A Kripke Logical Relation Between ML and Assembly

Technical Appendix
DRAFT

Chung-Kil Hur
gil@mpi-sws.org

Derek Dreyer
dreyer@mpi-sws.org

Original Draft: July 2010
Revised: November 2010

Contents

1 Languages

1.1 HIGH

1.1.1 Syntax & Dynamic Semantics

$$\begin{array}{lll}
\tau \in \text{Type} & ::= & \alpha \mid b \mid \tau_1 \times \tau_2 \mid \tau_1 \to \tau_2 \mid \forall\alpha.\,\tau \mid \exists\alpha.\,\tau \mid \mu\alpha.\,\tau \mid \mathsf{ref}\,\tau \\
& & \text{where } \alpha \in \text{TypeVar} \\
\\
e \in \text{HExp} & ::= & x \mid \ell \mid \langle e_1, e_2\rangle \mid e.1 \mid e.2 \mid \\
& & \lambda x{:}\tau.\,e \mid e_1\ e_2 \mid \Lambda\alpha.e \mid e\ \tau \mid \mathsf{pack}\ \langle \tau_1, e\rangle\ \mathsf{as}\ \tau_2 \mid \mathsf{unpack}\ e_1\ \mathsf{as}\ \langle \alpha, x\rangle\ \mathsf{in}\ e_2 \mid \\
& & \mathsf{roll}_\tau\ e \mid \mathsf{unroll}\ e \mid \mathsf{ref}\ e \mid e_1 := e_2 \mid !e \mid e_1 == e_2 \mid \ldots \\
& & \text{where } x \in \text{Var and } \ell \in \text{HLoc} \\
\\
v \in \text{HVal} & ::= & x \mid \ell \mid \langle v_1, v_2\rangle \mid \lambda x{:}\tau.\,e \mid \Lambda\alpha.e \mid \mathsf{pack}\ \langle \tau_1, v\rangle\ \mathsf{as}\ \tau_2 \mid \mathsf{roll}_\tau\ v \mid \ldots \\
\\
K \in \text{HCont} & ::= & \bullet \mid \langle K, e_2\rangle \mid \langle v_1, K\rangle \mid K.1 \mid K.2 \mid \\
& & K\ e_2 \mid v_1\ K \mid K\ \tau \mid \mathsf{pack}\ \langle \tau_1, K\rangle\ \mathsf{as}\ \tau_2 \mid \mathsf{unpack}\ K\ \mathsf{as}\ \langle \alpha, x\rangle\ \mathsf{in}\ e_2 \mid \\
& & \mathsf{roll}_\tau\ K \mid \mathsf{unroll}\ K \mid \mathsf{ref}\ K \mid K := e_2 \mid v_1 := K \mid !K \mid K == e_2 \mid v_1 == K \mid \ldots \\
\\
\text{HCVal} & \stackrel{\text{def}}{=} & \{\, v \in \text{HVal} \mid \text{ftv}(v) = \emptyset \wedge \text{fv}(v) = \emptyset \,\} \\
\text{HHeap} & \stackrel{\text{def}}{=} & \{\, h \in \text{HLoc} \rightharpoonup_{\text{fin}} \text{HCVal} \,\} \\
\\
\text{freshloc} & \in & \{\, f \in \mathbb{P}_{\text{fin}}(\text{HLoc}) \to \text{HLoc} \mid \forall S.\ f(S) \notin S \,\}
\end{array}$$

$\boxed{(h, e) \hookrightarrow (h', e')}$

$$\begin{array}{lll}
\langle h; K[\langle v_1, v_2\rangle.1]\rangle & \hookrightarrow \langle h; K[v_1]\rangle & \\
\langle h; K[\langle v_1, v_2\rangle.2]\rangle & \hookrightarrow \langle h; K[v_2]\rangle & \\
\langle h; K[(\lambda x{:}\tau.\,e)\ v]\rangle & \hookrightarrow \langle h; K[e[v/x]]\rangle & \\
\langle h; K[(\Lambda\alpha.e)\ \tau]\rangle & \hookrightarrow \langle h; K[e[\tau/\alpha]]\rangle & \\
\langle h; K[\mathsf{unpack}\ (\mathsf{pack}\ \langle \tau_1, v\rangle\ \mathsf{as}\ \tau_2)\ \mathsf{as}\ \langle \alpha, x\rangle\ \mathsf{in}\ e]\rangle & \hookrightarrow \langle h; K[e[\tau_1/\alpha][v/x]]\rangle & \\
\langle h; K[\mathsf{unroll}\ (\mathsf{roll}_\tau\ v)]\rangle & \hookrightarrow \langle h; K[v]\rangle & \\
\langle h; K[\mathsf{ref}\ v]\rangle & \hookrightarrow \langle h \uplus \{\ell{\mapsto}v\}; K[\ell]\rangle & (\ell = \text{freshloc}(\text{dom}(h))) \\
\langle h; K[\ell := v]\rangle & \hookrightarrow \langle h[\ell{\mapsto}v]; K[\langle\rangle]\rangle & (\ell \in \text{dom}(h)) \\
\langle h; K[!\ell]\rangle & \hookrightarrow \langle h; K[v]\rangle & (h(\ell) = v) \\
\langle h; K[\ell_1 == \ell_2]\rangle & \hookrightarrow \langle h; K[\mathsf{tt}]\rangle & (\ell_1 = \ell_2) \\
\langle h; K[\ell_1 == \ell_2]\rangle & \hookrightarrow \langle h; K[\mathsf{ff}]\rangle & (\ell_1 \neq \ell_2)
\end{array}$$

1.1.2 Static Semantics

$$\begin{array}{llll}
\text{Heap typings} & \Sigma & ::= & \cdot \mid \Sigma, \ell{:}\tau \quad \text{where } \text{ftv}(\tau) = \emptyset \\
\text{Type environments} & \Delta & ::= & \cdot \mid \Delta, \alpha \\
\text{Term environments} & \Gamma & ::= & \cdot \mid \Gamma, x{:}\tau
\end{array}$$

$\boxed{\Delta \vdash \tau, \Delta \vdash \Gamma}$

$$\frac{\mathrm{ftv}(\tau) \subseteq \Delta}{\Delta \vdash \tau} \qquad \frac{\forall x{:}\tau \in \Gamma.\ \Delta \vdash \tau}{\Delta \vdash \Gamma}$$

$\boxed{\Sigma; \Delta; \Gamma \vdash e : \tau}$

$$\frac{x{:}\tau \in \Gamma}{\Sigma; \Delta; \Gamma \vdash x : \tau} \qquad \frac{\ell{:}\tau \in \Sigma}{\Sigma; \Delta; \Gamma \vdash \ell : \mathsf{ref}\ \tau}$$

$$\frac{\Sigma; \Delta; \Gamma \vdash e_1 : \tau_1 \quad \Sigma; \Delta; \Gamma \vdash e_2 : \tau_2}{\Sigma; \Delta; \Gamma \vdash \langle e_1, e_2 \rangle : \tau_1 \times \tau_2} \qquad \frac{\Sigma; \Delta; \Gamma \vdash e : \tau_1 \times \tau_2}{\Sigma; \Delta; \Gamma \vdash e.1 : \tau_1} \qquad \frac{\Sigma; \Delta; \Gamma \vdash e : \tau_1 \times \tau_2}{\Sigma; \Delta; \Gamma \vdash e.2 : \tau_2}$$

$$\frac{\Sigma; \Delta; \Gamma, x{:}\tau_1 \vdash e : \tau_2}{\Sigma; \Delta; \Gamma \vdash \lambda x{:}\tau_1.\, e : \tau_1 \to \tau_2} \qquad \frac{\Sigma; \Delta; \Gamma \vdash e_1 : \tau_1 \to \tau_2 \quad \Sigma; \Delta; \Gamma \vdash e_2 : \tau_1}{\Sigma; \Delta; \Gamma \vdash e_1\ e_2 : \tau_2}$$

$$\frac{\Sigma; \Delta, \alpha; \Gamma \vdash e : \tau \quad \Delta \vdash \Gamma}{\Sigma; \Delta; \Gamma \vdash \Lambda\alpha.e : \forall\alpha.\, \tau} \qquad \frac{\Sigma; \Delta; \Gamma \vdash e : \forall\alpha.\, \tau_1}{\Sigma; \Delta; \Gamma \vdash e\ \tau_2 : \tau_1[\tau_2/\alpha]}$$

$$\frac{\Sigma; \Delta; \Gamma \vdash e : \tau_2[\tau_1/\alpha]}{\Sigma; \Delta; \Gamma \vdash \mathsf{pack}\ \langle \tau_1, e \rangle\ \mathsf{as}\ \exists\alpha.\, \tau_2 : \exists\alpha.\, \tau_2} \qquad \frac{\Sigma; \Delta; \Gamma \vdash e_1 : \exists\alpha.\, \tau_1 \quad \Sigma; \Delta, \alpha; \Gamma, x{:}\tau_1 \vdash e_2 : \tau_2 \quad \Delta \vdash \Gamma \quad \Delta \vdash \tau_2}{\Sigma; \Delta; \Gamma \vdash \mathsf{unpack}\ e_1\ \mathsf{as}\ \langle \alpha, x \rangle\ \mathsf{in}\ e_2 : \tau_2}$$

$$\frac{\Sigma; \Delta; \Gamma \vdash e : \tau[\mu\alpha.\, \tau/\alpha]}{\Sigma; \Delta; \Gamma \vdash \mathsf{roll}_{\mu\alpha.\, \tau}\ e : \mu\alpha.\, \tau} \qquad \frac{\Sigma; \Delta; \Gamma \vdash e : \mu\alpha.\, \tau}{\Sigma; \Delta; \Gamma \vdash \mathsf{unroll}\ e : \tau[\mu\alpha.\, \tau/\alpha]}$$

$$\frac{\Sigma; \Delta; \Gamma \vdash e : \tau}{\Sigma; \Delta; \Gamma \vdash \mathsf{ref}\ e : \mathsf{ref}\ \tau} \qquad \frac{\Sigma; \Delta; \Gamma \vdash e_1 : \mathsf{ref}\ \tau \quad \Sigma; \Delta; \Gamma \vdash e_2 : \tau}{\Sigma; \Delta; \Gamma \vdash e_1 := e_2 : \mathsf{unit}}$$

$$\frac{\Sigma; \Delta; \Gamma \vdash e : \mathsf{ref}\ \tau}{\Sigma; \Delta; \Gamma \vdash !e : \tau} \qquad \frac{\Sigma; \Delta; \Gamma \vdash e_1 : \mathsf{ref}\ \tau \quad \Sigma; \Delta; \Gamma \vdash e_2 : \mathsf{ref}\ \tau}{\Sigma; \Delta; \Gamma \vdash e_1 == e_2 : \mathsf{bool}}$$

$\ldots$

$\boxed{\Delta \vdash \delta : \Delta'}$

$$\frac{}{\Delta \vdash \emptyset : \cdot} \qquad \frac{\Delta \vdash \delta : \Delta' \quad \Delta \vdash \tau}{\Delta \vdash \delta, \alpha{\mapsto}\tau : \Delta', \alpha}$$

$\boxed{\Sigma; \Delta; \Gamma \vdash \gamma : \Gamma'}$

$$\frac{}{\Sigma; \Delta; \Gamma \vdash \emptyset : \cdot} \qquad \frac{\Sigma; \Delta; \Gamma \vdash \gamma : \Gamma' \quad \Sigma; \Delta; \Gamma \vdash v : \tau}{\Sigma; \Delta; \Gamma \vdash \gamma, x{\mapsto}v : \Gamma', x{:}\tau}$$

$\boxed{\vdash h : \Sigma}$

$$\frac{\forall \ell{:}\tau \in \Sigma.\ \Sigma; \cdot; \cdot \vdash h(\ell) : \tau}{\vdash h : \Sigma}$$

1.2 LOW

1.2.1 Syntax & Dynamic Semantics

$$
\begin{array}{lll}
\text{PConf} & \stackrel{\text{def}}{=} & \{\,(\Phi, \text{pc}) \in \text{PMem} \times \text{PAddr}\,\} \\
\text{PMem} & \stackrel{\text{def}}{=} & \{\,\Phi = (\text{code}, \text{reg}, \text{stk}, \text{hp}) \in \text{PCode} \times \text{PRegFile} \times \text{PStack} \times \text{PHeap}\,\} \\
\text{PCode} & \stackrel{\text{def}}{=} & \text{PAddr} \to \text{Instruction} \\
\text{PRegFile} & \stackrel{\text{def}}{=} & \text{Register} \to \text{PWord} \\
\text{PStack} & \stackrel{\text{def}}{=} & \text{PAddr} \to \text{PWord} \\
\text{PHeap} & \stackrel{\text{def}}{=} & \text{PAddr} \to \text{PWord} \\
\text{PAddr} & \stackrel{\text{def}}{=} & \{\,a \in \mathbb{N}\,\} \\
\text{PWord} & \stackrel{\text{def}}{=} & \{\,w \in \{\,0,1\,\} \times \mathbb{N}\,\} \\
r \in \text{Register} & ::= & \text{sp} \mid \text{sv}_0 \mid \ldots \mid \text{sv}_4 \mid \text{wk}_0 \mid \ldots \mid \text{wk}_5 \\
\text{lv} \in \text{PLvalue} & ::= & \lfloor r \rfloor \mid \langle a \rangle_{\text{s}} \mid \langle r - o \rangle_{\text{s}} \mid \langle a \rangle_{\text{h}} \mid \langle r + o \rangle_{\text{h}} \quad \text{for } r \in \text{Register}, a \in \text{PAddr}, o \in \mathbb{N} \\
\text{rv} \in \text{PRvalue} & ::= & \text{lv} \mid w \quad \text{for lv} \in \text{PLvalue}, w \in \text{PWord} \\
\iota \in \text{Instruction} & ::= & \texttt{fail} \mid \texttt{halt} \mid \texttt{jmp}\ \text{rv} \mid \texttt{jnz}\ \text{rv}\ \text{rv} \mid \texttt{jneq}\ \text{rv}\ \text{rv}\ \text{rv} \mid \texttt{jptr}\ \text{rv}\ \text{rv} \mid \\
 & & \texttt{move}\ \text{lv}\ \text{rv} \mid \texttt{setptr}\ \text{lv} \mid \texttt{plus}\ \text{lv}\ \text{rv}\ \text{rv} \mid \texttt{minus}\ \text{lv}\ \text{rv}\ \text{rv} \mid \\
 & & \texttt{isr}\ \text{lv}\ \text{rv} \mid \texttt{isw}\ \text{rv}\ \text{rv} \\
\\
|w| & \stackrel{\text{def}}{=} & \pi_2(w) \\
\text{isptr}(w) & \stackrel{\text{def}}{=} & \pi_1(w) = 1 \\
\underline{n} & \stackrel{\text{def}}{=} & (0, n) \qquad \in \text{PWord} \\
\widehat{a} & \stackrel{\text{def}}{=} & (1, a) \qquad \in \text{PWord}
\end{array}
$$

$\boxed{\Phi(\text{rv}) \in \text{PWord}}$

$$
\begin{array}{lll}
\Phi(\lfloor r \rfloor) & \stackrel{\text{def}}{=} & \Phi.\text{reg}(r) \\
\Phi(\langle a \rangle_{\text{s}}) & \stackrel{\text{def}}{=} & \Phi.\text{stk}(a) \\
\Phi(\langle r - o \rangle_{\text{s}}) & \stackrel{\text{def}}{=} & \Phi.\text{stk}(|\Phi(\lfloor r \rfloor)| - o) \\
\Phi(\langle a \rangle_{\text{h}}) & \stackrel{\text{def}}{=} & \Phi.\text{hp}(a) \\
\Phi(\langle r + o \rangle_{\text{h}}) & \stackrel{\text{def}}{=} & \Phi.\text{hp}(|\Phi(\lfloor r \rfloor)| + o) \\
\Phi(w) & \stackrel{\text{def}}{=} & w
\end{array}
$$

$\boxed{\Phi[\text{lv} \mapsto w] \in \text{PMem}}$

$$
\begin{array}{lll}
\Phi[\lfloor r \rfloor \mapsto w] & \stackrel{\text{def}}{=} & (\Phi.\text{code}, \Phi.\text{reg}[r \mapsto w], \Phi.\text{stk}, \Phi.\text{hp}) \\
\Phi[\langle a \rangle_{\text{s}} \mapsto w] & \stackrel{\text{def}}{=} & (\Phi.\text{code}, \Phi.\text{reg}, \Phi.\text{stk}[a \mapsto w], \Phi.\text{hp}) \\
\Phi[\langle r - o \rangle_{\text{s}} \mapsto w] & \stackrel{\text{def}}{=} & (\Phi.\text{code}, \Phi.\text{reg}, \Phi.\text{stk}[|\Phi(\lfloor r \rfloor)| - o \mapsto w], \Phi.\text{hp}) \\
\Phi[\langle a \rangle_{\text{h}} \mapsto w] & \stackrel{\text{def}}{=} & (\Phi.\text{code}, \Phi.\text{reg}, \Phi.\text{stk}, \Phi.\text{hp}[a \mapsto w]) \\
\Phi[\langle r + o \rangle_{\text{h}} \mapsto w] & \stackrel{\text{def}}{=} & (\Phi.\text{code}, \Phi.\text{reg}, \Phi.\text{stk}, \Phi.\text{hp}[|\Phi(\lfloor r \rfloor)| + o \mapsto w])
\end{array}
$$

$\boxed{[\![\iota]\!]\,(\Phi, \mathrm{pc}) \in \mathrm{PConf} \uplus \{\, \mathit{halt}, \mathit{fail} \,\}}$

$$
\begin{array}{ll}
[\![\texttt{fail}]\!]\,(\Phi, \mathrm{pc}) & \stackrel{\mathrm{def}}{=} \mathit{fail} \\
[\![\texttt{halt}]\!]\,(\Phi, \mathrm{pc}) & \stackrel{\mathrm{def}}{=} \mathit{halt} \\
[\![\texttt{jmp}\ \mathrm{rv}]\!]\,(\Phi, \mathrm{pc}) & \stackrel{\mathrm{def}}{=} (\Phi, |\Phi(\mathrm{rv})|) \\
[\![\texttt{jnz}\ \mathrm{rv}_1\ \mathrm{rv}_2]\!]\,(\Phi, \mathrm{pc}) & \stackrel{\mathrm{def}}{=} \text{if } \Phi(\mathrm{rv}_2) \neq \underline{0} \text{ then } (\Phi, |\Phi(\mathrm{rv}_1)|) \text{ else } (\Phi, \mathrm{pc}+1) \\
[\![\texttt{jneq}\ \mathrm{rv}_1\ \mathrm{rv}_2\ \mathrm{rv}_3]\!]\,(\Phi, \mathrm{pc}) & \stackrel{\mathrm{def}}{=} \text{if } \Phi(\mathrm{rv}_2) \neq \Phi(\mathrm{rv}_3) \text{ then } (\Phi, |\Phi(\mathrm{rv}_1)|) \text{ else } (\Phi, \mathrm{pc}+1) \\
[\![\texttt{jptr}\ \mathrm{rv}_1\ \mathrm{rv}_2]\!]\,(\Phi, \mathrm{pc}) & \stackrel{\mathrm{def}}{=} \text{if } \mathrm{isptr}(\Phi(\mathrm{rv}_2)) \text{ then } (\Phi, |\Phi(\mathrm{rv}_1)|) \text{ else } (\Phi, \mathrm{pc}+1) \\
[\![\texttt{move}\ \mathrm{lv}\ \mathrm{rv}]\!]\,(\Phi, \mathrm{pc}) & \stackrel{\mathrm{def}}{=} (\Phi[\mathrm{lv} \mapsto \Phi(\mathrm{rv})], \mathrm{pc}+1) \\
[\![\texttt{setptr}\ \mathrm{lv}]\!]\,(\Phi, \mathrm{pc}) & \stackrel{\mathrm{def}}{=} (\Phi[\mathrm{lv} \mapsto \widehat{|\Phi(\mathrm{lv})|}], \mathrm{pc}+1) \\
[\![\texttt{plus}\ \mathrm{lv}\ \mathrm{rv}_1\ \mathrm{rv}_2]\!]\,(\Phi, \mathrm{pc}) & \stackrel{\mathrm{def}}{=} (\Phi[\mathrm{lv} \mapsto \underline{|\Phi(\mathrm{rv}_1)| + |\Phi(\mathrm{rv}_2)|}], \mathrm{pc}+1) \\
[\![\texttt{minus}\ \mathrm{lv}\ \mathrm{rv}_1\ \mathrm{rv}_2]\!]\,(\Phi, \mathrm{pc}) & \stackrel{\mathrm{def}}{=} (\Phi[\mathrm{lv} \mapsto \underline{|\Phi(\mathrm{rv}_1)| - |\Phi(\mathrm{rv}_2)|}], \mathrm{pc}+1) \\
[\![\texttt{isr}\ \mathrm{lv}\ \mathrm{rv}]\!]\,(\Phi, \mathrm{pc}) & \stackrel{\mathrm{def}}{=} (\Phi[\mathrm{lv} \mapsto \underline{\mathbb{E}(\Phi.\mathrm{code}(|\Phi(\mathrm{rv})|))}], \mathrm{pc}+1) \\
[\![\texttt{isw}\ \mathrm{rv}_1\ \mathrm{rv}_2]\!]\,(\Phi, \mathrm{pc}) & \stackrel{\mathrm{def}}{=} ((\Phi.\mathrm{code}[\,|\Phi(\mathrm{rv}_1)| \mapsto \mathbb{D}(|\Phi(\mathrm{rv}_2)|)], \Phi.\mathrm{reg}, \Phi.\mathrm{stk}, \Phi.\mathrm{hp}), \mathrm{pc}+1)
\end{array}
$$

where

$\mathbb{E} \in \mathrm{Instruction} \to \mathbb{N}$ is a bijection, and $\mathbb{D} := \mathbb{E}^{-1}$.

$\boxed{\mathrm{PConf} \hookrightarrow \mathrm{PConf} \uplus \{\, \mathit{halt}, \mathit{fail} \,\}}$

$$(\Phi, \mathrm{pc}) \;\hookrightarrow\; [\![\Phi.\mathrm{code}(\mathrm{pc})]\!]\,(\Phi, \mathrm{pc})$$

2 Specifications

2.1 Language Specification

$$
\begin{aligned}
\text{LangSpec} \stackrel{\text{def}}{=} \{\, & (\text{Val}, \text{Com}, \text{Cont}, \text{Mem}, \text{Conf}, \\
& \text{plugv}, \text{plugc}, \text{step}, \text{mdom}, \text{mdisj}, \\
& \text{oftype}, \text{base}_b, \text{pair}, \text{app}, \text{appty}, \text{pack}, \text{roll}, \text{ref}, \text{asgn}) \mid \\
& \text{Val}, \text{Com}, \text{Cont}, \text{Mem}, \text{Conf} \in \text{Set} \wedge \\
& \text{plugv} \in \text{Val} \times \text{Cont} \times \text{Mem} \to \mathbb{P}(\text{Conf}) \wedge \\
& \text{plugc} \in \text{Com} \times \text{Cont} \times \text{Mem} \to \mathbb{P}(\text{Conf}) \wedge \\
& \text{step} \in \text{Conf} \to \text{Conf} \uplus \{\, \mathit{fail}, \mathit{halt} \,\} \wedge \\
& \text{mdom} \in \text{Mem} \to \mathbb{P}(\text{Val}) \wedge \\
& \text{mdisj} \in \text{Mem} \times \text{Mem} \to \mathbb{P}(\text{Mem}) \wedge \\
& \text{oftype} \in \text{CType} \to \mathbb{P}(\text{Val} \times \text{Mem}) \wedge \\
& \text{base}_b \in [\![b]\!] \to \mathbb{P}(\text{Val} \times \text{Mem}) \wedge \\
& \text{pair} \in \text{Val} \times \text{Val} \to \mathbb{P}(\text{Val} \times \text{Mem}) \wedge \\
& \text{app} \in \text{Val} \times \text{Val} \to \mathbb{P}(\text{Com}) \wedge \\
& \text{appty} \in \text{Val} \times \text{CType} \to \mathbb{P}(\text{Com}) \wedge \\
& \text{pack} \in \text{CType} \times \text{Val} \to \mathbb{P}(\text{Val} \times \text{Mem}) \wedge \\
& \text{roll} \in \text{Val} \to \mathbb{P}(\text{Val} \times \text{Mem}) \wedge \\
& \text{ref} \in \text{Val} \to \mathbb{P}(\text{Val} \times \text{Mem}) \wedge \\
& \text{asgn} \in \text{Mem} \times \text{Val} \times \text{Val} \rightharpoonup \text{Mem} \wedge \\
& \forall M_1, M_2.\ \forall M \in \text{mdisj}(M_1, M_2).\ \text{mdom}(M) \supseteq \text{mdom}(M_1) \uplus \text{mdom}(M_2) \,\}
\end{aligned}
$$

$$
\begin{aligned}
\text{mdisjlist}() &\stackrel{\text{def}}{=} \{\, M \in \text{Mem} \,\} \\
\text{mdisjlist}(M_1, \ldots, M_{n+1}) &\stackrel{\text{def}}{=} \{\, M \in \text{Mem} \mid \exists M'.\ M' \in \text{mdisjlist}(M_1, \ldots, M_n) \wedge M \in \text{mdisj}(M', M_{n+1}) \,\}
\end{aligned}
$$

$$\boxed{\text{Conf} \stackrel{k}{\hookrightarrow} \text{Conf} \uplus \{\, \mathit{fail}, \mathit{halt} \,\}}$$

$$
\begin{aligned}
C &\stackrel{0}{\hookrightarrow} C \\
C &\stackrel{k+1}{\hookrightarrow} \mathit{fail} && \text{if } \text{step}(C) = \mathit{fail} \\
C &\stackrel{k+1}{\hookrightarrow} \mathit{halt} && \text{if } \text{step}(C) = \mathit{halt} \\
C &\stackrel{k+1}{\hookrightarrow} R && \text{if } \text{step}(C) = C' \wedge C' \stackrel{k}{\hookrightarrow} R
\end{aligned}
$$

$$\boxed{\text{obsk} : \mathbb{N} \times \text{Conf} \to \{\, \mathit{fail}, \mathit{halt}, \mathit{running} \,\}}$$

$$
\text{obsk}(k, C) \stackrel{\text{def}}{=} \begin{cases}
\mathit{fail} & \text{if } C \stackrel{k}{\hookrightarrow} \mathit{fail} \\
\mathit{halt} & \text{if } C \stackrel{k}{\hookrightarrow} \mathit{halt} \\
\mathit{running} & \text{if } C \stackrel{k}{\hookrightarrow} C'
\end{cases}
$$

$\boxed{\text{observe} : \text{Conf} \to \{\, \mathit{fail}, \mathit{halt}, \mathit{diverge} \,\}}$

$$\text{observe}(C) \stackrel{\text{def}}{=} \begin{cases} \mathit{fail} & \text{if } \exists k.\ \text{obsk}(k, C) = \mathit{fail} \\ \mathit{halt} & \text{if } \exists k.\ \text{obsk}(k, C) = \mathit{halt} \\ \mathit{diverge} & \text{otherwise, } \textit{i.e.,} \text{ if } \forall k.\ \text{obsk}(k, C) = \mathit{running} \end{cases}$$

2.2 World Specification

For $\mathcal{L}_1, \mathcal{L}_2 \in \text{LangSpec}$,

$$\begin{aligned}
\text{WorldSpec} \stackrel{\text{def}}{=} \{\, & (\text{World}, \text{lev}, \mathcal{M}, \mathcal{B}, \mathcal{O}, \triangleright, \sqsupseteq, \sqsupseteq_{\text{pub}}) \mid \\
& \text{World} \in \text{Set} \wedge \\
& \text{lev} \in \text{World} \to \mathbb{N} \wedge \\
& \mathcal{M} \in \text{World} \to \mathbb{P}(\mathcal{L}_1.\text{Mem} \times \mathcal{L}_2.\text{Mem}) \wedge \\
& \mathcal{B} \in \text{World} \to \mathbb{P}(\mathcal{L}_1.\text{Val} \times \mathcal{L}_2.\text{Val}) \wedge \\
& \mathcal{O} \in \text{World} \to \mathbb{P}(\mathcal{L}_1.\text{Conf} \times \mathcal{L}_2.\text{Conf}) \wedge \\
& \triangleright \in \text{World} \to \text{World} \wedge \\
& \sqsupseteq \in \mathbb{P}(\text{World} \times \text{World}) \wedge \\
& \sqsupseteq_{\text{pub}} \in \mathbb{P}(\text{World} \times \text{World}) \wedge \\
& \sqsupseteq, \sqsupseteq_{\text{pub}} \text{ are preorders} \wedge \sqsupseteq_{\text{pub}} \subseteq \sqsupseteq \ \wedge \\
& \forall W' \sqsupseteq W.\ \triangleright W' \sqsupseteq \triangleright W \wedge \\
& \forall W' \sqsupseteq_{\text{pub}} W.\ \triangleright W' \sqsupseteq_{\text{pub}} \triangleright W \wedge \\
& \forall W.\ \triangleright W \sqsupseteq_{\text{pub}} W \wedge \\
& \forall W' \sqsupseteq W.\ \text{lev}(W') \leq \text{lev}(W) \wedge \\
& \forall W.\ \text{lev}(W) > 0 \implies \text{lev}(\triangleright W) = \text{lev}(W) - 1 \,\}
\end{aligned}$$

$$\begin{aligned}
\sqsupset_{\triangleright} &\stackrel{\text{def}}{=} \{\, (W', W) \in \text{World} \times \text{World} \mid \text{lev}(W) > 0 \wedge W' \sqsupseteq \triangleright W \,\} \\
\text{WVRel} &\stackrel{\text{def}}{=} \{\, R \in \mathbb{P}(\text{World} \times \mathcal{L}_1.\text{Val} \times \mathcal{L}_2.\text{Val}) \,\} \\
R(W) &\stackrel{\text{def}}{=} \{\, (\mathbf{v}_1, v_2) \mid (W, \mathbf{v}_1, v_2) \in R \,\} \quad \text{for } R \in \text{WVRel} \\
\triangleright R &\stackrel{\text{def}}{=} \{\, (W, \mathbf{v}_1, v_2) \mid \text{lev}(W) > 0 \implies (\triangleright W, \mathbf{v}_1, v_2) \in R \,\} \quad \text{for } R \in \text{WVRel} \\
\Box R &\stackrel{\text{def}}{=} \{\, (W, \mathbf{v}_1, v_2) \mid \forall W' \sqsupseteq W.\ (W', \mathbf{v}_1, v_2) \in R \,\} \quad \text{for } R \in \text{WVRel} \\
R_{\sqsupset_{\triangleright} W} &\stackrel{\text{def}}{=} \{\, (W', \mathbf{v}_1, v_2) \mid W' \sqsupset_{\triangleright} W \wedge (W', \mathbf{v}_1, v_2) \in R \,\} \quad \text{for } R \in \text{WVRel} \\
\overline{(R_1, R_2)} &\stackrel{\text{def}}{=} \{\, (W, \mathbf{v}_1, v_2) \mid \forall (\mathbf{M}_1, M_2) \in \mathcal{M}(W).\ (\mathbf{v}_1, \mathbf{M}_1) \in R_1 \wedge (v_2, M_2) \in R_2 \,\} \\
&\quad \text{for } R_1 \in \mathbb{P}(\mathcal{L}_1.\text{Val} \times \mathcal{L}_1.\text{Mem}), R_2 \in \mathbb{P}(\mathcal{L}_2.\text{Val} \times \mathcal{L}_2.\text{Mem})
\end{aligned}$$

Lemma 1. $\sqsupset_{\triangleright}$ is well-founded.

Proof. Because the level of worlds strictly decreases. □

Lemma 2.

1. $\forall W'', W', W.\ W'' \sqsupset_{\triangleright} W' \wedge W' \sqsupset_{\triangleright} W \implies W'' \sqsupset_{\triangleright} W$
2. $\forall W'', W', W.\ W'' \sqsupset_{\triangleright} W' \wedge W' \sqsupseteq W \implies W'' \sqsupset_{\triangleright} W$
3. $\forall W'', W', W.\ W'' \sqsupseteq W' \wedge W' \sqsupset_{\triangleright} W \implies W'' \sqsupset_{\triangleright} W$

Proof. By the definition of $\sqsupset_{\triangleright}$ and the assumptions on $\sqsupseteq, \sqsupseteq_{\text{pub}}, \triangleright$,lev. □

3 Logical Relations

3.1 Definitions

Let $\mathcal{L}_1, \mathcal{L}_2 \in \text{LangSpec}, \mathcal{W} \in \text{WorldSpec}$.

Define $\mathcal{V}[\![\tau]\!]\rho \in \text{WVRel}$ by structural induction on τ:

$$
\begin{array}{rcl}
\text{TyValRel} & \stackrel{\text{def}}{=} & \{\, (\tau_1, \tau_2, R) \mid \tau_1, \tau_2 \in \text{CType} \wedge R \in \text{WVRel} \,\} \\
\rho & \in & \text{TypeVar} \rightharpoonup \text{TyValRel} \\
\rho.1(\tau) & \stackrel{\text{def}}{=} & \tau[\rho(\alpha).\tau_1/\alpha] \\
\rho.2(\tau) & \stackrel{\text{def}}{=} & \tau[\rho(\alpha).\tau_2/\alpha] \\
\text{oftype}(\tau, \rho) & \stackrel{\text{def}}{=} & \Box\overline{(\mathcal{L}_1.\text{oftype}(\rho.1(\tau)), \mathcal{L}_2.\text{oftype}(\rho.2(\tau)))}
\end{array}
$$

$$
\begin{array}{rcl}
\mathcal{V}[\![\alpha]\!]\rho & \stackrel{\text{def}}{=} & \{\, (W, \mathbf{v}_1, v_2) \in \text{oftype}(\alpha, \rho) \mid (W, \mathbf{v}_1, v_2) \in \Box\rho(\alpha).R \,\} \\
\mathcal{V}[\![b]\!]\rho & \stackrel{\text{def}}{=} & \{\, (W, \mathbf{v}_1, v_2) \in \text{oftype}(b, \rho) \mid \exists x \in [\![b]\!]\,.\ (W, \mathbf{v}_1, v_2) \in \Box\overline{(\mathcal{L}_1.\text{base}_b(x), \mathcal{L}_2.\text{base}_b(x))} \,\} \\
\mathcal{V}[\![\tau \times \tau']\!]\rho & \stackrel{\text{def}}{=} & \{\, (W, \mathbf{v}_1, v_2) \in \text{oftype}(\tau \times \tau', \rho) \mid \exists (\mathbf{u}_1, u_2) \in \triangleright\mathcal{V}[\![\tau]\!]\rho(W).\ \exists (\mathbf{u}_1', u_2') \in \triangleright\mathcal{V}[\![\tau']\!]\rho(W). \\
& & \quad (W, \mathbf{v}_1, v_2) \in \Box\overline{(\mathcal{L}_1.\text{pair}(\mathbf{u}_1, \mathbf{u}_1'), \mathcal{L}_2.\text{pair}(u_2, u_2'))} \,\} \\
\mathcal{V}[\![\tau' \to \tau]\!]\rho & \stackrel{\text{def}}{=} & \{\, (W, \mathbf{v}_1, v_2) \in \text{oftype}(\tau' \to \tau, \rho) \mid \forall W' \sqsupset_\triangleright W. \\
& & \quad \forall (\mathbf{u}_1, u_2) \in \mathcal{V}[\![\tau']\!]\rho(W').\ \forall \mathbf{e}_1 \in \mathcal{L}_1.\text{app}(\mathbf{v}_1, \mathbf{u}_1).\ \forall e_2 \in \mathcal{L}_2.\text{app}(v_2, u_2). \\
& & \quad (W', \mathbf{e}_1, e_2) \in \mathcal{E}[\![\tau]\!]\rho \,\} \\
\mathcal{V}[\![\forall\alpha.\,\tau]\!]\rho & \stackrel{\text{def}}{=} & \{\, (W, \mathbf{v}_1, v_2) \in \text{oftype}(\forall\alpha.\,\tau, \rho) \mid \forall W' \sqsupset_\triangleright W. \\
& & \quad \forall (\tau_1, \tau_2, R) \in \text{TyValRel}.\ \forall \mathbf{e}_1 \in \mathcal{L}_1.\text{appty}(\mathbf{v}_1, \tau_1).\ \forall e_2 \in \mathcal{L}_2.\text{appty}(v_2, \tau_2). \\
& & \quad (W', \mathbf{e}_1, e_2) \in \mathcal{E}[\![\tau]\!]\rho[\alpha \mapsto (\tau_1, \tau_2, R)] \,\} \\
\mathcal{V}[\![\exists\alpha.\,\tau]\!]\rho & \stackrel{\text{def}}{=} & \{\, (W, \mathbf{v}_1, v_2) \in \text{oftype}(\exists\alpha.\,\tau, \rho) \mid \\
& & \quad \exists (\tau_1, \tau_2, R) \in \text{TyValRel}.\ \exists (\mathbf{u}_1, u_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto (\tau_1, \tau_2, R)](W). \\
& & \quad (W, \mathbf{v}_1, v_2) \in \Box\overline{(\mathcal{L}_1.\text{pack}(\tau_1, \mathbf{u}_1), \mathcal{L}_2.\text{pack}(\tau_2, u_2))} \,\} \\
\mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho & \stackrel{\text{def}}{=} & \mu(F_{\alpha,\tau,\rho}) \\
F_{\alpha,\tau,\rho} & \stackrel{\text{def}}{=} & \lambda R.\, \{\, (W, \mathbf{v}_1, v_2) \in \text{oftype}(\mu\alpha.\,\tau, \rho) \mid \\
& & \qquad \exists (\mathbf{u}_1, u_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto (\rho.1(\mu\alpha.\,\tau), \rho.2(\mu\alpha.\,\tau), R)](W). \\
& & \qquad (W, \mathbf{v}_1, v_2) \in \Box\overline{(\mathcal{L}_1.\text{roll}(\mathbf{u}_1), \mathcal{L}_2.\text{roll}(u_2))} \,\} \\
\mu(F)(W) & \stackrel{\text{def}}{=} & F(\mu(F)_{\sqsupset_\triangleright W})(W) \quad \text{for } F \in \text{WVRel} \to \text{WVRel} \\
\mathcal{V}[\![\mathsf{ref}\ \tau]\!]\rho & \stackrel{\text{def}}{=} & \{\, (W, \mathbf{v}_1, v_2) \in \text{oftype}(\mathsf{ref}\ \tau, \rho) \mid \forall W' \sqsupseteq W.\ \forall (\mathbf{M}_1, M_2) \in \mathcal{M}(W'). \\
& & \quad (\mathbf{v}_1, v_2) \in \mathcal{B}(W') \wedge \\
& & \quad \big(\exists (\mathbf{u}_1, u_2) \in \triangleright\mathcal{V}[\![\tau]\!]\rho(W').\ (\mathbf{v}_1, \mathbf{M}_1) \in \mathcal{L}_1.\text{ref}(\mathbf{u}_1) \wedge (v_2, M_2) \in \mathcal{L}_2.\text{ref}(u_2)\big) \wedge \\
& & \quad \big(\forall (\mathbf{u}_1, u_2) \in \triangleright\mathcal{V}[\![\tau]\!]\rho(W').\ (\mathcal{L}_1.\text{asgn}(\mathbf{M}_1, \mathbf{v}_1, \mathbf{u}_1), \mathcal{L}_2.\text{asgn}(M_2, v_2, u_2)) \in \mathcal{M}(W')\big) \,\}
\end{array}
$$

$$
\begin{array}{rcl}
\mathcal{K}[\![\tau]\!]\rho & \stackrel{\text{def}}{=} & \{\, (W, \mathbf{K}_1, K_2) \in \text{World} \times \mathcal{L}_1.\text{Cont} \times \mathcal{L}_2.\text{Cont} \mid \forall W' \sqsupseteq_{\text{pub}} W. \\
& & \quad \forall (\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho(W').\ \forall (\mathbf{M}_1, M_2) \in \mathcal{M}(W'). \\
& & \quad \forall C_1 \in \mathcal{L}_1.\text{plugv}(\mathbf{v}_1, \mathbf{K}_1, \mathbf{M}_1).\ \forall C_2 \in \mathcal{L}_2.\text{plugv}(v_2, K_2, M_2).\ (C_1, C_2) \in \mathcal{O}(W') \,\} \\
\mathcal{E}[\![\tau]\!]\rho & \stackrel{\text{def}}{=} & \{\, (W, \mathbf{e}_1, e_2) \in \text{World} \times \mathcal{L}_1.\text{Com} \times \mathcal{L}_2.\text{Com} \mid \\
& & \quad \forall (\mathbf{K}_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho(W).\ \forall (\mathbf{M}_1, M_2) \in \mathcal{M}(W). \\
& & \quad \forall C_1 \in \mathcal{L}_1.\text{plugc}(\mathbf{e}_1, \mathbf{K}_1, \mathbf{M}_1).\ \forall C_2 \in \mathcal{L}_2.\text{plugc}(e_2, K_2, M_2).\ (C_1, C_2) \in \mathcal{O}(W) \,\}
\end{array}
$$

Contractiveness

$$
\begin{array}{rcl}
F \text{ contractive} & \stackrel{\text{def}}{=} & \forall W, R_1, R_2.\ (\forall W' \sqsupset_\triangleright W.\ R_1(W') = R_2(W')) \implies F(R_1)(W) = F(R_2)(W) \\
& & \text{for } F \in \text{WVRel} \to \text{WVRel} \\
\tau\ \alpha\text{-non-contractive} & \stackrel{\text{def}}{=} & \tau = \alpha \\
& | & \tau = \exists \beta.\, \tau' \text{ for some } \beta, \tau' \text{ such that } \beta \neq \alpha \wedge \tau'\ \alpha\text{-non-contractive} \\
& | & \tau = \mu \beta.\, \tau' \text{ for some } \beta, \tau' \text{ such that } \beta \neq \alpha \wedge \tau'\ \alpha\text{-non-contractive} \\
\tau\ \alpha\text{-contractive} & \stackrel{\text{def}}{=} & \neg\, \tau\ \alpha\text{-non-contractive}
\end{array}
$$

3.2 Properties

Theorem 1 (Fixpoint)**.** $\forall F.\ F \text{ contractive} \implies \mu(F) = F(\mu(F))$.

Proof. For F contractive, we prove $\forall W.\ \mu(F)(W) = F(\mu(F))(W)$ by well-founded induction on W w.r.t. $\sqsupset_\triangleright$.

- For W, assume $\forall W' \sqsupset_\triangleright W.\ \mu(F)(W') = F(\mu(F))(W')$.
- We need to show that $\mu(F)(W) = F(\mu(F))(W)$.
- We have $\mu(F)(W) = F(\mu(F)_{\sqsupset_\triangleright W})(W)$ by definition.
- By contractivness of F, it suffices to show that $\forall W' \sqsupset_\triangleright W.\ \mu(F)(W') = \mu(F)_{\sqsupset_\triangleright W}(W')$, which holds vacuously.

□

Theorem 2 (Uniqueness)**.** $\forall F, R_1, R_2.\ F \text{ contractive} \wedge R_1 = F(R_1) \wedge R_2 = F(R_2) \implies R_1 = R_2$.

Proof. For F contractive and R_1, R_2 fixpoints of F, we prove that $\forall W.\ R_1(W) = R_2(W)$ by well-founded induction on W w.r.t. $\sqsupset_\triangleright$.

- For W, assume $\forall W' \sqsupset_\triangleright W.\ R_1(W') = R_2(W')$.
- We need to show that $R_1(W) = R_2(W)$.
- As R_1, R_2 are fixpoints, it suffices to show that $F(R_1)(W) = F(R_2)(W)$.
- By contractivness of F, it suffices to show that $\forall W' \sqsupset_\triangleright W.\ R_1(W') = R_2(W')$, which is exactly the induction hypothesis.

□

Lemma 3. For all α, τ, ρ, W with $\text{ftv}(\mu\alpha.\,\tau) \subseteq \text{dom}\,\rho$,

$$\mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho(W) \subseteq \{\, (\mathbf{v}_1, v_2) \mid \exists (\mathbf{u}_1, u_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto (\rho.1(\mu\alpha.\,\tau), \rho.2(\mu\alpha.\,\tau), \mu(F_{\alpha,\tau,\rho})_{\sqsupset_\triangleright W})](W) \,\}\ .$$

Proof.

$$
\begin{array}{rl}
& \mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho(W) \\
= & \mu(F_{\alpha,\tau,\rho})(W) \\
= & F_{\alpha,\tau,\rho}(\mu(F_{\alpha,\tau,\rho})_{\sqsupset_\triangleright W})(W) \\
\subseteq & \{\, (\mathbf{v}_1, v_2) \mid \exists (\mathbf{u}_1, u_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto (\rho.1(\mu\alpha.\,\tau), \rho.2(\mu\alpha.\,\tau), \mu(F_{\alpha,\tau,\rho})_{\sqsupset_\triangleright W})](W) \,\}
\end{array}
$$

□

Lemma 4.

$$\forall \alpha, \tau, \rho.\ \tau\ \alpha\text{-non-contractive} \wedge \mathrm{ftv}(\mu\alpha.\,\tau) \subseteq \mathrm{dom}\,\rho \implies \forall \tau_1, \tau_2, R, W.\ \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto (\tau_1, \tau_2, R_{\sqsupset_\triangleright W})](W) = \emptyset$$

Proof. We prove this by structural induction on τ α-non-contractive.

- When $\tau = \alpha$:
  $\mathcal{V}[\![\alpha]\!]\rho[\alpha \mapsto (\tau_1, \tau_2, R_{\sqsupset_\triangleright W})](W) \ \subseteq\ R_{\sqsupset_\triangleright W}(W) \ =\ \emptyset$.

- When $\tau = \exists\beta.\,\tau'$ with $\beta \neq \alpha \wedge \tau'$ α-non-contractive:
  Let $\rho' = \rho[\alpha \mapsto (\tau_1, \tau_2, R_{\sqsupset_\triangleright W})]$. Then we have

  $$\begin{aligned} &\mathcal{V}[\![\exists\beta.\,\tau']\!]\rho'(W) \\ \subseteq\ &\{\, (W, \mathbf{v}_1, v_2) \mid \exists(\tau_1', \tau_2', R') \in \mathrm{TyValRel}.\ \exists(\mathbf{u}_1, u_2) \in \mathcal{V}[\![\tau']\!]\rho'[\beta \mapsto (\tau_1', \tau_2', R')](W) \,\} \end{aligned}$$

  As $\beta \neq \alpha$, by induction hypothesis, for all $(\tau_1', \tau_2', R') \in \mathrm{TyValRel}$ we have

  $$\mathcal{V}[\![\tau']\!]\rho'[\beta \mapsto (\tau_1', \tau_2', R')](W) = \mathcal{V}[\![\tau']\!]\rho[\beta \mapsto (\tau_1', \tau_2', R')][\alpha \mapsto (\tau_1, \tau_2, R_{\sqsupset_\triangleright W})](W) = \emptyset\ .$$

  Therefore, $\mathcal{V}[\![\exists\beta.\,\tau']\!]\rho[\alpha \mapsto (\tau_1, \tau_2, R_{\sqsupset_\triangleright W})](W) = \emptyset$.

- When $\tau = \mu\beta.\,\tau'$ with $\beta \neq \alpha \wedge \tau'$ α-non-contractive:
  Let $\rho' = \rho[\alpha \mapsto (\tau_1, \tau_2, R_{\sqsupset_\triangleright W})]$.
  Then, by Lemma 3, we have

  $$\begin{aligned} &\mathcal{V}[\![\mu\beta.\,\tau']\!]\rho'(W) \\ \subseteq\ &\{\, (\mathbf{v}_1, v_2) \mid \exists(\mathbf{u}_1, u_2) \in \mathcal{V}[\![\tau']\!]\rho'[\beta \mapsto (\rho'.1(\mu\beta.\,\tau'), \rho'.2(\mu\beta.\,\tau'), \mu(F_{\beta,\tau',\rho'})_{\sqsupset_\triangleright W})](W) \,\}\ . \end{aligned}$$

  As $\beta \neq \alpha$, by induction hypothesis, we have

  $$\begin{aligned} &\mathcal{V}[\![\tau']\!]\rho'[\beta \mapsto (\rho'.1(\mu\beta.\,\tau'), \rho'.2(\mu\beta.\,\tau'), \mu(F_{\beta,\tau',\rho'})_{\sqsupset_\triangleright W})](W) \\ =\ &\mathcal{V}[\![\tau']\!]\rho[\beta \mapsto (\rho'.1(\mu\beta.\,\tau'), \rho'.2(\mu\beta.\,\tau'), \mu(F_{\beta,\tau',\rho'})_{\sqsupset_\triangleright W})][\alpha \mapsto (\tau_1, \tau_2, R_{\sqsupset_\triangleright W})](W) \\ =\ &\emptyset \end{aligned}$$

  Therefore, $\mathcal{V}[\![\mu\beta.\,\tau']\!]\rho[\alpha \mapsto (\tau_1, \tau_2, R_{\sqsupset_\triangleright W})](W) = \emptyset$.

□

Theorem 3.

$$\forall \alpha, \tau, \rho.\ \mathrm{ftv}(\mu\alpha.\,\tau) \subseteq \mathrm{dom}\,\rho \implies \mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho = F_{\alpha,\tau,\rho}(\mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho)$$

Proof.

When τ α-contractive

- As $\mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho = \mu(F_{\alpha,\tau,\rho})$, by Theorem 1, it suffices to show that $F_{\alpha,\tau,\rho}$ is contractive.

- By an easy induction on τ, one can show that for all α, τ such that τ α-contractive, all free occurrences of α in τ are under one of the type constructors $\times$, $\to$, $\forall$, ref .

- For any $\tau_1, \tau_2, \beta, \tau', \rho, W$, the relations $\mathcal{V}[\![\tau_1 \times \tau_2]\!]\rho(W)$, $\mathcal{V}[\![\tau_1 \to \tau_2]\!]\rho(W)$, $\mathcal{V}[\![\forall\beta.\,\tau']\!]\rho(W)$, $\mathcal{V}[\![\mathsf{ref}\ \tau_1]\!]\rho(W)$ only depend on $\mathcal{V}[\![\tau_1]\!]\rho(W')$, $\mathcal{V}[\![\tau_2]\!]\rho(W')$ and $\mathcal{V}[\![\tau']\!]\rho[\beta \mapsto r](W')$ for any r and $W' \sqsupset_\triangleright W$.

- By Lemma 2 and the above facts, it follows that the relation $\mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto (\rho.1(\mu\alpha.\,\tau), \rho.2(\mu\alpha.\,\tau), R)](W)$ only depends on $R(W')$ for $W' \sqsupset_\triangleright W$.
- Therefore, $F_{\alpha,\tau,\rho}(R)(W)$ only depends on $R(W')$ for $W' \sqsupset_\triangleright W$ and thus $F_{\alpha,\tau,\rho}$ is contractive.

When τ α-non-contractive

- By Lemma 3 and 4, we have $\mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho = \emptyset$.
- Again by Lemma 4, we have

$$\begin{array}{ll} & F_{\alpha,\tau,\rho}(\mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho)(W) \\ = & F_{\alpha,\tau,\rho}(\emptyset_{\sqsupset_\triangleright W})(W) \\ \subseteq & \{\, (\mathbf{v}_1, v_2) \mid \exists (\mathbf{u}_1, u_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto (\rho.1(\mu\alpha.\,\tau), \rho.2(\mu\alpha.\,\tau), \emptyset_{\sqsupset_\triangleright W})](W) \,\} \\ = & \emptyset \end{array}$$

- Thus, $\mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho = F_{\alpha,\tau,\rho}(\mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho) = \emptyset$.

□

Lemma 5. $\triangleright$ preserves monotonicity: $\forall R\ .R \subseteq \Box R \implies \triangleright R \subseteq \Box \triangleright R$.

Proof. By definition and the assumptions on $\triangleright$, lev. □

Theorem 4 (Well-typedness)**.** $\mathcal{V}[\![\tau]\!]\rho \subseteq \mathrm{oftype}(\tau, \rho)$.

Proof. By case analysis on τ, each case holds vacuously by definition, except for $\tau = \mu\alpha.\,\tau'$. In this case, for all worlds W, we have

$$\mathcal{V}[\![\mu\alpha.\,\tau']\!]\rho(W) = \mu(F_{\alpha,\tau',\rho})(W) = F_{\alpha,\tau',\rho}(\mu(F_{\alpha,\tau',\rho})_{\sqsupset_\triangleright W})(W) \subseteq \mathrm{oftype}(\mu\alpha.\,\tau', \rho)(W)\ .$$

□

Theorem 5 (Monotonicity)**.** $\forall \tau, \rho.\ \mathrm{ftv}(\tau) \subseteq \mathrm{dom}\,\rho \implies \mathcal{V}[\![\tau]\!]\rho \subseteq \Box\mathcal{V}[\![\tau]\!]\rho$.

Proof. By structural induction on τ:

- For $\tau = \alpha, \tau = b$:
  $\mathcal{V}[\![\tau]\!]\rho$ is monotone, as all relations appearing in the definition are monotone.
- For $\tau = \tau_1 \to \tau_2, \tau = \forall\alpha.\,\tau', \tau = \mathsf{ref}\ \tau'$:
  $\mathcal{V}[\![\tau]\!]\rho$ is trivially monotone by definition and Lemma 2.
- For $\tau = \tau_1 \times \tau_2, \tau = \exists\alpha.\,\tau'$:
  $\mathcal{V}[\![\tau]\!]\rho$ is monotone, as all relations appearing in the definition are monotone by induction hypothesis and Lemma 5.
- For $\tau = \mu\alpha.\,\tau'$:
  By Theorem 3, we have

$$\begin{array}{l} \quad \mathcal{V}[\![\mu\alpha.\,\tau']\!]\rho \\ = F_{\alpha,\tau',\rho}(\mathcal{V}[\![\mu\alpha.\,\tau']\!]\rho) \\ = \{\, (W, \mathbf{v}_1, v_2) \in \mathrm{oftype}(\mu\alpha.\,\tau', \rho) \mid \\ \qquad \exists (\mathbf{u}_1, u_2) \in \mathcal{V}[\![\tau']\!]\rho[\alpha \mapsto (\rho.1(\mu\alpha.\,\tau'), \rho.2(\mu\alpha.\,\tau'), \mathcal{V}[\![\mu\alpha.\,\tau']\!]\rho)](W). \\ \qquad (W, \mathbf{v}_1, v_2) \in \Box\overline{(\mathcal{L}_1.\mathrm{roll}(\mathbf{u}_1), \mathcal{L}_2.\mathrm{roll}(u_2))}\,\} \ . \end{array}$$

As $\mathcal{V}[\![\tau']\!]\rho[\alpha \mapsto (\rho.1(\mu\alpha.\,\tau'), \rho.2(\mu\alpha.\,\tau'), \mathcal{V}[\![\mu\alpha.\,\tau']\!]\rho)]$ is monotone by induction hypothesis, it follows that $\mathcal{V}[\![\mu\alpha.\,\tau']\!]\rho$ is monotone.

□

Theorem 6. $\forall \tau, \rho.\ \mathrm{ftv}(\tau) \subseteq \mathrm{dom}\,\rho \implies \forall W' \sqsupseteq_{\mathrm{pub}} W.\ \mathcal{K}[\![\tau]\!]\rho(W) \subseteq \mathcal{K}[\![\tau]\!]\rho(W')$.

Proof. It trivially holds by definition. □

Theorem 7 (Substitution)**.**

$$\mathcal{V}[\![\tau[\tau'/\alpha]]\!]\rho = \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto (\rho.1(\tau'), \rho.2(\tau'), \mathcal{V}[\![\tau']\!]\rho)]$$

Proof. By an easy structural induction on τ. The only non-trivial case is when $\tau = \alpha$. In this case, we need to show that

$$\begin{array}{rcl} \mathcal{V}[\![\tau']\!]\rho & = & \{\, (W, \mathbf{v}_1, v_2) \in \mathrm{oftype}(\alpha, \rho[\alpha \mapsto (\rho.1(\tau'), \rho.2(\tau'), \mathcal{V}[\![\tau']\!]\rho)]) \mid (W, \mathbf{v}_1, v_2) \in \Box\mathcal{V}[\![\tau']\!]\rho \,\} \\ & = & \{\, (W, \mathbf{v}_1, v_2) \in \Box(\mathcal{L}.\mathrm{oftype}(\rho.1(\tau')), \mathcal{H}.\mathrm{oftype}(\rho.2(\tau'))) \mid (W, \mathbf{v}_1, v_2) \in \Box\mathcal{V}[\![\tau']\!]\rho \,\} \\ & = & \{\, (W, \mathbf{v}_1, v_2) \in \mathrm{oftype}(\tau', \rho) \mid (W, \mathbf{v}_1, v_2) \in \Box\mathcal{V}[\![\tau']\!]\rho \,\} \end{array}$$

This holds because by Theorem 5, $\Box\mathcal{V}[\![\tau']\!]\rho = \mathcal{V}[\![\tau']\!]\rho$, and by Theorem 4, $\mathcal{V}[\![\tau']\!]\rho \subseteq \mathrm{oftype}(\tau', \rho)$. □

4 Possible Worlds

4.1 Definitions

For $R \in \mathbb{P}(X \times Y)$,

$$
\begin{aligned}
R \text{ pbijective} &\stackrel{\text{def}}{=} \big(\forall x, y, y'.\ (x,y),(x,y') \in R \implies y = y'\big) \wedge \big(\forall x, x', y.\ (x,y),(x',y) \in R \implies x = x'\big) \\
\mathrm{dom}_1(R) &\stackrel{\text{def}}{=} \{\, x \mid \exists y.\ (x,y) \in R \,\} \\
\mathrm{dom}_2(R) &\stackrel{\text{def}}{=} \{\, y \mid \exists x.\ (x,y) \in R \,\}
\end{aligned}
$$

Let $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{LangSpec}$.

$$
\begin{aligned}
\mathrm{MemRel}_n &\stackrel{\text{def}}{=} \mathbb{P}(\mathrm{World}_n \times \mathcal{L}_1.\mathrm{Mem} \times \mathcal{L}_2.\mathrm{Mem}) \\
R \text{ monotone} &\stackrel{\text{def}}{=} \forall (W, \mathbf{M}_1, M_2) \in R.\ \forall W' \sqsupseteq W.\ (W', \mathbf{M}_1, M_2) \in R \\
&\quad \text{for } R \in \mathrm{MemRel}_n \\
\mathrm{Island}_n &\stackrel{\text{def}}{=} \{\, \iota = (s, S, \delta, \varphi, MR, Bij) \mid \\
&\qquad s \in S \wedge S \in \mathrm{Set} \wedge \delta, \varphi \in \mathbb{P}(S \times S) \wedge \\
&\qquad MR \in S \to \mathrm{MemRel}_n \wedge Bij \in S \to \mathbb{P}(\mathcal{L}_1.\mathrm{Val} \times \mathcal{L}_2.\mathrm{Val}) \wedge \\
&\qquad \varphi \subseteq \delta \wedge \varphi, \delta \text{ are preorders } \wedge \\
&\qquad \forall s.\ MR(s) \text{ monotone} \wedge \\
&\qquad \forall s.\ \forall (W, \mathbf{M}_1, M_2) \in MR(s).\ Bij(s) \text{ pbijective} \wedge \\
&\qquad\quad \mathrm{dom}_1(Bij(s)) \subseteq \mathcal{L}_1.\mathrm{mdom}(\mathbf{M}_1) \wedge \mathrm{dom}_2(Bij(s)) \subseteq \mathcal{L}_2.\mathrm{mdom}(M_2) \,\} \\
\mathrm{World}_n &\stackrel{\text{def}}{=} \{\, W = (k, \omega, GR) \mid k < n \wedge \exists m.\ \omega \in \mathrm{Island}_k^m \wedge GR \in \mathbb{P}(\mathcal{L}_1.\mathrm{Mem} \times \mathcal{L}_2.\mathrm{Mem}) \,\} \\
\mathrm{World} &\stackrel{\text{def}}{=} \textstyle\bigcup_{n \in \mathbb{N}} \mathrm{World}_n
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{lev}(W) &\stackrel{\text{def}}{=} W.k \\
\\
\lfloor (\iota_1, \ldots, \iota_m) \rfloor_k &\stackrel{\text{def}}{=} (\lfloor \iota_1 \rfloor_k, \ldots, \lfloor \iota_m \rfloor_k) \\
\lfloor (s, S, \delta, \varphi, MR, Bij) \rfloor_k &\stackrel{\text{def}}{=} (s, S, \delta, \varphi, \lfloor MR \rfloor_k, Bij) \\
\lfloor MR \rfloor_k &\stackrel{\text{def}}{=} \lambda s.\ \lfloor MR(s) \rfloor_k \\
\lfloor R \rfloor_k &\stackrel{\text{def}}{=} \{\, (W, \mathbf{M}_1, M_2) \in R \mid \mathrm{lev}(W) < k \,\} \\
\\
\triangleright(0, \omega, GR) &\stackrel{\text{def}}{=} (0, \omega, GR) \\
\triangleright(k+1, \omega, GR) &\stackrel{\text{def}}{=} (k, \lfloor \omega \rfloor_k GR)
\end{aligned}
$$

$$
\begin{aligned}
(k', \omega', GR') \sqsupseteq (k, \omega, GR) &\stackrel{\text{def}}{=} k' \le k \wedge \omega' \sqsupseteq \lfloor \omega \rfloor_{k'} \wedge GR' = GR \\
(\iota'_1, \ldots, \iota'_{m'}) \sqsupseteq (\iota_1, \ldots, \iota_m) &\stackrel{\text{def}}{=} m' \ge m \wedge \forall j \in \{1 \ldots m\}.\ \iota'_j \sqsupseteq \iota_j \\
(s', S', \delta', \varphi', MR', Bij') \sqsupseteq (s, S, \delta, \varphi, MR, Bij) &\stackrel{\text{def}}{=} (S', \delta', \varphi', MR', Bij') = (S, \delta, \varphi, MR, Bij) \wedge (s, s') \in \delta \\
\\
(k', \omega', GR') \sqsupseteq_{\mathrm{pub}} (k, \omega, GR) &\stackrel{\text{def}}{=} k' \le k \wedge \omega' \sqsupseteq_{\mathrm{pub}} \lfloor \omega \rfloor_{k'} \wedge GR' = GR \\
(\iota'_1, \ldots, \iota'_{m'}) \sqsupseteq_{\mathrm{pub}} (\iota_1, \ldots, \iota_m) &\stackrel{\text{def}}{=} m' \ge m \wedge \forall j \in \{1 \ldots m\}.\ \iota'_j \sqsupseteq_{\mathrm{pub}} \iota_j \\
(s', S', \delta', \varphi', MR', Bij') \sqsupseteq_{\mathrm{pub}} (s, S, \delta, \varphi, MR, Bij) &\stackrel{\text{def}}{=} (S', \delta', \varphi', MR', Bij') = (S, \delta, \varphi, MR, Bij) \wedge (s, s') \in \varphi
\end{aligned}
$$

$$
\begin{array}{rcl}
\mathcal{M}(W) & \stackrel{\text{def}}{=} & \{\, (\mathbf{M}_1, M_2) \mid \mathrm{lev}(W) > 0 \implies \exists \mathbf{M}_1^1, \ldots, \mathbf{M}_1^{|W.\omega|}, M_2^1, \ldots, M_2^{|W.\omega|}. \\
& & \quad \mathbf{M}_1 \in \mathcal{L}_1.\mathrm{mdisjlist}(\mathbf{M}_1^1, \ldots, \mathbf{M}_1^{|W.\omega|}) \wedge M_2 \in \mathcal{L}_2.\mathrm{mdisjlist}(M_2^1, \ldots, M_2^{|W.\omega|}) \wedge \\
& & \quad (\mathbf{M}_1, M_2) \in W.GR \wedge \forall j.\ (\triangleright W, \mathbf{M}_1^j, M_2^j) \in W.\omega(j).MR(W.\omega(j).s)\,\} \\
\mathcal{B}(W) & \stackrel{\text{def}}{=} & \bigcup_{j \in \{1,\ldots,|W.\omega|\}} W.\omega(j).Bij(W.\omega(j).s) \\
\mathcal{O}(W) & \stackrel{\text{def}}{=} & \{\, (C_1, C_2) \mid (\exists k_1.\ \mathcal{L}_1.\mathrm{obsk}(k_1, C_1) = \mathit{halt} \wedge \exists k_2.\ \mathcal{L}_2.\mathrm{obsk}(k_2, C_2) = \mathit{halt}) \vee \\
& & \quad (\mathcal{L}_1.\mathrm{obsk}(\mathrm{lev}(W), C_1) = \mathit{running} \wedge \mathcal{L}_2.\mathrm{obsk}(\mathrm{lev}(W), C_2) = \mathit{running})\,\}
\end{array}
$$

$$
\begin{array}{rcl}
\iota[\rightsquigarrow s] & \stackrel{\text{def}}{=} & (s, \iota.S, \iota.\delta, \iota.\varphi, \iota.MR, \iota.Bij) \\
W[i \rightsquigarrow s] & \stackrel{\text{def}}{=} & (W.k, W.\omega[i \mapsto W.\omega(i)[\rightsquigarrow s]], W.GR) \\
W +\!\!+ \iota & \stackrel{\text{def}}{=} & (W.k, W.\omega +\!\!+ [\iota], W.GR) \\
\iota^{\text{single}}(MR, Bij) & \stackrel{\text{def}}{=} & (\star, \{\star\}, \{(\star,\star)\}, \{(\star,\star)\}, \lambda\star.\, MR, \lambda\star.\, Bij)
\end{array}
$$

4.2 Properties

Theorem 8 (Bijectivity)**.** $\forall W.\ \forall (\mathbf{M}_1, M_2) \in \mathcal{M}(W).\ \mathcal{B}(W)$ pbijective.

Proof.

- By the definition of $\mathcal{M}$, we have $\mathbf{M}_1^j, M_2^j$'s such that $(\triangleright W, \mathbf{M}_1^j, M_2^j) \in W.\omega(j).MR(W.\omega(j).s)$.
- By the assumptions on islands, for each j, we have
  - $W.\omega(j).Bij(W.\omega(j).s)$ pbijective
  - $\mathrm{dom}_1(W.\omega(j).Bij(W.\omega(j).s)) \subseteq \mathcal{L}_1.\mathrm{mdom}(\mathbf{M}_1^j)$
  - $\mathrm{dom}_2(W.\omega(j).Bij(W.\omega(j).s)) \subseteq \mathcal{L}_1.\mathrm{mdom}(M_2^j)$
- As $\mathbf{M}_1 \in \mathcal{L}_1.\mathrm{mdisjlist}(\mathbf{M}_1^1, \ldots, \mathbf{M}_1^{|W.\omega|})$ and $M_2 \in \mathcal{L}_2.\mathrm{mdisjlist}(M_2^1, \ldots, M_2^{|W.\omega|})$, by assumptions on $\mathcal{L}_1.\mathrm{mdisj}$ and $\mathcal{L}_2.\mathrm{mdisj}$, we have that $\mathcal{L}_1.\mathrm{mdom}(\mathbf{M}_1^j) \cap \mathcal{L}_1.\mathrm{mdom}(\mathbf{M}_1^{j'}) = \emptyset$ and $\mathcal{L}_2.\mathrm{mdom}(M_2^j) \cap \mathcal{L}_2.\mathrm{mdom}(M_2^{j'}) = \emptyset$ for all $j \neq j'$.
- Therefore, $\mathcal{B}(W) = \bigcup_{j \in \{1\ldots|W.\omega|\}} W.\omega(j).Bij(W.\omega(j).s)$ is also a partial bijection.

□

Theorem 9 (Closed under anti-reduction)**.**

$$
\begin{array}{l}
\forall k_1, C_1, C_1', k_2, C_2, C_2', W, W'. \\
\quad C_1 \overset{k_1}{\hookrightarrow} C_1' \wedge C_2 \overset{k_2}{\hookrightarrow} C_2' \wedge (C_1', C_2') \in \mathcal{O}(W') \wedge \mathrm{lev}(W) \leq \mathrm{lev}(W') + \min(k_1, k_2) \\
\quad \implies (C_1, C_2) \in \mathcal{O}(W)
\end{array}
$$

Proof. If C_1' and C_2' halt, then C_1 and C_2 halt. If C_1' and C_2' take at least $\mathrm{lev}(W')$ steps, then C_1 and C_2 take at least $(\mathrm{lev}(W') + \min(k_1, k_2))$ steps. □

Theorem 10. $(\mathrm{World}, \mathrm{lev}, \mathcal{M}, \mathcal{B}, \mathcal{O}, \triangleright, \sqsupseteq, \sqsupseteq_{\text{pub}}) \in \mathrm{WorldSpec}$.

Proof. We need to prove the following.

- $\sqsupseteq, \sqsupseteq_{\text{pub}}$ are preorders $\wedge\ \sqsupseteq_{\text{pub}} \subseteq \sqsupseteq$

- $\forall W' \sqsupseteq W.\ \triangleright W' \sqsupseteq \triangleright W$
- $\forall W' \sqsupseteq_{\text{pub}} W.\ \triangleright W' \sqsupseteq_{\text{pub}} \triangleright W$
- $\forall W.\ \triangleright W \sqsupseteq_{\text{pub}} W$
- $\forall W' \sqsupseteq W.\ \text{lev} W' \leq \text{lev} W$
- $\forall W.\ Wk. > 0 \implies \text{lev}(\triangleright W) = \text{lev}(W) - 1$

These are all simple consequences of definition. □

5 Specification of HIGH

5.1 LangSpec of HIGH

$$
\begin{array}{ll}
\text{Val} & \stackrel{\text{def}}{=} \{\, v \in \text{HVal} \mid \text{ftv}(v) = \emptyset \wedge \text{fv}(v) = \emptyset \,\} \\
\text{Com} & \stackrel{\text{def}}{=} \{\, e \in \text{HExp} \mid \text{ftv}(e) = \emptyset \wedge \text{fv}(e) = \emptyset \,\} \\
\text{Cont} & \stackrel{\text{def}}{=} \{\, K \in \text{HCont} \mid \text{ftv}(K) = \emptyset \wedge \text{fv}(K) = \emptyset \,\} \\
\text{Mem} & \stackrel{\text{def}}{=} \{\, M = (h, \Sigma) \mid h \in \text{HHeap} \wedge \Sigma \in \text{Heap typings} \uplus \text{undef} \,\} \\
\text{Conf} & \stackrel{\text{def}}{=} \{\, (h, e) \mid h \in \text{HHeap} \wedge e \in \text{Com} \,\} \\
\text{plugv}(v, K, M) & \stackrel{\text{def}}{=} \{\, (M.h, K[v]) \,\} \\
\text{plugc}(e, K, M) & \stackrel{\text{def}}{=} \{\, (M.h, K[e]) \,\} \\
\text{step}(h, e) & \stackrel{\text{def}}{=} \begin{cases} (h', e') & \text{if } (h, e) \hookrightarrow (h', e') \\ \mathit{halt} & \text{if } e \text{ is a value} \\ \mathit{fail} & \text{otherwise} \end{cases} \\
\text{mdom}(M) & \stackrel{\text{def}}{=} \{\, \ell \in \text{HLoc} \subseteq \text{Val} \mid \ell \in \text{dom}(M.h) \,\} \\
\text{mdisj}(M_1, M_2) & \stackrel{\text{def}}{=} \{\, M \mid M.h \supseteq M_1.h \uplus M_2.h \wedge \\
 & \qquad ((M.\Sigma = M_1.\Sigma \wedge M_2.\Sigma = \text{undef}) \wedge (M.\Sigma = M_2.\Sigma \wedge M_1.\Sigma = \text{undef})) \,\} \\
\text{oftype}(\tau) & \stackrel{\text{def}}{=} \{\, (v, M) \in \text{Val} \times \text{Mem} \mid M.\Sigma; \emptyset; \emptyset \vdash v : \tau \,\} \\
\text{base}_b(x) & \stackrel{\text{def}}{=} \{\, (x, M) \in \text{Val} \times \text{Mem} \,\} \quad \text{for } x \in [\![b]\!] \\
\text{pair}(v_1, v_2) & \stackrel{\text{def}}{=} \{\, (\langle v_1, v_2 \rangle, M) \in \text{Val} \times \text{Mem} \,\} \\
\text{app}(v_1, v_2) & \stackrel{\text{def}}{=} \{\, e \in \text{Com} \mid \exists x, \tau, e_1.\ v_1 = \lambda x{:}\tau.\, e_1 \wedge e = e_1[v_2/x] \,\} \\
\text{appty}(v, \tau) & \stackrel{\text{def}}{=} \{\, e \in \text{Com} \mid \exists \alpha, e_1.\ v = \Lambda\alpha.e_1 \wedge e = e_1[\tau/\alpha] \,\} \\
\text{pack}(\tau, v) & \stackrel{\text{def}}{=} \{\, (v', M) \in \text{Val} \times \text{Mem} \mid \exists \tau'.\ v' = \mathsf{pack}\ \langle \tau, v \rangle\ \mathsf{as}\ \tau' \,\} \\
\text{roll}(v) & \stackrel{\text{def}}{=} \{\, (v', M) \in \text{Val} \times \text{Mem} \mid \exists \tau.\ v' = \mathsf{roll}_\tau\ v \,\} \\
\text{ref}(v) & \stackrel{\text{def}}{=} \{\, (\ell, M) \in \text{Val} \times \text{Mem} \mid M.h(\ell) = v \,\} \\
\text{asgn}(M, v_1, v_2) & \stackrel{\text{def}}{=} \begin{cases} (M.h[\ell \mapsto v_2], M.\Sigma) & \text{if } v_1 = \ell \wedge \ell \in \text{dom}(M.h) \\ \text{undef} & \text{otherwise} \end{cases} \\
\mathcal{H} & \stackrel{\text{def}}{=} (\text{Val}, \text{Com}, \text{Cont}, \text{Mem}, \text{Conf}, \\
 & \qquad \text{plugv}, \text{plugc}, \text{step}, \text{mdom}, \text{mdisj}, \\
 & \qquad \text{oftype}, \text{base}_b, \text{pair}, \text{app}, \text{appty}, \text{pack}, \text{roll}, \text{ref}, \text{asgn})
\end{array}
$$

Theorem 11.

$$\mathcal{H} \in \text{LangSpec}$$

Proof. We need to prove the following.

- $\forall M, M_1, M_2.\ M \in \text{mdisj}(M_1, M_2) \implies \text{mdom}(M) \supseteq \text{mdom}(M_1) \uplus \text{mdom}(M_2)$

It directly follows from definition. □

6 Specification of LOW

6.1 LangSpec of LOW

$$
\begin{array}{lcl}
\text{List } X & \stackrel{\text{def}}{=} & \{\,(x_0,\ldots,x_{n-1}) \mid n \in \mathbb{N} \wedge x_0,\ldots,x_{n-1} \in X\,\} \\
\text{Loc} & \stackrel{\text{def}}{=} & \{\,\boldsymbol{l} \in \mathbb{N}\,\} \\
\text{Word} & \stackrel{\text{def}}{=} & \{\,w \in \mathbb{N}\,\} \\
\mathbf{v} \in \text{Val} & ::= & \underline{w} \mid \widehat{\boldsymbol{l}} \quad \text{for } w \in \text{Word}, \boldsymbol{l} \in \text{Loc} \\
\text{lv} \in \text{Lvalue} & ::= & \lfloor r \rfloor \mid \langle a \rangle_{\text{s}} \mid \langle r - o \rangle_{\text{s}} \mid \langle \boldsymbol{l} : o \rangle_{\text{h}} \mid \langle r + o \rangle_{\text{h}} \quad \text{for } r \in \text{Register}, a \in \text{PAddr}, \boldsymbol{l} \in \text{Loc}, o \in \mathbb{N} \\
\text{rv} \in \text{Rvalue} & ::= & \text{lv} \mid \mathbf{v} \quad \text{for lv} \in \text{Lvalue}, \mathbf{v} \in \text{Val} \\
\text{Com} & \stackrel{\text{def}}{=} & \{\,\mathbf{e} = (\text{cpc}, \text{kpc}, \text{vloc}, \text{data}) \in \text{Rvalue} \times \text{Rvalue} \times \text{Lvalue} \times \mathbb{P}(\text{Mem})\,\} \\
\text{Cont} & \stackrel{\text{def}}{=} & \{\,\mathbf{K} = (\text{kpc}, \text{vloc}) \in \text{PAddr} \times \text{Lvalue}\,\} \\
\text{CodeFrag} & \stackrel{\text{def}}{=} & \text{PAddr} \rightharpoonup_{\text{fin}} \text{Instruction} \\
\text{RegFile} & \stackrel{\text{def}}{=} & (\text{Register} \setminus \{\text{sp}\} \to \text{Val}) \uplus \{\,\text{undef}\,\} \\
\text{Stack} & \stackrel{\text{def}}{=} & \text{List Val} \uplus \{\,\text{undef}\,\} \\
\text{Heap} & \stackrel{\text{def}}{=} & \text{Loc} \rightharpoonup_{\text{fin}} \text{List Val} \\
\text{Table} & \stackrel{\text{def}}{=} & (\text{Loc} \rightharpoonup_{\text{fin}} \mathbb{N} \times \text{PAddr}) \uplus \{\,\text{undef}\,\} \\
\text{SysHeap} & \stackrel{\text{def}}{=} & (\text{PAddr} \rightharpoonup \text{Word}) \uplus \{\,\text{undef}\,\} \\
\text{Mem} & \stackrel{\text{def}}{=} & \{\,\mathbf{M} = (\text{code}, \text{reg}, \text{stk}, \text{hp}, \text{tab}, \text{shp}) \\
 & & \quad \in \text{CodeFrag} \times \text{RegFile} \times \text{Stack} \times \text{Heap} \times \text{Table} \times \text{SysHeap}\,\} \\
\text{Conf} & \stackrel{\text{def}}{=} & \text{PConf}
\end{array}
$$

$$
\begin{array}{lcl}
|\mathbf{v}| & \stackrel{\text{def}}{=} & \begin{cases} w & \text{if } \mathbf{v} = \underline{w} \\ \boldsymbol{l} & \text{if } \mathbf{v} = \widehat{\boldsymbol{l}} \end{cases} \\
\mathbf{M}(\mathbf{v}) & \stackrel{\text{def}}{=} & \mathbf{v} \\
\mathbf{M}(\lfloor r \rfloor) & \stackrel{\text{def}}{=} & \mathbf{M}.\text{reg}(r) \\
\mathbf{M}(\langle a \rangle_{\text{s}}) & \stackrel{\text{def}}{=} & \mathbf{M}.\text{stk}(a) \\
\mathbf{M}(\langle r - o \rangle_{\text{s}}) & \stackrel{\text{def}}{=} & \mathbf{M}.\text{stk}(|\mathbf{M}.\text{reg}(r)| - o) \\
\mathbf{M}(\langle \boldsymbol{l} : o \rangle_{\text{h}}) & \stackrel{\text{def}}{=} & \mathbf{M}.\text{hp}(\boldsymbol{l})(o) \\
\mathbf{M}(\langle r + o \rangle_{\text{h}}) & \stackrel{\text{def}}{=} & \mathbf{M}.\text{hp}(|\mathbf{M}.\text{reg}(r)|)(o)
\end{array}
$$

$$
\begin{array}{lcl}
\mathbf{M}[a \mapsto \iota_1,\ldots,\iota_n]_{\text{code}} & \stackrel{\text{def}}{=} & (\mathbf{M}.\text{code}[a \mapsto \iota_1,\ldots,\iota_n], \mathbf{M}.\text{reg}, \mathbf{M}.\text{stk}, \mathbf{M}.\text{hp}, \mathbf{M}.\text{tab}, \mathbf{M}.\text{shp}) \\
\mathbf{M}[r \mapsto \mathbf{v}]_{\text{reg}} & \stackrel{\text{def}}{=} & (\mathbf{M}.\text{code}, \mathbf{M}.\text{reg}[r \mapsto \mathbf{v}], \mathbf{M}.\text{stk}, \mathbf{M}.\text{hp}, \mathbf{M}.\text{tab}, \mathbf{M}.\text{shp}) \\
\mathbf{M}[{+\!\!+}\,\mathbf{v}_0,\ldots,\mathbf{v}_{j-1}]_{\text{stk}} & \stackrel{\text{def}}{=} & (\mathbf{M}.\text{code}, \mathbf{M}.\text{reg}, \mathbf{M}.\text{stk} {+\!\!+} (\mathbf{v}_0,\ldots,\mathbf{v}_{j-1}), \mathbf{M}.\text{hp}, \mathbf{M}.\text{tab}, \mathbf{M}.\text{shp}) \\
\mathbf{M}[-k]_{\text{stk}} & \stackrel{\text{def}}{=} & (\mathbf{M}.\text{code}, \mathbf{M}.\text{reg}, (\mathbf{v}_0,\ldots,\mathbf{v}_{n-k-1}), \mathbf{M}.\text{hp}, \mathbf{M}.\text{tab}, \mathbf{M}.\text{shp}) \\
 & & \quad \text{if } \mathbf{M}.\text{stk} = (\mathbf{v}_0,\ldots,\mathbf{v}_{n-1}) \wedge n \geq k \\
\mathbf{M}[j \mapsto \mathbf{v}]_{\text{stk}} & \stackrel{\text{def}}{=} & (\mathbf{M}.\text{code}, \mathbf{M}.\text{reg}, \mathbf{M}.\text{stk}[j \mapsto \mathbf{v}], \mathbf{M}.\text{hp}, \mathbf{M}.\text{tab}, \mathbf{M}.\text{shp}) \quad \text{if } j < |\mathbf{M}.\text{stk}| \\
\mathbf{M}[\boldsymbol{l} : o \mapsto \mathbf{v}]_{\text{hp}} & \stackrel{\text{def}}{=} & (\mathbf{M}.\text{code}, \mathbf{M}.\text{reg}, \mathbf{M}.\text{stk}, \mathbf{M}.\text{hp}[\boldsymbol{l} \mapsto (\mathbf{v}_0,\ldots,\mathbf{v}_{o-1}, \mathbf{v}, \mathbf{v}_{o+1},\ldots,\mathbf{v}_{n-1})], \\
 & & \quad \mathbf{M}.\text{tab}, \mathbf{M}.\text{shp}) \\
 & & \quad \text{if } \mathbf{M}.\text{hp}(\boldsymbol{l}) = (\mathbf{v}_0,\ldots,\mathbf{v}_{n-1}) \wedge o < n \\
\mathbf{M}[[T, S]] & \stackrel{\text{def}}{=} & (\mathbf{M}.\text{code}, \mathbf{M}.\text{reg}, \mathbf{M}.\text{stk}, \mathbf{M}.\text{hp}, T, S)
\end{array}
$$

$$\mathrm{phyv}(\mathbf{M})(\mathbf{v}) \stackrel{\text{def}}{=} \begin{cases} \underline{w} & \text{if } \mathbf{v} = \underline{w} \\ \widehat{a} & \text{if } \mathbf{v} = \widehat{\boldsymbol{l}} \wedge \mathbf{M}.\mathrm{tab}(\boldsymbol{l}) = (n, a) \\ \text{undef} & \text{otherwise} \end{cases}$$

$$\mathrm{phyh}(\mathbf{M}) \stackrel{\text{def}}{=} \biguplus_{\substack{\mathbf{M}.\mathrm{tab}(\boldsymbol{l})=(n,a) \,\wedge\, n>0 \\ \wedge\, \mathbf{M}.\mathrm{hp}(\boldsymbol{l})=(\mathbf{v}_0,\ldots,\mathbf{v}_{n-1})}} [a \mapsto \mathrm{phyv}(\mathbf{M})(\mathbf{v}_0), \ldots, \mathrm{phyv}(\mathbf{M})(\mathbf{v}_{n-1})]$$

$$\begin{aligned} \mathbf{M} \text{ repr } \Phi \stackrel{\text{def}}{=}\ & \Phi.\mathrm{code} \supseteq \mathbf{M}.\mathrm{code} \wedge \\ & \Phi.\mathrm{reg} \supseteq \mathrm{phyv}(\mathbf{M}) \circ \mathbf{M}.\mathrm{reg} \wedge \Phi.\mathrm{reg}(\mathrm{sp}) = \underline{|\mathbf{M}.\mathrm{stk}|} \wedge \\ & \forall j < |\mathbf{M}.\mathrm{stk}|.\ \Phi.\mathrm{stk}(j) = \mathrm{phyv}(\mathbf{M})(\mathbf{M}.\underline{\mathrm{stk}(j)}) \wedge \\ & \Phi.\mathrm{hp} \supseteq \mathrm{phyh}(\mathbf{M}) \uplus \mathbf{M}.\mathrm{shp} \wedge \\ & \forall \boldsymbol{l}, n, a.\ \mathbf{M}.\mathrm{tab}(\boldsymbol{l}) = (n, a) \wedge n > 0 \implies |\mathbf{M}.\mathrm{hp}(\boldsymbol{l})| = n \end{aligned}$$

$$\begin{aligned} \mathrm{plugv}(\mathbf{v}, \mathbf{K}, \mathbf{M}) \stackrel{\text{def}}{=}\ & \{\, (\Phi, \mathrm{pc}) \in \mathrm{Conf} \mid \mathbf{M} \text{ repr } \Phi \wedge \\ & \quad \mathrm{pc} = \mathbf{K}.\mathrm{kpc} \wedge \mathbf{M}(\mathbf{K}.\mathrm{vloc}) = \mathbf{v} \,\} \end{aligned}$$

$$\begin{aligned} \mathrm{plugc}(\mathbf{e}, \mathbf{K}, \mathbf{M}) \stackrel{\text{def}}{=}\ & \{\, (\Phi, \mathrm{pc}) \in \mathrm{Conf} \mid \mathbf{M} \text{ repr } \Phi \wedge \mathbf{M} \in \mathbf{e}.\mathrm{data} \wedge \\ & \quad \underline{\mathrm{pc}} = \mathbf{M}(\mathbf{e}.\mathrm{cpc}) \wedge \mathbf{M}(\mathbf{e}.\mathrm{kpc}) = \underline{\mathbf{K}.\mathrm{kpc}} \wedge \mathbf{e}.\mathrm{vloc} = \mathbf{K}.\mathrm{vloc} \,\} \end{aligned}$$

$$\mathrm{step}(\Phi, \mathrm{pc}) \stackrel{\text{def}}{=} R \quad \text{with } (\Phi, \mathrm{pc}) \hookrightarrow R$$

$$\mathrm{mdom}(\mathbf{M}) \stackrel{\text{def}}{=} \{\, \widehat{\boldsymbol{l}} \in \mathrm{Val} \mid \boldsymbol{l} \in \mathrm{dom}(\mathbf{M}.\mathrm{hp}) \,\}$$

$$\begin{aligned} \mathrm{mdisj}(\mathbf{M}_1, \mathbf{M}_2) \stackrel{\text{def}}{=}\ & \{\, \mathbf{M} \in \mathrm{Mem} \mid \\ & \quad \mathbf{M}.\mathrm{code} \supseteq \mathbf{M}_1.\mathrm{code} \uplus \mathbf{M}_2.\mathrm{code} \wedge \\ & \quad \mathbf{M}.\mathrm{hp} \supseteq \mathbf{M}_1.\mathrm{hp} \uplus \mathbf{M}_2.\mathrm{hp} \wedge \\ & \quad \mathrm{nosh}(\mathbf{M}.\mathrm{reg}, \mathbf{M}_1.\mathrm{reg}, \mathbf{M}_2.\mathrm{reg}) \wedge \\ & \quad \mathrm{nosh}(\mathbf{M}.\mathrm{stk}, \mathbf{M}_1.\mathrm{stk}, \mathbf{M}_2.\mathrm{stk}) \wedge \\ & \quad \mathrm{nosh}(\mathbf{M}.\mathrm{tab}, \mathbf{M}_1.\mathrm{tab}, \mathbf{M}_2.\mathrm{tab}) \wedge \\ & \quad \mathrm{nosh}(\mathbf{M}.\mathrm{shp}, \mathbf{M}_1.\mathrm{shp}, \mathbf{M}_2.\mathrm{shp}) \,\} \end{aligned}$$

$$\begin{aligned} \mathrm{nosh}(X, X_1, X_2) \stackrel{\text{def}}{=}\ & (X_1 \neq \text{undef} \implies X_2{=}\text{undef} \wedge X{=}X_1) \wedge \\ & (X_2 \neq \text{undef} \implies X_1{=}\text{undef} \wedge X{=}X_2) \end{aligned}$$

$$\mathbf{M}_1 \uplus \mathbf{M}_2 \stackrel{\text{def}}{=} \begin{cases} (\mathbf{M}_1.\mathrm{code} \uplus \mathbf{M}_2.\mathrm{code},\ \mathbf{M}_i.\mathrm{reg},\ \mathbf{M}_j.\mathrm{stk},\ \mathbf{M}_1.\mathrm{hp} \uplus \mathbf{M}_2.\mathrm{hp},\ \mathbf{M}_k.\mathrm{tab},\ \mathbf{M}_l.\mathrm{shp}) \\ \qquad \text{if } \mathbf{M}_1.\mathrm{code} \uplus \mathbf{M}_2.\mathrm{code} \neq \text{undef} \wedge \mathbf{M}_1.\mathrm{hp} \uplus \mathbf{M}_2.\mathrm{hp} \neq \text{undef} \wedge \\ \qquad\quad \mathbf{M}_{3-i}.\mathrm{reg} = \text{undef} \wedge \mathbf{M}_{3-j}.\mathrm{stk} = \text{undef} \wedge \\ \qquad\quad \mathbf{M}_{3-k}.\mathrm{tab} = \text{undef} \wedge \mathbf{M}_{3-l}.\mathrm{shp} = \text{undef} \\ \text{undef} \qquad \text{otherwise} \end{cases}$$

$$\begin{aligned} \mathbf{M}_1 \supseteq \mathbf{M}_2 \stackrel{\text{def}}{=}\ & \mathbf{M}_1.\mathrm{code} \supseteq \mathbf{M}_2.\mathrm{code} \wedge \\ & \mathbf{M}_1.\mathrm{hp} \supseteq \mathbf{M}_2.\mathrm{hp} \wedge \\ & (\mathbf{M}_2.\mathrm{reg} \neq \text{undef} \implies \mathbf{M}_1.\mathrm{reg} = \mathbf{M}_2.\mathrm{reg}) \wedge \\ & (\mathbf{M}_2.\mathrm{stk} \neq \text{undef} \implies \mathbf{M}_1.\mathrm{stk} = \mathbf{M}_2.\mathrm{stk}) \wedge \\ & (\mathbf{M}_2.\mathrm{tab} \neq \text{undef} \implies \mathbf{M}_1.\mathrm{tab} = \mathbf{M}_2.\mathrm{tab}) \wedge \\ & (\mathbf{M}_2.\mathrm{shp} \neq \text{undef} \implies \mathbf{M}_1.\mathrm{shp} = \mathbf{M}_2.\mathrm{shp}) \end{aligned}$$

$$
\begin{array}{ll}
\mathrm{oftype}(\tau) & \stackrel{\text{def}}{=} \{\, (\mathbf{v},\mathbf{M}) \in \mathrm{Val}\times\mathrm{Mem} \mid \\
& \quad \forall \tau_1,\tau_2.\ \tau = \tau_1 \to \tau_2 \implies \exists \boldsymbol{l}, w.\ \mathbf{v} = \widehat{\boldsymbol{l}} \wedge \mathbf{M}.\mathrm{hp}(\boldsymbol{l})(0) = \underline{w} \wedge \\
& \quad \forall \alpha,\tau'.\ \tau = \forall \alpha.\,\tau' \implies \exists \boldsymbol{l}, w.\ \mathbf{v} = \widehat{\boldsymbol{l}} \wedge \mathbf{M}.\mathrm{hp}(\boldsymbol{l})(0) = \underline{w} \,\} \\
\mathrm{base}_b(x) & \stackrel{\text{def}}{=} \{\, (\mathbf{v},\mathbf{M}) \in \mathrm{Val}\times\mathrm{Mem} \mid \mathbf{v} \text{ is a representation of } x \,\} \quad \text{for } x \in [\![b]\!] \\
\mathrm{pair}(\mathbf{v}_1,\mathbf{v}_2) & \stackrel{\text{def}}{=} \{\, (\mathbf{v},\mathbf{M}) \in \mathrm{Val}\times\mathrm{Mem} \mid \exists \boldsymbol{l}.\ \mathbf{v} = \widehat{\boldsymbol{l}} \wedge \mathbf{M}.\mathrm{hp}(\boldsymbol{l})(0) = \mathbf{v}_1 \wedge \mathbf{M}.\mathrm{hp}(\boldsymbol{l})(1) = \mathbf{v}_2 \,\} \\
\mathrm{app}(\mathbf{v}_1,\mathbf{v}_2) & \stackrel{\text{def}}{=} \{\, \mathbf{e} \in \mathrm{Com} \mid \exists \boldsymbol{l}.\ \mathbf{v}_1 = \widehat{\boldsymbol{l}} \wedge \mathbf{e}.\mathrm{cpc} = \langle \boldsymbol{l} : 0 \rangle_{\mathrm{h}} \wedge \mathbf{e}.\mathrm{kpc} = \lfloor \mathrm{wk}_0 \rfloor \wedge \mathbf{e}.\mathrm{vloc} = \lfloor \mathrm{wk}_5 \rfloor \wedge \\
& \qquad \mathbf{e}.\mathrm{data} = \{\, \mathbf{M} \in \mathrm{Mem} \mid \mathbf{M}.\mathrm{reg}(\mathrm{wk}_1) = \mathbf{v}_1 \wedge \mathbf{M}.\mathrm{reg}(\mathrm{wk}_2) = \mathbf{v}_2 \,\} \,\} \\
\mathrm{appty}(\mathbf{v},\tau) & \stackrel{\text{def}}{=} \{\, \mathbf{e} \in \mathrm{Com} \mid \exists \boldsymbol{l}.\ \mathbf{v} = \widehat{\boldsymbol{l}} \wedge \mathbf{e}.\mathrm{cpc} = \langle \boldsymbol{l} : 0 \rangle_{\mathrm{h}} \wedge \mathbf{e}.\mathrm{kpc} = \lfloor \mathrm{wk}_0 \rfloor \wedge \mathbf{e}.\mathrm{vloc} = \lfloor \mathrm{wk}_5 \rfloor \wedge \\
& \qquad \mathbf{e}.\mathrm{data} = \{\, \mathbf{M} \in \mathrm{Mem} \mid \mathbf{M}.\mathrm{reg}(\mathrm{wk}_1) = \mathbf{v} \,\} \,\} \\
\mathrm{pack}(\tau,\mathbf{v}) & \stackrel{\text{def}}{=} \{\, (\mathbf{v}',\mathbf{M}) \in \mathrm{Val}\times\mathrm{Mem} \mid \mathbf{v}' = \mathbf{v} \,\} \\
\mathrm{roll}(\mathbf{v}) & \stackrel{\text{def}}{=} \{\, (\mathbf{v}',\mathbf{M}) \in \mathrm{Val}\times\mathrm{Mem} \mid \mathbf{v}' = \mathbf{v} \,\} \\
\mathrm{ref}(\mathbf{v}) & \stackrel{\text{def}}{=} \{\, (\mathbf{v}',\mathbf{M}) \in \mathrm{Val}\times\mathrm{Mem} \mid \exists \boldsymbol{l}.\ \mathbf{v}' = \widehat{\boldsymbol{l}} \wedge \mathbf{M}.\mathrm{hp}(\boldsymbol{l})(0) = \mathbf{v} \,\} \\
\mathrm{asgn}(\mathbf{M},\mathbf{v}_1,\mathbf{v}_2) & \stackrel{\text{def}}{=} \begin{cases} \mathbf{M}[\boldsymbol{l} : 0 \mapsto \mathbf{v}_2]_{\mathrm{hp}} & \text{if } \mathbf{v}_1 = \widehat{\boldsymbol{l}} \wedge |\mathbf{M}.\mathrm{hp}(\boldsymbol{l})| > 0 \\ \mathrm{undef} & \text{otherwise} \end{cases} \\
\mathcal{L} & \stackrel{\text{def}}{=} (\mathrm{Val}, \mathrm{Com}, \mathrm{Cont}, \mathrm{Mem}, \mathrm{Conf}, \\
& \quad \mathrm{plugv}, \mathrm{plugc}, \mathrm{step}, \mathrm{mdom}, \mathrm{mdisj}, \\
& \quad \mathrm{oftype}, \mathrm{base}_b, \mathrm{pair}, \mathrm{app}, \mathrm{appty}, \mathrm{pack}, \mathrm{roll}, \mathrm{ref}, \mathrm{asgn})
\end{array}
$$

Notation.

$$
\begin{array}{ll}
[\mathrm{bg} \Mapsto \mathrm{instrs}] & \stackrel{\text{def}}{=} [\mathrm{bg} \mapsto \mathrm{instrs}(0), \ldots, \mathrm{instrs}(|\mathrm{instrs}| - 1)] \\
\{C\}_{\mathrm{code}} & \stackrel{\text{def}}{=} (C, \mathrm{undef}, \mathrm{undef}, \emptyset, \mathrm{undef}, \mathrm{undef}) \in \mathrm{Mem} \\
\{H\}_{\mathrm{heap}} & \stackrel{\text{def}}{=} (\emptyset, \mathrm{undef}, \mathrm{undef}, H, \mathrm{undef}, \mathrm{undef}) \in \mathrm{Mem}
\end{array}
$$

Lemma 6. For all $\mathbf{M}_1$, $\mathbf{M}_2$ and $\mathbf{M} \in \mathrm{mdisj}(\mathbf{M}_1, \mathbf{M}_2)$,

$$\mathbf{M} \supseteq \mathbf{M}_1 \uplus \mathbf{M}_2 \ .$$

Proof. It immediately follows from the definitions of $\mathrm{mdisj}, \uplus, \supseteq$. □

Theorem 12.

$$\mathcal{L} \in \mathrm{LangSpec}$$

Proof. We need to prove the following.

- $\forall m, m_1, m_2.\ m \in \mathrm{mdisj}(m_1, m_2) \implies \mathrm{mdom}(m) \supseteq \mathrm{mdom}(m_1) \uplus \mathrm{mdom}(m_2)$

It directly follows from definition. □

6.2 Garbage Collector Specification

$$\mathbf{v} \text{ live in } \mathbf{M} \stackrel{\text{def}}{=} \begin{cases} \top & \text{if } \mathbf{v} = \underline{w} \\ \exists n, a.\ \mathbf{M}.\mathrm{tab}(\boldsymbol{l}) = (n, a) \wedge n > 0 & \text{if } \mathbf{v} = \widehat{\boldsymbol{l}} \end{cases}$$

$$\mathrm{reach}_0(\mathbf{M}) \stackrel{\text{def}}{=} \{\, \boldsymbol{l} \mid \exists r \in \mathrm{Register}.\ \widehat{\boldsymbol{l}} = \mathbf{M}.\mathrm{reg}(r) \,\} \cup \{\, \boldsymbol{l} \mid \exists j < |\mathbf{M}.\mathrm{stk}|.\ \widehat{\boldsymbol{l}} = \mathbf{M}.\mathrm{stk}(j) \,\}$$

$$\mathrm{reach}_{i+1}(\mathbf{M}) \stackrel{\text{def}}{=} \mathrm{reach}_i(\mathbf{M}) \cup \{\, \boldsymbol{l} \mid \exists \boldsymbol{l}' \in \mathrm{reach}_i(\mathbf{M}).\ \exists j.\ \widehat{\boldsymbol{l}} = \mathbf{M}.\mathrm{hp}(\boldsymbol{l}')(j) \,\}$$

$$\mathrm{reach}(\mathbf{M}) \stackrel{\text{def}}{=} \textstyle\bigcup_{i \in \mathbb{N}} \mathrm{reach}_i(\mathbf{M})$$

$$\begin{aligned}
\mathrm{AllocSpec} \stackrel{\text{def}}{=} \{\, & \mathcal{A} \in \mathrm{PAddr} \to \\
& \quad \{\, (\mathrm{init}, \mathrm{alloc}, \mathrm{instrs}, I) \in \mathrm{PAddr} \times \mathrm{PAddr} \times \mathrm{List\ Instruction} \times \mathbb{P}(\mathrm{Table} \times \mathrm{SysHeap}) \,\} \mid \\
& \quad \forall \mathrm{gcbg}, \Phi, \mathrm{pc}. \\
& \qquad \Phi.\mathrm{code} \supseteq [\mathrm{gcbg} \Rightarrow \mathcal{A}(\mathrm{gcbg}).\mathrm{instrs}] \wedge \Phi.\mathrm{reg}(\mathrm{wk}_4) = \underline{\mathrm{pc}} \\
& \qquad \Longrightarrow\ \exists k, \mathbf{M}', \Phi'. \\
& \qquad\quad (\Phi, \mathcal{A}(\mathrm{gcbg}).\mathrm{init}) \overset{k}{\hookrightarrow} (\Phi', \mathrm{pc}) \wedge \\
& \qquad\quad \mathbf{M}' \text{ repr } \Phi' \wedge \mathbf{M}' \in \mathcal{A}.GR(\mathrm{gcbg}) \wedge \mathbf{M}' \in \mathcal{A}.MR(\mathrm{gcbg}) \wedge \\
& \qquad\quad \Phi'.\mathrm{code} = \Phi.\mathrm{code} \wedge \mathbf{M}'.\mathrm{code} = [\mathrm{gcbg} \Rightarrow \mathcal{A}(\mathrm{gcbg}).\mathrm{instrs}] \wedge \\
& \quad \forall \mathrm{gcbg}, \mathbf{M}, \Phi, \mathrm{pc}, n. \\
& \qquad \mathbf{M} \text{ repr } \Phi \wedge \mathbf{M} \in \mathcal{A}.GR(\mathrm{gcbg}) \wedge \mathbf{M} \in \mathcal{A}.MR(\mathrm{gcbg}) \wedge \\
& \qquad \mathbf{M}.\mathrm{reg}(\mathrm{wk}_4) = \underline{\mathrm{pc}} \wedge \mathbf{M}.\mathrm{reg}(\mathrm{wk}_5) = \underline{n} \\
& \qquad \Longrightarrow\ \exists k, \Phi', \mathbf{M}', T, S, w, \boldsymbol{l}, w_0, \ldots, w_{n-1}. \\
& \qquad\quad (\Phi, \mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}) \overset{k}{\hookrightarrow} (\Phi', \mathrm{pc}) \wedge \\
& \qquad\quad \mathbf{M}' \text{ repr } \Phi' \wedge \mathbf{M}' \in \mathcal{A}.GR(\mathrm{gcbg}) \wedge \mathbf{M}' \in \mathcal{A}.MR(\mathrm{gcbg}) \wedge \\
& \qquad\quad \mathbf{M}' = \mathbf{M}[[T, S]][\mathrm{wk}_4 \mapsto \underline{w}]_{\mathrm{reg}}[\mathrm{wk}_5 \mapsto \widehat{\boldsymbol{l}}]_{\mathrm{reg}} \uplus \{[\boldsymbol{l} \mapsto (\underline{w_0}, \ldots, \underline{w_{n-1}})]\}_{\mathrm{heap}} \,\}
\end{aligned}$$

$$\mathcal{A}.GR(\mathrm{gcbg}) \stackrel{\text{def}}{=} \{\, \mathbf{M} \in \mathrm{Mem} \mid \forall \boldsymbol{l} \in \mathrm{reach}(\mathbf{M}).\ \widehat{\boldsymbol{l}} \text{ live in } \mathbf{M} \,\}$$

$$\mathcal{A}.MR(\mathrm{gcbg}) \stackrel{\text{def}}{=} \{\, \mathbf{M} \in \mathrm{Mem} \mid (\mathbf{M}.\mathrm{tab}, \mathbf{M}.\mathrm{shp}) \in \mathcal{A}(\mathrm{gcbg}).I \wedge \mathbf{M}.\mathrm{code} \supseteq [\mathrm{gcbg} \Rightarrow \mathcal{A}(\mathrm{gcbg}).\mathrm{instrs}] \,\}$$

7 Low High Relations

7.1 Initial Worlds

Let $\mathcal{A} \in \text{AllocSpec}$.

$$W_k^\circ(\mathcal{A}, \text{gcbg}) \stackrel{\text{def}}{=} (k, [\iota^{\text{regstk}}, \iota^{\text{htyping}}, \iota^{\text{gc}}(\mathcal{A}, \text{gcbg})], GR^\circ(\mathcal{A}, \text{gcbg}))$$

$$\begin{array}{ll}
S_{\text{regstk}} & \stackrel{\text{def}}{=} \{\, s = (\text{reg}, \text{stk}) \in (\{\text{sv}_0, \ldots, \text{sv}_4\} \to \text{Val}) \times \text{List Val} \,\} \\
\delta_{\text{regstk}} & \stackrel{\text{def}}{=} \{\, (s, s') \in S_{\text{regstk}} \times S_{\text{regstk}} \,\} \\
\varphi_{\text{regstk}} & \stackrel{\text{def}}{=} \{\, (s, s') \in S_{\text{regstk}} \times S_{\text{regstk}} \mid s' = s \,\} \\
MR_{\text{regstk}}(s) & \stackrel{\text{def}}{=} \{\, (W, \mathbf{M}, M) \mid \mathbf{M}.\text{stk} = s.\text{stk} \wedge \forall j.\ \mathbf{M}.\text{reg}(\text{sv}_j) = s.\text{reg}(\text{sv}_j) \,\} \\
\iota^{\text{regstk}} & \stackrel{\text{def}}{=} ((\lambda r.\ \underline{0}, []), S_{\text{regstk}}, \delta_{\text{regstk}}, \varphi_{\text{regstk}}, MR_{\text{regstk}}, \lambda s.\ \emptyset)
\end{array}$$

$$\begin{array}{ll}
S_{\text{htyping}} & \stackrel{\text{def}}{=} \{\, \Sigma \in \text{Heap typings} \,\} \\
\delta_{\text{htyping}} & \stackrel{\text{def}}{=} \{\, (\Sigma, \Sigma') \mid \Sigma \subseteq \Sigma' \,\} \\
\varphi_{\text{htyping}} & \stackrel{\text{def}}{=} \delta_{\text{htyping}} \\
MR_{\text{htyping}}(\Sigma) & \stackrel{\text{def}}{=} \{\, (W, \mathbf{M}, M) \mid M.\Sigma = \Sigma \,\} \\
\iota^{\text{htyping}} & \stackrel{\text{def}}{=} (\emptyset, S_{\text{htyping}}, \delta_{\text{htyping}}, \varphi_{\text{htyping}}, MR_{\text{htyping}}, \lambda\Sigma.\ \emptyset)
\end{array}$$

$$\iota^{\text{gc}}(\mathcal{A}, \text{gcbg}) \stackrel{\text{def}}{=} \iota^{\text{single}}(\{\, (W, \mathbf{M}, M) \mid \mathbf{M} \in \mathcal{A}.MR(\text{gcbg}) \,\}, \emptyset)$$

$$GR^\circ(\mathcal{A}, \text{gcbg}) \stackrel{\text{def}}{=} \{\, (\mathbf{M}, M) \mid \mathbf{M} \in \mathcal{A}.GR(\text{gcbg}) \wedge \vdash M.h : M.\Sigma \,\}$$

$$\iota^{\text{code}}(\text{code}) \stackrel{\text{def}}{=} \iota^{\text{single}}(\{\, (W, \mathbf{M}, M) \mid \mathbf{M}.\text{code} \supseteq \text{code} \,\}, \emptyset)$$

7.2 Program Equivalence

$$\begin{array}{rl}
\mathcal{L}.\text{Prog} & \stackrel{\text{def}}{=} \{\, p \in \text{PAddr} \times \text{PAddr} \to \text{List Instruction} \,\} \\
\mathcal{H}.\text{Prog} & \stackrel{\text{def}}{=} \{\, e \in \text{HExp} \mid \text{floc}(e) = \emptyset \,\}
\end{array}$$

$$\begin{array}{rcl}
\mathcal{G}[\![\cdot]\!]\rho & \stackrel{\text{def}}{=} & \{\, (W, \mathbf{v}, \emptyset) \mid W \in \text{World} \wedge \mathbf{v} \in \mathcal{L}.\text{Val} \,\} \\
\mathcal{G}[\![\Gamma, x : \tau]\!]\rho & \stackrel{\text{def}}{=} & \{\, (W, \mathbf{v}, (\gamma, x \mapsto v)) \mid \exists \mathbf{v}_1, \mathbf{v}_2. \\
& & \quad (W, \mathbf{v}, \langle\rangle) \in \square\overline{(\mathcal{L}.\text{pair}(\mathbf{v}_1, \mathbf{v}_2), \mathcal{H}.\text{Val} \times \mathcal{H}.\text{Mem})} \wedge \\
& & \quad (W, \mathbf{v}_1, v) \in \mathcal{V}[\![\tau]\!]\rho \wedge (W, \mathbf{v}_2, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho \,\}
\end{array}$$

$$\begin{array}{rcl}
\mathcal{D}[\![\cdot]\!] & \stackrel{\text{def}}{=} & \emptyset \\
\mathcal{D}[\![\Delta, \alpha]\!] & \stackrel{\text{def}}{=} & \{\, (\rho, \alpha \mapsto R) \mid \rho \in \mathcal{D}[\![\Delta]\!] \wedge R \in \text{TyValRel} \,\}
\end{array}$$

For $\mathrm{bg} \in \mathrm{PAddr}, e \in \mathcal{H}.\mathrm{Prog}$,

$$\begin{aligned}\Delta;\Gamma \vdash \mathrm{bg} \approx_W e : \tau \stackrel{\text{def}}{=}\ & \forall W' \sqsupseteq W.\ \forall \rho \in \mathcal{D}[\![\Delta]\!]\,.\ \forall (\mathbf{v},\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho(W').\\ & \quad ((\underline{\mathrm{bg}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v} \,\}), \gamma\rho e) \in \mathcal{E}[\![\tau]\!]\rho(W')\\ & \quad \text{where } \gamma\rho e ::= e[\rho(\alpha).\tau_2/\alpha][\gamma(x)/x]\ .\end{aligned}$$

For $p \in \mathcal{L}.\mathrm{Prog}, e \in \mathcal{H}.\mathrm{Prog}$,

$$\begin{aligned}\Delta;\Gamma \vdash p \approx e : \tau \stackrel{\text{def}}{=}\ & \emptyset;\Delta;\Gamma \vdash e : \tau \wedge\\ & \forall \mathcal{A}, \mathrm{gcbg}, \mathrm{bg}.\ \forall k, W \sqsupseteq W^\circ_k(\mathcal{A}, \mathrm{gcbg}).\ \forall (\mathbf{M}, M) \in \mathcal{M}(W).\\ & \forall \mathbf{M'}.\ \mathbf{M'} = \mathbf{M} \uplus \{[\mathrm{bg} \Mapsto p(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg})]\}_{\mathrm{code}} \implies\\ & \exists W' \sqsupseteq W.\ \mathrm{lev}(W') = \mathrm{lev}(W) \wedge (\mathbf{M'}, M) \in \mathcal{M}(W') \wedge\\ & \qquad \Delta;\Gamma \vdash \mathrm{bg} \approx_{W'} e : \tau\ .\end{aligned}$$

Theorem 13 (Monotonicity of $\mathcal{G}[\![\Gamma]\!]\rho$)**.**

$$\forall \Gamma, \rho.\ \ \mathcal{G}[\![\Gamma]\!]\rho \subseteq \Box\mathcal{G}[\![\Gamma]\!]\rho$$

Proof. By an easy structural induction on Γ. □

7.3 Adequacy and Compositionality

$\mathrm{load}(\mathcal{A}, p) ::=$
$\mathrm{let}\ (\mathrm{init}, \mathrm{alloc}, \mathrm{gcinstrs}, \_) := \mathcal{A}(105),$
$\quad \mathrm{instrs}^p := p(\mathrm{alloc}, 105 + |\mathrm{gcinstrs}|),$
$\quad \mathrm{loadinstrs}^p := [$

$(*\ 100\ *)$	`move`	$\lfloor \mathrm{wk}_4 \rfloor$	$\underline{102}$
	`jmp`	$\underline{\mathrm{init}}$	
$(*\ 102\ *)$	`move`	$\lfloor \mathrm{wk}_0 \rfloor$	$\underline{104}$
	`jmp`	$\underline{105 + \lvert\mathrm{gcinstrs}\rvert}$	
$(*\ 104\ *)$	`halt`		
	gcinstrs		
	instrs^p		

$]\ \mathrm{in}$
$\{\, (\Phi, 100) \in \mathrm{PConf} \mid \Phi.\mathrm{code} \supseteq [100 \Mapsto \mathrm{loadinstrs}^p] \,\}$

Theorem 14 (Adequacy)**.** For all $\emptyset;\emptyset \vdash p \approx e : \tau$,

$$\begin{aligned}&\forall \mathcal{A} \in \mathrm{AllocSpec}.\ \forall (\Phi, \mathrm{pc}) \in \mathrm{load}(\mathcal{A}, p).\ \forall h \in \mathrm{HHeap}.\\ &\mathrm{observe}(\Phi, \mathrm{pc}) = \mathrm{observe}(h, e) \neq \mathit{fail}\end{aligned}$$

Proof.
Let $(\mathrm{init}, \mathrm{alloc}, \mathrm{gcinstrs}, \_) = \mathcal{A}(105)$.
Let $\mathrm{code} := [100 \Mapsto \mathrm{loadinstrs}^p]$.
Let $\mathrm{code}^{\mathrm{gc}} := [105 \Mapsto \mathrm{gcinstrs}]$.
Let $\mathrm{code}^p := [105 + |\mathrm{gcinstrs}| \Mapsto p(\mathrm{alloc}, 105 + |\mathrm{gcinstrs}|)]$.
Let $\mathrm{code}^\bullet := \mathrm{code} \setminus \mathrm{code}^{\mathrm{gc}} \setminus \mathrm{code}^p$.

- By definition of load, we have $\mathrm{pc} = 100$ and $\Phi.\mathrm{code} \supseteq \mathrm{code}$. We execute the two instructions from the address 100 and get the following configurations.

$$(\Phi^1, \mathrm{init}) \quad (h, e)$$

such that
- $\Phi^1 = \Phi[\lfloor \mathrm{wk}_4 \rfloor \mapsto \underline{102}]$

- By the specifications of $\mathcal{A}$, after some finite number of steps of execution, we have two configurations

$$(\Phi^2, 102) \quad (M^2.h, e)$$

with $\mathbf{M}^2$ and M^2 such that
- $\mathbf{M}^2$ repr Φ^2,
- $\Phi^2.\mathrm{code} = \Phi.\mathrm{code}$,
- $\mathbf{M}^2.\mathrm{code} = \mathrm{code}^{\mathrm{gc}}$,
- $M^2 := (h, \emptyset)$

- Let $\mathbf{M}^3 := \mathbf{M}^2 \uplus \{\mathrm{code}^\bullet\}_{\mathrm{code}}$.
Still, $\mathbf{M}^3$ repr Φ^2.

- Let $W_k^3 := W_k^\circ(\mathrm{gcbg})[1 \rightsquigarrow (\mathbf{M}^3.\mathrm{reg}|_{\mathrm{sv}_0 \ldots \mathrm{sv}_4}, \mathbf{M}^3.\mathrm{stk})] +\!\!+ \iota^{\mathrm{code}}(\mathrm{code}^\bullet)$.
Then $\forall k.\ (\mathbf{M}^3, M^2) \in \mathcal{M}(W_k^3)$.

- Now the goal is to show that both the configurations $(\Phi^2, 102)$ and $(M^2.h, e)$ diverge or both halt (in other words, both

equi-terminate without fail). For this, it suffices to show that, for any k, $((\Phi^2, 102), (M^2.h, e)) \in \mathcal{O}(W)$ for some world W of level k, which means by definition that they equi-terminate up to k steps without fail.

- For any k,
Let $\mathbf{M}^4 := \mathbf{M}^3 \uplus \{\mathrm{code}^p\}_{\mathrm{code}}$.
Still, $\mathbf{M}^4$ repr Φ^2.
From $p \approx_\tau e$, we have W^4 such that
- $W^4 \sqsupseteq W_k^3 \wedge \mathrm{lev}(W^4) = \mathrm{lev}(W_k^3) = k$
- $(\mathbf{M}^4, M^2) \in \mathcal{M}(W^4)$
$(*)$ $\forall W' \sqsupseteq W^4.\ \forall \mathbf{v}.\ ((\underline{105 + |\mathrm{gcinstrs}|}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v} \,\}), e) \in \mathcal{E}[\![\tau]\!]\emptyset(W')$.

- Now it suffices to show that $((\Phi^2, 102), (M^2.h, e)) \in \mathcal{O}(W^4)$.

- We execute the two instructions from the address 102 and get the two configurations

$$(\Phi^5, 105 + |\mathrm{gcinstrs}|), \quad (M^2.h, e)$$

such that
- $\mathbf{M}^5 := \mathbf{M}^4[\mathrm{wk}_0 \mapsto \underline{104}]_{\mathrm{reg}}$,
- $\mathbf{M}^5$ repr Φ^5.

- Still, $(\mathbf{M}^5, M^2) \in \mathcal{M}(W^4)$
By Theorem 9, it suffices to show that $((\Phi^5, 105 + |\mathrm{gcinstrs}|), (M^2.h, e)) \in \mathcal{O}(W^4)$.

- By $(*)$, it suffices to show that $((104, \lfloor \mathrm{wk}_5 \rfloor), [-]) \in \mathcal{K}[\![\tau]\!]\emptyset(W^4)$, which holds vacuously as both continuations immediately halt.

□

Theorem 15 (Compositionality)**.** Lemma 11 (the compatibility for App) to be introduced in Section 9 can be seen as *compositionality*.

8 Self-Modifying Awkward Example

8.1 Definitions

$e := \mathsf{let}\ x = \mathsf{ref}\ 0\ \mathsf{in}\ \lambda f{:}\mathsf{unit} \to \mathsf{unit}.\ x := 1; f\ \langle\rangle; !x$
$p := \lambda\ \mathrm{alloc}\ \mathrm{bg}.\ [$

bg	`move`	$\lfloor \mathrm{wk}_4 \rfloor$	$\underline{\mathrm{bg}+3}$		
	`move`	$\lfloor \mathrm{wk}_5 \rfloor$	$\underline{1}$		
	`jmp`	$\underline{\mathrm{alloc}}$			
$\mathrm{bg}+3$	`move`	$\langle \mathrm{wk}_5 + 0 \rangle_{\mathrm{h}}$	$\underline{\mathrm{bg}+5}$		
	`jmp`	$\lfloor \mathrm{wk}_0 \rfloor$			
$\mathrm{bg}+5$	`move`	$\lfloor \mathrm{wk}_3 \rfloor$	$\underline{\mathrm{bg}+10}$		
$\mathrm{bg}+6$	`isr`	$\lfloor \mathrm{wk}_4 \rfloor$	$\lfloor \mathrm{wk}_3 \rfloor$		
	`minus`	$\lfloor \mathrm{wk}_4 \rfloor$	$\lfloor \mathrm{wk}_4 \rfloor$	$\underline{666}$	
	`isw`	$\lfloor \mathrm{wk}_3 \rfloor$	$\lfloor \mathrm{wk}_4 \rfloor$		
	`plus`	$\lfloor \mathrm{wk}_3 \rfloor$	$\lfloor \mathrm{wk}_3 \rfloor$	$\underline{1}$	
$\mathrm{bg}+10$	$\mathbb{D}(\mathbb{E}($`jneq`	$\mathrm{bg}+6$	$\lfloor \mathrm{wk}_3 \rfloor$	$\underline{\mathrm{bg}+21}$	$)+666)$
$\mathrm{bg}+11$	$\mathbb{D}(\mathbb{E}($`isw`	$\underline{\mathrm{bg}+5}$	$\mathbb{E}($`jmp` $\underline{\mathrm{bg}+12})$		$)+666)$
$\mathrm{bg}+12$	$\mathbb{D}(\mathbb{E}($`move`	$\langle \mathrm{wk}_1 + 0 \rangle_{\mathrm{h}}$	$\underline{\mathrm{bg}+13}$		$)+666)$
$\mathrm{bg}+13$	$\mathbb{D}(\mathbb{E}($`plus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{1}$	$)+666)$
	$\mathbb{D}(\mathbb{E}($`move`	$\langle \mathrm{sp} - 1 \rangle_{\mathrm{s}}$	$\lfloor \mathrm{wk}_0 \rfloor$		$)+666)$
	$\mathbb{D}(\mathbb{E}($`move`	$\lfloor \mathrm{wk}_1 \rfloor$	$\lfloor \mathrm{wk}_2 \rfloor$		$)+666)$
	$\mathbb{D}(\mathbb{E}($`move`	$\lfloor \mathrm{wk}_0 \rfloor$	$\underline{\mathrm{bg}+18}$		$)+666)$
	$\mathbb{D}(\mathbb{E}($`jmp`	$\langle \mathrm{wk}_1 + 0 \rangle_{\mathrm{h}}$			$)+666)$
$\mathrm{bg}+18$	$\mathbb{D}(\mathbb{E}($`move`	$\lfloor \mathrm{wk}_5 \rfloor$	$\underline{1}$		$)+666)$
	$\mathbb{D}(\mathbb{E}($`minus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{1}$	$)+666)$
$\mathrm{bg}+20$	$\mathbb{D}(\mathbb{E}($`jmp`	$\langle \mathrm{sp} - 0 \rangle_{\mathrm{s}}$			$)+666)$

$]$

8.2 Properties

Theorem 16. $\Delta; \Gamma \vdash p \approx e : (\mathsf{unit} \to \mathsf{unit}) \to \mathsf{int}$

Proof.

- For any $\mathcal{A}, \mathrm{gcbg}, \mathrm{bg}, k$, suppose
  - $W \sqsupseteq W_k^\circ(\mathcal{A}, \mathrm{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$,
  - $\mathrm{code}^p := [\mathrm{bg} \Mapsto p(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg})]$,
  - $\mathbf{M}' = \mathbf{M} \uplus \{\mathrm{code}^p\}_{\mathrm{code}}$.

- plaininstrs^p := [

bg	`move`	$\lfloor \mathrm{wk}_4 \rfloor$	$\underline{\mathrm{bg}+3}$	
	`move`	$\lfloor \mathrm{wk}_5 \rfloor$	$\underline{1}$	
	`jmp`	$\underline{\mathrm{alloc}}$		
$\mathrm{bg}+3$	`move`	$\langle \mathrm{wk}_5 + 0 \rangle_{\mathrm{h}}$	$\underline{\mathrm{bg}+5}$	
	`jmp`	$\lfloor \mathrm{wk}_0 \rfloor$		
$\mathrm{bg}+5$	`jmp`	$\underline{\mathrm{bg}+12}$		
$\mathrm{bg}+6$	`isr`	$\lfloor \mathrm{wk}_4 \rfloor$	$\lfloor \mathrm{wk}_3 \rfloor$	
	`minus`	$\lfloor \mathrm{wk}_4 \rfloor$	$\lfloor \mathrm{wk}_4 \rfloor$	$\underline{666}$
	`isw`	$\lfloor \mathrm{wk}_3 \rfloor$	$\lfloor \mathrm{wk}_4 \rfloor$	
	`plus`	$\lfloor \mathrm{wk}_3 \rfloor$	$\lfloor \mathrm{wk}_3 \rfloor$	$\underline{1}$
$\mathrm{bg}+10$	`jneq`	$\mathrm{bg}+6$	$\lfloor \mathrm{wk}_3 \rfloor$	$\underline{\mathrm{bg}+21}$
$\mathrm{bg}+11$	`isw`	$\underline{\mathrm{bg}+5}$	$\mathbb{E}(\texttt{jmp}\ \underline{\mathrm{bg}+12})$	
$\mathrm{bg}+12$	`move`	$\langle \mathrm{wk}_1 + 0 \rangle_{\mathrm{h}}$	$\underline{\mathrm{bg}+13}$	
$\mathrm{bg}+13$	`plus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{1}$
	`move`	$\langle \mathrm{sp} - 1 \rangle_{\mathrm{s}}$	$\lfloor \mathrm{wk}_0 \rfloor$	
	`move`	$\lfloor \mathrm{wk}_1 \rfloor$	$\lfloor \mathrm{wk}_2 \rfloor$	
	`move`	$\lfloor \mathrm{wk}_0 \rfloor$	$\underline{\mathrm{bg}+18}$	
	`jmp`	$\langle \mathrm{wk}_1 + 0 \rangle_{\mathrm{h}}$		
$\mathrm{bg}+18$	`move`	$\lfloor \mathrm{wk}_5 \rfloor$	$\underline{1}$	
	`minus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{1}$
$\mathrm{bg}+20$	`jmp`	$\langle \mathrm{sp} - 0 \rangle_{\mathrm{s}}$		

]

- plaincode^p := [bg $\mapsto$ plaininstrs^p]

- Goal: find W^{pe} such that
  - $W^{pe} \sqsupseteq W \wedge \mathrm{lev}(W^{pe}) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta; \Gamma \vdash \mathrm{bg} \approx_{W^{pe}} e : (\mathsf{unit} \to \mathsf{unit}) \to \mathsf{int}$

- Let $S^p := \{\, \mathrm{enc}, \mathrm{dec} \,\}$.
  Let $\delta^p := \{\, (\mathrm{enc}, \mathrm{dec}) \,\}^*$.
  Let $\varphi^p := \delta^p$.
  Let $MR^p(\mathrm{enc}) := \{\, (W, \mathbf{M}, M) \mid \mathbf{M}.\mathrm{code} \supseteq \mathrm{code}^p \,\}$.
  Let $MR^p(\mathrm{dec}) := \{\, (W, \mathbf{M}, M) \mid \mathbf{M}.\mathrm{code} \supseteq \mathrm{plaincode}^p \,\}$.
  Let $\iota^p_{\mathrm{enc}} := (\mathrm{enc}, S^p, \delta^p, \varphi^p, MR^p, \lambda s.\ \emptyset)$.
  Let $\iota^p_{\mathrm{dec}} := (\mathrm{dec}, S^p, \delta^p, \varphi^p, MR^p, \lambda s.\ \emptyset)$.

- Choose $W^{pe} ::= W +\!\!+ \iota^p_{\mathrm{enc}}$ and let i^p be the index of ι^p_{enc} in $W^{pe}.\omega$, *i.e.*, $W^{pe}.\omega(i^p) = \iota^p_{\mathrm{enc}}$.

- $W^{pe} \sqsupseteq W \wedge \mathrm{lev}(W^{pe}) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$ holds trivially.

- To show: $\forall W^1 \sqsupseteq W^{pe}.\ \forall \rho \in \mathcal{D}[\![\Delta]\!]\,.\ \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho(W^1)$.
  $((\underline{\mathrm{bg}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v} \,\}), \gamma\rho e) \in \mathcal{E}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{int}]\!]\rho(W^1)$

- By definition of $\mathcal{E}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{int}]\!]\rho(W^1)$ and plugc, we suppose
  - $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{int}]\!]\rho(W^1)$,
  - $(\mathbf{M}^1, M^1) \in \mathcal{M}(W^1)$,
  - $\mathbf{M}^1$ repr Φ^1,
  - $\mathbf{M}^1.\mathrm{reg}(\mathrm{wk}_0) = \underline{\mathrm{kpc}}$,
  - $\mathbf{M}^1.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v}$.
- To show: $((\Phi^1, \mathrm{bg}), (M^1.h, K[e])) \in \mathcal{O}(W^1)$
- As W^1 includes ι^p_{enc} or ι^p_{dec}, we execute the three instructions from bg on the low side and get the configurations
$$(\Phi^2, \mathrm{alloc}), \quad (M^1.h, K[e])$$
such that
  - $\mathbf{M}^2 := \mathbf{M}^1[\mathrm{wk}_4 \mapsto \underline{\mathrm{bg} + 3}]_{\mathrm{reg}}[\mathrm{wk}_5 \mapsto \underline{1}]_{\mathrm{reg}}$,
  - $\mathbf{M}^2$ repr Φ^2.
- By the specifications of $\mathcal{A}$, after some finite number of steps of execution, we have configurations
$$(\Phi^3, \mathrm{bg} + 3), \quad (M^1.h, K[e])$$
such that
  - $\mathbf{M}^3 := \mathbf{M}^2[[T, S]][\mathrm{wk}_4 \mapsto \underline{w}]_{\mathrm{reg}}[\mathrm{wk}_5 \mapsto \widehat{\boldsymbol{l}_1}\,]_{\mathrm{reg}} \uplus \{[\boldsymbol{l}_1 \mapsto (\underline{w_0})]\}_{\mathrm{heap}}$ for some $w, \boldsymbol{l}_1, w_0$,
  - $\mathbf{M}^3 \in \mathcal{A}.GR(\mathrm{gcbg}) \wedge \mathbf{M}^3 \in \mathcal{A}.MR(\mathrm{gcbg})$,
  - $\mathbf{M}^3$ repr Φ^3.
- As $\mathbf{M}^3.\mathrm{code} = \mathbf{M}^2.\mathrm{code}$, we execute the two instructions from $\mathrm{bg} + 3$ on the low side and get
$$(\Phi^4, \mathrm{kpc}), \quad (M^1.h, K[e])$$
such that
  - $\mathbf{M}^4 := \mathbf{M}^3[\boldsymbol{l}_1 : 0 \mapsto \mathrm{bg} + 5]_{\mathrm{hp}}$
  - $\mathbf{M}^4$ repr Φ^4.
- Now we execute the term e on the high side and get
$$(\Phi^4, \mathrm{kpc}), \quad (M^4.h, K[v^1])$$
such that
  - $M^4 := (M^1.h \uplus [\ell_2 \mapsto 0], \{M^1.\Sigma, \ell_2 : \mathsf{int}\})$ for some ℓ_2,
  - $v^1 := \lambda f{:}\mathsf{unit} \to \mathsf{unit}.\, \ell_2 := 1; f\ \langle\rangle; !\ell_2$.
- Let $W^4 := W^1[+\ell_2 : \mathsf{int}]_2 +\!\!+ \iota^1_{\mathrm{fst}}$ where
  - $S^1 := \{\, \mathrm{fst}, \mathrm{sub} \,\}$,
  - $\delta^1 := \{\, (\mathrm{fst}, \mathrm{sub}) \,\}^*$,
  - $\varphi^1 := \delta^1$,
  - $MR^1(\mathrm{fst}) := \{\, (W, \mathbf{M}, M) \mid \mathbf{M}.\mathrm{hp}(\boldsymbol{l}_1)(0) = \underline{\mathrm{bg} + 5} \wedge M.h(\ell_2) = 0 \,\}$,
  - $MR^1(\mathrm{sub}) := \{\, (W, \mathbf{M}, M) \mid W.\omega(i^p).s = \mathrm{dec} \wedge \mathbf{M}.\mathrm{hp}(\boldsymbol{l}_1)(0) = \underline{\mathrm{bg} + 13} \wedge M.h(\ell_2) = 1 \,\}$,
  - $\iota^1_{\mathrm{fst}} = (\mathrm{fst}, S^1, \delta^1, \varphi^1, MR^1, \lambda s.\, \emptyset)$,
  - $\iota^1_{\mathrm{sub}} = (\mathrm{sub}, S^1, \delta^1, \varphi^1, MR^1, \lambda s.\, \emptyset)$,
  - It is important to note that $MR^1(\mathrm{sub})$ is monotone because there is no transition out of dec.
  - Let i^1 be the index of ι^1_{fst} in $W^4.\omega$.

- Then, $(\mathbf{M}^4, M^4) \in \mathcal{M}(W^4)$
- By Theorem 9, it suffices to show that $((\Phi^4, \mathrm{kpc}), (M^4.h, K[v^1])) \in \mathcal{O}(W^4)$.
- As $W^4 \sqsupseteq_{\mathrm{pub}} W^1$ and $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{int}]\!]\rho(W^1)$, it suffices to show that $(\widehat{\boldsymbol{l}_1}, v^1) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{int}]\!]\rho(W^4)$.
- It is easy to check that $(\widehat{\boldsymbol{l}_1}, v^1) \in \mathrm{oftype}((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{int}, \rho)(W^4)$.
- Suppose
  $W^5 \sqsupset_{\triangleright} W^4$,
  $(\mathbf{u}_1, u_2) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\rho(W^5)$.
- To show:
  $$(\mathbf{e}^5, e^5) \in \mathcal{E}[\![\mathsf{int}]\!]\rho(W^5)$$
  where
  $\mathbf{e}^5 := (\langle \boldsymbol{l}_1 : 0 \rangle_{\mathrm{h}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{wk}_1) = \widehat{\boldsymbol{l}_1} \wedge \mathbf{M}.\mathrm{reg}(\mathrm{wk}_2) = \mathbf{u}_1 \,\})$,
  $e^5 := (\ell_2 := 1; u_2\ \langle\rangle; !\ell_2)$.
- By definition of $\mathcal{E}[\![\mathsf{int}]\!]\rho(W^5)$ and plugc, suppose
  - $((\mathrm{kpc}^5, \lfloor \mathrm{wk}_5 \rfloor), K^5) \in \mathcal{K}[\![\mathsf{int}]\!]\rho(W^5)$
  - $(\mathbf{M}^5, M^5) \in \mathcal{M}(W^5)$
  - $\mathbf{M}^5$ repr Φ^5
  - $\mathbf{M}^5.\mathrm{reg}(\mathrm{wk}_0) = \underline{\mathrm{kpc}^5}$
  - $\mathbf{M}^5.\mathrm{reg}(\mathrm{wk}_1) = \widehat{\boldsymbol{l}_1}$
  - $\mathbf{M}^5.\mathrm{reg}(\mathrm{wk}_2) = \mathbf{u}_1$
- To show:
  $$((\Phi^5, \mathbf{M}^5.\mathrm{hp}(\boldsymbol{l}_1)(0)), (M^5.h, K^5[e^5])) \in \mathcal{O}(W^5)$$
- If $\mathrm{lev}(W^5) = 0$ then it holds trivially. Thus, assume that $\mathrm{lev}(W^5) > 0$.
- We now prove that after taking a finite number of steps in the low side, we get the configurations
  $$(\Phi^6, \mathrm{bg} + 13) \quad (M^5.h, K^5[e^5])$$
  such that
  - $\mathbf{M}^6 := \mathbf{M}^5[\mathrm{bg} \Rrightarrow \mathrm{plaininstrs}^p]_{\mathrm{code}}[\boldsymbol{l}_1 : 0 \mapsto \mathrm{bg} + 13]_{\mathrm{hp}}$
  - $\mathbf{M}^6$ repr Φ^6.
  - When $W^5.\omega(i^p).s = \mathrm{enc} \wedge W^5.\omega(i^1).s = \mathrm{fst}$:
    As $\mathbf{M}^5.\mathrm{code} \supseteq \mathrm{code}^p$ and $\mathbf{M}^5.\mathrm{hp}(\boldsymbol{l}_1)(0) = \mathrm{bg} + 5$, it first decodes the instructions from $\mathrm{bg} + 10$ to $\mathrm{bg} + 20$, write the instruction `jmp` $\mathrm{bg} + 12$ at the address $\mathrm{bg} + 5$ in the code memory, and write $(\mathrm{bg} + 13)$ at the physical address corresponding to the logical address $\boldsymbol{l}_1 : 0$. Then the pc becomes $(\mathrm{bg} + 13)$ and $\mathbf{M}^6$ represents the updated physical memory.
  - When $W^5.\omega(i^p).s = \mathrm{enc} \wedge W^5.\omega(i^1).s = \mathrm{sub}$:
    This case is not possible by definition of $MR^1(\mathrm{sub})$.

– When $W^5.\omega(i^p).s = \mathrm{dec} \wedge W^5.\omega(i^1).s = \mathrm{fst}$:
As $\mathbf{M}^5.\mathrm{code} \supseteq \mathrm{plaincode}^p$ and $\mathbf{M}^5.\mathrm{hp}(\boldsymbol{l}_1)(0) = \mathrm{bg} + 5$, it first jumps to $\mathrm{bg} + 12$, and write $(\mathrm{bg} + 13)$ at the physical address corresponding to the logical address $\boldsymbol{l}_1 : 0$. Then the pc becomes $(\mathrm{bg} + 13)$ and $\mathbf{M}^6$ represents the updated physical memory.

– When $W^5.\omega(i^p).s = \mathrm{dec} \wedge W^5.\omega(i^1).s = \mathrm{sub}$:
As $\mathbf{M}^5.\mathrm{code} \supseteq \mathrm{plaincode}^p$ and $\mathbf{M}^5.\mathrm{hp}(\boldsymbol{l}_1)(0) = \mathrm{bg} + 13$, the current pc is $(\mathrm{bg} + 13)$ and $\mathbf{M}^6 = \mathbf{M}^5$ represents the current physical memory Φ^5.

- We take one step on the high side and get the following

$$(\Phi^6, \mathrm{bg} + 13) \quad (M^6.h, K^5[u_2\ \langle\rangle; !\ell_2])$$

such that
- $M^6 := (M^5.h[\ell_2 \mapsto 1], M^5.\Sigma)$

- Let $W^6 := W^5[i^p \rightsquigarrow \mathrm{dec}][i^1 \rightsquigarrow \mathrm{sub}]$.
Then $(\mathbf{M}^6, M^6) \in \mathcal{M}(W^6)$.

- As $(\mathbf{u}_1, u_2) \in \mathsf{oftype}(\mathsf{unit} \to \mathsf{unit}, \rho)(W^6)$ by Theorem 5 and 4, we have
- $\mathbf{u}_1 = \widehat{\boldsymbol{l}'_1}$ for some $\boldsymbol{l}'_1$
- $\mathbf{M}^6.\mathrm{hp}(\boldsymbol{l}'_1)(0) = \underline{w'}$ for some w'
- $u_2 = \lambda x{:}\mathsf{unit}.\, e'$ for some e'

- We execute the configurations in both side and get the following

$$(\Phi^7, w') \quad (M^7.h, K^5[e'[\langle\rangle/x]; !\ell_2])$$

such that
- $\mathbf{M}^7 := \mathbf{M}^6[{+\!+}\,\mathrm{kpc}^5]_{\mathrm{stk}}[\mathrm{wk}_1 \mapsto \mathbf{u}_1]_{\mathrm{reg}}[\mathrm{wk}_0 \mapsto \mathrm{bg} + 18]$
- $\mathbf{M}^7$ repr Φ^7
- $M^7 := \mathbf{M}^6$

- Let $W^7 := \triangleright W^6[{+\!+}\,\mathrm{kpc}^5]_1$.
Then $(\mathbf{M}^7, M^7) \in \mathcal{M}(W^7)$.
By Theorem 9, it suffices to show that $((\Phi^7, w'), (M^7.h, K^5[e'[\langle\rangle/x]; !\ell_2])) \in \mathcal{O}(W^7)$.

- If $\mathrm{lev}(W^7) = 0$ then it holds trivially. Thus, assume that $\mathrm{lev}(W^7) > 0$.

- As $(\mathbf{u}_1, u_2) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\rho(W^5)$, $W^7 \sqsupset_\triangleright W^5$ and $(\mathbf{M}^7.\mathrm{reg}(\mathrm{wk}_2), \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\rho(W^7)$, we have

$$((\langle \boldsymbol{l}'_1 : 0\rangle_{\mathrm{h}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{wk}_1) = \widehat{\boldsymbol{l}'_1} \wedge \mathbf{M}.\mathrm{reg}(\mathrm{wk}_2) = \mathbf{M}^7.\mathrm{reg}(\mathrm{wk}_2)\,\}), e'[\langle\rangle/x]) \in \mathcal{E}[\![\mathsf{unit}]\!]\rho(W^7)$$

- By definition of $\mathcal{E}[\![\mathsf{unit}]\!]\rho$, it suffices to show that

$$((\mathrm{bg} + 18, \lfloor \mathrm{wk}_5 \rfloor), K^5[-; !\ell_2]) \in \mathcal{K}[\![\mathsf{unit}]\!]\rho(W^7)\ .$$

- Suppose
  $W^8 \sqsupseteq_{\text{pub}} W^7$,
  $(\mathbf{u}'_1, u'_2) \in \mathcal{V}[\![\mathsf{unit}]\!]\rho(W^8)$,
  $(\mathbf{M}^8, M^8) \in \mathcal{M}(W^8)$,
  $\mathbf{M}^8.\text{reg}(\text{wk}_5) = \mathbf{u}'_1$,
  $\mathbf{M}^8$ repr Φ^8.

- To show:
$$((\Phi^8, \text{bg} + 18), (M^8.h, K^5[\mathbf{u}'_1; !\ell_2])) \in \mathcal{O}(W^8)$$

- As $W^8 \sqsupseteq_{\text{pub}} W^7$, we have $W^8.\omega(i^1).s = \text{sub}$, and thus $M^8.h(\ell_2) = 1$. We execute the configurations and get
$$(\Phi^9, \text{kpc}^5) \quad (M^9.h, K^5[1])$$
  such that
  - $\mathbf{M}^9 := \mathbf{M}^8[\text{wk}_5 \mapsto \underline{1}]_{\text{reg}}[-1]_{\text{stk}}$
  - $\mathbf{M}^9$ repr Φ^9
  - $M^9 := M^8$

- Let $W^9 := W^8[-1]_1$.
  Then $(\mathbf{M}^9, M^9) \in \mathcal{M}(W^9)$.
  By Theorem 9, it suffices to show that $((\Phi^9, \text{kpc}^5), (M^9.h, K^5[1])) \in \mathcal{O}(W^9)$.

- This holds because $(\underline{1}, 1) \in \mathcal{V}[\![\mathsf{int}]\!]\rho(W^9)$ and $((\text{kpc}^5, \lfloor \text{wk}_5 \rfloor), K^5) \in \mathcal{K}[\![\mathsf{int}]\!]\rho(W^9)$, which follows from $((\text{kpc}^5, \lfloor \text{wk}_5 \rfloor), K^5) \in \mathcal{K}[\![\mathsf{int}]\!]\rho(W^5)$ and $W^9 \sqsupseteq_{\text{pub}} W^5$ by Theorem 6.

□

9 Compiler Correctness

9.1 Compiler Definition and Correctness

For $\emptyset; \Delta; \Gamma \vdash e : \tau$,
$(\!|\Gamma \vdash e|\!) \in \mathrm{PAddr} \times \mathrm{PAddr} \to \mathrm{List\ Instruction}$

$$\begin{aligned} \mathrm{idx}(\Gamma, x : \tau \vdash x) &\stackrel{\mathrm{def}}{=} 0 \\ \mathrm{idx}(\Gamma, y : \tau \vdash x) &\stackrel{\mathrm{def}}{=} \mathrm{idx}(\Gamma \vdash x) + 1 \qquad \text{if } y \neq x \end{aligned}$$

The compiler $(\!|\Gamma \vdash e|\!)$ for $\emptyset; \Delta; \Gamma \vdash e : \tau$ is defined by a structural recursion on e, each component of which is defined in the subsequent sections.

Theorem 17 (Compiler Correctness)**.** For $\emptyset; \Delta; \Gamma \vdash e : \tau$,

$$\Delta; \Gamma \vdash (\!|\Gamma \vdash e|\!) \approx e : \tau \ .$$

Proof. By a structural induction on e: each case by the compatibility lemmas in the subsequent sections. □

9.2 Var

$$\begin{aligned} &(\!|\Gamma \vdash x|\!) ::= \mathrm{Pvar}(\mathrm{idx}(\Gamma \vdash x)) \\ &\mathrm{Pvar}(n) ::= \lambda\, \mathrm{alloc}, \mathrm{bg}.\ [\\ &\quad \mathrm{bg} \quad \texttt{move} \quad \lfloor \mathrm{wk}_5 \rfloor \quad \lfloor \mathrm{sv}_0 \rfloor \\ &\qquad\quad \texttt{move} \quad \lfloor \mathrm{wk}_5 \rfloor \quad \langle \mathrm{wk}_5 + 1 \rangle_{\mathrm{h}} \\ &\qquad\quad \vdots \ (n \text{ times}) \\ &\qquad\quad \texttt{move} \quad \lfloor \mathrm{wk}_5 \rfloor \quad \langle \mathrm{wk}_5 + 1 \rangle_{\mathrm{h}} \\ &\qquad\quad \texttt{move} \quad \lfloor \mathrm{wk}_5 \rfloor \quad \langle \mathrm{wk}_5 + 0 \rangle_{\mathrm{h}} \\ &\qquad\quad \texttt{jmp} \quad \lfloor \mathrm{wk}_0 \rfloor \\ &\ ] \end{aligned}$$

Lemma 7 (Compatibility: Var)**.**

$$\Delta; \Gamma \vdash \mathrm{Pvar}(\mathrm{idx}(\Gamma \vdash x)) \approx x : \tau$$

Proof.

- For any $\mathcal{A}, \mathrm{gcbg}, \mathrm{bg}, k$, suppose
  - $W \sqsupseteq W_k^\circ(\mathcal{A}, \mathrm{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$
  - $\mathrm{code} := [\mathrm{bg} \Mapsto \mathrm{Pvar}(\mathrm{idx}(\Gamma \vdash x))(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg})]$
  - $\mathbf{M}' = \mathbf{M} \uplus \{\mathrm{code}\}_{\mathrm{code}}$.
- Goal: find W^{pe} such that
  - $W^{pe} \sqsupseteq W \wedge \mathrm{lev}(W^{pe}) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta; \Gamma \vdash \mathrm{bg} \approx_{W^{pe}} x : \tau$
- Let $W^1 := W +\!\!+ \iota^{\mathrm{code}}(\mathrm{code})$ and choose W^{pe} to be W^1.

- $W^1 \sqsupseteq W \wedge \mathrm{lev}(W^1) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^1)$ holds vacuously.
- To show: $\forall W^2 \sqsupseteq W^1.\ \forall \rho \in \mathcal{D}[\![\Delta]\!]\,.\ \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho(W^2).$
  $((\underline{\mathrm{bg}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v} \,\}), \gamma\rho x) \in \mathcal{E}[\![\tau]\!]\rho(W^2)$
- By definition of $\mathcal{E}[\![\tau]\!]\rho(W^2)$ and plugc, we suppose
  - $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau]\!]\rho(W^2)$,
  - $(\mathbf{M}^2, M^2) \in \mathcal{M}(W^2)$,
  - $\mathbf{M}^2$ repr Φ^2,
  - $\mathbf{M}^2.\mathrm{reg}(\mathrm{wk}_0) = \underline{\mathrm{kpc}}$,
  - $\mathbf{M}^2.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v}$.
- To show: $((\Phi^2, \mathrm{bg}), (M^2.h, K[\gamma(x)])) \in \mathcal{O}(W^2)$
- As W^2 includes $\iota^{\mathrm{code}}(\mathrm{code})$, we execute the instructions from bg on the low side (by induction on $\mathrm{idx}(\Gamma \vdash x)$) and get the configurations

  $$(\Phi^3, \mathrm{kpc}), \quad (M^2.h, K[\gamma(x)])$$

  such that
  - $\mathbf{M}^3 := \mathbf{M}^2[\mathrm{wk}_5 \mapsto \mathbf{v}_1]$ for some $\mathbf{v}_1$ such that $(\mathbf{v}_1, \gamma(x)) \in \mathcal{V}[\![\tau]\!]\rho(W^2)$
  - $\mathbf{M}^3$ repr Φ^3.
- Still, $(\mathbf{M}^3, M^2) \in \mathcal{M}(W^2)$.
  By Theorem 9, it suffices to show that $((\Phi^3, \mathrm{kpc}), (M^2.h, K[\gamma(x)])) \in \mathcal{O}(W^2)$.
- As$((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau]\!]\rho(W^2)$, it suffices to show that

  $$(\mathbf{v}_1, \gamma(x)) \in \mathcal{V}[\![\tau]\!]\rho(W^2)$$

  which is one of the assumptions.

□

9.3 Pair

$$(\!|\Gamma \vdash \langle e_1, e_2\rangle|\!) ::= \mathrm{Ppair}((\!|\Gamma \vdash e_1|\!), (\!|\Gamma \vdash e_2|\!))$$

$\mathrm{Ppair}(p_1, p_2) ::= \lambda\, \mathrm{alloc}, \mathrm{bg}.$
$\mathrm{let}\ \mathrm{instrs}_1 := p_1(\mathrm{alloc}, \mathrm{bg}+4),\ c_1 := |\mathrm{instrs}_1|,$
$\quad \mathrm{instrs}_2 := p_2(\mathrm{alloc}, \mathrm{bg}+c_1+6),\ c_2 := |\mathrm{instrs}_2| \quad \mathrm{in} \quad [$

bg	`plus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{2}$
	`move`	$\langle \mathrm{sp}-2 \rangle_{\mathrm{s}}$	$\lfloor \mathrm{wk}_0 \rfloor$	
	`move`	$\langle \mathrm{sp}-1 \rangle_{\mathrm{s}}$	$\underline{0}$	
	`move`	$\lfloor \mathrm{wk}_0 \rfloor$	$\underline{\mathrm{bg}+c_1+4}$	
	instrs_1			
$\mathrm{bg}+c_1+4$	`move`	$\langle \mathrm{sp}-1 \rangle_{\mathrm{s}}$	$\lfloor \mathrm{wk}_5 \rfloor$	
	`move`	$\lfloor \mathrm{wk}_0 \rfloor$	$\underline{\mathrm{bg}+c_1+c_2+6}$	
	instrs_2			
$\mathrm{bg}+c_1+c_2+6$	`move`	$\lfloor \mathrm{wk}_3 \rfloor$	$\lfloor \mathrm{wk}_5 \rfloor$	
	`move`	$\lfloor \mathrm{wk}_4 \rfloor$	$\underline{\mathrm{bg}+c_1+c_2+10}$	
	`move`	$\lfloor \mathrm{wk}_5 \rfloor$	$\underline{2}$	
	`jmp`	$\underline{\mathrm{alloc}}$		
$\mathrm{bg}+c_1+c_2+10$	`move`	$\langle \mathrm{wk}_5+0 \rangle_{\mathrm{h}}$	$\langle \mathrm{sp}-1 \rangle_{\mathrm{s}}$	
	`move`	$\langle \mathrm{wk}_5+1 \rangle_{\mathrm{h}}$	$\lfloor \mathrm{wk}_3 \rfloor$	
	`minus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{2}$
	`jmp`	$\langle \mathrm{sp}-0 \rangle_{\mathrm{s}}$		

$]$

Lemma 8 (Compatibility: Pair)**.**

$$\Delta;\Gamma \vdash p_1 \approx e_1 : \tau_1 \wedge \Delta;\Gamma \vdash p_2 \approx e_2 : \tau_2 \implies \Delta;\Gamma \vdash \mathrm{Ppair}(p_1, p_2) \approx \langle e_1, e_2\rangle : \tau_1 \times \tau_2$$

Proof.

- For any $\mathcal{A}, \mathrm{gcbg}, \mathrm{bg}, k$, suppose
  - $W \sqsupseteq W_k^\circ(\mathcal{A}, \mathrm{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$
  - $\mathrm{code} := [\mathrm{bg} \Mapsto \mathrm{Ppair}(p_1, p_2)(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg})]$
  - $\mathrm{code}^{p_1} := [\mathrm{bg}+4 \Mapsto p_1(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg}+4)],\ c_1 := |\mathrm{code}^{p_1}|$
  - $\mathrm{code}^{p_2} := [\mathrm{bg}+c_1+6 \Mapsto p_2(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg}+c_1+6)],\ c_2 := |\mathrm{code}^{p_2}|$
  - $\mathrm{code}^\bullet := \mathrm{code} \setminus \mathrm{code}^{p_1} \setminus \mathrm{code}^{p_2}$
  - $\mathbf{M}' = \mathbf{M} \uplus \{\mathrm{code}\}_{\mathrm{code}}$.
- Goal: find W^{pe} such that
  - $W^{pe} \sqsupseteq W \wedge \mathrm{lev}(W^{pe}) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta;\Gamma \vdash \mathrm{bg} \approx_{W^{pe}} \langle e_1, e_2\rangle : \tau_1 \times \tau_2$
- Let $\mathbf{M}^1 := \mathbf{M} \uplus \{\mathrm{code}^\bullet\}_{\mathrm{code}}$.
  Let $W^1 := W +\!\!+ \iota^{\mathrm{code}}(\mathrm{code}^\bullet)$.
  By definition, we have $(\mathbf{M}^1, M) \in \mathcal{M}(W^1)$.
- Let $\mathbf{M}^2 := \mathbf{M}^1 \uplus \{\mathrm{code}^{p_1}\}_{\mathrm{code}}$.
  From $\Delta;\Gamma \vdash p_1 \approx e_1 : \tau_1$, we have W^2 such that

- $W^2 \sqsupseteq W^1 \wedge \mathrm{lev}(W^2) = \mathrm{lev}(W^1)$
- $(\mathbf{M}^2, M) \in \mathcal{M}(W^2)$
- $(*)$ $\Delta; \Gamma \vdash \mathrm{bg} + 4 \approx_{W^2} e_1 : \tau_1$

- Let $\mathbf{M}^3 := \mathbf{M}^2 \uplus \{\mathrm{code}^{p_2}\}_{\mathrm{code}}$.
  From $\Delta; \Gamma \vdash p_2 \approx e_2 : \tau_2$, we have W^3 such that
  - $W^3 \sqsupseteq W^2 \wedge \mathrm{lev}(W^3) = \mathrm{lev}(W^2)$
  - $(\mathbf{M}^3, M) \in \mathcal{M}(W^3)$
  - $(**)$ $\Delta; \Gamma \vdash \mathrm{bg} + c_1 + 6 \approx_{W^3} e_2 : \tau_2$

- We now choose W^{pe} to be W^3 and show the required properties.

- $W^3 \sqsupseteq W \wedge \mathrm{lev}(W^3) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^3)$ holds vacuously.

- To show: $\forall W^4 \sqsupseteq W^3.\ \forall \rho \in \mathcal{D}[\![\Delta]\!].\ \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho(W^4).$
  $((\underline{\mathrm{bg}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v} \,\}), \gamma\rho(\langle e_1, e_2 \rangle)) \in \mathcal{E}[\![\tau_1 \times \tau_2]\!]\rho(W^4)$

- By definition of $\mathcal{E}[\![\tau_1 \times \tau_2]\!]\rho(W^4)$ and plugc, we suppose
  - $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau_1 \times \tau_2]\!]\rho(W^4)$,
  - $(\mathbf{M}^4, M^4) \in \mathcal{M}(W^4)$,
  - $\mathbf{M}^4$ repr Φ^4,
  - $\mathbf{M}^4.\mathrm{reg}(\mathrm{wk}_0) = \underline{\mathrm{kpc}}$,
  - $\mathbf{M}^4.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v}$.

- To show: $((\Phi^4, \mathrm{bg}), (M^4.h, K[\gamma\rho(\langle e_1, e_2 \rangle)])) \in \mathcal{O}(W^4)$

- As W^4 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the four instructions from bg on the low side and get the configurations

$$(\Phi^5, \mathrm{bg} + 4), \quad (M^4.h, K[\langle (\gamma\rho e_1), (\gamma\rho e_2) \rangle])$$

  such that
  - $\mathbf{M}^5 := \mathbf{M}^4[{+\!+}\, \underline{\mathrm{kpc}}, \underline{0}]_{\mathrm{stk}}[\mathrm{wk}_0 \mapsto \underline{\mathrm{bg} + c_1 + 4}]_{\mathrm{reg}}$,
  - $\mathbf{M}^5$ repr Φ^5.

- Let $W^5 := W^4[{+\!+}\, \underline{\mathrm{kpc}}, \underline{0}]_1$.
  Then $(\mathbf{M}^5, M^4) \in \mathcal{M}(W^5)$.
  By Theorem 9, it suffices to show that $((\Phi^5, \mathrm{bg} + 4), (M^4.h, K[\langle (\gamma\rho e_1), (\gamma\rho e_2) \rangle])) \in \mathcal{O}(W^5)$.

- By $(*)$, it suffices to show that $((\mathrm{bg} + c_1 + 4, \lfloor \mathrm{wk}_5 \rfloor), K[\langle (-), (\gamma\rho e_2) \rangle]) \in \mathcal{K}[\![\tau_1]\!]\rho(W^5)$.

- Suppose
  $W^6 \sqsupseteq_{\mathrm{pub}} W^5$,
  $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau_1]\!]\rho(W^6)$,
  $(\mathbf{M}^6, M^6) \in \mathcal{M}(W^6)$,
  $\mathbf{M}^6.\mathrm{reg}(\mathrm{wk}_5) = \mathbf{v}_1$,
  $\mathbf{M}^6$ repr Φ^6.

- To show: $((\Phi^6, \mathrm{bg} + c_1 + 4), (M^6.h, K[\langle v_2, (\gamma\rho e_2) \rangle])) \in \mathcal{O}(W^6)$

- As W^6 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the two instructions from $\mathrm{bg}+c_1+4$ on the low side and get the configurations

$$(\Phi^7, \mathrm{bg}+c_1+6), \quad (M^6.h, K[\langle v_2, (\gamma\rho e_2)\rangle])$$

such that
- $\mathbf{M}^7 := \mathbf{M}^6[|\mathbf{M}^7.\mathrm{stk}|-1 \mapsto \mathbf{v}_1]_{\mathrm{stk}}[\mathrm{wk}_0 \mapsto \underline{\mathrm{bg}+c_1+c_2+6}]_{\mathrm{reg}}$,
- $\mathbf{M}^7$ repr Φ^7.

- Let $W^7 := W^6[|\mathbf{M}^7.\mathrm{stk}|-1 \mapsto \mathbf{v}_1]_1$.
Then $(\mathbf{M}^7, M^6) \in \mathcal{M}(W^7)$.
By Theorem 9, it suffices to show that $((\Phi^7, \mathrm{bg}+c_1+6), (M^6.h, K[\langle v_2, (\gamma\rho e_2)\rangle])) \in \mathcal{O}(W^7)$.

- By $(**)$, it suffices to show that $((\mathrm{bg}+c_1+c_2+6, \lfloor \mathrm{wk}_5 \rfloor), K[\langle v_2, (-)\rangle]) \in \mathcal{K}[\![\tau_2]\!]\rho(W^7)$.

- Suppose
$W^8 \sqsupseteq_{\mathrm{pub}} W^7$,
$(\mathbf{v}_3, v_4) \in \mathcal{V}[\![\tau_2]\!]\rho(W^8)$,
$(\mathbf{M}^8, M^8) \in \mathcal{M}(W^8)$,
$\mathbf{M}^8.\mathrm{reg}(\mathrm{wk}_5) = \mathbf{v}_3$,
$\mathbf{M}^8$ repr Φ^8.

- To show: $((\Phi^8, \mathrm{bg}+c_1+c_2+6), (M^8.h, K[\langle v_2, v_4\rangle])) \in \mathcal{O}(W^8)$

- As W^8 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the four instructions from $\mathrm{bg}+c_1+c_2+6$ on the low side and get the following configurations

$$(\Phi^9, \mathrm{alloc}) \quad (M^8.h, K[\langle v_2, v_4\rangle])$$

such that
- $\mathbf{M}^9 := \mathbf{M}^8[\mathrm{wk}_3 \mapsto \mathbf{v}_3]_{\mathrm{reg}}[\mathrm{wk}_4 \mapsto \underline{\mathrm{bg}+c_1+c_2+10}]_{\mathrm{reg}}[\mathrm{wk}_5 \mapsto \underline{2}]_{\mathrm{reg}}$,
- $\mathbf{M}^9$ repr Φ^9.

- By the specifications of $\mathcal{A}$, after some finite number of steps of execution, we have configurations

$$(\Phi^{10}, \mathrm{bg}+c_1+c_2+10), \quad (M^8.h, K[\langle v_2, v_4\rangle])$$

such that
- $\mathbf{M}^{10} := \mathbf{M}^9[[T,S]][\mathrm{wk}_4 \mapsto \underline{w}]_{\mathrm{reg}}[\mathrm{wk}_5 \mapsto \widehat{\boldsymbol{l}_1}\,]_{\mathrm{reg}} \uplus \{[\boldsymbol{l}_1 \mapsto (\underline{w_0, w_1})]\}_{\mathrm{heap}}$ for some $w, \boldsymbol{l}_1, w_0, w_1$,
- $\mathbf{M}^{10} \in \mathcal{A}.GR(\mathrm{gcbg}) \wedge \mathbf{M}^{10} \in \mathcal{A}.MR(\mathrm{gcbg})$,
- $\mathbf{M}^{10}$ repr Φ^{10}.

- We execute the four instructions from $\mathrm{bg}+c_1+c_2+10$ on the low side and get the following configurations

$$(\Phi^{11}, \mathrm{kpc}) \quad (M^8.h, K[\langle v_2, v_4\rangle])$$

such that
- $\mathbf{M}^{11} := \mathbf{M}^{10}[\boldsymbol{l}_1 : 0 \mapsto \mathbf{v}_1]_{\mathrm{hp}}[\boldsymbol{l}_1 : 1 \mapsto \mathbf{v}_3]_{\mathrm{hp}}[-2]_{\mathrm{stk}}$,
- $\mathbf{M}^{11}$ repr Φ^{11}.

- Let $W^{11} := W^8[-2]_1 +\!\!+ \iota_{\boldsymbol{l}_1}$.
  Let $\iota_{\boldsymbol{l}_1} := \iota^{\text{single}}(\{\, (W, \mathbf{M}, M) \mid \mathbf{M}.\text{hp}(\boldsymbol{l}_1)(0) = \mathbf{v}_1 \wedge \mathbf{M}.\text{hp}(\boldsymbol{l}_1)(1) = \mathbf{v}_3 \,\}, \emptyset)$.
  Then $(\Phi^{11}, M^8) \in \mathcal{M}(W^{11})$.
- By Theorem 9, it suffices to show that $((\Phi^{11}, \text{kpc}), (M^8.h, K[\langle v_2, v_4 \rangle])) \in \mathcal{O}(W^{11})$.
- As $W^{11} \sqsupseteq_{\text{pub}} W^4$ and $((\text{kpc}, \lfloor \text{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau_1 \times \tau_2]\!]\rho(W^4)$, it suffices to show that
$$(\widehat{\boldsymbol{l}_1}, \langle v_2, v_4 \rangle) \in \mathcal{V}[\![\tau_1 \times \tau_2]\!]\rho(W^{11})$$
- It is easy to check that $(\widehat{\boldsymbol{l}_1}, \langle v_2, v_4 \rangle) \in \text{oftype}(\tau_1 \times \tau_2, \rho)(W^{11})$.
- As W^{11} includes $\iota_{\boldsymbol{l}_1}$, by definition of $\mathcal{V}[\![\tau_1 \times \tau_2]\!]\rho(W^{11})$, it just remains to show that
$$(\mathbf{v}_1, v_2) \in \triangleright\mathcal{V}[\![\tau_1]\!]\rho(W^{11}) \wedge (\mathbf{v}_3, v_4) \in \triangleright\mathcal{V}[\![\tau_2]\!]\rho(W^{11})$$
  which follows from $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau_1]\!]\rho(W^6)$ and $(\mathbf{v}_3, v_4) \in \mathcal{V}[\![\tau_2]\!]\rho(W^8)$ by Theorem 5.

□

9.4 Fst

$$(\!|\Gamma \vdash e.1|\!) ::= \text{Pfst}((\!|\Gamma \vdash e|\!))$$

$\text{Pfst}(p) ::= \lambda\, \text{alloc}, \text{bg}.$
$\text{let code} := p(\text{alloc}, \text{bg} + 3),\ c := |\text{code}| \quad \text{in} \quad [$

bg	`plus`	$\lfloor \text{sp} \rfloor$	$\lfloor \text{sp} \rfloor$	$\underline{1}$
	`move`	$\langle \text{sp} - 1 \rangle_{\text{s}}$	$\lfloor \text{wk}_0 \rfloor$	
	`move`	$\lfloor \text{wk}_0 \rfloor$	$\underline{\text{bg} + c + 3}$	
	code			
$\text{bg} + c + 3$	`move`	$\lfloor \text{wk}_5 \rfloor$	$\langle \text{wk}_5 + 0 \rangle_{\text{h}}$	
	`minus`	$\lfloor \text{sp} \rfloor$	$\lfloor \text{sp} \rfloor$	$\underline{1}$
	`jmp`	$\langle \text{sp} - 0 \rangle_{\text{s}}$		

]

Lemma 9 (Compatibility: Fst)**.**

$$\Delta; \Gamma \vdash p \approx e : \tau_1 \times \tau_2 \implies \Delta; \Gamma \vdash \text{Pfst}(p) \approx e.1 : \tau_1$$

Proof.

- For any $\mathcal{A}, \text{gcbg}, \text{bg}, k$, suppose
  - $W \sqsupseteq W_k^\circ(\mathcal{A}, \text{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$
  - $\text{code} := [\text{bg} \Mapsto \text{Pfst}(p)(\mathcal{A}(\text{gcbg}).\text{alloc}, \text{bg})]$
  - $\text{code}^p := [\text{bg} + 3 \Mapsto p(\mathcal{A}(\text{gcbg}).\text{alloc}, \text{bg} + 3)],\ c := |\text{code}^p|$
  - $\text{code}^\bullet := \text{code} \setminus \text{code}^p$
  - $\mathbf{M}' = \mathbf{M} \uplus \{\text{code}\}_{\text{code}}$.
- Goal: find W^{pe} such that
  - $W^{pe} \sqsupseteq W \wedge \text{lev}(W^{pe}) = \text{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta; \Gamma \vdash \text{bg} \approx_{W^{pe}} e.1 : \tau_1$

- Let $\mathbf{M}^1 := \mathbf{M} \uplus \{\text{code}^\bullet\}_{\text{code}}$.
  Let $W^1 := W +\!\!+ \iota^{\text{code}}(\text{code}^\bullet)$.
  By definition, we have $(\mathbf{M}^1, M) \in \mathcal{M}(W^1)$.

- Let $\mathbf{M}^2 := \mathbf{M}^1 \uplus \{\text{code}^p\}_{\text{code}}$.
  From $\Delta; \Gamma \vdash p \approx e : \tau_1 \times \tau_2$, we have W^2 such that
  - $W^2 \sqsupseteq W^1 \wedge \text{lev}(W^2) = \text{lev}(W^1)$
  - $(\mathbf{M}^2, M) \in \mathcal{M}(W^2)$
  - $(*)$ $\Delta; \Gamma \vdash \text{bg} + 3 \approx_{W^2} e : \tau_1 \times \tau_2$

- We now choose W^{pe} to be W^2 and show the required properties.

- $W^2 \sqsupseteq W \wedge \text{lev}(W^2) = \text{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^2)$ holds vacuously.

- To show: $\forall W^3 \sqsupseteq W^2.\ \forall \rho \in \mathcal{D}[\![\Delta]\!].\ \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho(W^3).$
  $((\underline{\text{bg}}, \lfloor \text{wk}_0 \rfloor, \lfloor \text{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\text{reg}(\text{sv}_0) = \mathbf{v} \,\}), \gamma\rho(e.1)) \in \mathcal{E}[\![\tau_1]\!]\rho(W^3)$

- By definition of $\mathcal{E}[\![\tau_1]\!]\rho(W^3)$ and plugc, we suppose
  - $((\text{kpc}, \lfloor \text{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau_1]\!]\rho(W^3)$,
  - $(\mathbf{M}^3, M^3) \in \mathcal{M}(W^3)$,
  - $\mathbf{M}^3$ repr Φ^3,
  - $\mathbf{M}^3.\text{reg}(\text{wk}_0) = \underline{\text{kpc}}$,
  - $\mathbf{M}^3.\text{reg}(\text{sv}_0) = \mathbf{v}$.

- To show: $((\Phi^3, \text{bg}), (M^3.h, K[\gamma\rho(e.1)])) \in \mathcal{O}(W^3)$

- As W^3 includes $\iota^{\text{code}}(\text{code}^\bullet)$, we execute the three instructions from bg on the low side and get the configurations
  $$(\Phi^4, \text{bg} + 3), \quad (M^3.h, K[\gamma\rho e.1])$$
  such that
  - $\mathbf{M}^4 := \mathbf{M}^3[+\!\!+ \underline{\text{kpc}}]_{\text{stk}}[\text{wk}_0 \mapsto \underline{\text{bg} + c + 3}]_{\text{reg}}$,
  - $\mathbf{M}^4$ repr Φ^4.

- Let $W^4 := W^3[+\!\!+ \underline{\text{kpc}}]_1$.
  Then $(\mathbf{M}^4, M^3) \in \mathcal{M}(W^4)$.
  By Theorem 9, it suffices to show that $((\Phi^4, \text{bg} + 3), (M^3.h, K[\gamma\rho e.1])) \in \mathcal{O}(W^4)$.

- By $(*)$, it suffices to show that $((\text{bg} + c + 3, \lfloor \text{wk}_5 \rfloor), K[-.1]) \in \mathcal{K}[\![\tau_1 \times \tau_2]\!]\rho(W^4)$.

- Suppose
  $W^5 \sqsupseteq_{\text{pub}} W^4$,
  $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau_1 \times \tau_2]\!]\rho(W^5)$,
  $(\mathbf{M}^5, M^5) \in \mathcal{M}(W^5)$,
  $\mathbf{M}^5.\text{reg}(\text{wk}_5) = \mathbf{v}_1$,
  $\mathbf{M}^5$ repr Φ^5.

- To show: $((\Phi^5, \text{bg} + c + 3), (M^5.h, K[v_2.1])) \in \mathcal{O}(W^5)$

- If $\text{lev}(W^5) = 0$ then it trivially holds.
  Assume that $\text{lev}(W^5) > 0$.

- As $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau_1 \times \tau_2]\!]\rho(W^5)$
  - $\mathbf{v}_1 = \widehat{\boldsymbol{l}_1}$, $\mathbf{M}^5.\mathrm{hp}(\boldsymbol{l}_1)(0) = \mathbf{u}_1$, $\mathbf{M}^5.\mathrm{hp}(\boldsymbol{l}_1)(1) = \mathbf{u}_2$ for some $\boldsymbol{l}_1, \mathbf{u}_1, \mathbf{u}_2$
  - $v_2 = \langle u_1, u_2 \rangle$ for some u_1, u_2
  - $(\mathbf{u}_1, u_1) \in \triangleright\mathcal{V}[\![\tau_1]\!]\rho(W^5)$
  - $(\mathbf{u}_2, u_2) \in \triangleright\mathcal{V}[\![\tau_2]\!]\rho(W^5)$
- As W^5 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the three instructions from $\mathrm{bg} + c + 3$ on the low side, take one step on the high side, and get the configurations

  $$(\Phi^6, \mathrm{kpc}), \quad (M^6.h, K[u_1])$$

  such that
  - $\mathbf{M}^6 := \mathbf{M}^5[\mathrm{wk}_5 \mapsto \mathbf{u}_1]_{\mathrm{reg}}[-1]_{\mathrm{stk}}$,
  - $\mathbf{M}^6$ repr Φ^6,
  - $M^6 := M^5$.
- Let $W^6 := \triangleright W^5[-1]_1$.
  Then $(\mathbf{M}^6, M^6) \in \mathcal{M}(W^6)$.

- By Theorem 9, it suffices to show that $((\Phi^6, \mathrm{kpc}), (M^6.h, K[u_1])) \in \mathcal{O}(W^6)$.
- As $W^6 \sqsupseteq_{\mathrm{pub}} W^3$ and $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau_1]\!]\rho(W^3)$, it suffices to show that

  $$(\mathbf{u}_1, u_1) \in \mathcal{V}[\![\tau_1]\!]\rho(W^6)$$

  which follows from $(\mathbf{u}_1, u_1) \in \triangleright\mathcal{V}[\![\tau_1]\!]\rho(W^5)$ by monotonicity of $\mathcal{V}[\![\tau_1]\!]\rho$.

□

9.5 Snd

Similarly for Fst.

9.6 Abs

$$(\!|\Gamma \vdash \lambda x{:}\tau.\, e|\!) ::= \mathrm{Pabs}((\!|\Gamma, x : \tau \vdash e|\!))$$

$\mathrm{Pabs}(p) ::= \lambda\, \mathrm{alloc}, \mathrm{bg}.$
$\mathrm{let\ code} := p(\mathrm{alloc}, \mathrm{bg} + 16),\ c := |\mathrm{code}| \quad \mathrm{in} \quad [$

bg	`move`	$\lfloor \mathrm{wk}_4 \rfloor$	$\underline{\mathrm{bg} + 3}$	
	`move`	$\lfloor \mathrm{wk}_5 \rfloor$	$\underline{2}$	
	`jmp`	$\underline{\mathrm{alloc}}$		
$\mathrm{bg} + 3$	`move`	$\langle \mathrm{wk}_5 + 0 \rangle_{\mathrm{h}}$	$\underline{\mathrm{bg} + 6}$	
	`move`	$\langle \mathrm{wk}_5 + 1 \rangle_{\mathrm{h}}$	$\underline{\lfloor \mathrm{sv}_0 \rfloor}$	
	`jmp`	$\lfloor \mathrm{wk}_0 \rfloor$		
$\mathrm{bg} + 6$	`plus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{2}$
	`move`	$\langle \mathrm{sp} - 2 \rangle_{\mathrm{s}}$	$\lfloor \mathrm{wk}_0 \rfloor$	
	`move`	$\langle \mathrm{sp} - 1 \rangle_{\mathrm{s}}$	$\lfloor \mathrm{sv}_0 \rfloor$	
	`move`	$\lfloor \mathrm{wk}_4 \rfloor$	$\underline{\mathrm{bg} + 12}$	
	`move`	$\lfloor \mathrm{wk}_5 \rfloor$	$\underline{2}$	
	`jmp`	$\underline{\mathrm{alloc}}$		
$\mathrm{bg} + 12$	`move`	$\langle \mathrm{wk}_5 + 0 \rangle_{\mathrm{h}}$	$\lfloor \mathrm{wk}_2 \rfloor$	
	`move`	$\langle \mathrm{wk}_5 + 1 \rangle_{\mathrm{h}}$	$\langle \mathrm{wk}_1 + 1 \rangle_{\mathrm{h}}$	
	`move`	$\lfloor \mathrm{sv}_0 \rfloor$	$\lfloor \mathrm{wk}_5 \rfloor$	
	`move`	$\lfloor \mathrm{wk}_0 \rfloor$	$\underline{\mathrm{bg} + c + 16}$	
	code			
$\mathrm{bg} + c + 16$	`move`	$\lfloor \mathrm{sv}_0 \rfloor$	$\langle \mathrm{sp} - 1 \rangle_{\mathrm{s}}$	
	`minus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{2}$
	`jmp`	$\langle \mathrm{sp} - 0 \rangle_{\mathrm{s}}$		

$]$

Lemma 10 (Compatibility: Abs)**.**

$$\Delta; \Gamma, x : \tau' \vdash p \approx e : \tau \implies \Delta; \Gamma \vdash \mathrm{Pabs}(p) \approx \lambda x{:}\tau'.\, e : \tau' \to \tau$$

Proof.

- For any $\mathcal{A}, \mathrm{gcbg}, \mathrm{bg}, k$, suppose
  - $W \sqsupseteq W_k^\circ(\mathcal{A}, \mathrm{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$
  - $\mathrm{code} := [\mathrm{bg} \Mapsto \mathrm{Pabs}(p)(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg})]$
  - $\mathrm{code}^p := [\mathrm{bg} + 16 \Mapsto p(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg} + 16)],\ c := |\mathrm{code}^p|$
  - $\mathrm{code}^\bullet := \mathrm{code} \setminus \mathrm{code}^p$
  - $\mathbf{M}' = \mathbf{M} \uplus \{\mathrm{code}\}_{\mathrm{code}}$.
- Goal: find W^{pe} such that
  - $W^{pe} \sqsupseteq W \wedge \mathrm{lev}(W^{pe}) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta; \Gamma \vdash \mathrm{bg} \approx_{W^{pe}} \lambda x{:}\tau'.\, e : \tau' \to \tau$
- Let $\mathbf{M}^1 := \mathbf{M} \uplus \{\mathrm{code}^\bullet\}_{\mathrm{code}}$.
  Let $W^1 := W +\!\!+ \iota^{\mathrm{code}}(\mathrm{code}^\bullet)$.
  By definition, we have $(\mathbf{M}^1, M) \in \mathcal{M}(W^1)$.

- Let $\mathbf{M}^2 := \mathbf{M}^1 \uplus \{\mathrm{code}^p\}_{\mathrm{code}}$.
  From $\Delta; \Gamma, x : \tau' \vdash p \approx e : \tau$, we have W^2 such that
  - $W^2 \sqsupseteq W^1 \wedge \mathrm{lev}(W^2) = \mathrm{lev}(W^1)$
  - $(\mathbf{M}^2, M) \in \mathcal{M}(W^2)$
  - $(*)$ $\Delta; \Gamma, x : \tau' \vdash \mathrm{bg} + 16 \approx_{W^2} e : \tau$

- We now choose W^{pe} to be W^2 and show the required properties.

- $W^2 \sqsupseteq W \wedge \mathrm{lev}(W^2) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^2)$ holds vacuously.

- To show: $\forall W^3 \sqsupseteq W^2.\ \forall \rho \in \mathcal{D}[\![\Delta]\!].\ \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho(W^3).$
  $((\underline{\mathrm{bg}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v} \,\}), \gamma\rho(\lambda x{:}\tau'.\, e)) \in \mathcal{E}[\![\tau' \to \tau]\!]\rho(W^3)$

- By definition of $\mathcal{E}[\![\tau' \to \tau]\!]\rho(W^3)$ and plugc, we suppose
  - $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau' \to \tau]\!]\rho(W^3)$,
  - $(\mathbf{M}^3, M^3) \in \mathcal{M}(W^3)$,
  - $\mathbf{M}^3$ repr Φ^3,
  - $\mathbf{M}^3.\mathrm{reg}(\mathrm{wk}_0) = \underline{\mathrm{kpc}}$,
  - $\mathbf{M}^3.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v}$.

- To show: $((\Phi^3, \mathrm{bg}), (M^3.h, K[\gamma\rho(\lambda x{:}\tau'.\, e)])) \in \mathcal{O}(W^3)$

- As W^3 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the three instructions from bg on the low side and get the configurations
  $$(\Phi^4, \mathrm{alloc}), \quad (M^3.h, K[\gamma\rho(\lambda x{:}\tau'.\, e)])$$
  such that
  - $\mathbf{M}^4 := \mathbf{M}^3[\mathrm{wk}_4 \mapsto \underline{\mathrm{bg} + 3}]_{\mathrm{reg}}[\mathrm{wk}_5 \mapsto \underline{2}]_{\mathrm{reg}}$,
  - $\mathbf{M}^4$ repr Φ^4.

- By the specifications of $\mathcal{A}$, after some finite number of steps of execution, we have configurations
  $$(\Phi^5, \mathrm{bg} + 3), \quad (M^3.h, K[\gamma\rho(\lambda x{:}\tau'.\, e)])$$
  such that
  - $\mathbf{M}^5 := \mathbf{M}^4[[T, S]][\mathrm{wk}_4 \mapsto \underline{w}]_{\mathrm{reg}}[\mathrm{wk}_5 \mapsto \widehat{\boldsymbol{l}_1}\,]_{\mathrm{reg}} \uplus \{[\boldsymbol{l}_1 \mapsto (\underline{w_0}, \underline{w_1})]\}_{\mathrm{heap}}$ for some $w, \boldsymbol{l}_1, w_0, w_1$,
  - $\mathbf{M}^5 \in \mathcal{A}.GR(\mathrm{gcbg}) \wedge \mathbf{M}^5 \in \mathcal{A}.MR(\mathrm{gcbg})$,
  - $\mathbf{M}^5$ repr Φ^5.

- As $\mathbf{M}^5.\mathrm{code} = \mathbf{M}^4.\mathrm{code}$, we execute the three instructions from $\mathrm{bg} + 3$ on the low side and get
  $$(\Phi^6, \mathrm{kpc}), \quad (M^3.h, K[\gamma\rho(\lambda x{:}\tau'.\, e)])$$
  such that
  - $\mathbf{M}^6 := \mathbf{M}^5[\boldsymbol{l}_1 : 0 \mapsto \mathrm{bg} + 6]_{\mathrm{hp}}[\boldsymbol{l}_1 : 1 \mapsto \mathbf{v}]_{\mathrm{hp}}$
  - $\mathbf{M}^6$ repr Φ^6.

- Let $W^6 := W^3 +\!\!+ \iota_{\boldsymbol{l}_1}$.
  Let $\iota_{\boldsymbol{l}_1} := \iota^{\mathrm{single}}(MR_{\boldsymbol{l}_1}, \emptyset)$.
  Let $MR_{\boldsymbol{l}_1} := \{\, (W, \mathbf{M}, M) \mid \mathbf{M}.\mathrm{hp}(\boldsymbol{l}_1)(0) = \underline{\mathrm{bg} + 6} \wedge \mathbf{M}.\mathrm{hp}(\boldsymbol{l}_1)(1) = \mathbf{v} \,\}$.
  Then $(\Phi^6, M^3) \in \mathcal{M}(W^6)$.

- By Theorem 9, it suffices to show that $((\Phi^6, \mathrm{kpc}), (M^3.h, K[\gamma\rho(\lambda x{:}\tau'.\, e)])) \in \mathcal{O}(W^6)$.
- As $W^6 \sqsupseteq_{\mathrm{pub}} W^3$ and $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau' \to \tau]\!]\rho(W^3)$, it suffices to show that
$$(\widehat{\boldsymbol{l}_1}, \lambda x{:}\rho.2(\tau').\, \gamma\rho e) \in \mathcal{V}[\![\tau' \to \tau]\!]\rho(W^6)$$
- It is easy to check that $(\widehat{\boldsymbol{l}_1}, \lambda x{:}\rho.2(\tau').\, \gamma\rho e) \in \mathrm{oftype}(\tau' \to \tau, \rho)(W^6)$.
- Suppose
$W^7 \sqsupseteq_{\triangleright} W^6$,
$(\mathbf{u}_1, u_2) \in \mathcal{V}[\![\tau']\!]\rho(W^7)$.
- To show:
$$(\mathbf{e}^7, (\gamma\rho e)[u_2/x]) \in \mathcal{E}[\![\tau]\!]\rho(W^7)$$
where
$\mathbf{e}^7 = (\langle \boldsymbol{l}_1 : 0 \rangle_{\mathrm{h}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{wk}_1) = \widehat{\boldsymbol{l}_1} \wedge \mathbf{M}.\mathrm{reg}(\mathrm{wk}_2) = \mathbf{u}_1 \,\})$
- By definition of $\mathcal{E}[\![\tau]\!]\rho(W^7)$ and plugc, suppose
- $((\mathrm{kpc}^7, \lfloor \mathrm{wk}_5 \rfloor), K^7) \in \mathcal{K}[\![\tau]\!]\rho(W^7)$
- $(\mathbf{M}^7, M^7) \in \mathcal{M}(W^7)$
- $\mathbf{M}^7$ repr Φ^7
- $\mathbf{M}^7.\mathrm{reg}(\mathrm{wk}_0) = \underline{\mathrm{kpc}^7}$
- $\mathbf{M}^7.\mathrm{reg}(\mathrm{wk}_1) = \widehat{\boldsymbol{l}_1}$
- $\mathbf{M}^7.\mathrm{reg}(\mathrm{wk}_2) = \mathbf{u}_1$
- As W^7 includes $\iota_{\boldsymbol{l}_1}$, we have $\mathbf{M}^7.\mathrm{hp}(\boldsymbol{l}_1)(0) = \underline{\mathrm{bg} + 6}$
- To show:
$$((\Phi^7, \mathrm{bg} + 6), (M^7.h, K^7[(\gamma, x \mapsto u_2)\rho e])) \in \mathcal{O}(W^7)$$
- As W^7 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the six instructions from $\mathrm{bg} + 6$ on the low side and get the following configurations
$$(\Phi^8, \mathrm{alloc}) \quad (M^7.h, K^7[(\gamma, x \mapsto u_2)\rho e])$$
such that
- $\mathbf{v}' := \mathbf{M}^7.\mathrm{reg}(\mathrm{sv}_0)$
- $\mathbf{M}^8 := \mathbf{M}^7[+\!+ \underline{\mathrm{kpc}^7}, \mathbf{v}']_{\mathrm{stk}}[\mathrm{wk}_4 \mapsto \underline{\mathrm{bg} + 12}]_{\mathrm{reg}}[\mathrm{wk}_5 \mapsto \underline{2}]_{\mathrm{reg}}$,
- $\mathbf{M}^8$ repr Φ^8.
- By the specifications of $\mathcal{A}$, after some finite number of steps of execution, we have configurations
$$(\Phi^9, \mathrm{bg} + 12), \quad (M^7.h, K^7[(\gamma, x \mapsto u_2)\rho e])$$
such that
- $\mathbf{M}^9 := \mathbf{M}^8[[T, S]][\mathrm{wk}_4 \mapsto \underline{w}]_{\mathrm{reg}}[\mathrm{wk}_5 \mapsto \widehat{\boldsymbol{l}_2}\,]_{\mathrm{reg}} \uplus \{[\boldsymbol{l}_2 \mapsto (\underline{w_0, w_1})]\}_{\mathrm{heap}}$ for some $w, \boldsymbol{l}_2, w_0, w_1$,
- $\mathbf{M}^9 \in \mathcal{A}.GR(\mathrm{gcbg}) \wedge \mathbf{M}^9 \in \mathcal{A}.MR(\mathrm{gcbg})$,
- $\mathbf{M}^9$ repr Φ^9.

- As W^7 includes $\iota_{\boldsymbol{l}_1}$, we have $\mathbf{M}^9.\mathrm{hp}(\boldsymbol{l}_1)(1) = \mathbf{M}^7.\mathrm{hp}(\boldsymbol{l}_1)(1) = \mathbf{v}$.
- We execute the four instructions from $\mathrm{bg}+12$ on the low side and get the following configurations
$$(\Phi^{10}, \mathrm{bg}+16) \quad (M^7.h, K^7[(\gamma, x \mapsto u_2)\rho e])$$
such that
- $\mathbf{M}^{10} := \mathbf{M}^9[\boldsymbol{l}_2 : 0 \mapsto \mathbf{u}_1]_{\mathrm{hp}}[\boldsymbol{l}_2 : 1 \mapsto \mathbf{v}]_{\mathrm{hp}}[\mathrm{sv}_0 \mapsto \widehat{\boldsymbol{l}_2}]_{\mathrm{reg}}[\mathrm{wk}_0 \mapsto \underline{\mathrm{bg}+c+16}]_{\mathrm{reg}}$,
- $\mathbf{M}^{10}$ repr Φ^{10}.
- Let $W^{10} := W^7[+\!\!+ \underline{\mathrm{kpc}^7}, \mathbf{v}']_1[\mathrm{sv}_0 \mapsto \widehat{\boldsymbol{l}_2}]_1 +\!\!+ \iota_{\boldsymbol{l}_2}$.
Let $\iota_{\boldsymbol{l}_2} := \iota^{\mathrm{single}}(MR_{\boldsymbol{l}_2}, \emptyset)$.
Let $MR_{\boldsymbol{l}_2} := \{\, (W, \mathbf{M}, M) \mid \mathbf{M}.\mathrm{hp}(\boldsymbol{l}_2)(0) = \mathbf{u}_1 \wedge \mathbf{M}.\mathrm{hp}(\boldsymbol{l}_2)(1) = \mathbf{v} \,\}$.
Then $(\Phi^{10}, M^7) \in \mathcal{M}(W^{10})$.
- By Theorem 9, it suffices to show that $((\Phi^{10}, \mathrm{bg}+16), (M^7.h, K^7[(\gamma, x \mapsto u_2)\rho e])) \in \mathcal{O}(W^{10})$.
- It is easy to check that $(W^{10}, \widehat{\boldsymbol{l}_2}, (\gamma, x \mapsto u_2)) \in \mathcal{G}[\![\Gamma, x : \tau']\!]\rho$.
- Thus, by $(*)$, it suffices to show that
$$((\mathrm{bg}+c+16, \lfloor \mathrm{wk}_5 \rfloor), K^7[-]) \in \mathcal{K}[\![\tau]\!]\rho(W^{10})$$
- Suppose
$W^{11} \sqsupseteq_{\mathrm{pub}} W^{10}$,
$(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho(W^{11})$,
$(\mathbf{M}^{11}, M^{11}) \in \mathcal{M}(W^{11})$,
$\mathbf{M}^{11}.\mathrm{reg}(\mathrm{wk}_5) = \mathbf{v}_1$,
$\mathbf{M}^{11}$ repr Φ^{11}.
- To show: $((\Phi^{11}, \mathrm{bg}+c+16), (M^{11}.h, K^7[v_2])) \in \mathcal{O}(W^{11})$
- As W^{11} includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the three instructions from $\mathrm{bg}+c+16$ on the low side and get the configurations
$$(\Phi^{12}, \mathrm{kpc}^7), \quad (M^{11}.h, K^7[v_2])$$
such that
- $\mathbf{M}^{12} := \mathbf{M}^{11}[\mathrm{sv}_0 \mapsto \mathbf{v}']_{\mathrm{reg}}[-2]_{\mathrm{stk}}$,
- $\mathbf{M}^{12}$ repr Φ^{12}.
- Let $W^{12} := W^{11}[\mathrm{sv}_0 \mapsto \mathbf{v}']_1[-2]_1$.
Then, $(\mathbf{M}^{12}, M^{11}) \in \mathcal{M}(W^{12})$.
- By Theorem 9, it suffices to show that $((\Phi^{12}, \mathrm{kpc}^7), (M^{11}.h, K^7[v_2])) \in \mathcal{O}(W^{12})$.
- As $W^{12} \sqsupseteq_{\mathrm{pub}} W^7$ and $((\mathrm{kpc}^7, \lfloor \mathrm{wk}_5 \rfloor), K^7) \in \mathcal{K}[\![\tau]\!]\rho(W^7)$, it suffices to show that
$$(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho(W^{12})$$
which follows from $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho(W^{11})$ by monotonicity of $\mathcal{V}[\![\tau]\!]\rho$.

□

9.7 App

$$(\!|\Gamma \vdash e_1\ e_2|\!) ::= \mathrm{Papp}((\!|\Gamma \vdash e_1|\!), (\!|\Gamma \vdash e_2|\!))$$

$\mathrm{Papp}(p_1, p_2) ::= \lambda\, \mathrm{alloc}, \mathrm{bg}.$
$\mathrm{let}\ \mathrm{instrs}_1 := p_1(\mathrm{alloc}, \mathrm{bg}+4),\ c_1 := |\mathrm{instrs}_1|,$
$\quad \mathrm{instrs}_2 := p_2(\mathrm{alloc}, \mathrm{bg}+c_1+6),\ c_2 := |\mathrm{instrs}_2|$
$\quad \mathrm{in}\quad [$

bg	`plus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{2}$
	`move`	$\langle \mathrm{sp}-2 \rangle_{\mathrm{s}}$	$\lfloor \mathrm{wk}_0 \rfloor$	
	`move`	$\langle \mathrm{sp}-1 \rangle_{\mathrm{s}}$	$\underline{0}$	
	`move`	$\lfloor \mathrm{wk}_0 \rfloor$	$\underline{\mathrm{bg}+c_1+4}$	
	instrs_1			
$\mathrm{bg}+c_1+4$	`move`	$\langle \mathrm{sp}-1 \rangle_{\mathrm{s}}$	$\lfloor \mathrm{wk}_5 \rfloor$	
	`move`	$\lfloor \mathrm{wk}_0 \rfloor$	$\underline{\mathrm{bg}+c_1+c_2+6}$	
	instrs_2			
$\mathrm{bg}+c_1+c_2+6$	`move`	$\lfloor \mathrm{wk}_0 \rfloor$	$\langle \mathrm{sp}-2 \rangle_{\mathrm{s}}$	
	`move`	$\lfloor \mathrm{wk}_1 \rfloor$	$\langle \mathrm{sp}-1 \rangle_{\mathrm{s}}$	
	`move`	$\lfloor \mathrm{wk}_2 \rfloor$	$\lfloor \mathrm{wk}_5 \rfloor$	
	`minus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{2}$
	`jmp`	$\langle \mathrm{wk}_1+0 \rangle_{\mathrm{h}}$		

$]$

Lemma 11 (Compatibility: App)**.**

$$\Delta;\Gamma \vdash p_1 \approx e_1 : \tau' \to \tau \wedge \Delta;\Gamma \vdash p_2 \approx e_2 : \tau' \implies \Delta;\Gamma \vdash \mathrm{Papp}(p_1,p_2) \approx e_1\ e_2 : \tau$$

Proof.

- For any $\mathcal{A}, \mathrm{gcbg}, \mathrm{bg}, k$, suppose
  - $W \sqsupseteq W_k^\circ(\mathcal{A}, \mathrm{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$
  - $\mathrm{code} := [\mathrm{bg} \Mapsto \mathrm{Papp}(p_1,p_2)(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg})]$
  - $\mathrm{code}^{p_1} := [\mathrm{bg}+4 \Mapsto p_1(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg}+4)],\ c_1 := |\mathrm{code}^{p_1}|$
  - $\mathrm{code}^{p_2} := [\mathrm{bg}+c_1+6 \Mapsto p_2(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg}+c_1+6)],\ c_2 := |\mathrm{code}^{p_2}|$
  - $\mathrm{code}^\bullet := \mathrm{code} \setminus \mathrm{code}^{p_1} \setminus \mathrm{code}^{p_2}$
  - $\mathbf{M}' = \mathbf{M} \uplus \{\mathrm{code}\}_{\mathrm{code}}$.
- Goal: find W^{pe} such that
  - $W^{pe} \sqsupseteq W \wedge \mathrm{lev}(W^{pe}) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta;\Gamma \vdash \mathrm{bg} \approx_{W^{pe}} e_1\ e_2 : \tau$
- Let $\mathbf{M}^1 := \mathbf{M} \uplus \{\mathrm{code}^\bullet\}_{\mathrm{code}}$.
  Let $W^1 := W +\!\!+ \iota^{\mathrm{code}}(\mathrm{code}^\bullet)$.
  By definition, we have $(\mathbf{M}^1, M) \in \mathcal{M}(W^1)$.
- Let $\mathbf{M}^2 := \mathbf{M}^1 \uplus \{\mathrm{code}^{p_1}\}_{\mathrm{code}}$.
  From $\Delta;\Gamma \vdash p_1 \approx e_1 : \tau' \to \tau$, we have W^2 such that
  - $W^2 \sqsupseteq W^1 \wedge \mathrm{lev}(W^2) = \mathrm{lev}(W^1)$
  - $(\mathbf{M}^2, M) \in \mathcal{M}(W^2)$
  - $(*)\ \Delta;\Gamma \vdash \mathrm{bg}+4 \approx_{W^2} e_1 : \tau' \to \tau$

- Let $\mathbf{M}^3 := \mathbf{M}^2 \uplus \{\mathrm{code}^{p_2}\}_{\mathrm{code}}$.
  From $\Delta; \Gamma \vdash p_2 \approx e_2 : \tau'$, we have W^3 such that
  - $W^3 \sqsupseteq W^2 \wedge \mathrm{lev}(W^3) = \mathrm{lev}(W^2)$
  - $(\mathbf{M}^3, M) \in \mathcal{M}(W^3)$
  - $(**)$ $\Delta; \Gamma \vdash \mathrm{bg} + c_1 + 6 \approx_{W^3} e_2 : \tau'$
- We now choose W^{pe} to be W^3 and show the required properties.
- $W^3 \sqsupseteq W \wedge \mathrm{lev}(W^3) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^3)$ holds vacuously.
- To show: $\forall W^4 \sqsupseteq W^3.\ \forall \rho \in \mathcal{D}[\![\Delta]\!].\ \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho(W^4).$
  $((\underline{\mathrm{bg}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v} \,\}), \gamma\rho(e_1\ e_2)) \in \mathcal{E}[\![\tau]\!]\rho(W^4)$
- By definition of $\mathcal{E}[\![\tau]\!]\rho(W^4)$ and plugc, we suppose
  - $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau]\!]\rho(W^4)$,
  - $(\mathbf{M}^4, M^4) \in \mathcal{M}(W^4)$,
  - $\mathbf{M}^4$ repr Φ^4,
  - $\mathbf{M}^4.\mathrm{reg}(\mathrm{wk}_0) = \underline{\mathrm{kpc}}$,
  - $\mathbf{M}^4.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v}$.
- To show: $((\Phi^4, \mathrm{bg}), (M^4.h, K[\gamma\rho(e_1\ e_2)])) \in \mathcal{O}(W^4)$
- As W^4 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the four instructions from bg on the low side and get the configurations

  $$(\Phi^5, \mathrm{bg} + 4), \quad (M^4.h, K[(\gamma\rho e_1)\ (\gamma\rho e_2)])$$

  such that
  - $\mathbf{M}^5 := \mathbf{M}^4[{+\!+}\, \underline{\mathrm{kpc}}, \underline{0}]_{\mathrm{stk}}[\mathrm{wk}_0 \mapsto \underline{\mathrm{bg} + c_1 + 4}]_{\mathrm{reg}}$,
  - $\mathbf{M}^5$ repr Φ^5.
- Let $W^5 := W^4[{+\!+}\, \underline{\mathrm{kpc}}, \underline{0}]_1$.
  Then $(\mathbf{M}^5, M^4) \in \mathcal{M}(W^5)$.
  By Theorem 9, it suffices to show that $((\Phi^5, \mathrm{bg} + 4), (M^4.h, K[(\gamma\rho e_1)\ (\gamma\rho e_2)])) \in \mathcal{O}(W^5)$.
- By $(*)$, it suffices to show that $((\mathrm{bg} + c_1 + 4, \lfloor \mathrm{wk}_5 \rfloor), K[(-)\ (\gamma\rho e_2)]) \in \mathcal{K}[\![\tau' \to \tau]\!]\rho(W^5)$.
- Suppose
  $W^6 \sqsupseteq_{\mathrm{pub}} W^5$,
  $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau' \to \tau]\!]\rho(W^6)$,
  $(\mathbf{M}^6, M^6) \in \mathcal{M}(W^6)$,
  $\mathbf{M}^6.\mathrm{reg}(\mathrm{wk}_5) = \mathbf{v}_1$,
  $\mathbf{M}^6$ repr Φ^6.
- To show: $((\Phi^6, \mathrm{bg} + c_1 + 4), (M^6.h, K[v_2\ (\gamma\rho e_2)])) \in \mathcal{O}(W^6)$
- As W^6 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the two instructions from $\mathrm{bg} + c_1 + 4$ on the low side and get the configurations

  $$(\Phi^7, \mathrm{bg} + c_1 + 6), \quad (M^6.h, K[v_2\ (\gamma\rho e_2)])$$

such that
- $\mathbf{M}^7 := \mathbf{M}^6[|\mathbf{M}^7.\mathrm{stk}| - 1 \mapsto \mathbf{v}_1]_{\mathrm{stk}}[\mathrm{wk}_0 \mapsto \underline{\mathrm{bg} + c_1 + c_2 + 6}]_{\mathrm{reg}}$,
- $\mathbf{M}^7$ repr Φ^7.

- Let $W^7 := W^6[|\mathbf{M}^7.\mathrm{stk}| - 1 \mapsto \mathbf{v}_1]_1$.
  Then $(\mathbf{M}^7, M^6) \in \mathcal{M}(W^7)$.
  By Theorem 9, it suffices to show that $((\Phi^7, \mathrm{bg} + c_1 + 6), (M^6.h, K[v_2\ (\gamma\rho e_2)])) \in \mathcal{O}(W^7)$.

- By $(**)$, it suffices to show that $((\mathrm{bg} + c_1 + c_2 + 6, \lfloor \mathrm{wk}_5 \rfloor), K[v_2\ (-)]) \in \mathcal{K}[\![\tau']\!]\rho(W^7)$.

- Suppose
  $W^8 \sqsupseteq_{\mathrm{pub}} W^7$,
  $(\mathbf{v}_3, v_4) \in \mathcal{V}[\![\tau']\!]\rho(W^8)$,
  $(\mathbf{M}^8, M^8) \in \mathcal{M}(W^8)$,
  $\mathbf{M}^8.\mathrm{reg}(\mathrm{wk}_5) = \mathbf{v}_3$,
  $\mathbf{M}^8$ repr Φ^8.

- To show: $((\Phi^8, \mathrm{bg} + c_1 + c_2 + 6), (M^8.h, K[v_2\ v_4])) \in \mathcal{O}(W^8)$

- As $(\mathbf{v}_1, v_2) \in \mathrm{oftype}(\tau' \to \tau, \rho)(W^8)$ by Theorems 5 and 4, we have
  - $\mathbf{v}_1 = \widehat{\boldsymbol{l}_1}$,
  - $\mathbf{M}^8.\mathrm{hp}(\boldsymbol{l}_1)(0) = \underline{w}$ for some w,
  - $v_2 = \lambda x{:}\tau'.\, e_2$ for some e_2.

- As W^8 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the five instructions from $\mathrm{bg} + c_1 + c_2 + 6$ in the low side, take one step in the high side and get the two configurations

$$(\Phi^9, w), \quad (M^8, K[e_2[v_4/x]])$$

  such that
  - $\mathbf{M}^9 := \mathbf{M}^8[\mathrm{wk}_0 \mapsto \underline{\mathrm{kpc}}]_{\mathrm{reg}}[\mathrm{wk}_1 \mapsto \widehat{\boldsymbol{l}_1}]_{\mathrm{reg}}[\mathrm{wk}_2 \mapsto \mathbf{v}_3]_{\mathrm{reg}}[-2]_{\mathrm{stk}}$,
  - $\mathbf{M}^9$ repr Φ^9.

- Let $W^9 := \triangleright W^8[-2]_1$.
  Then $(\mathbf{M}^9, M^8) \in \mathcal{M}(W^9)$
  By Theorem 9, it suffices to show that $((\Phi^9, w), (M^8, K[e_2[v_4/x]])) \in \mathcal{O}(W^9)$.

- We have
  - $W^9 \sqsupseteq_{\triangleright} W^6$ by Lemma 2,
  - $(\mathbf{v}_3, v_4) \in \mathcal{V}[\![\tau']\!]\rho(W^9)$ by Theorem 5.
  Thus from $(\widehat{\boldsymbol{l}_1}, \lambda x{:}\tau'.\, e_2) \in \mathcal{V}[\![\tau' \to \tau]\!]\rho(W^6)$, we have
  - $((\langle \boldsymbol{l}_1 : 0\rangle_{\mathrm{h}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{wk}_1) = \widehat{\boldsymbol{l}_1} \wedge \mathbf{M}.\mathrm{reg}(\mathrm{wk}_2) = \mathbf{v}_3\}), e_2[v_4/x]) \in \mathcal{E}[\![\tau]\!]\rho(W^9)$.

- By definition of $\mathcal{E}[\![\tau]\!]\rho(W^9)$, it suffices to show that $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau]\!]\rho(W^9)$, which follows from the fact that $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau]\!]\rho(W^4)$ and $W^9 \sqsupseteq_{\mathrm{pub}} W^4$ by Theorem 6.

□

9.8 Gen

$$(\!|\Gamma \vdash \Lambda\alpha.e|\!) ::= \mathrm{Pgen}((\!|\Gamma \vdash e|\!))$$

$\mathrm{Pgen}(p) := \lambda\, \mathrm{alloc}, \mathrm{bg}.$
$\mathrm{let\ code} := p(\mathrm{alloc}, \mathrm{bg}+11),\ c := |\mathrm{code}| \quad \mathrm{in} \quad [$

bg	`move`	$\lfloor \mathrm{wk}_4 \rfloor$	$\underline{\mathrm{bg}+3}$	
	`move`	$\lfloor \mathrm{wk}_5 \rfloor$	$\underline{2}$	
	`jmp`	$\underline{\mathrm{alloc}}$		
$\mathrm{bg}+3$	`move`	$\langle \mathrm{wk}_5 + 0 \rangle_{\mathrm{h}}$	$\underline{\mathrm{bg}+6}$	
	`move`	$\langle \mathrm{wk}_5 + 1 \rangle_{\mathrm{h}}$	$\underline{\lfloor \mathrm{sv}_0 \rfloor}$	
	`jmp`	$\lfloor \mathrm{wk}_0 \rfloor$		
$\mathrm{bg}+6$	`plus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{2}$
	`move`	$\langle \mathrm{sp}-2 \rangle_{\mathrm{s}}$	$\lfloor \mathrm{wk}_0 \rfloor$	
	`move`	$\langle \mathrm{sp}-1 \rangle_{\mathrm{s}}$	$\lfloor \mathrm{sv}_0 \rfloor$	
	`move`	$\lfloor \mathrm{sv}_0 \rfloor$	$\langle \mathrm{wk}_1 + 1 \rangle_{\mathrm{h}}$	
	`move`	$\lfloor \mathrm{wk}_0 \rfloor$	$\underline{\mathrm{bg}+c+11}$	
	code			
$\mathrm{bg}+c+11$	`move`	$\lfloor \mathrm{sv}_0 \rfloor$	$\langle \mathrm{sp}-1 \rangle_{\mathrm{s}}$	
	`minus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{2}$
	`jmp`	$\langle \mathrm{sp}-0 \rangle_{\mathrm{s}}$		

$]$

Lemma 12 (Compatibility: Gen)**.**

$$\Delta, \alpha; \Gamma \vdash p \approx e : \tau \implies \Delta; \Gamma \vdash \mathrm{Pgen}(p) \approx \Lambda\alpha.e : \forall\alpha.\, \tau$$

Proof.

- For any $\mathcal{A}, \mathrm{gcbg}, \mathrm{bg}, k$, suppose
  - $W \sqsupseteq W_k^\circ(\mathcal{A}, \mathrm{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$
  - $\mathrm{code} := [\mathrm{bg} \Mapsto \mathrm{Pgen}(p)(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg})]$
  - $\mathrm{code}^p := [\mathrm{bg}+11 \Mapsto p(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg}+11)],\ c := |\mathrm{code}^p|$
  - $\mathrm{code}^\bullet := \mathrm{code} \setminus \mathrm{code}^p$
  - $\mathbf{M}' = \mathbf{M} \uplus \{\mathrm{code}\}_{\mathrm{code}}$.

- Goal: find W^{pe} such that
  - $W^{pe} \sqsupseteq W \wedge \mathrm{lev}(W^{pe}) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta; \Gamma \vdash \mathrm{bg} \approx_{W^{pe}} \Lambda\alpha.e : \forall\alpha.\, \tau$

- Let $\mathbf{M}^1 := \mathbf{M} \uplus \{\mathrm{code}^\bullet\}_{\mathrm{code}}$.
  Let $W^1 := W +\!\!+ \iota^{\mathrm{code}}(\mathrm{code}^\bullet)$.
  By definition, we have $(\mathbf{M}^1, M) \in \mathcal{M}(W^1)$.

- Let $\mathbf{M}^2 := \mathbf{M}^1 \uplus \{\mathrm{code}^p\}_{\mathrm{code}}$.
  From $\Delta, \alpha; \Gamma \vdash p \approx e : \tau$, we have W^2 such that
  - $W^2 \sqsupseteq W^1 \wedge \mathrm{lev}(W^2) = \mathrm{lev}(W^1)$
  - $(\mathbf{M}^2, M) \in \mathcal{M}(W^2)$
  - $(*)\ \Delta, \alpha; \Gamma \vdash \mathrm{bg}+11 \approx_{W^2} e : \tau$

- We now choose W^{pe} to be W^2 and show the required properties.
- $W^2 \sqsupseteq W \wedge \mathrm{lev}(W^2) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^2)$ holds vacuously.
- To show: $\forall W^3 \sqsupseteq W^2.\ \forall \rho \in \mathcal{D}[\![\Delta]\!].\ \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho(W^3).$
  $((\underline{\mathrm{bg}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v} \,\}), \gamma\rho(\Lambda\alpha.e)) \in \mathcal{E}[\![\forall\alpha.\,\tau]\!]\rho(W^3)$
- By definition of $\mathcal{E}[\![\forall\alpha.\,\tau]\!]\rho(W^3)$ and plugc, we suppose
  - $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\forall\alpha.\,\tau]\!]\rho(W^3)$,
  - $(\mathbf{M}^3, M^3) \in \mathcal{M}(W^3)$,
  - $\mathbf{M}^3$ repr Φ^3,
  - $\mathbf{M}^3.\mathrm{reg}(\mathrm{wk}_0) = \underline{\mathrm{kpc}}$,
  - $\mathbf{M}^3.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v}$.
- To show: $((\Phi^3, \mathrm{bg}), (M^3.h, K[\gamma\rho(\Lambda\alpha.e)])) \in \mathcal{O}(W^3)$
- As W^3 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the three instructions from bg on the low side and get the configurations
  $$(\Phi^4, \mathrm{alloc}), \quad (M^3.h, K[\gamma\rho(\Lambda\alpha.e)])$$
  such that
  - $\mathbf{M}^4 := \mathbf{M}^3[\mathrm{wk}_4 \mapsto \underline{\mathrm{bg}+3}]_{\mathrm{reg}}[\mathrm{wk}_5 \mapsto \underline{2}]_{\mathrm{reg}}$,
  - $\mathbf{M}^4$ repr Φ^4.
- By the specifications of $\mathcal{A}$, after some finite number of steps of execution, we have configurations
  $$(\Phi^5, \mathrm{bg}+3), \quad (M^3.h, K[\gamma\rho(\Lambda\alpha.e)])$$
  such that
  - $\mathbf{M}^5 := \mathbf{M}^4[[T, S]][\mathrm{wk}_4 \mapsto \underline{w}]_{\mathrm{reg}}[\mathrm{wk}_5 \mapsto \widehat{\boldsymbol{l}_1}\,]_{\mathrm{reg}} \uplus \{[\boldsymbol{l}_1 \mapsto (\underline{w_0}, \underline{w_1})]\}_{\mathrm{heap}}$ for some $w, \boldsymbol{l}_1, w_0, w_1$,
  - $\mathbf{M}^5 \in \mathcal{A}.GR(\mathrm{gcbg}) \wedge \mathbf{M}^5 \in \mathcal{A}.MR(\mathrm{gcbg})$,
  - $\mathbf{M}^5$ repr Φ^5.
- As $\mathbf{M}^5.\mathrm{code} = \mathbf{M}^4.\mathrm{code}$, we execute the three instructions from $\mathrm{bg}+3$ on the low side and get
  $$(\Phi^6, \mathrm{kpc}), \quad (M^3.h, K[\gamma\rho(\Lambda\alpha.e)])$$
  such that
  - $\mathbf{M}^6 := \mathbf{M}^5[\boldsymbol{l}_1 : 0 \mapsto \mathrm{bg}+6]_{\mathrm{hp}}[\boldsymbol{l}_1 : 1 \mapsto \mathbf{v}]_{\mathrm{hp}}$
  - $\mathbf{M}^6$ repr Φ^6.
- Let $W^6 := W^3 +\!\!+ \iota_{\boldsymbol{l}_1}$.
  Let $\iota_{\boldsymbol{l}_1} := \iota^{\mathrm{single}}(MR_{\boldsymbol{l}_1}, \emptyset)$.
  Let $MR_{\boldsymbol{l}_1} := \{\, (W, \mathbf{M}, M) \mid \mathbf{M}.\mathrm{hp}(\boldsymbol{l}_1)(0) = \underline{\mathrm{bg}+6} \wedge \mathbf{M}.\mathrm{hp}(\boldsymbol{l}_1)(1) = \mathbf{v} \,\}$.
  Then $(\Phi^6, M^3) \in \mathcal{M}(W^6)$.
- By Theorem 9, it suffices to show that $((\Phi^6, \mathrm{kpc}), (M^3.h, K[\gamma\rho(\Lambda\alpha.e)])) \in \mathcal{O}(W^6)$.
- As $W^6 \sqsupseteq_{\mathrm{pub}} W^3$ and $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\forall\alpha.\,\tau]\!]\rho(W^3)$, it suffices to show that
  $$(\widehat{\boldsymbol{l}_1}, \Lambda\alpha.\gamma\rho e) \in \mathcal{V}[\![\forall\alpha.\,\tau]\!]\rho(W^6)$$

- It is easy to check that $(\widehat{\boldsymbol{l}_1}, \Lambda\alpha.\gamma\rho e) \in \mathrm{oftype}(\forall\alpha.\,\tau, \rho)(W^6)$.
- Suppose
  $W^7 \sqsupset_{\triangleright} W^6$,
  $(\tau_1', \tau_2', R) \in \mathrm{TyValRel}$.
- To show:
  $$(\mathbf{e}^7, (\gamma\rho e)[\tau_2'/\alpha]) \in \mathcal{E}[\![\tau]\!]\rho(W^7)$$
  where
  $\mathbf{e}^7 = (\langle \boldsymbol{l}_1 : 0\rangle_{\mathrm{h}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{wk}_1) = \widehat{\boldsymbol{l}_1} \,\})$
- By definition of $\mathcal{E}[\![\tau]\!]\rho(W^7)$ and plugc, suppose
  - $((\mathrm{kpc}^7, \lfloor \mathrm{wk}_5 \rfloor), K^7) \in \mathcal{K}[\![\tau]\!]\rho(W^7)$
  - $(\mathbf{M}^7, M^7) \in \mathcal{M}(W^7)$
  - $\mathbf{M}^7$ repr Φ^7
  - $\mathbf{M}^7.\mathrm{reg}(\mathrm{wk}_0) = \underline{\mathrm{kpc}^7}$
  - $\mathbf{M}^7.\mathrm{reg}(\mathrm{wk}_1) = \widehat{\boldsymbol{l}_1}$
- As W^7 includes $\iota_{\boldsymbol{l}_1}$, we have $\mathbf{M}^7.\mathrm{hp}(\boldsymbol{l}_1)(0) = \underline{\mathrm{bg} + 6}$
- To show:
  $$((\Phi^7, \mathrm{bg} + 6), (M^7.h, K^7[\gamma(\rho, \alpha \mapsto (\tau_1', \tau_2', R))e])) \in \mathcal{O}(W^7)$$
- As W^7 includes $\iota_{\boldsymbol{l}_1}$, we have $\mathbf{M}^7.\mathrm{hp}(\boldsymbol{l}_1)(1) = \mathbf{v}$.
- As W^7 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the five instructions from $\mathrm{bg} + 6$ on the low side and get the following configurations
  $$(\Phi^8, \mathrm{alloc}) \quad (M^7.h, K^7[\gamma(\rho, \alpha \mapsto (\tau_1', \tau_2', R))e])$$
  such that
  - $\mathbf{v}' := \mathbf{M}^7.\mathrm{reg}(\mathrm{sv}_0)$
  - $\mathbf{M}^8 := \mathbf{M}^7[{+\!+}\,\underline{\mathrm{kpc}^7}, \mathbf{v}']_{\mathrm{stk}}[\mathrm{sv}_0 \mapsto \mathbf{v}]_{\mathrm{reg}}[\mathrm{wk}_0 \mapsto \underline{\mathrm{bg} + c + 11}]_{\mathrm{reg}}$,
  - $\mathbf{M}^8$ repr Φ^8.
- Let $W^8 := W^7[{+\!+}\,\underline{\mathrm{kpc}^7}, \mathbf{v}']_1[\mathrm{sv}_0 \mapsto \mathbf{v}]_1$.
  Then $(\Phi^8, M^7) \in \mathcal{M}(W^8)$.
- By Theorem 9, it suffices to show that
  $$((\Phi^8, \mathrm{bg} + 16), (M^7.h, K^7[\gamma(\rho, \alpha \mapsto (\tau_1', \tau_2', R))e])) \in \mathcal{O}(W^8)$$
- As $(\mathbf{v}, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho(W^3)$, we have $(\mathbf{v}, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho(W^8)$ by Theorem 13. Also, as $\alpha \notin \mathrm{dom}(\rho)$, we have $(\mathbf{v}, \gamma) \in \mathcal{G}[\![\Gamma]\!](\rho, \alpha \mapsto (\tau_1', \tau_2', R))(W^8)$.
- Thus, by $(*)$, it suffices to show that
  $$((\mathrm{bg} + c + 11, \lfloor \mathrm{wk}_5 \rfloor), K^7[-]) \in \mathcal{K}[\![\tau]\!]\rho(W^8)$$

- Suppose
  $W^9 \sqsupseteq_{\text{pub}} W^8$,
  $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho(W^9)$,
  $(\mathbf{M}^9, M^9) \in \mathcal{M}(W^9)$,
  $\mathbf{M}^9.\text{reg}(\text{wk}_5) = \mathbf{v}_1$,
  $\mathbf{M}^9$ repr Φ^9.
- To show: $((\Phi^9, \text{bg} + c + 11), (M^9.h, K^7[v_2])) \in \mathcal{O}(W^9)$
- As W^9 includes $\iota^{\text{code}}(\text{code}^\bullet)$, we execute the three instructions from $\text{bg} + c + 11$ on the low side and get the configurations

  $$(\Phi^{10}, \text{kpc}^7), \quad (M^9.h, K^7[v_2])$$

  such that
  - $\mathbf{M}^{10} := \mathbf{M}^9[\text{sv}_0 \mapsto \mathbf{v}']_{\text{reg}}[-2]_{\text{stk}}$,
  - $\mathbf{M}^{10}$ repr Φ^{10}.
- Let $W^{10} := W^9[\text{sv}_0 \mapsto \mathbf{v}']_1[-2]_1$.
  Then, $(\mathbf{M}^{10}, M^9) \in \mathcal{M}(W^{10})$.
- By Theorem 9, it suffices to show that $((\Phi^{10}, \text{kpc}^7), (M^9.h, K^7[v_2])) \in \mathcal{O}(W^{10})$.
- As $W^{10} \sqsupseteq_{\text{pub}} W^7$ and $((\text{kpc}^7, \lfloor \text{wk}_5 \rfloor), K^7) \in \mathcal{K}[\![\tau]\!]\rho(W^7)$, it suffices to show that

  $$(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho(W^{10})$$

  which follows from $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho(W^9)$ by monotonicity of $\mathcal{V}[\![\tau]\!]\rho$.

□

9.9 Inst

$$(\!|\Gamma \vdash e\ \tau|\!) ::= \text{Pinst}((\!|\Gamma \vdash e|\!))$$

$\text{Pinst}(p) ::= \lambda\, \text{alloc}, \text{bg}.$
let code $:= p(\text{alloc}, \text{bg} + 3),\ c := |\text{code}|$ in [

bg	`plus`	$\lfloor \text{sp} \rfloor$	$\lfloor \text{sp} \rfloor$	$\underline{1}$
	`move`	$\langle \text{sp} - 1 \rangle_{\text{s}}$	$\lfloor \text{wk}_0 \rfloor$	
	`move`	$\lfloor \text{wk}_0 \rfloor$	$\underline{\text{bg} + c + 3}$	
	code			
$\text{bg} + c + 3$	`move`	$\lfloor \text{wk}_0 \rfloor$	$\langle \text{sp} - 1 \rangle_{\text{s}}$	
	`move`	$\lfloor \text{wk}_1 \rfloor$	$\lfloor \text{wk}_5 \rfloor$	
	`minus`	$\lfloor \text{sp} \rfloor$	$\lfloor \text{sp} \rfloor$	$\underline{1}$
	`jmp`	$\langle \text{wk}_1 + 0 \rangle_{\text{h}}$		

]

Lemma 13 (Compatibility: Inst)**.**

$$\Delta; \Gamma \vdash p \approx e : \forall \alpha.\, \tau \implies \Delta; \Gamma \vdash \text{Pinst}(p) \approx e\ \tau' : \tau[\tau'/\alpha]$$

Proof.

- For any $\mathcal{A}, \mathrm{gcbg}, \mathrm{bg}, k$, suppose
  - $W \sqsupseteq W_k^\circ(\mathcal{A}, \mathrm{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$
  - $\mathrm{code} := [\mathrm{bg} \Mapsto \mathrm{Pinst}(p)(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg})]$
  - $\mathrm{code}^p := [\mathrm{bg}+3 \Mapsto p(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg}+3)]$, $c := |\mathrm{code}^p|$
  - $\mathrm{code}^\bullet := \mathrm{code} \setminus \mathrm{code}^p$
  - $\mathbf{M}' = \mathbf{M} \uplus \{\mathrm{code}\}_{\mathrm{code}}$.
- Goal: find W^{pe} such that
  - $W^{pe} \sqsupseteq W \wedge \mathrm{lev}(W^{pe}) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta; \Gamma \vdash \mathrm{bg} \approx_{W^{pe}} e\ \tau' : \tau[\tau'/\alpha]$
- Let $\mathbf{M}^1 := \mathbf{M} \uplus \{\mathrm{code}^\bullet\}_{\mathrm{code}}$.
  Let $W^1 := W +\!\!+ \iota^{\mathrm{code}}(\mathrm{code}^\bullet)$.
  By definition, we have $(\mathbf{M}^1, M) \in \mathcal{M}(W^1)$.
- Let $\mathbf{M}^2 := \mathbf{M}^1 \uplus \{\mathrm{code}^p\}_{\mathrm{code}}$.
  From $\Delta; \Gamma \vdash p \approx e : \forall\alpha.\,\tau$, we have W^2 such that
  - $W^2 \sqsupseteq W^1 \wedge \mathrm{lev}(W^2) = \mathrm{lev}(W^1)$
  - $(\mathbf{M}^2, M) \in \mathcal{M}(W^2)$
  - $(*)$ $\Delta; \Gamma \vdash \mathrm{bg}+3 \approx_{W^2} e : \forall\alpha.\,\tau$
- We now choose W^{pe} to be W^2 and show the required properties.
- $W^2 \sqsupseteq W \wedge \mathrm{lev}(W^2) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^2)$ holds vacuously.
- To show: $\forall W^3 \sqsupseteq W^2.\ \forall\rho \in \mathcal{D}[\![\Delta]\!].\ \forall(\mathbf{v}, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho(W^3).$
  $((\underline{\mathrm{bg}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v} \,\}), \gamma\rho(e\ \tau')) \in \mathcal{E}[\![\tau[\tau'/\alpha]]\!]\rho(W^3)$
- By definition of $\mathcal{E}[\![\tau[\tau'/\alpha]]\!]\rho(W^3)$ and plugc, we suppose
  - $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau[\tau'/\alpha]]\!]\rho(W^3)$,
  - $(\mathbf{M}^3, M^3) \in \mathcal{M}(W^3)$,
  - $\mathbf{M}^3$ repr Φ^3,
  - $\mathbf{M}^3.\mathrm{reg}(\mathrm{wk}_0) = \underline{\mathrm{kpc}}$,
  - $\mathbf{M}^3.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v}$.
- To show: $((\Phi^3, \mathrm{bg}), (M^3.h, K[\gamma\rho(e\ \tau')])) \in \mathcal{O}(W^3)$
- As W^3 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the three instructions from bg on the low side and get the configurations

$$(\Phi^4, \mathrm{bg}+3), \quad (M^3.h, K[(\gamma\rho e)\ (\rho.2(\tau'))])$$

  such that
  - $\mathbf{M}^4 := \mathbf{M}^3[+\!\!+ \underline{\mathrm{kpc}}]_{\mathrm{stk}}[\mathrm{wk}_0 \mapsto \underline{\mathrm{bg}+c+3}]_{\mathrm{reg}}$,
  - $\mathbf{M}^4$ repr Φ^4.
- Let $W^4 := W^3[+\!\!+ \underline{\mathrm{kpc}}]_1$.
  Then $(\mathbf{M}^4, M^3) \in \mathcal{M}(W^4)$.
  By Theorem 9, it suffices to show that $((\Phi^4, \mathrm{bg}+3), (M^3.h, K[(\gamma\rho e)\ (\rho.2(\tau'))])) \in \mathcal{O}(W^4)$.

- By $(*)$, it suffices to show that $((\mathrm{bg}+c+3, \lfloor \mathrm{wk}_5 \rfloor), K[-\ (\rho.2(\tau'))]) \in \mathcal{K}[\![\forall\alpha.\,\tau]\!]\rho(W^4)$.

- Suppose
  $W^5 \sqsupseteq_{\mathrm{pub}} W^4$,
  $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\forall\alpha.\,\tau]\!]\rho(W^5)$,
  $(\mathbf{M}^5, M^5) \in \mathcal{M}(W^5)$,
  $\mathbf{M}^5.\mathrm{reg}(\mathrm{wk}_5) = \mathbf{v}_1$,
  $\mathbf{M}^5$ repr Φ^5.

- To show: $((\Phi^5, \mathrm{bg}+c+3), (M^5.h, K[v_2\ (\rho.2(\tau'))])) \in \mathcal{O}(W^5)$

- If $\mathrm{lev}(W^5) = 0$ then it trivially holds.
  Assume that $\mathrm{lev}(W^5) > 0$.

- As $(\mathbf{v}_1, v_2) \in \mathrm{oftype}(\forall\alpha.\,\tau, \rho)(W^5)$ by Theorems 5 and 4, we have
  - $\mathbf{v}_1 = \widehat{\boldsymbol{l}_1}$,
  - $\mathbf{M}^5.\mathrm{hp}(\boldsymbol{l}_1)(0) = \underline{w}$ for some w,
  - $v_2 = \Lambda\alpha.e_2$ for some e_2.

- As W^5 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the four instructions from $\mathrm{bg}+c+3$ in the low side, take one step in the high side and get the two configurations

$$(\Phi^6, w), \quad (M^5, K[e_2[\rho.2(\tau')/\alpha]])$$

  such that
  - $\mathbf{M}^6 := \mathbf{M}^5[\mathrm{wk}_0 \mapsto \underline{\mathrm{kpc}}]_{\mathrm{reg}}[\mathrm{wk}_1 \mapsto \widehat{\boldsymbol{l}_1}]_{\mathrm{reg}}[-1]_{\mathrm{stk}}$,
  - $\mathbf{M}^6$ repr Φ^6.

- Let $W^6 := \triangleright W^5[-1]_1$.
  Then $(\mathbf{M}^6, M^5) \in \mathcal{M}(W^6)$
  By Theorem 9, it suffices to show that $((\Phi^6, w), (M^5, K[e_2[\rho.2(\tau')/\alpha]])) \in \mathcal{O}(W^6)$.

- We have
  - $W^6 \sqsupset_{\triangleright} W^5$ by Lemma 2,
  - $(\rho.1(\tau'), \rho.2(\tau'), \mathcal{V}[\![\tau']\!]\rho) \in \mathrm{WVRel}$.
  Thus from $(\widehat{\boldsymbol{l}_1}, \Lambda\alpha.e_2) \in \mathcal{V}[\![\forall\alpha.\,\tau]\!]\rho(W^5)$, we have
  - $((\langle \boldsymbol{l}_1 : 0\rangle_{\mathrm{h}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{wk}_1) = \widehat{\boldsymbol{l}_1}\}), e_2[\rho.2(\tau')/\alpha]) \in \mathcal{E}[\![\tau]\!](\rho, \alpha \mapsto (\rho.1(\tau'), \rho.2(\tau'), \mathcal{V}[\![\tau']\!]\rho))(W^6)$.

- By definition of $\mathcal{E}[\![\tau]\!](\rho, \alpha \mapsto (\rho.1(\tau'), \rho.2(\tau'), \mathcal{V}[\![\tau']\!]\rho))(W^6)$, it suffices to show that

$$((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau]\!](\rho, \alpha \mapsto (\rho.1(\tau'), \rho.2(\tau'), \mathcal{V}[\![\tau']\!]\rho))(W^6)$$

- As $\mathcal{V}[\![\tau]\!](\rho, \alpha \mapsto (\rho.1(\tau'), \rho.2(\tau'), \mathcal{V}[\![\tau']\!]\rho)) = \mathcal{V}[\![\tau[\tau'/\alpha]]\!]\rho$ by Theorem 7, it suffices to show that $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau[\tau'/\alpha]]\!]\rho(W^6)$, which follows from $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau[\tau'/\alpha]]\!]\rho(W^3)$ and $W^6 \sqsupseteq_{\mathrm{pub}} W^3$ by Theorem 6.

□

9.10 Pack

$$(\!|\Gamma \vdash \mathsf{pack}\ \langle \tau_1, e\rangle\ \mathsf{as}\ \tau_2|\!) ::= \mathrm{Ppack}((\!|\Gamma \vdash e|\!))$$

$$\mathrm{Ppack}(p) ::= p$$

Lemma 14 (Compatibility: Pack)**.**

$$\Delta; \Gamma \vdash p \approx e : \tau[\tau'/\alpha] \implies \Delta; \Gamma \vdash \mathrm{Ppack}(p) \approx \mathsf{pack}\ \langle \tau', e\rangle\ \mathsf{as}\ \exists\alpha.\,\tau : \exists\alpha.\,\tau$$

Proof.

- For any $\mathcal{A}, \mathrm{gcbg}, \mathrm{bg}, k$, suppose
  - $W \sqsupseteq W_k^\circ(\mathcal{A}, \mathrm{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$
  - $\mathrm{code} := [\mathrm{bg} \Mapsto p(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg})]$
  - $\mathbf{M}' = \mathbf{M} \uplus \{\mathrm{code}\}_{\mathrm{code}}$.
- Goal: find W^{pe} such that
  - $W^{pe} \sqsupseteq W \wedge \mathrm{lev}(W^{pe}) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta; \Gamma \vdash \mathrm{bg} \approx_{W^{pe}} \mathsf{pack}\ \langle \tau', e\rangle\ \mathsf{as}\ \exists\alpha.\,\tau : \exists\alpha.\,\tau$
- From $\Delta; \Gamma \vdash p \approx e : \tau[\tau'/\alpha]$, we have W^1 such that
  - $W^1 \sqsupseteq W \wedge \mathrm{lev}(W^1) = \mathrm{lev}(W)$
  - $(\mathbf{M}', M) \in \mathcal{M}(W^1)$
  - $(*)\ \Delta; \Gamma \vdash \mathrm{bg} \approx_{W^1} e : \tau[\tau'/\alpha]$
- We now choose W^{pe} to be W^1 and show the required properties.
- $W^1 \sqsupseteq W \wedge \mathrm{lev}(W^1) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^1)$ holds vacuously.
- To show: $\forall W^2 \sqsupseteq W^1.\ \forall \rho \in \mathcal{D}[\![\Delta]\!].\ \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho(W^2).$
  $((\underline{\mathrm{bg}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v}\,\}), \gamma\rho(\mathsf{pack}\ \langle \tau', e\rangle\ \mathsf{as}\ \exists\alpha.\,\tau)) \in \mathcal{E}[\![\exists\alpha.\,\tau]\!]\rho(W^2)$
- By definition of $\mathcal{E}[\![\exists\alpha.\,\tau]\!]\rho(W^2)$ and plugc, we suppose
  - $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\exists\alpha.\,\tau]\!]\rho(W^2)$,
  - $(\mathbf{M}^2, M^2) \in \mathcal{M}(W^2)$,
  - $\mathbf{M}^2$ repr Φ^2,
  - $\mathbf{M}^2.\mathrm{reg}(\mathrm{wk}_0) = \underline{\mathrm{kpc}}$,
  - $\mathbf{M}^2.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v}$.
- To show: $((\Phi^2, \mathrm{bg}), (M^2.h, K[\mathsf{pack}\ \langle \rho.2(\tau'), \gamma\rho e\rangle\ \mathsf{as}\ \exists\alpha.\,\rho.2(\tau)])) \in \mathcal{O}(W^2)$
- By $(*)$, it suffices to show that $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K[\mathsf{pack}\ \langle \rho.2(\tau'), -\rangle\ \mathsf{as}\ \exists\alpha.\,\rho.2(\tau)]) \in \mathcal{K}[\![\tau[\tau'/\alpha]]\!]\rho(W^2)$.
- Suppose
  $W^3 \sqsupseteq_{\mathrm{pub}} W^2$,
  $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau[\tau'/\alpha]]\!]\rho(W^3)$,
  $(\mathbf{M}^3, M^3) \in \mathcal{M}(W^3)$,
  $\mathbf{M}^3.\mathrm{reg}(\mathrm{wk}_5) = \mathbf{v}_1$,
  $\mathbf{M}^3$ repr Φ^3.
- To show: $((\Phi^3, \mathrm{kpc}), (M^3.h, K[\mathsf{pack}\ \langle \rho.2(\tau'), v_2\rangle\ \mathsf{as}\ \exists\alpha.\,\rho.2(\tau)])) \in \mathcal{O}(W^3)$

- As $W^3 \sqsupseteq_{\text{pub}} W^2$ and $((\text{kpc}, \lfloor \text{wk}_5 \rfloor), K) \in \mathcal{K}[\![\exists \alpha.\, \tau]\!]\rho(W^2)$, it suffices to show that

$$(\mathbf{v}_1, \mathsf{pack}\ \langle \rho.2(\tau'), v_2 \rangle\ \mathsf{as}\ \exists \alpha.\, \rho.2(\tau)) \in \mathcal{V}[\![\exists \alpha.\, \tau]\!]\rho(W^3)$$

- By definition of $\mathcal{V}[\![\exists \alpha.\, \tau]\!]\rho$ and instantiating α with $(\rho.1(\tau'), \rho.2(\tau'), \mathcal{V}[\![\tau']\!]\rho)$, it remains to show that

$$(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto (\rho.1(\tau'), \rho.2(\tau'), \mathcal{V}[\![\tau']\!]\rho)](W^3)$$

- It follows from $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau[\tau'/\alpha]]\!]\rho(W^3)$ by Theorem 7.

□

9.11 Unpack

$$(\!|\Gamma \vdash \mathsf{unpack}\ e_1\ \mathsf{as}\ \langle \alpha, x \rangle\ \mathsf{in}\ e_2|\!) ::= \text{Punpack}((\!|\Gamma \vdash e_1|\!), (\!|\Gamma, x \vdash e_2|\!))$$

$\text{Punpack}(p_1, p_2) := \lambda\, \text{alloc}, \text{bg}.$
let $\text{instrs}_1 := p_1(\text{alloc}, \text{bg} + 3),\ c_1 := |\text{instrs}_1|,$
$\quad \text{instrs}_2 := p_2(\text{alloc}, \text{bg} + c_1 + 11),\ c_2 := |\text{instrs}_2|$ in [

bg	`plus`	$\lfloor \text{sp} \rfloor$	$\lfloor \text{sp} \rfloor$	$\underline{1}$
	`move`	$\langle \text{sp} - 1 \rangle_{\text{s}}$	$\lfloor \text{wk}_0 \rfloor$	
	`move`	$\lfloor \text{wk}_0 \rfloor$	$\underline{\text{bg} + c_1 + 3}$	
	instrs_1			
$\text{bg} + c_1 + 3$	`move`	$\lfloor \text{wk}_3 \rfloor$	$\lfloor \text{wk}_5 \rfloor$	
	`move`	$\lfloor \text{wk}_4 \rfloor$	$\underline{\text{bg} + c_1 + 7}$	
	`move`	$\lfloor \text{wk}_5 \rfloor$	$\underline{2}$	
	`jmp`	$\underline{\text{alloc}}$		
$\text{bg} + c_1 + 7$	`move`	$\langle \text{wk}_5 + 0 \rangle_{\text{h}}$	$\lfloor \text{wk}_3 \rfloor$	
	`move`	$\langle \text{wk}_5 + 1 \rangle_{\text{h}}$	$\lfloor \text{sv}_0 \rfloor$	
	`move`	$\lfloor \text{sv}_0 \rfloor$	$\lfloor \text{wk}_5 \rfloor$	
	`move`	$\lfloor \text{wk}_0 \rfloor$	$\underline{\text{bg} + c_1 + c_2 + 11}$	
	instrs_2			
$\text{bg} + c_1 + c_2 + 11$	`move`	$\lfloor \text{sv}_0 \rfloor$	$\langle \text{sv}_0 + 1 \rangle_{\text{h}}$	
	`minus`	$\lfloor \text{sp} \rfloor$	$\lfloor \text{sp} \rfloor$	$\underline{1}$
	`jmp`	$\langle \text{sp} - 0 \rangle_{\text{s}}$		

]

Lemma 15 (Compatibility: Unpack)**.**

$$\begin{aligned} &\Delta; \Gamma \vdash p_1 \approx e_1 : \exists \alpha.\, \tau_1 \wedge \Delta, \alpha; \Gamma, x : \tau_1 \vdash p_2 \approx e_2 : \tau_2 \\ \Longrightarrow\ &\Delta; \Gamma \vdash \text{Punpack}(p_1, p_2) \approx \mathsf{unpack}\ e_1\ \mathsf{as}\ \langle \alpha, x \rangle\ \mathsf{in}\ e_2 : \tau_2 \end{aligned}$$

Proof.

- For any $\mathcal{A}, \text{gcbg}, \text{bg}, k$, suppose
  - $W \sqsupseteq W_k^\circ(\mathcal{A}, \text{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$
  - $\text{code} := [\text{bg} \Mapsto \text{Punpack}(p_1, p_2)(\mathcal{A}(\text{gcbg}).\text{alloc}, \text{bg})]$
  - $\text{code}^{p_1} := [\text{bg} + 4 \Mapsto p_1(\mathcal{A}(\text{gcbg}).\text{alloc}, \text{bg} + 3)],\ c_1 := |\text{code}^{p_1}|$

- $\mathrm{code}^{p_2} := [\mathrm{bg} + c_1 + 6 \Mapsto p_2(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg} + c_1 + 11)]$, $c_2 := |\mathrm{code}^{p_2}|$
- $\mathrm{code}^\bullet := \mathrm{code} \setminus \mathrm{code}^{p_1} \setminus \mathrm{code}^{p_2}$
- $\mathbf{M}' = \mathbf{M} \uplus \{\mathrm{code}\}_{\mathrm{code}}$.

- Goal: find W^{pe} such that
  - $W^{pe} \sqsupseteq W \wedge \mathrm{lev}(W^{pe}) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta; \Gamma \vdash \mathrm{bg} \approx_{W^{pe}} \mathsf{unpack}\ e_1\ \mathsf{as}\ \langle \alpha, x \rangle\ \mathsf{in}\ e_2 : \tau_2$

- Let $\mathbf{M}^1 := \mathbf{M} \uplus \{\mathrm{code}^\bullet\}_{\mathrm{code}}$.
  Let $W^1 := W +\!\!+ \iota^{\mathrm{code}}(\mathrm{code}^\bullet)$.
  By definition, we have $(\mathbf{M}^1, M) \in \mathcal{M}(W^1)$.

- Let $\mathbf{M}^2 := \mathbf{M}^1 \uplus \{\mathrm{code}^{p_1}\}_{\mathrm{code}}$.
  From $\Delta; \Gamma \vdash p_1 \approx e_1 : \exists \alpha.\, \tau_1$, we have W^2 such that
  - $W^2 \sqsupseteq W^1 \wedge \mathrm{lev}(W^2) = \mathrm{lev}(W^1)$
  - $(\mathbf{M}^2, M) \in \mathcal{M}(W^2)$
  - $(*)$ $\Delta; \Gamma \vdash \mathrm{bg} + 3 \approx_{W^2} e_1 : \exists \alpha.\, \tau_1$

- Let $\mathbf{M}^3 := \mathbf{M}^2 \uplus \{\mathrm{code}^{p_2}\}_{\mathrm{code}}$.
  From $\Delta, \alpha; \Gamma, x : \tau_1 \vdash p_2 \approx e_2 : \tau_2$, we have W^3 such that
  - $W^3 \sqsupseteq W^2 \wedge \mathrm{lev}(W^3) = \mathrm{lev}(W^2)$
  - $(\mathbf{M}^3, M) \in \mathcal{M}(W^3)$
  - $(**)$ $\Delta, \alpha; \Gamma, x : \tau_1 \vdash \mathrm{bg} + c_1 + 11 \approx_{W^3} e_2 : \tau_2$

- We now choose W^{pe} to be W^3 and show the required properties.

- $W^3 \sqsupseteq W \wedge \mathrm{lev}(W^3) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^3)$ holds vacuously.

- To show: $\forall W^4 \sqsupseteq W^3.\ \forall \rho \in \mathcal{D}[\![\Delta]\!].\ \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho(W^4).$
  $((\underline{\mathrm{bg}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v} \,\}), \gamma\rho(\mathsf{unpack}\ e_1\ \mathsf{as}\ \langle \alpha, x \rangle\ \mathsf{in}\ e_2)) \in \mathcal{E}[\![\tau_2]\!]\rho(W^4)$

- By definition of $\mathcal{E}[\![\tau_2]\!]\rho(W^4)$ and plugc, we suppose
  - $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau_2]\!]\rho(W^4)$,
  - $(\mathbf{M}^4, M^4) \in \mathcal{M}(W^4)$,
  - $\mathbf{M}^4$ repr Φ^4,
  - $\mathbf{M}^4.\mathrm{reg}(\mathrm{wk}_0) = \underline{\mathrm{kpc}}$,
  - $\mathbf{M}^4.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v}$.

- To show: $((\Phi^4, \mathrm{bg}), (M^4.h, K[\gamma\rho(\mathsf{unpack}\ e_1\ \mathsf{as}\ \langle \alpha, x \rangle\ \mathsf{in}\ e_2)])) \in \mathcal{O}(W^4)$

- As W^4 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the three instructions from bg on the low side and get the configurations

$$(\Phi^5, \mathrm{bg} + 3), \quad (M^4.h, K[\mathsf{unpack}\ (\gamma\rho e_1)\ \mathsf{as}\ \langle \alpha, x \rangle\ \mathsf{in}\ (\gamma\rho e_2)])$$

  such that
  - $\mathbf{M}^5 := \mathbf{M}^4[+\!\!+ \underline{\mathrm{kpc}}]_{\mathrm{stk}}[\mathrm{wk}_0 \mapsto \underline{\mathrm{bg} + c_1 + 3}]_{\mathrm{reg}}$,
  - $\mathbf{M}^5$ repr Φ^5.

- Let $W^5 := W^4[+\!\!+ \underline{\text{kpc}}]_1$.
  Then $(\mathbf{M}^5, M^4) \in \mathcal{M}(W^5)$.
  By Theorem 9, it suffices to show that

$$((\Phi^5, \text{bg} + 3), (M^4.h, K[\mathsf{unpack}\ (\gamma\rho e_1)\ \mathsf{as}\ \langle\alpha, x\rangle\ \mathsf{in}\ (\gamma\rho e_2)])) \in \mathcal{O}(W^5)$$

- By $(*)$, it suffices to show that

$$((\text{bg} + c_1 + 3, \lfloor \text{wk}_5 \rfloor), K[\mathsf{unpack}\ (-)\ \mathsf{as}\ \langle\alpha, x\rangle\ \mathsf{in}\ (\gamma\rho e_2)]) \in \mathcal{K}[\![\exists\alpha.\, \tau_1]\!]\rho(W^5)$$

- Suppose
  $W^6 \sqsupseteq_{\text{pub}} W^5$,
  $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\exists\alpha.\, \tau_1]\!]\rho(W^6)$,
  $(\mathbf{M}^6, M^6) \in \mathcal{M}(W^6)$,
  $\mathbf{M}^6.\text{reg}(\text{wk}_5) = \mathbf{v}_1$,
  $\mathbf{M}^6$ repr Φ^6.

- To show: $((\Phi^6, \text{bg} + c_1 + 3), (M^6.h, K[\mathsf{unpack}\ v_2\ \mathsf{as}\ \langle\alpha, x\rangle\ \mathsf{in}\ (\gamma\rho e_2)])) \in \mathcal{O}(W^6)$

- As W^6 includes $\iota^{\text{code}}(\text{code}^\bullet)$, we execute the four instructions from $\text{bg} + c_1 + 3$ on the low side and get the following configurations

$$(\Phi^7, \text{alloc}) \quad (M^6.h, K[\mathsf{unpack}\ v_2\ \mathsf{as}\ \langle\alpha, x\rangle\ \mathsf{in}\ (\gamma\rho e_2)])$$

  such that
  - $\mathbf{M}^7 := \mathbf{M}^6[\text{wk}_3 \mapsto \mathbf{v}_1]_{\text{reg}}[\text{wk}_4 \mapsto \underline{\text{bg} + c_1 + 7}]_{\text{reg}}[\text{wk}_5 \mapsto \underline{2}]_{\text{reg}}$,
  - $\mathbf{M}^7$ repr Φ^7.

- By the specifications of $\mathcal{A}$, after some finite number of steps of execution, we have configurations

$$(\Phi^8, \text{bg} + c_1 + 7), \quad (M^6.h, K[\mathsf{unpack}\ v_2\ \mathsf{as}\ \langle\alpha, x\rangle\ \mathsf{in}\ (\gamma\rho e_2)])$$

  such that
  - $\mathbf{M}^8 := \mathbf{M}^7[[T, S]][\text{wk}_4 \mapsto \underline{w}]_{\text{reg}}[\text{wk}_5 \mapsto \widehat{\boldsymbol{l}_2}\,]_{\text{reg}} \uplus \{[\boldsymbol{l}_2 \mapsto (\underline{w_0, w_1})]\}_{\text{heap}}$ for some $w, \boldsymbol{l}_2, w_0, w_1$,
  - $\mathbf{M}^8 \in \mathcal{A}.GR(\text{gcbg}) \wedge \mathbf{M}^8 \in \mathcal{A}.MR(\text{gcbg})$,
  - $\mathbf{M}^8$ repr Φ^8.

- As $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\exists\alpha.\, \tau_1]\!]\rho(W^6)$, we have
  - $(\tau_1', \tau_2', R) \in \text{TyValRel}$
  - $\rho' := \rho[\alpha \mapsto (\tau_1', \tau_2', R)]$
  - $(\mathbf{u}_1, u_2) \in \mathcal{V}[\![\tau_1]\!]\rho'(W^6)$
  - $\mathbf{v}_1 = \mathbf{u}_1$
  - $v_2 = \mathsf{pack}\ \langle\tau_2', u_2\rangle\ \mathsf{as}\ \exists\alpha.\, \rho.2(\tau_1)$

- We execute the four instructions from $\text{bg} + c_1 + 7$ on the low side, take one step on the high side and get the following configurations

$$(\Phi^9, \text{bg} + c_1 + 11) \quad (M^9.h, K[(\gamma\rho e_2)[\tau_2'/\alpha][u_2/x]])$$

such that
- $\mathbf{M}^9 := \mathbf{M}^8[\boldsymbol{l}_2 : 0 \mapsto \mathbf{v}_1]_{\mathrm{hp}}[\boldsymbol{l}_2 : 1 \mapsto \mathbf{v}]_{\mathrm{hp}}[\mathrm{sv}_0 \mapsto \widehat{\boldsymbol{l}_2}]_{\mathrm{reg}}[\mathrm{wk}_0 \mapsto \underline{\mathrm{bg} + c_1 + c_2 + 11}]_{\mathrm{reg}}$,
- $\mathbf{M}^9$ repr Φ^9,
- $M^9 := M^6$

- Let $W^9 := W^6[\mathrm{sv}_0 \mapsto \widehat{\boldsymbol{l}_2}]_1 +\!\!+ \iota_{\boldsymbol{l}_2}$.
  Let $\iota_{\boldsymbol{l}_2} := \iota^{\mathrm{single}}(MR_{\boldsymbol{l}_2}, \emptyset)$.
  Let $MR_{\boldsymbol{l}_2} := \{\, (W, \mathbf{M}, M) \mid \mathbf{M}.\mathrm{hp}(\boldsymbol{l}_2)(0) = \mathbf{v}_1 \wedge \mathbf{M}.\mathrm{hp}(\boldsymbol{l}_2)(1) = \mathbf{v} \,\}$.
  Then $(\Phi^9, M^6) \in \mathcal{M}(W^9)$.

- Let $\gamma' := (\gamma, x \mapsto u_2)$.
  As W^9 include $\iota_{\boldsymbol{l}_2}$, we have
  - $\rho' \in \mathcal{D}[\![\Delta, \alpha]\!]$
  - $(W^9, \widehat{\boldsymbol{l}_2}, \gamma') \in \mathcal{G}[\![\Gamma, x : \tau_1]\!]\rho'$.

- As $(\gamma\rho e_2)[\tau_2'/\alpha][u_2/x] = \gamma'\rho' e_2$, by Theorem 9, it suffices to show that
$$((\Phi^9, \mathrm{bg} + c_1 + 11), (M^9.h, K[\gamma'\rho' e_2])) \in \mathcal{O}(W^9)$$

- Thus, by $(**)$, it suffices to show that
$$((\mathrm{bg} + c_1 + c_2 + 11, \lfloor \mathrm{wk}_5 \rfloor), K[-]) \in \mathcal{K}[\![\tau_2]\!]\rho'(W^9)$$

- Suppose
  $W^{10} \sqsupseteq_{\mathrm{pub}} W^9$,
  $(\mathbf{v}_1', v_2') \in \mathcal{V}[\![\tau_2]\!]\rho'(W^{10})$,
  $(\mathbf{M}^{10}, M^{10}) \in \mathcal{M}(W^{10})$,
  $\mathbf{M}^{10}.\mathrm{reg}(\mathrm{wk}_5) = \mathbf{v}_1'$,
  $\mathbf{M}^{11}$ repr Φ^{10}.

- To show: $((\Phi^{10}, \mathrm{bg} + c_1 + c_2 + 11), (M^{10}.h, K[v_2'])) \in \mathcal{O}(W^{10})$

- As W^{10} includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the three instructions from $\mathrm{bg} + c_1 + c_2 + 11$ on the low side and get the configurations
$$(\Phi^{11}, \mathrm{kpc}), \quad (M^{10}.h, K[v_2'])$$
  such that
  - $\mathbf{M}^{11} := \mathbf{M}^{10}[\mathrm{sv}_0 \mapsto \mathbf{v}]_{\mathrm{reg}}[-1]_{\mathrm{stk}}$,
  - $\mathbf{M}^{11}$ repr Φ^{11}.

- Let $W^{11} := W^{10}[\mathrm{sv}_0 \mapsto \mathbf{v}]_1[-1]_1$.
  Then, $(\mathbf{M}^{11}, M^{10}) \in \mathcal{M}(W^{11})$.

- By Theorem 9, it suffices to show that $((\Phi^{11}, \mathrm{kpc}), (M^{10}.h, K[v_2'])) \in \mathcal{O}(W^{11})$.

- As $W^{11} \sqsupseteq_{\mathrm{pub}} W^4$ and $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau_2]\!]\rho'(W^4)$, it suffices to show that
$$(\mathbf{v}_1', v_2') \in \mathcal{V}[\![\tau_2]\!]\rho'(W^{11})$$
  which follows from $(\mathbf{v}_1', v_2') \in \mathcal{V}[\![\tau_2]\!]\rho'(W^{10})$ by monotonicity of $\mathcal{V}[\![\tau_2]\!]\rho'$.

□

9.12 Roll

$$(\!|\Gamma \vdash \mathsf{roll}_\tau\ e|\!) ::= \mathrm{Proll}((\!|\Gamma \vdash e|\!))$$
$$\mathrm{Proll}(p) ::= p$$

Lemma 16 (Compatibility: Roll)**.**

$$\Delta; \Gamma \vdash p \approx e : \tau[\mu\alpha.\,\tau/\alpha] \implies \Delta; \Gamma \vdash \mathrm{Proll}(p) \approx \mathsf{roll}_{\mu\alpha.\,\tau}\ e : \mu\alpha.\,\tau$$

Proof.

- For any $\mathcal{A}, \mathrm{gcbg}, \mathrm{bg}, k$, suppose
  - $W \sqsupseteq W_k^\circ(\mathcal{A}, \mathrm{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$
  - $\mathrm{code} := [\mathrm{bg} \Mapsto p(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg})]$
  - $\mathbf{M}' = \mathbf{M} \uplus \{\mathrm{code}\}_{\mathrm{code}}$.
- Goal: find W^{pe} such that
  - $W^{pe} \sqsupseteq W \wedge \mathrm{lev}(W^{pe}) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta; \Gamma \vdash \mathrm{bg} \approx_{W^{pe}} \mathsf{roll}_{\mu\alpha.\,\tau}\ e : \mu\alpha.\,\tau$
- From $\Delta; \Gamma \vdash p \approx e : \tau[\mu\alpha.\,\tau/\alpha]$, we have W^1 such that
  - $W^1 \sqsupseteq W \wedge \mathrm{lev}(W^1) = \mathrm{lev}(W)$
  - $(\mathbf{M}', M) \in \mathcal{M}(W^1)$
  - $(*)$ $\Delta; \Gamma \vdash \mathrm{bg} \approx_{W^1} e : \tau[\mu\alpha.\,\tau/\alpha]$
- We now choose W^{pe} to be W^1 and show the required properties.
- $W^1 \sqsupseteq W \wedge \mathrm{lev}(W^1) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^1)$ holds vacuously.
- To show: $\forall W^2 \sqsupseteq W^1.\ \forall \rho \in \mathcal{D}[\![\Delta]\!].\ \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho(W^2).$
  $((\underline{\mathrm{bg}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v} \,\}), \gamma\rho(\mathsf{roll}_{\mu\alpha.\,\tau}\ e)) \in \mathcal{E}[\![\mu\alpha.\,\tau]\!]\rho(W^2)$
- By definition of $\mathcal{E}[\![\mu\alpha.\,\tau]\!]\rho(W^2)$ and plugc, we suppose
  - $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\mu\alpha.\,\tau]\!]\rho(W^2)$,
  - $(\mathbf{M}^2, M^2) \in \mathcal{M}(W^2)$,
  - $\mathbf{M}^2$ repr Φ^2,
  - $\mathbf{M}^2.\mathrm{reg}(\mathrm{wk}_0) = \underline{\mathrm{kpc}}$,
  - $\mathbf{M}^2.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v}$.
- To show: $((\Phi^2, \mathrm{bg}), (M^2.h, K[\mathsf{roll}_{\mu\alpha.\,\rho.2(\tau)}\ \gamma\rho e])) \in \mathcal{O}(W^2)$
- By $(*)$, it suffices to show that $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K[\mathsf{roll}_{\mu\alpha.\,\rho.2(\tau)}\ -]) \in \mathcal{K}[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\rho(W^2)$.
- Suppose
  $W^3 \sqsupseteq_{\mathrm{pub}} W^2$,
  $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\rho(W^3)$,
  $(\mathbf{M}^3, M^3) \in \mathcal{M}(W^3)$,
  $\mathbf{M}^3.\mathrm{reg}(\mathrm{wk}_5) = \mathbf{v}_1$,
  $\mathbf{M}^3$ repr Φ^3.
- To show: $((\Phi^3, \mathrm{kpc}), (M^3.h, K[\mathsf{roll}_{\mu\alpha.\,\rho.2(\tau)}\ v_2])) \in \mathcal{O}(W^3)$

- As $W^3 \sqsupseteq_{\text{pub}} W^2$ and $((\text{kpc}, \lfloor \text{wk}_5 \rfloor), K) \in \mathcal{K}[\![\mu\alpha.\,\tau]\!]\rho(W^2)$, it suffices to show that

$$(\mathbf{v}_1, \mathsf{roll}_{\mu\alpha.\,\rho.2(\tau)}\ v_2) \in \mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho(W^3)$$

- By Theorem 3, we have

$$\begin{array}{ll} & \mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho \\ = & F_{\alpha,\tau,\rho}(\mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho) \\ = & \{\, (W, \mathbf{v}_1, v_2) \in \text{oftype}(\mu\alpha.\,\tau, \rho) \mid \\ & \quad \exists (\mathbf{u}_1, u_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto (\rho.1(\mu\alpha.\,\tau), \rho.2(\mu\alpha.\,\tau), \mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho)](W). \\ & \quad (W, \mathbf{v}_1, v_2) \in \Box(\mathcal{L}_1.\text{roll}(\mathbf{u}_1), \mathcal{L}_2.\text{roll}(u_2))\,\} \ . \end{array}$$

- Thus, it suffices to show that $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto (\rho.1(\mu\alpha.\,\tau), \rho.2(\mu\alpha.\,\tau), \mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho)](W^3)$, which follows from $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\rho(W^3)$ by Theorem 7.

□

9.13 Unroll

$$(\!|\Gamma \vdash \mathsf{unroll}\ e|\!) ::= \text{Punroll}((\!|\Gamma \vdash e|\!))$$

$$\text{Punroll}(p) ::= p$$

Lemma 17 (Compatibility: Unroll)**.**

$$\Delta; \Gamma \vdash p \approx e : \mu\alpha.\,\tau \implies \Delta; \Gamma \vdash \text{Punroll}(p) \approx \mathsf{unroll}\ e : \tau[\mu\alpha.\,\tau/\alpha]$$

Proof.

- For any $\mathcal{A}, \text{gcbg}, \text{bg}, k$, suppose
  - $W \sqsupseteq W_k^\circ(\mathcal{A}, \text{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$
  - $\text{code} := [\text{bg} \Mapsto p(\mathcal{A}(\text{gcbg}).\text{alloc}, \text{bg})]$
  - $\mathbf{M}' = \mathbf{M} \uplus \{\text{code}\}_{\text{code}}$.
- Goal: find W^{pe} such that
  - $W^{pe} \sqsupseteq W \wedge \text{lev}(W^{pe}) = \text{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta; \Gamma \vdash \text{bg} \approx_{W^{pe}} \mathsf{unroll}\ e : \tau[\mu\alpha.\,\tau/\alpha]$
- From $\Delta; \Gamma \vdash p \approx e : \mu\alpha.\,\tau$, we have W^1 such that
  - $W^1 \sqsupseteq W \wedge \text{lev}(W^1) = \text{lev}(W)$
  - $(\mathbf{M}', M) \in \mathcal{M}(W^1)$
  - $(*)$ $\Delta; \Gamma \vdash \text{bg} \approx_{W^1} e : \mu\alpha.\,\tau$
- We now choose W^{pe} to be W^1 and show the required properties.
- $W^1 \sqsupseteq W \wedge \text{lev}(W^1) = \text{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^1)$ holds vacuously.
- To show: $\forall W^2 \sqsupseteq W^1.\ \forall \rho \in \mathcal{D}[\![\Delta]\!]\,.\ \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho(W^2).$
  $((\underline{\text{bg}}, \lfloor \text{wk}_0 \rfloor, \lfloor \text{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\text{reg}(\text{sv}_0) = \mathbf{v}\,\}), \gamma\rho(\mathsf{unroll}\ e)) \in \mathcal{E}[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\rho(W^2)$

- By definition of $\mathcal{E}[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\rho(W^2)$ and plugc, we suppose
  - $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\rho(W^2)$,
  - $(\mathbf{M}^2, M^2) \in \mathcal{M}(W^2)$,
  - $\mathbf{M}^2$ repr Φ^2,
  - $\mathbf{M}^2.\mathrm{reg}(\mathrm{wk}_0) = \underline{\mathrm{kpc}}$,
  - $\mathbf{M}^2.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v}$.
- To show: $((\Phi^2, \mathrm{bg}), (M^2.h, K[\mathsf{unroll}\ \gamma\rho e])) \in \mathcal{O}(W^2)$
- By $(*)$, it suffices to show that $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K[\mathsf{unroll}\ -]) \in \mathcal{K}[\![\mu\alpha.\,\tau]\!]\rho(W^2)$.
- Suppose
  $W^3 \sqsupseteq_{\mathrm{pub}} W^2$,
  $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho(W^3)$,
  $(\mathbf{M}^3, M^3) \in \mathcal{M}(W^3)$,
  $\mathbf{M}^3.\mathrm{reg}(\mathrm{wk}_5) = \mathbf{v}_1$,
  $\mathbf{M}^3$ repr Φ^3.
- To show: $((\Phi^3, \mathrm{kpc}), (M^3.h, K[\mathsf{unroll}\ v_2])) \in \mathcal{O}(W^3)$
- By Theorem 3, we have

$$\begin{aligned}(W^3, \mathbf{v}_1, v_2) \in \{\, (W, \mathbf{v}_1, v_2) \in \mathrm{oftype}(\mu\alpha.\,\tau, \rho) \mid \\ \exists (\mathbf{u}_1, u_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto (\rho.1(\mu\alpha.\,\tau), \rho.2(\mu\alpha.\,\tau), \mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho)](W). \\ (W, \mathbf{v}_1, v_2) \in \Box(\mathcal{L}_1.\mathrm{roll}(\mathbf{u}_1), \mathcal{L}_2.\mathrm{roll}(u_2))\,\}\ .\end{aligned}$$

- Thus we have
  - $v_2 = \mathsf{roll}_{\mu\alpha.\,\tau}\ u_2$ for some u_2
  - $(\mathbf{v}_1, u_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto (\rho.1(\mu\alpha.\,\tau), \rho.2(\mu\alpha.\,\tau), \mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho)](W^3)$
- As $v_2 = \mathsf{roll}_{\mu\alpha.\,\tau}\ u_2$, we take one step on the high side and get the following configurations:

$$(\Phi^3, \mathrm{kpc}) \quad (M^3.h, K[u_2]))$$

- As $W^3 \sqsupseteq_{\mathrm{pub}} W^2$ and $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\rho(W^2)$, it suffices to show that

$$(\mathbf{v}_1, u_2) \in \mathcal{V}[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\rho(W^3)$$

  which follows from $(\mathbf{v}_1, u_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto (\rho.1(\mu\alpha.\,\tau), \rho.2(\mu\alpha.\,\tau), \mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho)](W^3)$ by Theorem 7.

□

9.14 New

$$(\!|\Gamma \vdash \mathsf{ref}\ e|\!) ::= \mathrm{Pnew}((\!|\Gamma \vdash e|\!))$$

$\mathrm{Pnew}(p) ::= \lambda\, \mathrm{alloc}, \mathrm{bg}.$
let code $:= p(\mathrm{alloc}, \mathrm{bg}+3),\ c := |\mathrm{code}|$ in [

bg	`plus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{1}$
	`move`	$\langle \mathrm{sp}-1 \rangle_{\mathrm{s}}$	$\lfloor \mathrm{wk}_0 \rfloor$	
	`move`	$\lfloor \mathrm{wk}_0 \rfloor$	$\underline{\mathrm{bg}+c+3}$	
	code			
$\mathrm{bg}+c+3$	`move`	$\lfloor \mathrm{wk}_3 \rfloor$	$\lfloor \mathrm{wk}_5 \rfloor$	
	`move`	$\lfloor \mathrm{wk}_4 \rfloor$	$\underline{\mathrm{bg}+c+7}$	
	`move`	$\lfloor \mathrm{wk}_5 \rfloor$	$\underline{1}$	
	`jmp`	$\underline{\mathrm{alloc}}$		
$\mathrm{bg}+c+7$	`move`	$\langle \mathrm{wk}_5 + 0 \rangle_{\mathrm{h}}$	$\lfloor \mathrm{wk}_3 \rfloor$	
	`minus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{1}$
	`jmp`	$\langle \mathrm{sp}-0 \rangle_{\mathrm{s}}$		

]

Lemma 18 (Compatibility: New)**.**

$$\Delta; \Gamma \vdash p \approx e : \tau \implies \Delta; \Gamma \vdash \mathrm{Pnew}(p) \approx \mathsf{ref}\ e : \mathsf{ref}\ \tau$$

Proof.

- For any $\mathcal{A}, \mathrm{gcbg}, \mathrm{bg}, k$, suppose
  - $W \sqsupseteq W_k^\circ(\mathcal{A}, \mathrm{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$
  - $\mathrm{code} := [\mathrm{bg} \Mapsto \mathrm{Pnew}(p)(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg})]$
  - $\mathrm{code}^p := [\mathrm{bg}+3 \Mapsto p(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg}+3)],\ c := |\mathrm{code}^p|$
  - $\mathrm{code}^\bullet := \mathrm{code} \setminus \mathrm{code}^p$
  - $\mathbf{M}' = \mathbf{M} \uplus \{\mathrm{code}\}_{\mathrm{code}}$.
- Goal: find W^{pe} such that
  - $W^{pe} \sqsupseteq W \wedge \mathrm{lev}(W^{pe}) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta; \Gamma \vdash \mathrm{bg} \approx_{W^{pe}} \mathsf{ref}\ e : \mathsf{ref}\ \tau$
- Let $\mathbf{M}^1 := \mathbf{M} \uplus \{\mathrm{code}^\bullet\}_{\mathrm{code}}$.
  Let $W^1 := W +\!\!+ \iota^{\mathrm{code}}(\mathrm{code}^\bullet)$.
  By definition, we have $(\mathbf{M}^1, M) \in \mathcal{M}(W^1)$.
- Let $\mathbf{M}^2 := \mathbf{M}^1 \uplus \{\mathrm{code}^p\}_{\mathrm{code}}$.
  From $\Delta; \Gamma \vdash p \approx e : \tau$, we have W^2 such that
  - $W^2 \sqsupseteq W^1 \wedge \mathrm{lev}(W^2) = \mathrm{lev}(W^1)$
  - $(\mathbf{M}^2, M) \in \mathcal{M}(W^2)$
  - $(*)\ \Delta; \Gamma \vdash \mathrm{bg}+3 \approx_{W^2} e : \tau$
- We now choose W^{pe} to be W^2 and show the required properties.
- $W^2 \sqsupseteq W \wedge \mathrm{lev}(W^2) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^2)$ holds vacuously.

- To show: $\forall W^3 \sqsupseteq W^2.\ \forall \rho \in \mathcal{D}[\![\Delta]\!].\ \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho(W^3).$
  $((\underline{\mathrm{bg}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v} \,\}), \gamma\rho(\mathsf{ref}\ e)) \in \mathcal{E}[\![\mathsf{ref}\ \tau]\!]\rho(W^3)$

- By definition of $\mathcal{E}[\![\mathsf{ref}\ \tau]\!]\rho(W^3)$ and plugc, we suppose
  - $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\mathsf{ref}\ \tau]\!]\rho(W^3)$,
  - $(\mathbf{M}^3, M^3) \in \mathcal{M}(W^3)$,
  - $\mathbf{M}^3$ repr Φ^3,
  - $\mathbf{M}^3.\mathrm{reg}(\mathrm{wk}_0) = \underline{\mathrm{kpc}}$,
  - $\mathbf{M}^3.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v}$.

- To show: $((\Phi^3, \mathrm{bg}), (M^3.h, K[\gamma\rho(\mathsf{ref}\ e)])) \in \mathcal{O}(W^3)$

- As W^3 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the three instructions from bg on the low side and get the configurations
  $$(\Phi^4, \mathrm{bg} + 3), \quad (M^3.h, K[\mathsf{ref}\ \gamma\rho e])$$
  such that
  - $\mathbf{M}^4 := \mathbf{M}^3[{+\!+}\, \underline{\mathrm{kpc}}]_{\mathrm{stk}}[\mathrm{wk}_0 \mapsto \underline{\mathrm{bg} + c + 3}]_{\mathrm{reg}}$,
  - $\mathbf{M}^4$ repr Φ^4.

- Let $W^4 := W^3[{+\!+}\, \underline{\mathrm{kpc}}]_1$.
  Then $(\mathbf{M}^4, M^3) \in \mathcal{M}(W^4)$.
  By Theorem 9, it suffices to show that $((\Phi^4, \mathrm{bg} + 3), (M^3.h, K[\mathsf{ref}\ \gamma\rho e])) \in \mathcal{O}(W^4)$.

- By $(*)$, it suffices to show that $((\mathrm{bg} + c + 3, \lfloor \mathrm{wk}_5 \rfloor), K[\mathsf{ref}\ -]) \in \mathcal{K}[\![\tau]\!]\rho(W^4)$.

- Suppose
  $W^5 \sqsupseteq_{\mathrm{pub}} W^4$,
  $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho(W^5)$,
  $(\mathbf{M}^5, M^5) \in \mathcal{M}(W^5)$,
  $\mathbf{M}^5.\mathrm{reg}(\mathrm{wk}_5) = \mathbf{v}_1$,
  $\mathbf{M}^5$ repr Φ^5.

- To show: $((\Phi^5, \mathrm{bg} + c + 3), (M^5.h, K[\mathsf{ref}\ v_2])) \in \mathcal{O}(W^5)$

- As W^5 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the four instructions from $\mathrm{bg} + c + 3$ on the low side and get the configurations
  $$(\Phi^6, \mathrm{alloc}), \quad (M^5.h, K[\mathsf{ref}\ v_2])$$
  such that
  - $\mathbf{M}^6 := \mathbf{M}^5[\mathrm{wk}_3 \mapsto \mathbf{v}_1]_{\mathrm{reg}}[\mathrm{wk}_4 \mapsto \underline{\mathrm{bg} + c + 7}]_{\mathrm{reg}}[\mathrm{wk}_5 \mapsto \underline{1}]_{\mathrm{reg}}$,
  - $\mathbf{M}^6$ repr Φ^6.

- By the specifications of $\mathcal{A}$, after some finite number of steps of execution, we have configurations
  $$(\Phi^7, \mathrm{bg} + c + 7), \quad (M^5.h, K[\mathsf{ref}\ v_2])$$
  such that
  - $\mathbf{M}^7 := \mathbf{M}^6[[T, S]][\mathrm{wk}_4 \mapsto \underline{w}]_{\mathrm{reg}}[\mathrm{wk}_5 \mapsto \widehat{\boldsymbol{l}_1}\,]_{\mathrm{reg}} \uplus \{[\boldsymbol{l}_1 \mapsto (\underline{w_0})]\}_{\mathrm{heap}}$ for some $w, \boldsymbol{l}_1, w_0$,
  - $\mathbf{M}^7 \in \mathcal{A}.GR(\mathrm{gcbg}) \wedge \mathbf{M}^7 \in \mathcal{A}.MR(\mathrm{gcbg})$,
  - $\mathbf{M}^7$ repr Φ^7.

- As $\mathbf{M}^7.\mathrm{code} = \mathbf{M}^6.\mathrm{code}$, we execute the three instructions from $\mathrm{bg} + c + 7$ on the low side, take one step on the high side and get

$$(\Phi^8, \mathrm{kpc}), \quad (M^8.h, K[\ell_2])$$

such that
- $\mathbf{M}^8 := \mathbf{M}^7[\boldsymbol{l}_1 : 0 \mapsto \mathbf{v}_1]_{\mathrm{hp}}[-1]_{\mathrm{stk}}$
- $\mathbf{M}^8$ repr Φ^8
- $M^8 := (M^5.h \uplus [\ell_2 \mapsto v_2], \{M^5.\Sigma, \ell_2 : \tau\})$

- Let $W^8 := W^5[-1]_1 +\!\!+ \iota_{\boldsymbol{l}_1,\ell_2}$.
  Let $MR_{\boldsymbol{l}_1,\ell_2} := \{\, (W, \mathbf{M}, M) \mid (W, \mathbf{M}.\mathrm{hp}(\boldsymbol{l}_1)(0), M.h(\ell_2)) \in \mathcal{V}[\![\tau]\!]\rho \,\}$
  Let $Bij_{\boldsymbol{l}_1,\ell_2} := \{\, (\widehat{\boldsymbol{l}_1}, \ell_2) \,\}$
  Let $\iota_{\boldsymbol{l}_1,\ell_2} := \iota^{\mathrm{single}}(MR_{\boldsymbol{l}_1,\ell_2}, Bij_{\boldsymbol{l}_1,\ell_2})$.
  It is easy to check that $\iota_{\boldsymbol{l}_1,\ell_2}$ forms an island.
  Then $(\mathbf{M}^8, M^8) \in \mathcal{M}(W^8)$ because $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho(W^5)$ and thus $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho(\triangleright W^8)$.

- By Theorem 9, it suffices to show that $((\Phi^8, \mathrm{kpc}), (M^8.h, K[\ell_2])) \in \mathcal{O}(W^8)$.

- As $W^8 \sqsupseteq_{\mathrm{pub}} W^3$ and $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\mathsf{ref}\ \tau]\!]\rho(W^3)$, it suffices to show that

$$(\widehat{\boldsymbol{l}_1}, \ell_2) \in \mathcal{V}[\![\mathsf{ref}\ \tau]\!]\rho(W^8)$$

- By definition of $\mathcal{V}[\![\mathsf{ref}\ \tau]\!]\rho(W^8)$, for all $W^9 \sqsupseteq W^8$ and $(\mathbf{M}, M) \in \mathcal{M}(W^9)$, it suffices to show that
  - $(\widehat{\boldsymbol{l}_1}, \ell_2) \in \mathcal{B}(W^9)$: trivial as W^9 includes $\iota_{\boldsymbol{l}_1,\ell_2}$.
  - $\exists (\mathbf{u}_1, u_2) \in \triangleright\mathcal{V}[\![\tau]\!]\rho(W^9).\ (\widehat{\boldsymbol{l}_1}, \mathbf{M}) \in \mathcal{L}.\mathrm{ref}(\mathbf{u}_1) \wedge (\ell_2, M) \in \mathcal{H}.\mathrm{ref}(u_2)$: trivial as W^9 includes $\iota_{\boldsymbol{l}_1,\ell_2}$.
  - $\forall (\mathbf{u}_1, u_2) \in \triangleright\mathcal{V}[\![\tau]\!]\rho(W^9).\ (\mathcal{L}.\mathrm{asgn}(\mathbf{M}, \widehat{\boldsymbol{l}_1}, \mathbf{u}_1), \mathcal{H}.\mathrm{asgn}(M, \ell_2, u_2)) \in \mathcal{M}(W^9)$: trivial as W^9 includes $\iota_{\boldsymbol{l}_1,\ell_2}$.

□

9.15 Asgn

$$(\!|\Gamma \vdash e_1 := e_2|\!) ::= \mathrm{Pasgn}((\!|\Gamma \vdash e_1|\!), (\!|\Gamma \vdash e_2|\!))$$

$\mathrm{Pasgn}(p_1, p_2) ::= \lambda\, \mathrm{alloc}, \mathrm{bg}.$
let $\mathrm{instrs}_1 := p_1(\mathrm{alloc}, \mathrm{bg}+4),\ c_1 := |\mathrm{instrs}_1|,$
$\quad \mathrm{instrs}_2 := p_2(\mathrm{alloc}, \mathrm{bg}+c_1+6),\ c_2 := |\mathrm{instrs}_2|$ in [

bg	`plus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{2}$
	`move`	$\langle \mathrm{sp}-2 \rangle_{\mathrm{s}}$	$\lfloor \mathrm{wk}_0 \rfloor$	
	`move`	$\langle \mathrm{sp}-1 \rangle_{\mathrm{s}}$	$\underline{0}$	
	`move`	$\lfloor \mathrm{wk}_0 \rfloor$	$\underline{\mathrm{bg}+c_1+4}$	
	instrs_1			
$\mathrm{bg}+c_1+4$	`move`	$\langle \mathrm{sp}-1 \rangle_{\mathrm{s}}$	$\lfloor \mathrm{wk}_5 \rfloor$	
	`move`	$\lfloor \mathrm{wk}_0 \rfloor$	$\underline{\mathrm{bg}+c_1+c_2+6}$	
	instrs_2			
$\mathrm{bg}+c_1+c_2+6$	`move`	$\lfloor \mathrm{wk}_3 \rfloor$	$\langle \mathrm{sp}-1 \rangle_{\mathrm{s}}$	
	`move`	$\langle \mathrm{wk}_3+0 \rangle_{\mathrm{h}}$	$\lfloor \mathrm{wk}_5 \rfloor$	
	`minus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{2}$
	`jmp`	$\langle \mathrm{sp}-0 \rangle_{\mathrm{s}}$		

]

Lemma 19 (Compatibility: Assign)**.**

$$\Delta;\Gamma \vdash p_1 \approx e_1 : \mathsf{ref}\ \tau \wedge \Delta;\Gamma \vdash p_2 \approx e_2 : \tau \implies \Delta;\Gamma \vdash \mathrm{Pasgn}(p_1,p_2) \approx e_1 := e_2 : \mathsf{unit}$$

Proof.

- For any $\mathcal{A}, \mathrm{gcbg}, \mathrm{bg}, k$, suppose
  - $W \sqsupseteq W_k^\circ(\mathcal{A}, \mathrm{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$
  - $\mathrm{code} := [\mathrm{bg} \Mapsto \mathrm{Pasgn}(p_1,p_2)(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg})]$
  - $\mathrm{code}^{p_1} := [\mathrm{bg}+4 \Mapsto p_1(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg}+4)],\ c_1 := |\mathrm{code}^{p_1}|$
  - $\mathrm{code}^{p_2} := [\mathrm{bg}+c_1+6 \Mapsto p_2(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg}+c_1+6)],\ c_2 := |\mathrm{code}^{p_2}|$
  - $\mathrm{code}^\bullet := \mathrm{code} \setminus \mathrm{code}^{p_1} \setminus \mathrm{code}^{p_2}$
  - $\mathbf{M}' = \mathbf{M} \uplus \{\mathrm{code}\}_{\mathrm{code}}$.
- Goal: find W^{pe} such that
  - $W^{pe} \sqsupseteq W \wedge \mathrm{lev}(W^{pe}) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta;\Gamma \vdash \mathrm{bg} \approx_{W^{pe}} e_1 := e_2 : \mathsf{unit}$
- Let $\mathbf{M}^1 := \mathbf{M} \uplus \{\mathrm{code}^\bullet\}_{\mathrm{code}}$.
  Let $W^1 := W +\!\!+ \iota^{\mathrm{code}}(\mathrm{code}^\bullet)$.
  By definition, we have $(\mathbf{M}^1, M) \in \mathcal{M}(W^1)$.
- Let $\mathbf{M}^2 := \mathbf{M}^1 \uplus \{\mathrm{code}^{p_1}\}_{\mathrm{code}}$.
  From $\Delta;\Gamma \vdash p_1 \approx e_1 : \mathsf{ref}\ \tau$, we have W^2 such that
  - $W^2 \sqsupseteq W^1 \wedge \mathrm{lev}(W^2) = \mathrm{lev}(W^1)$
  - $(\mathbf{M}^2, M) \in \mathcal{M}(W^2)$
  - $(*)\ \Delta;\Gamma \vdash \mathrm{bg}+4 \approx_{W^2} e_1 : \mathsf{ref}\ \tau$

- Let $\mathbf{M}^3 := \mathbf{M}^2 \uplus \{\mathrm{code}^{p_2}\}_{\mathrm{code}}$.
  From $\Delta; \Gamma \vdash p_2 \approx e_2 : \tau$, we have W^3 such that
  - $W^3 \sqsupseteq W^2 \wedge \mathrm{lev}(W^3) = \mathrm{lev}(W^2)$
  - $(\mathbf{M}^3, M) \in \mathcal{M}(W^3)$
  - $(**)$ $\Delta; \Gamma \vdash \mathrm{bg} + c_1 + 6 \approx_{W^3} e_2 : \tau$
- We now choose W^{pe} to be W^3 and show the required properties.
- $W^3 \sqsupseteq W \wedge \mathrm{lev}(W^3) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^3)$ holds vacuously.
- To show: $\forall W^4 \sqsupseteq W^3.\ \forall \rho \in \mathcal{D}[\![\Delta]\!].\ \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho(W^4).$
  $((\underline{\mathrm{bg}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v} \,\}), \gamma\rho(e_1 := e_2)) \in \mathcal{E}[\![\mathsf{unit}]\!]\rho(W^4)$
- By definition of $\mathcal{E}[\![\mathsf{unit}]\!]\rho(W^3)$ and plugc, we suppose
  - $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\mathsf{unit}]\!]\rho(W^4)$,
  - $(\mathbf{M}^4, M^4) \in \mathcal{M}(W^4)$,
  - $\mathbf{M}^4$ repr Φ^4,
  - $\mathbf{M}^4.\mathrm{reg}(\mathrm{wk}_0) = \underline{\mathrm{kpc}}$,
  - $\mathbf{M}^4.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v}$.
- To show: $((\Phi^4, \mathrm{bg}), (M^4.h, K[\gamma\rho(e_1 := e_2)])) \in \mathcal{O}(W^4)$
- As W^4 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the four instructions from bg on the low side and get the configurations
  $$(\Phi^5, \mathrm{bg} + 4), \quad (M^4.h, K[\gamma\rho e_1 := \gamma\rho e_2])$$
  such that
  - $\mathbf{M}^5 := \mathbf{M}^4[{+\!+}\, \underline{\mathrm{kpc}}, \underline{0}]_{\mathrm{stk}}[\mathrm{wk}_0 \mapsto \underline{\mathrm{bg} + c_1 + 4}]_{\mathrm{reg}}$,
  - $\mathbf{M}^5$ repr Φ^5.
- Let $W^5 := W^4[{+\!+}\, \underline{\mathrm{kpc}}, \underline{0}]_1$.
  Then $(\mathbf{M}^5, M^4) \in \mathcal{M}(W^5)$.
  By Theorem 9, it suffices to show that $((\Phi^5, \mathrm{bg} + 4), (M^4.h, K[\gamma\rho e_1 := \gamma\rho e_2])) \in \mathcal{O}(W^5)$.
- By $(*)$, it suffices to show that $((\mathrm{bg} + c_1 + 4, \lfloor \mathrm{wk}_5 \rfloor), K[- := \gamma\rho e_2]) \in \mathcal{K}[\![\mathsf{ref}\ \tau]\!]\rho(W^5)$.
- Suppose
  $W^6 \sqsupseteq_{\mathrm{pub}} W^5$,
  $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\mathsf{ref}\ \tau]\!]\rho(W^6)$,
  $(\mathbf{M}^6, M^6) \in \mathcal{M}(W^6)$,
  $\mathbf{M}^6.\mathrm{reg}(\mathrm{wk}_5) = \mathbf{v}_1$,
  $\mathbf{M}^6$ repr Φ^6.
- To show: $((\Phi^6, \mathrm{bg} + c_1 + 4), (M^6.h, K[v_2 := \gamma\rho e_2])) \in \mathcal{O}(W^6)$
- As W^6 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the two instructions from $\mathrm{bg} + c_1 + 4$ on the low side and get the configurations
  $$(\Phi^7, \mathrm{bg} + c_1 + 6), \quad (M^6.h, K[v_2 := \gamma\rho e_2])$$

such that
- $\mathbf{M}^7 := \mathbf{M}^6[|\mathbf{M}^7.\mathrm{stk}| - 1 \mapsto \mathbf{v}_1]_{\mathrm{stk}}[\mathrm{wk}_0 \mapsto \underline{\mathrm{bg} + c_1 + c_2 + 6}]_{\mathrm{reg}}$,
- $\mathbf{M}^7$ repr Φ^7.

- Let $W^7 := W^6[|\mathbf{M}^7.\mathrm{stk}| - 1 \mapsto \mathbf{v}_1]_1$.
  Then $(\mathbf{M}^7, M^6) \in \mathcal{M}(W^7)$.
  By Theorem 9, it suffices to show that $((\Phi^7, \mathrm{bg} + c_1 + 6), (M^6.h, K[v_2 := \gamma\rho e_2])) \in \mathcal{O}(W^7)$.

- By $(**)$, it suffices to show that $((\mathrm{bg} + c_1 + c_2 + 6, \lfloor \mathrm{wk}_5 \rfloor), K[v_2 := -]) \in \mathcal{K}[\![\tau]\!]\rho(W^7)$.

- Suppose
  $W^8 \sqsupseteq_{\mathrm{pub}} W^7$,
  $(\mathbf{v}_3, v_4) \in \mathcal{V}[\![\tau]\!]\rho(W^8)$,
  $(\mathbf{M}^8, M^8) \in \mathcal{M}(W^8)$,
  $\mathbf{M}^8.\mathrm{reg}(\mathrm{wk}_5) = \mathbf{v}_3$,
  $\mathbf{M}^8$ repr Φ^8.

- To show: $((\Phi^8, \mathrm{bg} + c_1 + c_2 + 6), (M^8.h, K[v_2 := v_4])) \in \mathcal{O}(W^8)$

- As $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\mathsf{ref}\ \tau]\!]\rho(W^6)$ and $W^8 \sqsupseteq W^6$,
  - $\mathbf{v}_1 = \widehat{\boldsymbol{l}_1}$, $\mathbf{M}^8.\mathrm{hp}(\boldsymbol{l}_1)(0) = \mathbf{u}_1$ for some $\boldsymbol{l}_1, \mathbf{u}_1$
  - $v_2 = \ell_2$, $M^8.h(\ell_2) = u_2$ for some ℓ_2, u_2
  - $(\mathbf{u}_1, u_2) \in \triangleright\mathcal{V}[\![\tau]\!]\rho(W^8)$

- As W^8 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the four instructions from $\mathrm{bg} + c_1 + c_2 + 6$ on the low side, take one step on the high side and get the configurations

$$(\Phi^9, \mathrm{kpc}), \quad (M^9.h, K[\langle\rangle])$$

  such that
  - $\mathbf{M}^9 := \mathbf{M}^8[-2]_{\mathrm{stk}}[\boldsymbol{l}_1 : 0 \mapsto \mathbf{v}_3]_{\mathrm{hp}}$
  - $\mathbf{M}^9$ repr Φ^9
  - $M^9 := (M^8.h[\ell_2 \mapsto v_4], M.\Sigma)$

- Let $W^9 := W^8[-2]_1$.
  Then, $(\mathbf{M}^8[-2]_{\mathrm{stk}}, M^8) \in \mathcal{M}(W^9)$.

- As $(\widehat{\boldsymbol{l}_1}, \ell_2) \in \mathcal{V}[\![\mathsf{ref}\ \tau]\!]\rho(W^6)$, $W^9 \sqsupseteq W^6$, $(\mathbf{v}_3, v_4) \in \triangleright\mathcal{V}[\![\tau]\!]\rho(W^9)$, $\mathbf{M}^9 = \mathcal{L}.\mathrm{asgn}(\mathbf{M}^8[-2]_{\mathrm{stk}}, \widehat{\boldsymbol{l}_1}, \mathbf{v}_3)$ and $M^9 = \mathcal{H}.\mathrm{asgn}(M^8, \ell_2, v_4)$,
  - $(\mathbf{M}^9, M^9) \in W^9$

- By Theorem 9, it suffices to show that $((\Phi^9, \mathrm{kpc}), (M^9.h, K[\langle\rangle])) \in \mathcal{O}(W^9)$.

- As $W^9 \sqsupseteq_{\mathrm{pub}} W^4$ and $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\mathsf{unit}]\!]\rho(W^4)$, it suffices to show that

$$(\mathbf{M}^9.\mathrm{reg}(\mathrm{wk}_5), \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\rho(W^9)$$

  which trivially holds by definition.

□

9.16 Deref

$$(\!|\Gamma \vdash !e|\!) ::= \mathrm{Pderef}((\!|\Gamma \vdash e|\!))$$

$\mathrm{Pderef}(p) ::= \lambda\, \mathrm{alloc}, \mathrm{bg}.$
let code $:= p(\mathrm{alloc}, \mathrm{bg}+3)$, $c := |\mathrm{code}|$ in [

bg	`plus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{1}$
	`move`	$\langle \mathrm{sp}-1 \rangle_{\mathrm{s}}$	$\lfloor \mathrm{wk}_0 \rfloor$	
	`move`	$\lfloor \mathrm{wk}_0 \rfloor$	$\underline{\mathrm{bg}+c+3}$	
	code			
$\mathrm{bg}+c+3$	`move`	$\lfloor \mathrm{wk}_5 \rfloor$	$\langle \mathrm{wk}_5 + 0 \rangle_{\mathrm{h}}$	
	`minus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{1}$
	`jmp`	$\langle \mathrm{sp}-0 \rangle_{\mathrm{s}}$		

]

Lemma 20 (Compatibility: Deref)**.**

$$\Delta; \Gamma \vdash p \approx e : \mathsf{ref}\,\tau \implies \Delta; \Gamma \vdash \mathrm{Pderef}(p) \approx !e : \tau$$

Proof.

- For any $\mathcal{A}, \mathrm{gcbg}, \mathrm{bg}, k$, suppose
  - $W \sqsupseteq W_k^\circ(\mathcal{A}, \mathrm{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$
  - $\mathrm{code} := [\mathrm{bg} \Mapsto \mathrm{Pderef}(p)(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg})]$
  - $\mathrm{code}^p := [\mathrm{bg}+3 \Mapsto p(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg}+3)]$, $c := |\mathrm{code}^p|$
  - $\mathrm{code}^\bullet := \mathrm{code} \setminus \mathrm{code}^p$
  - $\mathbf{M}' = \mathbf{M} \uplus \{\mathrm{code}\}_{\mathrm{code}}$.
- Goal: find W^{pe} such that
  - $W^{pe} \sqsupseteq W \wedge \mathrm{lev}(W^{pe}) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta; \Gamma \vdash \mathrm{bg} \approx_{W^{pe}} !e : \tau$
- Let $\mathbf{M}^1 := \mathbf{M} \uplus \{\mathrm{code}^\bullet\}_{\mathrm{code}}$.
  Let $W^1 := W +\!\!+ \iota^{\mathrm{code}}(\mathrm{code}^\bullet)$.
  By definition, we have $(\mathbf{M}^1, M) \in \mathcal{M}(W^1)$.
- Let $\mathbf{M}^2 := \mathbf{M}^1 \uplus \{\mathrm{code}^p\}_{\mathrm{code}}$.
  From $\Delta; \Gamma \vdash p \approx e : \mathsf{ref}\,\tau$, we have W^2 such that
  - $W^2 \sqsupseteq W^1 \wedge \mathrm{lev}(W^2) = \mathrm{lev}(W^1)$
  - $(\mathbf{M}^2, M) \in \mathcal{M}(W^2)$
  - $(*)$ $\Delta; \Gamma \vdash \mathrm{bg}+3 \approx_{W^2} e : \mathsf{ref}\,\tau$
- We now choose W^{pe} to be W^2 and show the required properties.
- $W^2 \sqsupseteq W \wedge \mathrm{lev}(W^2) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^2)$ holds vacuously.
- To show: $\forall W^3 \sqsupseteq W^2.\ \forall \rho \in \mathcal{D}[\![\Delta]\!].\ \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho(W^3).$
  $((\underline{\mathrm{bg}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v} \,\}), \gamma\rho(!e)) \in \mathcal{E}[\![\tau]\!]\rho(W^3)$

- By definition of $\mathcal{E}[\![\tau]\!]\rho(W^3)$ and plugc, we suppose
  - $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau]\!]\rho(W^3)$,
  - $(\mathbf{M}^3, M^3) \in \mathcal{M}(W^3)$,
  - $\mathbf{M}^3$ repr Φ^3,
  - $\mathbf{M}^3.\mathrm{reg}(\mathrm{wk}_0) = \underline{\mathrm{kpc}}$,
  - $\mathbf{M}^3.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v}$.
- To show: $((\Phi^3, \mathrm{bg}), (M^3.h, K[\gamma\rho(!e)])) \in \mathcal{O}(W^3)$
- As W^3 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the three instructions from bg on the low side and get the configurations
$$(\Phi^4, \mathrm{bg} + 3), \quad (M^3.h, K[!\gamma\rho e])$$
such that
  - $\mathbf{M}^4 := \mathbf{M}^3[{+\!+}\, \underline{\mathrm{kpc}}]_{\mathrm{stk}}[\mathrm{wk}_0 \mapsto \underline{\mathrm{bg} + c + 3}]_{\mathrm{reg}}$,
  - $\mathbf{M}^4$ repr Φ^4.
- Let $W^4 := W^3[{+\!+}\, \underline{\mathrm{kpc}}]_1$.
  Then $(\mathbf{M}^4, M^3) \in \mathcal{M}(W^4)$.
  By Theorem 9, it suffices to show that $((\Phi^4, \mathrm{bg} + 3), (M^3.h, K[!\gamma\rho e])) \in \mathcal{O}(W^4)$.
- By $(*)$, it suffices to show that $((\mathrm{bg} + c + 3, \lfloor \mathrm{wk}_5 \rfloor), K[!-]) \in \mathcal{K}[\![\mathsf{ref}\ \tau]\!]\rho(W^4)$.
- Suppose
  $W^5 \sqsupseteq_{\mathrm{pub}} W^4$,
  $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\mathsf{ref}\ \tau]\!]\rho(W^5)$,
  $(\mathbf{M}^5, M^5) \in \mathcal{M}(W^5)$,
  $\mathbf{M}^5.\mathrm{reg}(\mathrm{wk}_5) = \mathbf{v}_1$,
  $\mathbf{M}^5$ repr Φ^5.
- To show: $((\Phi^5, \mathrm{bg} + c + 3), (M^5.h, K[!v_2])) \in \mathcal{O}(W^5)$
- If $\mathrm{lev}(W^5) = 0$ then it trivially holds.
  Assume that $\mathrm{lev}(W^5) > 0$.
- As $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\mathsf{ref}\ \tau]\!]\rho(W^5)$
  - $\mathbf{v}_1 = \widehat{\boldsymbol{l}_1}$, $\mathbf{M}^5.\mathrm{hp}(\boldsymbol{l}_1)(0) = \mathbf{u}_1$ for some $\boldsymbol{l}_1, \mathbf{u}_1$
  - $v_2 = \ell_2$, $M^5.h(\ell_2) = u_2$ for some ℓ_2, u_2
  - $(\mathbf{u}_1, u_2) \in \triangleright\mathcal{V}[\![\tau]\!]\rho(W^5)$
- As W^5 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the three instructions from $\mathrm{bg} + c + 3$ on the low side, take one step on the high side, and get the configurations
$$(\Phi^6, \mathrm{kpc}), \quad (M^6.h, K[u_2])$$
such that
  - $\mathbf{M}^6 := \mathbf{M}^5[\mathrm{wk}_5 \mapsto \mathbf{u}_1]_{\mathrm{reg}}[-1]_{\mathrm{stk}}$,
  - $\mathbf{M}^6$ repr Φ^6,
  - $M^6 := M^5$.

- Let $W^6 := \triangleright W^5[-1]_1$.
  Then $(\mathbf{M}^6, M^6) \in \mathcal{M}(W^6)$.

- By Theorem 9, it suffices to show that $((\Phi^6, \mathrm{kpc}), (M^6.h, K[u_2])) \in \mathcal{O}(W^6)$.
- As $W^6 \sqsupseteq_{\mathrm{pub}} W^3$ and $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau]\!]\rho(W^3)$, it suffices to show that

$$(\mathbf{u}_1, u_2) \in \mathcal{V}[\![\tau]\!]\rho(W^6)$$

  which follows from $(\mathbf{u}_1, u_2) \in \triangleright\mathcal{V}[\![\tau]\!]\rho(W^5)$ by monotonicity of $\mathcal{V}[\![\tau]\!]\rho$.

□

9.17 Refeq

$$(\!|\Gamma \vdash e_1 == e_2|\!) ::= \mathrm{Prefeq}((\!|\Gamma \vdash e_1|\!), (\!|\Gamma \vdash e_2|\!))$$

$\mathrm{Prefeq}(p_1, p_2) ::= \lambda\, \mathrm{alloc}, \mathrm{bg}.$
let $\mathrm{instrs}_1 := p_1(\mathrm{alloc}, \mathrm{bg} + 4),\ c_1 := |\mathrm{instrs}_1|,$
$\quad \mathrm{instrs}_2 := p_2(\mathrm{alloc}, \mathrm{bg} + c_1 + 6),\ c_2 := |\mathrm{instrs}_2| \quad \text{in} \quad [$

bg	`plus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{2}$
	`move`	$\langle \mathrm{sp} - 2 \rangle_{\mathrm{s}}$	$\lfloor \mathrm{wk}_0 \rfloor$	
	`move`	$\langle \mathrm{sp} - 1 \rangle_{\mathrm{s}}$	$\underline{0}$	
	`move`	$\lfloor \mathrm{wk}_0 \rfloor$	$\underline{\mathrm{bg} + c_1 + 4}$	
	instrs_1			
$\mathrm{bg} + c_1 + 4$	`move`	$\langle \mathrm{sp} - 1 \rangle_{\mathrm{s}}$	$\lfloor \mathrm{wk}_5 \rfloor$	
	`move`	$\lfloor \mathrm{wk}_0 \rfloor$	$\underline{\mathrm{bg} + c_1 + c_2 + 6}$	
	instrs_2			
$\mathrm{bg} + c_1 + c_2 + 6$	`jneq`	$\underline{\mathrm{bg} + c_1 + c_2 + 9}$	$\langle \mathrm{sp} - 1 \rangle_{\mathrm{s}}$	$\lfloor \mathrm{wk}_5 \rfloor$
	`move`	$\lfloor \mathrm{wk}_5 \rfloor$	$\underline{1}$	
	`jmp`	$\underline{\mathrm{bg} + c_1 + c_2 + 10}$		
$\mathrm{bg} + c_1 + c_2 + 9$	`move`	$\lfloor \mathrm{wk}_5 \rfloor$	$\underline{0}$	
$\mathrm{bg} + c_1 + c_2 + 10$	`minus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{2}$
	`jmp`	$\langle \mathrm{sp} - 0 \rangle_{\mathrm{s}}$		

]

Lemma 21 (Compatibility: Refeq)**.**

$$\Delta; \Gamma \vdash p_1 \approx e_1 : \mathsf{ref}\ \tau \wedge \Delta; \Gamma \vdash p_2 \approx e_2 : \mathsf{ref}\ \tau \implies \Delta; \Gamma \vdash \mathrm{Prefeq}(p_1, p_2) \approx e_1 == e_2 : \mathsf{bool}$$

Proof.

- For any $\mathcal{A}, \mathrm{gcbg}, \mathrm{bg}, k$, suppose
  - $W \sqsupseteq W_k^\circ(\mathcal{A}, \mathrm{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$
  - $\mathrm{code} := [\mathrm{bg} \Mapsto \mathrm{Prefeq}(p_1, p_2)(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg})]$
  - $\mathrm{code}^{p_1} := [\mathrm{bg} + 4 \Mapsto p_1(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg} + 4)],\ c_1 := |\mathrm{code}^{p_1}|$
  - $\mathrm{code}^{p_2} := [\mathrm{bg} + c_1 + 6 \Mapsto p_2(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg} + c_1 + 6)],\ c_2 := |\mathrm{code}^{p_2}|$
  - $\mathrm{code}^\bullet := \mathrm{code} \setminus \mathrm{code}^{p_1} \setminus \mathrm{code}^{p_2}$
  - $\mathbf{M}' = \mathbf{M} \uplus \{\mathrm{code}\}_{\mathrm{code}}$.

- Goal: find W^{pe} such that
  - $W^{pe} \sqsupseteq W \wedge \mathrm{lev}(W^{pe}) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta; \Gamma \vdash \mathrm{bg} \approx_{W^{pe}} e_1 == e_2 : \mathsf{unit}$

- Let $\mathbf{M}^1 := \mathbf{M} \uplus \{\mathrm{code}^\bullet\}_{\mathrm{code}}$.
  Let $W^1 := W +\!\!+ \iota^{\mathrm{code}}(\mathrm{code}^\bullet)$.
  By definition, we have $(\mathbf{M}^1, M) \in \mathcal{M}(W^1)$.

- Let $\mathbf{M}^2 := \mathbf{M}^1 \uplus \{\mathrm{code}^{p_1}\}_{\mathrm{code}}$.
  From $\Delta; \Gamma \vdash p_1 \approx e_1 : \mathsf{ref}\ \tau$, we have W^2 such that
  - $W^2 \sqsupseteq W^1 \wedge \mathrm{lev}(W^2) = \mathrm{lev}(W^1)$
  - $(\mathbf{M}^2, M) \in \mathcal{M}(W^2)$
  - $(*)$ $\Delta; \Gamma \vdash \mathrm{bg} + 4 \approx_{W^2} e_1 : \mathsf{ref}\ \tau$

- Let $\mathbf{M}^3 := \mathbf{M}^2 \uplus \{\mathrm{code}^{p_2}\}_{\mathrm{code}}$.
  From $\Delta; \Gamma \vdash p_2 \approx e_2 : \mathsf{ref}\ \tau$, we have W^3 such that
  - $W^3 \sqsupseteq W^2 \wedge \mathrm{lev}(W^3) = \mathrm{lev}(W^2)$
  - $(\mathbf{M}^3, M) \in \mathcal{M}(W^3)$
  - $(**)$ $\Delta; \Gamma \vdash \mathrm{bg} + c_1 + 6 \approx_{W^3} e_2 : \mathsf{ref}\ \tau$

- We now choose W^{pe} to be W^3 and show the required properties.

- $W^3 \sqsupseteq W \wedge \mathrm{lev}(W^3) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^3)$ holds vacuously.

- To show: $\forall W^4 \sqsupseteq W^3.\ \forall \rho \in \mathcal{D}[\![\Delta]\!].\ \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho(W^4).$
  $((\underline{\mathrm{bg}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v} \,\}), \gamma\rho(e_1 == e_2)) \in \mathcal{E}[\![\mathsf{unit}]\!]\rho(W^4)$

- By definition of $\mathcal{E}[\![\mathsf{unit}]\!]\rho(W^4)$ and plugc, we suppose
  - $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\mathsf{unit}]\!]\rho(W^4)$,
  - $(\mathbf{M}^4, M^4) \in \mathcal{M}(W^4)$,
  - $\mathbf{M}^4$ repr Φ^4,
  - $\mathbf{M}^4.\mathrm{reg}(\mathrm{wk}_0) = \underline{\mathrm{kpc}}$,
  - $\mathbf{M}^4.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v}$.

- To show: $((\Phi^4, \mathrm{bg}), (M^4.h, K[\gamma\rho(e_1 == e_2)])) \in \mathcal{O}(W^4)$

- As W^4 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the four instructions from bg on the low side and get the configurations

$$(\Phi^5, \mathrm{bg} + 4), \quad (M^4.h, K[\gamma\rho e_1 == \gamma\rho e_2])$$

  such that
  - $\mathbf{M}^5 := \mathbf{M}^4[+\!\!+ \underline{\mathrm{kpc}}, \underline{0}]_{\mathrm{stk}}[\mathrm{wk}_0 \mapsto \underline{\mathrm{bg} + c_1 + 4}]_{\mathrm{reg}}$,
  - $\mathbf{M}^5$ repr Φ^5.

- Let $W^5 := W^4[+\!\!+ \underline{\mathrm{kpc}}, \underline{0}]_1$.
  Then $(\mathbf{M}^5, M^4) \in \mathcal{M}(W^5)$.
  By Theorem 9, it suffices to show that $((\Phi^5, \mathrm{bg} + 4), (M^4.h, K[\gamma\rho e_1 == \gamma\rho e_2])) \in \mathcal{O}(W^5)$.

- By $(*)$, it suffices to show that $((\mathrm{bg} + c_1 + 4, \lfloor \mathrm{wk}_5 \rfloor), K[- == \gamma\rho e_2]) \in \mathcal{K}[\![\mathsf{ref}\ \tau]\!]\rho(W^5)$.

- Suppose
  $W^6 \sqsupseteq_{\mathrm{pub}} W^5$,
  $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\mathsf{ref}\ \tau]\!]\rho(W^6)$,
  $(\mathbf{M}^6, M^6) \in \mathcal{M}(W^6)$,
  $\mathbf{M}^6.\mathrm{reg}(\mathrm{wk}_5) = \mathbf{v}_1$,
  $\mathbf{M}^6$ repr Φ^6.
- To show: $((\Phi^6, \mathrm{bg} + c_1 + 4), (M^6.h, K[v_2 == \gamma\rho e_2])) \in \mathcal{O}(W^6)$
- As W^6 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the two instructions from $\mathrm{bg} + c_1 + 4$ on the low side and get the configurations
  $$(\Phi^7, \mathrm{bg} + c_1 + 6), \quad (M^6.h, K[v_2 == \gamma\rho e_2])$$
  such that
  - $\mathbf{M}^7 := \mathbf{M}^6[|\mathbf{M}^7.\mathrm{stk}| - 1 \mapsto \mathbf{v}_1]_{\mathrm{stk}}[\mathrm{wk}_0 \mapsto \underline{\mathrm{bg} + c_1 + c_2 + 6}]_{\mathrm{reg}}$,
  - $\mathbf{M}^7$ repr Φ^7.
- Let $W^7 := W^6[|\mathbf{M}^7.\mathrm{stk}| - 1 \mapsto \mathbf{v}_1]_1$.
  Then $(\mathbf{M}^7, M^6) \in \mathcal{M}(W^7)$.
  By Theorem 9, it suffices to show that $((\Phi^7, \mathrm{bg} + c_1 + 6), (M^6.h, K[v_2 == \gamma\rho e_2])) \in \mathcal{O}(W^7)$.
- By $(**)$, it suffices to show that $((\mathrm{bg} + c_1 + c_2 + 6, \lfloor \mathrm{wk}_5 \rfloor), K[v_2 == -]) \in \mathcal{K}[\![\mathsf{ref}\ \tau]\!]\rho(W^7)$.
- Suppose
  $W^8 \sqsupseteq_{\mathrm{pub}} W^7$,
  $(\mathbf{v}_3, v_4) \in \mathcal{V}[\![\mathsf{ref}\ \tau]\!]\rho(W^8)$,
  $(\mathbf{M}^8, M^8) \in \mathcal{M}(W^8)$,
  $\mathbf{M}^8.\mathrm{reg}(\mathrm{wk}_5) = \mathbf{v}_3$,
  $\mathbf{M}^8$ repr Φ^8.
- To show: $((\Phi^8, \mathrm{bg} + c_1 + c_2 + 6), (M^8.h, K[v_2 == v_4])) \in \mathcal{O}(W^8)$
- As $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\mathsf{ref}\ \tau]\!]\rho(W^6)$ and $W^8 \sqsupseteq W^6$,
  - $(\mathbf{v}_1, v_2) \in \mathcal{B}(W^8)$
  - v_2 is a location
- As $(\mathbf{v}_3, v_4) \in \mathcal{V}[\![\mathsf{ref}\ \tau]\!]\rho(W^8)$,
  - $(\mathbf{v}_3, v_4) \in \mathcal{B}(W^8)$
  - v_4 is a location
- As W^8 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the instructions from $\mathrm{bg} + c_1 + c_2 + 6$ on the low side, take one step on the high side.
- If $v_2 = v_4$, then by the partial bijectiveness, we have $\mathbf{v}_1 = \mathbf{v}_3$, and thus we get the following configuration.
  $$(\Phi^9, \mathrm{kpc}), \quad (M^9.h, K[\mathsf{tt}])$$
  such that
  - $\mathbf{M}^9 := \mathbf{M}^8[\mathrm{wk}_5 \mapsto \underline{1}]_{\mathrm{reg}}[-2]_{\mathrm{stk}}$
  - $\mathbf{M}^9$ repr Φ^9
  - $M^9 := M^8$

– Let $W^9 := W^8[-2]_1$.
  Then, $(\mathbf{M}^9, M^9) \in \mathcal{M}(W^9)$.
– By Theorem 9, it suffices to show that $((\Phi^9, \mathrm{kpc}), (M^9.h, K[\mathsf{tt}])) \in \mathcal{O}(W^9)$.
– As $W^9 \sqsupseteq_{\mathrm{pub}} W^4$ and $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\mathsf{bool}]\!]\rho(W^4)$, it suffices to show that

$$(\underline{1}, \mathsf{tt}) \in \mathcal{V}[\![\mathsf{unit}]\!]\rho(W^9)$$

  which trivially holds by definition.

- If $v_2 \neq v_4$, then by the partial bijectiveness, we have $\mathbf{v}_1 \neq \mathbf{v}_3$, and thus we get the following configuration.

$$(\Phi^9, \mathrm{kpc}), \quad (M^9.h, K[\mathsf{ff}])$$

such that
- $\mathbf{M}^9 := \mathbf{M}^8[\mathrm{wk}_5 \mapsto \underline{0}]_{\mathrm{reg}}[-2]_{\mathrm{stk}}$
- $\mathbf{M}^9$ repr Φ^9
- $M^9 := M^8$

– Let $W^9 := W^8[-2]_1$.
  Then, $(\mathbf{M}^9, M^9) \in \mathcal{M}(W^9)$.
– By Theorem 9, it suffices to show that $((\Phi^9, \mathrm{kpc}), (M^9.h, K[\mathsf{ff}])) \in \mathcal{O}(W^9)$.
– As $W^9 \sqsupseteq_{\mathrm{pub}} W^4$ and $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\mathsf{bool}]\!]\rho(W^4)$, it suffices to show that

$$(\underline{0}, \mathsf{ff}) \in \mathcal{V}[\![\mathsf{unit}]\!]\rho(W^9)$$

  which trivially holds by definition.

□

9.18 If

$$(\!|\Gamma \vdash \mathsf{if}\ e_1\ \mathsf{then}\ e_2\ \mathsf{else}\ e_3|\!) ::= \mathrm{Pif}((\!|\Gamma \vdash e_1|\!), (\!|\Gamma \vdash e_2|\!), (\!|\Gamma \vdash e_3|\!))$$

$\mathrm{Pif}(p_1, p_2, p_3) ::= \lambda\, \mathrm{alloc}, \mathrm{bg}.$
let $\mathrm{instrs}_1 := p_1(\mathrm{alloc}, \mathrm{bg} + 3)$, $c_1 := |\mathrm{instrs}_1|$,
$\mathrm{instrs}_2 := p_2(\mathrm{alloc}, \mathrm{bg} + c_1 + c_3 + 5)$, $c_2 := |\mathrm{instrs}_2|$,
$\mathrm{instrs}_3 := p_3(\mathrm{alloc}, \mathrm{bg} + c_1 + 5)$, $c_3 := |\mathrm{instrs}_3|$ in [

bg	`plus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{1}$
	`move`	$\langle \mathrm{sp} - 1 \rangle_{\mathrm{s}}$	$\lfloor \mathrm{wk}_0 \rfloor$	
	`move`	$\lfloor \mathrm{wk}_0 \rfloor$	$\underline{\mathrm{bg} + c_1 + 3}$	
	instrs_1			
$\mathrm{bg} + c_1 + 3$	`move`	$\lfloor \mathrm{wk}_0 \rfloor$	$\underline{\mathrm{bg} + c_1 + c_2 + c_3 + 5}$	
	`jnz`	$\mathrm{bg} + c_1 + c_3 + 5$	$\lfloor \mathrm{wk}_5 \rfloor$	
	instrs_3			
	instrs_2			
$\mathrm{bg} + c_1 + c_2 + c_3 + 5$	`minus`	$\lfloor \mathrm{sp} \rfloor$	$\lfloor \mathrm{sp} \rfloor$	$\underline{1}$
	`jmp`	$\langle \mathrm{sp} - 0 \rangle_{\mathrm{s}}$		

]

Lemma 22 (Compatibility: If)**.**

$$\Delta;\Gamma \vdash p_1 \approx e_1 : \mathsf{bool} \wedge \Delta;\Gamma \vdash p_2 \approx e_2 : \tau \wedge \Delta;\Gamma \vdash p_3 \approx e_3 : \tau$$
$$\implies \Delta;\Gamma \vdash \mathrm{Pif}(p_1,p_2,p_3) \approx \mathsf{if}\ e_1\ \mathsf{then}\ e_2\ \mathsf{else}\ e_3 : \tau$$

Proof.

- For any $\mathcal{A}, \mathrm{gcbg}, \mathrm{bg}, k$, suppose
  - $W \sqsupseteq W_k^\circ(\mathcal{A}, \mathrm{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$
  - $\mathrm{code} := [\mathrm{bg} \Mapsto \mathrm{Pif}(p_1,p_2,p_3)(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg})]$
  - $\mathrm{code}^{p_1} := [\mathrm{bg}+3 \Mapsto p_1(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg}+3)]$, $c_1 := |\mathrm{code}^{p_1}|$
  - $\mathrm{code}^{p_3} := [\mathrm{bg}+c_1+5 \Mapsto p_3(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg}+c_1+5)]$, $c_3 := |\mathrm{code}^{p_3}|$
  - $\mathrm{code}^{p_2} := [\mathrm{bg}+c_1+c_3+5 \Mapsto p_2(\mathcal{A}(\mathrm{gcbg}).\mathrm{alloc}, \mathrm{bg}+c_1+c_3+5)]$, $c_2 := |\mathrm{code}^{p_2}|$
  - $\mathrm{code}^\bullet := \mathrm{code} \setminus \mathrm{code}^{p_1} \setminus \mathrm{code}^{p_3} \setminus \mathrm{code}^{p_2}$
  - $\mathbf{M}' = \mathbf{M} \uplus \{\mathrm{code}\}_{\mathrm{code}}$.
- Goal: find W^{pe} such that
  - $W^{pe} \sqsupseteq W \wedge \mathrm{lev}(W^{pe}) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta;\Gamma \vdash \mathrm{bg} \approx_{W^{pe}} \mathsf{if}\ e_1\ \mathsf{then}\ e_2\ \mathsf{else}\ e_3 : \tau$
- Let $\mathbf{M}^1 := \mathbf{M} \uplus \{\mathrm{code}^\bullet\}_{\mathrm{code}}$.
  Let $W^1 := W +\!\!+ \iota^{\mathrm{code}}(\mathrm{code}^\bullet)$.
  By definition, we have $(\mathbf{M}^1, M) \in \mathcal{M}(W^1)$.
- Let $\mathbf{M}^2 := \mathbf{M}^1 \uplus \{\mathrm{code}^{p_1}\}_{\mathrm{code}}$.
  From $\Delta;\Gamma \vdash p_1 \approx e_1 : \mathsf{bool}$, we have W^2 such that
  - $W^2 \sqsupseteq W^1 \wedge \mathrm{lev}(W^2) = \mathrm{lev}(W^1)$
  - $(\mathbf{M}^2, M) \in \mathcal{M}(W^2)$
  - $(*)$ $\Delta;\Gamma \vdash \mathrm{bg}+3 \approx_{W^2} e_1 : \mathsf{bool}$
- Let $\mathbf{M}^3 := \mathbf{M}^2 \uplus \{\mathrm{code}^{p_3}\}_{\mathrm{code}}$.
  From $\Delta;\Gamma \vdash p_3 \approx e_3 : \tau$, we have W^3 such that
  - $W^3 \sqsupseteq W^2 \wedge \mathrm{lev}(W^3) = \mathrm{lev}(W^2)$
  - $(\mathbf{M}^3, M) \in \mathcal{M}(W^3)$
  - $(**)$ $\Delta;\Gamma \vdash \mathrm{bg}+c_1+5 \approx_{W^3} e_3 : \tau$
- Let $\mathbf{M}^4 := \mathbf{M}^3 \uplus \{\mathrm{code}^{p_2}\}_{\mathrm{code}}$.
  From $\Delta;\Gamma \vdash p_2 \approx e_2 : \tau$, we have W^4 such that
  - $W^4 \sqsupseteq W^3 \wedge \mathrm{lev}(W^4) = \mathrm{lev}(W^3)$
  - $(\mathbf{M}^4, M) \in \mathcal{M}(W^4)$
  - $(***)$ $\Delta;\Gamma \vdash \mathrm{bg}+c_1+c_3+5 \approx_{W^4} e_2 : \tau$
- We now choose W^{pe} to be W^4 and show the required properties.
- $W^4 \sqsupseteq W \wedge \mathrm{lev}(W^4) = \mathrm{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^4)$ holds vacuously.
- To show: $\forall W^5 \sqsupseteq W^4.\ \forall \rho \in \mathcal{D}[\![\Delta]\!].\ \forall (\mathbf{v},\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho(W^5).$
  $((\underline{\mathrm{bg}}, \lfloor \mathrm{wk}_0 \rfloor, \lfloor \mathrm{wk}_5 \rfloor, \{\, \mathbf{M} \mid \mathbf{M}.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v} \,\}), \gamma\rho(\mathsf{if}\ e_1\ \mathsf{then}\ e_2\ \mathsf{else}\ e_3)) \in \mathcal{E}[\![\tau]\!]\rho(W^5)$

- By definition of $\mathcal{E}[\![\tau]\!]\rho(W^5)$ and plugc, we suppose
  - $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau]\!]\rho(W^5)$,
  - $(\mathbf{M}^5, M^5) \in \mathcal{M}(W^5)$,
  - $\mathbf{M}^5$ repr Φ^5,
  - $\mathbf{M}^5.\mathrm{reg}(\mathrm{wk}_0) = \underline{\mathrm{kpc}}$,
  - $\mathbf{M}^5.\mathrm{reg}(\mathrm{sv}_0) = \mathbf{v}$.
- To show: $((\Phi^5, \mathrm{bg}), (M^5.h, K[\gamma\rho(\mathsf{if}\ e_1\ \mathsf{then}\ e_2\ \mathsf{else}\ e_3)])) \in \mathcal{O}(W^5)$
- As W^5 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the three instructions from bg on the low side and get the configurations

  $$(\Phi^6, \mathrm{bg} + 3), \quad (M^5.h, K[\gamma\rho(\mathsf{if}\ e_1\ \mathsf{then}\ e_2\ \mathsf{else}\ e_3)])$$

  such that
  - $\mathbf{M}^6 := \mathbf{M}^5[{+\!+}\,\underline{\mathrm{kpc}}]_{\mathrm{stk}}[\mathrm{wk}_0 \mapsto \underline{\mathrm{bg} + c_1 + 3}]_{\mathrm{reg}}$,
  - $\mathbf{M}^6$ repr Φ^6.
- Let $W^6 := W^5[{+\!+}\,\underline{\mathrm{kpc}}]_1$.
  Then $(\mathbf{M}^6, M^5) \in \mathcal{M}(W^6)$.
  By Theorem 9, it suffices to show that $((\Phi^6, \mathrm{bg} + 3), (M^5.h, K[\gamma\rho(\mathsf{if}\ e_1\ \mathsf{then}\ e_2\ \mathsf{else}\ e_3)])) \in \mathcal{O}(W^6)$.
- By $(*)$, it suffices to show that

  $$((\mathrm{bg} + c_1 + 3, \lfloor \mathrm{wk}_5 \rfloor), K[\mathsf{if}\ -\ \mathsf{then}\ \gamma\rho e_2\ \mathsf{else}\ \gamma\rho e_3]) \in \mathcal{K}[\![\mathsf{bool}]\!]\rho(W^6)$$

- Suppose
  $W^7 \sqsupseteq_{\mathrm{pub}} W^6$,
  $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\mathsf{bool}]\!]\rho(W^7)$,
  $(\mathbf{M}^7, M^7) \in \mathcal{M}(W^7)$,
  $\mathbf{M}^7.\mathrm{reg}(\mathrm{wk}_5) = \mathbf{v}_1$,
  $\mathbf{M}^7$ repr Φ^7.
- To show: $((\Phi^7, \mathrm{bg} + c_1 + 3), (M^7.h, K[\mathsf{if}\ v_2\ \mathsf{then}\ \gamma\rho e_2\ \mathsf{else}\ \gamma\rho e_3])) \in \mathcal{O}(W^7)$
- As $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\mathsf{bool}]\!]\rho(W^7)$, we have two cases.

When $\mathbf{v}_1 \neq \underline{0}$ and $v_2 = \mathsf{tt}$

- As W^7 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the two instructions from $\mathrm{bg} + c_1 + 3$ on the low side, take one step on the high side, and get the configurations

  $$(\Phi^8, \mathrm{bg} + c_1 + c_3 + 5), \quad (M^7.h, K[\gamma\rho e_2])$$

  such that
  - $\mathbf{M}^8 := \mathbf{M}^7[\mathrm{wk}_0 \mapsto \underline{\mathrm{bg} + c_1 + c_2 + c_3 + 5}]_{\mathrm{reg}}$,
  - $\mathbf{M}^8$ repr Φ^8.

- Still, $(\mathbf{M}^8, M^7) \in \mathcal{M}(W^7)$.
  By Theorem 9, it suffices to show that

$$((\Phi^8, \mathrm{bg} + c_1 + c_3 + 5), (M^7.h, K[\gamma\rho e_2])) \in \mathcal{O}(W^7)$$

- By $(***)$, it suffices to show that $((\mathrm{bg} + c_1 + c_2 + c_3 + 5, \lfloor \mathrm{wk}_5 \rfloor), K[-]) \in \mathcal{K}[\![\tau]\!]\rho(W^7)$.
- Suppose
  $W^9 \sqsupseteq_{\mathrm{pub}} W^7$,
  $(\mathbf{v}_3, v_4) \in \mathcal{V}[\![\tau]\!]\rho(W^9)$,
  $(\mathbf{M}^9, M^9) \in \mathcal{M}(W^9)$,
  $\mathbf{M}^9.\mathrm{reg}(\mathrm{wk}_5) = \mathbf{v}_3$,
  $\mathbf{M}^9$ repr Φ^9.
- To show: $((\Phi^9, \mathrm{bg} + c_1 + c_2 + c_3 + 5), (M^9.h, K[v_4])) \in \mathcal{O}(W^9)$
- As W^9 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the instructions from $\mathrm{bg} + c_1 + c_2 + c_3 + 5$ on the low side and get the following

$$(\Phi^{10}, \mathrm{kpc}), \quad (M^9.h, K[v_4])$$

  such that
  - $\mathbf{M}^{10} := \mathbf{M}^9[-1]_{\mathrm{stk}}$
  - $\mathbf{M}^{10}$ repr Φ^{10}

- Let $W^{10} := W^9[-1]_1$.
  Then, $(\mathbf{M}^{10}, M^9) \in \mathcal{M}(W^{10})$.
- By Theorem 9, it suffices to show that $((\Phi^{10}, \mathrm{kpc}), (M^9.h, K[v_4])) \in \mathcal{O}(W^{10})$.
- As $W^{10} \sqsupseteq_{\mathrm{pub}} W^5$ and $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau]\!]\rho(W^5)$, it suffices to show that

$$(\mathbf{v}_3, v_4) \in \mathcal{V}[\![\tau]\!]\rho(W^{10})$$

  which follows from $(\mathbf{v}_3, v_4) \in \mathcal{V}[\![\tau]\!]\rho(W^9)$ by Theorem 5.

When $\mathbf{v}_1 = \underline{0}$ and $v_2 = \mathsf{ff}$

- As W^7 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the two instructions from $\mathrm{bg} + c_1 + 3$ on the low side, take one step on the high side, and get the configurations

$$(\Phi^8, \mathrm{bg} + c_1 + 5), \quad (M^7.h, K[\gamma\rho e_3])$$

  such that
  - $\mathbf{M}^8 := \mathbf{M}^7[\mathrm{wk}_0 \mapsto \underline{\mathrm{bg} + c_1 + c_2 + c_3 + 5}]_{\mathrm{reg}}$,
  - $\mathbf{M}^8$ repr Φ^8.

- Still, $(\mathbf{M}^8, M^7) \in \mathcal{M}(W^7)$.
  By Theorem 9, it suffices to show that

$$((\Phi^8, \mathrm{bg} + c_1 + 5), (M^7.h, K[\gamma\rho e_3])) \in \mathcal{O}(W^7)$$

- By $(**)$, it suffices to show that $((\mathrm{bg} + c_1 + c_2 + c_3 + 5, \lfloor \mathrm{wk}_5 \rfloor), K[-]) \in \mathcal{K}[\![\tau]\!]\rho(W^7)$.
- Suppose
  $W^9 \sqsupseteq_{\mathrm{pub}} W^7$,
  $(\mathbf{v}_3, v_4) \in \mathcal{V}[\![\tau]\!]\rho(W^9)$,
  $(\mathbf{M}^9, M^9) \in \mathcal{M}(W^9)$,
  $\mathbf{M}^9.\mathrm{reg}(\mathrm{wk}_5) = \mathbf{v}_3$,
  $\mathbf{M}^9$ repr Φ^9.
- To show: $((\Phi^9, \mathrm{bg} + c_1 + c_2 + c_3 + 5), (M^9.h, K[v_4])) \in \mathcal{O}(W^9)$
- As W^9 includes $\iota^{\mathrm{code}}(\mathrm{code}^\bullet)$, we execute the instructions from $\mathrm{bg} + c_1 + c_2 + c_3 + 5$ on the low side and get the following

  $$(\Phi^{10}, \mathrm{kpc}), \quad (M^9.h, K[v_4])$$

  such that
  - $\mathbf{M}^{10} := \mathbf{M}^9[-1]_{\mathrm{stk}}$
  - $\mathbf{M}^{10}$ repr Φ^{10}

- Let $W^{10} := W^9[-1]_1$.
  Then, $(\mathbf{M}^{10}, M^9) \in \mathcal{M}(W^{10})$.
- By Theorem 9, it suffices to show that $((\Phi^{10}, \mathrm{kpc}), (M^9.h, K[v_4])) \in \mathcal{O}(W^{10})$.
- As $W^{10} \sqsupseteq_{\mathrm{pub}} W^5$ and $((\mathrm{kpc}, \lfloor \mathrm{wk}_5 \rfloor), K) \in \mathcal{K}[\![\tau]\!]\rho(W^5)$, it suffices to show that

  $$(\mathbf{v}_3, v_4) \in \mathcal{V}[\![\tau]\!]\rho(W^{10})$$

  which follows from $(\mathbf{v}_3, v_4) \in \mathcal{V}[\![\tau]\!]\rho(W^9)$ by Theorem 5.

□

⋮