde{\sigma}'[f \mapsto \tilde{v}], \Phi \wedge \varphi$.

Case $e = !e$

Provided that $!e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and E-Deref $\dfrac{e, \sigma \downarrow l, \sigma'}{!e, \sigma \downarrow \sigma'(l), \sigma'}$, then by application of the induction hypothesis we obtain $\tilde{e}, \tilde{\sigma} \tilde{\downarrow} l, \tilde{\sigma}', \varphi$ and $l, \sigma' \leftrightarrows_M l, \tilde{\sigma}', \Phi \wedge \varphi$. By SE-Deref, we have $!\tilde{e}, \tilde{\sigma} \tilde{\downarrow} \tilde{\sigma}'(l), \tilde{\sigma}', \varphi$ and $\sigma'(l), \sigma' \leftrightarrows_M \tilde{\sigma}'(l), \tilde{\sigma}', \Phi \wedge \varphi$.

Case $e = e_1 := e_2$

Provided that $e_1 := e_2, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and E-Assign $\dfrac{e_1, \sigma \downarrow l, \sigma' \quad e_2, \sigma' \downarrow v_2, \sigma''}{e_1 := e_2, \sigma \downarrow \langle\rangle, \sigma''[l \mapsto v_2]}$, then by application of the induction hypothesis we obtain $\tilde{e}_1, \tilde{\sigma} \tilde{\downarrow} l, \tilde{\sigma}', \varphi_1$ and $l, \sigma' \leftrightarrows_M l, \tilde{\sigma}', \Phi \wedge \varphi_1$. A second application of the induction hypothesis gives us $\tilde{e}_2, \tilde{\sigma}' \tilde{\downarrow} \tilde{v}_2, \tilde{\sigma}'', \varphi_2$ and $v_2, \sigma'' \leftrightarrows_M \tilde{v}_2, \tilde{\sigma}'', \Phi \wedge \varphi_2$. By SE-Assign, we have $\tilde{e}_1 := \tilde{e}_2, \tilde{\sigma} \tilde{\downarrow} \langle\rangle, \tilde{\sigma}''[l \mapsto \tilde{v}_2], \varphi_1 \wedge \varphi_2$ and $\textsc{Unit}, \sigma''[l \mapsto v_2] \leftrightarrows_M \textsc{Unit}, \tilde{\sigma}''[l \mapsto \tilde{v}_2], \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $e = \Box\, e$

Provided that $\Box\, e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and E-Edit $\dfrac{e, \sigma \downarrow v, \sigma'}{\Box\, e, \sigma \downarrow \Box\, v, \sigma'}$, then by application of the induction hypothesis we obtain $\tilde{e}, \tilde{\sigma} \tilde{\downarrow} \tilde{v}, \tilde{\sigma}', \varphi$ and $v, \sigma' \leftrightarrows_M \tilde{v}, \tilde{\sigma}', \Phi \wedge \varphi$. By SE-Edit, we have $\Box\, \tilde{e}, \tilde{\sigma} \tilde{\downarrow} \Box\, \tilde{v}, \tilde{\sigma}', \varphi$ and $\Box\, v, \sigma' \leftrightarrows_M \Box\, \tilde{v}, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $e = \boxtimes\,\tau$

One rule applies, namely $\dfrac{}{\boxtimes\,\tau, \sigma \downarrow \boxtimes\,\tau, \sigma}$ E-Enter. Since $\boxtimes\,\tau, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$, we know that $\tilde{e} = \boxtimes\,\tau$. By SE-Enter, we have $\boxtimes\,\tau, \tilde{\sigma} \mathrel{\tilde{\downarrow}} \boxtimes\,\tau, \tilde{\sigma}, \mathsf{True}$. Since the expressions did not change, this case holds trivially.

Case $e = \blacksquare\, e$

Provided that $\blacksquare\, e, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and $\dfrac{e, \sigma \downarrow l, \sigma'}{\blacksquare\, e, \sigma \downarrow \blacksquare\, l, \sigma'}$ E-Update, then by application of the induction hypothesis we obtain $\tilde{e}, \tilde{\sigma} \mathrel{\tilde{\downarrow}} l, \tilde{\sigma}', \varphi$ and $l, \sigma' \leftrightarrows_M l, \tilde{\sigma}', \Phi \wedge \varphi$. By SE-Update, we have $\blacksquare\, \tilde{e}, \tilde{\sigma} \mathrel{\tilde{\downarrow}} \blacksquare\, l, \tilde{\sigma}', \varphi$ and $\blacksquare\, l, \sigma' \leftrightarrows_M \blacksquare\, l, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $e = e_1 \blacktriangleright e_2$

Provided that $e_1 \blacktriangleright e_2, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and $\dfrac{e_1, \sigma \downarrow t_1, \sigma'}{e_1 \blacktriangleright e_2, \sigma \downarrow t_1 \blacktriangleright e_2, \sigma'}$ E-Then, then by application of the induction hypothesis we obtain $\tilde{e}_1, \tilde{\sigma} \mathrel{\tilde{\downarrow}} \tilde{v}_1, \tilde{\sigma}', \varphi$ and $v_1, \sigma' \leftrightarrows_M \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi$. By SE-Then, we have $\tilde{e}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma} \mathrel{\tilde{\downarrow}} \tilde{v}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \varphi$ and $v_1 \blacktriangleright e_2, \sigma' \leftrightarrows_M \tilde{v}_1 \blacktriangleright \tilde{e}_2, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $e = e_1 \triangleright e_2$

Provided that $e_1 \triangleright e_2, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and $\dfrac{e_1, \sigma \downarrow t_1, \sigma'}{e_1 \triangleright e_2, \sigma \downarrow t_1 \triangleright e_2, \sigma'}$ E-Next, then by application of the induction hypothesis we obtain $\tilde{e}_1, \tilde{\sigma} \mathrel{\tilde{\downarrow}} \tilde{v}_1, \tilde{\sigma}', \varphi$ and $v_1, \sigma' \leftrightarrows_M \tilde{v}_1, \tilde{\sigma}', \Phi \wedge \varphi$. By SE-Next, we have $\tilde{e}_1 \triangleright \tilde{e}_2, \tilde{\sigma} \mathrel{\tilde{\downarrow}} \tilde{v}_1 \triangleright \tilde{e}_2, \tilde{\sigma}', \varphi$ and $v_1 \blacktriangleright e_2, \sigma' \leftrightarrows_M \tilde{v}_1 \triangleright \tilde{e}_2, \tilde{\sigma}', \Phi \wedge \varphi$.

Case $e = e_1 \blacklozenge e_2$

Provided that $e_1 \blacklozenge e_2, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$ and $\dfrac{e_1, \sigma \downarrow t_1, \sigma' \qquad e_2, \sigma' \downarrow t_2, \sigma''}{e_1 \blacklozenge e_2, \sigma \downarrow t_1 \blacklozenge t_2, \sigma''}$ E-Or, then by application of the induction hypothesis we obtain $\tilde{e}_1, \tilde{\sigma} \mathrel{\tilde{\downarrow}} \tilde{t}_1, \tilde{\sigma}', \varphi_1$ and $t_1, \sigma' \leftrightarrows_M \tilde{t}_1, \tilde{\sigma}', \Phi \wedge \varphi_1$.

A second application of the induction hypothesis gives us $\tilde{e}_2, \tilde{\sigma}' \mathrel{\tilde{\downarrow}} \tilde{t}_2, \tilde{\sigma}'', \varphi_2$ and $t_2, \sigma'' \leftrightarrows_M \tilde{t}_2, \tilde{\sigma}'', \Phi \wedge \varphi_2$. By SE-Or, we have $\tilde{e}_1 \blacklozenge \tilde{e}_2, \tilde{\sigma} \mathrel{\tilde{\downarrow}} \tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}'', \varphi_1 \wedge \varphi_2$ and $t_1 \blacklozenge t_2, \sigma'' \leftrightarrows_M \tilde{t}_1 \blacklozenge \tilde{t}_2, \tilde{\sigma}'', \Phi \wedge \varphi_1 \wedge \varphi_2$.

Case $e = e_1 \lozenge e_2$

One rule applies, namely $\dfrac{}{e_1 \lozenge e_2, \sigma \downarrow e_1 \lozenge e_2, \sigma}$ E-Xor. Since $e_1 \lozenge e_2, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$, we know that $\tilde{e} = \tilde{e}_1 \lozenge \tilde{e}_2$. By SE-Xor, we have $\tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma} \mathrel{\tilde{\downarrow}} \tilde{e}_1 \lozenge \tilde{e}_2, \tilde{\sigma}, \mathsf{True}$. Since the expressions did not change, this case holds trivially.

Case $e = \lightning$

One rule applies, namely $\dfrac{\textsc{E-Fail}}{\lightning, \sigma \downarrow \lightning, \sigma}$. Since $\lightning, \sigma \leftrightarrows_M \tilde{e}, \tilde{\sigma}, \Phi$, we know that $\tilde{e} = \lightning$. By SE-Fail, we have $\lightning, \tilde{\sigma} \tilde{\downarrow} \lightning, \tilde{\sigma}, \mathsf{True}$. Since the expressions did not change, this case holds trivially.