Separation Logic in the Presence of Garbage Collection

Technical Appendix

Chung-Kil Hur Derek Dreyer Viktor Vafeiadis

Max Planck Institute for Software Systems (MPI-SWS)

`{gil,dreyer,viktor}@mpi-sws.org`

April 2011

Contents

1 Language

1.1 Storage Model

$$\begin{array}{lcl}
\text{ProgVars} & \stackrel{\text{def}}{=} & \{\, \mathtt{x}, \mathtt{y}, \ldots \,\} \\
\text{Words} & \stackrel{\text{def}}{=} & \{\, w \in \mathbb{Z} \,\} \\
\text{Ptrs} & \stackrel{\text{def}}{=} & \{\, p \in \text{Words} \mid p > 0 \wedge p \text{ is a multiple of } 4 \,\} \\
\text{NonPtrs} & \stackrel{\text{def}}{=} & \{\, a \in \text{Words} \setminus \text{Ptrs} \,\} \\
\text{Stores} & \stackrel{\text{def}}{=} & \{\, s \in \text{ProgVars} \to \text{Words} \,\} \\
\text{Heaps} & \stackrel{\text{def}}{=} & \{\, h \in \text{Ptrs} \rightharpoonup_{\text{fin}} \text{Words} \,\}
\end{array}$$

1.2 Syntax

Expressions

$$\begin{array}{rcl}
E \in \text{Exps} & ::= & \mathtt{x} \\
& \mid & w \\
& \mid & E \star E \\
& \mid & \mathsf{not}\ E
\end{array}$$

where $\mathtt{x} \in \text{ProgVars}, w \in \text{Words}$ and $\star \in \{\, +, -, \times, \div, <, =, \mathsf{and} \,\}$

$$\begin{array}{lcl}
E_1 \ \mathsf{or}\ E_2 & \stackrel{\text{def}}{=} & \mathsf{not}\ (\mathsf{not}\ E_1 \ \mathsf{and}\ \mathsf{not}\ E_2) \\
E_1 \neq E_2 & \stackrel{\text{def}}{=} & \mathsf{not}\ (E_1 = E_2) \\
E_1 \leq E_2 & \stackrel{\text{def}}{=} & (E_1 = E_2) \ \mathsf{or}\ (E_1 < E_2) \\
\mathsf{ENC}(E) & \stackrel{\text{def}}{=} & 2 \times E + 1
\end{array}$$

Commands

$$\begin{array}{rcl}
C & ::= & \mathtt{x} := E \\
& \mid & \mathtt{x} := [E] \\
& \mid & [E] := E \\
& \mid & \mathsf{skip} \\
& \mid & \mathsf{if}\ E\ \mathsf{then}\ C\ \mathsf{else}\ C\ \mathsf{fi} \\
& \mid & \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od} \\
& \mid & C; C \\
& \mid & \mathsf{alloc}\ \mathtt{x}
\end{array}$$

where $\mathtt{x} \in \text{ProgVars}$ and $i \in \mathbb{N}$

$$\mathtt{x} := \mathsf{ALLOC}(E) \stackrel{\text{def}}{=} \mathtt{x} := E;\ \mathsf{alloc}\ \mathtt{x}$$

$\boxed{\text{Free variables}}$

$$
\begin{aligned}
\mathrm{FPV}(E) &\overset{\text{def}}{=} \text{the set of program variables appearing in the expression } E\\
\mathrm{FPV}(C) &\overset{\text{def}}{=} \text{the set of program variables appearing in the command } C\\
\mathrm{Mod}(C) &\overset{\text{def}}{=} \begin{cases} \{\,\mathtt{x}\,\} & \text{if } C = (\mathtt{x} := E) \vee C = (\mathtt{x} := [E]) \vee C = \mathsf{alloc}\ \mathtt{x}\\ \mathrm{Mod}(C') & \text{if } C = \mathsf{while}\ E\ \mathsf{do}\ C'\ \mathsf{od}\\ \mathrm{Mod}(C') \cup \mathrm{Mod}(C'') & \text{if } C = \mathsf{if}\ E\ \mathsf{then}\ C'\ \mathsf{else}\ C''\ \mathsf{fi} \vee C = C'; C''\\ \emptyset & \text{otherwise} \end{cases}
\end{aligned}
$$

1.3 Operational Semantics

$\boxed{[\![E]\!] \in \text{Stores} \rightharpoonup \text{Words}}$

$$
\begin{aligned}
[\![\mathtt{x}]\!]_s &::= s(\mathtt{x})\\
[\![w]\!]_s &::= w\\
[\![E_1 \star E_2]\!]_s &::= \begin{cases} w_1 \star w_2 & \text{if } [\![E_1]\!]_s = w_1 \wedge [\![E_2]\!]_s = w_2\\ \text{undef} & \text{otherwise} \end{cases}
\end{aligned}
$$

where $\star \in \{\, +, -, \times, \div, <, =, \mathsf{and}\,\}, w \div 0 = \text{undef}$,

$w_1 < w_2 \overset{\text{def}}{=} 1$ if $w_1 < w_2$; 0 otherwise,

$w_1 = w_2 \overset{\text{def}}{=} 1$ if $w_1 = w_2$; 0 otherwise,

$w_1\ \mathsf{and}\ w_2 \overset{\text{def}}{=} 1$ if $w_1 \neq 0 \wedge w_2 \neq 0$; 0 otherwise

$$
[\![\mathsf{not}\ E]\!]_s ::= \begin{cases} \mathsf{not}\ w & \text{if } [\![E]\!]_s = w\\ \text{undef} & \text{otherwise} \end{cases}
$$

where $\mathsf{not}\ w \overset{\text{def}}{=} 1$ if $w = 0$; 0 otherwise

$\boxed{C, s, h \rightsquigarrow C', s', h'}$

$$
\frac{[\![E]\!]_s \neq \text{undef}}{\mathtt{x} := E, s, h \rightsquigarrow \mathsf{skip}, (s \mid \mathtt{x} \mapsto [\![E]\!]_s), h}
$$

$$
\frac{[\![E]\!]_s = p \in \mathrm{dom}(h)}{\mathtt{x} := [E], s, h \rightsquigarrow \mathsf{skip}, (s \mid \mathtt{x} \mapsto h(p)), h}
$$

$$
\frac{[\![E]\!]_s = p \in \mathrm{dom}(h) \qquad [\![E']\!]_s \neq \text{undef}}{[E] := E', s, h \rightsquigarrow \mathsf{skip}, s, (h \mid p \mapsto [\![E']\!]_s)}
$$

$$
\frac{[\![E]\!]_s \in \text{Words}\backslash\{0\}}{\mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}, s, h \rightsquigarrow C_1, s, h}
$$

$$
\frac{[\![E]\!]_s = 0}{\mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}, s, h \rightsquigarrow C_2, s, h}
$$

$$
\frac{[\![E]\!]_s = 0}{\mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}, s, h \rightsquigarrow \mathsf{skip}, s, h}
$$

$$
\frac{[\![E]\!]_s \in \text{Words}\backslash\{0\}}{\mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}, s, h \rightsquigarrow (C; \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}), s, h}
$$

$$
\frac{}{(\mathsf{skip}; C), s, h \rightsquigarrow C, s, h} \qquad \frac{C_1, s, h \rightsquigarrow C_1', s', h'}{(C_1; C_2), s, h \rightsquigarrow (C_1'; C_2), s', h'}
$$

Notation

$$\begin{array}{ll}
C, s, h \rightsquigarrow - & \text{iff}\ \ \exists C', s', h'.\ C, s, h \rightsquigarrow C', s', h' \\
C, s, h \text{ diverges} & \text{iff}\ \ \exists \{\, C_i, s_i, h_i \,\}_{i \in \mathbb{N}}.\ (C_0, s_0, h_0) = (C, s, h) \wedge \forall i.\ C_i, s_i, h_i \rightsquigarrow C_{i+1}, s_{i+1}, h_{i+1}
\end{array}$$

1.4 Garbage Collector Specification

$$\begin{array}{lll}
\text{Shapes} & := & \{\, \sigma \in \text{Ptrs} \rightharpoonup_{\text{fin}} \mathbb{N}^+ \,\} \\
\overline{\text{dom}}(\sigma) & := & \biguplus_{p \in \text{dom}(\sigma)} \{\, p + 4 \times 0, \ldots, p + 4(\sigma(p) - 1) \,\} \\
\text{roots}(s) & \overset{\text{def}}{=} & \{\, p \in \text{Ptrs} \mid \exists \mathtt{x}.\ p = s(\mathtt{x}) \,\} \\
\text{reach}_0(R, h, \sigma) & \overset{\text{def}}{=} & R \\
\text{reach}_{n+1}(R, h, \sigma) & \overset{\text{def}}{=} & \text{reach}_n(R, h, \sigma) \cup \\
 & & \{\, p \in \text{Ptrs} \mid \exists p' \in \text{reach}_n(R, h, \sigma).\ \exists i < \sigma(p').\ p = h(p' + 4i) \,\} \\
\text{reach}(R, h, \sigma) & \overset{\text{def}}{=} & \bigcup_{n \in \mathbb{N}} \text{reach}_n(R, h, \sigma) \\
(s, h, \sigma) \cong (s', h', \sigma') & \overset{\text{def}}{=} & \exists r \in \text{Bij}(\text{reach}(\text{roots}(s), h, \sigma), \text{reach}(\text{roots}(s'), h', \sigma')). \\
 & & \quad \big(\forall \mathtt{x}.\ (s(\mathtt{x}), s'(\mathtt{x})) \in \overline{r}\ \big) \wedge \\
 & & \quad \big(\forall (p, p') \in r.\ \exists n.\ \sigma(p) = \sigma'(p') = n \wedge \forall i.\ 0 \le i < n \implies (h(p + 4i), h'(p' + 4i)) \in \overline{r}\big) \\
 & & \text{where } \overline{r} \overset{\text{def}}{=} r \cup \{\, (a, a) \mid a \in \text{NonPtrs} \,\}
\end{array}$$

$$[p \mapsto_n w_0, \ldots, w_{n-1}] \overset{\text{def}}{=} (\emptyset \mid p + 4 \times 0 \mapsto w_0 \mid \ldots \mid p + 4(n-1) \mapsto w_{n-1}) \quad \in \text{Heaps}$$

$$[p \mapsto n] \overset{\text{def}}{=} \begin{cases} (\emptyset \mid p \mapsto n) & \text{if } n > 0 \wedge p \in \text{Ptrs} \\ \emptyset & \text{if } n = 0 \wedge p = 0 \\ \text{undef} & \text{otherwise} \end{cases} \quad \in \text{Shapes}$$

Note that if $n = 0$ and $[p \mapsto n]$ is defined, then $p = 0$.

$$\begin{array}{l}
I_{\text{gc}} \ \in\ \mathbb{P}_{\text{fin}}(\text{Ptrs}) \times \text{Heaps} \rightharpoonup \text{Shapes} \quad \text{satisfying} \\
\qquad (\text{GCAxiom}_1) \\
\qquad\quad \forall R, h, \sigma = I_{\text{gc}}(R, h). \\
\qquad\qquad \overline{\text{dom}}(\sigma) \subseteq \text{dom}(h) \wedge \text{reach}(R, h, \sigma) \subseteq \text{dom}(\sigma) \\
\qquad (\text{GCAxiom}_2) \\
\qquad\quad \forall R, h, \sigma = I_{\text{gc}}(R, h). \\
\qquad\quad \forall R', h'.\ \overline{\text{dom}}(\sigma) \subseteq \text{dom}(h') \wedge \text{reach}(R', h', \sigma) \subseteq \text{dom}(\sigma) \wedge (\forall p \notin \overline{\text{dom}}(\sigma).\ h'(p) = h(p)) \implies \\
\qquad\qquad \exists \sigma' \subseteq \sigma.\ \sigma' = I_{\text{gc}}(R', h')
\end{array}$$

$$\begin{array}{l}
\forall s, h, \sigma, \mathtt{x}, n.\ \ \sigma = I_{\text{gc}}(\text{roots}(s), h) \wedge s(\mathtt{x}) = 2n + 1 \wedge n \ge 0 \implies \\
\quad (\mathsf{alloc}\ \mathtt{x}, s, h \rightsquigarrow -) \wedge \\
\quad (\forall C', s', h'.\ \mathsf{alloc}\ \mathtt{x}, s, h \rightsquigarrow C', s', h' \implies \\
\qquad \exists p, h'', \sigma''.\ C' = \mathsf{skip} \wedge \sigma'' \uplus [p \mapsto n] = I_{\text{gc}}(\text{roots}(s'), h') \wedge s'(\mathtt{x}) = p \wedge h' = h'' \uplus [p \mapsto_n 0, \ldots, 0] \wedge \\
\qquad\qquad\qquad (s, h, \sigma) \cong ((s' \mid \mathtt{x} \mapsto 2n + 1), h'', \sigma''))
\end{array}$$

2 Program Specifications

2.1 Logical Storage Model

$$
\begin{array}{lll}
\mathrm{Locs} & \overset{\mathrm{def}}{=} & \{\, \boldsymbol{\ell} \in \{\, \mathrm{loc}_1, \mathrm{loc}_2, \ldots \,\} \,\} \\
\mathrm{LogPtrs} & \overset{\mathrm{def}}{=} & \{\, \boldsymbol{\ell} \,\widehat{+}\, i \mid \boldsymbol{\ell} \in \mathrm{Locs} \wedge i \in \mathbb{Z} \,\} \\
\mathrm{LogVals} & \overset{\mathrm{def}}{=} & \{\, \mathbf{v} \in \mathrm{LogPtrs} \uplus \mathrm{Words} \,\} \\
\mathrm{LStores} & \overset{\mathrm{def}}{=} & \{\, \mathbf{s} \in \mathrm{ProgVars} \to \mathrm{LogVals} \,\} \\
\mathrm{Span}(\mathbf{h}) & \overset{\mathrm{def}}{=} & \{\, (\boldsymbol{\ell}, i) \in \mathrm{Locs} \times \mathbb{N} \mid i \in \mathrm{dom}(\mathbf{h}(\boldsymbol{\ell})) \,\} \quad \text{for } \mathbf{h} \in \mathrm{Locs} \to (\mathbb{N} \rightharpoonup_{\mathrm{fin}} \mathrm{LogVals}) \\
\mathrm{LHeaps} & \overset{\mathrm{def}}{=} & \{\, \mathbf{h} \in \mathrm{Locs} \to \mathbb{N} \rightharpoonup_{\mathrm{fin}} \mathrm{LogVals} \mid \mathrm{Span}(\mathbf{h}) \text{ is finite} \,\} \\
\mathrm{Table} & \overset{\mathrm{def}}{=} & \{\, \mathbf{T} \in \mathrm{Locs} \rightharpoonup_{\mathrm{fin}} \mathrm{Ptrs} \times \mathbb{N}^{+} \,\} \\
\mathrm{phyv}_{\mathbf{T}}(\mathbf{v}) & \overset{\mathrm{def}}{=} & \begin{cases} w & \text{if } \mathbf{v} = w \in \mathrm{Words} \\ p + i & \text{if } \mathbf{v} = \boldsymbol{\ell} \,\widehat{+}\, i \wedge \mathbf{T}(\boldsymbol{\ell}) = (p, n) \\ \mathrm{undef} & \text{otherwise} \end{cases} \\
\mathrm{phyh}_{\mathbf{T}}(\mathbf{h}) & \overset{\mathrm{def}}{=} & \biguplus_{(p,n)=\mathbf{T}(\boldsymbol{\ell})} \; [p \mapsto_n \mathrm{phyv}_{\mathbf{T}}(\mathbf{h}(\boldsymbol{\ell})(0)), \ldots, \mathrm{phyv}_{\mathbf{T}}(\mathbf{h}(\boldsymbol{\ell})(n-1))] \\
\mathrm{shape}(\mathbf{T}) & \overset{\mathrm{def}}{=} & \biguplus_{(p,n)=\mathbf{T}(\boldsymbol{\ell})} \; [p \mapsto n] \\
\mathrm{Safe}(\mathbf{L}) & \overset{\mathrm{def}}{=} & \{\, \boldsymbol{\ell} \,\widehat{+}\, 0 \mid \boldsymbol{\ell} \in \mathbf{L} \,\} \cup \mathrm{NonPtrs} \qquad \text{for } \mathbf{L} \subseteq \mathrm{Locs} \\
\mathbf{s} \sim_{\mathbf{T}} s & \text{iff} & \forall \mathtt{x}.\ s(\mathtt{x}) = \mathrm{phyv}_{\mathbf{T}}(\mathbf{s}(\mathtt{x})) \\
\mathbf{s} \approx_{\mathbf{T}} s & \text{iff} & \mathbf{s} \sim_{\mathbf{T}} s \wedge \forall \mathtt{x}.\ \mathbf{s}(\mathtt{x}) \in \mathrm{Safe}(\mathrm{dom}(\mathbf{T})) \\
\mathbf{h} : \mathbf{T} & \text{iff} & \forall \boldsymbol{\ell}.\ \forall (p, n) = \mathbf{T}(\boldsymbol{\ell}).\ \mathrm{dom}(\mathbf{h}(\boldsymbol{\ell})) = \{\, 0, \ldots, n-1 \,\} \\
\mathbf{h} \sim_{\mathbf{T}} h & \text{iff} & \mathbf{h} : \mathbf{T} \wedge \mathrm{phyh}_{\mathbf{T}}(\mathbf{h}) \subseteq h \\
\mathbf{h} :: \mathbf{T} & \text{iff} & \forall \boldsymbol{\ell}.\ \forall (p, n) = \mathbf{T}(\boldsymbol{\ell}).\ \forall i < n.\ \mathbf{h}(\boldsymbol{\ell})(i) \in \mathrm{Safe}(\mathrm{dom}(\mathbf{T})) \\
\mathbf{h} \approx_{\mathbf{T}} h & \text{iff} & \mathbf{h} \sim_{\mathbf{T}} h \wedge \mathbf{h} :: \mathbf{T} \wedge \mathrm{shape}(\mathbf{T}) \subseteq I_{\mathrm{gc}}(\mathrm{dom}(\mathrm{shape}(\mathbf{T})), h) \\
\mathbf{h}_1 \# \mathbf{h}_2 & \overset{\mathrm{def}}{=} & \mathrm{Span}(\mathbf{h}_1) \cap \mathrm{Span}(\mathbf{h}_2) = \emptyset \\
\mathbf{h}_1 \uplus \mathbf{h}_2 & \overset{\mathrm{def}}{=} & \begin{cases} \lambda \boldsymbol{\ell}.\ \mathbf{h}_1(\boldsymbol{\ell}) \uplus \mathbf{h}_2(\boldsymbol{\ell}) & \text{if } \mathbf{h}_1 \# \mathbf{h}_2 \\ \mathrm{undef} & \text{otherwise} \end{cases}
\end{array}
$$

2.2 Syntax

Logical Expressions

$$
\begin{array}{lcl}
\text{LogVars} & \overset{\text{def}}{=} & \{\, u, v, \ldots \,\} \\
\mathbf{E} \in \text{LExps} & ::= & v \\
 & | & \mathsf{x} \\
 & | & \mathbf{v} \\
 & | & \mathbf{E} \star \mathbf{E} \\
 & | & \mathsf{not}\ \mathbf{E}
\end{array}
$$

where $v \in \text{LogVars}, \mathsf{x} \in \text{ProgVars}, \mathbf{v} \in \text{LogVals}$ and $\star \in \{\, +, -, \times, \div, <, =, \mathsf{and} \,\}$

Note that Exps $\subseteq$ LExps.

Assertions

$$
\begin{array}{rcl}
P \in \text{Asserts} & := & \mathbf{E} \\
 & | & \mathbf{E} \hookrightarrow \mathbf{E} \;\;|\;\; P * P \;\;|\;\; P \mathrel{-\!\!*} P \\
 & | & P \Rightarrow P \;\;|\;\; P \wedge P \;\;|\;\; P \vee P \\
 & | & \forall v.\, P \;\;|\;\; \exists v.\, P
\end{array}
$$

Assertions with safety

$$
\begin{array}{rcl}
\mathbf{P} \in \text{AssertsL} & := & \mathsf{safe}(\mathbf{E}) \\
 & | & \mathbf{E} \\
 & | & \mathbf{E} \hookrightarrow \mathbf{E} \;\;|\;\; \mathbf{P} * \mathbf{P} \;\;|\;\; \mathbf{P} \mathrel{-\!\!*} \mathbf{P} \\
 & | & \mathbf{P} \Rightarrow \mathbf{P} \;\;|\;\; \mathbf{P} \wedge \mathbf{P} \;\;|\;\; \mathbf{P} \vee \mathbf{P} \\
 & | & \forall v.\, \mathbf{P} \;\;|\;\; \exists v.\, \mathbf{P}
\end{array}
$$

$$
\begin{array}{lcl}
\multicolumn{3}{l}{\mathsf{false} \overset{\text{def}}{=} 0; \quad \mathsf{true} \overset{\text{def}}{=} 1; \quad \neg\mathbf{P} \overset{\text{def}}{=} \mathbf{P} \Rightarrow \mathsf{false}} \\
\mathsf{defined}(\mathbf{E}) & \overset{\text{def}}{=} & \mathbf{E} = \mathbf{E} \\
\mathsf{word}(\mathbf{E}) & \overset{\text{def}}{=} & \mathbf{E} = 0 \vee \mathbf{E} \\
\mathsf{logptr}(\mathbf{E}) & \overset{\text{def}}{=} & \mathsf{defined}(\mathbf{E}) \wedge \neg(\mathsf{word}(\mathbf{E})) \\
\mathsf{nonptr}(\mathbf{E}) & \overset{\text{def}}{=} & \mathbf{E} = 0 \vee \exists v.\, \mathbf{E} = 2 \times v + 1 \\
\mathsf{offsafe}(\mathbf{E}) & \overset{\text{def}}{=} & \mathsf{word}(\mathbf{E}) \vee \exists i.\, \mathsf{safe}(\mathbf{E} + i) \\
\mathsf{p}(\{\, \mathbf{E}_1, \ldots, \mathbf{E}_n \,\}) & \overset{\text{def}}{=} & \mathsf{p}(\mathbf{E}_1) \wedge \ \ldots \ \wedge \mathsf{p}(\mathbf{E}_n) \\
 & & \text{for } \mathsf{p} = \mathsf{safe}, \mathsf{logptr}, \mathsf{word}, \mathsf{defined}, \mathsf{nonptr}, \mathsf{offsafe} \\
\mathbf{E} \hookrightarrow - & \overset{\text{def}}{=} & \exists v.\, \mathbf{E} \hookrightarrow v \\
\mathbf{E} \hookrightarrow_n \mathbf{E}_0, \ldots, \mathbf{E}_{n-1} & \overset{\text{def}}{=} & \mathbf{E} + 4 \times 0 \hookrightarrow \mathbf{E}_0 * \ldots * \mathbf{E} + 4(n-1) \hookrightarrow \mathbf{E}_{n-1}
\end{array}
$$

Note that Asserts $\subseteq$ AssertsL.

$\boxed{\text{Free variables}}$

$$\begin{array}{ll}
\mathrm{FPV}(\mathbf{E}) & \overset{\text{def}}{=} \text{ the set of program variables appearing in the logical expression } \mathbf{E} \\
\mathrm{FLV}(\mathbf{E}) & \overset{\text{def}}{=} \text{ the set of free logical variables appearing in the assertion } \mathbf{E} \\
\mathrm{FPV}(\mathbf{P}) & \overset{\text{def}}{=} \text{ the set of program variables appearing in the assertion } \mathbf{P} \\
\mathrm{FLV}(\mathbf{P}) & \overset{\text{def}}{=} \text{ the set of free logical variables appearing in the assertion } \mathbf{P}
\end{array}$$

$\boxed{\text{Program Specifications}}$

$$\begin{array}{rcl}
\{\mathbf{P}\}\ C\ \{\mathbf{Q}\} & : & \text{Inner-level partial correctness} \\
[\mathbf{P}]\ C\ [\mathbf{Q}] & : & \text{Inner-level total correctness} \\
\{\{P\}\}\ C\ \{\{Q\}\} & : & \text{Outer-level partial correctness} \\
[[P]]\ C\ [[Q]] & : & \text{Outer-level total correctness}
\end{array}$$

2.3 Semantics

$\boxed{\llbracket \mathbf{E} \rrbracket \in \text{LStores} \rightharpoonup \text{LogVals}}$

$$\begin{array}{ll}
\llbracket v \rrbracket_{\mathbf{s}} & ::= \ \text{undef} \\
\llbracket \mathrm{x} \rrbracket_{\mathbf{s}} & ::= \ \mathbf{s}(\mathrm{x}) \\
\llbracket \mathbf{v} \rrbracket_{\mathbf{s}} & ::= \ \mathbf{v} \\
\llbracket \mathbf{E}_1 \star \mathbf{E}_2 \rrbracket_{\mathbf{s}} & ::= \left\{ \begin{array}{ll}
w_1 \star w_2 & \text{if } \llbracket \mathbf{E}_1 \rrbracket_{\mathbf{s}} = w_1 \in \text{Words} \wedge \llbracket \mathbf{E}_2 \rrbracket_{\mathbf{s}} = w_2 \in \text{Words} \\
\boldsymbol{\ell}\widehat{+}(i+w) & \text{if } \star = + \wedge \llbracket \mathbf{E}_k \rrbracket_{\mathbf{s}} = \boldsymbol{\ell}\widehat{+}i \wedge \llbracket \mathbf{E}_{3-k} \rrbracket_{\mathbf{s}} = w \text{ for } k = 1,2 \\
\boldsymbol{\ell}\widehat{+}(i-w) & \text{if } \star = - \wedge \llbracket \mathbf{E}_1 \rrbracket_{\mathbf{s}} = \boldsymbol{\ell}\widehat{+}i \wedge \llbracket \mathbf{E}_2 \rrbracket_{\mathbf{s}} = w \\
i - j & \text{if } \star = - \wedge \llbracket \mathbf{E}_1 \rrbracket_{\mathbf{s}} = \boldsymbol{\ell}\widehat{+}i \wedge \llbracket \mathbf{E}_2 \rrbracket_{\mathbf{s}} = \boldsymbol{\ell}\widehat{+}j \\
i < j & \text{if } \star = < \wedge \llbracket \mathbf{E}_1 \rrbracket_{\mathbf{s}} = \boldsymbol{\ell}\widehat{+}i \wedge \llbracket \mathbf{E}_2 \rrbracket_{\mathbf{s}} = \boldsymbol{\ell}\widehat{+}j \\
i = j & \text{if } \star = = \wedge \llbracket \mathbf{E}_1 \rrbracket_{\mathbf{s}} = \boldsymbol{\ell}\widehat{+}i \wedge \llbracket \mathbf{E}_2 \rrbracket_{\mathbf{s}} = \boldsymbol{\ell}\widehat{+}j \\
\boldsymbol{\ell} = \boldsymbol{\ell}' & \text{if } \star = = \wedge \llbracket \mathbf{E}_1 \rrbracket_{\mathbf{s}} = \boldsymbol{\ell}\widehat{+}0 \wedge \llbracket \mathbf{E}_2 \rrbracket_{\mathbf{s}} = \boldsymbol{\ell}'\widehat{+}0 \\
0 & \text{if } \star = = \wedge \llbracket \mathbf{E}_k \rrbracket_{\mathbf{s}} = \boldsymbol{\ell}\widehat{+}4i \wedge i \geq 0 \wedge \llbracket \mathbf{E}_{3-k} \rrbracket_{\mathbf{s}} \in \text{NonPtrs for } k = 1,2 \\
\text{undef} & \text{otherwise}
\end{array} \right.
\end{array}$$

where $\star \in \{ +, -, \times, \div, <, =, \mathsf{and} \}, w \div 0 = \text{undef}$,

$w_1 < w_2 \overset{\text{def}}{=} 1$ if $w_1 < w_2$; 0 otherwise,

$w_1 = w_2 \overset{\text{def}}{=} 1$ if $w_1 = w_2$; 0 otherwise,

$w_1 \ \mathsf{and}\ w_2 \overset{\text{def}}{=} 1$ if $w_1 \neq 0 \wedge w_2 \neq 0$; 0 otherwise

$$\llbracket \mathsf{not}\ \mathbf{E} \rrbracket_{\mathbf{s}} \ \overset{\text{def}}{=} \left\{ \begin{array}{ll}
1 & \text{if } \llbracket \mathbf{E} \rrbracket_{\mathbf{s}} = 0 \\
0 & \text{if } \llbracket \mathbf{E} \rrbracket_{\mathbf{s}} \in \text{NonPtrs} \backslash \{0\} \\
\text{undef} & \text{otherwise}
\end{array} \right.$$

$$\boxed{\mathbf{s},\mathbf{h} \models_{\mathbf{L}} \mathbf{P}}$$

$$\begin{array}{lll}
\mathbf{s},\mathbf{h} \models_{\mathbf{L}} \mathsf{safe}(\mathbf{E}) & \text{iff} & [\![\mathbf{E}]\!]_{\mathbf{s}} \in \mathrm{Safe}(\mathbf{L}) \\
\mathbf{s},\mathbf{h} \models_{\mathbf{L}} \mathbf{E} & \text{iff} & [\![\mathbf{E}]\!]_{\mathbf{s}} \in \mathrm{Words}\backslash\{0\} \\
\mathbf{s},\mathbf{h} \models_{\mathbf{L}} \mathbf{E}_1 \hookrightarrow \mathbf{E}_2 & \text{iff} & \exists \boldsymbol{\ell}, i.\ [\![\mathbf{E}_1]\!]_{\mathbf{s}} = \boldsymbol{\ell}\widehat{+}4\,i \wedge [\![\mathbf{E}_2]\!]_{\mathbf{s}} = \mathbf{h}(\boldsymbol{\ell})(i) \neq \mathrm{undef} \\
\mathbf{s},\mathbf{h} \models_{\mathbf{L}} \mathbf{P} * \mathbf{Q} & \text{iff} & \exists \mathbf{h}_1, \mathbf{h}_2.\ \mathbf{h} = \mathbf{h}_1 \uplus \mathbf{h}_2 \wedge \mathbf{s},\mathbf{h}_1 \models_{\mathbf{L}} \mathbf{P} \wedge \mathbf{s},\mathbf{h}_2 \models_{\mathbf{L}} \mathbf{Q} \\
\mathbf{s},\mathbf{h} \models_{\mathbf{L}} \mathbf{P} \mathrel{-\!\!*} \mathbf{Q} & \text{iff} & \forall \mathbf{h}'.\ \mathbf{h}' \# \mathbf{h} \wedge \mathbf{s},\mathbf{h}' \models_{\mathbf{L}} \mathbf{P} \implies \mathbf{s},\mathbf{h} \uplus \mathbf{h}' \models_{\mathbf{L}} \mathbf{Q} \\
\mathbf{s},\mathbf{h} \models_{\mathbf{L}} \mathbf{P} \Rightarrow \mathbf{Q} & \text{iff} & \forall \mathbf{h}' \supseteq \mathbf{h}.\ \mathbf{s},\mathbf{h}' \models_{\mathbf{L}} \mathbf{P} \implies \mathbf{s},\mathbf{h}' \models_{\mathbf{L}} \mathbf{Q} \\
\mathbf{s},\mathbf{h} \models_{\mathbf{L}} \mathbf{P} \wedge \mathbf{Q} & \text{iff} & \mathbf{s},\mathbf{h} \models_{\mathbf{L}} \mathbf{P} \wedge \mathbf{s},\mathbf{h} \models_{\mathbf{L}} \mathbf{Q} \\
\mathbf{s},\mathbf{h} \models_{\mathbf{L}} \mathbf{P} \vee \mathbf{Q} & \text{iff} & \mathbf{s},\mathbf{h} \models_{\mathbf{L}} \mathbf{P} \vee \mathbf{s},\mathbf{h} \models_{\mathbf{L}} \mathbf{Q} \\
\mathbf{s},\mathbf{h} \models_{\mathbf{L}} \forall v.\,\mathbf{P} & \text{iff} & \forall \mathbf{v} \in \mathrm{LogVals}.\ \mathbf{s},\mathbf{h} \models_{\mathbf{L}} \mathbf{P}[\mathbf{v}/v] \\
\mathbf{s},\mathbf{h} \models_{\mathbf{L}} \exists v.\,\mathbf{P} & \text{iff} & \exists \mathbf{v} \in \mathrm{LogVals}.\ \mathbf{s},\mathbf{h} \models_{\mathbf{L}} \mathbf{P}[\mathbf{v}/v]
\end{array}$$

Note that

$$\begin{array}{lll}
\mathbf{s},\mathbf{h} \models_{\mathbf{L}} \mathsf{logptr}(\mathbf{E}) & \iff & [\![\mathbf{E}]\!]_{\mathbf{s}} \in \mathrm{LogPtrs} \\
\mathbf{s},\mathbf{h} \models_{\mathbf{L}} \mathsf{word}(\mathbf{E}) & \iff & [\![\mathbf{E}]\!]_{\mathbf{s}} \in \mathrm{Words}
\end{array}$$

$$\boxed{\mathbf{s},\mathbf{h} \models P}$$

$$\mathbf{s},\mathbf{h} \models P \quad \text{iff} \quad \mathbf{s},\mathbf{h} \models_{\emptyset} P$$

Notation

$$\begin{array}{lll}
\mathbf{P}[\rho] & \stackrel{\text{def}}{=} & \mathbf{P}[\rho(v_1)/v_1]\ldots[\rho(v_n)/v_n] \text{ where } \mathrm{dom}(\rho) = \{\, v_1, \ldots, v_n \,\} \text{ for } \rho \in \mathrm{LogVars} \rightharpoonup_{\mathrm{fin}} \mathrm{LogVals} \\
\mathrm{Env}(V) & \stackrel{\text{def}}{=} & \{\, \rho \in \mathrm{LogVars} \rightharpoonup_{\mathrm{fin}} \mathrm{LogVals} \mid \mathrm{dom}(\rho) \supseteq V \,\} \quad \text{for } V \subseteq_{\mathrm{fin}} \mathrm{LogVars} \\
\rho|^{V}(\mathtt{x}) & \stackrel{\text{def}}{=} & \begin{cases} \rho(\mathtt{x}) & \text{if } \mathtt{x} \in \mathrm{dom}(\rho) \\ 0 & \text{else if } \mathtt{x} \in V \\ \mathrm{undef} & \text{otherwise} \end{cases}
\end{array}$$

$$\boxed{\mathbf{P} \models \mathbf{Q}}$$

$$\begin{array}{ll}
\mathbf{P} \models \mathbf{Q} \ \text{ iff } & \forall \rho \in \mathrm{Env}(\mathrm{FLV}(\mathbf{P},\mathbf{Q})), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h. \\
& \quad \mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge \mathbf{s},\mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \implies \mathbf{s},\mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{Q}[\rho]
\end{array}$$

$$\boxed{\{\mathbf{P}\}\ C\ \{\mathbf{Q}\}}$$

$$\begin{array}{ll}
\{\mathbf{P}\}\ C\ \{\mathbf{Q}\} \ \text{ iff } & \forall \rho \in \mathrm{Env}(\mathrm{FLV}(\mathbf{P},\mathbf{Q})), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'. \\
& \quad \mathbf{s},\mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge \mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge C, s, h \rightsquigarrow^{*} C', s', h' \implies \\
& \qquad (C', s', h' \rightsquigarrow -) \vee \\
& \qquad (\exists \mathbf{s}', \mathbf{h}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathbf{Q}[\rho] \wedge \\
& \qquad\qquad (\forall \mathtt{x} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathtt{x}) = \mathbf{s}(\mathtt{x})) \wedge \mathbf{s}' \sim_{\mathbf{T}} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h')
\end{array}$$

$$\boxed{[\mathbf{P}]\ C\ [\mathbf{Q}]}$$

$$\begin{aligned}[\mathbf{P}]\ C\ [\mathbf{Q}]\ \text{ iff }\ & \{\mathbf{P}\}\ C\ \{\mathbf{Q}\} \land \\ & \forall \rho \in \mathrm{Env}(\mathrm{FLV}(\mathbf{P},\mathbf{Q})), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h. \\ & \quad \mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \land \mathbf{s} \sim_{\mathbf{T}} s \land \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \implies \neg(C, s, h \text{ diverges})\end{aligned}$$

$$\boxed{\{\{P\}\}\ C\ \{\{Q\}\}}$$

$$\begin{aligned}\{\{P\}\}\ C\ \{\{Q\}\}\ \text{ iff }\ & \forall \rho \in \mathrm{Env}(\mathrm{FLV}(P,Q)), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'. \\ & \quad \mathbf{s}, \mathbf{h} \models P[\rho] \land \mathbf{s} \approx_{\mathbf{T}} s \land \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \land C, s, h \rightsquigarrow^{*} C', s', h' \implies \\ & \qquad (C', s', h' \rightsquigarrow -) \lor \\ & \qquad (\exists \mathbf{s}', \mathbf{h}', \mathbf{T}'.\ C' = \mathsf{skip} \land \mathbf{s}', \mathbf{h}' \models Q[\rho] \land \\ & \qquad\qquad\qquad (\forall \mathtt{x} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathtt{x}) = \mathbf{s}(\mathtt{x})) \land \mathbf{s}' \approx_{\mathbf{T}'} s' \land \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}'} h')\end{aligned}$$

$$\boxed{[[P]]\ C\ [[Q]]}$$

$$\begin{aligned}[[P]]\ C\ [[Q]]\ \text{ iff }\ & \{\{P\}\}\ C\ \{\{Q\}\} \land \\ & \forall \rho \in \mathrm{Env}(\mathrm{FLV}(P,Q)), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h. \\ & \quad \mathbf{s}, \mathbf{h} \models P[\rho] \land \mathbf{s} \approx_{\mathbf{T}} s \land \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \implies \neg(C, s, h \text{ diverges})\end{aligned}$$

3 Program Logic

3.1 Inner-level rules

$$\frac{}{[\mathsf{true}]\ \mathsf{skip}\ [\mathsf{true}]} \tag{Skip}$$

$$\frac{}{[\mathtt{x} = v \wedge \mathsf{defined}(E)]\ \mathtt{x} := E\ [\mathtt{x} = E[v/\mathtt{x}]]} \tag{Assign}$$

$$\frac{}{[\mathtt{x} = u \wedge E \hookrightarrow v]\ \mathtt{x} := [E]\ [\mathtt{x} = v \wedge E[u/\mathtt{x}] \hookrightarrow v]} \tag{Read}$$

$$\frac{}{[E \hookrightarrow - \wedge \mathsf{safe}(E')]\ [E] := E'\ [E \hookrightarrow E']} \tag{Write}$$

$$\frac{\{\mathbf{P} \wedge E\}\ C_1\ \{\mathbf{Q}\} \qquad \{\mathbf{P} \wedge \mathsf{not}\ E\}\ C_2\ \{\mathbf{Q}\}}{\{\mathbf{P} \wedge \mathsf{word}(E)\}\ \mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}\ \{\mathbf{Q}\}} \quad \frac{[\mathbf{P} \wedge E]\ C_1\ [\mathbf{Q}] \qquad [\mathbf{P} \wedge \mathsf{not}\ E]\ C_2\ [\mathbf{Q}]}{[\mathbf{P} \wedge \mathsf{word}(E)]\ \mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}\ [\mathbf{Q}]} \tag{If}$$

$$\frac{\{\mathbf{P} \wedge E\}\ C\ \{\mathbf{P} \wedge \mathsf{word}(E)\}}{\{\mathbf{P} \wedge \mathsf{word}(E)\}\ \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}\ \{\mathbf{P} \wedge \mathsf{not}\ E\}} \tag{While}$$

$$\frac{[\mathbf{P} \wedge E \wedge 0 < \mathbf{E}' = v]\ C\ [\mathbf{P} \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}' < v] \qquad v \notin \mathrm{FLV}(\mathbf{P}, \mathbf{E}')}{[\mathbf{P} \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}']\ \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}\ [\mathbf{P} \wedge \mathsf{not}\ E]} \tag{WhileT}$$

$$\frac{\{\mathbf{P}\}\ C_1\ \{\mathbf{Q}\} \qquad \{\mathbf{Q}\}\ C_2\ \{\mathbf{R}\}}{\{\mathbf{P}\}\ C_1; C_2\ \{\mathbf{R}\}} \quad \frac{[\mathbf{P}]\ C_1\ [\mathbf{Q}] \qquad [\mathbf{Q}]\ C_2\ [\mathbf{R}]}{[\mathbf{P}]\ C_1; C_2\ [\mathbf{R}]} \tag{Seq}$$

$$\frac{\{\mathbf{P}\}\ C\ \{\mathbf{Q}\} \qquad \mathrm{FPV}(\mathbf{R}) \cap \mathrm{Mod}(C) = \emptyset}{\{\mathbf{P} * \mathbf{R}\}\ C\ \{\mathbf{Q} * \mathbf{R}\}} \quad \frac{[\mathbf{P}]\ C\ [\mathbf{Q}] \qquad \mathrm{FPV}(\mathbf{R}) \cap \mathrm{Mod}(C) = \emptyset}{[\mathbf{P} * \mathbf{R}]\ C\ [\mathbf{Q} * \mathbf{R}]} \tag{Frame}$$

$$\frac{\mathbf{P} \models \mathbf{P}' \qquad \{\mathbf{P}'\}\ C\ \{\mathbf{Q}'\} \qquad \mathbf{Q}' \models \mathbf{Q}}{\{\mathbf{P}\}\ C\ \{\mathbf{Q}\}} \quad \frac{\mathbf{P} \models \mathbf{P}' \qquad [\mathbf{P}']\ C\ [\mathbf{Q}'] \qquad \mathbf{Q}' \models \mathbf{Q}}{[\mathbf{P}]\ C\ [\mathbf{Q}]} \tag{Conseq}$$

$$\frac{\{\mathbf{P}\}\ C\ \{\mathbf{Q}\}}{\{\exists v.\, \mathbf{P}\}\ C\ \{\exists v.\, \mathbf{Q}\}} \quad \frac{[\mathbf{P}]\ C\ [\mathbf{Q}]}{[\exists v.\, \mathbf{P}]\ C\ [\exists v.\, \mathbf{Q}]} \tag{Ex}$$

$$\frac{\forall \mathbf{v} \in \mathrm{LogVals}.\ \{\mathbf{P}[\mathbf{v}/v]\}\ C\ \{\mathbf{Q}[\mathbf{v}/v]\}}{\{\mathbf{P}\}\ C\ \{\mathbf{Q}\}} \quad \frac{\forall \mathbf{v} \in \mathrm{LogVals}.\ [\mathbf{P}[\mathbf{v}/v]]\ C\ [\mathbf{Q}[\mathbf{v}/v]]}{[\mathbf{P}]\ C\ [\mathbf{Q}]} \tag{Gen}$$

$$\frac{[\mathbf{P}]\ C\ [\mathbf{Q}]}{\{\mathbf{P}\}\ C\ \{\mathbf{Q}\}} \tag{Total}$$

3.2 Outer-level rules

$$\frac{n \geq 0}{[[\mathsf{x} = 2n+1]]\ \mathsf{alloc}\ \mathtt{x}\ [[\mathsf{x} \hookrightarrow_n 0, \ldots, 0]]} \qquad \text{(Alloc)}$$

$$\frac{V \subseteq_{\text{fin}} \text{ProgVars} \qquad \{P \wedge \mathsf{safe}(V)\}\ C\ \{Q \wedge \mathsf{safe}(\text{Mod}(C))\}}{\{\{P\}\}\ C\ \{\{Q\}\}}$$

$$\frac{V \subseteq_{\text{fin}} \text{ProgVars} \qquad [P \wedge \mathsf{safe}(V)]\ C\ [Q \wedge \mathsf{safe}(\text{Mod}(C))]}{[[P]]\ C\ [[Q]]} \qquad \text{(Incl)}$$

$$\frac{\{\{P \wedge E\}\}\ C_1\ \{\{Q\}\} \qquad \{\{P \wedge \mathsf{not}\ E\}\}\ C_2\ \{\{Q\}\}}{\{\{P \wedge \mathsf{word}(E)\}\}\ \mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}\ \{\{Q\}\}} \quad \frac{[[P \wedge E]]\ C_1\ [[Q]] \qquad [[P \wedge \mathsf{not}\ E]]\ C_2\ [[Q]]}{[[P \wedge \mathsf{word}(E)]]\ \mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}\ [[Q]]}$$

$$\text{(If)}$$

$$\frac{\{\{P \wedge E\}\}\ C\ \{\{P \wedge \mathsf{word}(E)\}\}}{\{\{P \wedge \mathsf{word}(E)\}\}\ \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}\ \{\{P \wedge \mathsf{not}\ E\}\}} \qquad \text{(While)}$$

$$\frac{[[P \wedge E \wedge 0 < \mathbf{E}' = v]]\ C\ [[P \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}' < v]] \qquad v \notin \text{FLV}(P, \mathbf{E}')}{[[P \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}']]\ \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}\ [[P \wedge \mathsf{not}\ E]]} \qquad \text{(WhileT)}$$

$$\frac{\{\{P\}\}\ C_1\ \{\{Q\}\} \qquad \{\{Q\}\}\ C_2\ \{\{R\}\}}{\{\{P\}\}\ C_1; C_2\ \{\{R\}\}} \quad \frac{[[P]]\ C_1\ [[Q]] \qquad [[Q]]\ C_2\ [[R]]}{[[P]]\ C_1; C_2\ [[R]]} \qquad \text{(Seq)}$$

$$\frac{\{\{P\}\}\ C\ \{\{Q\}\} \qquad \text{FPV}(R) \cap \text{Mod}(C) = \emptyset}{\{\{P * R\}\}\ C\ \{\{Q * R\}\}} \quad \frac{[[P]]\ C\ [[Q]] \qquad \text{FPV}(R) \cap \text{Mod}(C) = \emptyset}{[[P * R]]\ C\ [[Q * R]]}$$

$$\text{(Frame)}$$

$$\frac{P \models P' \qquad \{\{P'\}\}\ C\ \{\{Q'\}\} \qquad Q' \models Q}{\{\{P\}\}\ C\ \{\{Q\}\}} \quad \frac{P \models P' \qquad [[P']]\ C\ [[Q']] \qquad Q' \models Q}{[[P]]\ C\ [[Q]]} \qquad \text{(Conseq)}$$

$$\frac{\{\{P\}\}\ C\ \{\{Q\}\}}{\{\{\exists v.\, P\}\}\ C\ \{\{\exists v.\, Q\}\}} \quad \frac{[[P]]\ C\ [[Q]]}{[[\exists v.\, P]]\ C\ [[\exists v.\, Q]]} \qquad \text{(Ex)}$$

$$\frac{\forall \mathbf{v} \in \text{LogVals}.\ \{\{P[\mathbf{v}/v]\}\}\ C\ \{\{Q[\mathbf{v}/v]\}\}}{\{\{P\}\}\ C\ \{\{Q\}\}} \quad \frac{\forall \mathbf{v} \in \text{LogVals}.\ [[P[\mathbf{v}/v]]]\ C\ [[Q[\mathbf{v}/v]]]}{[[P]]\ C\ [[Q]]} \qquad \text{(Gen)}$$

$$\frac{[[P]]\ C\ [[Q]]}{\{\{P\}\}\ C\ \{\{Q\}\}} \qquad \text{(Total)}$$

3.3 Assertion entailments

$$\mathsf{nonptr}(\mathbf{E}) \models \mathsf{safe}(\mathbf{E}) \tag{NPtrSafe}$$

$$\mathbf{E} \models \mathsf{word}(\mathbf{E}) \tag{BoolWord}$$

$$\mathbf{E} \hookrightarrow \mathbf{E}' \models \mathbf{E} \neq 0 \tag{PointstoNZero}$$

$$\mathsf{defined}(E) \models \mathsf{offsafe}(E) \tag{ExpSafe}$$

$$\mathbf{E} \hookrightarrow \mathbf{E}' \wedge \mathsf{offsafe}(\mathbf{E}) \models \mathsf{safe}(\mathbf{E}') \tag{HeapSafe}$$

$$E \hookrightarrow \mathbf{E}' \models \mathsf{safe}(\mathbf{E}') \tag{ExpHeapSafe}$$

$$\mathsf{safe}(\mathbf{E}, \mathbf{E}') \models \mathsf{defined}(\mathbf{E} = \mathbf{E}') \tag{SafeEq}$$

3.4 Derived rules

$$\frac{\{\mathbf{P}\}\ C\ \{\mathbf{Q}\} \qquad v \notin \mathrm{FLV}(\mathbf{Q})}{\{\exists v.\, \mathbf{P}\}\ C\ \{\mathbf{Q}\}} \quad \frac{[\mathbf{P}]\ C\ [\mathbf{Q}] \qquad v \notin \mathrm{FLV}(\mathbf{Q})}{[\exists v.\, \mathbf{P}]\ C\ [\mathbf{Q}]} \tag{Ex'}$$

$$\frac{\{\{P\}\}\ C\ \{\{Q\}\} \qquad v \notin \mathrm{FLV}(Q)}{\{\{\exists v.\, P\}\}\ C\ \{\{Q\}\}} \quad \frac{[[P]]\ C\ [[Q]] \qquad v \notin \mathrm{FLV}(Q)}{[[\exists v.\, P]]\ C\ [[Q]]} \tag{Ex'}$$

$$\frac{\{\mathbf{P}_1\}\ C\ \{\mathbf{Q}\} \qquad \{\mathbf{P}_2\}\ C\ \{\mathbf{Q}\}}{\{\mathbf{P}_1 \vee \mathbf{P}_2\}\ C\ \{\mathbf{Q}\}} \quad \frac{[\mathbf{P}_1]\ C\ [\mathbf{Q}] \qquad [\mathbf{P}_2]\ C\ [\mathbf{Q}]}{[\mathbf{P}_1 \vee \mathbf{P}_2]\ C\ [\mathbf{Q}]} \tag{Disj}$$

$$\frac{\{\{P_1\}\}\ C\ \{\{Q\}\} \qquad \{\{P_2\}\}\ C\ \{\{Q\}\}}{\{\{P_1 \vee P_2\}\}\ C\ \{\{Q\}\}} \quad \frac{[[P_1]]\ C\ [[Q]] \qquad [[P_2]]\ C\ [[Q]]}{[[P_1 \vee P_2]]\ C\ [[Q]]} \tag{Disj}$$

$$\frac{\{\mathbf{P}\}\ C\ \{\mathbf{Q}\} \qquad \mathrm{FPV}(\mathbf{E}) \cap \mathrm{Mod}(C) = \emptyset}{\{\mathbf{P}[\mathbf{E}/v] \wedge \mathsf{defined}(\mathbf{E})\}\ C\ \{\mathbf{Q}[\mathbf{E}/v]\}} \quad \frac{[\mathbf{P}]\ C\ [\mathbf{Q}] \qquad \mathrm{FPV}(\mathbf{E}) \cap \mathrm{Mod}(C) = \emptyset}{[\mathbf{P}[\mathbf{E}/v] \wedge \mathsf{defined}(\mathbf{E})]\ C\ [\mathbf{Q}[\mathbf{E}/v]]} \tag{Inst}$$

$$\frac{\{\{P\}\}\ C\ \{\{Q\}\} \qquad \mathrm{FPV}(\mathbf{E}) \cap \mathrm{Mod}(C) = \emptyset}{\{\{P[\mathbf{E}/v] \wedge \mathsf{defined}(\mathbf{E})\}\}\ C\ \{\{Q[\mathbf{E}/v]\}\}} \quad \frac{[[P]]\ C\ [[Q]] \qquad \mathrm{FPV}(\mathbf{E}) \cap \mathrm{Mod}(C) = \emptyset}{[[P[\mathbf{E}/v] \wedge \mathsf{defined}(\mathbf{E})]]\ C\ [[Q[\mathbf{E}/v]]]} \tag{Inst}$$

$$\frac{}{[\mathbf{P}[E/\mathtt{x}] \wedge \mathsf{defined}(E)]\ \mathtt{x} := E\ [\mathbf{P}]} \tag{Assign'}$$

$$\frac{\mathtt{x} \notin \mathrm{FPV}(E) \cup \mathrm{FPV}(\mathbf{E}')}{[E \hookrightarrow \mathbf{E}']\ \mathtt{x} := [E]\ [\mathtt{x} = \mathbf{E}' \wedge E \hookrightarrow \mathbf{E}']} \tag{Read'}$$

$$\frac{\mathtt{x} \notin \mathrm{FPV}(\mathbf{E}') \cup \mathrm{FPV}(\mathbf{E}'')}{[\mathtt{x} = \mathbf{E}' \wedge E \hookrightarrow \mathbf{E}'']\ \mathtt{x} := [E]\ [\mathtt{x} = \mathbf{E}'' \wedge E[\mathbf{E}'/\mathtt{x}] \hookrightarrow \mathbf{E}'']} \tag{Read''}$$

$$\frac{}{[[\mathbf{P}[\mathsf{y}/\mathsf{x}]]]\ \mathtt{x} := \mathtt{y}\ [[\mathbf{P}]]} \qquad \text{(ASSIGN)}$$

$$\frac{}{[[\mathbf{P}[E/\mathsf{x}] \wedge \mathsf{nonptr}(E)]]\ \mathtt{x} := E\ [[\mathbf{P}]]} \qquad \text{(ASSIGN')}$$

$$\frac{\mathsf{x} \notin \mathrm{FPV}(E) \cup \mathrm{FPV}(\mathbf{E}')}{[[E \hookrightarrow \mathbf{E}']]\ \mathtt{x} := [E]\ [[\mathsf{x} = \mathbf{E}' \wedge E \hookrightarrow \mathbf{E}']]} \qquad \text{(READ)}$$

$$\frac{\mathsf{x} \notin \mathrm{FPV}(\mathbf{E}') \cup \mathrm{FPV}(\mathbf{E}'')}{[[\mathsf{x} = \mathbf{E}' \wedge E \hookrightarrow \mathbf{E}'']]\ \mathtt{x} := [E]\ [[\mathsf{x} = \mathbf{E}'' \wedge E[\mathbf{E}'/\mathsf{x}] \hookrightarrow \mathbf{E}'']]} \qquad \text{(READ')}$$

$$\frac{}{[[E \hookrightarrow -]]\ [E] := \mathtt{x}\ [[E \hookrightarrow \mathsf{x}]]} \qquad \text{(WRITE)}$$

$$\frac{}{[[E \hookrightarrow - \wedge \mathsf{nonptr}(E')]]\ [E] := E'\ [[E \hookrightarrow E']]} \qquad \text{(WRITE')}$$

$$\frac{n \geq 0}{[[E = 2n+1]]\ \mathtt{x} := \mathsf{ALLOC}(E)\ [[\mathsf{x} \hookrightarrow_n 0, \ldots, 0]]} \qquad \text{(ALLOC)}$$

3.5 Problematic rules

$$\frac{\{\mathbf{P}\}\ C\ \{\mathbf{Q}_1\} \qquad \{\mathbf{P}\}\ C\ \{\mathbf{Q}_2\}}{\{\mathbf{P}\}\ C\ \{\mathbf{Q}_1 \wedge \mathbf{Q}_2\}} \quad \frac{[\mathbf{P}]\ C\ [\mathbf{Q}_1] \qquad [\mathbf{P}]\ C\ [\mathbf{Q}_2]}{[\mathbf{P}]\ C\ [\mathbf{Q}_1 \wedge \mathbf{Q}_2]} \qquad \text{(Conj)}$$

$$\frac{\{\{P\}\}\ C\ \{\{Q_1\}\} \qquad \{\{P\}\}\ C\ \{\{Q_2\}\}}{\{\{P\}\}\ C\ \{\{Q_1 \wedge Q_2\}\}} \quad \frac{[[P]]\ C\ [[Q_1]] \qquad [[P]]\ C\ [[Q_2]]}{[[P]]\ C\ [[Q_1 \wedge Q_2]]} \qquad \text{(Conj)}$$

$$\frac{\{\mathbf{P}\}\ C\ \{\mathbf{Q}\}}{\{\forall v.\, \mathbf{P}\}\ C\ \{\forall v.\, \mathbf{Q}\}} \quad \frac{[\mathbf{P}]\ C\ [\mathbf{Q}]}{[\forall v.\, \mathbf{P}]\ C\ [\forall v.\, \mathbf{Q}]} \qquad \text{(All)}$$

$$\frac{\{\{P\}\}\ C\ \{\{Q\}\}}{\{\{\forall v.\, P\}\}\ C\ \{\{\forall v.\, Q\}\}} \quad \frac{[[P]]\ C\ [[Q]]}{[[\forall v.\, P]]\ C\ [[\forall v.\, Q]]} \qquad \text{(All)}$$

Counter example. According to the semantics of $\{-\} - \{-\}$, the following hold:

$$\{\mathsf{x} = 0 \wedge \mathsf{y} \hookrightarrow 0\}\ \mathtt{x} := \mathtt{x}\ \{\mathsf{x} = 0\}$$
$$\{\mathsf{x} = 0 \wedge \mathsf{y} \hookrightarrow 0\}\ \mathtt{x} := \mathtt{x}\ \{\mathsf{logptr}(x)\}$$

However, the following conjunction does NOT hold:

$$\{\mathsf{x} = 0 \wedge \mathsf{y} \hookrightarrow 0\}\ \mathtt{x} := \mathtt{x}\ \{\mathsf{x} = 0 \wedge \mathsf{logptr}(x)\}$$

4 Examples

4.1 Array Assignment

$$\{\{\mathrm{y}+8 \hookrightarrow -\}\}$$

$$\{\mathrm{y}+8 \hookrightarrow - \wedge \underline{\mathsf{safe}(\mathrm{y})}\} \tag{Incl}$$

$$\mathrm{y} := \mathrm{y}+8;$$

$$\{\mathrm{y} \hookrightarrow - \wedge \underline{\mathsf{safe}(\mathrm{y}-8)}\} \tag{Assign$'$}$$

$$\{\mathrm{y} \hookrightarrow - \wedge \underline{\mathsf{safe}(\mathrm{y}-8, 0)}\}$$

$$[\mathrm{y}] := 0;$$

$$\{\mathrm{y} \hookrightarrow 0 \wedge \underline{\mathsf{safe}(\mathrm{y}-8)}\} \tag{Write}$$

$$\mathrm{y} := \mathrm{y}-8;$$

$$\{\mathrm{y}+8 \hookrightarrow 0 \wedge \underline{\mathsf{safe}(\mathrm{y})}\} \tag{Assign$'$}$$

$$\{\{\mathrm{y}+8 \hookrightarrow 0\}\} \tag{Incl}$$

4.2 Word Swap

$$\{\{\mathtt{x} \hookrightarrow_2 u, v\}\}$$

$$\mathtt{t} := \mathsf{ALLOC}(\mathsf{ENC}(0))$$

$$\{\{\mathtt{x} \hookrightarrow_2 u, v * \mathtt{t} \hookrightarrow_0 \cdot\}\} \tag{ALLOC}$$

$$\{\{\mathtt{x} \hookrightarrow_2 u, v\}\}$$

$$\mathtt{t} := [\mathtt{x}];$$

$$\{\{\mathtt{x} \hookrightarrow_2 u, v \wedge \mathtt{t} = u\}\} \tag{READ}$$

$$\mathtt{r} := [\mathtt{x}+4];$$

$$\{\{\mathtt{x} \hookrightarrow_2 u, v \wedge \mathtt{t} = u \wedge \mathtt{r} = v\}\} \tag{READ}$$

$$[\mathtt{x}] := \mathtt{r};$$

$$\{\{\mathtt{x} \hookrightarrow_2 \mathtt{r}, v \wedge \mathtt{t} = u \wedge \mathtt{r} = v\}\} \tag{WRITE}$$

$$[\mathtt{x}+4] := \mathtt{t};$$

$$\{\{\mathtt{x} \hookrightarrow_2 \mathtt{r}, \mathtt{t} \wedge \mathtt{t} = u \wedge \mathtt{r} = v\}\} \tag{WRITE}$$

$$\{\{\mathtt{x} \hookrightarrow_2 v, u\}\}$$

4.3 Linking of Assignment and Swap

From Sections 4.1 and 4.2, we have the following results.

$$\begin{array}{lcl}
\text{Assign} & \overset{\text{def}}{=} & \mathtt{y} := \mathtt{y}+8;\ [\mathtt{y}] := 0;\ \mathtt{y} := \mathtt{y}-8 \\
\text{Swap} & \overset{\text{def}}{=} & \mathtt{t} := 1;\ \mathsf{alloc}\ \mathtt{t};\ \mathtt{t} := [\mathtt{x}];\ \mathtt{r} := [\mathtt{x}+4];\ [\mathtt{x}] := \mathtt{r};\ [\mathtt{x}+4] := \mathtt{t}
\end{array}$$

$$\{\!\{\mathtt{y}+8 \hookrightarrow -\}\!\}\ \text{Assign}\ \{\!\{\mathtt{y}+8 \hookrightarrow 0\}\!\}$$

$$\{\!\{\mathtt{x} \hookrightarrow_2 u, v\}\!\}\ \text{Swap}\ \{\!\{\mathtt{x} \hookrightarrow_2 v, u\}\!\}$$

From these, we can reason about the linked program as follows.

$$\frac{\{\!\{\mathtt{y}+8 \hookrightarrow -\}\!\}\ \text{Assign}\ \{\!\{\mathtt{y}+8 \hookrightarrow 0\}\!\} \qquad \text{FPV}(\mathtt{x} \hookrightarrow_2 u, v) \cap \text{Mod}(\text{Assign}) = \emptyset}{\{\!\{\mathtt{x} \hookrightarrow_2 u, v * \mathtt{y}+8 \hookrightarrow -\}\!\}\ \text{Assign}\ \{\!\{\mathtt{x} \hookrightarrow_2 u, v * \mathtt{y}+8 \hookrightarrow 0\}\!\}}\ (\text{Frame})$$

$$\frac{\{\!\{\mathtt{x} \hookrightarrow_2 u, v\}\!\}\ \text{Swap}\ \{\!\{\mathtt{x} \hookrightarrow_2 v, u\}\!\} \qquad \text{FPV}(\mathtt{y}+8 \hookrightarrow 0) \cap \text{Mod}(\text{Swap}) = \emptyset}{\{\!\{\mathtt{x} \hookrightarrow_2 u, v * \mathtt{y}+8 \hookrightarrow 0\}\!\}\ \text{Swap}\ \{\!\{\mathtt{x} \hookrightarrow_2 v, u * \mathtt{y}+8 \hookrightarrow 0\}\!\}}\ (\text{Frame})$$

$$\frac{\begin{array}{c}\{\!\{\mathtt{x} \hookrightarrow_2 u, v * \mathtt{y}+8 \hookrightarrow -\}\!\}\ \text{Assign}\ \{\!\{\mathtt{x} \hookrightarrow_2 u, v * \mathtt{y}+8 \hookrightarrow 0\}\!\} \\ \{\!\{\mathtt{x} \hookrightarrow_2 u, v * \mathtt{y}+8 \hookrightarrow 0\}\!\}\ \text{Swap}\ \{\!\{\mathtt{x} \hookrightarrow_2 v, u * \mathtt{y}+8 \hookrightarrow 0\}\!\}\end{array}}{\{\!\{\mathtt{x} \hookrightarrow_2 u, v * \mathtt{y}+8 \hookrightarrow -\}\!\}\ \text{Assign};\ \text{Swap}\ \{\!\{\mathtt{x} \hookrightarrow_2 v, u * \mathtt{y}+8 \hookrightarrow 0\}\!\}}\ (\text{Seq})$$

4.4 Simple Addition

$$\begin{array}{ll}
\{\!\{\mathtt{x} = 2 \times n + 1 \wedge \mathtt{y} = 2 \times m + 1\}\!\} & \\
\{\mathtt{x} = 2 \times n + 1 \wedge \mathtt{y} = 2 \times m + 1\} & (\text{Incl}) \\
\{\mathtt{x}+\mathtt{y} = 2 \times (n+m) + 2 \wedge \mathtt{x} = 2 \times n + 1 \wedge \mathtt{y} = 2 \times m + 1\} & \\
\mathtt{z} := \mathtt{x} + \mathtt{y}; & \\
\{\mathtt{z} = 2 \times (n+m) + 2 \wedge \mathtt{x} = 2 \times n + 1 \wedge \mathtt{y} = 2 \times m + 1\} & (\text{Assign}') \\
\{\mathtt{z} - 1 = 2 \times (n+m) + 1 \wedge \mathtt{x} = 2 \times n + 1 \wedge \mathtt{y} = 2 \times m + 1\} & \\
\mathtt{z} := \mathtt{z} - 1; & \\
\{\mathtt{z} = 2 \times (n+m) + 1 \wedge \mathtt{x} = 2 \times n + 1 \wedge \mathtt{y} = 2 \times m + 1\} & (\text{Assign}') \\
\{\mathtt{z} = 2 \times (n+m) + 1 \wedge \mathtt{x} = 2 \times n + 1 \wedge \mathtt{y} = 2 \times m + 1 \wedge \underline{\mathsf{safe}(\mathtt{z})}\} & \\
\{\!\{\mathtt{z} = 2 \times (n+m) + 1 \wedge \mathtt{x} = 2 \times n + 1 \wedge \mathtt{y} = 2 \times m + 1\}\!\} & (\text{Incl})
\end{array}$$

4.5 Integer Arithmetic

Simple version

$$\{\!\{\mathtt{x} = 2 \times n + 1 \wedge \mathtt{y} = 2 \times m + 1\}\!\}$$

$\{\{2 \times ((\mathtt{x} \div 2 + \mathtt{y} \div 2) \times (\mathtt{x} \div 2 + \mathtt{y} \div 2) \times (\mathtt{x} \div 2 + \mathtt{y} \div 2) \times (\mathtt{x} \div 2 + \mathtt{y} \div 2)) + 1 =$
$2 \times (m + n) \times (m + n) \times (m + n) \times (m + n) + 1\}\}$

$\mathtt{x} := 2 \times ((\mathtt{x} \div 2 + \mathtt{y} \div 2) \times (\mathtt{x} \div 2 + \mathtt{y} \div 2) \times (\mathtt{x} \div 2 + \mathtt{y} \div 2) \times (\mathtt{x} \div 2 + \mathtt{y} \div 2)) + 1$

$\{\{\mathtt{x} = 2 \times (m + n) \times (m + n) \times (m + n) \times (m + n) + 1\}\}$ (ASSIGN′)

$\boxed{\text{Optimized version}}$

$\{\{\mathtt{x} = 2 \times n + 1 \wedge \mathtt{y} = 2 \times m + 1\}\}$
$\{\mathtt{x} = 2 \times n + 1 \wedge \mathtt{y} = 2 \times m + 1\}$ (Incl)
$\{\mathtt{x} + \mathtt{y} = 2 \times (n + m) + 2\}$

$\mathtt{x} := \mathtt{x} + \mathtt{y};$

$\{\mathtt{x} = 2 \times (n + m) + 2\}$ (Assign′)
$\{\mathtt{x} \div 2 - 1 = n + m \wedge \mathsf{word}(n, m)\}$

$\mathtt{x} := \mathtt{x} \div 2 - 1;$

$\{\mathtt{x} = n + m \wedge \mathsf{word}(n, m)\}$ (Assign′)
$\{\mathtt{x} \times \mathtt{x} = (n + m) \times (n + m)\}$

$\mathtt{x} := \mathtt{x} \times \mathtt{x};$

$\{\mathtt{x} = (n + m) \times (n + m)\}$ (Assign′)
$\{\mathtt{x} \times \mathtt{x} = (n + m) \times (n + m) \times (n + m) \times (n + m)\}$

$\mathtt{x} := \mathtt{x} \times \mathtt{x};$

$\{\mathtt{x} = (n + m) \times (n + m) \times (n + m) \times (n + m)\}$ (Assign′)
$\{2 \times \mathtt{x} + 1 = 2 \times (n + m) \times (n + m) \times (n + m) \times (n + m) + 1\}$

$\mathtt{x} := 2 \times \mathtt{x} + 1$

$\{\mathtt{x} = 2 \times (n + m) \times (n + m) \times (n + m) \times (n + m) + 1\}$ (Assign′)
$\{\mathtt{x} = 2 \times (m + n) \times (m + n) \times (m + n) \times (m + n) + 1 \wedge \underline{\mathsf{safe}(\mathtt{x})}\}$
$\{\{\mathtt{x} = 2 \times (m + n) \times (m + n) \times (m + n) \times (m + n) + 1\}\}$ (Incl)

4.6 List Reversal

$$
\begin{aligned}
\epsilon^{\dagger} &\stackrel{\text{def}}{=} \epsilon \\
(v \cdot \alpha)^{\dagger} &\stackrel{\text{def}}{=} \alpha^{\dagger} \cdot v \\
\mathsf{list}\, \epsilon\, \mathbf{E} &\stackrel{\text{def}}{=} \mathbf{E} = 0 \\
\mathsf{list}\, (v \cdot \alpha)\, \mathbf{E} &\stackrel{\text{def}}{=} \exists z.\, (\mathbf{E} \hookrightarrow_2 v, z) * \mathsf{list}\, \alpha\, z
\end{aligned}
$$

$\{\{\mathsf{list}\, \alpha_0\, \mathtt{x}\}\}$

```
$\{\{(\mathsf{list}\,\alpha_0\,\mathrm{x} * 0 = 0) \land \underline{\mathsf{defined}(0)}\}\}$
$\mathrm{y} := 0;$
$\{\{(\mathsf{list}\,\alpha_0\,\mathrm{x} * \mathrm{y} = 0)\}\}$    (ASSIGN′)
$\{\{(\mathsf{list}\,\alpha_0\,\mathrm{x} * \mathsf{list}\,\epsilon\,\mathrm{y})\}\}$
$\{\{\exists \alpha, \beta.\, (\mathsf{list}\,\alpha\,\mathrm{x} * \mathsf{list}\,\beta\,\mathrm{y}) \land \alpha_0^\dagger = \alpha^\dagger{\cdot}\beta \land \underline{\mathsf{word}(\mathrm{x} \neq 0)}\}\}$
while $\mathrm{x} \neq 0$ do
    $\{\{\exists \alpha, \beta.\, (\mathsf{list}\,\alpha\,\mathrm{x} * \mathsf{list}\,\beta\,\mathrm{y}) \land \alpha_0^\dagger = \alpha^\dagger{\cdot}\beta \land \mathrm{x} \neq 0\}\}$    (While)
    $\{\{\exists v, \alpha, \beta.\, (\mathsf{list}\,(v{\cdot}\alpha)\,\mathrm{x} * \mathsf{list}\,\beta\,\mathrm{y}) \land \alpha_0^\dagger = (v{\cdot}\alpha)^\dagger{\cdot}\beta\}\}$
    $\{\{\exists v, \alpha, \beta, z.\, (\mathrm{x} \hookrightarrow_2 v, z * \mathsf{list}\,\alpha\,z * \mathsf{list}\,\beta\,\mathrm{y}) \land \alpha_0^\dagger = (v{\cdot}\alpha)^\dagger{\cdot}\beta\}\}$
    $\{\{\exists v, \alpha, \beta.\, (\mathrm{x} \hookrightarrow_2 v, z * \mathsf{list}\,\alpha\,z * \mathsf{list}\,\beta\,\mathrm{y}) \land \alpha_0^\dagger = (v{\cdot}\alpha)^\dagger{\cdot}\beta\}\}$    (Ex′)
    $\mathrm{z} := [\mathrm{x} + 4];$
    $\{\{\exists v, \alpha, \beta.\, \mathrm{z} = z \land (\mathrm{x} \hookrightarrow_2 v, z * \mathsf{list}\,\alpha\,z * \mathsf{list}\,\beta\,\mathrm{y}) \land \alpha_0^\dagger = (v{\cdot}\alpha)^\dagger{\cdot}\beta\}\}$    (READ)
    $\{\{\exists v, \alpha, \beta.\, (\mathrm{x} \hookrightarrow_2 v, \mathrm{z} * \mathsf{list}\,\alpha\,\mathrm{z} * \mathsf{list}\,\beta\,\mathrm{y}) \land \alpha_0^\dagger = (v{\cdot}\alpha)^\dagger{\cdot}\beta\}\}$
    $[\mathrm{x} + 4] := \mathrm{y};$
    $\{\{\exists v, \alpha, \beta.\, (\mathrm{x} \hookrightarrow_2 v, \mathrm{y} * \mathsf{list}\,\alpha\,\mathrm{z} * \mathsf{list}\,\beta\,\mathrm{y}) \land \alpha_0^\dagger = (v{\cdot}\alpha)^\dagger{\cdot}\beta\}\}$    (WRITE)
    $\{\{\exists v, \alpha, \beta.\, (\mathsf{list}\,\alpha\,\mathrm{z} * \mathsf{list}\,(v{\cdot}\beta)\,\mathrm{x}) \land \alpha_0^\dagger = \alpha^\dagger{\cdot}v{\cdot}\beta\}\}$
    $\{\{\exists \alpha, \beta.\, (\mathsf{list}\,\alpha\,\mathrm{z} * \mathsf{list}\,\beta\,\mathrm{x}) \land \alpha_0^\dagger = \alpha^\dagger{\cdot}\beta \land \underline{\mathsf{defined}(\mathrm{x})}\}\}$
    $\mathrm{y} := \mathrm{x};$
    $\{\{\exists \alpha, \beta.\, (\mathsf{list}\,\alpha\,\mathrm{z} * \mathsf{list}\,\beta\,\mathrm{y}) \land \alpha_0^\dagger = \alpha^\dagger{\cdot}\beta \land \underline{\mathsf{defined}(\mathrm{z})}\}\}$    (ASSIGN)
    $\mathrm{x} := \mathrm{z}$
    $\{\{\exists \alpha, \beta.\, (\mathsf{list}\,\alpha\,\mathrm{x} * \mathsf{list}\,\beta\,\mathrm{y}) \land \alpha_0^\dagger = \alpha^\dagger{\cdot}\beta \land \underline{\mathsf{word}(\mathrm{x} \neq 0)}\}\}$    (ASSIGN)
od;
$\{\{\exists \alpha, \beta.\, (\mathsf{list}\,\alpha\,\mathrm{x} * \mathsf{list}\,\beta\,\mathrm{y}) \land \alpha_0^\dagger = \alpha^\dagger{\cdot}\beta \land \mathrm{x} = 0\}\}$    (While)
$\{\{\mathsf{list}\,\alpha_0^\dagger\,\mathrm{y}\}\}$
```

4.7 Array Copy

```
$\{\{\mathrm{x} \hookrightarrow_n v_1, \ldots, v_n\}\}$
$\mathrm{y} := \mathsf{ALLOC}(\mathsf{ENC}(n));$
$\{\{(\mathrm{x} \hookrightarrow_n v_1, \ldots, v_n * \mathrm{y} \hookrightarrow_n 0, \ldots, 0)\}\}$    (ALLOC)
```

$$\{(\mathtt{x} \hookrightarrow_n v_1, \ldots, v_n * \mathtt{y} \hookrightarrow_n 0, \ldots, 0) \land \underline{\mathsf{safe}(\mathtt{x}, \mathtt{y}, \mathtt{t})}\} \qquad \text{(Incl)}$$

$$\{(\mathtt{x} \hookrightarrow_n v_1, \ldots, v_n * \mathtt{y} \hookrightarrow_n 0, \ldots, 0) \land \mathtt{x} + 4n = \mathtt{x} + 4n \land \underline{\mathsf{safe}(\mathtt{x}, \mathtt{y}, \mathtt{t})} \land \underline{\mathsf{defined}(\mathtt{x} + 4n)}\}$$

$\mathtt{z} := \mathtt{x} + 4n;$

$$\{(\mathtt{x} \hookrightarrow_n v_1, \ldots, v_n * \mathtt{y} \hookrightarrow_n 0, \ldots, 0) \land \mathtt{z} = \mathtt{x} + 4n \land \underline{\mathsf{safe}(\mathtt{x}, \mathtt{y}, \mathtt{t})}\} \qquad \text{(Assign}'\text{)}$$

$$\{\exists k.\, (\mathtt{x} - 4k \hookrightarrow_n v_1, \ldots, v_n * \mathtt{y} - 4k \hookrightarrow_k v_1, \ldots, v_k * \mathtt{y} \hookrightarrow_{n-k} 0, \ldots, 0) \land \\ 0 \le k \le n \land \mathtt{z} = \mathtt{x} + 4(n-k) \land \underline{\mathsf{safe}(\mathtt{x} - 4k, \mathtt{y} - 4k, \mathtt{t})} \land \underline{\mathsf{word}(\mathtt{x} \neq \mathtt{z})}\}$$

while $\mathtt{x} \neq \mathtt{z}$ do

$$\{\exists k.\, (\mathtt{x} - 4k \hookrightarrow_n v_1, \ldots, v_n * \mathtt{y} - 4k \hookrightarrow_k v_1, \ldots, v_k * \mathtt{y} \hookrightarrow_{n-k} 0, \ldots, 0) \land \\ 0 \le k \le n \land \mathtt{z} = \mathtt{x} + 4(n-k) \land \underline{\mathsf{safe}(\mathtt{x} - 4k, \mathtt{y} - 4k, \mathtt{t})} \land \mathtt{x} \neq \mathtt{z}\} \qquad \text{(While)}$$

$$\{\exists k.\, (\mathtt{x} - 4k \hookrightarrow_n v_1, \ldots, v_n * \mathtt{y} - 4k \hookrightarrow_k v_1, \ldots, v_k * \mathtt{y} \hookrightarrow 0 * \mathtt{y} + 4 \hookrightarrow_{n-(k+1)} 0, \ldots, 0) \land \\ 0 \le k < n \land \mathtt{z} = \mathtt{x} + 4(n-k) \land \underline{\mathsf{safe}(\mathtt{x} - 4k, \mathtt{y} - 4k)}\}$$

$\mathtt{t} := [\mathtt{x}];$

$$\{\exists k.\, (\mathtt{x} - 4k \hookrightarrow_n v_1, \ldots, v_n * \mathtt{y} - 4k \hookrightarrow_k v_1, \ldots, v_k * \mathtt{y} \hookrightarrow 0 * \mathtt{y} + 4 \hookrightarrow_{n-(k+1)} 0, \ldots, 0) \land \\ 0 \le k < n \land \mathtt{z} = \mathtt{x} + 4(n-k) \land \underline{\mathsf{safe}(\mathtt{x} - 4k, \mathtt{y} - 4k)} \land \mathtt{t} = v_{k+1}\} \qquad \text{(Read}'\text{)}$$

$$\{\exists k.\, (\mathtt{x} - 4k \hookrightarrow_n v_1, \ldots, v_n * \mathtt{y} - 4k \hookrightarrow_k v_1, \ldots, v_k * \mathtt{y} \hookrightarrow 0 * \mathtt{y} + 4 \hookrightarrow_{n-(k+1)} 0, \ldots, 0) \land \\ 0 \le k < n \land \mathtt{z} = \mathtt{x} + 4(n-k) \land \underline{\mathsf{safe}(\mathtt{x} - 4k, \mathtt{y} - 4k, \mathtt{t})} \land \mathtt{t} = v_{k+1}\}$$

$[\mathtt{y}] := \mathtt{t};$

$$\{\exists k.\, (\mathtt{x} - 4k \hookrightarrow_n v_1, \ldots, v_n * \mathtt{y} - 4k \hookrightarrow_k v_1, \ldots, v_k * \mathtt{y} \hookrightarrow \mathtt{t} * \mathtt{y} + 4 \hookrightarrow_{n-(k+1)} 0, \ldots, 0) \land \\ 0 \le k < n \land \mathtt{z} = \mathtt{x} + 4(n-k) \land \underline{\mathsf{safe}(\mathtt{x} - 4k, \mathtt{y} - 4k)} \land \mathtt{t} = v_{k+1}\} \qquad \text{(Write)}$$

$$\{\exists k.\, (\mathtt{x} - 4k \hookrightarrow_n v_1, \ldots, v_n * \mathtt{y} - 4k \hookrightarrow_{k+1} v_1, \ldots, v_k, v_{k+1} * \mathtt{y} + 4 \hookrightarrow_{n-(k+1)} 0, \ldots, 0) \land \\ 0 \le k < n \land \mathtt{z} = \mathtt{x} + 4(n-k) \land \underline{\mathsf{safe}(\mathtt{x} - 4k, \mathtt{y} - 4k, \mathtt{t})} \land \underline{\mathsf{defined}(\mathtt{x} + 4)}\}$$

$\mathtt{x} := \mathtt{x} + 4;$

$$\{\exists k.\, (\mathtt{x} - 4(k+1) \hookrightarrow_n v_1, \ldots, v_n * \mathtt{y} - 4k \hookrightarrow_{k+1} v_1, \ldots, v_{k+1} * \mathtt{y} + 4 \hookrightarrow_{n-(k+1)} 0, \ldots, 0) \land \\ 0 \le k < n \land \mathtt{z} = \mathtt{x} + 4(n-(k+1)) \land \underline{\mathsf{safe}(\mathtt{x} - 4(k+1), \mathtt{y} - 4k, \mathtt{t})} \land \underline{\mathsf{defined}(\mathtt{y} + 4)}\} \qquad \text{(Assign}'\text{)}$$

$\mathtt{y} := \mathtt{y} + 4;$

$$\{\exists k.\, (\mathtt{x} - 4(k+1) \hookrightarrow_n v_1, \ldots, v_n * \mathtt{y} - 4(k+1) \hookrightarrow_{k+1} v_1, \ldots, v_{k+1} * \mathtt{y} \hookrightarrow_{n-(k+1)} 0, \ldots, 0) \land \\ 0 \le k < n \land \mathtt{z} = \mathtt{x} + 4(n-(k+1)) \land \underline{\mathsf{safe}(\mathtt{x} - 4(k+1), \mathtt{y} - 4(k+1), \mathtt{t})}\} \qquad \text{(Assign}'\text{)}$$

$$\{\exists k.\, (\mathtt{x} - 4k \hookrightarrow_n v_1, \ldots, v_n * \mathtt{y} - 4k \hookrightarrow_k v_1, \ldots, v_k * \mathtt{y} \hookrightarrow_{n-k} 0, \ldots, 0) \land \\ 0 \le k \le n \land \mathtt{z} = \mathtt{x} + 4(n-k) \land \underline{\mathsf{safe}(\mathtt{x} - 4k, \mathtt{y} - 4k, \mathtt{t})} \land \underline{\mathsf{word}(\mathtt{x} \neq \mathtt{z})}\}$$

od;

$$\{\exists k.\, (\mathtt{x} - 4k \hookrightarrow_n v_1, \ldots, v_n * \mathtt{y} - 4k \hookrightarrow_k v_1, \ldots, v_k * \mathtt{y} \hookrightarrow_{n-k} 0, \ldots, 0) \land \\ 0 \le k \le n \land \mathtt{z} = \mathtt{x} + 4(n-k) \land \underline{\mathsf{safe}(\mathtt{x} - 4k, \mathtt{y} - 4k, \mathtt{t})} \land \mathtt{x} = \mathtt{z}\} \qquad \text{(While)}$$

$$\{(\mathtt{x} - 4n \hookrightarrow_n v_1, \ldots, v_n * \mathtt{y} - 4n \hookrightarrow_n v_1, \ldots, v_n) \land \underline{\mathsf{safe}(\mathtt{x} - 4n, \mathtt{y} - 4n, \mathtt{t})}\}$$

$\mathtt{x} := \mathtt{x} - 4n;$

$\{(\mathtt{x} \hookrightarrow_n v_1, \ldots, v_n * \mathtt{y} - 4n \hookrightarrow_n v_1, \ldots, v_n) \wedge \underline{\mathsf{safe}(\mathtt{x}, \mathtt{y} - 4n, \mathtt{t})}\}$ (Assign′)

$\mathtt{y} := \mathtt{y} - 4n;$

$\{(\mathtt{x} \hookrightarrow_n v_1, \ldots, v_n * \mathtt{y} \hookrightarrow_n v_1, \ldots, v_n) \wedge \underline{\mathsf{safe}(\mathtt{x}, \mathtt{y}, \mathtt{t}, 0)}\}$ (Assign′)

$\mathtt{z} := 0$

$\{(\mathtt{x} \hookrightarrow_n v_1, \ldots, v_n * \mathtt{y} \hookrightarrow_n v_1, \ldots, v_n) \wedge \underline{\mathsf{safe}(\mathtt{x}, \mathtt{y}, \mathtt{t}, \mathtt{z})}\}$ (Assign′)

$\{\{\mathtt{x} \hookrightarrow_n v_1, \ldots, v_n * \mathtt{y} \hookrightarrow_n v_1, \ldots, v_n\}\}$ (Incl)

5 Soundness of Program Logic

5.1 Basic Lemmas

Lemma 1.

$$\llbracket \mathsf{defined}(\mathbf{E}) \rrbracket_{\mathbf{s}} \in \mathrm{Words}\backslash\{0\} \quad \text{iff} \quad \llbracket \mathbf{E} \rrbracket_{\mathbf{s}} \neq \mathrm{undef}$$

Proof. By a case analysis on $\llbracket \mathbf{E} \rrbracket_{\mathbf{s}}$: when $\llbracket \mathbf{E} \rrbracket_{\mathbf{s}} \in \mathrm{LogVals}$, we have $\llbracket \mathbf{E} = \mathbf{E} \rrbracket_{\mathbf{s}} = 1 \in \mathrm{Words}\backslash\{0\}$; when $\llbracket \mathbf{E} \rrbracket_{\mathbf{s}} = \mathrm{undef}$, we have $\llbracket \mathbf{E} = \mathbf{E} \rrbracket_{\mathbf{s}} = \mathrm{undef} \notin \mathrm{Words}\backslash\{0\}$. $\square$

Lemma 2.

$$\mathbf{s} \sim_{\mathbf{T}} s \wedge \llbracket E \rrbracket_{\mathbf{s}} \neq \mathrm{undef} \implies \llbracket E \rrbracket_s = \mathrm{phyv}_{\mathbf{T}}(\llbracket E \rrbracket_{\mathbf{s}}) \neq \mathrm{undef}$$

Proof. It can be shown by induction over E.

- When $E = \mathtt{x}$:
  From $\mathbf{s} \sim_{\mathbf{T}} s$, we have $\mathrm{phyv}_{\mathbf{T}}(\mathbf{s}(\mathtt{x})) = s(\mathtt{x}) \neq \mathrm{undef}$.
- When $E = w$:
  $\mathrm{phyv}_{\mathbf{T}}(\llbracket w \rrbracket_{\mathbf{s}}) = \mathrm{phyv}_{\mathbf{T}}(w) = w = \llbracket w \rrbracket_s \neq \mathrm{undef}$.
- When $E = (E_1 \star E_2)$:
  From $\llbracket E \rrbracket_{\mathbf{s}} \neq \mathrm{undef}$, we have the following cases:
  - When $\llbracket E_1 \rrbracket_{\mathbf{s}} = w_1 \in \mathrm{Words} \wedge \llbracket E_2 \rrbracket_{\mathbf{s}} = w_2 \in \mathrm{Words} \wedge \llbracket E \rrbracket_{\mathbf{s}} = w_1 \star w_2 \neq \mathrm{undef}$:
    By induction hypothesis, we have $\llbracket E_k \rrbracket_s = \mathrm{phyv}_{\mathbf{T}}(w_k) = w_k$ for $k = 1, 2$.
    Thus, we have $\mathrm{phyv}_{\mathbf{T}}(\llbracket E \rrbracket_{\mathbf{s}}) = \mathrm{phyv}_{\mathbf{T}}(w_1 \star w_2) = w_1 \star w_2 = \llbracket E \rrbracket_s \neq \mathrm{undef}$.
  - When $\star = + \wedge \llbracket E_k \rrbracket_{\mathbf{s}} = \boldsymbol{\ell} \widehat{+} i \wedge \llbracket E_{3-k} \rrbracket_{\mathbf{s}} = w \wedge \llbracket E \rrbracket_{\mathbf{s}} = \boldsymbol{\ell} \widehat{+} (i + w)$:
    By induction hypothesis, we have $\llbracket E_k \rrbracket_s = \mathrm{phyv}_{\mathbf{T}}(\boldsymbol{\ell} \widehat{+} i) = p + i$ for $(p, n) = \mathbf{T}(\boldsymbol{\ell})$; and $\llbracket E_{3-k} \rrbracket_s = \mathrm{phyv}_{\mathbf{T}}(w) = w$.
    So we have $\mathrm{phyv}_{\mathbf{T}}(\llbracket E \rrbracket_{\mathbf{s}}) = \mathrm{phyv}_{\mathbf{T}}(\boldsymbol{\ell} \widehat{+} (i + w)) = p + (i + w) = (p + i) + w = \llbracket E \rrbracket_s \neq \mathrm{undef}$.
  - When $\star = - \wedge \llbracket E_1 \rrbracket_{\mathbf{s}} = \boldsymbol{\ell} \widehat{+} i \wedge \llbracket E_2 \rrbracket_{\mathbf{s}} = w \wedge \llbracket E \rrbracket_{\mathbf{s}} = \boldsymbol{\ell} \widehat{+} (i - w)$:
    By induction hypothesis, we have $\llbracket E_1 \rrbracket_s = \mathrm{phyv}_{\mathbf{T}}(\boldsymbol{\ell} \widehat{+} i) = p + i$ for $(p, n) = \mathbf{T}(\boldsymbol{\ell})$; and $\llbracket E_2 \rrbracket_s = \mathrm{phyv}_{\mathbf{T}}(w) = w$.
    So we have $\mathrm{phyv}_{\mathbf{T}}(\llbracket E \rrbracket_{\mathbf{s}}) = \mathrm{phyv}_{\mathbf{T}}(\boldsymbol{\ell} \widehat{+} (i - w)) = p + (i - w) = (p + i) - w = \llbracket E \rrbracket_s \neq \mathrm{undef}$.
  - When $\star = - \wedge \llbracket E_1 \rrbracket_{\mathbf{s}} = \boldsymbol{\ell} \widehat{+} i \wedge \llbracket E_2 \rrbracket_{\mathbf{s}} = \boldsymbol{\ell} \widehat{+} j \wedge \llbracket E \rrbracket_{\mathbf{s}} = i - j$:
    By induction hypothesis, we have $\llbracket E_1 \rrbracket_s = \mathrm{phyv}_{\mathbf{T}}(\boldsymbol{\ell} \widehat{+} i) = p + i$ and $\llbracket E_2 \rrbracket_s = \mathrm{phyv}_{\mathbf{T}}(\boldsymbol{\ell} \widehat{+} j) = p + j$ for $(p, n) = \mathbf{T}(\boldsymbol{\ell})$.
    So we have $\mathrm{phyv}_{\mathbf{T}}(\llbracket E \rrbracket_{\mathbf{s}}) = \mathrm{phyv}_{\mathbf{T}}(i - j) = i - j = (p + i) - (p + j) = \llbracket E \rrbracket_s \neq \mathrm{undef}$.
  - When $\star = < \wedge \llbracket E_1 \rrbracket_{\mathbf{s}} = \boldsymbol{\ell} \widehat{+} i \wedge \llbracket E_2 \rrbracket_{\mathbf{s}} = \boldsymbol{\ell} \widehat{+} j \wedge \llbracket E \rrbracket_{\mathbf{s}} = i < j$:
    By induction hypothesis, we have $\llbracket E_1 \rrbracket_s = \mathrm{phyv}_{\mathbf{T}}(\boldsymbol{\ell} \widehat{+} i) = p + i$ and $\llbracket E_2 \rrbracket_s = \mathrm{phyv}_{\mathbf{T}}(\boldsymbol{\ell} \widehat{+} j) = p + j$ for $(p, n) = \mathbf{T}(\boldsymbol{\ell})$.
    So we have $\mathrm{phyv}_{\mathbf{T}}(\llbracket E \rrbracket_{\mathbf{s}}) = \mathrm{phyv}_{\mathbf{T}}(i < j) = i < j = (p + i) < (p + j) = \llbracket E \rrbracket_s \neq \mathrm{undef}$.
  - When $\star = = \wedge \llbracket E_1 \rrbracket_{\mathbf{s}} = \boldsymbol{\ell} \widehat{+} i \wedge \llbracket E_2 \rrbracket_{\mathbf{s}} = \boldsymbol{\ell} \widehat{+} j \wedge \llbracket E \rrbracket_{\mathbf{s}} = (i = j)$:
    By induction hypothesis, we have $\llbracket E_1 \rrbracket_s = \mathrm{phyv}_{\mathbf{T}}(\boldsymbol{\ell} \widehat{+} i) = p + i$ and $\llbracket E_2 \rrbracket_s = \mathrm{phyv}_{\mathbf{T}}(\boldsymbol{\ell} \widehat{+} j) = p + j$ for $(p, n) = \mathbf{T}(\boldsymbol{\ell})$.
    So we have $\mathrm{phyv}_{\mathbf{T}}(\llbracket E \rrbracket_{\mathbf{s}}) = \mathrm{phyv}_{\mathbf{T}}(i = j) = (i = j) = ((p + i) = (p + j)) = \llbracket E \rrbracket_s \neq \mathrm{undef}$.

  - When $\star = {=} \wedge \llbracket E_1 \rrbracket_{\mathbf{s}} = \boldsymbol{\ell} \mathbin{\hat{+}} 0 \wedge \llbracket E_2 \rrbracket_{\mathbf{s}} = \boldsymbol{\ell}' \mathbin{\hat{+}} 0 \wedge \llbracket E \rrbracket_{\mathbf{s}} = (\boldsymbol{\ell} = \boldsymbol{\ell}')$:
    By induction hypothesis, we have $[\![E_1]\!]_s = \mathrm{phyv}_{\mathbf{T}}(\boldsymbol{\ell} \mathbin{\hat{+}} 0) = p$ and $[\![E_2]\!]_s = \mathrm{phyv}_{\mathbf{T}}(\boldsymbol{\ell}' \mathbin{\hat{+}} 0) = p'$ for $(p, n) = \mathbf{T}(\boldsymbol{\ell})$ and $(p', n') = \mathbf{T}(\boldsymbol{\ell}')$.
    So we have $\mathrm{phyv}_{\mathbf{T}}(\llbracket E \rrbracket_{\mathbf{s}}) = \mathrm{phyv}_{\mathbf{T}}(\boldsymbol{\ell} = \boldsymbol{\ell}') = (\boldsymbol{\ell} = \boldsymbol{\ell}') = (p = p') = [\![E]\!]_s \neq \mathrm{undef}$.
  - When $\star = {=} \wedge \llbracket E_k \rrbracket_{\mathbf{s}} = \boldsymbol{\ell} \mathbin{\hat{+}} 4i \wedge i \geq 0 \wedge \llbracket E_{3-k} \rrbracket_{\mathbf{s}} \in \mathrm{NonPtrs} \wedge \llbracket E \rrbracket_{\mathbf{s}} = 0$
    By induction hypothesis, we have $[\![E_k]\!]_s = \mathrm{phyv}_{\mathbf{T}}(\boldsymbol{\ell} \mathbin{\hat{+}} 4i) = p + 4i \in \mathrm{Ptrs}$ for $(p, n) = \mathbf{T}(\boldsymbol{\ell})$, and $[\![E_{3-k}]\!]_s = \mathrm{phyv}_{\mathbf{T}}(\llbracket E_k \rrbracket_{\mathbf{s}}) = \llbracket E_k \rrbracket_{\mathbf{s}} \in \mathrm{NonPtrs}$.
    So we have $\mathrm{phyv}_{\mathbf{T}}(\llbracket E \rrbracket_{\mathbf{s}}) = \mathrm{phyv}_{\mathbf{T}}(0) = 0 = ([\![E_k]\!]_s = [\![E_{3-k}]\!]_s) = [\![E]\!]_s \neq \mathrm{undef}$.

- When $E = \mathsf{not}\ E'$:
  From $\llbracket E \rrbracket_{\mathbf{s}} \neq \mathrm{undef}$, we have $\llbracket E' \rrbracket_{\mathbf{s}} = w \in \mathrm{Words} \wedge \llbracket E \rrbracket_{\mathbf{s}} = \mathsf{not}\ w$.
  By induction hypothesis, we have $[\![E']\!]_s = \mathrm{phyv}_{\mathbf{T}}(w) = w$.
  Thus, we have $\mathrm{phyv}_{\mathbf{T}}(\llbracket E \rrbracket_{\mathbf{s}}) = \mathrm{phyv}_{\mathbf{T}}(\mathsf{not}\ w) = \mathsf{not}\ w = [\![E]\!]_s \neq \mathrm{undef}$.

$\square$

Corollary 3.

$$\mathbf{s} \sim_{\mathbf{T}} s \wedge \llbracket E \rrbracket_{\mathbf{s}} = \boldsymbol{\ell} \mathbin{\hat{+}} i \implies \boldsymbol{\ell} \in \mathrm{dom}(\mathbf{T})$$

Proof. By Lemma 2, we have $\mathrm{phyv}_{\mathbf{T}}(\boldsymbol{\ell} \mathbin{\hat{+}} i) \neq \mathrm{undef}$, from which it follows that $\boldsymbol{\ell} \in \mathrm{dom}(\mathbf{T})$. $\square$

Lemma 4. When $\llbracket \mathbf{E}' \rrbracket_{\mathbf{s}} \neq \mathrm{undef}$,

(1) $\llbracket \mathbf{E}[\mathbf{E}'/\mathrm{x}] \rrbracket_{\mathbf{s}} = \llbracket \mathbf{E} \rrbracket_{(\mathbf{s} \mid \mathrm{x} \mapsto \llbracket \mathbf{E}' \rrbracket_{\mathbf{s}})}$

(2) $\mathbf{s}, \mathbf{h} \models_{\mathbf{L}} \mathbf{P}[\mathbf{E}'/\mathrm{x}] \quad \text{iff} \quad (\mathbf{s} \mid \mathrm{x} \mapsto \llbracket \mathbf{E}' \rrbracket_{\mathbf{s}}), \mathbf{h} \models_{\mathbf{L}} \mathbf{P}$

Proof. (1) can be shown by an induction on $\mathbf{E}$. When $\mathbf{E} = \mathrm{y}$: if $\mathrm{y} = \mathrm{x}$, then both LHS and RHS are equal to $\llbracket \mathbf{E}' \rrbracket_{\mathbf{s}}$; otherwise, both are equal to $\mathbf{s}(\mathrm{y})$. The other cases are straightforward.
(2) follows from (1) by a simple induction on $\mathbf{P}$. $\square$

Lemma 5.

(1) $(\forall \mathrm{x} \in \mathrm{FPV}(\mathbf{E}).\ \mathbf{s}(\mathrm{x}) = \mathbf{s}'(\mathrm{x})) \implies \llbracket \mathbf{E} \rrbracket_{\mathbf{s}} = \llbracket \mathbf{E} \rrbracket_{\mathbf{s}'}$

(2) $(\forall \mathrm{x} \in \mathrm{FPV}(\mathbf{P}).\ \mathbf{s}(\mathrm{x}) = \mathbf{s}'(\mathrm{x})) \implies (\mathbf{s}, \mathbf{h} \models_{\mathbf{L}} \mathbf{P} \iff \mathbf{s}', \mathbf{h} \models_{\mathbf{L}} \mathbf{P})$

Proof.

(1) : By a simple induction on $\mathbf{E}$.

(2) : By a simple induction on $\mathbf{P}$ using (1).

$\square$

Lemma 6. $\mathbf{s}, \mathbf{h} \models_{\mathbf{L}} P \iff \mathbf{s}, \mathbf{h} \models P$

Proof. By a simple induction on P. $\square$

Lemma 7.

$$\mathbf{s}, \mathbf{h} \models_{\mathbf{L}} (\exists v.\, \mathbf{P})[\rho] \iff \exists \mathbf{v} \in \mathrm{LogVals}.\ \mathbf{s}, \mathbf{h} \models_{\mathbf{L}} \mathbf{P}[(\rho \mid v \mapsto \mathbf{v})]$$

Proof. Choose a fresh $u \notin \mathrm{dom}(\rho)$. Then the goal follows from

- $(\exists v.\, \mathbf{P})[\rho] \approx_\alpha (\exists u.\, \mathbf{P}[u/v])[\rho] = \exists u.\, \mathbf{P}[u/v][\rho]$,
- $\mathbf{s}, \mathbf{h} \models_{\mathbf{L}} \exists u.\, \mathbf{P}[u/v][\rho] \quad\iff\quad \exists \mathbf{v} \in \text{LogVals}.\ \mathbf{s}, \mathbf{h} \models_{\mathbf{L}} \mathbf{P}[u/v][\rho][\mathbf{v}/u]$,
- $\mathbf{P}[u/v][\rho][\mathbf{v}/u] = \mathbf{P}[u/v][\mathbf{v}/u][\rho] = \mathbf{P}[\mathbf{v}/v][\rho] = \mathbf{P}[(\rho \mid v \mapsto \mathbf{v})]$.

□

Lemma 8.

$$R \subseteq R' \wedge h \subseteq h' \wedge \sigma \subseteq \sigma' \implies \text{reach}(R, h, \sigma) \subseteq \text{reach}(R', h', \sigma')$$

Proof. One can easily show that $\text{reach}_n(R, h, \sigma) \subseteq \text{reach}_n(R', h', \sigma')$ by induction on n. □

Lemma 9. When $\overline{\text{dom}}(\sigma) \subseteq \text{dom}(h)$ and $\sigma \subseteq \sigma'$,

$$\text{reach}(\text{dom}(\sigma), h, \sigma') \subseteq \text{dom}(\sigma) \quad\iff\quad \forall p \in \overline{\text{dom}}(\sigma).\ h(p) \in \text{dom}(\sigma) \cup \text{NonPtrs}$$

Proof.

- $\implies$ part:
  Let $p \in \overline{\text{dom}}(\sigma)$. As $\overline{\text{dom}}(\sigma) \subseteq \text{dom}(h)$, we have $h(p) \in \text{Words}$.
  If $h(p) \in \text{NonPtrs}$, then trivially $h(p) \in \text{dom}(\sigma) \cup \text{NonPtrs}$.
  If $h(p) \in \text{Ptrs}$, then $h(p) \in \text{reach}_1(\text{dom}(\sigma), h, \sigma') \subseteq \text{dom}(\sigma) \subseteq \text{dom}(\sigma) \cup \text{NonPtrs}$.
- $\impliedby$ part:
  We prove $\text{reach}_n(\text{dom}(\sigma), h, \sigma') \subseteq \text{dom}(\sigma)$ by induction on n.
  Base case: $\text{reach}_0(\text{dom}(\sigma), h, \sigma') = \text{dom}(\sigma) \subseteq \text{dom}(\sigma)$.
  Inductive step: $\text{reach}_{n+1}(\text{dom}(\sigma), h, \sigma') \subseteq \text{dom}(\sigma)$ directly follows from
  (1) the induction hypothesis: $\text{reach}_n(\text{dom}(\sigma), h, \sigma') \subseteq \text{dom}(\sigma)$; and
  (2) the fact that $\forall p \in \overline{\text{dom}}(\sigma).\ h(p) \in \text{Ptrs} \implies h(p) \in \text{dom}(\sigma)$.

□

Lemma 10.

$$\mathbf{h} \sim_{\mathbf{T}} h \wedge \mathbf{h} :: \mathbf{T} \wedge \sigma \supseteq \text{shape}(\mathbf{T}) \quad\implies\quad \text{reach}(\text{dom}(\text{shape}(\mathbf{T})), h, \sigma) \subseteq \text{dom}(\text{shape}(\mathbf{T}))$$

Proof.

- Assume: $\mathbf{h} \approx_{\mathbf{T}} h$ and let $\sigma \supseteq \text{shape}(\mathbf{T})$.
- As $\text{phyh}_{\mathbf{T}}(\mathbf{h}) \subseteq h$, we have $\overline{\text{dom}}(\text{shape}(\mathbf{T})) = \text{dom}(\text{phyh}_{\mathbf{T}}(\mathbf{h})) \subseteq \text{dom}(h)$.
- To show: $\text{reach}(\text{dom}(\text{shape}(\mathbf{T})), h, \sigma) \subseteq \text{dom}(\text{shape}(\mathbf{T}))$.
- By Lemma 9, it suffices to show that $\forall p \in \overline{\text{dom}}(\text{shape}(\mathbf{T})).\ h(p) \in \text{dom}(\text{shape}(\mathbf{T})) \cup \text{NonPtrs}$.
- Let $p \in \overline{\text{dom}}(\text{shape}(\mathbf{T}))$.
  Since $\text{phyh}_{\mathbf{T}}(\mathbf{h}) \subseteq h$, there exists $\boldsymbol{\ell}', p', n', i$ such that $(p', n') = \mathbf{T}(\boldsymbol{\ell}') \wedge i < n' \wedge p = p' + 4i \wedge h(p) = \text{phyv}_{\mathbf{T}}(\mathbf{h}(\boldsymbol{\ell}')(i))$.
- From $\mathbf{h} :: \mathbf{T}$, it follows that $\mathbf{h}(\boldsymbol{\ell}')(i) \in \text{Safe}(\text{dom}(\mathbf{T}))$. Thus, we have two cases.

- When $\mathbf{h}(\boldsymbol{\ell}')(i) \in \mathrm{NonPtrs}$:
  $h(p) = \mathrm{phyv}_{\mathbf{T}}(\mathbf{h}(\boldsymbol{\ell}')(i)) = \mathbf{h}(\boldsymbol{\ell}')(i) \in \mathrm{NonPtrs} \subseteq \mathrm{dom}(\mathrm{shape}(\mathbf{T})) \cup \mathrm{NonPtrs}$.
- When $\mathbf{h}(\boldsymbol{\ell}')(i) = \boldsymbol{\ell}''\widehat{+}0$ for $\boldsymbol{\ell}'' \in \mathrm{dom}(\mathbf{T})$:
  $h(p) = \mathrm{phyv}_{\mathbf{T}}(\boldsymbol{\ell}''\widehat{+}0) = p''$ for $(p'', n'') = \mathbf{T}(\boldsymbol{\ell}'')$.
  Thus, $h(p) \in \mathrm{dom}(\mathrm{shape}(\mathbf{T})) \subseteq \mathrm{dom}(\mathrm{shape}(\mathbf{T})) \cup \mathrm{NonPtrs}$.

□

5.2 Soundness of Inner-level Rules

Definition 1 (Generalized triple)**.**

$$\begin{aligned}
\{\mathbf{P}\}\ C\ \{\mathbf{Q}\} : k \ \text{ iff } & \forall j \le k.\ \forall \rho \in \mathrm{Env}(\mathrm{FLV}(\mathbf{P}, \mathbf{Q})), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'. \\
& \mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge \mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge C, s, h \rightsquigarrow^{j} C', s', h' \implies \\
& \quad (C', s', h' \rightsquigarrow -) \vee \\
& \quad (\exists \mathbf{s}', \mathbf{h}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathbf{Q}[\rho] \wedge \\
& \qquad\qquad (\forall \mathtt{x} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathtt{x}) = \mathbf{s}(\mathtt{x})) \wedge \mathbf{s}' \sim_{\mathbf{T}} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h')
\end{aligned}$$

5.2.1 Skip

Theorem 1 (Soundness: Skip)**.**

$$\frac{}{[\mathsf{true}]\ \mathsf{skip}\ [\mathsf{true}]}$$

Proof.

- Assume: $\mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$ such that
  ✓ $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathsf{true} \wedge \mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge \mathsf{skip}, s, h \rightsquigarrow^{*} C', s', h'$
- skip, s, h does not diverge as it takes no step.
- To show:
  $(*)$ $C', s', h' \rightsquigarrow -$; or
  $(**)$ $\exists \mathbf{s}', \mathbf{h}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathsf{true} \wedge$
  $(\forall \mathtt{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathtt{y}) = \mathbf{s}(\mathtt{y})) \wedge \mathbf{s}' \sim_{\mathbf{T}} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h'$
- From $\mathsf{skip}, s, h \rightsquigarrow^{*} C', s', h'$, we have $C' = \mathsf{skip}$, $s' = s$ and $h' = h$.
- $(**)$ holds by letting $\mathbf{s}' = \mathbf{s}$ and $\mathbf{h}' = \mathbf{h}$.

□

5.2.2 Assign

Theorem 2 (Soundness: Assign)**.**

$$\frac{}{[\mathtt{x} = v \wedge \mathsf{defined}(E)]\ \mathtt{x} := E\ [\mathtt{x} = E[v/\mathtt{x}]]}$$

Proof.

- Substitute the logical variables v with an arbitrary logical words $\mathbf{v}$.

- Assume: $\mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$ such that
  ✓ $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} (\mathtt{x} = \mathbf{v} \land \mathsf{defined}(E)) \land \mathbf{s} \sim_{\mathbf{T}} s \land \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \land \mathtt{x} := E, s, h \rightsquigarrow^{*} C', s', h'$

- $\mathtt{x} := E, s, h$ does not diverge as it takes at most one step.

- To show:
  $(*)$ $C', s', h' \rightsquigarrow -$; or
  $(**)$ $\exists \mathbf{s}', \mathbf{h}'.\ C' = \mathsf{skip} \land \mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} (\mathtt{x} = E[\mathbf{v}/\mathtt{x}]) \land$
  $(\forall \mathtt{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathtt{y}) = \mathbf{s}(\mathtt{y})) \land \mathbf{s}' \sim_{\mathbf{T}} s' \land \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h'$

- As $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} (\mathtt{x} = \mathbf{v} \land \mathsf{defined}(E))$ and $\mathbf{s} \sim_{\mathbf{T}} s$, by Lemmas 1 and 2 we have
  ✓ $\mathbf{s}(\mathtt{x}) = \mathbf{v}$
  ✓ $\llbracket E \rrbracket_s = \mathrm{phyv}_{\mathbf{T}}(\boldsymbol{\llbracket} E \boldsymbol{\rrbracket}_{\mathbf{s}}) \neq \mathrm{undef}$

- From $\mathtt{x} := E, s, h \rightsquigarrow^{*} C', s', h'$, we have the following two cases:

- When $C' = (\mathtt{x} := E) \land s' = s \land h' = h$:
  As $\llbracket E \rrbracket_s \neq \mathrm{undef}$, it follows that $\mathtt{x} := E, s, h \rightsquigarrow \mathsf{skip}, (s \mid \mathtt{x} \mapsto \llbracket E \rrbracket_s), h$. Thus, $(*)$ holds.

- When $C' = \mathsf{skip} \land s' = (s \mid \mathtt{x} \mapsto \llbracket E \rrbracket_s) \land h' = h$:
  $(**)$ holds by letting $\mathbf{s}' = (\mathbf{s} \mid \mathtt{x} \mapsto \boldsymbol{\llbracket} E \boldsymbol{\rrbracket}_{\mathbf{s}})$ and $\mathbf{h}' = \mathbf{h}$ because
  - $\mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} (\mathtt{x} = E[\mathbf{v}/\mathtt{x}])$ follows from

    $$\mathbf{s}'(\mathtt{x}) = \boldsymbol{\llbracket} E \boldsymbol{\rrbracket}_{\mathbf{s}} = \boldsymbol{\llbracket} E \boldsymbol{\rrbracket}_{(\mathbf{s}' \mid \mathtt{x} \mapsto \mathbf{v})} = \boldsymbol{\llbracket} E[\mathbf{v}/\mathtt{x}] \boldsymbol{\rrbracket}_{\mathbf{s}'} \neq \mathrm{undef}\,,$$

    which holds by Lemmas 5 and 4 as $\mathbf{s}(\mathtt{x}) = \mathbf{v}$; and
  - $\mathbf{s}' \sim_{\mathbf{T}} s'$ holds since $\mathbf{s} \sim_{\mathbf{T}} s$ and $\llbracket E \rrbracket_s = \mathrm{phyv}_{\mathbf{T}}(\boldsymbol{\llbracket} E \boldsymbol{\rrbracket}_{\mathbf{s}})$.

□

5.2.3 Read

Theorem 3 (Soundness: Read)**.**

$$\frac{}{[\mathtt{x} = u \land E \hookrightarrow v]\ \mathtt{x} := [E]\ [\mathtt{x} = v \land E[u/\mathtt{x}] \hookrightarrow v]}$$

Proof.

- Substitute the logical variables u, v with two arbitrary logical words $\mathbf{v}_1, \mathbf{v}_2$.

- Assume: $\mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$ such that
  ✓ $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} (\mathtt{x} = \mathbf{v}_1 \land E \hookrightarrow \mathbf{v}_2) \land \mathbf{s} \sim_{\mathbf{T}} s \land \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \land \mathtt{x} := [E], s, h \rightsquigarrow^{*} C', s', h'$

- $\mathtt{x} := [E], s, h$ does not diverge as it takes at most one step.

- To show:
  $(*)$ $C', s', h' \rightsquigarrow -$; or
  $(**)$ $\exists \mathbf{s}', \mathbf{h}'.\ C' = \mathsf{skip} \land \mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} (\mathtt{x} = \mathbf{v}_2 \land E[\mathbf{v}_1/\mathtt{x}] \hookrightarrow \mathbf{v}_2) \land$
  $(\forall \mathtt{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathtt{y}) = \mathbf{s}(\mathtt{y})) \land \mathbf{s}' \sim_{\mathbf{T}} s' \land \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h'$

- From $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} (\mathtt{x} = \mathbf{v}_1 \wedge E \hookrightarrow \mathbf{v}_2)$, by Corollary 3 we have
  ✓ $\mathbf{s}(\mathrm{x}) = \mathbf{v}_1 \wedge [\![E]\!]_{\mathbf{s}} = \boldsymbol{\ell}\widehat{+}4i \wedge \mathbf{h}(\boldsymbol{\ell})(i) = \mathbf{v}_2 \wedge \boldsymbol{\ell} \in \mathrm{dom}(\mathbf{T})$.

- As $\mathbf{s} \sim_{\mathbf{T}} s$ and $[\![E]\!]_{\mathbf{s}} = \boldsymbol{\ell}\widehat{+}4i$, by Lemma 2 we have
  ✓ $[\![E]\!]_s = \mathrm{phyv}_{\mathbf{T}}(\boldsymbol{\ell}\widehat{+}4i) = p + 4i$ for $(p, n) = \mathbf{T}(\boldsymbol{\ell})$.

- From $\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} : \mathbf{T} \wedge (p, n) = \mathbf{T}(\boldsymbol{\ell}) \wedge \mathbf{h}(\boldsymbol{\ell})(i) \neq \mathrm{undef}$, we have
  ✓ $i < n$.

- From $\mathrm{phyh}_{\mathbf{T}}(\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}}) \subseteq h \wedge (p, n) = \mathbf{T}(\boldsymbol{\ell}) \wedge i < n$, we have
  ✓ $h(p + 4i) = \mathrm{phyv}_{\mathbf{T}}(\mathbf{h}(\boldsymbol{\ell})(i)) \neq \mathrm{undef}$.

- From $\mathtt{x} := [E], s, h \rightsquigarrow^* C', s', h'$, we have the following two cases:

- When $C' = (\mathtt{x} := [E]) \wedge s' = s \wedge h' = h$:
  As $[\![E]\!]_s = p + 4i \wedge h(p + 4i) \neq \mathrm{undef}$, we have $\mathtt{x} := [E], s, h \rightsquigarrow \mathsf{skip}, (s \mid \mathtt{x} \mapsto h(p + 4i)), h$.
  Thus, $(*)$ holds.

- When $C' = \mathsf{skip} \wedge s' = (s \mid \mathtt{x} \mapsto h(p + 4i)) \wedge h' = h$:
  $(**)$ holds by letting $\mathbf{s}' = (\mathbf{s} \mid \mathtt{x} \mapsto \mathbf{h}(\boldsymbol{\ell})(i))$ and $\mathbf{h}' = \mathbf{h}$ because

  - $\mathbf{s}' \sim_{\mathbf{T}} s'$ holds since $\mathbf{s} \sim_{\mathbf{T}} s$ and $h(p + 4i) = \mathrm{phyv}_{\mathbf{T}}(\mathbf{h}(\boldsymbol{\ell})(i))$;
  - $\mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathtt{x} = \mathbf{v}_2$ holds since $\mathbf{s}'(\mathrm{x}) = \mathbf{h}(\boldsymbol{\ell})(i) = \mathbf{v}_2$; and
  - $\mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} E[\mathbf{v}_1/\mathrm{x}] \hookrightarrow \mathbf{v}_2$ follows from
    $$\begin{aligned} (1)\ [\![E[\mathbf{v}_1/\mathrm{x}]]\!]_{\mathbf{s}'} &= [\![E]\!]_{(\mathbf{s}' \mid \mathtt{x} \mapsto \mathbf{v}_1)} && \text{(by Lemma 4)} \\ &= [\![E]\!]_{(\mathbf{s} \mid \mathtt{x} \mapsto \mathbf{v}_1)} && \text{(as } (\mathbf{s}' \mid \mathtt{x} \mapsto \mathbf{v}_1) = (\mathbf{s} \mid \mathtt{x} \mapsto \mathbf{v}_1)\text{)} \\ &= [\![E]\!]_{\mathbf{s}} && \text{(by Lemma 5, as } \mathbf{s}(\mathrm{x}) = \mathbf{v}_1\text{)} \\ &= \boldsymbol{\ell}\widehat{+}4i\,, \end{aligned}$$
    (2) $\mathbf{h}'(\boldsymbol{\ell})(i) = \mathbf{h}(\boldsymbol{\ell})(i) = \mathbf{v}_2 \neq \mathrm{undef}$.

□

5.2.4 Write

Theorem 4 (Soundness: Write)**.**

$$\frac{}{[E \hookrightarrow - \wedge \mathsf{safe}(E')]\ [E] := E'\ [E \hookrightarrow E']}$$

Proof.

- Assume: $\mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$ such that
  ✓ $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} (E \hookrightarrow - \wedge \mathsf{safe}(E')) \wedge \mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge [E] := E', s, h \rightsquigarrow^* C', s', h'$

- $[E] := E', s, h$ does not diverge as it takes at most one step.

- To show:
  $(*)$ $C', s', h' \rightsquigarrow -$; or
  $(**)$ $\exists \mathbf{s}', \mathbf{h}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} E \hookrightarrow E' \wedge$
  $(\forall \mathrm{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathbf{s}' \sim_{\mathbf{T}} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h'$

- From $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} (E \hookrightarrow - \wedge \mathsf{safe}(E'))$, by Corollary 3 we have
  ✓ $\llbracket E \rrbracket_{\mathbf{s}} = \boldsymbol{\ell} \widehat{+} 4i \wedge \mathbf{h}(\boldsymbol{\ell})(i) \neq \text{undef} \wedge \boldsymbol{\ell} \in \mathrm{dom}(\mathbf{T}) \ \wedge \llbracket E' \rrbracket_{\mathbf{s}} \in \mathrm{Safe}(\mathrm{dom}(\mathbf{T}))$.

- As $\mathbf{s} \sim_{\mathbf{T}} s$ and $\llbracket E \rrbracket_{\mathbf{s}} = \boldsymbol{\ell} \widehat{+} 4i$, by Lemma 2 we have
  ✓ $\llbracket E \rrbracket_{s} = \mathrm{phyv}_{\mathbf{T}}(\boldsymbol{\ell} \widehat{+} 4i) = p + 4i$ for $(p, n) = \mathbf{T}(\boldsymbol{\ell})$.

- As $\mathbf{s} \sim_{\mathbf{T}} s$ and $\wedge \llbracket E' \rrbracket_{\mathbf{s}} \neq \text{undef}$, by Lemma 2 we have
  ✓ $\llbracket E' \rrbracket_{s} = \mathrm{phyv}_{\mathbf{T}}(\llbracket E' \rrbracket_{\mathbf{s}}) \neq \text{undef}$.

- From $\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} : \mathbf{T} \wedge (p, n) = \mathbf{T}(\boldsymbol{\ell}) \wedge \mathbf{h}(\boldsymbol{\ell})(i) \neq \text{undef}$, we have
  ✓ $i < n$.

- From $\mathrm{phyh}_{\mathbf{T}}(\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}}) \subseteq h \wedge (p, n) = \mathbf{T}(\boldsymbol{\ell}) \wedge i < n \wedge \mathbf{h}(\boldsymbol{\ell})(i) \neq \text{undef}$, we have
  ✓ $\mathrm{phyv}_{\mathbf{T}}(\mathbf{h}(\boldsymbol{\ell})(i)) = h(p + 4i) \neq \text{undef}$.

- From $[E] := E', s, h \rightsquigarrow^{*} C', s', h'$, we have the following two cases:

- When $C' = ([E] := E') \wedge s' = s \wedge h' = h$:
  As $\llbracket E \rrbracket_{s} = p + 4i \wedge h(p + 4i) \neq \text{undef} \wedge \llbracket E' \rrbracket_{s} \neq \text{undef}$, we have

  $$[E] := E', s, h \rightsquigarrow \mathsf{skip}, s, (h \mid p + 4i \mapsto \llbracket E' \rrbracket_{s}) \,.$$

  Thus, $(*)$ holds.

- When $C' = \mathsf{skip} \wedge s' = s \wedge h' = (h \mid p + 4i \mapsto \llbracket E' \rrbracket_{s})$:
  Let $\mathbf{s}' = \mathbf{s}$ and $\mathbf{h}' = (\mathbf{h} \mid (\boldsymbol{\ell}, i) \mapsto \llbracket E' \rrbracket_{\mathbf{s}})$.
  To prove $(**)$, it suffices to show that
  (1) $\mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} E \hookrightarrow E'$; and
  (2) $\mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h'$.

- $\mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} E \hookrightarrow E'$ follows from
  - $\llbracket E \rrbracket_{\mathbf{s}'} = \llbracket E \rrbracket_{\mathbf{s}} = \boldsymbol{\ell} \widehat{+} 4i$;
  - $\llbracket E' \rrbracket_{\mathbf{s}'} = \llbracket E' \rrbracket_{\mathbf{s}} = \mathbf{h}'(\boldsymbol{\ell})(i) \neq \text{undef}$.

- We show $\mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h'$ as follows.

- From $\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} : \mathbf{T} \wedge \mathrm{Span}(\mathbf{h}') = \mathrm{Span}(\mathbf{h})$, we have
  ✓ $\mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} : \mathbf{T}$.

- From $\mathrm{phyh}_{\mathbf{T}}(\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}}) \subseteq h \wedge \llbracket E' \rrbracket_{s} = \mathrm{phyv}_{\mathbf{T}}(\llbracket E' \rrbracket_{\mathbf{s}})$, we have
  ✓ $\mathrm{phyh}_{\mathbf{T}}(\mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}}) \subseteq h'$.

- From $\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} :: \mathbf{T} \wedge \llbracket E' \rrbracket_{\mathbf{s}} \in \mathrm{Safe}(\mathrm{dom}(\mathbf{T}))$, we have
  ✓ $\mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} :: \mathbf{T}$.

- Now it suffices to show $\mathrm{shape}(\mathbf{T}) \subseteq I_{\mathrm{gc}}(\mathrm{dom}(\mathrm{shape}(\mathbf{T})), h')$.

- From $\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h$, we have σ such that
  ✓ $\sigma = I_{\mathrm{gc}}(\mathrm{dom}(\mathrm{shape}(\mathbf{T})), h) \wedge \mathrm{shape}(\mathbf{T}) \subseteq \sigma$.

- By GCAxiom_2 for $\sigma = I_{\text{gc}}(\text{dom}(\text{shape}(\mathbf{T})), h)$, we have σ' such that
  ✓ $\sigma' = I_{\text{gc}}(\text{dom}(\text{shape}(\mathbf{T})), h') \wedge \sigma' \subseteq \sigma$
  because
  - $\overline{\text{dom}}(\sigma) \subseteq \text{dom}(h) = \text{dom}(h')$ holds by GCAxiom_1;
  - $\text{reach}(\text{dom}(\text{shape}(\mathbf{T})), h', \sigma) \subseteq \text{dom}(\text{shape}(\mathbf{T})) \subseteq \text{dom}(\sigma)$ follows, by Lemma 10, from $\mathbf{h}' \uplus \mathbf{h}_{\text{F}} \sim_{\mathbf{T}} h' \wedge \mathbf{h}' \uplus \mathbf{h}_{\text{F}} :: \mathbf{T}$ and $\text{shape}(\mathbf{T}) \subseteq \sigma$;
  - $\forall p' \notin \overline{\text{dom}}(\sigma).\ h'(p') = h(p')$ holds since $p + 4i \in \overline{\text{dom}}(\text{shape}(\mathbf{T})) \subseteq \overline{\text{dom}}(\sigma)$.
- Now it suffices to show that $\text{shape}(\mathbf{T}) \subseteq \sigma'$, which follows from
  (1) $\text{shape}(\mathbf{T}) \subseteq \sigma \wedge \sigma' \subseteq \sigma$; and
  (2) $\text{dom}(\text{shape}(\mathbf{T})) \subseteq \text{reach}(\text{dom}(\text{shape}(\mathbf{T})), h', \sigma') \subseteq \text{dom}(\sigma')$ by GCAxiom_1.

□

5.2.5 Seq

Lemma 11 (Soundness: Generalized Seq)**.**

$$\frac{\{\mathbf{P}\}\ C_1\ \{\mathbf{Q}\} : k \qquad \{\mathbf{Q}\}\ C_2\ \{\mathbf{R}\} : k}{\{\mathbf{P}\}\ C_1; C_2\ \{\mathbf{R}\} : k}$$

Proof.

- Assume: $\{\mathbf{P}\}\ C_1\ \{\mathbf{Q}\} : k$
- Assume: $\{\mathbf{Q}\}\ C_2\ \{\mathbf{R}\} : k$
- Assume: $\rho \in \text{Env}(\text{FLV}(\mathbf{P}, \mathbf{R})), j, \mathbf{s}, \mathbf{h}, \mathbf{h}_{\text{F}}, \mathbf{T}, s, h, C', s', h'$ such that
  $j \leq k \wedge \mathbf{s}, \mathbf{h} \models_{\text{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge \mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\text{F}} \approx_{\mathbf{T}} h \wedge (C_1; C_2, s, h \leadsto^j C', s', h')$
- To show:
  $(*)$ $(C', s', h' \leadsto -) \vee$
  $(**)$ $(\exists \mathbf{s}', \mathbf{h}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models_{\text{dom}(\mathbf{T})} \mathbf{R}[\rho] \wedge$
  $(\forall \mathrm{y} \notin \text{Mod}(C_1; C_2).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathbf{s}' \sim_{\mathbf{T}} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\text{F}} \approx_{\mathbf{T}} h')$
- Let $\rho' := \rho|^{\text{FLV}(\mathbf{Q})}$.
- Then, as $\mathbf{P}[\rho] = \mathbf{P}[\rho']$, we have
  ✓ $\mathbf{s}, \mathbf{h} \models_{\text{dom}(\mathbf{T})} \mathbf{P}[\rho']$.
- From $C_1; C_2, s, h \leadsto^j C', s', h'$, we have two cases.
- When $C_1, s, h \leadsto^j C_1', s', h' \wedge C' = C_1'; C_2$:
  - By assumption we have two cases.
  - When $C_1', s', h' \leadsto -$:
    $(*)$ holds because $(C_1'; C_2), s', h' \leadsto -$.

  - When $C_1' = \mathsf{skip} \land (\mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathbf{Q}[\rho']) \land (\forall \mathrm{y} \notin \mathrm{Mod}(C_1).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \land \mathbf{s}' \sim_{\mathbf{T}} s' \land \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h'$ for some $\mathbf{s}', \mathbf{h}'$:
    $(*)$ holds because $(\mathsf{skip}; C_2), s', h' \rightsquigarrow C_2, s', h'$.

- When $C_1, s, h \rightsquigarrow^{j_1} \mathsf{skip}, s_1', h_1' \land C_2, s_1', h_1' \rightsquigarrow^{j_2} C', s', h' \land j = j_1 + j_2 + 1$:
  - As $j_1 \le k \land C_1, s, h \rightsquigarrow^{j_1}$, by assumption, we have $\mathbf{s}_1', \mathbf{h}_1'$ such that
    ✓ $\mathbf{s}_1', \mathbf{h}_1' \models_{\mathrm{dom}(\mathbf{T})} \mathbf{Q}[\rho'] \land (\forall \mathrm{y} \notin \mathrm{Mod}(C_1).\ \mathbf{s}_1'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \land \mathbf{s}_1' \sim_{\mathbf{T}} s_1' \land \mathbf{h}_1' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h_1'$.
  - As $j_2 \le k \land C_2, s_1', h_1' \rightsquigarrow^{j_2} C', s', h'$, by assumption we have two cases.
  - When $C', s', h' \rightsquigarrow -$:
    $(*)$ holds.
  - When $C' = \mathsf{skip} \land \mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathbf{R}[\rho'] \land (\forall \mathrm{y} \notin \mathrm{Mod}(C_2).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}_1'(\mathrm{y})) \land \mathbf{s}' \sim_{\mathbf{T}} s' \land \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h'$:
    $(**)$ holds because
    (1) $\mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathbf{R}[\rho]$ holds since $\mathbf{R}[\rho'] = \mathbf{R}[\rho]$;
    (2) $(\forall \mathrm{y} \notin \mathrm{Mod}(C_1; C_2).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y}))$ follows from $(\forall \mathrm{y} \notin \mathrm{Mod}(C_2).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}_1'(\mathrm{y}))$ and $(\forall \mathrm{y} \notin \mathrm{Mod}(C_1).\ \mathbf{s}_1'(\mathrm{y}) = \mathbf{s}(\mathrm{y}))$ since $\mathrm{Mod}(C_1; C_2) = \mathrm{Mod}(C_1) \cup \mathrm{Mod}(C_2)$.

□

Theorem 5 (Soundness: Seq (partial))**.**

$$\frac{\{\mathbf{P}\}\ C_1\ \{\mathbf{Q}\} \qquad \{\mathbf{Q}\}\ C_2\ \{\mathbf{R}\}}{\{\mathbf{P}\}\ C_1; C_2\ \{\mathbf{R}\}}$$

Proof. It holds by Lemma 11. □

Theorem 6 (Soundness: Seq (total))**.**

$$\frac{[\mathbf{P}]\ C_1\ [\mathbf{Q}] \qquad [\mathbf{Q}]\ C_2\ [\mathbf{R}]}{[\mathbf{P}]\ C_1; C_2\ [\mathbf{R}]}$$

Proof.

- Assume $[\mathbf{P}]\ C_1\ [\mathbf{Q}]$.
- Assume $[\mathbf{Q}]\ C_2\ [\mathbf{R}]$.
- By Theorem 5, we have $\{\mathbf{P}\}\ C_1; C_2\ \{\mathbf{R}\}$.
- Assume: $\rho \in \mathrm{Env}(\mathrm{FLV}(\mathbf{P}, \mathbf{R})), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h$ such that
  $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \land \mathbf{s} \sim_{\mathbf{T}} s \land \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h$.
- Now we show $\neg(C_1; C_2, s, h$ diverges$)$ by contradiction.
- Assume $\{\, D_i, s_i, h_i \,\}_{i \in \mathbb{N}}$ such that
  ✓ $(D_0, s_0, h_0) = (C_1; C_2, s, h) \land \forall i.\ D_i, s_i, h_i \rightsquigarrow D_{i+1}, s_{i+1}, h_{i+1}$.
- Let $\rho' := \rho|^{\mathrm{FLV}(\mathbf{Q})}$.

- Then, as $\mathbf{P}[\rho] = \mathbf{P}[\rho']$, we have $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho']$.
- By $[\mathbf{P}]\ C_1\ [\mathbf{Q}]$, we have $\neg(C_1, s, h$ diverges$)$.
- Thus, we have some k such that $D_k = (\mathsf{skip}; C_2)$ and $C_1, s, h \rightsquigarrow^k \mathsf{skip}, s_k, h_k$.
- As $D_k = (\mathsf{skip}; C_2)$, we have $D_{k+1} = C_2$, $s_{k+1} = s_k$, and $h_{k+1} = h_k$.
- By $[\mathbf{P}]\ C_1\ [\mathbf{Q}]$, we have $\mathbf{s}_k, \mathbf{h}_k$ such that
  ✓ $\mathbf{s}_k, \mathbf{h}_k \models_{\mathrm{dom}(\mathbf{T})} \mathbf{Q}[\rho'] \wedge (\forall \mathsf{y} \notin \mathrm{Mod}(C_1).\ \mathbf{s}_k(\mathsf{y}) = \mathbf{s}(\mathsf{y})) \wedge \mathbf{s}_k \sim_{\mathbf{T}} s_k \wedge \mathbf{h}_k \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h_k$.
- By $[\mathbf{Q}]\ C_2\ [\mathbf{R}]$, we have $\neg(C_2, s_k, h_k$ diverges$)$.
- Thus we have $\neg(D_{k+1}, s_{k+1}, h_{k+1}$ diverges$)$, which is a contradiction.

$\square$

5.2.6 Frame

Theorem 7 (Soundness: Frame)**.**

$$\frac{\{\mathbf{P}\}\ C\ \{\mathbf{Q}\} \qquad \mathrm{FPV}(\mathbf{R}) \cap \mathrm{Mod}(C) = \emptyset}{\{\mathbf{P} * \mathbf{R}\}\ C\ \{\mathbf{Q} * \mathbf{R}\}} \qquad \frac{[\mathbf{P}]\ C\ [\mathbf{Q}] \qquad \mathrm{FPV}(\mathbf{R}) \cap \mathrm{Mod}(C) = \emptyset}{[\mathbf{P} * \mathbf{R}]\ C\ [\mathbf{Q} * \mathbf{R}]}$$

Proof.

- Assume: $\mathrm{FPV}(\mathbf{R}) \cap \mathrm{Mod}(C) = \emptyset$
- Assume: $\forall \rho \in \mathrm{Env}(\mathrm{FLV}(\mathbf{P}, \mathbf{Q})), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$.
  $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge \mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge C, s, h \rightsquigarrow^* C', s', h' \implies$
  $\big((C', s', h' \rightsquigarrow -) \vee$
  $(\exists \mathbf{s}', \mathbf{h}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathbf{Q}[\rho] \wedge$
  $(\forall \mathsf{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathsf{y}) = \mathbf{s}(\mathsf{y})) \wedge \mathbf{s}' \sim_{\mathbf{T}} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h')\big)$
  [# $\wedge \neg(C, s, h$ diverges$)$ #]
- Assume: $\rho \in \mathrm{Env}(\mathrm{FLV}(\mathbf{P}, \mathbf{Q}, \mathbf{R})), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$ such that
  $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} (\mathbf{P}[\rho] * \mathbf{R}[\rho]) \wedge \mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge C, s, h \rightsquigarrow^* C', s', h'$
- To show:
  [# $\neg(C, s, h$ diverges$)$; and #]
  $(*)$ $(C', s', h' \rightsquigarrow -) \vee$
  $(**)$ $(\exists \mathbf{s}', \mathbf{h}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} (\mathbf{Q}[\rho] * \mathbf{R}[\rho]) \wedge$
  $(\forall \mathsf{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathsf{y}) = \mathbf{s}(\mathsf{y})) \wedge \mathbf{s}' \sim_{\mathbf{T}} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h')$
- From $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} (\mathbf{P}[\rho] * \mathbf{R}[\rho])$, we have $\mathbf{h}_1$ and $\mathbf{h}_2$ such that
  ✓ $\mathbf{h} = \mathbf{h}_1 \uplus \mathbf{h}_2$,
  ✓ $\mathbf{s}, \mathbf{h}_1 \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho]$,
  ✓ $\mathbf{s}, \mathbf{h}_2 \models_{\mathrm{dom}(\mathbf{T})} \mathbf{R}[\rho]$.
- [# $\neg(C, s, h$ diverges$)$ holds by assumption since $\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} = \mathbf{h}_1 \uplus (\mathbf{h}_2 \uplus \mathbf{h}_{\mathrm{F}}) \wedge \mathbf{s}, \mathbf{h}_1 \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho]$ #]
- Also by assumption we have two cases since $\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} = \mathbf{h}_1 \uplus (\mathbf{h}_2 \uplus \mathbf{h}_{\mathrm{F}}) \wedge \mathbf{s}, \mathbf{h}_1 \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho]$.

- When $C', s', h' \rightsquigarrow -$:
  $(*)$ holds.

- When $C' = \mathsf{skip} \wedge (\mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathbf{Q}[\rho]) \wedge (\forall \mathrm{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathbf{s}' \sim_{\mathbf{T}} s' \wedge \mathbf{h}' \uplus \mathbf{h}_2 \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h'$ for some $\mathbf{s}', \mathbf{h}'$:
  $(**)$ is shown as follows.

- To show $(**)$, it suffices to show that $\mathbf{s}', \mathbf{h}' \uplus \mathbf{h}_2 \models_{\mathrm{dom}(\mathbf{T})} \mathbf{Q}[\rho] * \mathbf{R}[\rho]$.

- We split the heap $\mathbf{h}' \uplus \mathbf{h}_2$ into $\mathbf{h}'$ and $\mathbf{h}_2$.

- As $\mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathbf{Q}[\rho]$ holds, we need to show $\mathbf{s}', \mathbf{h}_2 \models_{\mathrm{dom}(\mathbf{T})} \mathbf{R}[\rho]$, which follows from $(\mathbf{s}, \mathbf{h}_2 \models_{\mathrm{dom}(\mathbf{T})} \mathbf{R}[\rho]) \wedge (\forall \mathrm{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathrm{FPV}(\mathbf{R}) \cap \mathrm{Mod}(C) = \emptyset$ by Lemma 5.

□

5.2.7 Conseq

Theorem 8 (Soundness: Conseq)**.**

$$\frac{\mathbf{P} \models \mathbf{P}' \qquad \{\mathbf{P}'\}\ C\ \{\mathbf{Q}'\} \qquad \mathbf{Q}' \models \mathbf{Q}}{\{\mathbf{P}\}\ C\ \{\mathbf{Q}\}} \qquad \frac{\mathbf{P} \models \mathbf{P}' \qquad [\mathbf{P}']\ C\ [\mathbf{Q}'] \qquad \mathbf{Q}' \models \mathbf{Q}}{[\mathbf{P}]\ C\ [\mathbf{Q}]}$$

Proof.

- Assume: $\mathbf{P} \models \mathbf{P}'$ and $\mathbf{Q}' \models \mathbf{Q}$.

- Assume: $\forall \rho \in \mathrm{Env}(\mathrm{FLV}(\mathbf{P}', \mathbf{Q}')), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$.
  $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}'[\rho] \wedge \mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge C, s, h \rightsquigarrow^* C', s', h' \implies$
  $\big((C', s', h' \rightsquigarrow -) \vee$
  $(\exists \mathbf{s}', \mathbf{h}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathbf{Q}'[\rho] \wedge$
  $(\forall \mathrm{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathbf{s}' \sim_{\mathbf{T}} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h')\big)$
  [# $\wedge\, \neg(C, s, h$ diverges) #]

- Assume: $\rho \in \mathrm{Env}(\mathrm{FLV}(\mathbf{P}, \mathbf{Q})), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$ such that
  $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge \mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge C, s, h \rightsquigarrow^* C', s', h'$

- To show:
  [# $\neg(C, s, h$ diverges); and #]
  $(*)$ $(C', s', h' \rightsquigarrow -) \vee$
  $(**)$ $(\exists \mathbf{s}', \mathbf{h}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathbf{Q}[\rho] \wedge$
  $(\forall \mathrm{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathbf{s}' \sim_{\mathbf{T}} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h')$

- Let $\rho' := \rho|^{\mathrm{FLV}(\mathbf{P}', \mathbf{Q}')}$.

- From $\mathbf{P} \models \mathbf{P}'$ and $\mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge \mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho']$ (as $\mathbf{P}[\rho'] = \mathbf{P}[\rho]$), we have
  ✓ $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}'[\rho']$.

- [# $\neg(C, s, h$ diverges) holds by assumption. #]

- Also by assumption we have two cases.

- When $C', s', h' \rightsquigarrow -$:
  $(*)$ holds.

- When $C' = \mathsf{skip} \wedge (\mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathbf{Q}'[\rho']) \wedge (\forall \mathrm{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathbf{s}' \sim_{\mathbf{T}} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h'$ for some $\mathbf{s}', \mathbf{h}'$:
  $(**)$ holds because $\mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathbf{Q}[\rho]$ follows from $\mathbf{Q}' \models \mathbf{Q}$ and $\mathbf{s}' \sim_{\mathbf{T}} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h' \wedge \mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathbf{Q}'[\rho']$ (as $\mathbf{Q}[\rho'] = \mathbf{Q}[\rho]$).

$\square$

5.2.8 Ex

Theorem 9 (Soundness: Ex)**.**

$$\frac{\{\mathbf{P}\}\ C\ \{\mathbf{Q}\}}{\{\exists v.\,\mathbf{P}\}\ C\ \{\exists v.\,\mathbf{Q}\}} \qquad \frac{[\mathbf{P}]\ C\ [\mathbf{Q}]}{[\exists v.\,\mathbf{P}]\ C\ [\exists v.\,\mathbf{Q}]}$$

Proof.

- Assume: $\forall \rho \in \mathrm{Env}(\mathrm{FLV}(\mathbf{P}, \mathbf{Q})), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$.
  $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge \mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge C, s, h \rightsquigarrow^* C', s', h' \implies$
  $\big((C', s', h' \rightsquigarrow -) \vee$
  $(\exists \mathbf{s}', \mathbf{h}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathbf{Q}[\rho] \wedge$
  $(\forall \mathrm{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathbf{s}' \sim_{\mathbf{T}} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h')\big)$
  [# $\wedge \neg(C, s, h$ diverges) #]

- Assume: $\rho \in \mathrm{Env}(\mathrm{FLV}(\exists v.\,\mathbf{P}, \exists v.\,\mathbf{Q})), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$ such that
  $(\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} (\exists v.\,\mathbf{P})[\rho]) \wedge \mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge C, s, h \rightsquigarrow^* C', s', h'$

- To show:
  [# $\neg(C, s, h$ diverges); and #]
  $(*)$ $(C', s', h' \rightsquigarrow -) \vee$
  $(**)$ $(\exists \mathbf{s}', \mathbf{h}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} (\exists v.\,\mathbf{Q})[\rho] \wedge$
  $(\forall \mathrm{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathbf{s}' \sim_{\mathbf{T}} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h')$

- From $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} (\exists v.\,\mathbf{P})[\rho]$, by Lemma 7 we have
  ✓ $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[(\rho \mid v \mapsto \mathbf{v})]$ for some $\mathbf{v} \in \mathrm{LogVals}$.

- Let $\rho' := (\rho \mid v \mapsto \mathbf{v})$.

- [# $\neg(C, s, h$ diverges) holds by assumption. #]

- Also by assumption we have two cases.

- When $C', s', h' \rightsquigarrow -$:
  $(*)$ holds.

- When $C' = \mathsf{skip} \wedge (\mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathbf{Q}[\rho']) \wedge (\forall \mathrm{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathbf{s}' \sim_{\mathbf{T}} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h'$ for some $\mathbf{s}', \mathbf{h}'$:
  $(**)$ holds because $\mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} (\exists v.\,\mathbf{Q})[\rho]$ follows from $\mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathbf{Q}[\rho']$ by Lemma 7.

$\square$

5.2.9 Gen

Theorem 10 (Soundness: Gen)**.**

$$\frac{\forall \mathbf{v} \in \mathrm{LogVals}.\ \{\mathbf{P}[\mathbf{v}/v]\}\ C\ \{\mathbf{Q}[\mathbf{v}/v]\}}{\{\mathbf{P}\}\ C\ \{\mathbf{Q}\}} \qquad \frac{\forall \mathbf{v} \in \mathrm{LogVals}.\ [\mathbf{P}[\mathbf{v}/v]]\ C\ [\mathbf{Q}[\mathbf{v}/v]]}{[\mathbf{P}]\ C\ [\mathbf{Q}]}$$

Proof. The goal directly follows by definition because $\mathbf{P}[\rho] = \mathbf{P}[\rho(v)/v][\rho]$ and $\mathbf{Q}[\rho] = \mathbf{Q}[\rho(v)/v][\rho]$ for any $\rho \in \mathrm{Env}(\mathrm{FLV}(\mathbf{P}, \mathbf{Q}))$. ☐

5.2.10 Total

Theorem 11 (Soundness: Total)**.**

$$\frac{[\mathbf{P}]\ C\ [\mathbf{Q}]}{\{\mathbf{P}\}\ C\ \{\mathbf{Q}\}}$$

Proof. It holds vacuously by definition. ☐

5.2.11 If

Theorem 12 (Soundness: If)**.**

$$\frac{\{\mathbf{P} \wedge E\}\ C_1\ \{\mathbf{Q}\} \qquad \{\mathbf{P} \wedge \mathsf{not}\ E\}\ C_2\ \{\mathbf{Q}\}}{\{\mathbf{P} \wedge \mathsf{word}(E)\}\ \mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}\ \{\mathbf{Q}\}} \qquad \frac{[\mathbf{P} \wedge E]\ C_1\ [\mathbf{Q}] \qquad [\mathbf{P} \wedge \mathsf{not}\ E]\ C_2\ [\mathbf{Q}]}{[\mathbf{P} \wedge \mathsf{word}(E)]\ \mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}\ [\mathbf{Q}]}$$

Proof.

- Assume: $\forall \rho \in \mathrm{Env}(\mathrm{FLV}(\mathbf{P}, \mathbf{Q})), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'.$
  $(\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge E) \wedge \mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge C_1, s, h \rightsquigarrow^* C', s', h' \implies$
  $\big((C', s', h' \rightsquigarrow -) \vee$
  $(\exists \mathbf{s}', \mathbf{h}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathbf{Q}[\rho] \wedge$
  $(\forall \mathrm{y} \notin \mathrm{Mod}(C_1).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathbf{s}' \sim_{\mathbf{T}} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h')\big)$
  [# $\wedge \neg(C_1, s, h$ diverges) #]

- Assume: $\forall \rho \in \mathrm{Env}(\mathrm{FLV}(\mathbf{P}, \mathbf{Q})), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'.$
  $(\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge \mathsf{not}\ E) \wedge \mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge C_2, s, h \rightsquigarrow^* C', s', h' \implies$
  $\big((C', s', h' \rightsquigarrow -) \vee$
  $(\exists \mathbf{s}', \mathbf{h}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathbf{Q}[\rho] \wedge$
  $(\forall \mathrm{y} \notin \mathrm{Mod}(C_2).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathbf{s}' \sim_{\mathbf{T}} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h')\big)$
  [# $\wedge \neg(C_2, s, h$ diverges) #]

- Assume: $\rho \in \mathrm{Env}(\mathrm{FLV}(\mathbf{P}, \mathbf{Q})), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$ such that
  $(\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge \mathsf{word}(E)) \wedge \mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge \mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}, s, h \rightsquigarrow^* C', s', h'$

- To show:
  [# $\neg(\mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}, s, h$ diverges); and #]
  $(*)$ $(C', s', h' \rightsquigarrow -) \vee$
  $(**)$ $(\exists \mathbf{s}', \mathbf{h}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathbf{Q}[\rho] \wedge$
  $(\forall \mathrm{y} \notin \mathrm{Mod}(C_1, C_2).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathbf{s}' \sim_{\mathbf{T}} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h')$

- From $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathsf{word}(E)$, we have
  ✓ $[\![E]\!]_{\mathbf{s}} \in$ Words.
- By Lemma 2, we have
  ✓ $[\![E]\!]_s = \mathrm{phyv}_{\mathbf{T}}([\![E]\!]_{\mathbf{s}}) = [\![E]\!]_{\mathbf{s}}$.
- Thus, we have two cases.
- When $[\![E]\!]_{\mathbf{s}} \in \mathrm{Words}\backslash\{0\}$:
  - [# Since we have $\mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}, s, h \rightsquigarrow C_1, s, h$ and $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge E$, by assumption we have $\neg(C_1, s, h$ diverges) and thus $\neg(C, s, h$ diverges) holds. #]
  - From $\mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}, s, h \rightsquigarrow^* C', s', h'$ we have two cases.
  - When $C' = \mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi} \wedge s' = s \wedge h' = h$:
    ($*$) holds as we have $\mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}, s, h \rightsquigarrow C_1, s, h$.
  - When $C_1, s, h \rightsquigarrow^* C', s', h'$:
    ($*$) or ($**$) holds by assumption since we have $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge E$.
- When $[\![E]\!]_{\mathbf{s}} = 0$:
  - [# Since we have $\mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}, s, h \rightsquigarrow C_2, s, h$ and $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge \mathsf{not}\ E$, by assumption we have $\neg(C_2, s, h$ diverges) and thus $\neg(C, s, h$ diverges) holds. #]
  - From $\mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}, s, h \rightsquigarrow^* C', s', h'$ we have two cases.
  - When $C' = \mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi} \wedge s' = s \wedge h' = h$:
    ($*$) holds as we have $\mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}, s, h \rightsquigarrow C_2, s, h$.
  - When $C_2, s, h \rightsquigarrow^* C', s', h'$:
    ($*$) or ($**$) holds by assumption since we have $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge \mathsf{not}\ E$.

□

5.2.12 While

Theorem 13 (Soundness: While)**.**

$$\frac{\{\mathbf{P} \wedge E\}\ C\ \{\mathbf{P} \wedge \mathsf{word}(E)\}}{\{\mathbf{P} \wedge \mathsf{word}(E)\}\ \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}\ \{\mathbf{P} \wedge \mathsf{not}\ E\}}$$

Proof.

- Assume: $\{\mathbf{P} \wedge E\}\ C\ \{\mathbf{P} \wedge \mathsf{word}(E)\}$
- To show: $\forall k.\ \{\mathbf{P} \wedge \mathsf{word}(E)\}\ \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}\ \{\mathbf{P} \wedge \mathsf{not}\ E\} : k$
- We prove the goal by induction on k.
- (Base case) when $k = 0$,
  - Assume: $\rho \in \mathrm{Env}(\mathrm{FLV}(\mathbf{P})), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$ such that
    $(\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge \mathsf{word}(E)) \wedge \mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}, s, h \rightsquigarrow^k C', s', h'$.

  - It suffices to show
    $(*)\ \ C', s', h' \rightsquigarrow -$.
  - From $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathsf{word}(E)$, we have
    ✓ $[\![\![E]\!]\!]_{\mathbf{s}} \in \text{Words}$.
  - By Lemma 2, we have
    ✓ $\llbracket E \rrbracket_s = \mathrm{phyv}_{\mathbf{T}}([\![\![E]\!]\!]_{\mathbf{s}}) = [\![\![E]\!]\!]_{\mathbf{s}}$.
  - $(*)$ holds because $C' = \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od} \wedge s' = s \wedge h' = h$ and $\llbracket E \rrbracket_s \neq \text{undef}$.

- (Inductive step) when $k > 0 \wedge \forall j < k.\ \{\mathbf{P} \wedge \mathsf{word}(E)\}\ \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}\ \{\mathbf{P} \wedge \mathsf{not}\ E\} : j$,
  - Assume: $\rho \in \mathrm{Env}(\mathrm{FLV}(\mathbf{P})), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$ such that
    $(\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge \mathsf{word}(E)) \wedge \mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}, s, h \rightsquigarrow^{k} C', s', h'$.
  - To show:
    $(*)\ \ (C', s', h' \rightsquigarrow -) \vee$
    $(**)\ (\exists \mathbf{s}', \mathbf{h}'.\ C' = \mathsf{skip} \wedge (\mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge \mathsf{not}\ E) \wedge$
    $(\forall \mathrm{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathbf{s}' \sim_{\mathbf{T}} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h')$
  - From $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathsf{word}(E)$, we have
    ✓ $[\![\![E]\!]\!]_{\mathbf{s}} \in \text{Words}$.
  - By Lemma 2, we have
    ✓ $\llbracket E \rrbracket_s = \mathrm{phyv}_{\mathbf{T}}([\![\![E]\!]\!]_{\mathbf{s}}) = [\![\![E]\!]\!]_{\mathbf{s}}$.
  - Thus we have two cases.
  - When $\llbracket E \rrbracket_s = [\![\![E]\!]\!]_{\mathbf{s}} = 0$:
    - ◇ We have $\mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}, s, h \rightsquigarrow \mathsf{skip}, s, h$.
    - ◇ Thus we have $\mathsf{skip}, s, h \rightsquigarrow^{k-1} C', s', h'$, from which it follows that
      ✓ $C' = \mathsf{skip} \wedge s' = s \wedge h' = h$.
    - ◇ Thus $(**)$ holds because we have $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathsf{not}\ E$ from $[\![\![\mathsf{not}\ E]\!]\!]_{\mathbf{s}} = 1$.
  - When $\llbracket E \rrbracket_s = [\![\![E]\!]\!]_{\mathbf{s}} \in \text{Words}\backslash\{0\}$:
    - ◇ We have $\mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}, s, h \rightsquigarrow (C; \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}), s, h$, from which we have
      ✓ $(C; \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}), s, h \rightsquigarrow^{k-1} C', s', h'$.
    - ◇ From $\{\mathbf{P} \wedge E\}\ C\ \{\mathbf{P} \wedge \mathsf{word}(E)\}$ and $\{\mathbf{P} \wedge \mathsf{word}(E)\}\ \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}\ \{\mathbf{P} \wedge \mathsf{not}\ E\} : k-1$, by Lemma 11 we have
      ✓ $\{\mathbf{P} \wedge E\}\ C; \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}\ \{\mathbf{P} \wedge \mathsf{not}\ E\} : k-1$.
    - ◇ Thus $(*) \vee (**)$ holds since we have $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} E$ from $[\![\![E]\!]\!]_{\mathbf{s}} \in \text{Words}\backslash\{0\}$.

□

Theorem 14 (Soundness: WhileT)**.**

$$\frac{[\mathbf{P} \wedge E \wedge 0 < \mathbf{E}' = v]\ C\ [\mathbf{P} \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}' < v] \qquad v \notin \mathrm{FLV}(\mathbf{P}, \mathbf{E}')}{[\mathbf{P} \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}']\ \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}\ [\mathbf{P} \wedge \mathsf{not}\ E]}$$

Proof.

- Assume: $[\mathbf{P} \wedge E \wedge 0 < \mathbf{E}' = v]\ C\ [\mathbf{P} \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}' < v]$ and $v \notin \mathrm{FLV}(\mathbf{P}, \mathbf{E}')$.

- By Theorems 8, 9, 11 and 13, we have

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\mathbf{P} \wedge E \wedge 0 < \mathbf{E}' = v]\ C\ [\mathbf{P} \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}' < v]}{[\exists v.\, \mathbf{P} \wedge E \wedge 0 < \mathbf{E}' = v]\ C\ [\exists v.\, \mathbf{P} \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}' < v]}\,(\mathrm{Ex})}{[\mathbf{P} \wedge 0 < \mathbf{E}' \wedge E]\ C\ [\mathbf{P} \wedge 0 < \mathbf{E}' \wedge \mathsf{word}(E)]}\,(\mathrm{Conseq})}{\{\mathbf{P} \wedge 0 < \mathbf{E}' \wedge E\}\ C\ \{\mathbf{P} \wedge 0 < \mathbf{E}' \wedge \mathsf{word}(E)\}}\,(\mathrm{Total})}{\{\mathbf{P} \wedge 0 < \mathbf{E}' \wedge \mathsf{word}(E)\}\ \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}\ \{\mathbf{P} \wedge 0 < \mathbf{E}' \wedge \mathsf{not}\ E\}}\,(\mathrm{While})}{\{\mathbf{P} \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}'\}\ \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}\ \{\mathbf{P} \wedge \mathsf{not}\ E\}}\,(\mathrm{Conseq})$$

- Assume: $\rho \in \mathrm{Env}(\mathrm{FLV}(\mathbf{P}, \mathbf{E}')), \mathbf{s}, \mathbf{h}, \mathbf{h}_\mathrm{F}, \mathbf{T}, s, h$ such that
  $(\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}'[\rho]) \wedge \mathbf{s} \sim_\mathbf{T} s \wedge \mathbf{h} \uplus \mathbf{h}_\mathrm{F} \approx_\mathbf{T} h$.

- Now we show $\neg(\mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}, s, h$ diverges) by contradiction.

- Assume: $\{\, D_i, s_i, h_i \,\}_{i \in \mathbb{N}}$ such that
  ✓ $(D_0, s_0, h_0) = (\mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}, s, h) \wedge \forall i.\ D_i, s_i, h_i \rightsquigarrow D_{i+1}, s_{i+1}, h_{i+1}$.

- We show the following, which is a contradiction because $n_0 > n_1 > n_2 \ldots > 0$ is not possible.

- By induction on i, we find $\{\, k_i, n_i, \mathbf{s}_i, \mathbf{h}_i \,\}_{i \in \mathbb{N}}$ (with $n_i \in$ Words) such that
  ✓ $D_{k_i} = \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}$;
  ✓ $(\mathbf{s}_i, \mathbf{h}_i \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}'[\rho] = n_i) \wedge \mathbf{s}_i \sim_\mathbf{T} s_{k_i} \wedge \mathbf{h}_i \uplus \mathbf{h}_\mathrm{F} \approx_\mathbf{T} h_{k_i}$;
  ✓ if $i > 0$ then $0 < n_i < n_{i-1}$.

(Base Case)

- From $(\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} 0 < \mathbf{E}'[\rho])$, we have
  ✓ $[\![\mathbf{E}'[\rho]]\!]_\mathbf{s} \in$ Words.

- Let $k_0 = 0$, $\mathbf{s}_0 = \mathbf{s}$, $\mathbf{h}_0 = \mathbf{h}$ and $n_0 = [\![\mathbf{E}'[\rho]]\!]_{\mathbf{s}_0} \in$ Words.

- Then by assumption we have
  ✓ $D_{k_0} = \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}$,
  ✓ $(\mathbf{s}_0, \mathbf{h}_0 \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}'[\rho] = n_0) \wedge \mathbf{s}_0 \sim_\mathbf{T} s_{k_0} \wedge \mathbf{h}_0 \uplus \mathbf{h}_\mathrm{F} \approx_\mathbf{T} h_{k_0}$.

(Inductive step)

- Assume:
  ✓ $D_{k_i} = \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}$,
  ✓ $(\mathbf{s}_i, \mathbf{h}_i \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}'[\rho] = n_i) \wedge \mathbf{s}_i \sim_\mathbf{T} s_{k_i} \wedge \mathbf{h}_i \uplus \mathbf{h}_\mathrm{F} \approx_\mathbf{T} h_{k_i}$.

- As $(D_{k_i}, s_{k_i}, h_{k_i})$ diverges, we have
  ✓ $[\![E]\!]_{s_{k_i}} \in \mathrm{Words} \backslash \{0\}$,
  ✓ $(D_{k_i+1}, s_{k_i+1}, h_{k_i+1}) = (C; \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}, s_{k_i}, h_{k_i})$.

- From $\mathbf{s}_i, \mathbf{h}_i \models_{\mathrm{dom}(\mathbf{T})} \mathsf{word}(E)$, we have
  ✓ $[\![E]\!]_{\mathbf{s}_i} \in$ Words.

- By Lemma 2, we have $[\![E]\!]_{\mathbf{s}_i} = \mathrm{phyv}_\mathbf{T}([\![E]\!]_{\mathbf{s}_i}) = [\![E]\!]_{s_{k_i}} \in \mathrm{Words} \backslash \{0\}$, and thus we have
  ✓ $\mathbf{s}_i, \mathbf{h}_i \models_{\mathrm{dom}(\mathbf{T})} E$.

- By $[\mathbf{P} \wedge E \wedge 0 < \mathbf{E}' = v]\ C\ [\mathbf{P} \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}' < v]$, we have
  ✓ $\neg(C, s_{k_i+1}, h_{k_i+1}$ diverges).
- Thus, we have some j such that
  ✓ $D_{k_i+j+1} = (\mathsf{skip}; \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od})$,
  ✓ $C, s_{k_i+1}, h_{k_i+1} \rightsquigarrow^j \mathsf{skip}, s_{k_i+j+1}, h_{k_i+j+1}$.
- Then, by $[\mathbf{P} \wedge E \wedge 0 < \mathbf{E}' = v]\ C\ [\mathbf{P} \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}' < v]$, we have $\mathbf{s}_{i+1}$, $\mathbf{h}_{i+1}$ such that
  ✓ $(\mathbf{s}_{i+1}, \mathbf{h}_{i+1} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}'[\rho] < n_i) \wedge \mathbf{s}_{i+1} \sim_{\mathbf{T}} s_{k_i+j+1} \wedge \mathbf{h}_{i+1} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h_{k_i+j+1}$.
- Also we have
  ✓ $(D_{k_i+j+2}, s_{k_i+j+2}, h_{k_i+j+2}) = (\mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}, s_{k_i+j+1}, h_{k_i+j+1})$.
- From $\mathbf{s}_{i+1}, \mathbf{h}_{i+1} \models_{\mathrm{dom}(\mathbf{T})} 0 < \mathbf{E}'[\rho] < n_i$, we have
  ✓ $[\![\mathbf{E}'[\rho]]\!]_{\mathbf{s}_{i+1}} \in \mathrm{Words} \wedge 0 < [\![\mathbf{E}'[\rho]]\!]_{\mathbf{s}_{i+1}} < n_i$.
- Let $k_{i+1} = k_i + j + 2$ and $n_{i+1} = [\![\mathbf{E}'[\rho]]\!]_{\mathbf{s}_{i+1}}$.
- Then, we have
  ✓ $D_{k_{i+1}} = \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}$,
  ✓ $(\mathbf{s}_{i+1}, \mathbf{h}_{i+1} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{P}[\rho] \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}'[\rho] = n_{i+1}) \wedge \mathbf{s}_{i+1} \sim_{\mathbf{T}} s_{k_{i+1}} \wedge \mathbf{h}_{i+1} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h_{k_{i+1}}$,
  ✓ $0 < n_{i+1} < n_i$.

□

5.3 Soundness of Outer-level Rules

Definition 2 (Generalized triple)**.**

$$\begin{aligned}\{\{P\}\}\ C\ \{\{Q\}\} : k \ \text{ iff } \ & \forall j \leq k.\ \forall \rho \in \mathrm{Env}(\mathrm{FLV}(P, Q)), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'.\\ & \mathbf{s}, \mathbf{h} \models P[\rho] \wedge \mathbf{s} \approx_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge C, s, h \rightsquigarrow^j C', s', h' \implies\\ & \quad (C', s', h' \rightsquigarrow -) \vee\\ & \quad (\exists \mathbf{s}', \mathbf{h}', \mathbf{T}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models Q[\rho] \wedge\\ & \qquad\qquad (\forall \mathtt{x} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathtt{x}) = \mathbf{s}(\mathtt{x})) \wedge \mathbf{s}' \approx_{\mathbf{T}'} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}'} h')\end{aligned}$$

5.3.1 Alloc

Theorem 15 (Soundness: Alloc)**.**

$$\frac{m \geq 0}{[[\mathtt{x} = 2m + 1]]\ \mathsf{alloc}\ \mathtt{x}\ [[\mathtt{x} \hookrightarrow_m 0, \ldots, 0]]}$$

Proof.

- Assume: $m, \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$ such that
  ✓ $m \geq 0 \wedge \mathbf{s}, \mathbf{h} \models \mathtt{x} = 2m + 1 \wedge \mathbf{s} \approx_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge \mathsf{alloc}\ \mathtt{x}, s, h \rightsquigarrow^* C', s', h'$
- $\mathsf{alloc}\ \mathtt{x}, s, h$ does not diverge as it takes at most one step.
- To show:
  $(*)$ $C', s', h' \rightsquigarrow -$; or
  $(**)$ $\exists \mathbf{s}', \mathbf{h}', \mathbf{T}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models \mathtt{x} \hookrightarrow_m 0, \ldots, 0 \wedge$
  $(\forall \mathtt{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathtt{y}) = \mathbf{s}(\mathtt{y})) \wedge \mathbf{s}' \approx_{\mathbf{T}'} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}'} h'$

- From $\mathbf{s}, \mathbf{h} \models \mathtt{x} = 2m + 1$, we have
  ✓ $\mathbf{s}(\mathtt{x}) = 2m + 1$.

- From $\mathbf{s}(\mathtt{x}) = 2m + 1 \wedge \mathbf{s} \approx_{\mathbf{T}} s$, we have
  ✓ $s(\mathtt{x}) = 2m + 1$.

- From $\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h$, we have σ_0 such that
  ✓ $\sigma_0 = I_{\mathrm{gc}}(\mathrm{dom}(\mathrm{shape}(\mathbf{T})), h) \wedge \mathrm{shape}(\mathbf{T}) \subseteq \sigma_0$.

- From $\mathbf{s} \approx_{\mathbf{T}} s$, we have
  ✓ $\mathrm{roots}(s) \subseteq \mathrm{dom}(\mathrm{shape}(\mathbf{T})) \subseteq \mathrm{reach}(\mathrm{dom}(\mathrm{shape}(\mathbf{T})), h, \sigma_0)$.

- Thus, by $\mathrm{GCAxiom}_2$, we have σ_0' such that
  ✓ $\sigma_0' = I_{\mathrm{gc}}(\mathrm{roots}(s), h) \wedge \sigma_0' \subseteq \sigma_0$.

- By $\mathrm{GCAxiom}_1$, we have
  $\mathrm{reach}(\mathrm{roots}(s), h, \sigma_0') \subseteq \mathrm{dom}(\sigma_0')$.

- By Lemmas 8 and 10 we have
  ✓ $\mathrm{reach}(\mathrm{roots}(s), h, \sigma_0') \subseteq \mathrm{reach}(\mathrm{dom}(\mathrm{shape}(\mathbf{T})), h, \sigma_0) \subseteq \mathrm{dom}(\mathrm{shape}(\mathbf{T}))$

- By the specification of garbage collector, from $\mathsf{alloc}\ \mathtt{x}, s, h \leadsto^* C', s', h'$ we have the following two cases.

- When $C' = \mathsf{alloc}\ \mathtt{x} \wedge s' = s \wedge h' = h$:
  $(*)$ holds by the specification of garbage collector.

- When $C' = \mathsf{skip} \wedge$
  ✓ $\sigma_1 \uplus [p_1 \mapsto m] = I_{\mathrm{gc}}(\mathrm{roots}(s'), h') \wedge$
  ✓ $s'(\mathtt{x}) = p_1 \wedge$
  ✓ $h' = h_1 \uplus [p_1 \mapsto_m 0, \ldots, 0] \wedge$
  ✓ $(s, h, \sigma_0') \cong ((s' \mid \mathtt{x} \mapsto 2m + 1), h_1, \sigma_1)$
  for some p_1, h_1, σ_1:
  $(**)$ is shown as follows.

- Let $s_1 = (s' \mid \mathtt{x} \mapsto 2m + 1)$.

- From $(s, h, \sigma_0') \cong (s_1, h_1, \sigma_1)$, we have r such that

  ✓ $r \in \mathrm{Bij}(\mathrm{reach}(\mathrm{roots}(s), h, \sigma_0'), \mathrm{reach}(\mathrm{roots}(s_1), h_1, \sigma_1))$

  ✓ $\forall \mathrm{y}.\ (s(\mathrm{y}), s_1(\mathrm{y})) \in \overline{r}$

  ✓ $\forall (p, p') \in r.\ \exists n.\ \sigma_0'(p) = \sigma_1(p') = n \wedge \forall i < n.\ (h(p + 4i), h_1(p' + 4i)) \in \overline{r}$

  where $\overline{r} \overset{\mathrm{def}}{=} r \cup \{\, (a, a) \mid a \in \mathrm{NonPtrs} \,\}$.

- We define $\mathbf{T}_1$ as follows:
  ✓ $\mathbf{T}_1(\boldsymbol{\ell}) \overset{\mathrm{def}}{=} \begin{cases} (p, n) & \text{if } \mathbf{T}(\boldsymbol{\ell}) = (p', n) \wedge (p', p) \in r \\ \text{undef} & \text{otherwise} \end{cases}$
  $\mathbf{T}_1$ is well-defined because r is bijective.

- By definition, we have
  ✓ $\mathrm{dom}(\mathrm{shape}(\mathbf{T}_1)) \subseteq \mathrm{reach}(\mathrm{roots}(s_1), h_1, \sigma_1)$.

- ✓ $\mathrm{shape}(\mathbf{T}_1) \subseteq \sigma_1$ is shown as follows.

  - To have $\mathrm{shape}(\mathbf{T}_1) \neq \mathrm{undef}$, we need to show that $p \neq p'$ for any $(p, n) = \mathbf{T}_1(\boldsymbol{\ell})$ and $(p', n') = \mathbf{T}_1(\boldsymbol{\ell}')$ with $\boldsymbol{\ell} \neq \boldsymbol{\ell}'$.

    By definition of $\mathbf{T}_1$, we have p'', p''' such that
    ✓ $(p'', n) = \mathbf{T}(\boldsymbol{\ell}) \wedge (p'', p) \in r \wedge (p''', n') = \mathbf{T}(\boldsymbol{\ell}') \wedge (p''', p') \in r$.

    From $\mathrm{shape}(\mathbf{T}) \neq \mathrm{undef} \wedge \boldsymbol{\ell} \neq \boldsymbol{\ell}'$, we have
    ✓ $p'' \neq p'''$.

    Since r is bijective, we conclude $p \neq p'$ from $(p'', p) \in r \wedge (p''', p') \in r \wedge p'' \neq p'''$.

  - Now it remains to show $\sigma_1(p) = n$ for any p, n such that
    ✓ $\mathrm{shape}(\mathbf{T}_1)(p) = n$.

    By definition of $\mathrm{shape}(\mathbf{T}_1)$ and $\mathbf{T}_1$, we have $\boldsymbol{\ell}, p'$ such that
    ✓ $(p', n) = \mathbf{T}(\boldsymbol{\ell}) \wedge (p', p) \in r$.

    We thus have the equality

    $$\begin{aligned} \sigma_1(p) &= \sigma'_0(p') && (\text{by } (p', p) \in r) \\ &= \sigma_0(p') && (\text{by } \sigma'_0 \subseteq \sigma_0 \wedge p' \in \mathrm{reach}(\mathrm{roots}(s), h, \sigma'_0) \subseteq \mathrm{dom}(\sigma'_0)) \\ &= \mathrm{shape}(\mathbf{T})(p') && (\text{by } \mathrm{shape}(\mathbf{T}) \subseteq \sigma_0 \wedge p' \in \mathrm{dom}(\mathrm{shape}(\mathbf{T}))) \\ &= n\,. \end{aligned}$$

- ✓ $\mathbf{s} \approx_{\mathbf{T}_1} s_1$ is shown as follows.

  - $s_1(\mathtt{x}) = \mathrm{phyv}_{\mathbf{T}_1}(\mathbf{s}(\mathtt{x})) \wedge \mathbf{s}(\mathtt{x}) \in \mathrm{Safe}(\mathrm{dom}(\mathbf{T}_1))$ holds since $\mathbf{s}(\mathtt{x}) = s_1(\mathtt{x}) = 2m + 1$.
  - Now we need to show that $s_1(\mathtt{y}) = \mathrm{phyv}_{\mathbf{T}_1}(\mathbf{s}(\mathtt{y})) \wedge \mathbf{s}(\mathtt{y}) \in \mathrm{Safe}(\mathrm{dom}(\mathbf{T}_1))$ for any $\mathtt{y} \neq \mathtt{x}$.
  - From $\mathbf{s} \approx_{\mathbf{T}} s$, we have $\mathbf{s}(\mathtt{y}) \in \mathrm{Safe}(\mathrm{dom}(\mathbf{T}))$ and thus have the following two cases.
  - When $\mathbf{s}(\mathtt{y}) = a \in \mathrm{NonPtrs}$:

    We have $s(\mathtt{y}) = a$ from $\mathbf{s} \approx_{\mathbf{T}} s$.

    Thus we have $s_1(\mathtt{y}) = a$ from $(s(\mathtt{y}), s_1(\mathtt{y})) \in \overline{r}$.

    Thus we have $s_1(\mathtt{y}) = a = \mathrm{phyv}_{\mathbf{T}_1}(\mathbf{s}(\mathtt{y})) \wedge \mathbf{s}(\mathtt{y}) = a \in \mathrm{Safe}(\mathrm{dom}(\mathbf{T}_1))$.
  - When $\mathbf{s}(\mathtt{y}) = \boldsymbol{\ell} \widehat{+} 0$ for $\boldsymbol{\ell} \in \mathrm{dom}(\mathbf{T})$:

    We have $s(\mathtt{y}) = p$ for $(p, n) = \mathbf{T}(\boldsymbol{\ell})$ from $\mathbf{s} \approx_{\mathbf{T}} s$.

    Thus we have $s_1(\mathtt{y}) = p'$ for p' with $(p, p') \in r$ from $(s(\mathtt{y}), s_1(\mathtt{y})) \in \overline{r}$.

    Thus we have $\mathbf{T}_1(\boldsymbol{\ell}) = (p', n)$.

    Thus we have $s_1(\mathtt{y}) = p' = \mathrm{phyv}_{\mathbf{T}_1}(\mathbf{s}(\mathtt{y})) \wedge \mathbf{s}(\mathtt{y}) = \boldsymbol{\ell} \widehat{+} 0 \in \mathrm{Safe}(\mathrm{dom}(\mathbf{T}_1))$.

- From $\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} : \mathbf{T} \wedge \forall \boldsymbol{\ell} \in \mathrm{dom}(\mathbf{T}_1).\ \pi_2(\mathbf{T}_1(\boldsymbol{\ell})) = \pi_2(\mathbf{T}(\boldsymbol{\ell}))$, we have
  ✓ $\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} : \mathbf{T}_1$.

- ✓ $\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} :: \mathbf{T}_1 \wedge \mathrm{phyh}_{\mathbf{T}_1}(\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}}) \subseteq h_1$ is shown as follows.

  - Since $\mathrm{shape}(\mathbf{T}_1) \subseteq \sigma_1$ and $\overline{\mathrm{dom}}(\sigma_1 \uplus [p_1 \mapsto m]) \neq \mathrm{undef}$ by $\mathrm{GCAxiom}_1$, we have
    ✓ $\overline{\mathrm{dom}}(\mathrm{shape}(\mathbf{T}_1)) \neq \mathrm{undef}$.

  - Thus it suffices to show that for any $\boldsymbol{\ell}$, $(p, n) = \mathbf{T}_1(\boldsymbol{\ell})$ and $i < n$, the following holds:
    $(\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}})(\boldsymbol{\ell})(i) \in \mathrm{Safe}(\mathrm{dom}(\mathbf{T}_1)) \wedge h_1(p + 4i) = \mathrm{phyv}_{\mathbf{T}_1}((\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}})(\boldsymbol{\ell})(i)) \neq \mathrm{undef}$
  - By definition of $\mathbf{T}_1$ we have p' such that
    ✓ $(p', n) = \mathbf{T}(\boldsymbol{\ell})$ and $(p', p) \in r$.
  - From $\sigma_0' \subseteq \sigma_0 \wedge p' \in \mathrm{reach}(\mathrm{roots}(s), h, \sigma_0') \subseteq \mathrm{dom}(\sigma_0')) \wedge \mathrm{shape}(\mathbf{T}) \subseteq \sigma_0$, we have
    ✓ $\sigma_0'(p') = \sigma_0(p') = \mathrm{shape}(\mathbf{T})(p') = n$.
  - From $(p', p) \in r \wedge \sigma_0'(p') = n \wedge i < n$, we have
    ✓ $(h(p' + 4i), h_1(p + 4i)) \in \overline{r}$.
  - $(\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}})(\boldsymbol{\ell})(i) \in \mathrm{Safe}(\mathrm{dom}(\mathbf{T}))$ follows from $\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} :: \mathbf{T}$, and thus we have two cases.
  - When $(\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}})(\boldsymbol{\ell})(i) = a \in \mathrm{NonPtrs}$:
    ✓ $(\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}})(\boldsymbol{\ell})(i) = a \in \mathrm{Safe}(\mathrm{dom}(\mathbf{T}_1))$.

    From $\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h$, we have
    ✓ $h(p' + 4i) = \mathrm{phyv}_{\mathbf{T}}((\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}})(\boldsymbol{\ell})(i)) = a$.

    From $(h(p' + 4i), h_1(p + 4i)) \in \overline{r}$, we have
    ✓ $h_1(p + 4i) = a = \mathrm{phyv}_{\mathbf{T}_1}((\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}})(\boldsymbol{\ell})(i)) \neq \mathrm{undef}$
  - When $(\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}})(\boldsymbol{\ell})(i) = \boldsymbol{\ell}' \widehat{+} 0$ for $\boldsymbol{\ell}' \in \mathrm{dom}(\mathbf{T})$:

    From $\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h$, we have
    ✓ $h(p' + 4i) = \mathrm{phyv}_{\mathbf{T}}((\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}})(\boldsymbol{\ell})(i)) = p''$ for $(p'', n') = \mathbf{T}(\boldsymbol{\ell}')$.

    From $(h(p' + 4i), h_1(p + 4i)) \in \overline{r}$, we have
    ✓ $h_1(p + 4i) = p'''$ for $(p'', p''') \in r$.

    Since $\mathbf{T}_1(\boldsymbol{\ell}') = (p''', n')$, we have
    ✓ $(\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}})(\boldsymbol{\ell})(i) \in \mathrm{Safe}(\mathrm{dom}(\mathbf{T}_1))$
    ✓ $h_1(p + 4i) = p''' = \mathrm{phyv}_{\mathbf{T}_1}((\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}})(\boldsymbol{\ell})(i)) \neq \mathrm{undef}$.

- Now we do case analysis on m and show $(**)$.
- When $m = 0$:
  - We have
    ✓ $p_1 = 0 \wedge h' = h_1$.
  - Let
    ✓ $\mathbf{s}' = (\mathbf{s} \mid \mathtt{x} \mapsto 0)$,
    ✓ $\mathbf{h}' = \mathbf{h}$,
    ✓ $\mathbf{T}' = \mathbf{T}_1$.
  - $\mathbf{s}', \mathbf{h}' \models \mathtt{x} \hookrightarrow_m 0, \ldots, 0$ follows from $(\mathtt{x} \hookrightarrow_0 \epsilon) = \mathsf{true}$.
  - $\mathbf{s}' \approx_{\mathbf{T}'} s'$ follows from
    (1) $\mathbf{s} \approx_{\mathbf{T}_1} s_1$; and
    (2) $s'(\mathtt{x}) = p_1 = 0 = \mathrm{phyv}_{\mathbf{T}'}(\mathbf{s}'(\mathtt{x})) \wedge \mathbf{s}'(\mathtt{x}) = 0 \in \mathrm{Safe}(\mathrm{dom}(\mathbf{T}'))$.
  - To show $\mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}'} h'$, it suffices to show $\mathrm{shape}(\mathbf{T}') \subseteq I_{\mathrm{gc}}(\mathrm{dom}(\mathrm{shape}(\mathbf{T}')), h')$ since we already have $\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} : \mathbf{T}_1 \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} :: \mathbf{T}_1 \wedge \mathrm{phyh}_{\mathbf{T}_1}(\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}}) \subseteq h_1$.

    By $\mathrm{GCAxiom}_2$, from $\sigma_1 = I_{\mathrm{gc}}(\mathrm{roots}(s'), h')$ and $\mathrm{dom}(\mathrm{shape}(\mathbf{T}')) = \mathrm{dom}(\mathrm{shape}(\mathbf{T}_1)) \subseteq \mathrm{reach}(\mathrm{roots}(s_1), h_1, \sigma_1) = \mathrm{reach}(\mathrm{roots}(s'), h', \sigma_1)$, we have σ_2 such that

    ✓ $\sigma_2 = I_{\mathrm{gc}}(\mathrm{dom}(\mathrm{shape}(\mathbf{T}')), h') \wedge \sigma_2 \subseteq \sigma_1$.

    Now it suffices to show $\mathrm{shape}(\mathbf{T}') \subseteq \sigma_2$, which follows from

    (1) $\mathrm{shape}(\mathbf{T}') = \mathrm{shape}(\mathbf{T}_1) \subseteq \sigma_1 \wedge \sigma_2 \subseteq \sigma_1$; and

    (2) $\mathrm{dom}(\mathrm{shape}(\mathbf{T}')) \subseteq \mathrm{reach}(\mathrm{dom}(\mathrm{shape}(\mathbf{T}')), h', \sigma_2) \subseteq \mathrm{dom}(\sigma_2)$ by $\mathrm{GCAxiom}_1$.

- When $m > 0$:
  - Choose a fresh $\boldsymbol{\ell}_1$ such that $\boldsymbol{\ell}_1 \notin \mathrm{dom}(\mathbf{T}_1) \wedge \mathrm{dom}((\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}})(\boldsymbol{\ell}_1)) = \emptyset$.
  - Let
    ✓ $\mathbf{s}' = (\mathbf{s} \mid \mathtt{x} \mapsto \boldsymbol{\ell}_1 \widehat{+} 0)$,
    ✓ $\mathbf{h}' = \mathbf{h} \uplus [\boldsymbol{\ell}_1 \mapsto_m 0, \dots, 0]$,
    ✓ $\mathbf{T}' = \mathbf{T}_1 \uplus [\boldsymbol{\ell}_1 \mapsto (p_1, m)]$.
  - $\mathbf{s}', \mathbf{h}' \models \mathtt{x} \hookrightarrow_m 0, \dots, 0$ follows from $\mathbf{s}'(\mathtt{x}) = \boldsymbol{\ell}_1 \widehat{+} 0$ and $[\boldsymbol{\ell}_1 \mapsto_m 0, \dots, 0] \subseteq \mathbf{h}'$.
  - $\mathbf{s}' \approx_{\mathbf{T}'} s'$ follows from

    (1) $\mathbf{s} \approx_{\mathbf{T}_1} s_1 \wedge \mathbf{T}_1 \subseteq \mathbf{T}'$; and

    (2) $s'(\mathtt{x}) = p_1 = \mathrm{phyv}_{\mathbf{T}'}(\mathbf{s}'(\mathtt{x})) \wedge \mathbf{s}'(\mathtt{x}) = \boldsymbol{\ell}_1 \widehat{+} 0 \in \mathrm{Safe}(\mathrm{dom}(\mathbf{T}'))$.
  - $\mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}'} h'$ holds because

    (1) $\mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} : \mathbf{T}'$ follows from $\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} : \mathbf{T}_1 \wedge \mathrm{dom}((\mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}})(\boldsymbol{\ell}_1)) = \{0, \dots, m-1\}$;

    (2) $\mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} :: \mathbf{T}'$ follows from $\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} :: \mathbf{T}_1 \wedge \forall i < m.\ (\mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}})(\boldsymbol{\ell}_1)(i) = 0 \in \mathrm{Safe}(\mathrm{dom}(\mathbf{T}'))$;

    (3) $\mathrm{phyh}_{\mathbf{T}'}(\mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}}) \subseteq h'$ follows from $\mathrm{phyh}_{[\boldsymbol{\ell}_1 \mapsto (p_1, m)]}([\boldsymbol{\ell}_1 \mapsto_m 0, \dots, 0]) = [p_1 \mapsto_m 0, \dots, 0]$ and $\mathrm{phyh}_{\mathbf{T}_1}(\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}}) \subseteq h_1$; and

    (4) $\mathrm{shape}(\mathbf{T}') \subseteq I_{\mathrm{gc}}(\mathrm{dom}(\mathrm{shape}(\mathbf{T}')), h')$ is shown as follows.

    Since $\mathrm{dom}(\mathrm{shape}(\mathbf{T}_1)) \subseteq \mathrm{reach}(\mathrm{roots}(s_1), h_1, \sigma_1) \subseteq \mathrm{reach}(\mathrm{roots}(s'), h', \sigma_1 \uplus [p_1 \mapsto m])$ holds by Lemma 8, and since $p_1 \in \mathrm{roots}(s')$ holds, we have
    ✓ $\mathrm{dom}(\mathrm{shape}(\mathbf{T}')) = (\mathrm{dom}(\mathrm{shape}(\mathbf{T}_1)) \cup \{p_1\}) \subseteq \mathrm{reach}(\mathrm{roots}(s'), h', \sigma_1 \uplus [p_1 \mapsto m])$.
    Thus from $\sigma_1 \uplus [p_1 \mapsto m] = I_{\mathrm{gc}}(\mathrm{roots}(s'), h')$, by $\mathrm{GCAxiom}_2$ we have σ_2 such that
    ✓ $\sigma_2 = I_{\mathrm{gc}}(\mathrm{dom}(\mathrm{shape}(\mathbf{T}')), h') \wedge \sigma_2 \subseteq \sigma_1 \uplus [p_1 \mapsto m]$.
    Now it suffices to show $\mathrm{shape}(\mathbf{T}') \subseteq \sigma_2$, which follows from

    (1) $\mathrm{shape}(\mathbf{T}') \subseteq \sigma_1 \uplus [p_1 \mapsto m]$ by $\mathrm{shape}(\mathbf{T}_1) \subseteq \sigma_1$;

    (2) $\sigma_2 \subseteq \sigma_1 \uplus [p_1 \mapsto m]$; and

    (3) $\mathrm{dom}(\mathrm{shape}(\mathbf{T}')) \subseteq \mathrm{reach}(\mathrm{dom}(\mathrm{shape}(\mathbf{T}')), h', \sigma_2) \subseteq \mathrm{dom}(\sigma_2)$ by $\mathrm{GCAxiom}_1$.

□

5.3.2 Incl

Theorem 16 (Soundness: Incl)**.**

$$\frac{V \subseteq_{\mathrm{fin}} \mathrm{ProgVars} \qquad \{P \wedge \mathsf{safe}(V)\}\ C\ \{Q \wedge \mathsf{safe}(\mathrm{Mod}(C))\}}{\{\{P\}\}\ C\ \{\{Q\}\}}$$

$$\frac{V \subseteq_{\mathrm{fin}} \mathrm{ProgVars} \qquad [P \wedge \mathsf{safe}(V)]\ C\ [Q \wedge \mathsf{safe}(\mathrm{Mod}(C))]}{[[P]]\ C\ [[Q]]}$$

Proof.

- Assume: $\forall \rho \in \mathrm{Env}(\mathrm{FLV}(P, Q)), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$.
  $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} (P[\rho] \wedge \mathsf{safe}(V)) \wedge \mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge C, s, h \rightsquigarrow^{*} C', s', h' \implies$
  $\big((C', s', h' \rightsquigarrow -) \vee$
  $(\exists \mathbf{s}', \mathbf{h}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} (Q[\rho] \wedge \mathsf{safe}(\mathrm{Mod}(C))) \wedge$
  $(\forall \mathtt{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathtt{y}) = \mathbf{s}(\mathtt{y})) \wedge \mathbf{s}' \sim_{\mathbf{T}} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h')\big)$
  [# $\wedge\ \neg(C, s, h$ diverges) #]

- Assume: $\rho \in \mathrm{Env}(\mathrm{FLV}(P, Q)), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$ such that
  ✓ $\mathbf{s}, \mathbf{h} \models P[\rho] \wedge \mathbf{s} \approx_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge C, s, h \rightsquigarrow^{*} C', s', h'$

- To show:
  [# $\neg(C, s, h$ diverges); and #]
  $(*)$ $C', s', h' \rightsquigarrow -$; or
  $(**)$ $\exists \mathbf{s}', \mathbf{h}', \mathbf{T}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models Q[\rho] \wedge$
  $(\forall \mathtt{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathtt{y}) = \mathbf{s}(\mathtt{y})) \wedge \mathbf{s}' \approx_{\mathbf{T}'} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}'} h'$

- From $\mathbf{s}, \mathbf{h} \models P[\rho]$ and $\mathbf{s} \approx_{\mathbf{T}} s$, by Lemma 6 we have
  ✓ $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} P[\rho] \wedge \mathsf{safe}(V)$.

- [# $\neg(C, s, h$ diverges) by assumption #]

- Also by assumption we have two cases.

- When $C', s', h' \rightsquigarrow -$:
  $(*)$ holds.

- When $C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} (Q[\rho] \wedge \mathsf{safe}(\mathrm{Mod}(C))) \wedge (\forall \mathtt{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathtt{y}) = \mathbf{s}(\mathtt{y})) \wedge \mathbf{s}' \sim_{\mathbf{T}} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h'$ for some $\mathbf{s}', \mathbf{h}'$:
  $(**)$ is shown as follows.

- To show $(**)$, it suffices to show that $\mathbf{s}', \mathbf{h}' \models Q[\rho] \wedge \mathbf{s}' \approx_{\mathbf{T}} s'$.

- $\mathbf{s}', \mathbf{h}' \models Q[\rho]$ follows from $\mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} Q[\rho]$ by Lemmas 6.

- $\mathbf{s}'' \approx_{\mathbf{T}} s'$ holds as follows.
  - when $\mathtt{x} \in \mathrm{Mod}(C)$:
    $\mathrm{phyv}_{\mathbf{T}}(\mathbf{s}'(\mathtt{x})) = s'(\mathtt{x})$ follows from $\mathbf{s}' \sim_{\mathbf{T}} s'$.
    $\mathbf{s}'(\mathtt{x}) \in \mathrm{Safe}(\mathrm{dom}(\mathbf{T}))$ follows from $\mathbf{s}', \mathbf{h}' \models_{\mathrm{dom}(\mathbf{T})} \mathsf{safe}(\mathrm{Mod}(C))$.
  - when $\mathtt{x} \notin \mathrm{Mod}(C)$:
    $\mathrm{phyv}_{\mathbf{T}}(\mathbf{s}'(\mathtt{x})) = \mathrm{phyv}_{\mathbf{T}}(\mathbf{s}(\mathtt{x})) = s(\mathtt{x}) = s'(\mathtt{x})$ follows from $\mathbf{s} \approx_{\mathbf{T}} s$ and $s(\mathtt{x}) = s'(\mathtt{x})$.
    $\mathbf{s}'(\mathtt{x}) = \mathbf{s}(\mathtt{x}) \in \mathrm{Safe}(\mathrm{dom}(\mathbf{T}))$ follows from $\mathbf{s} \approx_{\mathbf{T}} s$.

□

5.3.3 Seq

Lemma 12 (Soundness: Generalized Seq)**.**

$$\frac{\{\{P\}\}\ C_1\ \{\{Q\}\} : k \qquad \{\{Q\}\}\ C_2\ \{\{R\}\} : k}{\{\{P\}\}\ C_1; C_2\ \{\{R\}\} : k}$$

Proof.

- Assume: $\{\{P\}\}\ C_1\ \{\{Q\}\} : k$
- Assume: $\{\{Q\}\}\ C_2\ \{\{R\}\} : k$
- Assume: $\rho \in \mathrm{Env}(\mathrm{FLV}(P, R)), j, \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$ such that
  $j \leq k \wedge \mathbf{s}, \mathbf{h} \models P[\rho] \wedge \mathbf{s} \approx_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge (C_1; C_2, s, h \rightsquigarrow^{j} C', s', h')$
- To show:
  $(*)$ $(C', s', h' \rightsquigarrow -) \vee$
  $(**)$ $(\exists \mathbf{s}', \mathbf{h}', \mathbf{T}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models R[\rho] \wedge$
  $(\forall \mathrm{y} \notin \mathrm{Mod}(C_1; C_2).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathbf{s}' \approx_{\mathbf{T}'} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}'} h')$
- Let $\rho' := \rho|^{\mathrm{FLV}(Q)}$.
- Then, as $P[\rho] = P[\rho']$, we have
  ✓ $\mathbf{s}, \mathbf{h} \models P[\rho']$.
- From $C_1; C_2, s, h \rightsquigarrow^{j} C', s', h'$, we have two cases.
- When $C_1, s, h \rightsquigarrow^{j} C_1', s', h' \wedge C' = C_1'; C_2$:
  - By assumption we have two cases.
  - When $C_1', s', h' \rightsquigarrow -$:
    $(*)$ holds because $(C_1'; C_2), s', h' \rightsquigarrow -$.
  - When $C_1' = \mathsf{skip} \wedge (\mathbf{s}', \mathbf{h}' \models Q[\rho']) \wedge (\forall \mathrm{y} \notin \mathrm{Mod}(C_1).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathbf{s}' \approx_{\mathbf{T}'} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}'} h'$ for some $\mathbf{s}', \mathbf{h}'$:
    $(*)$ holds because $(\mathsf{skip}; C_2), s', h' \rightsquigarrow C_2, s', h'$.
- When $C_1, s, h \rightsquigarrow^{j_1} \mathsf{skip}, s_1', h_1' \wedge C_2, s_1', h_1' \rightsquigarrow^{j_2} C', s', h' \wedge j = j_1 + j_2 + 1$:
  - As $j_1 \leq k \wedge C_1, s, h \rightsquigarrow^{j_1} \mathsf{skip}, s_1', h_1'$, by assumption we have $\mathbf{s}_1', \mathbf{h}_1', \mathbf{T}_1'$ such that
    ✓ $\mathbf{s}_1', \mathbf{h}_1' \models Q[\rho'] \wedge (\forall \mathrm{y} \notin \mathrm{Mod}(C_1).\ \mathbf{s}_1'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathbf{s}_1' \approx_{\mathbf{T}_1'} s_1' \wedge \mathbf{h}_1' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}_1'} h_1'$.
  - As $j_2 \leq k \wedge C_2, s_1', h_1' \rightsquigarrow^{j_2} C', s', h'$, by assumption we have two cases.
  - When $C', s', h' \rightsquigarrow -$:
    $(*)$ holds.
  - When $C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models R[\rho'] \wedge (\forall \mathrm{y} \notin \mathrm{Mod}(C_2).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}_1'(\mathrm{y})) \wedge \mathbf{s}' \approx_{\mathbf{T}'} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}'} h'$:
    $(**)$ holds because
    (1) $\mathbf{s}', \mathbf{h}' \models R[\rho]$ holds since $R[\rho'] = R[\rho]$;
    (2) $(\forall \mathrm{y} \notin \mathrm{Mod}(C_1; C_2).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y}))$ follows from $(\forall \mathrm{y} \notin \mathrm{Mod}(C_2).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}_1'(\mathrm{y}))$ and $(\forall \mathrm{y} \notin \mathrm{Mod}(C_1).\ \mathbf{s}_1'(\mathrm{y}) = \mathbf{s}(\mathrm{y}))$ since $\mathrm{Mod}(C_1; C_2) = \mathrm{Mod}(C_1) \cup \mathrm{Mod}(C_2)$.

□

Theorem 17 (Soundness: Seq (partial))**.**

$$\frac{\{\{P\}\}\ C_1\ \{\{Q\}\} \qquad \{\{Q\}\}\ C_2\ \{\{R\}\}}{\{\{P\}\}\ C_1; C_2\ \{\{R\}\}}$$

Proof. It holds by Lemma 12. □

Theorem 18 (Soundness: Seq (total))**.**

$$\frac{[[P]]\ C_1\ [[Q]] \qquad [[Q]]\ C_2\ [[R]]}{[[P]]\ C_1; C_2\ [[R]]}$$

Proof.

- Assume $[[P]]\ C_1\ [[Q]]$.
- Assume $[[Q]]\ C_2\ [[R]]$.
- By Theorem 17, we have $\{\{P\}\}\ C_1; C_2\ \{\{R\}\}$.
- Assume: $\rho \in \mathrm{Env}(\mathrm{FLV}(P, R)), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h$ such that
  $\mathbf{s}, \mathbf{h} \models P[\rho] \wedge \mathbf{s} \approx_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h$.
- Now we show $\neg(C_1; C_2, s, h$ diverges) by contradiction.
- Assume $\{\, D_i, s_i, h_i \,\}_{i \in \mathbb{N}}$ such that
  ✓ $(D_0, s_0, h_0) = (C_1; C_2, s, h) \wedge \forall i.\ D_i, s_i, h_i \rightsquigarrow D_{i+1}, s_{i+1}, h_{i+1}$.
- Let $\rho' := \rho|^{\mathrm{FLV}(Q)}$.
- Then, as $P[\rho] = P[\rho']$, we have $\mathbf{s}, \mathbf{h} \models P[\rho']$.
- By $[[P]]\ C_1\ [[Q]]$, we have $\neg(C_1, s, h$ diverges).
- Thus, we have some k such that $D_k = (\mathsf{skip}; C_2)$ and $C_1, s, h \rightsquigarrow^k \mathsf{skip}, s_k, h_k$.
- As $D_k = (\mathsf{skip}; C_2)$, we have $D_{k+1} = C_2$, $s_{k+1} = s_k$, and $h_{k+1} = h_k$.
- By $[[P]]\ C_1\ [[Q]]$, we have $\mathbf{s}', \mathbf{h}', \mathbf{T}'$ such that
  ✓ $\mathbf{s}', \mathbf{h}' \models Q[\rho'] \wedge (\forall \mathrm{y} \notin \mathrm{Mod}(C_1).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathbf{s}' \approx_{\mathbf{T}'} s_k \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}'} h_k$.
- By $[[Q]]\ C_2\ [[R]]$, we have $\neg(C_2, s_k, h_k$ diverges).
- Thus we have $\neg(D_{k+1}, s_{k+1}, h_{k+1}$ diverges), which is a contradiction.

□

5.3.4 Frame

Theorem 19 (Soundness: Frame)**.**

$$\frac{\{\{P\}\}\ C\ \{\{Q\}\} \qquad \mathrm{FPV}(R)\cap\mathrm{Mod}(C)=\emptyset}{\{\{P*R\}\}\ C\ \{\{Q*R\}\}} \qquad\qquad \frac{[[P]]\ C\ [[Q]] \qquad \mathrm{FPV}(R)\cap\mathrm{Mod}(C)=\emptyset}{[[P*R]]\ C\ [[Q*R]]}$$

Proof.

- Assume: $\mathrm{FPV}(R)\cap\mathrm{Mod}(C)=\emptyset$

- Assume: $\forall\rho\in\mathrm{Env}(\mathrm{FLV}(P,Q)),\mathbf{s},\mathbf{h},\mathbf{h}_{\mathrm{F}},\mathbf{T},s,h,C',s',h'.$
  $\mathbf{s},\mathbf{h}\models P[\rho]\wedge\mathbf{s}\approx_{\mathbf{T}} s\wedge\mathbf{h}\uplus\mathbf{h}_{\mathrm{F}}\approx_{\mathbf{T}} h\wedge C,s,h\rightsquigarrow^{*} C',s',h' \implies$
  $\big((C',s',h'\rightsquigarrow -)\vee$
  $(\exists\mathbf{s}',\mathbf{h}',\mathbf{T}'.\ C'=\mathsf{skip}\wedge\mathbf{s}',\mathbf{h}'\models Q[\rho]\wedge$
  $(\forall\mathrm{y}\notin\mathrm{Mod}(C).\ \mathbf{s}'(\mathrm{y})=\mathbf{s}(\mathrm{y}))\wedge\mathbf{s}'\approx_{\mathbf{T}'} s'\wedge\mathbf{h}'\uplus\mathbf{h}_{\mathrm{F}}\approx_{\mathbf{T}'} h')\big)$
  [# $\wedge\neg(C,s,h$ diverges$)$ #]

- Assume: $\rho\in\mathrm{Env}(\mathrm{FLV}(P,Q,R)),\mathbf{s},\mathbf{h},\mathbf{h}_{\mathrm{F}},\mathbf{T},s,h,C',s',h'$ such that
  $\mathbf{s},\mathbf{h}\models(P[\rho]*R[\rho])\wedge\mathbf{s}\approx_{\mathbf{T}} s\wedge\mathbf{h}\uplus\mathbf{h}_{\mathrm{F}}\approx_{\mathbf{T}} h\wedge C,s,h\rightsquigarrow^{*} C',s',h'$

- To show:
  [# $\neg(C,s,h$ diverges$)$; and #]
  $(*)$ $(C',s',h'\rightsquigarrow -)\vee$
  $(**)$ $(\exists\mathbf{s}',\mathbf{h}',\mathbf{T}'.\ C'=\mathsf{skip}\wedge\mathbf{s}',\mathbf{h}'\models(Q[\rho]*R[\rho])\wedge$
  $(\forall\mathrm{y}\notin\mathrm{Mod}(C).\ \mathbf{s}'(\mathrm{y})=\mathbf{s}(\mathrm{y}))\wedge\mathbf{s}'\approx_{\mathbf{T}'} s'\wedge\mathbf{h}'\uplus\mathbf{h}_{\mathrm{F}}\approx_{\mathbf{T}'} h')$

- From $\mathbf{s},\mathbf{h}\models(P[\rho]*R[\rho])$, we have $\mathbf{h}_1$ and $\mathbf{h}_2$ such that
  ✓ $\mathbf{h}=\mathbf{h}_1\uplus\mathbf{h}_2$,
  ✓ $\mathbf{s},\mathbf{h}_1\models P[\rho]$,
  ✓ $\mathbf{s},\mathbf{h}_2\models R[\rho]$.

- [# $\neg(C,s,h$ diverges$)$ holds by assumption since $\mathbf{h}\uplus\mathbf{h}_{\mathrm{F}}=\mathbf{h}_1\uplus(\mathbf{h}_2\uplus\mathbf{h}_{\mathrm{F}})\wedge\mathbf{s},\mathbf{h}_1\models P[\rho]$ #]

- Also by assumption we have two cases since $\mathbf{h}\uplus\mathbf{h}_{\mathrm{F}}=\mathbf{h}_1\uplus(\mathbf{h}_2\uplus\mathbf{h}_{\mathrm{F}})\wedge\mathbf{s},\mathbf{h}_1\models P[\rho]$.

- When $C',s',h'\rightsquigarrow -$:
  $(*)$ holds.

- When $C'=\mathsf{skip}\wedge(\mathbf{s}',\mathbf{h}'\models Q[\rho])\wedge(\forall\mathrm{y}\notin\mathrm{Mod}(C).\ \mathbf{s}'(\mathrm{y})=\mathbf{s}(\mathrm{y}))\wedge\mathbf{s}'\approx_{\mathbf{T}'} s'\wedge\mathbf{h}'\uplus\mathbf{h}_2\uplus\mathbf{h}_{\mathrm{F}}\approx_{\mathbf{T}'} h'$ for some $\mathbf{s}',\mathbf{h}'$:
  $(**)$ is shown as follows.

- To show $(**)$, it suffices to show that $\mathbf{s}',\mathbf{h}'\uplus\mathbf{h}_2\models Q[\rho]*R[\rho]$.

- We split the heap $\mathbf{h}'\uplus\mathbf{h}_2$ into $\mathbf{h}'$ and $\mathbf{h}_2$.

- As $\mathbf{s}',\mathbf{h}'\models Q[\rho]$ holds, we need to show $\mathbf{s}',\mathbf{h}_2\models R[\rho]$, which follows from $(\mathbf{s},\mathbf{h}_2\models R[\rho])\wedge(\forall\mathrm{y}\notin\mathrm{Mod}(C).\ \mathbf{s}'(\mathrm{y})=\mathbf{s}(\mathrm{y}))\wedge\mathrm{FPV}(R)\cap\mathrm{Mod}(C)=\emptyset$ by Lemma 5.

□

5.3.5 Conseq

Theorem 20 (Soundness: Conseq)**.**

$$\frac{P \models P' \qquad \{\{P'\}\}\ C\ \{\{Q'\}\} \qquad Q' \models Q}{\{\{P\}\}\ C\ \{\{Q\}\}} \qquad \frac{P \models P' \qquad [[P']]\ C\ [[Q']] \qquad Q' \models Q}{[[P]]\ C\ [[Q]]}$$

Proof.

- Assume: $P \models P'$ and $Q' \models Q$.
- Assume: $\forall \rho \in \mathrm{Env}(\mathrm{FLV}(P', Q')), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'.$
  $\mathbf{s}, \mathbf{h} \models P'[\rho] \land \mathbf{s} \approx_{\mathbf{T}} s \land \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \land C, s, h \leadsto^* C', s', h' \implies$
  $\big((C', s', h' \leadsto -) \lor$
  $(\exists \mathbf{s}', \mathbf{h}', \mathbf{T}'.\ C' = \mathsf{skip} \land \mathbf{s}', \mathbf{h}' \models Q'[\rho] \land$
  $(\forall \mathrm{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \land \mathbf{s}' \approx_{\mathbf{T}'} s' \land \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}'} h')\big)$
  [# $\land \neg(C, s, h$ diverges) #]
- Assume: $\rho \in \mathrm{Env}(\mathrm{FLV}(P, Q)), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$ such that
  $\mathbf{s}, \mathbf{h} \models P[\rho] \land \mathbf{s} \approx_{\mathbf{T}} s \land \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \land C, s, h \leadsto^* C', s', h'$
- To show:
  [# $\neg(C, s, h$ diverges); and #]
  $(*)$ $(C', s', h' \leadsto -) \lor$
  $(**)$ $(\exists \mathbf{s}', \mathbf{h}', \mathbf{T}'.\ C' = \mathsf{skip} \land \mathbf{s}', \mathbf{h}' \models Q[\rho] \land$
  $(\forall \mathrm{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \land \mathbf{s}' \approx_{\mathbf{T}'} s' \land \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}'} h')$
- Let $\rho' \stackrel{\mathrm{def}}{=} \rho|^{\mathrm{FLV}(P', Q')}$.
- From $P \models P'$ and $\mathbf{s} \approx_{\mathbf{T}} s \land \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \land \mathbf{s}, \mathbf{h} \models P[\rho']$ (as $P[\rho'] = P[\rho]$), we have
  ✓ $\mathbf{s}, \mathbf{h} \models P'[\rho']$.
- [# $\neg(C, s, h$ diverges) holds by assumption. #]
- Also by assumption we have two cases.
- When $C', s', h' \leadsto -$:
  $(*)$ holds.
- When $C' = \mathsf{skip} \land (\mathbf{s}', \mathbf{h}' Q'[\rho']) \land (\forall \mathrm{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \land \mathbf{s}' \approx_{\mathbf{T}'} s' \land \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}'} h'$ for some $\mathbf{s}', \mathbf{h}'$:
  $(**)$ holds because $\mathbf{s}', \mathbf{h}' \models Q[\rho]$ follows from $Q' \models Q$ and $\mathbf{s}' \approx_{\mathbf{T}'} s' \land \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}'} h' \land \mathbf{s}', \mathbf{h}' \models Q'[\rho']$ (as $Q[\rho'] = Q[\rho]$)..

□

5.3.6 Ex

Theorem 21 (Soundness: Ex)**.**

$$\frac{\{\{P\}\}\ C\ \{\{Q\}\}}{\{\{\exists v.\, P\}\}\ C\ \{\{\exists v.\, Q\}\}} \qquad \frac{[[P]]\ C\ [[Q]]}{[[\exists v.\, P]]\ C\ [[\exists v.\, Q]]}$$

Proof.

- Assume: $\forall \rho \in \mathrm{Env}(\mathrm{FLV}(P, Q)), \mathbf{s}, \mathbf{h}, \mathbf{h}_\mathrm{F}, \mathbf{T}, s, h, C', s', h'.$
  $\mathbf{s}, \mathbf{h} \models P[\rho] \wedge \mathbf{s} \approx_\mathbf{T} s \wedge \mathbf{h} \uplus \mathbf{h}_\mathrm{F} \approx_\mathbf{T} h \wedge C, s, h \rightsquigarrow^* C', s', h' \implies$
  $\big((C', s', h' \rightsquigarrow -) \vee$
  $(\exists \mathbf{s}', \mathbf{h}', \mathbf{T}'.\ C' = \textsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models Q[\rho] \wedge$
  $(\forall \mathbf{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathbf{y}) = \mathbf{s}(\mathbf{y})) \wedge \mathbf{s}' \approx_{\mathbf{T}'} s' \wedge \mathbf{h}' \uplus \mathbf{h}_\mathrm{F} \approx_{\mathbf{T}'} h')\big)$
  [# $\wedge \neg(C, s, h$ diverges) #]
- Assume: $\rho \in \mathrm{Env}(\mathrm{FLV}(\exists v.\, P, \exists v.\, Q)), \mathbf{s}, \mathbf{h}, \mathbf{h}_\mathrm{F}, \mathbf{T}, s, h, C', s', h'$ such that
  $(\mathbf{s}, \mathbf{h} \models (\exists v.\, P)[\rho]) \wedge \mathbf{s} \approx_\mathbf{T} s \wedge \mathbf{h} \uplus \mathbf{h}_\mathrm{F} \approx_\mathbf{T} h \wedge C, s, h \rightsquigarrow^* C', s', h'$
- To show:
  [# $\neg(C, s, h$ diverges); and #]
  $(*)$ $(C', s', h' \rightsquigarrow -) \vee$
  $(**)$ $(\exists \mathbf{s}', \mathbf{h}', \mathbf{T}'.\ C' = \textsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models (\exists v.\, Q)[\rho] \wedge$
  $(\forall \mathbf{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathbf{y}) = \mathbf{s}(\mathbf{y})) \wedge \mathbf{s}' \approx_{\mathbf{T}'} s' \wedge \mathbf{h}' \uplus \mathbf{h}_\mathrm{F} \approx_{\mathbf{T}'} h')$
- From $\mathbf{s}, \mathbf{h} \models (\exists v.\, P)[\rho]$, by Lemma 7 we have
  ✓ $\mathbf{s}, \mathbf{h} \models P[(\rho \mid v \mapsto \mathbf{v})]$ for some $\mathbf{v} \in \mathrm{LogVals}$.
- Let $\rho' := (\rho \mid v \mapsto \mathbf{v})$.
- [# $\neg(C, s, h$ diverges) holds by assumption. #]
- Also by assumption we have two cases.
- When $C', s', h' \rightsquigarrow -$:
  $(*)$ holds.
- When $C' = \textsf{skip} \wedge (\mathbf{s}', \mathbf{h}' \models Q[\rho']) \wedge (\forall \mathbf{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathbf{y}) = \mathbf{s}(\mathbf{y})) \wedge \mathbf{s}' \approx_{\mathbf{T}'} s' \wedge \mathbf{h}' \uplus \mathbf{h}_\mathrm{F} \approx_{\mathbf{T}'} h'$ for some $\mathbf{s}', \mathbf{h}'$:
  $(**)$ holds because $\mathbf{s}', \mathbf{h}' \models (\exists v.\, Q)[\rho]$ follows from $\mathbf{s}', \mathbf{h}' \models Q[\rho']$ by Lemma 7.

□

5.3.7 Gen

Theorem 22 (Soundness: Gen)**.**

$$\frac{\forall \mathbf{v} \in \mathrm{LogVals}.\ \{\{P[\mathbf{v}/v]\}\}\ C\ \{\{Q[\mathbf{v}/v]\}\}}{\{\{P\}\}\ C\ \{\{Q\}\}} \qquad \frac{\forall \mathbf{v} \in \mathrm{LogVals}.\ [[P[\mathbf{v}/v]]]\ C\ [[Q[\mathbf{v}/v]]]}{[[P]]\ C\ [[Q]]}$$

Proof. The goal directly follows by definition because $P[\rho] = P[\rho(v)/v][\rho]$ and $Q[\rho] = Q[\rho(v)/v][\rho]$ for any $\rho \in \mathrm{Env}(\mathrm{FLV}(P, Q))$. □

5.3.8 Total

Theorem 23 (Soundness: Total)**.**

$$\frac{[[P]]\ C\ [[Q]]}{\{\{P\}\}\ C\ \{\{Q\}\}}$$

Proof. It holds vacuously by definition. □

5.3.9 If

Theorem 24 (Soundness: If)**.**

$$\frac{\{\{P \wedge E\}\}\ C_1\ \{\{Q\}\} \qquad \{\{P \wedge \mathsf{not}\ E\}\}\ C_2\ \{\{Q\}\}}{\{\{P \wedge \mathsf{word}(E)\}\}\ \mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}\ \{\{Q\}\}} \qquad \frac{[[P \wedge E]]\ C_1\ [[Q]] \qquad [[P \wedge \mathsf{not}\ E]]\ C_2\ [[Q]]}{[[P \wedge \mathsf{word}(E)]]\ \mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}\ [[Q]]}$$

Proof.

- Assume: $\forall \rho \in \mathrm{Env}(\mathrm{FLV}(P, Q)), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$.
  $(\mathbf{s}, \mathbf{h} \models P[\rho] \wedge E) \wedge \mathbf{s} \approx_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge C_1, s, h \rightsquigarrow^* C', s', h' \implies$
  $\big((C', s', h' \rightsquigarrow -) \vee$
  $(\exists \mathbf{s}', \mathbf{h}', \mathbf{T}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models Q[\rho] \wedge$
  $(\forall \mathrm{y} \notin \mathrm{Mod}(C_1).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathbf{s}' \approx_{\mathbf{T}'} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}'} h')\big)$
  [# $\wedge \neg(C_1, s, h$ diverges) #]

- Assume: $\forall \rho \in \mathrm{Env}(\mathrm{FLV}(P, Q)), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$.
  $(\mathbf{s}, \mathbf{h} \models P[\rho] \wedge \mathsf{not}\ E) \wedge \mathbf{s} \approx_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge C_2, s, h \rightsquigarrow^* C', s', h' \implies$
  $\big((C', s', h' \rightsquigarrow -) \vee$
  $(\exists \mathbf{s}', \mathbf{h}', \mathbf{T}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models Q[\rho] \wedge$
  $(\forall \mathrm{y} \notin \mathrm{Mod}(C_2).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathbf{s}' \approx_{\mathbf{T}'} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}'} h')\big)$
  [# $\wedge \neg(C_2, s, h$ diverges) #]

- Assume: $\rho \in \mathrm{Env}(\mathrm{FLV}(P, Q)), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$ such that
  $(\mathbf{s}, \mathbf{h} \models P[\rho] \wedge \mathsf{word}(E)) \wedge \mathbf{s} \approx_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge \mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}, s, h \rightsquigarrow^* C', s', h'$

- To show:
  [# $\neg$(if E then C_1 else C_2 fi$, s, h$ diverges); and #]
  $(*)\ \ (C', s', h' \rightsquigarrow -) \vee$
  $(**)\ (\exists \mathbf{s}', \mathbf{h}', \mathbf{T}'.\ C' = \mathsf{skip} \wedge \mathbf{s}', \mathbf{h}' \models Q[\rho] \wedge$
  $(\forall \mathrm{y} \notin \mathrm{Mod}(C_1, C_2).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathbf{s}' \approx_{\mathbf{T}'} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}'} h')$

- From $\mathbf{s}, \mathbf{h} \models \mathsf{word}(E)$, we have
  ✓ $[\![\![E]\!]\!]_{\mathbf{s}} \in \mathrm{Words}$.

- By Lemma 2, we have
  ✓ $[\![E]\!]_s = \mathrm{phyv}_{\mathbf{T}}([\![\![E]\!]\!]_{\mathbf{s}}) = [\![\![E]\!]\!]_{\mathbf{s}}$.

- Thus, we have two cases.

- When $[\![\![E]\!]\!]_{\mathbf{s}} \in \mathrm{Words} \backslash \{0\}$:
  - [# Since we have if E then C_1 else C_2 fi$, s, h \rightsquigarrow C_1, s, h$ and $\mathbf{s}, \mathbf{h} \models P[\rho] \wedge E$, by assumption we have $\neg(C_1, s, h$ diverges) and thus $\neg(C, s, h$ diverges) holds. #]
  - From if E then C_1 else C_2 fi$, s, h \rightsquigarrow^* C', s', h'$ we have two cases.
  - When $C' = \mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi} \wedge s' = s \wedge h' = h$:
    $(*)$ holds as we have if E then C_1 else C_2 fi$, s, h \rightsquigarrow C_1, s, h$.
  - When $C_1, s, h \rightsquigarrow^* C', s', h'$:
    $(*)$ or $(**)$ holds by assumption since we have $\mathbf{s}, \mathbf{h} \models P[\rho] \wedge E$.

- When $[\![E]\!]_{\mathbf{s}} = 0$:
  - [# Since we have $\mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}, s, h \rightsquigarrow C_2, s, h$ and $\mathbf{s}, \mathbf{h} \models P[\rho] \wedge \mathsf{not}\ E$, by assumption we have $\neg(C_2, s, h$ diverges) and thus $\neg(C, s, h$ diverges) holds. #]
  - From $\mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}, s, h \rightsquigarrow^* C', s', h'$ we have two cases.
  - When $C' = \mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi} \wedge s' = s \wedge h' = h$:
    $(*)$ holds as we have $\mathsf{if}\ E\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ \mathsf{fi}, s, h \rightsquigarrow C_2, s, h$.
  - When $C_2, s, h \rightsquigarrow^* C', s', h'$:
    $(*)$ or $(**)$ holds by assumption since we have $\mathbf{s}, \mathbf{h} \models P[\rho] \wedge \mathsf{not}\ E$.

□

5.3.10 While

Theorem 25 (Soundness: While)**.**

$$\frac{\{\{P \wedge E\}\}\ C\ \{\{P \wedge \mathsf{word}(E)\}\}}{\{\{P \wedge \mathsf{word}(E)\}\}\ \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}\ \{\{P \wedge \mathsf{not}\ E\}\}}$$

Proof.

- Assume: $\{\{P \wedge E\}\}\ C\ \{\{P \wedge \mathsf{word}(E)\}\}$
- To show: $\forall k.\ \{\{P \wedge \mathsf{word}(E)\}\}\ \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}\ \{\{P \wedge \mathsf{not}\ E\}\} : k$
- We prove the goal by induction on k.
- (Base case) when $k = 0$,
  - Assume: $\rho \in \mathrm{Env}(\mathrm{FLV}(P)), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$ such that
    $(\mathbf{s}, \mathbf{h} \models P[\rho] \wedge \mathsf{word}(E)) \wedge \mathbf{s} \approx_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}, s, h \rightsquigarrow^k C', s', h'$.
  - It suffices to show
    $(*)\quad C', s', h' \rightsquigarrow -$.
  - From $\mathbf{s}, \mathbf{h} \models \mathsf{word}(E)$, we have
    ✓ $[\![E]\!]_{\mathbf{s}} \in \mathrm{Words}$.
  - By Lemma 2, we have
    ✓ $[\![E]\!]_s = \mathrm{phyv}_{\mathbf{T}}([\![E]\!]_{\mathbf{s}}) = [\![E]\!]_{\mathbf{s}}$.
  - $(*)$ holds because $C' = \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od} \wedge s' = s \wedge h' = h$ and $[\![E]\!]_s \neq \mathrm{undef}$.
- (Inductive step) when $k > 0 \wedge \forall j < k.\ \{\{P \wedge \mathsf{word}(E)\}\}\ \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}\ \{\{P \wedge \mathsf{not}\ E\}\} : j$,
  - Assume: $\rho \in \mathrm{Env}(\mathrm{FLV}(P)), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h, C', s', h'$ such that
    $(\mathbf{s}, \mathbf{h} \models P[\rho] \wedge \mathsf{word}(E)) \wedge \mathbf{s} \approx_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h \wedge \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}, s, h \rightsquigarrow^k C', s', h'$.
  - To show:
    $(*)\quad (C', s', h' \rightsquigarrow -) \vee$
    $(**)\ (\exists \mathbf{s}', \mathbf{h}', \mathbf{T}'.\ C' = \mathsf{skip} \wedge (\mathbf{s}', \mathbf{h}' \models P[\rho] \wedge \mathsf{not}\ E) \wedge$
    $(\forall \mathrm{y} \notin \mathrm{Mod}(C).\ \mathbf{s}'(\mathrm{y}) = \mathbf{s}(\mathrm{y})) \wedge \mathbf{s}' \approx_{\mathbf{T}'} s' \wedge \mathbf{h}' \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}'} h')$

- From $\mathbf{s}, \mathbf{h} \models \mathsf{word}(E)$, we have
  ✓ $[\![\![E]\!]\!]_{\mathbf{s}} \in \text{Words}$.
- By Lemma 2, we have
  ✓ $[\![E]\!]_s = \text{phyv}_{\mathbf{T}}([\![\![E]\!]\!]_{\mathbf{s}}) = [\![\![E]\!]\!]_{\mathbf{s}}$.
- Thus we have two cases.
- When $[\![E]\!]_s = [\![\![E]\!]\!]_{\mathbf{s}} = 0$:
  - ◇ We have $\mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}, s, h \rightsquigarrow \mathsf{skip}, s, h$.
  - ◇ Thus we have $\mathsf{skip}, s, h \rightsquigarrow^{k-1} C', s', h'$, from which it follows that
    ✓ $C' = \mathsf{skip} \wedge s' = s \wedge h' = h$.
  - ◇ Thus $(**)$ holds because we have $\mathbf{s}, \mathbf{h} \models \mathsf{not}\ E$ from $[\![\![\mathsf{not}\ E]\!]\!]_{\mathbf{s}} = 1$.
- When $[\![E]\!]_s = [\![\![E]\!]\!]_{\mathbf{s}} \in \text{Words}\backslash\{0\}$:
  - ◇ We have $\mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}, s, h \rightsquigarrow (C; \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}), s, h$, from which we have
    ✓ $(C; \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}), s, h \rightsquigarrow^{k-1} C', s', h'$.
  - ◇ From $\{\{P \wedge E\}\}\ C\ \{\{P \wedge \mathsf{word}(E)\}\}$ and $\{\{P \wedge \mathsf{word}(E)\}\}\ \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}\ \{\{P \wedge \mathsf{not}\ E\}\} : k-1$, by Lemma 12 we have
    ✓ $\{\{P \wedge E\}\}\ C; \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}\ \{\{P \wedge \mathsf{not}\ E\}\} : k-1$.
  - ◇ Thus $(*) \vee (**)$ holds since we have $\mathbf{s}, \mathbf{h} \models E$ from $[\![\![E]\!]\!]_{\mathbf{s}} \in \text{Words}\backslash\{0\}$.

□

Theorem 26 (Soundness: WhileT)**.**

$$\frac{[[P \wedge E \wedge 0 < \mathbf{E}' = v]]\ C\ [[P \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}' < v]] \qquad v \notin \text{FLV}(P, \mathbf{E}')}{[[P \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}']]\ \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}\ [[P \wedge \mathsf{not}\ E]]}$$

Proof.

- Assume: $[[P \wedge E \wedge 0 < \mathbf{E}' = v]]\ C\ [[P \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}' < v]]$ and $v \notin \text{FLV}(P, \mathbf{E}')$.
- By Theorems 20, 21, 23 and 25, we have

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[[P \wedge E \wedge 0 < \mathbf{E}' = v]]\ C\ [[P \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}' < v]]}{[[\exists v.\, P \wedge E \wedge 0 < \mathbf{E}' = v]]\ C\ [[\exists v.\, P \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}' < v]]}\,\text{(Ex)}}{[[P \wedge 0 < \mathbf{E}' \wedge E]]\ C\ [[P \wedge 0 < \mathbf{E}' \wedge \mathsf{word}(E)]]}\,\text{(Conseq)}}{\{\{P \wedge 0 < \mathbf{E}' \wedge E\}\}\ C\ \{\{P \wedge 0 < \mathbf{E}' \wedge \mathsf{word}(E)\}\}}\,\text{(Total)}}{\{\{P \wedge 0 < \mathbf{E}' \wedge \mathsf{word}(E)\}\}\ \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}\ \{\{P \wedge 0 < \mathbf{E}' \wedge \mathsf{not}\ E\}\}}\,\text{(While)}}{\{\{P \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}'\}\}\ \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}\ \{\{P \wedge \mathsf{not}\ E\}\}}\,\text{(Conseq)}$$

- Assume: $\rho \in \text{Env}(\text{FLV}(P, \mathbf{E}')), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\text{F}}, \mathbf{T}, s, h$ such that
  $(\mathbf{s}, \mathbf{h} \models P[\rho] \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}'[\rho]) \wedge \mathbf{s} \approx_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\text{F}} \approx_{\mathbf{T}} h$.
- Now we show $\neg(\mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}, s, h$ diverges) by contradiction.
- Assume: $\{\, D_i, s_i, h_i \,\}_{i \in \mathbb{N}}$ such that
  ✓ $(D_0, s_0, h_0) = (\mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}, s, h) \wedge \forall i.\ D_i, s_i, h_i \rightsquigarrow D_{i+1}, s_{i+1}, h_{i+1}$.

- We show the following, which is a contradiction because $n_0 > n_1 > n_2 \ldots > 0$ is not possible.
- By induction on i, we find $\{ k_i, n_i, \mathbf{s}_i, \mathbf{h}_i, \mathbf{T}_i \}_{i \in \mathbb{N}}$ (with $n_i \in$ Words) such that
  ✓ $D_{k_i} = \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}$;
  ✓ $(\mathbf{s}_i, \mathbf{h}_i \models P[\rho] \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}'[\rho] = n_i) \wedge \mathbf{s}_i \approx_{\mathbf{T}_i} s_{k_i} \wedge \mathbf{h}_i \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}_i} h_{k_i}$;
  ✓ if $i > 0$ then $0 < n_i < n_{i-1}$.

(Base Case)

- From $(\mathbf{s}, \mathbf{h} \models 0 < \mathbf{E}'[\rho])$, we have
  ✓ $[\![\mathbf{E}'[\rho]]\!]_{\mathbf{s}} \in$ Words.
- Let $k_0 = 0$, $\mathbf{s}_0 = \mathbf{s}$, $\mathbf{h}_0 = \mathbf{h}$, $\mathbf{T}_0 = \mathbf{T}$ and $n_0 = [\![\mathbf{E}'[\rho]]\!]_{\mathbf{s}_0} \in$ Words.
- Then by assumption we have
  ✓ $D_{k_0} = \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}$,
  ✓ $(\mathbf{s}_0, \mathbf{h}_0 \models P[\rho] \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}'[\rho] = n_0) \wedge \mathbf{s}_0 \approx_{\mathbf{T}_0} s_{k_0} \wedge \mathbf{h}_0 \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}_0} h_{k_0}$.

(Inductive step)

- Assume:
  ✓ $D_{k_i} = \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}$,
  ✓ $(\mathbf{s}_i, \mathbf{h}_i \models P[\rho] \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}'[\rho] = n_i) \wedge \mathbf{s}_i \approx_{\mathbf{T}_i} s_{k_i} \wedge \mathbf{h}_i \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}_i} h_{k_i}$.
- As $(D_{k_i}, s_{k_i}, h_{k_i})$ diverges, we have
  ✓ $[\![E]\!]_{s_{k_i}} \in \text{Words}\backslash\{0\}$,
  ✓ $(D_{k_i+1}, s_{k_i+1}, h_{k_i+1}) = (C; \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}, s_{k_i}, h_{k_i})$.
- From $\mathbf{s}_i, \mathbf{h}_i \models \mathsf{word}(E)$, we have
  ✓ $[\![E]\!]_{\mathbf{s}_i} \in$ Words.
- By Lemma 2, we have $[\![E]\!]_{\mathbf{s}_i} = \mathrm{phyv}_{\mathbf{T}_i}([\![E]\!]_{\mathbf{s}_i}) = [\![E]\!]_{s_{k_i}} \in \text{Words}\backslash\{0\}$, and thus we have
  ✓ $\mathbf{s}_i, \mathbf{h}_i \models E$.
- By $[[P \wedge E \wedge 0 < \mathbf{E}' = v]]\ C\ [[P \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}' < v]]$, we have
  ✓ $\neg(C, s_{k_i+1}, h_{k_i+1}$ diverges).
- Thus, we have some j such that
  ✓ $D_{k_i+j+1} = (\mathsf{skip}; \mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od})$,
  ✓ $C, s_{k_i+1}, h_{k_i+1} \leadsto^j \mathsf{skip}, s_{k_i+j+1}, h_{k_i+j+1}$.
- Then, by $[[P \wedge E \wedge 0 < \mathbf{E}' = v]]\ C\ [[P \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}' < v]]$, we have $\mathbf{s}_{i+1}$, $\mathbf{h}_{i+1}$, $\mathbf{T}_{i+1}$ such that
  ✓ $(\mathbf{s}_{i+1}, \mathbf{h}_{i+1} \models P[\rho] \wedge \mathsf{word}(E) \wedge 0 < \mathbf{E}'[\rho] < n_i) \wedge \mathbf{s}_{i+1} \approx_{\mathbf{T}_{i+1}} s_{k_i+j+1} \wedge \mathbf{h}_{i+1} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}_{i+1}} h_{k_i+j+1}$.
- Also we have
  ✓ $(D_{k_i+j+2}, s_{k_i+j+2}, h_{k_i+j+2}) = (\mathsf{while}\ E\ \mathsf{do}\ C\ \mathsf{od}, s_{k_i+j+1}, h_{k_i+j+1})$.
- From $\mathbf{s}_{i+1}, \mathbf{h}_{i+1} \models 0 < \mathbf{E}'[\rho] < n_i$, we have
  ✓ $[\![\mathbf{E}'[\rho]]\!]_{\mathbf{s}_{i+1}} \in \text{Words} \wedge 0 < [\![\mathbf{E}'[\rho]]\!]_{\mathbf{s}_{i+1}} < n_i$.
- Let $k_{i+1} = k_i + j + 2$ and $n_{i+1} = [\![\mathbf{E}'[\rho]]\!]_{\mathbf{s}_{i+1}}$.

- Then, we have
  ✓ $D_{k_{i+1}} = \textsf{while}\ E\ \textsf{do}\ C\ \textsf{od}$,
  ✓ $(\mathbf{s}_{i+1}, \mathbf{h}_{i+1} \models P[\rho] \wedge \textsf{word}(E) \wedge 0 < \mathbf{E}'[\rho] = n_{i+1}) \wedge \mathbf{s}_{i+1} \approx_{\mathbf{T}_{i+1}} s_{k_{i+1}} \wedge \mathbf{h}_{i+1} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}_{i+1}} h_{k_{i+1}}$,
  ✓ $0 < n_{i+1} < n_i$.

□

5.4 Soundness of Assertion Entailments

5.4.1 NPtrSafe

Theorem 27 (NPtrSafe).

$$\textsf{nonptr}(\mathbf{E}) \models \textsf{safe}(\mathbf{E})$$

Proof. It holds vacuously by definition. □

5.4.2 BoolWord

Theorem 28 (BoolWord).

$$\mathbf{E} \models \textsf{word}(\mathbf{E})$$

Proof.

- For any $\rho \in \mathrm{Env}(\mathrm{FLV}(\mathbf{E}, \mathbf{E}')), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h$ such that $\mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h$, we need to show that $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{E}[\rho] \implies \mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \textsf{word}(\mathbf{E}[\rho])$.
- From $\mathbf{s}, \mathbf{h} \models_{\mathbf{T}} \mathbf{E}[\rho]$, we have $[\![\mathbf{E}[\rho]]\!]_{\mathbf{s}} \in \mathrm{Words} \backslash \{0\} \subseteq \mathrm{Words}$.
- Thus $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \textsf{word}(\mathbf{E}[\rho])$ holds.

□

5.4.3 PointstoNZero

Theorem 29 (PointstoNZero).

$$\mathbf{E} \hookrightarrow \mathbf{E}' \models \mathbf{E} \neq 0$$

Proof.

- For any $\rho \in \mathrm{Env}(\mathrm{FLV}(\mathbf{E}, \mathbf{E}')), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h$ such that $\mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h$, we need to show that $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{E}[\rho] \hookrightarrow \mathbf{E}'[\rho] \implies \mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \textsf{word}(\mathbf{E}[\rho] = 0)$.
- From $\mathbf{s}, \mathbf{h} \models_{\mathbf{T}} \mathbf{E}[\rho] \hookrightarrow \mathbf{E}'[\rho]$, we have $[\![\mathbf{E}[\rho]]\!]_{\mathbf{s}} = \boldsymbol{\ell} \widehat{+} 4i$ and $[\![\mathbf{E}'[\rho]]\!]_{\mathbf{s}} = \mathbf{h}(\boldsymbol{\ell})(i)$ for some $\boldsymbol{\ell} \in \mathrm{dom}(\mathbf{T})$ and $i \in \mathbb{Z}$.
- As $\mathbf{h}(\boldsymbol{\ell})(i) \neq \mathrm{undef}$, from $\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} : \mathbf{T}$ we have $0 \leq i < n$ for $(p, n) = \mathbf{T}(\boldsymbol{\ell})$.
- Thus $[\![\mathbf{E}[\rho] \neq 0]\!]_{\mathbf{s}} = [\![\textsf{not}\ (\boldsymbol{\ell} \widehat{+} 4i = 0)]\!]_{\mathbf{s}} = 1$ as $i \geq 0$.
- Thus $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{E}[\rho] \neq 0$ holds.

□

5.4.4 ExpSafe

Theorem 30 (ExpSafe)**.**

$$\mathsf{defined}(E) \models \mathsf{offsafe}(E)$$

Proof.

- For any $\mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h$ such that $\mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h$, we need to show that $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathsf{defined}(E) \implies \mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathsf{offsafe}(E)$.
- From $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathsf{defined}(E)$, we have two cases.
- When $[\![E]\!]_{\mathbf{s}} = w \in \mathrm{Words}$:
  By definition $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathsf{offsafe}(E)$ holds.
- When $[\![E]\!]_{\mathbf{s}} = \boldsymbol{\ell} \widehat{+} i$ for some $\boldsymbol{\ell} \in \mathrm{Locs}$ and $i \in \mathbb{Z}$:
  By Corollary 3, we have $\boldsymbol{\ell} \in \mathrm{dom}(\mathbf{T})$ and thus $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathsf{offsafe}(E)$ holds.

□

5.4.5 HeapSafe

Theorem 31 (HeapSafe)**.**

$$\mathbf{E} \hookrightarrow \mathbf{E}' \wedge \mathsf{offsafe}(\mathbf{E}) \models \mathsf{safe}(\mathbf{E}')$$

Proof.

- For any $\rho \in \mathrm{Env}(\mathrm{FLV}(\mathbf{E}, \mathbf{E}')), \mathbf{s}, \mathbf{h}, \mathbf{h}_{\mathrm{F}}, \mathbf{T}, s, h$ such that $\mathbf{s} \sim_{\mathbf{T}} s \wedge \mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} \approx_{\mathbf{T}} h$, we need to show that $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{E} \hookrightarrow \mathbf{E}' \wedge \mathsf{offsafe}(\mathbf{E}) \implies \mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathsf{safe}(\mathbf{E}'[\rho])$.
- From $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathbf{E} \hookrightarrow \mathbf{E}' \wedge \mathsf{offsafe}(\mathbf{E})$, we have $[\![\mathbf{E}[\rho]]\!]_{\mathbf{s}} = \boldsymbol{\ell} \widehat{+} 4i$ and $[\![\mathbf{E}'[\rho]]\!]_{\mathbf{s}} = \mathbf{h}(\boldsymbol{\ell})(i)$ for some $\boldsymbol{\ell} \in \mathrm{dom}(\mathbf{T})$ and $i \in \mathbb{Z}$.
- As $\mathbf{h}(\boldsymbol{\ell})(i) \neq \mathrm{undef}$, from $\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} : \mathbf{T}$ we have $0 \leq i < n$ for $(p, n) = \mathbf{T}(\boldsymbol{\ell})$.
- From $\mathbf{h} \uplus \mathbf{h}_{\mathrm{F}} :: \mathbf{T}$, we have $[\![\mathbf{E}'[\rho]]\!]_{\mathbf{s}} = \mathbf{h}(\boldsymbol{\ell})(i) \in \mathrm{Safe}(\mathrm{dom}(\mathbf{T}))$.
- Thus $\mathbf{s}, \mathbf{h} \models_{\mathrm{dom}(\mathbf{T})} \mathsf{safe}(\mathbf{E}'[\rho])$ holds.

□

5.4.6 ExpHeapSafe

Corollary 13 (ExpHeapSafe)**.**

$$E \hookrightarrow \mathbf{E}' \models \mathsf{safe}(\mathbf{E}')$$

Proof. It follows as a corollary from (ExpSafe) and (HeapSafe). □

5.4.7 SafeEq

Theorem 32 (SafeEq)**.**

$$\mathsf{safe}(\mathbf{E}, \mathbf{E}') \models \mathsf{defined}(\mathbf{E} = \mathbf{E}')$$

Proof. It is obvious by definition. □

5.5 Soundness of Derived Rules

5.5.1 Ex'

Theorem 33 (Soundness: Ex')**.**
For $(\langle,\rangle, \mathcal{P}, \mathcal{Q}) \in \{\, (\{,\}, \mathbf{P}, \mathbf{Q}), ([,], \mathbf{P}, \mathbf{Q}), (\{\{,\}\}, P, Q), ([[,]], P, Q) \,\}$,

$$\frac{\langle \mathcal{P} \rangle\ C\ \langle \mathcal{Q} \rangle \qquad v \notin \mathrm{FLV}(\mathcal{Q})}{\langle \exists v.\, \mathcal{P} \rangle\ C\ \langle \mathcal{Q} \rangle}$$

Proof.

$$\frac{\dfrac{\langle \mathcal{P} \rangle\ C\ \langle \mathcal{Q} \rangle}{\langle \exists v.\, \mathcal{P} \rangle\ C\ \langle \exists v.\, \mathcal{Q} \rangle}\,(\mathrm{Ex}) \qquad v \notin \mathrm{FLV}(\mathcal{Q})}{\langle \exists v.\, \mathcal{P} \rangle\ C\ \langle \mathcal{Q} \rangle}\,(\mathrm{Conseq})$$

$\square$

5.5.2 Disj

Theorem 34 (Soundness: Disj)**.**
For $(\langle,\rangle, \mathcal{P}_1, \mathcal{P}_2, \mathcal{Q}) \in \{\, (\{,\}, \mathbf{P}_1, \mathbf{P}_2, \mathbf{Q}), ([,], \mathbf{P}_1, \mathbf{P}_2, \mathbf{Q}), (\{\{,\}\}, P_1, P_2, Q), ([[,]], P_1, P_2, Q) \,\}$,

$$\frac{\langle \mathcal{P}_1 \rangle\ C\ \langle \mathcal{Q} \rangle \qquad \langle \mathcal{P}_2 \rangle\ C\ \langle \mathcal{Q} \rangle}{\langle \mathcal{P}_1 \vee \mathcal{P}_2 \rangle\ C\ \langle \mathcal{Q} \rangle}$$

Proof. Choose a fresh variable u such that $u \notin \mathrm{FLV}(\mathcal{P}_1, \mathcal{P}_2, \mathcal{Q})$.

$$\cfrac{\cfrac{\cfrac{\cfrac{\langle \mathcal{P}_1 \rangle\ C\ \langle \mathcal{Q} \rangle \qquad \langle \mathcal{P}_2 \rangle\ C\ \langle \mathcal{Q} \rangle}{\forall \mathbf{v} \in \mathrm{LogVals}.\ \langle (\mathbf{v} = 1 \wedge \mathcal{P}_1) \vee (\mathbf{v} = 2 \wedge \mathcal{P}_2) \rangle\ C\ \langle \mathcal{Q} \rangle}}{\langle (u = 1 \wedge \mathcal{P}_1) \vee (u = 2 \wedge \mathcal{P}_2) \rangle\ C\ \langle \mathcal{Q} \rangle}\,(\mathrm{Gen})}{\langle \exists u.\, (u = 1 \wedge \mathcal{P}_1) \vee (u = 2 \wedge \mathcal{P}_2) \rangle\ C\ \langle \mathcal{Q} \rangle}\,(\mathrm{Ex}')}{\langle \mathcal{P}_1 \vee \mathcal{P}_2 \rangle\ C\ \langle \mathcal{Q} \rangle}\,(\mathrm{Conseq})$$

$\square$

5.5.3 Inst

Lemma 14.
For $(\langle,\rangle, \mathcal{P}, \mathcal{Q}) \in \{\, (\{,\}, \mathbf{P}, \mathbf{Q}), ([,], \mathbf{P}, \mathbf{Q}), (\{\{,\}\}, P, Q), ([[,]], P, Q) \,\}$,

$$\frac{\langle \mathcal{P} \rangle\ C\ \langle \mathcal{Q} \rangle \qquad \mathrm{FPV}(\mathbf{E}) \cap \mathrm{Mod}(C) = \emptyset \qquad v \notin \mathrm{FLV}(\mathbf{E})}{\langle \mathcal{P}[\mathbf{E}/v] \wedge \mathsf{defined}(\mathbf{E}) \rangle\ C\ \langle \mathcal{Q}[\mathbf{E}/v] \rangle}$$

Proof. Assume: $\langle \mathcal{P} \rangle\ C\ \langle \mathcal{Q} \rangle \wedge \mathrm{FPV}(\mathbf{E}) \cap \mathrm{Mod}(C) = \emptyset \wedge v \notin \mathrm{FLV}(\mathbf{E})$.

$$\begin{array}{ll}
\langle \mathcal{P}[\mathbf{E}/v] \wedge \mathsf{defined}(\mathbf{E}) \rangle & \\
\langle \exists v.\, \mathcal{P}[\mathbf{E}/v] * v = \mathbf{E} \rangle & \\
\langle \mathcal{P}[\mathbf{E}/v] * v = \mathbf{E} \rangle & (\mathrm{Ex}') \\
\langle \mathcal{P} * v = \mathbf{E} \rangle &
\end{array}$$

$$C$$

$$\langle \mathcal{Q} * v = \mathbf{E} \rangle$$

$$\langle \mathcal{Q}[\mathbf{E}/v] * v = \mathbf{E} \rangle$$

$$\langle \mathcal{Q}[\mathbf{E}/v] \rangle$$

□

Theorem 35 (Soundness: Inst)**.**
For $(\langle,\rangle, \mathcal{P}, \mathcal{Q}) \in \{\, (\{,\}, \mathbf{P}, \mathbf{Q}), ([,], \mathbf{P}, \mathbf{Q}), (\{\{,\}\}, P, Q), ([[,]], P, Q) \,\}$,

$$\frac{\langle \mathcal{P} \rangle\ C\ \langle \mathcal{Q} \rangle \qquad \mathrm{FPV}(\mathbf{E}) \cap \mathrm{Mod}(C) = \emptyset}{\langle \mathcal{P}[\mathbf{E}/v] \wedge \mathsf{defined}(\mathbf{E}) \rangle\ C\ \langle \mathcal{Q}[\mathbf{E}/v] \rangle}$$

Proof. Choose a fresh variable u such that $u \notin \mathrm{FLV}(\mathcal{P}, \mathcal{Q}, \mathbf{E}, v)$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\langle \mathcal{P} \rangle\ C\ \langle \mathcal{Q} \rangle}{\langle \mathcal{P}[u/v] \wedge \mathsf{defined}(u) \rangle\ C\ \langle \mathcal{Q}[u/v] \rangle}\,(\text{Lemma 14})}{\langle \mathcal{P}[u/v] \rangle\ C\ \langle \mathcal{Q}[u/v] \rangle}\,(\text{Conseq})}{\langle \mathcal{P}[u/v][\mathbf{E}/u] \wedge \mathsf{defined}(\mathbf{E}) \rangle\ C\ \langle \mathcal{Q}[u/v][\mathbf{E}/u] \rangle}\,(\text{Lemma 14})}{\langle \mathcal{P}[\mathbf{E}/v] \wedge \mathsf{defined}(\mathbf{E}) \rangle\ C\ \langle \mathcal{Q}[\mathbf{E}/v] \rangle}\,(\text{Conseq})$$

□

5.5.4 Assign'

Theorem 36 (Soundness: Assign')**.**

$$\frac{}{[\mathbf{P}[E/\mathtt{x}] \wedge \mathsf{defined}(E)]\ \mathtt{x} := E\ [\mathbf{P}]}$$

Proof. Choose a fresh variable v such that $v \notin \mathrm{FLV}(\mathbf{P})$.

$$\langle \mathbf{P}[E/\mathtt{x}] \wedge \mathsf{defined}(E) \rangle$$

$$\langle \exists v.\, \mathbf{P}[E/\mathtt{x}] \wedge \mathsf{defined}(E) \wedge \mathtt{x} = v \rangle$$

$$\langle \mathbf{P}[E/\mathtt{x}] \wedge \mathsf{defined}(E) \wedge \mathtt{x} = v \rangle \qquad (\mathrm{Ex}')$$

$$\langle \mathbf{P}[E[v/\mathtt{x}]/\mathtt{x}] * (\mathsf{defined}(E) \wedge \mathtt{x} = v) \rangle$$

$$\mathtt{x} := E$$

$$\langle \mathbf{P}[E[v/\mathtt{x}]/\mathtt{x}] * (\mathtt{x} = E[v/\mathtt{x}]) \rangle \qquad (\text{Assign})$$

$$\langle \mathbf{P} \wedge \mathtt{x} = E[v/\mathtt{x}] \rangle$$

$$\langle \mathbf{P} \rangle$$

□

5.5.5 Read' and Read"

Theorem 37 (Soundness: Read").

$$\frac{\mathtt{x} \notin \mathrm{FPV}(\mathbf{E}') \cup \mathrm{FPV}(\mathbf{E}'')}{[\mathtt{x} = \mathbf{E}' \wedge E \hookrightarrow \mathbf{E}'']\ \mathtt{x} := [E]\ [\mathtt{x} = \mathbf{E}'' \wedge E[\mathbf{E}'/\mathtt{x}] \hookrightarrow \mathbf{E}'']}$$

Proof. Assume: $\mathtt{x} \notin \mathrm{FPV}(\mathbf{E}') \cup \mathrm{FPV}(\mathbf{E}'')$.
Choose fresh variables u, v such that $u, v \notin \mathrm{FLV}(\mathbf{E}', \mathbf{E}'') \wedge u \neq v$.

$$\dfrac{\dfrac{\dfrac{}{[\mathtt{x} = u \wedge E \hookrightarrow v]\ \mathtt{x} := [E]\ [\mathtt{x} = v \wedge E[u/\mathtt{x}] \hookrightarrow v]}\ (\text{Read})}{[\mathtt{x} = \mathbf{E}' \wedge E \hookrightarrow \mathbf{E}'' \wedge \mathsf{defined}(\mathbf{E}') \wedge \mathsf{defined}(\mathbf{E}'')]\ \mathtt{x} := [E]\ [\mathtt{x} = \mathbf{E}'' \wedge E[\mathbf{E}'/\mathtt{x}] \hookrightarrow \mathbf{E}'']}\ (\text{Inst})}{[\mathtt{x} = \mathbf{E}' \wedge E \hookrightarrow \mathbf{E}'']\ \mathtt{x} := [E]\ [\mathtt{x} = \mathbf{E}'' \wedge E[\mathbf{E}'/\mathtt{x}] \hookrightarrow \mathbf{E}'']}\ (\text{Conseq})$$

□

Theorem 38 (Soundness: Read').

$$\frac{\mathtt{x} \notin \mathrm{FPV}(E) \cup \mathrm{FPV}(\mathbf{E}')}{[E \hookrightarrow \mathbf{E}']\ \mathtt{x} := [E]\ [\mathtt{x} = \mathbf{E}' \wedge E \hookrightarrow \mathbf{E}']}$$

Proof. Assume: $\mathtt{x} \notin \mathrm{FPV}(E) \cup \mathrm{FPV}(\mathbf{E}')$.
Choose a fresh name v such that $v \notin \mathrm{FLV}(\mathbf{E}')$.

$$\dfrac{\dfrac{\dfrac{}{[\mathtt{x} = v \wedge E \hookrightarrow \mathbf{E}']\ \mathtt{x} := [E]\ [\mathtt{x} = \mathbf{E}' \wedge E \hookrightarrow \mathbf{E}']}\ (\text{Read}'')}{[\exists v.\, \mathtt{x} = v \wedge E \hookrightarrow \mathbf{E}']\ \mathtt{x} := [E]\ [\mathtt{x} = \mathbf{E}' \wedge E \hookrightarrow \mathbf{E}']}\ (\text{Ex}')}{[E \hookrightarrow \mathbf{E}']\ \mathtt{x} := [E]\ [\mathtt{x} = \mathbf{E}' \wedge E \hookrightarrow \mathbf{E}']}\ (\text{Conseq})$$

□

5.5.6 ASSIGN and ASSIGN'

Theorem 39 (Soundness: ASSIGN).

$$\frac{}{[[\mathbf{P}[\mathtt{y}/\mathtt{x}]]]\ \mathtt{x} := \mathtt{y}\ [[\mathbf{P}]]}$$

Proof.

$$\begin{array}{ll}
[[\mathbf{P}[\mathtt{y}/\mathtt{x}]]] & \\
[\mathbf{P}[\mathtt{y}/\mathtt{x}] \wedge \mathsf{safe}(\mathtt{y})] & (\text{Incl}) \\
[\mathbf{P}[\mathtt{y}/\mathtt{x}] \wedge \mathsf{safe}(\mathtt{y}) \wedge \mathsf{defined}(\mathtt{y})] & \\
\mathtt{x} := \mathtt{y} & \\
[\mathbf{P} \wedge \mathsf{safe}(\mathtt{x})] & (\text{Assign}') \\
[[\mathbf{P}]] & (\text{Incl})
\end{array}$$

□

Theorem 40 (Soundness: ASSIGN').

$$\frac{}{[[\mathbf{P}[E/\mathtt{x}] \wedge \mathsf{nonptr}(E)]]\ \mathtt{x} := E\ [[\mathbf{P}]]}$$

Proof.

$$\begin{array}{lr}
[[\mathbf{P}[E/\mathtt{x}] \wedge \mathsf{nonptr}(E)]] & \\
[\mathbf{P}[E/\mathtt{x}] \wedge \mathsf{nonptr}(E)] & \text{(Incl)} \\
[\mathbf{P}[E/\mathtt{x}] \wedge \mathsf{nonptr}(E) \wedge \mathsf{defined}(E)] & \\
\mathtt{x} := E & \\
[\mathbf{P} \wedge \mathsf{nonptr}(\mathtt{x})] & (\text{Assign}') \\
[\mathbf{P} \wedge \mathsf{safe}(\mathtt{x})] & \\
[[\mathbf{P}]] & \text{(Incl)}
\end{array}$$

$\square$

5.5.7 READ and READ'

Theorem 41 (Soundness: READ).

$$\frac{\mathtt{x} \notin \mathrm{FPV}(E) \cup \mathrm{FPV}(\mathbf{E}')}{[[E \hookrightarrow \mathbf{E}']]\ \mathtt{x} := [E]\ [[\mathtt{x} = \mathbf{E}' \wedge E \hookrightarrow \mathbf{E}']]}$$

Proof. Asuume: $\mathtt{x} \notin \mathrm{FPV}(E) \cup \mathrm{FPV}(\mathbf{E}')$.

$$\begin{array}{lr}
[[E \hookrightarrow \mathbf{E}']] & \\
[E \hookrightarrow \mathbf{E}'] & \text{(Incl)} \\
\mathtt{x} := [E] & \\
[\mathtt{x} = \mathbf{E}' \wedge E \hookrightarrow \mathbf{E}'] & (\text{Read}') \\
[\mathtt{x} = \mathbf{E}' \wedge E \hookrightarrow \mathbf{E}' \wedge \mathsf{safe}(\mathtt{x})] & \\
[[\mathtt{x} = \mathbf{E}' \wedge E \hookrightarrow \mathbf{E}']] & \text{(Incl)}
\end{array}$$

$\square$

Theorem 42 (Soundness: READ').

$$\frac{\mathtt{x} \notin \mathrm{FPV}(\mathbf{E}') \cup \mathrm{FPV}(\mathbf{E}'')}{[[\mathtt{x} = \mathbf{E}' \wedge E \hookrightarrow \mathbf{E}'']]\ \mathtt{x} := [E]\ [[\mathtt{x} = \mathbf{E}'' \wedge E[\mathbf{E}'/\mathtt{x}] \hookrightarrow \mathbf{E}'']]}$$

Proof. Asuume: $\mathtt{x} \notin \mathrm{FPV}(\mathbf{E}') \cup \mathrm{FPV}(\mathbf{E}'')$.

$$\begin{array}{lr}
[[\mathtt{x} = \mathbf{E}' \wedge E \hookrightarrow \mathbf{E}'']] & \\
[\mathtt{x} = \mathbf{E}' \wedge E \hookrightarrow \mathbf{E}''] & \text{(Incl)} \\
[\mathtt{x} = \mathbf{E}' \wedge E \hookrightarrow \mathbf{E}'' * \mathsf{safe}(\mathbf{E}'')] & \\
\mathtt{x} := [E] &
\end{array}$$

$$
\begin{array}{ll}
[\mathtt{x} = \mathbf{E}'' \wedge E[\mathbf{E}'/\mathtt{x}] \hookrightarrow \mathbf{E}'' * \mathsf{safe}(\mathbf{E}'')] & (\text{Read}'') \\
[\mathtt{x} = \mathbf{E}'' \wedge E[\mathbf{E}'/\mathtt{x}] \hookrightarrow \mathbf{E}'' \wedge \mathsf{safe}(\mathtt{x})] & \\
[[\mathtt{x} = \mathbf{E}'' \wedge E[\mathbf{E}'/\mathtt{x}] \hookrightarrow \mathbf{E}'']] & (\text{Incl})
\end{array}
$$

□

5.5.8 WRITE and WRITE'

Theorem 43 (Soundness: WRITE)**.**

$$\frac{}{[[E \hookrightarrow -]]\ [E] := \mathtt{x}\ [[E \hookrightarrow \mathtt{x}]]}$$

Proof.

$$
\begin{array}{ll}
[[E \hookrightarrow -]] & \\
[E \hookrightarrow - \wedge \mathsf{safe}(\mathtt{x})] & (\text{Incl}) \\
[E] := \mathtt{x} & \\
[E \hookrightarrow \mathtt{x}] & (\text{Write}) \\
[[E \hookrightarrow \mathtt{x}]] & (\text{Incl})
\end{array}
$$

□

Theorem 44 (Soundness: WRITE')**.**

$$\frac{}{[[E \hookrightarrow - \wedge \mathsf{nonptr}(E')]]\ [E] := E'\ [[E \hookrightarrow E']]}$$

Proof.

$$
\begin{array}{ll}
[[E \hookrightarrow - \wedge \mathsf{nonptr}(E')]] & \\
[E \hookrightarrow - \wedge \mathsf{nonptr}(E')] & (\text{Incl}) \\
[E \hookrightarrow - \wedge \mathsf{safe}(E')] & \\
[E] := E' & \\
[E \hookrightarrow E'] & (\text{Write}) \\
[[E \hookrightarrow E']] & (\text{Incl})
\end{array}
$$

□

5.5.9 ALLOC

Theorem 45 (Soundness: ALLOC)**.**

$$\frac{n \geq 0}{[[E = 2n+1]]\ \mathtt{x} := \mathsf{ALLOC}(E)\ [[\mathtt{x} \hookrightarrow_n 0, \ldots, 0]]}$$

Proof. Assume: $n \geq 0$.

$$
\begin{array}{ll}
[[E = 2n + 1]] & \\
[[E = 2n + 1 \wedge \mathsf{nonptr}(E)]] & \\
\mathtt{x} := E; & \\
[[\mathtt{x} = 2n + 1]] & (\text{ASSIGN}') \\
\mathsf{alloc}\ \mathtt{x} & \\
[[\mathtt{x} \hookrightarrow_n 0, \ldots, 0]] & (\text{Alloc})
\end{array}
$$

□