

# A Kripke Logical Relation Between ML and Assembly

## Technical Appendix

Chung-Kil Hur  
gil@mpi-sws.org

Derek Dreyer  
dreyer@mpi-sws.org

Original Draft: July 2010  
Revised: November 2010

# Contents

<b>1</b>	<b>Languages</b>	<b>4</b>
1.1	<b>HIGH</b> . . . . .	4
1.1.1	Syntax & Dynamic Semantics . . . . .	4
1.1.2	Static Semantics . . . . .	4
1.2	<b>LOW</b> . . . . .	6
1.2.1	Syntax & Dynamic Semantics . . . . .	6
<b>2</b>	<b>Specifications</b>	<b>8</b>
2.1	Language Specification . . . . .	8
2.2	World Specification . . . . .	9
<b>3</b>	<b>Logical Relations</b>	<b>10</b>
3.1	Definitions . . . . .	10
3.2	Properties . . . . .	11
<b>4</b>	<b>Possible Worlds</b>	<b>15</b>
4.1	Definitions . . . . .	15
4.2	Properties . . . . .	16
<b>5</b>	<b>Specification of HIGH</b>	<b>18</b>
5.1	LangSpec of <b>HIGH</b> . . . . .	18
<b>6</b>	<b>Specification of LOW</b>	<b>19</b>
6.1	LangSpec of <b>LOW</b> . . . . .	19
6.2	Garbage Collector Specification . . . . .	22
<b>7</b>	<b>Low High Relations</b>	<b>23</b>
7.1	Initial Worlds . . . . .	23
7.2	Program Equivalence . . . . .	23
7.3	Adequacy and Compositionality . . . . .	24
<b>8</b>	<b>Self-Modifying Awkward Example</b>	<b>27</b>
8.1	Definitions . . . . .	27
8.2	Properties . . . . .	27
<b>9</b>	<b>Compiler Correctness</b>	<b>33</b>
9.1	Compiler Definition and Correctness . . . . .	33
9.2	Var . . . . .	33
9.3	Pair . . . . .	35
9.4	Fst . . . . .	38
9.5	Snd . . . . .	40
9.6	Abs . . . . .	41
9.7	App . . . . .	45
9.8	Gen . . . . .	48
9.9	Inst . . . . .	51
9.10	Pack . . . . .	54

9.11 Unpack . . . . .	55
9.12 Roll . . . . .	59
9.13 Unroll . . . . .	60
9.14 New . . . . .	62
9.15 Asgn . . . . .	65
9.16 Deref . . . . .	68
9.17 Refeq . . . . .	70
9.18 If . . . . .	73

# 1 Languages

## 1.1 HIGH

### 1.1.1 Syntax & Dynamic Semantics

$\tau \in \text{Type} ::= \alpha \mid b \mid \tau_1 \times \tau_2 \mid \tau_1 \rightarrow \tau_2 \mid \forall \alpha. \tau \mid \exists \alpha. \tau \mid \mu \alpha. \tau \mid \text{ref } \tau$   
 where  $\alpha \in \text{TypeVar}$

$e \in \text{HExp} ::= x \mid \ell \mid \langle e_1, e_2 \rangle \mid e.1 \mid e.2 \mid$   
 $\lambda x:\tau. e \mid e_1 e_2 \mid \Lambda \alpha. e \mid e \tau \mid \text{pack } \langle \tau_1, e \rangle \text{ as } \tau_2 \mid \text{unpack } e_1 \text{ as } \langle \alpha, x \rangle \text{ in } e_2 \mid$   
 $\text{roll}_\tau e \mid \text{unroll } e \mid \text{ref } e \mid e_1 := e_2 \mid !e \mid e_1 == e_2 \mid \dots$   
 where  $x \in \text{Var}$  and  $\ell \in \text{HLoc}$

$v \in \text{HVal} ::= x \mid \ell \mid \langle v_1, v_2 \rangle \mid \lambda x:\tau. e \mid \Lambda \alpha. e \mid \text{pack } \langle \tau_1, v \rangle \text{ as } \tau_2 \mid \text{roll}_\tau v \mid \dots$

$K \in \text{HCont} ::= \bullet \mid \langle K, e_2 \rangle \mid \langle v_1, K \rangle \mid K.1 \mid K.2 \mid$   
 $K e_2 \mid v_1 K \mid K \tau \mid \text{pack } \langle \tau_1, K \rangle \text{ as } \tau_2 \mid \text{unpack } K \text{ as } \langle \alpha, x \rangle \text{ in } e_2 \mid$   
 $\text{roll}_\tau K \mid \text{unroll } K \mid \text{ref } K \mid K := e_2 \mid v_1 := K \mid !K \mid K == e_2 \mid v_1 == K \mid \dots$

$\text{HCVal} \stackrel{\text{def}}{=} \{ v \in \text{HVal} \mid \text{ftv}(v) = \emptyset \wedge \text{fv}(v) = \emptyset \}$

$\text{HHeap} \stackrel{\text{def}}{=} \{ h \in \text{HLoc} \rightarrow_{\text{fin}} \text{HCVal} \}$

$\text{freshloc} \in \{ f \in \mathbb{P}_{\text{fin}}(\text{HLoc}) \rightarrow \text{HLoc} \mid \forall S. f(S) \notin S \}$

$(h, e) \hookrightarrow (h', e')$

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

### 1.1.2 Static Semantics

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

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

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

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

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

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

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

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

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

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

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

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

...

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

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

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

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

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

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

## 1.2 LOW

### 1.2.1 Syntax & Dynamic Semantics

PConf	$\stackrel{\text{def}}{=} \{ (\Phi, \text{pc}) \in \text{PMem} \times \text{PAddr} \}$
PMem	$\stackrel{\text{def}}{=} \{ \Phi = (\text{code}, \text{reg}, \text{stk}, \text{hp}) \in \text{PCode} \times \text{PRegFile} \times \text{PStack} \times \text{PHeap} \}$
PCode	$\stackrel{\text{def}}{=} \text{PAddr} \rightarrow \text{Instruction}$
PRegFile	$\stackrel{\text{def}}{=} \text{Register} \rightarrow \text{PWord}$
PStack	$\stackrel{\text{def}}{=} \text{PAddr} \rightarrow \text{PWord}$
PHeap	$\stackrel{\text{def}}{=} \text{PAddr} \rightarrow \text{PWord}$
PAddr	$\stackrel{\text{def}}{=} \{ a \in \mathbb{N} \}$
PWord	$\stackrel{\text{def}}{=} \{ w \in \{0, 1\} \times \mathbb{N} \}$
$r \in \text{Register}$	$::= \text{sp} \mid \text{sv}_0 \mid \dots \mid \text{sv}_4 \mid \text{wk}_0 \mid \dots \mid \text{wk}_5$
$\text{lv} \in \text{PLvalue}$	$::= [r] \mid \langle a \rangle_s \mid \langle r - o \rangle_s \mid \langle a \rangle_h \mid \langle r + o \rangle_h$ for $r \in \text{Register}, a \in \text{PAddr}, o \in \mathbb{N}$
$\text{rv} \in \text{PRvalue}$	$::= \text{lv} \mid w$ for $\text{lv} \in \text{PLvalue}, w \in \text{PWord}$
$\iota \in \text{Instruction}$	$::= \text{fail} \mid \text{halt} \mid \text{jmp } \text{rv} \mid \text{jnz } \text{rv } \text{rv} \mid \text{jneq } \text{rv } \text{rv } \text{rv} \mid \text{jptr } \text{rv } \text{rv} \mid$ $\text{move } \text{lv } \text{rv} \mid \text{setptr } \text{lv} \mid \text{plus } \text{lv } \text{rv } \text{rv} \mid \text{minus } \text{lv } \text{rv } \text{rv} \mid$ $\text{isr } \text{lv } \text{rv} \mid \text{isw } \text{rv } \text{rv}$
$ w $	$\stackrel{\text{def}}{=} \pi_2(w)$
$\text{isptr}(w)$	$\stackrel{\text{def}}{=} \pi_1(w) = 1$
$\underline{n}$	$\stackrel{\text{def}}{=} (0, n) \in \text{PWord}$
$\hat{a}$	$\stackrel{\text{def}}{=} (1, a) \in \text{PWord}$

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

$\Phi([r])$	$\stackrel{\text{def}}{=} \Phi.\text{reg}(r)$
$\Phi(\langle a \rangle_s)$	$\stackrel{\text{def}}{=} \Phi.\text{stk}(a)$
$\Phi(\langle r - o \rangle_s)$	$\stackrel{\text{def}}{=} \Phi.\text{stk}( \Phi([r])  - o)$
$\Phi(\langle a \rangle_h)$	$\stackrel{\text{def}}{=} \Phi.\text{hp}(a)$
$\Phi(\langle r + o \rangle_h)$	$\stackrel{\text{def}}{=} \Phi.\text{hp}( \Phi([r])  + o)$
$\Phi(w)$	$\stackrel{\text{def}}{=} w$

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

$\Phi[[r] \mapsto w]$	$\stackrel{\text{def}}{=} (\Phi.\text{code}, \Phi.\text{reg}[r \mapsto w], \Phi.\text{stk}, \Phi.\text{hp})$
$\Phi[\langle a \rangle_s \mapsto w]$	$\stackrel{\text{def}}{=} (\Phi.\text{code}, \Phi.\text{reg}, \Phi.\text{stk}[a \mapsto w], \Phi.\text{hp})$
$\Phi[\langle r - o \rangle_s \mapsto w]$	$\stackrel{\text{def}}{=} (\Phi.\text{code}, \Phi.\text{reg}, \Phi.\text{stk}[ \Phi([r])  - o \mapsto w], \Phi.\text{hp})$
$\Phi[\langle a \rangle_h \mapsto w]$	$\stackrel{\text{def}}{=} (\Phi.\text{code}, \Phi.\text{reg}, \Phi.\text{stk}, \Phi.\text{hp}[a \mapsto w])$
$\Phi[\langle r + o \rangle_h \mapsto w]$	$\stackrel{\text{def}}{=} (\Phi.\text{code}, \Phi.\text{reg}, \Phi.\text{stk}, \Phi.\text{hp}[ \Phi([r])  + o \mapsto w])$

$$\llbracket \iota \rrbracket (\Phi, \text{pc}) \in \text{PConf} \uplus \{ \text{halt}, \text{fail} \}$$

$$\begin{aligned}
\llbracket \text{fail} \rrbracket (\Phi, \text{pc}) &\stackrel{\text{def}}{=} \text{fail} \\
\llbracket \text{halt} \rrbracket (\Phi, \text{pc}) &\stackrel{\text{def}}{=} \text{halt} \\
\llbracket \text{jmp } rv \rrbracket (\Phi, \text{pc}) &\stackrel{\text{def}}{=} (\Phi, |\Phi(rv)|) \\
\llbracket \text{jnz } rv_1 \text{ } rv_2 \rrbracket (\Phi, \text{pc}) &\stackrel{\text{def}}{=} \text{if } \Phi(rv_2) \neq \underline{0} \text{ then } (\Phi, |\Phi(rv_1)|) \text{ else } (\Phi, \text{pc} + 1) \\
\llbracket \text{jneq } rv_1 \text{ } rv_2 \text{ } rv_3 \rrbracket (\Phi, \text{pc}) &\stackrel{\text{def}}{=} \text{if } \Phi(rv_2) \neq \Phi(rv_3) \text{ then } (\Phi, |\Phi(rv_1)|) \text{ else } (\Phi, \text{pc} + 1) \\
\llbracket \text{jptr } rv_1 \text{ } rv_2 \rrbracket (\Phi, \text{pc}) &\stackrel{\text{def}}{=} \text{if } \text{isptr}(\Phi(rv_2)) \text{ then } (\Phi, |\Phi(rv_1)|) \text{ else } (\Phi, \text{pc} + 1) \\
\llbracket \text{move } lv \text{ } rv \rrbracket (\Phi, \text{pc}) &\stackrel{\text{def}}{=} (\Phi[lv \mapsto \Phi(rv)], \text{pc} + 1) \\
\llbracket \text{setptr } lv \rrbracket (\Phi, \text{pc}) &\stackrel{\text{def}}{=} (\Phi[lv \mapsto \widehat{|\Phi(lv)|}], \text{pc} + 1) \\
\llbracket \text{plus } lv \text{ } rv_1 \text{ } rv_2 \rrbracket (\Phi, \text{pc}) &\stackrel{\text{def}}{=} (\Phi[lv \mapsto \underline{|\Phi(rv_1)| + |\Phi(rv_2)|}], \text{pc} + 1) \\
\llbracket \text{minus } lv \text{ } rv_1 \text{ } rv_2 \rrbracket (\Phi, \text{pc}) &\stackrel{\text{def}}{=} (\Phi[lv \mapsto \underline{|\Phi(rv_1)| - |\Phi(rv_2)|}], \text{pc} + 1) \\
\llbracket \text{isr } lv \text{ } rv \rrbracket (\Phi, \text{pc}) &\stackrel{\text{def}}{=} (\Phi[lv \mapsto \underline{\mathbb{E}(\Phi.\text{code}(|\Phi(rv)|))}], \text{pc} + 1) \\
\llbracket \text{isw } rv_1 \text{ } rv_2 \rrbracket (\Phi, \text{pc}) &\stackrel{\text{def}}{=} ((\Phi.\text{code}[|\Phi(rv_1)| \mapsto \mathbb{D}(|\Phi(rv_2)|)], \Phi.\text{reg}, \Phi.\text{stk}, \Phi.\text{hp}), \text{pc} + 1)
\end{aligned}$$

where

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

$$\text{PConf} \hookrightarrow \text{PConf} \uplus \{ \text{halt}, \text{fail} \}$$

$$(\Phi, \text{pc}) \hookrightarrow \llbracket \Phi.\text{code}(\text{pc}) \rrbracket (\Phi, \text{pc})$$

## 2 Specifications

### 2.1 Language Specification

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

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

$$\boxed{\text{Conf} \xrightarrow{k} \text{Conf} \uplus \{ \text{fail}, \text{halt} \}}$$

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

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

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



observe : Conf  $\rightarrow$  { fail, halt, diverge }

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

## 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 \\ &\quad \text{World} \in \text{Set} \wedge \\ &\quad \text{lev} \in \text{World} \rightarrow \mathbb{N} \wedge \\ &\quad \mathcal{M} \in \text{World} \rightarrow \mathbb{P}(\mathcal{L}_1.\text{Mem} \times \mathcal{L}_2.\text{Mem}) \wedge \\ &\quad \mathcal{B} \in \text{World} \rightarrow \mathbb{P}(\mathcal{L}_1.\text{Val} \times \mathcal{L}_2.\text{Val}) \wedge \\ &\quad \mathcal{O} \in \text{World} \rightarrow \mathbb{P}(\mathcal{L}_1.\text{Conf} \times \mathcal{L}_2.\text{Conf}) \wedge \\ &\quad \triangleright \in \text{World} \rightarrow \text{World} \wedge \\ &\quad \sqsupseteq \in \mathbb{P}(\text{World} \times \text{World}) \wedge \\ &\quad \sqsupseteq_{\text{pub}} \in \mathbb{P}(\text{World} \times \text{World}) \wedge \\ &\quad \sqsupseteq, \sqsupseteq_{\text{pub}} \text{ are preorders} \wedge \sqsupseteq_{\text{pub}} \subseteq \sqsupseteq \wedge \\ &\quad \forall W' \sqsupseteq W. \triangleright W' \sqsupseteq \triangleright W \wedge \\ &\quad \forall W' \sqsupseteq_{\text{pub}} W. \triangleright W' \sqsupseteq_{\text{pub}} \triangleright W \wedge \\ &\quad \forall W. \triangleright W \sqsupseteq_{\text{pub}} W \wedge \\ &\quad \forall W' \sqsupseteq W. \text{lev}(W') \leq \text{lev}(W) \wedge \\ &\quad \forall W. \text{lev}(W) > 0 \implies \text{lev}(\triangleright W) = \text{lev}(W) - 1 \} \\ \sqsupseteq_{\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 \} \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 \} \text{ for } R \in \text{WVRel} \\ \square R &\stackrel{\text{def}}{=} \{ (W, \mathbf{v}_1, v_2) \mid \forall W' \sqsupseteq W. (W', \mathbf{v}_1, v_2) \in R \} \text{ for } R \in \text{WVRel} \\ \overline{R_{\sqsupseteq_{\triangleright} W}} &\stackrel{\text{def}}{=} \{ (W', \mathbf{v}_1, v_2) \mid W' \sqsupseteq_{\triangleright} W \wedge (W', \mathbf{v}_1, v_2) \in R \} \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.**  $\sqsupseteq_{\triangleright}$  is well-founded.

*Proof.* Because the level of worlds strictly decreases. □

**Lemma 2.**

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

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

### 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  $\tau$ :

$$\begin{aligned}
\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} \rightarrow \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}}{=} \overline{\square(\mathcal{L}_1.\text{oftype}(\rho.1(\tau)), \mathcal{L}_2.\text{oftype}(\rho.2(\tau)))} \\
\\
\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 \square\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 \overline{\square(\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 \overline{\square(\mathcal{L}_1.\text{pair}(\mathbf{u}_1, \mathbf{u}'_1), \mathcal{L}_2.\text{pair}(u_2, u'_2))} \} \\
\mathcal{V}[\tau' \rightarrow \tau]\rho &\stackrel{\text{def}}{=} \{ (W, \mathbf{v}_1, v_2) \in \text{oftype}(\tau' \rightarrow \tau, \rho) \mid \forall W' \supseteq_b 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' \supseteq_b 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 \overline{\square(\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 \\
&\quad \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). \\
&\quad (W, \mathbf{v}_1, v_2) \in \overline{\square(\mathcal{L}_1.\text{roll}(\mathbf{u}_1), \mathcal{L}_2.\text{roll}(u_2))} \} \\
\mu(F)(W) &\stackrel{\text{def}}{=} F(\mu(F)_{\supseteq_b W})(W) \quad \text{for } F \in \text{WVRel} \rightarrow \text{WVRel} \\
\mathcal{V}[\text{ref } \tau]\rho &\stackrel{\text{def}}{=} \{ (W, \mathbf{v}_1, v_2) \in \text{oftype}(\text{ref } \tau, \rho) \mid \forall W' \supseteq W. \forall(\mathbf{M}_1, M_2) \in \mathcal{M}(W'). \\
&\quad (\mathbf{v}_1, v_2) \in \mathcal{B}(W') \wedge \\
&\quad (\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)) \wedge \\
&\quad (\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')) \} \\
\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' \supseteq_{\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{aligned}$$



**Lemma 4.**

$$\begin{aligned} \forall \alpha, \tau, \rho. \tau \text{ } \alpha\text{-non-contractible} \wedge \text{ftv}(\mu\alpha. \tau) \subseteq \text{dom } \rho \\ \implies \forall \tau_1, \tau_2, R, W. \mathcal{V}[\tau]\rho[\alpha \mapsto (\tau_1, \tau_2, R_{\sqsupset_b W})](W) = \emptyset \end{aligned}$$

*Proof.* We prove this by structural induction on  $\tau$   $\alpha$ -non-contractible.

- When  $\tau = \alpha$ :  
 $\mathcal{V}[\alpha]\rho[\alpha \mapsto (\tau_1, \tau_2, R_{\sqsupset_b W})](W) \subseteq R_{\sqsupset_b W}(W) = \emptyset$ .
- When  $\tau = \exists\beta. \tau'$  with  $\beta \neq \alpha \wedge \tau'$   $\alpha$ -non-contractible:  
Let  $\rho' = \rho[\alpha \mapsto (\tau_1, \tau_2, R_{\sqsupset_b W})]$ . Then we have

$$\begin{aligned} \mathcal{V}[\exists\beta. \tau']\rho'(W) \\ \subseteq \{ (W, \mathbf{v}_1, v_2) \mid \exists (\tau'_1, \tau'_2, R') \in \text{TyValRel}. \exists (\mathbf{u}_1, u_2) \in \mathcal{V}[\tau']\rho'[\beta \mapsto (\tau'_1, \tau'_2, R')](W) \} \end{aligned}$$

As  $\beta \neq \alpha$ , by induction hypothesis, for all  $(\tau'_1, \tau'_2, R') \in \text{TyValRel}$  we have

$$\mathcal{V}[\tau']\rho'[\beta \mapsto (\tau'_1, \tau'_2, R')](W) = \mathcal{V}[\tau']\rho[\beta \mapsto (\tau'_1, \tau'_2, R')][\alpha \mapsto (\tau_1, \tau_2, R_{\sqsupset_b W})](W) = \emptyset.$$

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

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

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

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

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

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

□

**Theorem 3.**

$$\begin{aligned} \forall \alpha, \tau, \rho. \text{ftv}(\mu\alpha. \tau) \subseteq \text{dom } \rho \\ \implies \mathcal{V}[\mu\alpha. \tau]\rho = F_{\alpha, \tau, \rho}(\mathcal{V}[\mu\alpha. \tau]\rho) \end{aligned}$$

*Proof.*

When  $\tau$   $\alpha$ -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  $\tau$ , one can show that for all  $\alpha, \tau$  such that  $\tau$   $\alpha$ -contractive, all free occurrences of  $\alpha$  in  $\tau$  are under one of the type constructors  $\times, \rightarrow, \forall, \text{ref}$ .
- For any  $\tau_1, \tau_2, \beta, \tau', \rho, W$ , the relations  $\mathcal{V}[\tau_1 \times \tau_2]\rho(W)$ ,  $\mathcal{V}[\tau_1 \rightarrow \tau_2]\rho(W)$ ,  $\mathcal{V}[\forall\beta. \tau']\rho(W)$ ,  $\mathcal{V}[\text{ref } \tau_1]\rho(W)$  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  $W' \sqsupset_b W$ .

- 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  $\tau$   $\alpha$ -non-contractive

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

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

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

□

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

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

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

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

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

□

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

*Proof.* By structural induction on  $\tau$ :

- For  $\tau = \alpha, \tau = b$ :  
 $\mathcal{V}[\![\tau]\!] \rho$  is monotone, as all relations appearing in the definition are monotone.
- For  $\tau = \tau_1 \rightarrow \tau_2, \tau = \forall \alpha. \tau', \tau = \text{ref } \tau'$ :  
 $\mathcal{V}[\![\tau]\!] \rho$  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

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

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

*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  $\tau$ . The only non-trivial case is when  $\tau = \alpha$ . In this case, we need to show that

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

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

## 4 Possible Worlds

### 4.1 Definitions

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

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

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

$$\begin{aligned} \text{MemRel}_n &\stackrel{\text{def}}{=} \mathbb{P}(\text{World}_n \times \mathcal{L}_1.\text{Mem} \times \mathcal{L}_2.\text{Mem}) \\ R \text{ monotone} &\stackrel{\text{def}}{=} \forall (W, \mathbf{M}_1, M_2) \in R. \forall W' \supseteq W. (W', \mathbf{M}_1, M_2) \in R \\ &\text{for } R \in \text{MemRel}_n \\ \text{Island}_n &\stackrel{\text{def}}{=} \{ \iota = (s, S, \delta, \varphi, MR, Bij) \mid \\ &\quad s \in S \wedge S \in \text{Set} \wedge \delta, \varphi \in \mathbb{P}(S \times S) \wedge \\ &\quad MR \in S \rightarrow \text{MemRel}_n \wedge Bij \in S \rightarrow \mathbb{P}(\mathcal{L}_1.\text{Val} \times \mathcal{L}_2.\text{Val}) \wedge \\ &\quad \varphi \subseteq \delta \wedge \varphi, \delta \text{ are preorders} \wedge \\ &\quad \forall s. MR(s) \text{ monotone} \wedge \\ &\quad \forall s. \forall (W, \mathbf{M}_1, M_2) \in MR(s). Bij(s) \text{ pbijjective} \wedge \\ &\quad \text{dom}_1(Bij(s)) \subseteq \mathcal{L}_1.\text{mdom}(\mathbf{M}_1) \wedge \text{dom}_2(Bij(s)) \subseteq \mathcal{L}_2.\text{mdom}(M_2) \} \\ \text{World}_n &\stackrel{\text{def}}{=} \{ W = (k, \omega, GR) \mid k < n \wedge \exists m. \omega \in \text{Island}_k^m \wedge GR \in \mathbb{P}(\mathcal{L}_1.\text{Mem} \times \mathcal{L}_2.\text{Mem}) \} \\ \text{World} &\stackrel{\text{def}}{=} \bigcup_{n \in \mathbb{N}} \text{World}_n \\ \text{lev}(W) &\stackrel{\text{def}}{=} W.k \\ \lfloor \iota_1, \dots, \iota_m \rfloor_k &\stackrel{\text{def}}{=} (\lfloor \iota_1 \rfloor_k, \dots, \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 \text{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) \\ (k', \omega', GR') \supseteq (k, \omega, GR) &\stackrel{\text{def}}{=} k' \leq k \wedge \omega' \supseteq \lfloor \omega \rfloor_{k'} \wedge GR' = GR \\ (\iota'_1, \dots, \iota'_{m'}) \supseteq (\iota_1, \dots, \iota_m) &\stackrel{\text{def}}{=} m' \geq m \wedge \forall j \in \{1 \dots m\}. \iota'_j \supseteq \iota_j \\ (s', S', \delta', \varphi', MR', Bij') \supseteq (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') \supseteq_{\text{pub}} (k, \omega, GR) &\stackrel{\text{def}}{=} k' \leq k \wedge \omega' \supseteq_{\text{pub}} \lfloor \omega \rfloor_{k'} \wedge GR' = GR \\ (\iota'_1, \dots, \iota'_{m'}) \supseteq_{\text{pub}} (\iota_1, \dots, \iota_m) &\stackrel{\text{def}}{=} m' \geq m \wedge \forall j \in \{1 \dots m\}. \iota'_j \supseteq_{\text{pub}} \iota_j \\ (s', S', \delta', \varphi', MR', Bij') \supseteq_{\text{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}$$

$$\begin{aligned}
\mathcal{M}(W) &\stackrel{\text{def}}{=} \{ (\mathbf{M}_1, M_2) \mid \text{lev}(W) > 0 \implies \exists \mathbf{M}_1^1, \dots, \mathbf{M}_1^{|\mathcal{W}^\omega|}, M_2^1, \dots, M_2^{|\mathcal{W}^\omega|}. \\
&\quad \mathbf{M}_1 \in \mathcal{L}_1.\text{mdisjlist}(\mathbf{M}_1^1, \dots, \mathbf{M}_1^{|\mathcal{W}^\omega|}) \wedge M_2 \in \mathcal{L}_2.\text{mdisjlist}(M_2^1, \dots, M_2^{|\mathcal{W}^\omega|}) \wedge \\
&\quad (\mathbf{M}_1, M_2) \in W.GR \wedge \forall j. (\triangleright W, \mathbf{M}_1^j, M_2^j) \in W.\omega(j).MR(W.\omega(j).s) \} \\
\mathcal{B}(W) &\stackrel{\text{def}}{=} \bigcup_{j \in \{1, \dots, |\mathcal{W}^\omega|\}} W.\omega(j).Bij(W.\omega(j).s) \\
\mathcal{O}(W) &\stackrel{\text{def}}{=} \{ (C_1, C_2) \mid (\exists k_1. \mathcal{L}_1.\text{obsk}(k_1, C_1) = \text{halt} \wedge \exists k_2. \mathcal{L}_2.\text{obsk}(k_2, C_2) = \text{halt}) \vee \\
&\quad (\mathcal{L}_1.\text{obsk}(\text{lev}(W), C_1) = \text{running} \wedge \mathcal{L}_2.\text{obsk}(\text{lev}(W), C_2) = \text{running}) \} \\
\iota[\rightsquigarrow s] &\stackrel{\text{def}}{=} (s, \iota.S, \iota.\delta, \iota.\varphi, \iota.MR, \iota.Bij) \\
W[i \rightsquigarrow s] &\stackrel{\text{def}}{=} (W.k, W.\omega[i \mapsto W.\omega(i)[\rightsquigarrow s]], W.GR) \\
W \dashv\vdash \iota &\stackrel{\text{def}}{=} (W.k, W.\omega \dashv\vdash [\iota], W.GR) \\
\iota^{\text{single}}(MR, Bij) &\stackrel{\text{def}}{=} (\star, \{\star\}, \{\{\star, \star\}\}, \{\{\star, \star\}\}, \lambda \star. MR, \lambda \star. Bij)
\end{aligned}$$

## 4.2 Properties

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

*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
  - $W.\omega(j).Bij(W.\omega(j).s)$  pbijjective
  - $\text{dom}_1(W.\omega(j).Bij(W.\omega(j).s)) \subseteq \mathcal{L}_1.\text{mdom}(\mathbf{M}_1^j)$
  - $\text{dom}_2(W.\omega(j).Bij(W.\omega(j).s)) \subseteq \mathcal{L}_2.\text{mdom}(M_2^j)$
- As  $\mathbf{M}_1 \in \mathcal{L}_1.\text{mdisjlist}(\mathbf{M}_1^1, \dots, \mathbf{M}_1^{|\mathcal{W}^\omega|})$  and  $M_2 \in \mathcal{L}_2.\text{mdisjlist}(M_2^1, \dots, M_2^{|\mathcal{W}^\omega|})$ , by assumptions on  $\mathcal{L}_1.\text{mdisj}$  and  $\mathcal{L}_2.\text{mdisj}$ , we have that  $\mathcal{L}_1.\text{mdom}(\mathbf{M}_1^j) \cap \mathcal{L}_1.\text{mdom}(\mathbf{M}_1^{j'}) = \emptyset$  and  $\mathcal{L}_2.\text{mdom}(M_2^j) \cap \mathcal{L}_2.\text{mdom}(M_2^{j'}) = \emptyset$  for all  $j \neq j'$ .
- Therefore,  $\mathcal{B}(W) = \bigcup_{j \in \{1, \dots, |\mathcal{W}^\omega|\}} W.\omega(j).Bij(W.\omega(j).s)$  is also a partial bijection.

□

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

$$\begin{aligned}
&\forall k_1, C_1, C'_1, k_2, C_2, C'_2, W, W'. \\
&C_1 \xrightarrow{k_1} C'_1 \wedge C_2 \xrightarrow{k_2} C'_2 \wedge (C'_1, C'_2) \in \mathcal{O}(W') \wedge \text{lev}(W) \leq \text{lev}(W') + \min(k_1, k_2) \\
&\implies (C_1, C_2) \in \mathcal{O}(W)
\end{aligned}$$

*Proof.* If  $C'_1$  and  $C'_2$  halt, then  $C_1$  and  $C_2$  halt. If  $C'_1$  and  $C'_2$  take at least  $\text{lev}(W')$  steps, then  $C_1$  and  $C_2$  take at least  $(\text{lev}(W') + \min(k_1, k_2))$  steps. □

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

*Proof.* We need to prove the following.

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



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

These are all simple consequences of definition. □

## 5 Specification of HIGH

### 5.1 LangSpec of HIGH

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

**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

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

$$|\mathbf{v}| \stackrel{\text{def}}{=} \begin{cases} w & \text{if } \mathbf{v} = \underline{w} \\ \mathbf{l} & \text{if } \mathbf{v} = \widehat{\mathbf{l}} \end{cases}$$

$$\mathbf{M}(\mathbf{v}) \stackrel{\text{def}}{=} \mathbf{v}$$

$$\mathbf{M}(\lfloor r \rfloor) \stackrel{\text{def}}{=} \mathbf{M}.\text{reg}(r)$$

$$\mathbf{M}(\langle a \rangle_s) \stackrel{\text{def}}{=} \mathbf{M}.\text{stk}(a)$$

$$\mathbf{M}(\langle r - o \rangle_s) \stackrel{\text{def}}{=} \mathbf{M}.\text{stk}(|\mathbf{M}.\text{reg}(r)| - o)$$

$$\mathbf{M}(\langle \mathbf{l} : o \rangle_h) \stackrel{\text{def}}{=} \mathbf{M}.\text{hp}(\mathbf{l})(o)$$

$$\mathbf{M}(\langle r + o \rangle_h) \stackrel{\text{def}}{=} \mathbf{M}.\text{hp}(|\mathbf{M}.\text{reg}(r)|)(o)$$

$$\mathbf{M}[a \mapsto \iota_1, \dots, \iota_n]_{\text{code}} \stackrel{\text{def}}{=} (\mathbf{M}.\text{code}[a \mapsto \iota_1, \dots, \iota_n], \mathbf{M}.\text{reg}, \mathbf{M}.\text{stk}, \mathbf{M}.\text{hp}, \mathbf{M}.\text{tab}, \mathbf{M}.\text{shp})$$

$$\mathbf{M}[r \mapsto \mathbf{v}]_{\text{reg}} \stackrel{\text{def}}{=} (\mathbf{M}.\text{code}, \mathbf{M}.\text{reg}[r \mapsto \mathbf{v}], \mathbf{M}.\text{stk}, \mathbf{M}.\text{hp}, \mathbf{M}.\text{tab}, \mathbf{M}.\text{shp})$$

$$\mathbf{M}[++ \mathbf{v}_0, \dots, \mathbf{v}_{j-1}]_{\text{stk}} \stackrel{\text{def}}{=} (\mathbf{M}.\text{code}, \mathbf{M}.\text{reg}, \mathbf{M}.\text{stk} ++ (\mathbf{v}_0, \dots, \mathbf{v}_{j-1}), \mathbf{M}.\text{hp}, \mathbf{M}.\text{tab}, \mathbf{M}.\text{shp})$$

$$\mathbf{M}[-k]_{\text{stk}} \stackrel{\text{def}}{=} (\mathbf{M}.\text{code}, \mathbf{M}.\text{reg}, (\mathbf{v}_0, \dots, \mathbf{v}_{n-k-1}), \mathbf{M}.\text{hp}, \mathbf{M}.\text{tab}, \mathbf{M}.\text{shp})$$

if  $\mathbf{M}.\text{stk} = (\mathbf{v}_0, \dots, \mathbf{v}_{n-1}) \wedge n \geq k$

$$\mathbf{M}[j \mapsto \mathbf{v}]_{\text{stk}} \stackrel{\text{def}}{=} (\mathbf{M}.\text{code}, \mathbf{M}.\text{reg}, \mathbf{M}.\text{stk}[j \mapsto \mathbf{v}], \mathbf{M}.\text{hp}, \mathbf{M}.\text{tab}, \mathbf{M}.\text{shp}) \quad \text{if } j < |\mathbf{M}.\text{stk}|$$

$$\mathbf{M}[\mathbf{l} : o \mapsto \mathbf{v}]_{\text{hp}} \stackrel{\text{def}}{=} (\mathbf{M}.\text{code}, \mathbf{M}.\text{reg}, \mathbf{M}.\text{stk}, \mathbf{M}.\text{hp}[\mathbf{l} \mapsto (\mathbf{v}_0, \dots, \mathbf{v}_{o-1}, \mathbf{v}, \mathbf{v}_{o+1}, \dots, \mathbf{v}_{n-1})],$$

$\mathbf{M}.\text{tab}, \mathbf{M}.\text{shp}$ )

if  $\mathbf{M}.\text{hp}(\mathbf{l}) = (\mathbf{v}_0, \dots, \mathbf{v}_{n-1}) \wedge o < n$

$$\mathbf{M}[[T, S]] \stackrel{\text{def}}{=} (\mathbf{M}.\text{code}, \mathbf{M}.\text{reg}, \mathbf{M}.\text{stk}, \mathbf{M}.\text{hp}, T, S)$$

$$\begin{aligned}
\text{phyv}(\mathbf{M})(\mathbf{v}) &\stackrel{\text{def}}{=} \begin{cases} w & \text{if } \mathbf{v} = w \\ \widehat{a} & \text{if } \mathbf{v} = \widehat{\mathbf{l}} \wedge \mathbf{M}.\text{tab}(\mathbf{l}) = (n, a) \\ \text{undef} & \text{otherwise} \end{cases} \\
\text{phyh}(\mathbf{M}) &\stackrel{\text{def}}{=} \bigsqcup_{\substack{\mathbf{M}.\text{tab}(\mathbf{l})=(n,a) \wedge n>0 \\ \wedge \mathbf{M}.\text{hp}(\mathbf{l})=(\mathbf{v}_0, \dots, \mathbf{v}_{n-1})}} [a \mapsto \text{phyv}(\mathbf{M})(\mathbf{v}_0), \dots, \text{phyv}(\mathbf{M})(\mathbf{v}_{n-1})] \\
\mathbf{M} \text{ repr } \Phi &\stackrel{\text{def}}{=} \Phi.\text{code} \supseteq \mathbf{M}.\text{code} \wedge \\
&\Phi.\text{reg} \supseteq \text{phyv}(\mathbf{M}) \circ \mathbf{M}.\text{reg} \wedge \Phi.\text{reg}(\text{sp}) = |\mathbf{M}.\text{stk}| \wedge \\
&\forall j < |\mathbf{M}.\text{stk}|. \Phi.\text{stk}(j) = \text{phyv}(\mathbf{M})(\mathbf{M}.\text{stk}(j)) \wedge \\
&\Phi.\text{hp} \supseteq \text{phyh}(\mathbf{M}) \uplus \mathbf{M}.\text{shp} \wedge \\
&\forall \mathbf{l}, n, a. \mathbf{M}.\text{tab}(\mathbf{l}) = (n, a) \wedge n > 0 \implies |\mathbf{M}.\text{hp}(\mathbf{l})| = n \\
\text{plugv}(\mathbf{v}, \mathbf{K}, \mathbf{M}) &\stackrel{\text{def}}{=} \{ (\Phi, \text{pc}) \in \text{Conf} \mid \mathbf{M} \text{ repr } \Phi \wedge \\
&\text{pc} = \mathbf{K}.\text{kpc} \wedge \mathbf{M}(\mathbf{K}.\text{vloc}) = \mathbf{v} \} \\
\text{plugc}(\mathbf{e}, \mathbf{K}, \mathbf{M}) &\stackrel{\text{def}}{=} \{ (\Phi, \text{pc}) \in \text{Conf} \mid \mathbf{M} \text{ repr } \Phi \wedge \mathbf{M} \in \mathbf{e}.\text{data} \wedge \\
&\text{pc} = \mathbf{M}(\mathbf{e}.\text{cpc}) \wedge \mathbf{M}(\mathbf{e}.\text{kpc}) = \mathbf{K}.\text{kpc} \wedge \mathbf{e}.\text{vloc} = \mathbf{K}.\text{vloc} \} \\
\text{step}(\Phi, \text{pc}) &\stackrel{\text{def}}{=} R \quad \text{with } (\Phi, \text{pc}) \leftrightarrow R \\
\text{mdom}(\mathbf{M}) &\stackrel{\text{def}}{=} \{ \widehat{\mathbf{l}} \in \text{Val} \mid \mathbf{l} \in \text{dom}(\mathbf{M}.\text{hp}) \} \\
\text{mdisj}(\mathbf{M}_1, \mathbf{M}_2) &\stackrel{\text{def}}{=} \{ \mathbf{M} \in \text{Mem} \mid \\
&\mathbf{M}.\text{code} \supseteq \mathbf{M}_1.\text{code} \uplus \mathbf{M}_2.\text{code} \wedge \\
&\mathbf{M}.\text{hp} \supseteq \mathbf{M}_1.\text{hp} \uplus \mathbf{M}_2.\text{hp} \wedge \\
&\text{nosh}(\mathbf{M}.\text{reg}, \mathbf{M}_1.\text{reg}, \mathbf{M}_2.\text{reg}) \wedge \\
&\text{nosh}(\mathbf{M}.\text{stk}, \mathbf{M}_1.\text{stk}, \mathbf{M}_2.\text{stk}) \wedge \\
&\text{nosh}(\mathbf{M}.\text{tab}, \mathbf{M}_1.\text{tab}, \mathbf{M}_2.\text{tab}) \wedge \\
&\text{nosh}(\mathbf{M}.\text{shp}, \mathbf{M}_1.\text{shp}, \mathbf{M}_2.\text{shp}) \} \\
\text{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) \\
\mathbf{M}_1 \uplus \mathbf{M}_2 &\stackrel{\text{def}}{=} \begin{cases} (\mathbf{M}_1.\text{code} \uplus \mathbf{M}_2.\text{code}, \mathbf{M}_i.\text{reg}, \mathbf{M}_j.\text{stk}, \mathbf{M}_1.\text{hp} \uplus \mathbf{M}_2.\text{hp}, \mathbf{M}_k.\text{tab}, \mathbf{M}_l.\text{shp}) \\ \text{if } \mathbf{M}_1.\text{code} \uplus \mathbf{M}_2.\text{code} \neq \text{undef} \wedge \mathbf{M}_1.\text{hp} \uplus \mathbf{M}_2.\text{hp} \neq \text{undef} \wedge \\ \mathbf{M}_{3-i}.\text{reg} = \text{undef} \wedge \mathbf{M}_{3-j}.\text{stk} = \text{undef} \wedge \\ \mathbf{M}_{3-k}.\text{tab} = \text{undef} \wedge \mathbf{M}_{3-l}.\text{shp} = \text{undef} \\ \text{undef} \quad \text{otherwise} \end{cases} \\
\mathbf{M}_1 \supseteq \mathbf{M}_2 &\stackrel{\text{def}}{=} \mathbf{M}_1.\text{code} \supseteq \mathbf{M}_2.\text{code} \wedge \\
&\mathbf{M}_1.\text{hp} \supseteq \mathbf{M}_2.\text{hp} \wedge \\
&(\mathbf{M}_2.\text{reg} \neq \text{undef} \implies \mathbf{M}_1.\text{reg} = \mathbf{M}_2.\text{reg}) \wedge \\
&(\mathbf{M}_2.\text{stk} \neq \text{undef} \implies \mathbf{M}_1.\text{stk} = \mathbf{M}_2.\text{stk}) \wedge \\
&(\mathbf{M}_2.\text{tab} \neq \text{undef} \implies \mathbf{M}_1.\text{tab} = \mathbf{M}_2.\text{tab}) \wedge \\
&(\mathbf{M}_2.\text{shp} \neq \text{undef} \implies \mathbf{M}_1.\text{shp} = \mathbf{M}_2.\text{shp})
\end{aligned}$$

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

**Notation.**

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

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

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

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

**Theorem 12.**

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

*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. □

## 6.2 Garbage Collector Specification

$$\begin{aligned}
\mathbf{v} \text{ live in } \mathbf{M} &\stackrel{\text{def}}{=} \begin{cases} \top & \text{if } \mathbf{v} = \underline{w} \\ \exists n, a. \mathbf{M}.\text{tab}(\mathbf{l}) = (n, a) \wedge n > 0 & \text{if } \mathbf{v} = \widehat{\mathbf{l}} \end{cases} \\
\text{reach}_0(\mathbf{M}) &\stackrel{\text{def}}{=} \{ \mathbf{l} \mid \exists r \in \text{Register}. \widehat{\mathbf{l}} = \mathbf{M}.\text{reg}(r) \} \cup \\
&\quad \{ \mathbf{l} \mid \exists j < |\mathbf{M}.\text{stk}|. \widehat{\mathbf{l}} = \mathbf{M}.\text{stk}(j) \} \\
\text{reach}_{i+1}(\mathbf{M}) &\stackrel{\text{def}}{=} \text{reach}_i(\mathbf{M}) \cup \{ \mathbf{l} \mid \exists \mathbf{l}' \in \text{reach}_i(\mathbf{M}). \exists j. \widehat{\mathbf{l}} = \mathbf{M}.\text{hp}(\mathbf{l}')(j) \} \\
\text{reach}(\mathbf{M}) &\stackrel{\text{def}}{=} \bigcup_{i \in \mathbb{N}} \text{reach}_i(\mathbf{M}) \\
\text{AllocSpec} &\stackrel{\text{def}}{=} \{ \mathcal{A} \in \text{PAddr} \rightarrow \\
&\quad \{ (\text{init}, \text{alloc}, \text{instrs}, I) \in \text{PAddr} \times \text{PAddr} \times \text{List Instruction} \times \mathbb{P}(\text{Table} \times \text{SysHeap}) \} \mid \\
&\quad \forall \text{gcbg}, \Phi, \text{pc}. \\
&\quad \Phi.\text{code} \supseteq [\text{gcbg} \Rightarrow \mathcal{A}(\text{gcbg}).\text{instrs}] \wedge \Phi.\text{reg}(\text{wk}_4) = \underline{\text{pc}} \\
&\quad \implies \exists k, \mathbf{M}', \Phi'. \\
&\quad (\Phi, \mathcal{A}(\text{gcbg}).\text{init}) \xrightarrow{k} (\Phi', \text{pc}) \wedge \\
&\quad \mathbf{M}' \text{ repr } \Phi' \wedge \mathbf{M}' \in \mathcal{A}.\text{GR}(\text{gcbg}) \wedge \mathbf{M}' \in \mathcal{A}.\text{MR}(\text{gcbg}) \wedge \\
&\quad \Phi'.\text{code} = \Phi.\text{code} \wedge \mathbf{M}'.\text{code} = [\text{gcbg} \Rightarrow \mathcal{A}(\text{gcbg}).\text{instrs}] \wedge \\
&\quad \forall \text{gcbg}, \mathbf{M}, \Phi, \text{pc}, n. \\
&\quad \mathbf{M} \text{ repr } \Phi \wedge \mathbf{M} \in \mathcal{A}.\text{GR}(\text{gcbg}) \wedge \mathbf{M} \in \mathcal{A}.\text{MR}(\text{gcbg}) \wedge \\
&\quad \mathbf{M}.\text{reg}(\text{wk}_4) = \underline{\text{pc}} \wedge \mathbf{M}.\text{reg}(\text{wk}_5) = \underline{n} \\
&\quad \implies \exists k, \Phi', \mathbf{M}', T, S, w, \mathbf{l}, w_0, \dots, w_{n-1}. \\
&\quad (\Phi, \mathcal{A}(\text{gcbg}).\text{alloc}) \xrightarrow{k} (\Phi', \text{pc}) \wedge \\
&\quad \mathbf{M}' \text{ repr } \Phi' \wedge \mathbf{M}' \in \mathcal{A}.\text{GR}(\text{gcbg}) \wedge \mathbf{M}' \in \mathcal{A}.\text{MR}(\text{gcbg}) \wedge \\
&\quad \mathbf{M}' = \mathbf{M}[[T, S]][\text{wk}_4 \mapsto \underline{w}]_{\text{reg}}[\text{wk}_5 \mapsto \widehat{\mathbf{l}}]_{\text{reg}} \uplus \{ \mathbf{l} \mapsto (\underline{w}_0, \dots, \underline{w}_{n-1}) \}_{\text{heap}} \} \\
\mathcal{A}.\text{GR}(\text{gcbg}) &\stackrel{\text{def}}{=} \{ \mathbf{M} \in \text{Mem} \mid \forall \mathbf{l} \in \text{reach}(\mathbf{M}). \widehat{\mathbf{l}} \text{ live in } \mathbf{M} \} \\
\mathcal{A}.\text{MR}(\text{gcbg}) &\stackrel{\text{def}}{=} \{ \mathbf{M} \in \text{Mem} \mid (\mathbf{M}.\text{tab}, \mathbf{M}.\text{shp}) \in \mathcal{A}(\text{gcbg}).I \wedge \\
&\quad \mathbf{M}.\text{code} \supseteq [\text{gcbg} \Rightarrow \mathcal{A}(\text{gcbg}).\text{instrs}] \}
\end{aligned}$$

## 7 Low High Relations

### 7.1 Initial Worlds

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

$$\begin{aligned}
W_k^\circ(\mathcal{A}, \text{gcbg}) &\stackrel{\text{def}}{=} (k, [\iota^{\text{regstk}}, \iota^{\text{htyping}}, \iota^{\text{gc}}(\mathcal{A}, \text{gcbg})], GR^\circ(\mathcal{A}, \text{gcbg})) \\
S_{\text{regstk}} &\stackrel{\text{def}}{=} \{s = (\text{reg}, \text{stk}) \in (\{\text{sv}_0, \dots, \text{sv}_4\} \rightarrow \text{Val}) \times \text{List Val}\} \\
\delta_{\text{regstk}} &\stackrel{\text{def}}{=} \{(s, s') \in S_{\text{regstk}} \times S_{\text{regstk}}\} \\
\varphi_{\text{regstk}} &\stackrel{\text{def}}{=} \{(s, s') \in S_{\text{regstk}} \times S_{\text{regstk}} \mid s' = s\} \\
MR_{\text{regstk}}(s) &\stackrel{\text{def}}{=} \{(W, \mathbf{M}, M) \mid \mathbf{M}.\text{stk} = s.\text{stk} \wedge \forall j. \mathbf{M}.\text{reg}(\text{sv}_j) = s.\text{reg}(\text{sv}_j)\} \\
\iota^{\text{regstk}} &\stackrel{\text{def}}{=} ((\lambda r. \underline{0}, []), S_{\text{regstk}}, \delta_{\text{regstk}}, \varphi_{\text{regstk}}, MR_{\text{regstk}}, \lambda s. \emptyset) \\
\\
S_{\text{htyping}} &\stackrel{\text{def}}{=} \{\Sigma \in \text{Heap typings}\} \\
\delta_{\text{htyping}} &\stackrel{\text{def}}{=} \{(\Sigma, \Sigma') \mid \Sigma \subseteq \Sigma'\} \\
\varphi_{\text{htyping}} &\stackrel{\text{def}}{=} \delta_{\text{htyping}} \\
MR_{\text{htyping}}(\Sigma) &\stackrel{\text{def}}{=} \{(W, \mathbf{M}, M) \mid M.\Sigma = \Sigma\} \\
\iota^{\text{htyping}} &\stackrel{\text{def}}{=} (\emptyset, S_{\text{htyping}}, \delta_{\text{htyping}}, \varphi_{\text{htyping}}, MR_{\text{htyping}}, \lambda \Sigma. \emptyset) \\
\\
\iota^{\text{gc}}(\mathcal{A}, \text{gcbg}) &\stackrel{\text{def}}{=} \iota^{\text{single}}(\{(W, \mathbf{M}, M) \mid \mathbf{M} \in \mathcal{A}.MR(\text{gcbg})\}, \emptyset) \\
\\
GR^\circ(\mathcal{A}, \text{gcbg}) &\stackrel{\text{def}}{=} \{(\mathbf{M}, M) \mid \mathbf{M} \in \mathcal{A}.GR(\text{gcbg}) \wedge \vdash M.h : M.\Sigma\}
\end{aligned}$$

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

### 7.2 Program Equivalence

$$\begin{aligned}
\mathcal{L}.\text{Prog} &\stackrel{\text{def}}{=} \{p \in \text{PAddr} \times \text{PAddr} \rightarrow \text{List Instruction}\} \\
\mathcal{H}.\text{Prog} &\stackrel{\text{def}}{=} \{e \in \text{HExp} \mid \text{floc}(e) = \emptyset\} \\
\\
\mathcal{G}[\cdot]\rho &\stackrel{\text{def}}{=} \{(W, \mathbf{v}, \emptyset) \mid W \in \text{World} \wedge \mathbf{v} \in \mathcal{L}.\text{Val}\} \\
\mathcal{G}[\Gamma, x : \tau]\rho &\stackrel{\text{def}}{=} \{(W, \mathbf{v}, (\gamma, x \mapsto v)) \mid \exists \mathbf{v}_1, \mathbf{v}_2. \\
&\quad (W, \mathbf{v}, \langle \rangle) \in \square(\mathcal{L}.\text{pair}(\mathbf{v}_1, \mathbf{v}_2), \mathcal{H}.\text{Val} \times \mathcal{H}.\text{Mem}) \wedge \\
&\quad (W, \mathbf{v}_1, v) \in \mathcal{V}[\tau]\rho \wedge (W, \mathbf{v}_2, \gamma) \in \mathcal{G}[\Gamma]\rho\} \\
\\
\mathcal{D}[\cdot] &\stackrel{\text{def}}{=} \emptyset \\
\mathcal{D}[\Delta, \alpha] &\stackrel{\text{def}}{=} \{(\rho, \alpha \mapsto R) \mid \rho \in \mathcal{D}[\Delta] \wedge R \in \text{TyValRel}\}
\end{aligned}$$

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

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

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

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

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

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

*Proof.* By an easy structural induction on  $\Gamma$ . □

### 7.3 Adequacy and Compositionality

$$\begin{aligned} \text{load}(\mathcal{A}, p) &::= \\ \text{let } (\text{init}, \text{alloc}, \text{gcinstrs}, \_) &:= \mathcal{A}(105), \\ \text{instrs}^p &:= p(\text{alloc}, 105 + |\text{gcinstrs}|), \\ \text{loadinstrs}^p &:= [ \\ &(* 100 *) \quad \text{move} \quad \lfloor \text{wk}_4 \rfloor \quad \underline{102} \\ &\quad \quad \quad \text{jmp} \quad \underline{\text{init}} \\ &(* 102 *) \quad \text{move} \quad \lfloor \text{wk}_0 \rfloor \quad \underline{104} \\ &\quad \quad \quad \text{jmp} \quad \underline{105 + |\text{gcinstrs}|} \\ &(* 104 *) \quad \text{halt} \\ &\quad \quad \quad \text{gcinstrs} \\ &\quad \quad \quad \text{instrs}^p \\ &] \text{ in} \\ &\{ (\Phi, 100) \in \text{PConf} \mid \Phi.\text{code} \supseteq [100 \Rightarrow \text{loadinstrs}^p] \} \end{aligned}$$

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

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

*Proof.*

Let  $(\text{init}, \text{alloc}, \text{gcinstrs}, \_) = \mathcal{A}(105)$ .

Let  $\text{code} := [100 \Rightarrow \text{loadinstrs}^p]$ .

Let  $\text{code}^{\text{gc}} := [105 \Rightarrow \text{gcinstrs}]$ .

Let  $\text{code}^p := [105 + |\text{gcinstrs}| \Rightarrow p(\text{alloc}, 105 + |\text{gcinstrs}|)]$ .

Let  $\text{code}^{\bullet} := \text{code} \setminus \text{code}^{\text{gc}} \setminus \text{code}^p$ .



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

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

such that

$$- \Phi^1 = \Phi[[\text{wk}_4] \mapsto \underline{102}]$$

- 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  $\Phi^2$ ,
- $\Phi^2.code = \Phi.code$ ,
- $\mathbf{M}^2.code = code^{sc}$ ,
- $M^2 := (h, \emptyset)$

- Let  $\mathbf{M}^3 := \mathbf{M}^2 \uplus \{code^\bullet\}_{code}$ .  
Still,  $\mathbf{M}^3$  repr  $\Phi^2$ .
- Let  $W_k^3 := W_k^\circ(\text{gcbg})[1 \rightsquigarrow (\mathbf{M}^3.reg|_{sv_0 \dots sv_4}, \mathbf{M}^3.stk)] \uplus \iota^{code}(code^\bullet)$ .  
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  $\mathbf{M}^4 := \mathbf{M}^3 \uplus \{code^p\}_{code}$ .  
Still,  $\mathbf{M}^4$  repr  $\Phi^2$ .  
From  $p \approx_\tau e$ , we have  $W^4$  such that
  - $W^4 \supseteq W_k^3 \wedge \text{lev}(W^4) = \text{lev}(W_k^3) = k$
  - $(\mathbf{M}^4, M^2) \in \mathcal{M}(W^4)$
  - (\*)  $\forall W' \supseteq W^4. \forall \mathbf{v}. ((105 + |\text{gcinstrs}|, [\text{wk}_0], [\text{wk}_5], \{\mathbf{M} \mid \mathbf{M}.reg(sv_0) = \mathbf{v}\}), e) \in \mathcal{E}[\tau]\emptyset(W')$ .

- 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

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

such that

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

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

- By (\*), it suffices to show that  $((104, [\text{wk}_5]), [-]) \in \mathcal{K}[\tau]\emptyset(W^4)$ , 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

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

	bg	move	[wk <sub>4</sub> ]	<u>bg + 3</u>	
		move	[wk <sub>5</sub> ]	<u>1</u>	
		jmp	alloc		
bg + 3		move	$\langle \text{wk}_5 + 0 \rangle_{\text{h}}$	<u>bg + 5</u>	
		jmp	[wk <sub>0</sub> ]		
bg + 5		move	[wk <sub>3</sub> ]	<u>bg + 10</u>	
bg + 6		isr	[wk <sub>4</sub> ]	[wk <sub>3</sub> ]	
		minus	[wk <sub>4</sub> ]	[wk <sub>4</sub> ]	<u>666</u>
		isw	[wk <sub>3</sub> ]	[wk <sub>4</sub> ]	
		plus	[wk <sub>3</sub> ]	[wk <sub>3</sub> ]	<u>1</u>
bg + 10		$\mathbb{D}(\mathbb{E}(\text{jneq}$	bg + 6	[wk <sub>3</sub> ]	<u>bg + 21</u> ) + 666)
bg + 11		$\mathbb{D}(\mathbb{E}(\text{isw}$	<u>bg + 5</u>	$\mathbb{E}(\text{jmp } \text{bg} + 12)$	) + 666)
bg + 12		$\mathbb{D}(\mathbb{E}(\text{move}$	$\langle \text{wk}_1 + 0 \rangle_{\text{h}}$	<u>bg + 13</u>	) + 666)
bg + 13		$\mathbb{D}(\mathbb{E}(\text{plus}$	[sp]	[sp]	<u>1</u> ) + 666)
		$\mathbb{D}(\mathbb{E}(\text{move}$	$\langle \text{sp} - 1 \rangle_{\text{s}}$	[wk <sub>0</sub> ]	) + 666)
		$\mathbb{D}(\mathbb{E}(\text{move}$	[wk <sub>1</sub> ]	[wk <sub>2</sub> ]	) + 666)
		$\mathbb{D}(\mathbb{E}(\text{move}$	[wk <sub>0</sub> ]	<u>bg + 18</u>	) + 666)
		$\mathbb{D}(\mathbb{E}(\text{jmp}$	$\langle \text{wk}_1 + 0 \rangle_{\text{h}}$		) + 666)
bg + 18		$\mathbb{D}(\mathbb{E}(\text{move}$	[wk <sub>5</sub> ]	<u>1</u>	) + 666)
		$\mathbb{D}(\mathbb{E}(\text{minus}$	[sp]	[sp]	<u>1</u> ) + 666)
bg + 20		$\mathbb{D}(\mathbb{E}(\text{jmp}$	$\langle \text{sp} - 0 \rangle_{\text{s}}$		) + 666)

]

### 8.2 Properties

**Theorem 16.**  $\Delta; \Gamma \vdash p \approx e : (\text{unit} \rightarrow \text{unit}) \rightarrow \text{int}$

*Proof.*

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

- plaininstrs<sup>p</sup> := [

	bg	move	[wk <sub>4</sub> ]	<u>bg + 3</u>	
		move	[wk <sub>5</sub> ]	<u>1</u>	
		jmp	alloc		
bg + 3	move		⟨wk <sub>5</sub> + 0⟩ <sub>h</sub>	<u>bg + 5</u>	
	jmp		[wk <sub>0</sub> ]		
bg + 5	jmp		<u>bg + 12</u>		
bg + 6	isr		[wk <sub>4</sub> ]	[wk <sub>3</sub> ]	
	minus		[wk <sub>4</sub> ]	[wk <sub>4</sub> ]	<u>666</u>
	isw		[wk <sub>3</sub> ]	[wk <sub>4</sub> ]	
	plus		[wk <sub>3</sub> ]	[wk <sub>3</sub> ]	<u>1</u>
bg + 10	jneq		bg + 6	[wk <sub>3</sub> ]	<u>bg + 21</u>
bg + 11	isw		<u>bg + 5</u>	$\mathbb{E}(\text{jmp } \text{bg} + 12)$	
bg + 12	move		⟨wk <sub>1</sub> + 0⟩ <sub>h</sub>	<u>bg + 13</u>	
bg + 13	plus		[sp]	[sp]	<u>1</u>
	move		⟨sp - 1⟩ <sub>s</sub>	[wk <sub>0</sub> ]	
	move		[wk <sub>1</sub> ]	[wk <sub>2</sub> ]	
	move		[wk <sub>0</sub> ]	<u>bg + 18</u>	
	jmp		⟨wk <sub>1</sub> + 0⟩ <sub>h</sub>		
bg + 18	move		[wk <sub>5</sub> ]	<u>1</u>	
	minus		[sp]	[sp]	<u>1</u>
bg + 20	jmp		⟨sp - 0⟩ <sub>s</sub>		

]

- plaincode<sup>p</sup> := [bg ⇒ plaininstrs<sup>p</sup>]

- Goal: find  $W^{pe}$  such that
  - $W^{pe} \sqsupseteq W \wedge \text{lev}(W^{pe}) = \text{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta; \Gamma \vdash \text{bg} \approx_{W^{pe}} e : (\text{unit} \rightarrow \text{unit}) \rightarrow \text{int}$
- Let  $S^p := \{\text{enc}, \text{dec}\}$ .  
 Let  $\delta^p := \{(\text{enc}, \text{dec})\}^*$ .  
 Let  $\varphi^p := \delta^p$ .  
 Let  $MR^p(\text{enc}) := \{(W, \mathbf{M}, M) \mid \mathbf{M}.\text{code} \sqsupseteq \text{code}^p\}$ .  
 Let  $MR^p(\text{dec}) := \{(W, \mathbf{M}, M) \mid \mathbf{M}.\text{code} \sqsupseteq \text{plaincode}^p\}$ .  
 Let  $\iota_{\text{enc}}^p := (\text{enc}, S^p, \delta^p, \varphi^p, MR^p, \lambda s. \emptyset)$ .  
 Let  $\iota_{\text{dec}}^p := (\text{dec}, S^p, \delta^p, \varphi^p, MR^p, \lambda s. \emptyset)$ .
- Choose  $W^{pe} ::= W \# \iota_{\text{enc}}^p$  and let  $i^p$  be the index of  $\iota_{\text{enc}}^p$  in  $W^{pe}.\omega$ , i.e.,  $W^{pe}.\omega(i^p) = \iota_{\text{enc}}^p$ .
- $W^{pe} \sqsupseteq W \wedge \text{lev}(W^{pe}) = \text{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$  holds trivially.
- To show:  $\forall W^1 \sqsupseteq W^{pe}. \forall \rho \in \mathcal{D}[\Delta]. \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\Gamma]\rho(W^1)$ .  
 $((\text{bg}, [\text{wk}_0], [\text{wk}_5], \{\mathbf{M} \mid \mathbf{M}.\text{reg}(\text{sv}_0) = \mathbf{v}\}), \gamma\rho e) \in \mathcal{E}[(\text{unit} \rightarrow \text{unit}) \rightarrow \text{int}]\rho(W^1)$

- By definition of  $\mathcal{E}[(\text{unit} \rightarrow \text{unit}) \rightarrow \text{int}] \rho(W^1)$  and `plugc`, we suppose
  - $((\text{kpc}, \lfloor \text{wk}_5 \rfloor), K) \in \mathcal{K}[(\text{unit} \rightarrow \text{unit}) \rightarrow \text{int}] \rho(W^1)$ ,
  - $(\mathbf{M}^1, M^1) \in \mathcal{M}(W^1)$ ,
  - $\mathbf{M}^1 \text{ repr } \Phi^1$ ,
  - $\mathbf{M}^1.\text{reg}(\text{wk}_0) = \text{kpc}$ ,
  - $\mathbf{M}^1.\text{reg}(\text{sv}_0) = \mathbf{v}$ .
- To show:  $((\Phi^1, \text{bg}), (M^1.h, K[e])) \in \mathcal{O}(W^1)$
- As  $W^1$  includes  $\iota_{\text{enc}}^p$  or  $\iota_{\text{dec}}^p$ , we execute the three instructions from `bg` on the low side and get the configurations

$$(\Phi^2, \text{alloc}), \quad (M^1.h, K[e])$$

such that

- $\mathbf{M}^2 := \mathbf{M}^1[\text{wk}_4 \mapsto \underline{\text{bg} + 3}]_{\text{reg}}[\text{wk}_5 \mapsto \underline{1}]_{\text{reg}}$ ,
- $\mathbf{M}^2 \text{ repr } \Phi^2$ .

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

$$(\Phi^3, \text{bg} + 3), \quad (M^1.h, K[e])$$

such that

- $\mathbf{M}^3 := \mathbf{M}^2[[T, S]][\text{wk}_4 \mapsto \underline{w}]_{\text{reg}}[\text{wk}_5 \mapsto \widehat{\mathbf{l}}_1]_{\text{reg}} \uplus \{[\mathbf{l}_1 \mapsto (\underline{w}_0)]\}_{\text{heap}}$  for some  $w, \mathbf{l}_1, w_0$ ,
- $\mathbf{M}^3 \in \mathcal{A}.GR(\text{gcbg}) \wedge \mathbf{M}^3 \in \mathcal{A}.MR(\text{gcbg})$ ,
- $\mathbf{M}^3 \text{ repr } \Phi^3$ .

- As  $\mathbf{M}^3.\text{code} = \mathbf{M}^2.\text{code}$ , we execute the two instructions from `bg + 3` on the low side and get

$$(\Phi^4, \text{kpc}), \quad (M^1.h, K[e])$$

such that

- $\mathbf{M}^4 := \mathbf{M}^3[\mathbf{l}_1 : 0 \mapsto \text{bg} + 5]_{\text{hp}}$
- $\mathbf{M}^4 \text{ repr } \Phi^4$ .

- Now we execute the term  $e$  on the high side and get

$$(\Phi^4, \text{kpc}), \quad (M^4.h, K[v^1])$$

such that

- $M^4 := (M^1.h \uplus [\ell_2 \mapsto 0], \{M^1.\Sigma, \ell_2 : \text{int}\})$  for some  $\ell_2$ ,
- $v^1 := \lambda f : \text{unit} \rightarrow \text{unit}. \ell_2 := 1; f \langle \rangle; !\ell_2$ .

- Let  $W^4 := W^1[+\ell_2 : \text{int}]_2 \uparrow \iota_{\text{fst}}^1$  where
  - $S^1 := \{ \text{fst}, \text{sub} \}$ ,
  - $\delta^1 := \{ (\text{fst}, \text{sub}) \}^*$ ,
  - $\varphi^1 := \delta^1$ ,
  - $MR^1(\text{fst}) := \{ (W, \mathbf{M}, M) \mid \mathbf{M}.\text{hp}(\mathbf{l}_1)(0) = \underline{\text{bg} + 5} \wedge M.h(\ell_2) = 0 \}$ ,
  - $MR^1(\text{sub}) := \{ (W, \mathbf{M}, M) \mid W.\omega(i^p).s = \text{dec} \wedge \mathbf{M}.\text{hp}(\mathbf{l}_1)(0) = \underline{\text{bg} + 13} \wedge M.h(\ell_2) = 1 \}$ ,
  - $\iota_{\text{fst}}^1 = (\text{fst}, S^1, \delta^1, \varphi^1, MR^1, \lambda s. \emptyset)$ ,
  - $\iota_{\text{sub}}^1 = (\text{sub}, S^1, \delta^1, \varphi^1, MR^1, \lambda s. \emptyset)$ ,
  - It is important to note that  $MR^1(\text{sub})$  is monotone because there is no transition out of `dec`.
  - Let  $i^1$  be the index of  $\iota_{\text{fst}}^1$  in  $W^4.\omega$ .

- Then,  $(\mathbf{M}^4, M^4) \in \mathcal{M}(W^4)$
- By Theorem 9, it suffices to show that  $((\Phi^4, \text{kpc}), (M^4.h, K[v^1])) \in \mathcal{O}(W^4)$ .
- As  $W^4 \sqsupseteq_{\text{pub}} W^1$  and  $((\text{kpc}, \lfloor \text{wk}_5 \rfloor), K) \in \mathcal{K}[\![\text{unit} \rightarrow \text{unit}] \rightarrow \text{int}]\!] \rho(W^1)$ , it suffices to show that  $(\widehat{\mathbf{l}}_1, v^1) \in \mathcal{V}[\![\text{unit} \rightarrow \text{unit}] \rightarrow \text{int}]\!] \rho(W^4)$ .
- It is easy to check that  $(\widehat{\mathbf{l}}_1, v^1) \in \text{oftype}((\text{unit} \rightarrow \text{unit}) \rightarrow \text{int}, \rho)(W^4)$ .
- Suppose
  - $W^5 \sqsupseteq_{\text{p}} W^4$ ,
  - $(\mathbf{u}_1, u_2) \in \mathcal{V}[\![\text{unit} \rightarrow \text{unit}]\!] \rho(W^5)$ .

- To show:

$$(e^5, e^5) \in \mathcal{E}[\![\text{int}]\!] \rho(W^5)$$

where

$$\begin{aligned} e^5 &:= (\langle \mathbf{l}_1 : 0 \rangle_{\text{h}}, \lfloor \text{wk}_0 \rfloor, \lfloor \text{wk}_5 \rfloor, \{ \mathbf{M} \mid \mathbf{M}.\text{reg}(\text{wk}_1) = \widehat{\mathbf{l}}_1 \wedge \mathbf{M}.\text{reg}(\text{wk}_2) = \mathbf{u}_1 \}), \\ e^5 &:= (\ell_2 := 1; u_2 \langle \rangle; !\ell_2). \end{aligned}$$

- By definition of  $\mathcal{E}[\![\text{int}]\!] \rho(W^5)$  and plugc, suppose
  - $((\text{kpc}^5, \lfloor \text{wk}_5 \rfloor), K^5) \in \mathcal{K}[\![\text{int}]\!] \rho(W^5)$
  - $(\mathbf{M}^5, M^5) \in \mathcal{M}(W^5)$
  - $\mathbf{M}^5 \text{ repr } \Phi^5$
  - $\mathbf{M}^5.\text{reg}(\text{wk}_0) = \text{kpc}^5$
  - $\mathbf{M}^5.\text{reg}(\text{wk}_1) = \widehat{\mathbf{l}}_1$
  - $\mathbf{M}^5.\text{reg}(\text{wk}_2) = \mathbf{u}_1$

- To show:

$$((\Phi^5, \mathbf{M}^5.\text{hp}(\mathbf{l}_1)(0)), (M^5.h, K^5[e^5])) \in \mathcal{O}(W^5)$$

- If  $\text{lev}(W^5) = 0$  then it holds trivially. Thus, assume that  $\text{lev}(W^5) > 0$ .
- We now prove that after taking a finite number of steps in the low side, we get the configurations

$$(\Phi^6, \text{bg} + 13) \quad (M^5.h, K^5[e^5])$$

such that

- $\mathbf{M}^6 := \mathbf{M}^5[\text{bg} \mapsto \text{plaininstrs}^p]_{\text{code}}[\mathbf{l}_1 : 0 \mapsto \text{bg} + 13]_{\text{hp}}$
- $\mathbf{M}^6 \text{ repr } \Phi^6$ .

- When  $W^5.\omega(i^p).s = \text{enc} \wedge W^5.\omega(i^1).s = \text{fst}$ :  
As  $\mathbf{M}^5.\text{code} \supseteq \text{code}^p$  and  $\mathbf{M}^5.\text{hp}(\mathbf{l}_1)(0) = \text{bg} + 5$ , it first decodes the instructions from  $\text{bg} + 10$  to  $\text{bg} + 20$ , write the instruction `jmp bg + 12` at the address  $\text{bg} + 5$  in the code memory, and write  $(\text{bg} + 13)$  at the physical address corresponding to the logical address  $\mathbf{l}_1 : 0$ . Then the pc becomes  $(\text{bg} + 13)$  and  $\mathbf{M}^6$  represents the updated physical memory.
- When  $W^5.\omega(i^p).s = \text{enc} \wedge W^5.\omega(i^1).s = \text{sub}$ :  
This case is not possible by definition of  $MR^1(\text{sub})$ .

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

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

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

such that

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

- Let  $W^6 := W^5[i^p \rightsquigarrow \text{dec}][i^1 \rightsquigarrow \text{sub}]$ .  
Then  $(\mathbf{M}^6, M^6) \in \mathcal{M}(W^6)$ .
- As  $(\mathbf{u}_1, u_2) \in \text{oftype}(\text{unit} \rightarrow \text{unit}, \rho)(W^6)$  by Theorem 5 and 4, we have
  - $\mathbf{u}_1 = \hat{\mathbf{l}}'_1$  for some  $\mathbf{l}'_1$
  - $\mathbf{M}^6.\text{hp}(\mathbf{l}'_1)(0) = \underline{w'}$  for some  $w'$
  - $u_2 = \lambda x:\text{unit}. e'$  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

$$\begin{aligned} - \mathbf{M}^7 &:= \mathbf{M}^6[+\text{kp}c^5]_{\text{stk}}[\text{wk}_1 \mapsto \mathbf{u}_1]_{\text{reg}}[\text{wk}_0 \mapsto \text{bg} + 18] \\ - \mathbf{M}^7 &\text{ repr } \Phi^7 \\ - M^7 &:= \mathbf{M}^6 \end{aligned}$$

- Let  $W^7 := \triangleright W^6[+\text{kp}c^5]_1$ .  
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  $\text{lev}(W^7) = 0$  then it holds trivially. Thus, assume that  $\text{lev}(W^7) > 0$ .
- As  $(\mathbf{u}_1, u_2) \in \mathcal{V}[\text{unit} \rightarrow \text{unit}]_\rho(W^5)$ ,  $W^7 \sqsupset W^5$  and  $(\mathbf{M}^7.\text{reg}(\text{wk}_2), \langle \rangle) \in \mathcal{V}[\text{unit}]_\rho(W^7)$ , we have

$$((\hat{\mathbf{l}}'_1 : 0)_{\text{h}}, [\text{wk}_0], [\text{wk}_5], \{ \mathbf{M} \mid \mathbf{M}.\text{reg}(\text{wk}_1) = \hat{\mathbf{l}}'_1 \wedge \mathbf{M}.\text{reg}(\text{wk}_2) = \mathbf{M}^7.\text{reg}(\text{wk}_2) \}), e'[\langle \rangle/x]) \in \mathcal{E}[\text{unit}]_\rho(W^7)$$

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

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

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

- 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

- $\mathbf{M}^9 := \mathbf{M}^8[\text{wk}_5 \mapsto \underline{1}]_{\text{reg}}[-1]_{\text{stk}}$
- $\mathbf{M}^9 \text{ repr } \Phi^9$
- $M^9 := M^8$

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

□



## 9 Compiler Correctness

### 9.1 Compiler Definition and Correctness

For  $\emptyset; \Delta; \Gamma \vdash e : \tau$ ,  
 $\langle \Gamma \vdash e \rangle \in \text{PAddr} \times \text{PAddr} \rightarrow \text{List Instruction}$

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

The compiler  $\langle \Gamma \vdash e \rangle$  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  $\emptyset; \Delta; \Gamma \vdash e : \tau$ ,

$$\Delta; \Gamma \vdash \langle \Gamma \vdash e \rangle \approx e : \tau .$$

*Proof.* By a structural induction on  $e$ : each case by the compatibility lemmas in the subsequent sections.  $\square$

### 9.2 Var

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

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

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

*Proof.*

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

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

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

such that

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

$$\begin{aligned}
& (\Gamma \vdash \langle e_1, e_2 \rangle) ::= \text{Ppair}(\langle \Gamma \vdash e_1 \rangle, \langle \Gamma \vdash e_2 \rangle) \\
& \text{Ppair}(p_1, p_2) ::= \lambda \text{ alloc, bg.} \\
& \text{let instrs}_1 := p_1(\text{alloc, bg} + 4), \quad c_1 := |\text{instrs}_1|, \\
& \quad \text{instrs}_2 := p_2(\text{alloc, bg} + c_1 + 6), \quad c_2 := |\text{instrs}_2| \quad \text{in} \quad [ \\
& \quad \text{bg} \quad \quad \quad \text{plus} \quad [sp] \quad \quad [sp] \quad \quad \quad \underline{2} \\
& \quad \quad \quad \text{move} \quad \langle sp - 2 \rangle_s \quad [wk_0] \\
& \quad \quad \quad \text{move} \quad \langle sp - 1 \rangle_s \quad \underline{0} \\
& \quad \quad \quad \text{move} \quad [wk_0] \quad \underline{bg + c_1 + 4} \\
& \quad \quad \quad \text{instrs}_1 \\
& \quad \text{bg} + c_1 + 4 \quad \text{move} \quad \langle sp - 1 \rangle_s \quad [wk_5] \\
& \quad \quad \quad \text{move} \quad [wk_0] \quad \underline{bg + c_1 + c_2 + 6} \\
& \quad \quad \quad \text{instrs}_2 \\
& \quad \text{bg} + c_1 + c_2 + 6 \quad \text{move} \quad [wk_3] \quad [wk_5] \\
& \quad \quad \quad \text{move} \quad [wk_4] \quad \underline{bg + c_1 + c_2 + 10} \\
& \quad \quad \quad \text{move} \quad [wk_5] \quad \underline{2} \\
& \quad \quad \quad \text{jmp} \quad \underline{\text{alloc}} \\
& \quad \text{bg} + c_1 + c_2 + 10 \quad \text{move} \quad \langle wk_5 + 0 \rangle_h \quad \langle sp - 1 \rangle_s \\
& \quad \quad \quad \text{move} \quad \langle wk_5 + 1 \rangle_h \quad [wk_3] \\
& \quad \quad \quad \text{minus} \quad [sp] \quad [sp] \quad \quad \quad \underline{2} \\
& \quad \quad \quad \text{jmp} \quad \langle sp - 0 \rangle_s \\
& \quad ]
\end{aligned}$$

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

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

*Proof.*

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

- $W^2 \sqsupseteq W^1 \wedge \text{lev}(W^2) = \text{lev}(W^1)$
- $(\mathbf{M}^2, M) \in \mathcal{M}(W^2)$
- $(*) \Delta; \Gamma \vdash \text{bg} + 4 \approx_{W^2} e_1 : \tau_1$
- Let  $\mathbf{M}^3 := \mathbf{M}^2 \uplus \{\text{code}^{p_2}\}_{\text{code}}$ .  
From  $\Delta; \Gamma \vdash p_2 \approx e_2 : \tau_2$ , we have  $W^3$  such that
  - $W^3 \sqsupseteq W^2 \wedge \text{lev}(W^3) = \text{lev}(W^2)$
  - $(\mathbf{M}^3, M) \in \mathcal{M}(W^3)$
  - $(**) \Delta; \Gamma \vdash \text{bg} + c_1 + 6 \approx_{W^3} e_2 : \tau_2$
- We now choose  $W^{pe}$  to be  $W^3$  and show the required properties.
- $W^3 \sqsupseteq W \wedge \text{lev}(W^3) = \text{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^3)$  holds vacuously.
- To show:  $\forall W^4 \sqsupseteq W^3. \forall \rho \in \mathcal{D}[\Delta]. \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\Gamma]\rho(W^4).$   
 $((\underline{\text{bg}}, [\text{wk}_0], [\text{wk}_5], \{\mathbf{M} \mid \mathbf{M}.\text{reg}(\text{sv}_0) = \mathbf{v}\}), \gamma\rho(\langle e_1, e_2 \rangle)) \in \mathcal{E}[\tau_1 \times \tau_2]\rho(W^4)$
- By definition of  $\mathcal{E}[\tau_1 \times \tau_2]\rho(W^4)$  and `plugc`, we suppose
  - $((\text{kpc}, [\text{wk}_5]), K) \in \mathcal{K}[\tau_1 \times \tau_2]\rho(W^4)$ ,
  - $(\mathbf{M}^4, M^4) \in \mathcal{M}(W^4)$ ,
  - $\mathbf{M}^4 \text{ repr } \Phi^4$ ,
  - $\mathbf{M}^4.\text{reg}(\text{wk}_0) = \text{kpc}$ ,
  - $\mathbf{M}^4.\text{reg}(\text{sv}_0) = \mathbf{v}$ .
- To show:  $((\Phi^4, \text{bg}), (M^4.h, K[\gamma\rho(\langle e_1, e_2 \rangle)])) \in \mathcal{O}(W^4)$
- As  $W^4$  includes  $\iota^{\text{code}}(\text{code}^\bullet)$ , we execute the four instructions from `bg` on the low side and get the configurations

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

such that

- $\mathbf{M}^5 := \mathbf{M}^4[+\text{kpc}, \underline{0}]_{\text{stk}}[\text{wk}_0 \mapsto \underline{\text{bg} + c_1 + 4}]_{\text{reg}}$ ,
- $\mathbf{M}^5 \text{ repr } \Phi^5$ .
- Let  $W^5 := W^4[+\text{kpc}, \underline{0}]_1$ .  
Then  $(\mathbf{M}^5, M^4) \in \mathcal{M}(W^5)$ .  
By Theorem 9, it suffices to show that  $((\Phi^5, \text{bg} + 4), (M^4.h, K[\langle (\gamma\rho e_1), (\gamma\rho e_2) \rangle])) \in \mathcal{O}(W^5)$ .
- By  $(*)$ , it suffices to show that  $((\text{bg} + c_1 + 4, [\text{wk}_5]), K[\langle (-), (\gamma\rho e_2) \rangle]) \in \mathcal{K}[\tau_1]\rho(W^5)$ .
- Suppose
  - $W^6 \sqsupseteq_{\text{pub}} W^5$ ,
  - $(\mathbf{v}_1, v_2) \in \mathcal{V}[\tau_1]\rho(W^6)$ ,
  - $(\mathbf{M}^6, M^6) \in \mathcal{M}(W^6)$ ,
  - $\mathbf{M}^6.\text{reg}(\text{wk}_5) = \mathbf{v}_1$ ,
  - $\mathbf{M}^6 \text{ repr } \Phi^6$ .
- To show:  $((\Phi^6, \text{bg} + c_1 + 4), (M^6.h, K[\langle v_2, (\gamma\rho e_2) \rangle])) \in \mathcal{O}(W^6)$

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

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

such that

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

- Let  $W^7 := W^6[|\mathbf{M}^7.\text{stk}| - 1 \mapsto \mathbf{v}_1]_1$ .  
Then  $(\mathbf{M}^7, M^6) \in \mathcal{M}(W^7)$ .  
By Theorem 9, it suffices to show that  $((\Phi^7, \text{bg} + c_1 + 6), (M^6.h, K[\langle v_2, (\gamma\rho e_2) \rangle])) \in \mathcal{O}(W^7)$ .
- By (\*\*), it suffices to show that  $((\text{bg} + c_1 + c_2 + 6, \lfloor \text{wk}_5 \rfloor), K[\langle v_2, (-) \rangle]) \in \mathcal{K}[\tau_2]\rho(W^7)$ .

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

- To show:  $((\Phi^8, \text{bg} + c_1 + c_2 + 6), (M^8.h, K[\langle v_2, v_4 \rangle])) \in \mathcal{O}(W^8)$
- As  $W^8$  includes  $\iota^{\text{code}}(\text{code}^\bullet)$ , we execute the four instructions from  $\text{bg} + c_1 + c_2 + 6$  on the low side and get the following configurations

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

such that

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

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

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

such that

- $\mathbf{M}^{10} := \mathbf{M}^9[[T, S][\text{wk}_4 \mapsto \underline{w}]_{\text{reg}}[\text{wk}_5 \mapsto \widehat{\mathbf{l}}_1]_{\text{reg}} \uplus \{[\mathbf{l}_1 \mapsto (\underline{w}_0, \underline{w}_1)]\}_{\text{heap}}]$  for some  $w, \mathbf{l}_1, w_0, w_1$ ,
- $\mathbf{M}^{10} \in \mathcal{A}.GR(\text{gcbg}) \wedge \mathbf{M}^{10} \in \mathcal{A}.MR(\text{gcbg})$ ,
- $\mathbf{M}^{10}$  repr  $\Phi^{10}$ .

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

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

such that

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

- Let  $W^{11} := W^8[-2]_1 ++ \iota_1$ .  
Let  $\iota_1 := \iota^{\text{single}}(\{(W, \mathbf{M}, M) \mid \mathbf{M}.\text{hp}(\iota_1)(0) = \mathbf{v}_1 \wedge \mathbf{M}.\text{hp}(\iota_1)(1) = \mathbf{v}_3\}, \emptyset)$ .  
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  $((\text{kpc}, [\text{wk}_5]), K) \in \mathcal{K}[\tau_1 \times \tau_2]\rho(W^4)$ , it suffices to show that

$$(\widehat{\iota}_1, \langle v_2, v_4 \rangle) \in \mathcal{V}[\tau_1 \times \tau_2]\rho(W^{11})$$

- It is easy to check that  $(\widehat{\iota}_1, \langle v_2, v_4 \rangle) \in \text{oftype}(\tau_1 \times \tau_2, \rho)(W^{11})$ .
- As  $W^{11}$  includes  $\iota_1$ , 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

$$\begin{aligned}
(\Gamma \vdash e.1) &::= \text{Pfst}((\Gamma \vdash e)) \\
\text{Pfst}(p) &::= \lambda \text{ alloc, bg.} \\
\text{let code} &:= p(\text{alloc, bg} + 3), \ c := |\text{code}| \ \text{in} \ [ \\
&\quad \text{bg} \quad \quad \text{plus} \quad [\text{sp}] \quad \quad [\text{sp}] \quad \quad \underline{1} \\
&\quad \quad \quad \text{move} \quad \langle \text{sp} - 1 \rangle_s \quad [\text{wk}_0] \\
&\quad \quad \quad \text{move} \quad [\text{wk}_0] \quad \quad \underline{\text{bg} + c + 3} \\
&\quad \quad \quad \text{code} \\
&\quad \text{bg} + c + 3 \quad \text{move} \quad [\text{wk}_5] \quad \quad \langle \text{wk}_5 + 0 \rangle_h \\
&\quad \quad \quad \text{minus} \quad [\text{sp}] \quad \quad [\text{sp}] \quad \quad \underline{1} \\
&\quad \quad \quad \text{jmp} \quad \quad \langle \text{sp} - 0 \rangle_s \\
&\quad ]
\end{aligned}$$

**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  $\mathcal{A}$ , gcbg, bg,  $k$ , suppose
  - $W \sqsupseteq W_k^\circ(\mathcal{A}, \text{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$
  - $\text{code} := [\text{bg} \Rightarrow \text{Pfst}(p)(\mathcal{A}(\text{gcbg}).\text{alloc}, \text{bg})]$
  - $\text{code}^p := [\text{bg} + 3 \Rightarrow p(\mathcal{A}(\text{gcbg}).\text{alloc}, \text{bg} + 3)]$ ,  $c := |\text{code}^p|$
  - $\text{code}^\bullet := \text{code} \setminus \text{code}^p$
  - $\mathbf{M}' = \mathbf{M} \uplus \{\text{code}\}_{\text{code}}$ .
- 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  $W^1 := W \uplus \iota^{\text{code}}(\text{code}^\bullet)$ .  
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:  $\forall W^3 \sqsupseteq W^2. \forall \rho \in \mathcal{D}[\Delta]. \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\Gamma]\rho(W^3)$ .  
 $((\text{bg}, \lfloor \text{wk}_0 \rfloor, \lfloor \text{wk}_5 \rfloor, \{\mathbf{M} \mid \mathbf{M}.\text{reg}(\text{sv}_0) = \mathbf{v}\}), \gamma\rho(e.1)) \in \mathcal{E}[\tau_1]\rho(W^3)$
- By definition of  $\mathcal{E}[\tau_1]\rho(W^3)$  and `plugc`, we suppose
  - $((\text{kpc}, \lfloor \text{wk}_5 \rfloor), K) \in \mathcal{K}[\tau_1]\rho(W^3)$ ,
  - $(\mathbf{M}^3, M^3) \in \mathcal{M}(W^3)$ ,
  - $\mathbf{M}^3 \text{ repr } \Phi^3$ ,
  - $\mathbf{M}^3.\text{reg}(\text{wk}_0) = \text{kpc}$ ,
  - $\mathbf{M}^3.\text{reg}(\text{sv}_0) = \mathbf{v}$ .
- 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

  - $\mathbf{M}^4 := \mathbf{M}^3[+\text{kpc}]_{\text{stk}}[\text{wk}_0 \mapsto \text{bg} + c + 3]_{\text{reg}}$ ,
  - $\mathbf{M}^4 \text{ repr } \Phi^4$ .
- Let  $W^4 := W^3[+\text{kpc}]_1$ .  
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
  - $W^5 \sqsupseteq_{\text{pub}} W^4$ ,
  - $(\mathbf{v}_1, v_2) \in \mathcal{V}[\tau_1 \times \tau_2]\rho(W^5)$ ,
  - $(\mathbf{M}^5, M^5) \in \mathcal{M}(W^5)$ ,
  - $\mathbf{M}^5.\text{reg}(\text{wk}_5) = \mathbf{v}_1$ ,
  - $\mathbf{M}^5 \text{ repr } \Phi^5$ .
- 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  $(\mathbf{v}_1, v_2) \in \mathcal{V}[\tau_1 \times \tau_2]\rho(W^5)$ 
  - $\mathbf{v}_1 = \widehat{\mathbf{l}}_1$ ,  $\mathbf{M}^5.\text{hp}(\mathbf{l}_1)(0) = \mathbf{u}_1$ ,  $\mathbf{M}^5.\text{hp}(\mathbf{l}_1)(1) = \mathbf{u}_2$  for some  $\mathbf{l}_1, \mathbf{u}_1, \mathbf{u}_2$
  - $v_2 = \langle u_1, u_2 \rangle$  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  $\iota^{\text{code}}(\text{code}^\bullet)$ , we execute the three instructions from  $\text{bg} + c + 3$  on the low side, take one step on the high side, and get the configurations

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

such that

- $\mathbf{M}^6 := \mathbf{M}^5[\text{wk}_5 \mapsto \mathbf{u}_1]_{\text{reg}}[-1]_{\text{stk}}$ ,
- $\mathbf{M}^6$  repr  $\Phi^6$ ,
- $M^6 := M^5$ .
- 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  $((\Phi^6, \text{kpc}), (M^6.h, K[u_1])) \in \mathcal{O}(W^6)$ .
- As  $W^6 \supseteq_{\text{pub}} W^3$  and  $((\text{kpc}, \lfloor \text{wk}_5 \rfloor), K) \in \mathcal{K}[\tau_1]\rho(W^3)$ , 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

$$\begin{aligned}
 (\Gamma \vdash \lambda x:\tau. e) &::= \text{Pabs}((\Gamma, x:\tau \vdash e)) \\
 \text{Pabs}(p) &::= \lambda \text{alloc}, \text{bg}. \\
 \text{let code} &:= p(\text{alloc}, \text{bg} + 16), c := |\text{code}| \quad \text{in} \quad [ \\
 &\quad \text{bg} \quad \quad \text{move} \quad [wk_4] \quad \quad \underline{\text{bg} + 3} \\
 &\quad \quad \quad \text{move} \quad [wk_5] \quad \quad \underline{2} \\
 &\quad \quad \quad \text{jmp} \quad \quad \underline{\text{alloc}} \\
 &\quad \text{bg} + 3 \quad \text{move} \quad \langle wk_5 + 0 \rangle_h \quad \underline{\text{bg} + 6} \\
 &\quad \quad \quad \text{move} \quad \langle wk_5 + 1 \rangle_h \quad \underline{[sv_0]} \\
 &\quad \quad \quad \text{jmp} \quad [wk_0] \\
 &\quad \text{bg} + 6 \quad \text{plus} \quad [sp] \quad \quad [sp] \quad \quad \underline{2} \\
 &\quad \quad \quad \text{move} \quad \langle sp - 2 \rangle_s \quad [wk_0] \\
 &\quad \quad \quad \text{move} \quad \langle sp - 1 \rangle_s \quad [sv_0] \\
 &\quad \quad \quad \text{move} \quad [wk_4] \quad \quad \underline{\text{bg} + 12} \\
 &\quad \quad \quad \text{move} \quad [wk_5] \quad \quad \underline{2} \\
 &\quad \quad \quad \text{jmp} \quad \underline{\text{alloc}} \\
 &\quad \text{bg} + 12 \quad \text{move} \quad \langle wk_5 + 0 \rangle_h \quad [wk_2] \\
 &\quad \quad \quad \text{move} \quad \langle wk_5 + 1 \rangle_h \quad \langle wk_1 + 1 \rangle_h \\
 &\quad \quad \quad \text{move} \quad [sv_0] \quad [wk_5] \\
 &\quad \quad \quad \text{move} \quad [wk_0] \quad \underline{\text{bg} + c + 16} \\
 &\quad \quad \quad \text{code} \\
 &\quad \text{bg} + c + 16 \quad \text{move} \quad [sv_0] \quad \quad \langle sp - 1 \rangle_s \\
 &\quad \quad \quad \text{minus} \quad [sp] \quad \quad [sp] \quad \quad \underline{2} \\
 &\quad \quad \quad \text{jmp} \quad \langle sp - 0 \rangle_s \\
 &\quad ]
 \end{aligned}$$

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

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

*Proof.*

- For any  $\mathcal{A}$ , gcbg, bg,  $k$ , suppose
  - $W \sqsupseteq W_k^o(\mathcal{A}, \text{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$
  - $\text{code} := [\text{bg} \mapsto \text{Pabs}(p)(\mathcal{A}(\text{gcbg}).\text{alloc}, \text{bg})]$
  - $\text{code}^p := [\text{bg} + 16 \mapsto p(\mathcal{A}(\text{gcbg}).\text{alloc}, \text{bg} + 16)], c := |\text{code}^p|$
  - $\text{code}^\bullet := \text{code} \setminus \text{code}^p$
  - $\mathbf{M}' = \mathbf{M} \uplus \{\text{code}\}_{\text{code}}$ .
- Goal: find  $W^{pe}$  such that
  - $W^{pe} \sqsupseteq W \wedge \text{lev}(W^{pe}) = \text{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta; \Gamma \vdash \text{bg} \approx_{W^{pe}} \lambda x:\tau'. e : \tau' \rightarrow \tau$
- Let  $\mathbf{M}^1 := \mathbf{M} \uplus \{\text{code}^\bullet\}_{\text{code}}$ .  
 Let  $W^1 := W \uparrow \iota^{\text{code}}(\text{code}^\bullet)$ .  
 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  $\Delta; \Gamma, x : \tau' \vdash p \approx e : \tau$ , we have  $W^2$  such that
  - $W^2 \sqsupseteq W^1 \wedge \text{lev}(W^2) = \text{lev}(W^1)$
  - $(\mathbf{M}^2, M) \in \mathcal{M}(W^2)$
  - $(*) \Delta; \Gamma, x : \tau' \vdash \text{bg} + 16 \approx_{W^2} e : \tau$
- We now choose  $W^{pe}$  to be  $W^2$  and show the required properties.
- $W^2 \sqsupseteq W \wedge \text{lev}(W^2) = \text{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^2)$  holds vacuously.
- To show:  $\forall W^3 \sqsupseteq W^2. \forall \rho \in \mathcal{D}[\Delta]. \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\Gamma]\rho(W^3).$   
 $((\underline{\text{bg}}, \lfloor \text{wk}_0 \rfloor, \lfloor \text{wk}_5 \rfloor, \{ \mathbf{M} \mid \mathbf{M}.\text{reg}(\text{sv}_0) = \mathbf{v} \}), \gamma\rho(\lambda x:\tau'. e)) \in \mathcal{E}[\tau' \rightarrow \tau]\rho(W^3)$
- By definition of  $\mathcal{E}[\tau' \rightarrow \tau]\rho(W^3)$  and plugc, we suppose
  - $((\text{kpc}, \lfloor \text{wk}_5 \rfloor), K) \in \mathcal{K}[\tau' \rightarrow \tau]\rho(W^3),$
  - $(\mathbf{M}^3, M^3) \in \mathcal{M}(W^3),$
  - $\mathbf{M}^3 \text{ repr } \Phi^3,$
  - $\mathbf{M}^3.\text{reg}(\text{wk}_0) = \underline{\text{kpc}},$
  - $\mathbf{M}^3.\text{reg}(\text{sv}_0) = \mathbf{v}.$
- To show:  $((\Phi^3, \text{bg}), (M^3.h, K[\gamma\rho(\lambda x:\tau'. e)])) \in \mathcal{O}(W^3)$
- As  $W^3$  includes  $\iota^{\text{code}}(\text{code}^\bullet)$ , we execute the three instructions from  $\text{bg}$  on the low side and get the configurations
 
$$(\Phi^4, \text{alloc}), \quad (M^3.h, K[\gamma\rho(\lambda x:\tau'. e)])$$
 such that
  - $\mathbf{M}^4 := \mathbf{M}^3[\text{wk}_4 \mapsto \underline{\text{bg}} + 3]_{\text{reg}}[\text{wk}_5 \mapsto \underline{2}]_{\text{reg}},$
  - $\mathbf{M}^4 \text{ repr } \Phi^4.$
- By the specifications of  $\mathcal{A}$ , after some finite number of steps of execution, we have configurations
 
$$(\Phi^5, \text{bg} + 3), \quad (M^3.h, K[\gamma\rho(\lambda x:\tau'. e)])$$
 such that
  - $\mathbf{M}^5 := \mathbf{M}^4[[T, S]][\text{wk}_4 \mapsto \underline{w}]_{\text{reg}}[\text{wk}_5 \mapsto \widehat{\mathbf{l}}_1]_{\text{reg}} \uplus \{[\mathbf{l}_1 \mapsto (\underline{w}_0, \underline{w}_1)]\}_{\text{heap}}$  for some  $w, \mathbf{l}_1, w_0, w_1,$
  - $\mathbf{M}^5 \in \mathcal{A}.GR(\text{gcbg}) \wedge \mathbf{M}^5 \in \mathcal{A}.MR(\text{gcbg}),$
  - $\mathbf{M}^5 \text{ repr } \Phi^5.$
- As  $\mathbf{M}^5.\text{code} = \mathbf{M}^4.\text{code}$ , we execute the three instructions from  $\text{bg} + 3$  on the low side and get
 
$$(\Phi^6, \text{kpc}), \quad (M^3.h, K[\gamma\rho(\lambda x:\tau'. e)])$$
 such that
  - $\mathbf{M}^6 := \mathbf{M}^5[\mathbf{l}_1 : 0 \mapsto \text{bg} + 6]_{\text{hp}}[\mathbf{l}_1 : 1 \mapsto \mathbf{v}]_{\text{hp}}$
  - $\mathbf{M}^6 \text{ repr } \Phi^6.$
- Let  $W^6 := W^3 \upuparrows \iota_1.$   
 Let  $\iota_1 := \iota^{\text{single}}(MR_{\mathbf{l}_1}, \emptyset).$   
 Let  $MR_{\mathbf{l}_1} := \{ (W, \mathbf{M}, M) \mid \mathbf{M}.\text{hp}(\mathbf{l}_1)(0) = \underline{\text{bg}} + 6 \wedge \mathbf{M}.\text{hp}(\mathbf{l}_1)(1) = \mathbf{v} \}.$   
 Then  $(\Phi^6, M^3) \in \mathcal{M}(W^6).$

- By Theorem 9, it suffices to show that  $((\Phi^6, \text{kpc}), (M^3.h, K[\gamma\rho(\lambda x:\tau'.e)])) \in \mathcal{O}(W^6)$ .
- As  $W^6 \sqsupseteq_{\text{pub}} W^3$  and  $((\text{kpc}, \lfloor \text{wk}_5 \rfloor), K) \in \mathcal{K}[\tau' \rightarrow \tau]\rho(W^3)$ , it suffices to show that

$$(\widehat{\mathbf{l}}_1, \lambda x:\rho.2(\tau').\gamma\rho e) \in \mathcal{V}[\tau' \rightarrow \tau]\rho(W^6)$$

- It is easy to check that  $(\widehat{\mathbf{l}}_1, \lambda x:\rho.2(\tau').\gamma\rho e) \in \text{oftype}(\tau' \rightarrow \tau, \rho)(W^6)$ .
- Suppose
  - $W^7 \sqsupseteq_{\text{p}} W^6$ ,
  - $(\mathbf{u}_1, u_2) \in \mathcal{V}[\tau']\rho(W^7)$ .

- To show:

$$(\mathbf{e}^7, (\gamma\rho e)[u_2/x]) \in \mathcal{E}[\tau]\rho(W^7)$$

where

$$\mathbf{e}^7 = (\langle \mathbf{l}_1 : 0 \rangle_{\text{h}}, \lfloor \text{wk}_0 \rfloor, \lfloor \text{wk}_5 \rfloor, \{ \mathbf{M} \mid \mathbf{M}.\text{reg}(\text{wk}_1) = \widehat{\mathbf{l}}_1 \wedge \mathbf{M}.\text{reg}(\text{wk}_2) = \mathbf{u}_1 \})$$

- By definition of  $\mathcal{E}[\tau]\rho(W^7)$  and `plugc`, suppose
  - $((\text{kpc}^7, \lfloor \text{wk}_5 \rfloor), K^7) \in \mathcal{K}[\tau]\rho(W^7)$
  - $(\mathbf{M}^7, M^7) \in \mathcal{M}(W^7)$
  - $\mathbf{M}^7$  repr  $\Phi^7$
  - $\mathbf{M}^7.\text{reg}(\text{wk}_0) = \text{kpc}^7$
  - $\mathbf{M}^7.\text{reg}(\text{wk}_1) = \widehat{\mathbf{l}}_1$
  - $\mathbf{M}^7.\text{reg}(\text{wk}_2) = \mathbf{u}_1$

- As  $W^7$  includes  $u_1$ , we have  $\mathbf{M}^7.\text{hp}(\mathbf{l}_1)(0) = \underline{\text{bg} + 6}$

- To show:

$$((\Phi^7, \text{bg} + 6), (M^7.h, K^7[(\gamma, x \mapsto u_2)\rho e])) \in \mathcal{O}(W^7)$$

- As  $W^7$  includes  $\iota^{\text{code}}(\text{code}^\bullet)$ , we execute the six instructions from `bg + 6` on the low side and get the following configurations

$$(\Phi^8, \text{alloc}) \quad (M^7.h, K^7[(\gamma, x \mapsto u_2)\rho e])$$

such that

- $\mathbf{v}' := \mathbf{M}^7.\text{reg}(\text{sv}_0)$
- $\mathbf{M}^8 := \mathbf{M}^7[+\text{kpc}^7, \mathbf{v}']_{\text{stk}}[\text{wk}_4 \mapsto \underline{\text{bg} + 12}]_{\text{reg}}[\text{wk}_5 \mapsto \underline{2}]_{\text{reg}}$ ,
- $\mathbf{M}^8$  repr  $\Phi^8$ .

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

$$(\Phi^9, \text{bg} + 12), \quad (M^7.h, K^7[(\gamma, x \mapsto u_2)\rho e])$$

such that

- $\mathbf{M}^9 := \mathbf{M}^8[[T, S]][\text{wk}_4 \mapsto \underline{w}]_{\text{reg}}[\text{wk}_5 \mapsto \widehat{\mathbf{l}}_2]_{\text{reg}} \uplus \{[\mathbf{l}_2 \mapsto (\underline{w}_0, \underline{w}_1)]\}_{\text{heap}}$  for some  $w, \mathbf{l}_2, w_0, w_1$ ,
- $\mathbf{M}^9 \in \mathcal{A}.\text{GR}(\text{gcbg}) \wedge \mathbf{M}^9 \in \mathcal{A}.\text{MR}(\text{gcbg})$ ,
- $\mathbf{M}^9$  repr  $\Phi^9$ .

- As  $W^7$  includes  $u_1$ , we have  $\mathbf{M}^9.\text{hp}(\mathbf{l}_1)(1) = \mathbf{M}^7.\text{hp}(\mathbf{l}_1)(1) = \mathbf{v}$ .
- We execute the four instructions from  $\text{bg} + 12$  on the low side and get the following configurations

$$(\Phi^{10}, \text{bg} + 16) \quad (M^7.h, K^7[(\gamma, x \mapsto u_2)\rho e])$$

such that

- $\mathbf{M}^{10} := \mathbf{M}^9[\mathbf{l}_2 : 0 \mapsto \mathbf{u}_1]_{\text{hp}}[\mathbf{l}_2 : 1 \mapsto \mathbf{v}]_{\text{hp}}[\text{sv}_0 \mapsto \widehat{\mathbf{l}}_2]_{\text{reg}}[\text{wk}_0 \mapsto \underline{\text{bg} + c + 16}]_{\text{reg}}$ ,
- $\mathbf{M}^{10}$  repr  $\Phi^{10}$ .

- Let  $W^{10} := W^7[+\text{kpc}^7, \mathbf{v}']_1[\text{sv}_0 \mapsto \widehat{\mathbf{l}}_2]_1 + u_2$ .  
Let  $u_2 := \iota^{\text{single}}(MR_{\mathbf{l}_2}, \emptyset)$ .  
Let  $MR_{\mathbf{l}_2} := \{(W, \mathbf{M}, M) \mid \mathbf{M}.\text{hp}(\mathbf{l}_2)(0) = \mathbf{u}_1 \wedge \mathbf{M}.\text{hp}(\mathbf{l}_2)(1) = \mathbf{v}\}$ .  
Then  $(\Phi^{10}, M^7) \in \mathcal{M}(W^{10})$ .
- By Theorem 9, it suffices to show that  $((\Phi^{10}, \text{bg} + 16), (M^7.h, K^7[(\gamma, x \mapsto u_2)\rho e])) \in \mathcal{O}(W^{10})$ .
- It is easy to check that  $(W^{10}, \widehat{\mathbf{l}}_2, (\gamma, x \mapsto u_2)) \in \mathcal{G}[\Gamma, x : \tau']\rho$ .
- Thus, by (\*), it suffices to show that

$$((\text{bg} + c + 16, \lfloor \text{wk}_5 \rfloor), K^7[-]) \in \mathcal{K}[\tau]\rho(W^{10})$$

- Suppose  
 $W^{11} \sqsupseteq_{\text{pub}} W^{10}$ ,  
 $(\mathbf{v}_1, v_2) \in \mathcal{V}[\tau]\rho(W^{11})$ ,  
 $(\mathbf{M}^{11}, M^{11}) \in \mathcal{M}(W^{11})$ ,  
 $\mathbf{M}^{11}.\text{reg}(\text{wk}_5) = \mathbf{v}_1$ ,  
 $\mathbf{M}^{11}$  repr  $\Phi^{11}$ .
- To show:  $((\Phi^{11}, \text{bg} + c + 16), (M^{11}.h, K^7[v_2])) \in \mathcal{O}(W^{11})$
- As  $W^{11}$  includes  $\iota^{\text{code}}(\text{code}^\bullet)$ , we execute the three instructions from  $\text{bg} + c + 16$  on the low side and get the configurations

$$(\Phi^{12}, \text{kpc}^7), \quad (M^{11}.h, K^7[v_2])$$

such that

- $\mathbf{M}^{12} := \mathbf{M}^{11}[\text{sv}_0 \mapsto \mathbf{v}']_{\text{reg}}[-2]_{\text{stk}}$ ,
- $\mathbf{M}^{12}$  repr  $\Phi^{12}$ .

- Let  $W^{12} := W^{11}[\text{sv}_0 \mapsto \mathbf{v}']_1[-2]_1$ .  
Then,  $(\mathbf{M}^{12}, M^{11}) \in \mathcal{M}(W^{12})$ .
- By Theorem 9, it suffices to show that  $((\Phi^{12}, \text{kpc}^7), (M^{11}.h, K^7[v_2])) \in \mathcal{O}(W^{12})$ .
- As  $W^{12} \sqsupseteq_{\text{pub}} W^7$  and  $((\text{kpc}^7, \lfloor \text{wk}_5 \rfloor), K^7) \in \mathcal{K}[\tau]\rho(W^7)$ , it suffices to show that

$$(\mathbf{v}_1, v_2) \in \mathcal{V}[\tau]\rho(W^{12})$$

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

$$\begin{aligned}
& (\Gamma \vdash e_1 e_2) ::= \text{Papp}((\Gamma \vdash e_1), (\Gamma \vdash e_2)) \\
& \text{Papp}(p_1, p_2) ::= \lambda \text{ alloc, bg.} \\
& \text{let instrs}_1 := p_1(\text{alloc, bg} + 4), \quad c_1 := |\text{instrs}_1|, \\
& \quad \text{instrs}_2 := p_2(\text{alloc, bg} + c_1 + 6), \quad c_2 := |\text{instrs}_2| \\
& \text{in } [ \\
& \quad \text{bg} \qquad \text{plus} \quad [\text{sp}] \qquad \quad [\text{sp}] \qquad \quad \underline{\quad} \\
& \qquad \qquad \text{move} \quad \langle \text{sp} - 2 \rangle_s \quad [\text{wk}_0] \\
& \qquad \qquad \text{move} \quad \langle \text{sp} - 1 \rangle_s \quad \underline{0} \\
& \qquad \qquad \text{move} \quad [\text{wk}_0] \qquad \quad \underline{\text{bg} + c_1 + 4} \\
& \qquad \quad \text{instrs}_1 \\
& \quad \text{bg} + c_1 + 4 \quad \text{move} \quad \langle \text{sp} - 1 \rangle_s \quad [\text{wk}_5] \\
& \qquad \qquad \text{move} \quad [\text{wk}_0] \qquad \quad \underline{\text{bg} + c_1 + c_2 + 6} \\
& \qquad \quad \text{instrs}_2 \\
& \quad \text{bg} + c_1 + c_2 + 6 \quad \text{move} \quad [\text{wk}_0] \qquad \quad \langle \text{sp} - 2 \rangle_s \\
& \qquad \qquad \text{move} \quad [\text{wk}_1] \qquad \quad \langle \text{sp} - 1 \rangle_s \\
& \qquad \qquad \text{move} \quad [\text{wk}_2] \qquad \quad [\text{wk}_5] \\
& \qquad \qquad \text{minus} \quad [\text{sp}] \qquad \quad [\text{sp}] \qquad \quad \underline{\quad} \\
& \qquad \qquad \text{jmp} \quad \langle \text{wk}_1 + 0 \rangle_h \\
& \quad ]
\end{aligned}$$

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

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

*Proof.*

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

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

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

such that

- $\mathbf{M}^5 := \mathbf{M}^4[+\text{kpc}, \text{0}]_{\text{stk}}[\text{wk}_0 \mapsto \text{bg} + c_1 + 4]_{\text{reg}}$ ,
- $\mathbf{M}^5 \text{ repr } \Phi^5$ .

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

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

such that

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

- Let  $W^7 := W^6[|\mathbf{M}^7.\text{stk}| - 1 \mapsto \mathbf{v}_1]_1$ .  
Then  $(\mathbf{M}^7, M^6) \in \mathcal{M}(W^7)$ .  
By Theorem 9, it suffices to show that  $((\Phi^7, \text{bg} + c_1 + 6), (M^6.h, K[v_2(\gamma\rho e_2)])) \in \mathcal{O}(W^7)$ .
- By (\*\*), it suffices to show that  $((\text{bg} + c_1 + c_2 + 6, \lfloor \text{wk}_5 \rfloor), K[v_2(-)]) \in \mathcal{K}[\tau']\rho(W^7)$ .

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

- To show:  $((\Phi^8, \text{bg} + c_1 + c_2 + 6), (M^8.h, K[v_2 v_4])) \in \mathcal{O}(W^8)$
- As  $(\mathbf{v}_1, v_2) \in \text{oftype}(\tau' \rightarrow \tau, \rho)(W^8)$  by Theorems 5 and 4, we have
  - $\mathbf{v}_1 = \hat{\mathbf{l}}_1$ ,
  - $\mathbf{M}^8.\text{hp}(\hat{\mathbf{l}}_1)(0) = \underline{w}$  for some  $w$ ,
  - $v_2 = \lambda x : \tau'. e_2$  for some  $e_2$ .
- As  $W^8$  includes  $\iota^{\text{code}}(\text{code}^\bullet)$ , we execute the five instructions from  $\text{bg} + c_1 + c_2 + 6$  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

- $\mathbf{M}^9 := \mathbf{M}^8[\text{wk}_0 \mapsto \underline{\text{kpc}}]_{\text{reg}}[\text{wk}_1 \mapsto \hat{\mathbf{l}}_1]_{\text{reg}}[\text{wk}_2 \mapsto \mathbf{v}_3]_{\text{reg}}[-2]_{\text{stk}}$ ,
- $\mathbf{M}^9 \text{ repr } \Phi^9$ .

- 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  $(\hat{\mathbf{l}}_1, \lambda x : \tau'. e_2) \in \mathcal{V}[\tau' \rightarrow \tau]\rho(W^6)$ , we have
  - $((\langle \hat{\mathbf{l}}_1 : 0 \rangle_{\text{h}}, \lfloor \text{wk}_0 \rfloor, \lfloor \text{wk}_5 \rfloor, \{\mathbf{M} \mid \mathbf{M}.\text{reg}(\text{wk}_1) = \hat{\mathbf{l}}_1 \wedge \mathbf{M}.\text{reg}(\text{wk}_2) = \mathbf{v}_3\}), e_2[v_4/x]) \in \mathcal{E}[\tau]\rho(W^9)$ .
- By definition of  $\mathcal{E}[\tau]\rho(W^9)$ , it suffices to show that  $((\text{kpc}, \lfloor \text{wk}_5 \rfloor), K) \in \mathcal{K}[\tau]\rho(W^9)$ , which follows from the fact that  $((\text{kpc}, \lfloor \text{wk}_5 \rfloor), K) \in \mathcal{K}[\tau]\rho(W^4)$  and  $W^9 \sqsupseteq_{\text{pub}} W^4$  by Theorem 6.

□

## 9.8 Gen

$$\begin{aligned}
& (\Gamma \vdash \Lambda\alpha.e) ::= \text{Pgen}((\Gamma \vdash e)) \\
& \text{Pgen}(p) := \lambda \text{ alloc, bg.} \\
& \text{let code} := p(\text{alloc, bg} + 11), c := |\text{code}| \text{ in } [ \\
& \quad \text{bg} \quad \quad \text{move} \quad [wk_4] \quad \underline{\text{bg} + 3} \\
& \quad \quad \quad \text{move} \quad [wk_5] \quad \underline{2} \\
& \quad \quad \quad \text{jmp} \quad \underline{\text{alloc}} \\
& \quad \text{bg} + 3 \quad \text{move} \quad \langle wk_5 + 0 \rangle_h \quad \underline{\text{bg} + 6} \\
& \quad \quad \quad \text{move} \quad \langle wk_5 + 1 \rangle_h \quad [sv_0] \\
& \quad \quad \quad \text{jmp} \quad [wk_0] \\
& \quad \text{bg} + 6 \quad \text{plus} \quad [sp] \quad [sp] \quad \underline{2} \\
& \quad \quad \quad \text{move} \quad \langle sp - 2 \rangle_s \quad [wk_0] \\
& \quad \quad \quad \text{move} \quad \langle sp - 1 \rangle_s \quad [sv_0] \\
& \quad \quad \quad \text{move} \quad [sv_0] \quad \langle wk_1 + 1 \rangle_h \\
& \quad \quad \quad \text{move} \quad [wk_0] \quad \underline{\text{bg} + c + 11} \\
& \quad \quad \quad \text{code} \\
& \quad \text{bg} + c + 11 \quad \text{move} \quad [sv_0] \quad \langle sp - 1 \rangle_s \\
& \quad \quad \quad \text{minus} \quad [sp] \quad [sp] \quad \underline{2} \\
& \quad \quad \quad \text{jmp} \quad \langle sp - 0 \rangle_s \\
& \quad ]
\end{aligned}$$

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

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

*Proof.*

- For any  $\mathcal{A}$ , gcbg, bg,  $k$ , suppose
  - $W \sqsupseteq W_k^\circ(\mathcal{A}, \text{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$
  - $\text{code} := [\text{bg} \mapsto \text{Pgen}(p)(\mathcal{A}(\text{gcbg}).\text{alloc}, \text{bg})]$
  - $\text{code}^p := [\text{bg} + 11 \mapsto p(\mathcal{A}(\text{gcbg}).\text{alloc}, \text{bg} + 11)], c := |\text{code}^p|$
  - $\text{code}^\bullet := \text{code} \setminus \text{code}^p$
  - $\mathbf{M}' = \mathbf{M} \uplus \{\text{code}\}_{\text{code}}$ .
- Goal: find  $W^{pe}$  such that
  - $W^{pe} \sqsupseteq W \wedge \text{lev}(W^{pe}) = \text{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta; \Gamma \vdash \text{bg} \approx_{W^{pe}} \Lambda\alpha.e : \forall\alpha. \tau$
- Let  $\mathbf{M}^1 := \mathbf{M} \uplus \{\text{code}^\bullet\}_{\text{code}}$ .  
Let  $W^1 := W \uparrow \iota^{\text{code}}(\text{code}^\bullet)$ .  
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  $\Delta, \alpha; \Gamma \vdash p \approx e : \tau$ , we have  $W^2$  such that
  - $W^2 \sqsupseteq W^1 \wedge \text{lev}(W^2) = \text{lev}(W^1)$
  - $(\mathbf{M}^2, M) \in \mathcal{M}(W^2)$
  - (\*)  $\Delta, \alpha; \Gamma \vdash \text{bg} + 11 \approx_{W^2} e : \tau$



- We now choose  $W^{pe}$  to be  $W^2$  and show the required properties.
- $W^2 \sqsupseteq W \wedge \text{lev}(W^2) = \text{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^2)$  holds vacuously.
- To show:  $\forall W^3 \sqsupseteq W^2. \forall \rho \in \mathcal{D}[\Delta]. \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\Gamma]\rho(W^3).$   
 $((\underline{\text{bg}}, \lfloor \text{wk}_0 \rfloor, \lfloor \text{wk}_5 \rfloor, \{ \mathbf{M} \mid \mathbf{M}.\text{reg}(\text{sv}_0) = \mathbf{v} \}), \gamma\rho(\Lambda\alpha.e)) \in \mathcal{E}[\forall\alpha.\tau]\rho(W^3)$
- By definition of  $\mathcal{E}[\forall\alpha.\tau]\rho(W^3)$  and `plugc`, we suppose
  - $((\text{kpc}, \lfloor \text{wk}_5 \rfloor), K) \in \mathcal{K}[\forall\alpha.\tau]\rho(W^3),$
  - $(\mathbf{M}^3, M^3) \in \mathcal{M}(W^3),$
  - $\mathbf{M}^3 \text{ repr } \Phi^3,$
  - $\mathbf{M}^3.\text{reg}(\text{wk}_0) = \text{kpc},$
  - $\mathbf{M}^3.\text{reg}(\text{sv}_0) = \mathbf{v}.$
- To show:  $((\Phi^3, \text{bg}), (M^3.h, K[\gamma\rho(\Lambda\alpha.e)])) \in \mathcal{O}(W^3)$
- 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

$$(\Phi^4, \text{alloc}), \quad (M^3.h, K[\gamma\rho(\Lambda\alpha.e)])$$

such that

- $\mathbf{M}^4 := \mathbf{M}^3[\text{wk}_4 \mapsto \underline{\text{bg}} + 3]_{\text{reg}}[\text{wk}_5 \mapsto \underline{2}]_{\text{reg}},$
- $\mathbf{M}^4 \text{ repr } \Phi^4.$

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

$$(\Phi^5, \text{bg} + 3), \quad (M^3.h, K[\gamma\rho(\Lambda\alpha.e)])$$

such that

- $\mathbf{M}^5 := \mathbf{M}^4[[T, S]][\text{wk}_4 \mapsto \underline{w}]_{\text{reg}}[\text{wk}_5 \mapsto \widehat{\mathbf{l}}_1]_{\text{reg}} \uplus \{[\mathbf{l}_1 \mapsto (\underline{w}_0, \underline{w}_1)]\}_{\text{heap}}$  for some  $w, \mathbf{l}_1, w_0, w_1,$
- $\mathbf{M}^5 \in \mathcal{A}.GR(\text{gcbg}) \wedge \mathbf{M}^5 \in \mathcal{A}.MR(\text{gcbg}),$
- $\mathbf{M}^5 \text{ repr } \Phi^5.$

- As  $\mathbf{M}^5.\text{code} = \mathbf{M}^4.\text{code}$ , we execute the three instructions from `bg + 3` on the low side and get

$$(\Phi^6, \text{kpc}), \quad (M^3.h, K[\gamma\rho(\Lambda\alpha.e)])$$

such that

- $\mathbf{M}^6 := \mathbf{M}^5[\mathbf{l}_1 : 0 \mapsto \text{bg} + 6]_{\text{hp}}[\mathbf{l}_1 : 1 \mapsto \mathbf{v}]_{\text{hp}}$
- $\mathbf{M}^6 \text{ repr } \Phi^6.$

- Let  $W^6 := W^3 \uparrow \iota_1.$

Let  $\iota_1 := \iota^{\text{single}}(MR_{\mathbf{l}_1}, \emptyset).$

Let  $MR_{\mathbf{l}_1} := \{ (W, \mathbf{M}, M) \mid \mathbf{M}.\text{hp}(\mathbf{l}_1)(0) = \underline{\text{bg}} + 6 \wedge \mathbf{M}.\text{hp}(\mathbf{l}_1)(1) = \mathbf{v} \}.$

Then  $(\Phi^6, M^3) \in \mathcal{M}(W^6).$

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

$$(\widehat{\mathbf{l}}_1, \Lambda\alpha.\gamma\rho e) \in \mathcal{V}[\forall\alpha.\tau]\rho(W^6)$$

- It is easy to check that  $(\widehat{l}_1, \Lambda\alpha.\gamma\rho e) \in \text{oftype}(\forall\alpha.\tau, \rho)(W^6)$ .

- Suppose  $W^7 \sqsupset W^6$ ,  
 $(\tau'_1, \tau'_2, R) \in \text{TyValRel}$ .

- To show:

$$(e^7, (\gamma\rho e)[\tau'_2/\alpha]) \in \mathcal{E}[\tau]\rho(W^7)$$

where

$$e^7 = (\langle l_1 : 0 \rangle_h, \lfloor \text{wk}_0 \rfloor, \lfloor \text{wk}_5 \rfloor, \{ \mathbf{M} \mid \mathbf{M}.\text{reg}(\text{wk}_1) = \widehat{l}_1 \})$$

- By definition of  $\mathcal{E}[\tau]\rho(W^7)$  and `plugc`, suppose
  - $((\text{kpc}^7, \lfloor \text{wk}_5 \rfloor), K^7) \in \mathcal{K}[\tau]\rho(W^7)$
  - $(\mathbf{M}^7, M^7) \in \mathcal{M}(W^7)$
  - $\mathbf{M}^7$  repr  $\Phi^7$
  - $\mathbf{M}^7.\text{reg}(\text{wk}_0) = \text{kpc}^7$
  - $\mathbf{M}^7.\text{reg}(\text{wk}_1) = \widehat{l}_1$

- As  $W^7$  includes  $\iota_{l_1}$ , we have  $\mathbf{M}^7.\text{hp}(l_1)(0) = \underline{\text{bg} + 6}$

- To show:

$$((\Phi^7, \text{bg} + 6), (M^7.h, K^7[\gamma(\rho, \alpha \mapsto (\tau'_1, \tau'_2, R))e])) \in \mathcal{O}(W^7)$$

- As  $W^7$  includes  $\iota_{l_1}$ , we have  $\mathbf{M}^7.\text{hp}(l_1)(1) = \mathbf{v}$ .

- As  $W^7$  includes  $\iota^{\text{code}}(\text{code}^\bullet)$ , we execute the five instructions from `bg + 6` on the low side and get the following configurations

$$(\Phi^8, \text{alloc}) \quad (M^7.h, K^7[\gamma(\rho, \alpha \mapsto (\tau'_1, \tau'_2, R))e])$$

such that

- $\mathbf{v}' := \mathbf{M}^7.\text{reg}(\text{sv}_0)$
- $\mathbf{M}^8 := \mathbf{M}^7[+\text{kpc}^7, \mathbf{v}']_{\text{stk}}[\text{sv}_0 \mapsto \mathbf{v}]_{\text{reg}}[\text{wk}_0 \mapsto \underline{\text{bg} + c + 11}]_{\text{reg}}$ ,
- $\mathbf{M}^8$  repr  $\Phi^8$ .

- Let  $W^8 := W^7[+\text{kpc}^7, \mathbf{v}']_1[\text{sv}_0 \mapsto \mathbf{v}]_1$ .  
Then  $(\Phi^8, M^7) \in \mathcal{M}(W^8)$ .

- By Theorem 9, it suffices to show that

$$((\Phi^8, \text{bg} + 16), (M^7.h, K^7[\gamma(\rho, \alpha \mapsto (\tau'_1, \tau'_2, R))e])) \in \mathcal{O}(W^8)$$

- 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  $\alpha \notin \text{dom}(\rho)$ , 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

$$((\text{bg} + c + 11, \lfloor \text{wk}_5 \rfloor), K^7[-]) \in \mathcal{K}[\tau]\rho(W^8)$$

- Suppose
  - $W^9 \sqsupseteq_{\text{pub}} W^8$ ,
  - $(\mathbf{v}_1, v_2) \in \mathcal{V}[\![\tau]\!] \rho(W^9)$ ,
  - $(\mathbf{M}^9, M^9) \in \mathcal{M}(W^9)$ ,
  - $\mathbf{M}^9.\text{reg}(\text{wk}_5) = \mathbf{v}_1$ ,
  - $\mathbf{M}^9 \text{ repr } \Phi^9$ .
- 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

- $\mathbf{M}^{10} := \mathbf{M}^9[\text{sv}_0 \mapsto \mathbf{v}']_{\text{reg}[-2]} \text{stk}$ ,
- $\mathbf{M}^{10} \text{ repr } \Phi^{10}$ .

- 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

$$\begin{aligned}
 & \langle \Gamma \vdash e \tau \rangle ::= \text{Pinst}(\langle \Gamma \vdash e \rangle) \\
 & \text{Pinst}(p) ::= \lambda \text{ alloc, bg.} \\
 & \text{let code} := p(\text{alloc}, \text{bg} + 3), \quad c := |\text{code}| \quad \text{in} \quad [ \\
 & \quad \text{bg} \quad \quad \quad \mathbf{plus} \quad \lfloor \text{sp} \rfloor \quad \lfloor \text{sp} \rfloor \quad \underline{1} \\
 & \quad \quad \quad \mathbf{move} \quad \langle \text{sp} - 1 \rangle_s \quad \lfloor \text{wk}_0 \rfloor \\
 & \quad \quad \quad \mathbf{move} \quad \lfloor \text{wk}_0 \rfloor \quad \underline{\text{bg} + c + 3} \\
 & \quad \quad \quad \text{code} \\
 & \quad \text{bg} + c + 3 \quad \mathbf{move} \quad \lfloor \text{wk}_0 \rfloor \quad \langle \text{sp} - 1 \rangle_s \\
 & \quad \quad \quad \mathbf{move} \quad \lfloor \text{wk}_1 \rfloor \quad \lfloor \text{wk}_5 \rfloor \\
 & \quad \quad \quad \mathbf{minus} \quad \lfloor \text{sp} \rfloor \quad \lfloor \text{sp} \rfloor \quad \underline{1} \\
 & \quad \quad \quad \mathbf{jmp} \quad \langle \text{wk}_1 + 0 \rangle_h \\
 & \quad ]
 \end{aligned}$$

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

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

such that

- $\mathbf{M}^4 := \mathbf{M}^3[+\text{kpc}]_{\text{stk}}[\text{wk}_0 \mapsto \text{bg} + c + 3]_{\text{reg}}$ ,
- $\mathbf{M}^4 \text{ repr } \Phi^4$ .

- Let  $W^4 := W^3[+\text{kpc}]_1$ .  
 Then  $(\mathbf{M}^4, M^3) \in \mathcal{M}(W^4)$ .  
 By Theorem 9, it suffices to show that  $((\Phi^4, \text{bg} + 3), (M^3.h, K[(\gamma\rho e) (\rho.2(\tau'))])) \in \mathcal{O}(W^4)$ .

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

- Suppose

$$\begin{aligned} W^5 &\sqsupseteq_{\text{pub}} W^4, \\ (\mathbf{v}_1, v_2) &\in \mathcal{V}[\forall\alpha.\tau]\rho(W^5), \\ (\mathbf{M}^5, M^5) &\in \mathcal{M}(W^5), \\ \mathbf{M}^5.\text{reg}(\text{wk}_5) &= \mathbf{v}_1, \\ \mathbf{M}^5 \text{ repr } \Phi^5. \end{aligned}$$

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

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

Assume that  $\text{lev}(W^5) > 0$ .

- As  $(\mathbf{v}_1, v_2) \in \text{oftype}(\forall\alpha.\tau, \rho)(W^5)$  by Theorems 5 and 4, we have

- $\mathbf{v}_1 = \widehat{\mathbf{l}}_1$ ,
- $\mathbf{M}^5.\text{hp}(\widehat{\mathbf{l}}_1)(0) = \underline{w}$  for some  $w$ ,
- $v_2 = \Lambda\alpha.e_2$  for some  $e_2$ .

- As  $W^5$  includes  $\iota^{\text{code}}(\text{code}^\bullet)$ , we execute the four instructions from  $\text{bg} + c + 3$  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

- $\mathbf{M}^6 := \mathbf{M}^5[\text{wk}_0 \mapsto \text{kpc}]_{\text{reg}}[\text{wk}_1 \mapsto \widehat{\mathbf{l}}_1]_{\text{reg}}[-1]_{\text{stk}}$ ,
- $\mathbf{M}^6 \text{ repr } \Phi^6$ .

- 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

- $W^6 \sqsupseteq_{\triangleright} W^5$  by Lemma 2,
- $(\rho.1(\tau'), \rho.2(\tau'), \mathcal{V}[\tau']\rho) \in \text{WVRel}$ .

Thus from  $(\widehat{\mathbf{l}}_1, \Lambda\alpha.e_2) \in \mathcal{V}[\forall\alpha.\tau]\rho(W^5)$ , we have

- $((\widehat{\mathbf{l}}_1 : 0)_{\text{h}}, \lfloor \text{wk}_0 \rfloor, \lfloor \text{wk}_5 \rfloor, \{\mathbf{M} \mid \mathbf{M}.\text{reg}(\text{wk}_1) = \widehat{\mathbf{l}}_1\}, e_2[\rho.2(\tau')/\alpha]) \in \mathcal{E}[\tau](\rho, \alpha \mapsto (\rho.1(\tau'), \rho.2(\tau'), \mathcal{V}[\tau']\rho))(W^6)$ .

- 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

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

- 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  $((\text{kpc}, \lfloor \text{wk}_5 \rfloor), K) \in \mathcal{K}[\tau[\tau'/\alpha]]\rho(W^6)$ , which follows from  $((\text{kpc}, \lfloor \text{wk}_5 \rfloor), K) \in \mathcal{K}[\tau[\tau'/\alpha]]\rho(W^3)$  and  $W^6 \sqsupseteq_{\text{pub}} W^3$  by Theorem 6.

□

## 9.10 Pack

$$\begin{aligned} (\Gamma \vdash \text{pack } \langle \tau_1, e \rangle \text{ as } \tau_2) &::= \text{Ppack}((\Gamma \vdash e)) \\ \text{Ppack}(p) &::= p \end{aligned}$$

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

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

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

- 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

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

- By definition of  $\mathcal{V}[\exists \alpha. \tau]\rho$  and instantiating  $\alpha$  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

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

$$\text{Punpack}(p_1, p_2) := \lambda \text{ alloc, bg.}$$

$$\text{let instrs}_1 := p_1(\text{alloc, bg} + 3), \quad c_1 := |\text{instrs}_1|,$$

$$\text{instrs}_2 := p_2(\text{alloc, bg} + c_1 + 11), \quad c_2 := |\text{instrs}_2| \quad \text{in } [$$

bg	<b>plus</b>	$\lfloor \text{sp} \rfloor$	$\lfloor \text{sp} \rfloor$	<u>1</u>
	<b>move</b>	$\langle \text{sp} - 1 \rangle_s$	$\lfloor \text{wk}_0 \rfloor$	
	<b>move</b>	$\lfloor \text{wk}_0 \rfloor$	<u><math>\text{bg} + c_1 + 3</math></u>	
	$\text{instrs}_1$			
$\text{bg} + c_1 + 3$	<b>move</b>	$\lfloor \text{wk}_3 \rfloor$	$\lfloor \text{wk}_5 \rfloor$	
	<b>move</b>	$\lfloor \text{wk}_4 \rfloor$	<u><math>\text{bg} + c_1 + 7</math></u>	
	<b>move</b>	$\lfloor \text{wk}_5 \rfloor$	<u>2</u>	
	<b>jmp</b>	<u>alloc</u>		
$\text{bg} + c_1 + 7$	<b>move</b>	$\langle \text{wk}_5 + 0 \rangle_h$	$\lfloor \text{wk}_3 \rfloor$	
	<b>move</b>	$\langle \text{wk}_5 + 1 \rangle_h$	$\lfloor \text{sv}_0 \rfloor$	
	<b>move</b>	$\lfloor \text{sv}_0 \rfloor$	$\lfloor \text{wk}_5 \rfloor$	
	<b>move</b>	$\lfloor \text{wk}_0 \rfloor$	<u><math>\text{bg} + c_1 + c_2 + 11</math></u>	
	$\text{instrs}_2$			
$\text{bg} + c_1 + c_2 + 11$	<b>move</b>	$\lfloor \text{sv}_0 \rfloor$	$\langle \text{sv}_0 + 1 \rangle_h$	
	<b>minus</b>	$\lfloor \text{sp} \rfloor$	$\lfloor \text{sp} \rfloor$	<u>1</u>
	<b>jmp</b>	$\langle \text{sp} - 0 \rangle_s$		

]

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

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

*Proof.*

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

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

- Goal: find  $W^{pe}$  such that
  - $W^{pe} \sqsupseteq W \wedge \text{lev}(W^{pe}) = \text{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta; \Gamma \vdash \text{bg} \approx_{W^{pe}} \text{unpack } e_1 \text{ as } \langle \alpha, x \rangle \text{ in } e_2 : \tau_2$
- Let  $\mathbf{M}^1 := \mathbf{M} \uplus \{\text{code}^\bullet\}_{\text{code}}$ .  
Let  $W^1 := W \uparrow \iota^{\text{code}}(\text{code}^\bullet)$ .  
By definition, we have  $(\mathbf{M}^1, M) \in \mathcal{M}(W^1)$ .
- Let  $\mathbf{M}^2 := \mathbf{M}^1 \uplus \{\text{code}^{p_1}\}_{\text{code}}$ .  
From  $\Delta; \Gamma \vdash p_1 \approx e_1 : \exists \alpha. \tau_1$ , we have  $W^2$  such that
  - $W^2 \sqsupseteq W^1 \wedge \text{lev}(W^2) = \text{lev}(W^1)$
  - $(\mathbf{M}^2, M) \in \mathcal{M}(W^2)$
  - $(*) \Delta; \Gamma \vdash \text{bg} + 3 \approx_{W^2} e_1 : \exists \alpha. \tau_1$
- Let  $\mathbf{M}^3 := \mathbf{M}^2 \uplus \{\text{code}^{p_2}\}_{\text{code}}$ .  
From  $\Delta, \alpha; \Gamma, x : \tau_1 \vdash p_2 \approx e_2 : \tau_2$ , we have  $W^3$  such that
  - $W^3 \sqsupseteq W^2 \wedge \text{lev}(W^3) = \text{lev}(W^2)$
  - $(\mathbf{M}^3, M) \in \mathcal{M}(W^3)$
  - $(**) \Delta, \alpha; \Gamma, x : \tau_1 \vdash \text{bg} + c_1 + 11 \approx_{W^3} e_2 : \tau_2$
- We now choose  $W^{pe}$  to be  $W^3$  and show the required properties.
- $W^3 \sqsupseteq W \wedge \text{lev}(W^3) = \text{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^3)$  holds vacuously.
- To show:  $\forall W^4 \sqsupseteq W^3. \forall \rho \in \mathcal{D}[\Delta]. \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\Gamma]\rho(W^4)$ .  
 $((\text{bg}, [\text{wk}_0], [\text{wk}_5], \{\mathbf{M} \mid \mathbf{M}.\text{reg}(\text{sv}_0) = \mathbf{v}\}), \gamma\rho(\text{unpack } e_1 \text{ as } \langle \alpha, x \rangle \text{ in } e_2)) \in \mathcal{E}[\tau_2]\rho(W^4)$
- By definition of  $\mathcal{E}[\tau_2]\rho(W^4)$  and `plugc`, we suppose
  - $((\text{kpc}, [\text{wk}_5]), K) \in \mathcal{K}[\tau_2]\rho(W^4)$ ,
  - $(\mathbf{M}^4, M^4) \in \mathcal{M}(W^4)$ ,
  - $\mathbf{M}^4 \text{ repr } \Phi^4$ ,
  - $\mathbf{M}^4.\text{reg}(\text{wk}_0) = \text{kpc}$ ,
  - $\mathbf{M}^4.\text{reg}(\text{sv}_0) = \mathbf{v}$ .
- To show:  $((\Phi^4, \text{bg}), (M^4.h, K[\gamma\rho(\text{unpack } e_1 \text{ as } \langle \alpha, x \rangle \text{ in } e_2)])) \in \mathcal{O}(W^4)$
- As  $W^4$  includes  $\iota^{\text{code}}(\text{code}^\bullet)$ , we execute the three instructions from `bg` on the low side and get the configurations

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

such that

- $\mathbf{M}^5 := \mathbf{M}^4 \uparrow \uparrow \text{kpc} \uparrow \text{stk}[\text{wk}_0 \mapsto \text{bg} + c_1 + 3]_{\text{reg}}$ ,
- $\mathbf{M}^5 \text{ repr } \Phi^5$ .



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

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

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

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

- Suppose

$$\begin{aligned} &W^6 \sqsupseteq_{\text{pub}} W^5, \\ &(\mathbf{v}_1, v_2) \in \mathcal{V}[\exists\alpha. \tau_1]\rho(W^6), \\ &(\mathbf{M}^6, M^6) \in \mathcal{M}(W^6), \\ &\mathbf{M}^6.\text{reg}(\text{wk}_5) = \mathbf{v}_1, \\ &\mathbf{M}^6 \text{ repr } \Phi^6. \end{aligned}$$

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

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

such that

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

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

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

such that

$$\begin{aligned} - \mathbf{M}^8 &:= \mathbf{M}^7[[T, S]][\text{wk}_4 \mapsto \underline{w}]_{\text{reg}}[\text{wk}_5 \mapsto \widehat{\mathbf{l}}_2]_{\text{reg}} \uplus \{[\mathbf{l}_2 \mapsto (\underline{w}_0, \underline{w}_1)]\}_{\text{heap}} \text{ for some } w, \mathbf{l}_2, w_0, w_1, \\ - \mathbf{M}^8 &\in \mathcal{A}.GR(\text{gcbg}) \wedge \mathbf{M}^8 \in \mathcal{A}.MR(\text{gcbg}), \\ - \mathbf{M}^8 &\text{ repr } \Phi^8. \end{aligned}$$

- As  $(\mathbf{v}_1, v_2) \in \mathcal{V}[\exists\alpha. \tau_1]\rho(W^6)$ , we have

$$\begin{aligned} - (\tau'_1, \tau'_2, R) &\in \text{TyValRel} \\ - \rho' &:= \rho[\alpha \mapsto (\tau'_1, \tau'_2, R)] \\ - (\mathbf{u}_1, u_2) &\in \mathcal{V}[\tau_1]\rho'(W^6) \\ - \mathbf{v}_1 &= \mathbf{u}_1 \\ - v_2 &= \text{pack } \langle \tau'_2, u_2 \rangle \text{ as } \exists\alpha. \rho.2(\tau_1) \end{aligned}$$

- 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

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

- Let  $W^9 := W^6[\text{sv}_0 \mapsto \widehat{\mathbf{l}}_2]_1 \uparrow \uparrow u_2$ .  
Let  $u_2 := \iota^{\text{single}}(MR_{\mathbf{l}_2}, \emptyset)$ .  
Let  $MR_{\mathbf{l}_2} := \{ (W, \mathbf{M}, M) \mid \mathbf{M}.\text{hp}(\mathbf{l}_2)(0) = \mathbf{v}_1 \wedge \mathbf{M}.\text{hp}(\mathbf{l}_2)(1) = \mathbf{v} \}$ .  
Then  $(\Phi^9, M^6) \in \mathcal{M}(W^9)$ .

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

- As  $(\gamma\rho e_2)[\tau_2'/\alpha][u_2/x] = \gamma'\rho'e_2$ , by Theorem 9, it suffices to show that

$$((\Phi^9, \text{bg} + c_1 + 11), (M^9.h, K[\gamma'\rho'e_2])) \in \mathcal{O}(W^9)$$

- Thus, by (\*\*), it suffices to show that

$$((\text{bg} + c_1 + c_2 + 11, [\text{wk}_5]), K[-]) \in \mathcal{K}[\tau_2]\rho'(W^9)$$

- Suppose  
 $W^{10} \sqsupseteq_{\text{pub}} W^9$ ,  
 $(\mathbf{v}'_1, v'_2) \in \mathcal{V}[\tau_2]\rho'(W^{10})$ ,  
 $(\mathbf{M}^{10}, M^{10}) \in \mathcal{M}(W^{10})$ ,  
 $\mathbf{M}^{10}.\text{reg}(\text{wk}_5) = \mathbf{v}'_1$ ,  
 $\mathbf{M}^{11}$  repr  $\Phi^{10}$ .

- To show:  $((\Phi^{10}, \text{bg} + c_1 + c_2 + 11), (M^{10}.h, K[v'_2])) \in \mathcal{O}(W^{10})$

- As  $W^{10}$  includes  $\iota^{\text{code}}(\text{code}^\bullet)$ , we execute the three instructions from  $\text{bg} + c_1 + c_2 + 11$  on the low side and get the configurations

$$(\Phi^{11}, \text{kpc}), \quad (M^{10}.h, K[v'_2])$$

such that

- $\mathbf{M}^{11} := \mathbf{M}^{10}[\text{sv}_0 \mapsto \mathbf{v}]_{\text{reg}}[-1]_{\text{stk}}$ ,
- $\mathbf{M}^{11}$  repr  $\Phi^{11}$ .

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

- By Theorem 9, it suffices to show that  $((\Phi^{11}, \text{kpc}), (M^{10}.h, K[v'_2])) \in \mathcal{O}(W^{11})$ .

- As  $W^{11} \sqsupseteq_{\text{pub}} W^4$  and  $((\text{kpc}, [\text{wk}_5]), K) \in \mathcal{K}[\tau_2]\rho'(W^4)$ , 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

$$\begin{aligned} (\Gamma \vdash \text{roll}_\tau e) &::= \text{Proll}((\Gamma \vdash e)) \\ \text{Proll}(p) &::= p \end{aligned}$$

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

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

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

- 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

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

- By Theorem 3, we have

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

- 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

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

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

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

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

*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
  - $W^{pe} \sqsupseteq W \wedge \text{lev}(W^{pe}) = \text{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta; \Gamma \vdash \text{bg} \approx_{W^{pe}} \text{unroll } e : \tau[\mu\alpha. \tau/\alpha]$
- 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:  $\forall W^2 \sqsupseteq W^1. \forall \rho \in \mathcal{D}[\Delta]. \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\Gamma]\rho(W^2).$   
 $((\text{bg}, \lfloor \text{wk}_0 \rfloor, \lfloor \text{wk}_5 \rfloor, \{ \mathbf{M} \mid \mathbf{M}.\text{reg}(\text{sv}_0) = \mathbf{v} \}), \gamma\rho(\text{unroll } e)) \in \mathcal{E}[\tau[\mu\alpha. \tau/\alpha]]\rho(W^2)$

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

- To show:  $((\Phi^3, \text{kpc}), (M^3.h, K[\text{unroll } v_2])) \in \mathcal{O}(W^3)$
- By Theorem 3, we have

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

- Thus we have
  - $v_2 = \text{roll}_{\mu\alpha.\tau} u_2$  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  $v_2 = \text{roll}_{\mu\alpha.\tau} u_2$ , we take one step on the high side and get the following configurations:

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

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

$$\begin{aligned}
& (\Gamma \vdash \text{ref } e) ::= \text{Pnew}((\Gamma \vdash e)) \\
& \text{Pnew}(p) ::= \lambda \text{ alloc, bg.} \\
& \text{let code} := p(\text{alloc, bg} + 3), c := |\text{code}| \text{ in } [ \\
& \quad \text{bg} \quad \text{plus} \quad \frac{[\text{sp}]}{\langle \text{sp} - 1 \rangle_s} \quad \frac{[\text{sp}]}{[\text{wk}_0]} \quad \underline{1} \\
& \quad \quad \text{move} \quad \frac{[\text{wk}_0]}{\text{bg} + c + 3} \\
& \quad \quad \text{code} \\
& \quad \text{bg} + c + 3 \quad \text{move} \quad \frac{[\text{wk}_3]}{[\text{wk}_5]} \quad \frac{[\text{wk}_5]}{\text{bg} + c + 7} \\
& \quad \quad \text{move} \quad \frac{[\text{wk}_4]}{\underline{1}} \\
& \quad \quad \text{move} \quad \frac{[\text{wk}_5]}{\underline{1}} \\
& \quad \quad \text{jmp} \quad \underline{\text{alloc}} \\
& \quad \text{bg} + c + 7 \quad \text{move} \quad \frac{\langle \text{wk}_5 + 0 \rangle_h}{[\text{sp}]} \quad \frac{[\text{wk}_3]}{[\text{sp}]} \quad \underline{1} \\
& \quad \quad \text{minus} \quad \frac{[\text{sp}]}{\langle \text{sp} - 0 \rangle_s} \\
& \quad \quad \text{jmp} \quad \langle \text{sp} - 0 \rangle_s \\
& ]
\end{aligned}$$

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

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

*Proof.*

- For any  $\mathcal{A}$ ,  $\text{gcbg}$ ,  $\text{bg}$ ,  $k$ , suppose
  - $W \sqsupseteq W_k^o(\mathcal{A}, \text{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$
  - $\text{code} := [\text{bg} \Rightarrow \text{Pnew}(p)(\mathcal{A}(\text{gcbg}).\text{alloc}, \text{bg})]$
  - $\text{code}^p := [\text{bg} + 3 \Rightarrow p(\mathcal{A}(\text{gcbg}).\text{alloc}, \text{bg} + 3)]$ ,  $c := |\text{code}^p|$
  - $\text{code}^\bullet := \text{code} \setminus \text{code}^p$
  - $\mathbf{M}' = \mathbf{M} \uplus \{\text{code}\}_{\text{code}}$ .
- Goal: find  $W^{pe}$  such that
  - $W^{pe} \sqsupseteq W \wedge \text{lev}(W^{pe}) = \text{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta; \Gamma \vdash \text{bg} \approx_{W^{pe}} \text{ref } e : \text{ref } \tau$
- Let  $\mathbf{M}^1 := \mathbf{M} \uplus \{\text{code}^\bullet\}_{\text{code}}$ .  
Let  $W^1 := W \uparrow \iota^{\text{code}}(\text{code}^\bullet)$ .  
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  $\Delta; \Gamma \vdash p \approx e : \tau$ , we have  $W^2$  such that
  - $W^2 \sqsupseteq W^1 \wedge \text{lev}(W^2) = \text{lev}(W^1)$
  - $(\mathbf{M}^2, M) \in \mathcal{M}(W^2)$
  - (\*)  $\Delta; \Gamma \vdash \text{bg} + 3 \approx_{W^2} e : \tau$
- 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:  $\forall W^3 \sqsupseteq W^2. \forall \rho \in \mathcal{D}[\Delta]. \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\Gamma]\rho(W^3).$   
 $((\text{bg}, \lfloor \text{wk}_0 \rfloor, \lfloor \text{wk}_5 \rfloor, \{ \mathbf{M} \mid \mathbf{M}.\text{reg}(\text{sv}_0) = \mathbf{v} \}), \gamma\rho(\text{ref } e)) \in \mathcal{E}[\text{ref } \tau]\rho(W^3)$
- By definition of  $\mathcal{E}[\text{ref } \tau]\rho(W^3)$  and *plugs*, we suppose
  - $((\text{kpc}, \lfloor \text{wk}_5 \rfloor), K) \in \mathcal{K}[\text{ref } \tau]\rho(W^3),$
  - $(\mathbf{M}^3, M^3) \in \mathcal{M}(W^3),$
  - $\mathbf{M}^3 \text{ repr } \Phi^3,$
  - $\mathbf{M}^3.\text{reg}(\text{wk}_0) = \text{kpc},$
  - $\mathbf{M}^3.\text{reg}(\text{sv}_0) = \mathbf{v}.$
- To show:  $((\Phi^3, \text{bg}), (M^3.h, K[\gamma\rho(\text{ref } e)])) \in \mathcal{O}(W^3)$
- 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
$$(\Phi^4, \text{bg} + 3), \quad (M^3.h, K[\text{ref } \gamma\rho e])$$
such that
  - $\mathbf{M}^4 := \mathbf{M}^3[+\text{kpc}]_{\text{stk}}[\text{wk}_0 \mapsto \text{bg} + c + 3]_{\text{reg}},$
  - $\mathbf{M}^4 \text{ repr } \Phi^4.$
- Let  $W^4 := W^3[+\text{kpc}]_1.$   
Then  $(\mathbf{M}^4, M^3) \in \mathcal{M}(W^4).$   
By Theorem 9, it suffices to show that  $((\Phi^4, \text{bg} + 3), (M^3.h, K[\text{ref } \gamma\rho e])) \in \mathcal{O}(W^4).$
- By (\*), it suffices to show that  $((\text{bg} + c + 3, \lfloor \text{wk}_5 \rfloor), K[\text{ref } -]) \in \mathcal{K}[\tau]\rho(W^4).$
- Suppose
$$W^5 \sqsupseteq_{\text{pub}} W^4,$$

$$(\mathbf{v}_1, v_2) \in \mathcal{V}[\tau]\rho(W^5),$$

$$(\mathbf{M}^5, M^5) \in \mathcal{M}(W^5),$$

$$\mathbf{M}^5.\text{reg}(\text{wk}_5) = \mathbf{v}_1,$$

$$\mathbf{M}^5 \text{ repr } \Phi^5.$$
- To show:  $((\Phi^5, \text{bg} + c + 3), (M^5.h, K[\text{ref } v_2])) \in \mathcal{O}(W^5)$
- As  $W^5$  includes  $\iota^{\text{code}}(\text{code}^\bullet)$ , we execute the four instructions from *bg* + *c* + 3 on the low side and get the configurations
$$(\Phi^6, \text{alloc}), \quad (M^5.h, K[\text{ref } v_2])$$
such that
  - $\mathbf{M}^6 := \mathbf{M}^5[\text{wk}_3 \mapsto \mathbf{v}_1]_{\text{reg}}[\text{wk}_4 \mapsto \text{bg} + c + 7]_{\text{reg}}[\text{wk}_5 \mapsto \underline{1}]_{\text{reg}},$
  - $\mathbf{M}^6 \text{ repr } \Phi^6.$
- By the specifications of  $\mathcal{A}$ , after some finite number of steps of execution, we have configurations
$$(\Phi^7, \text{bg} + c + 7), \quad (M^5.h, K[\text{ref } v_2])$$
such that
  - $\mathbf{M}^7 := \mathbf{M}^6[[T, S]][\text{wk}_4 \mapsto \underline{w}]_{\text{reg}}[\text{wk}_5 \mapsto \widehat{\mathbf{l}}_1]_{\text{reg}} \uplus \{[\mathbf{l}_1 \mapsto (\underline{w}_0)]\}_{\text{heap}}$  for some  $w, \mathbf{l}_1, w_0,$
  - $\mathbf{M}^7 \in \mathcal{A}.\text{GR}(\text{gcbg}) \wedge \mathbf{M}^7 \in \mathcal{A}.\text{MR}(\text{gcbg}),$
  - $\mathbf{M}^7 \text{ repr } \Phi^7.$

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

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

such that

- $\mathbf{M}^8 := \mathbf{M}^7[l_1 : 0 \mapsto \mathbf{v}_1]_{\text{hp}}[-1]_{\text{stk}}$
- $\mathbf{M}^8 \text{ repr } \Phi^8$
- $M^8 := (M^5.h \uplus [\ell_2 \mapsto v_2], \{M^5.\Sigma, \ell_2 : \tau\})$

- Let  $W^8 := W^5[-1]_1 \uparrow \uparrow u_{1, \ell_2}$ .  
Let  $MR_{l_1, \ell_2} := \{(W, \mathbf{M}, M) \mid (W, \mathbf{M}.\text{hp}(l_1)(0), M.h(\ell_2)) \in \mathcal{V}[\tau]\rho\}$   
Let  $Bij_{l_1, \ell_2} := \{(\widehat{l}_1, \ell_2)\}$   
Let  $u_{1, \ell_2} := \iota^{\text{single}}(MR_{l_1, \ell_2}, Bij_{l_1, \ell_2})$ .  
It is easy to check that  $u_{1, \ell_2}$  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  $((\Phi^8, \text{kpc}), (M^8.h, K[\ell_2])) \in \mathcal{O}(W^8)$ .
- As  $W^8 \sqsupseteq_{\text{pub}} W^3$  and  $((\text{kpc}, [\text{wk}_5]), K) \in \mathcal{K}[\text{ref } \tau]\rho(W^3)$ , it suffices to show that

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

- By definition of  $\mathcal{V}[\text{ref } \tau]\rho(W^8)$ , for all  $W^9 \sqsupseteq W^8$  and  $(\mathbf{M}, M) \in \mathcal{M}(W^9)$ , it suffices to show that
  - $(\widehat{l}_1, \ell_2) \in \mathcal{B}(W^9)$  : trivial as  $W^9$  includes  $u_{1, \ell_2}$ .
  - $\exists(\mathbf{u}_1, u_2) \in \triangleright \mathcal{V}[\tau]\rho(W^9)$ .  $(\widehat{l}_1, \mathbf{M}) \in \mathcal{L}.\text{ref}(\mathbf{u}_1) \wedge (\ell_2, M) \in \mathcal{H}.\text{ref}(u_2)$  : trivial as  $W^9$  includes  $u_{1, \ell_2}$ .
  - $\forall(\mathbf{u}_1, u_2) \in \triangleright \mathcal{V}[\tau]\rho(W^9)$ .  $(\mathcal{L}.\text{asgn}(\mathbf{M}, \widehat{l}_1, \mathbf{u}_1), \mathcal{H}.\text{asgn}(M, \ell_2, u_2)) \in \mathcal{M}(W^9)$  : trivial as  $W^9$  includes  $u_{1, \ell_2}$ .

□



## 9.15 Asgn

$$\begin{aligned}
& (\Gamma \vdash e_1 := e_2) ::= \text{Pasgn}(\langle \Gamma \vdash e_1 \rangle, \langle \Gamma \vdash e_2 \rangle) \\
& \text{Pasgn}(p_1, p_2) ::= \lambda \text{ alloc, bg.} \\
& \text{let instrs}_1 := p_1(\text{alloc, bg} + 4), c_1 := |\text{instrs}_1|, \\
& \quad \text{instrs}_2 := p_2(\text{alloc, bg} + c_1 + 6), c_2 := |\text{instrs}_2| \text{ in } [ \\
& \quad \text{bg} \quad \quad \quad \text{plus} \quad \langle \text{sp} \rangle \quad \quad \langle \text{sp} \rangle \quad \quad \underline{\quad} \\
& \quad \quad \quad \text{move} \quad \langle \text{sp} - 2 \rangle_s \quad \langle \text{wk}_0 \rangle \\
& \quad \quad \quad \text{move} \quad \langle \text{sp} - 1 \rangle_s \quad \underline{0} \\
& \quad \quad \quad \text{move} \quad \langle \text{wk}_0 \rangle \quad \underline{\text{bg} + c_1 + 4} \\
& \quad \quad \quad \text{instrs}_1 \\
& \quad \text{bg} + c_1 + 4 \quad \text{move} \quad \langle \text{sp} - 1 \rangle_s \quad \langle \text{wk}_5 \rangle \\
& \quad \quad \quad \text{move} \quad \langle \text{wk}_0 \rangle \quad \underline{\text{bg} + c_1 + c_2 + 6} \\
& \quad \quad \quad \text{instrs}_2 \\
& \quad \text{bg} + c_1 + c_2 + 6 \quad \text{move} \quad \langle \text{wk}_3 \rangle \quad \langle \text{sp} - 1 \rangle_s \\
& \quad \quad \quad \text{move} \quad \langle \text{wk}_3 + 0 \rangle_h \quad \langle \text{wk}_5 \rangle \\
& \quad \quad \quad \text{minus} \quad \langle \text{sp} \rangle \quad \langle \text{sp} \rangle \quad \quad \underline{\quad} \\
& \quad \quad \quad \text{jmp} \quad \langle \text{sp} - 0 \rangle_s \\
& \quad ]
\end{aligned}$$

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

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

*Proof.*

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

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

such that

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

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

such that

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

- Let  $W^7 := W^6[|\mathbf{M}^7.\text{stk}| - 1 \mapsto \mathbf{v}_1]_1$ .  
Then  $(\mathbf{M}^7, M^6) \in \mathcal{M}(W^7)$ .  
By Theorem 9, it suffices to show that  $((\Phi^7, \text{bg} + c_1 + 6), (M^6.h, K[v_2 := \gamma\rho e_2])) \in \mathcal{O}(W^7)$ .
- By (\*\*), it suffices to show that  $((\text{bg} + c_1 + c_2 + 6, \lfloor \text{wk}_5 \rfloor), K[v_2 := -]) \in \mathcal{K}[\tau]\rho(W^7)$ .

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

- To show:  $((\Phi^8, \text{bg} + c_1 + c_2 + 6), (M^8.h, K[v_2 := v_4])) \in \mathcal{O}(W^8)$
- As  $(\mathbf{v}_1, v_2) \in \mathcal{V}[\text{ref } \tau]\rho(W^6)$  and  $W^8 \supseteq W^6$ ,  
-  $\mathbf{v}_1 = \hat{\mathbf{l}}_1$ ,  $\mathbf{M}^8.\text{hp}(\hat{\mathbf{l}}_1)(0) = \mathbf{u}_1$  for some  $\mathbf{l}_1, \mathbf{u}_1$   
-  $v_2 = \ell_2$ ,  $M^8.h(\ell_2) = u_2$  for some  $\ell_2, u_2$   
-  $(\mathbf{u}_1, u_2) \in \triangleright\mathcal{V}[\tau]\rho(W^8)$
- As  $W^8$  includes  $\iota^{\text{code}}(\text{code}^\bullet)$ , we execute the four instructions from  $\text{bg} + c_1 + c_2 + 6$  on the low side, take one step on the high side and get the configurations

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

such that

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

- Let  $W^9 := W^8[-2]_1$ .  
Then,  $(\mathbf{M}^8[-2]_{\text{stk}}, M^8) \in \mathcal{M}(W^9)$ .
- As  $(\hat{\mathbf{l}}_1, \ell_2) \in \mathcal{V}[\text{ref } \tau]\rho(W^6)$ ,  $W^9 \supseteq W^6$ ,  $(\mathbf{v}_3, v_4) \in \triangleright\mathcal{V}[\tau]\rho(W^9)$ ,  $\mathbf{M}^9 = \mathcal{L}.\text{asgn}(\mathbf{M}^8[-2]_{\text{stk}}, \hat{\mathbf{l}}_1, \mathbf{v}_3)$   
and  $M^9 = \mathcal{H}.\text{asgn}(M^8, \ell_2, v_4)$ ,  
-  $(\mathbf{M}^9, M^9) \in W^9$
- By Theorem 9, it suffices to show that  $((\Phi^9, \text{kpc}), (M^9.h, K[\langle \rangle])) \in \mathcal{O}(W^9)$ .
- As  $W^9 \sqsupseteq_{\text{pub}} W^4$  and  $((\text{kpc}, \lfloor \text{wk}_5 \rfloor), K) \in \mathcal{K}[\text{unit}]\rho(W^4)$ , it suffices to show that

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

which trivially holds by definition.

□

## 9.16 Deref

$$\begin{aligned}
& (\Gamma \vdash !e) ::= \text{Pderef}((\Gamma \vdash e)) \\
& \text{Pderef}(p) ::= \lambda \text{ alloc, bg.} \\
& \text{let code} := p(\text{alloc, bg} + 3), c := |\text{code}| \text{ in } [ \\
& \quad \text{bg} \quad \quad \text{plus} \quad [\text{sp}] \quad \quad [\text{sp}] \quad \quad \underline{1} \\
& \quad \quad \quad \text{move} \quad \langle \text{sp} - 1 \rangle_s \quad [\text{wk}_0] \\
& \quad \quad \quad \text{move} \quad [\text{wk}_0] \quad \quad \underline{\text{bg} + c + 3} \\
& \quad \quad \quad \text{code} \\
& \quad \text{bg} + c + 3 \quad \text{move} \quad [\text{wk}_5] \quad \quad \langle \text{wk}_5 + 0 \rangle_h \\
& \quad \quad \quad \text{minus} \quad [\text{sp}] \quad \quad [\text{sp}] \quad \quad \underline{1} \\
& \quad \quad \quad \text{jmp} \quad \quad \langle \text{sp} - 0 \rangle_s \\
& ]
\end{aligned}$$

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

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

*Proof.*

- For any  $\mathcal{A}$ , gcbg, bg,  $k$ , suppose
  - $W \sqsupseteq W_k^o(\mathcal{A}, \text{gcbg}) \wedge (\mathbf{M}, M) \in \mathcal{M}(W)$
  - $\text{code} := [\text{bg} \Rightarrow \text{Pderef}(p)(\mathcal{A}(\text{gcbg}).\text{alloc}, \text{bg})]$
  - $\text{code}^p := [\text{bg} + 3 \Rightarrow p(\mathcal{A}(\text{gcbg}).\text{alloc}, \text{bg} + 3)]$ ,  $c := |\text{code}^p|$
  - $\text{code}^\bullet := \text{code} \setminus \text{code}^p$
  - $\mathbf{M}' = \mathbf{M} \uplus \{\text{code}\}_{\text{code}}$ .
- Goal: find  $W^{pe}$  such that
  - $W^{pe} \sqsupseteq W \wedge \text{lev}(W^{pe}) = \text{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta; \Gamma \vdash \text{bg} \approx_{W^{pe}} !e : \tau$
- Let  $\mathbf{M}^1 := \mathbf{M} \uplus \{\text{code}^\bullet\}_{\text{code}}$ .  
Let  $W^1 := W \uparrow \iota^{\text{code}}(\text{code}^\bullet)$ .  
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  $\Delta; \Gamma \vdash p \approx e : \text{ref } \tau$ , we have  $W^2$  such that
  - $W^2 \sqsupseteq W^1 \wedge \text{lev}(W^2) = \text{lev}(W^1)$
  - $(\mathbf{M}^2, M) \in \mathcal{M}(W^2)$
  - (\*)  $\Delta; \Gamma \vdash \text{bg} + 3 \approx_{W^2} e : \text{ref } \tau$
- 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:  $\forall W^3 \sqsupseteq W^2. \forall \rho \in \mathcal{D}[\Delta]. \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\Gamma]\rho(W^3)$ .  
 $((\underline{\text{bg}}, [\text{wk}_0], [\text{wk}_5], \{\mathbf{M} \mid \mathbf{M}.\text{reg}(\text{sv}_0) = \mathbf{v}\}), \gamma\rho(!e)) \in \mathcal{E}[\tau]\rho(W^3)$

- By definition of  $\mathcal{E}[\tau]\rho(W^3)$  and `plugc`, we suppose
  - $((\text{kpc}, \lfloor \text{wk}_5 \rfloor), K) \in \mathcal{K}[\tau]\rho(W^3)$ ,
  - $(\mathbf{M}^3, M^3) \in \mathcal{M}(W^3)$ ,
  - $\mathbf{M}^3 \text{ repr } \Phi^3$ ,
  - $\mathbf{M}^3.\text{reg}(\text{wk}_0) = \text{kpc}$ ,
  - $\mathbf{M}^3.\text{reg}(\text{sv}_0) = \mathbf{v}$ .
- To show:  $((\Phi^3, \text{bg}), (M^3.h, K[\gamma\rho(!e)])) \in \mathcal{O}(W^3)$
- 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

$$(\Phi^4, \text{bg} + 3), \quad (M^3.h, K[!\gamma\rho e])$$

such that

- $\mathbf{M}^4 := \mathbf{M}^3[+\text{kpc}]_{\text{stk}}[\text{wk}_0 \mapsto \text{bg} + c + 3]_{\text{reg}}$ ,
- $\mathbf{M}^4 \text{ repr } \Phi^4$ .

- Let  $W^4 := W^3[+\text{kpc}]_1$ .  
Then  $(\mathbf{M}^4, M^3) \in \mathcal{M}(W^4)$ .  
By Theorem 9, it suffices to show that  $((\Phi^4, \text{bg} + 3), (M^3.h, K[!\gamma\rho e])) \in \mathcal{O}(W^4)$ .
- By (\*), it suffices to show that  $((\text{bg} + c + 3, \lfloor \text{wk}_5 \rfloor), K[!-]) \in \mathcal{K}[\text{ref } \tau]\rho(W^4)$ .

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

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

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

- As  $(\mathbf{v}_1, v_2) \in \mathcal{V}[\text{ref } \tau]\rho(W^5)$ 
  - $\mathbf{v}_1 = \widehat{\mathbf{l}}_1$ ,  $\mathbf{M}^5.\text{hp}(\mathbf{l}_1)(0) = \mathbf{u}_1$  for some  $\mathbf{l}_1, \mathbf{u}_1$
  - $v_2 = \ell_2$ ,  $M^5.h(\ell_2) = u_2$  for some  $\ell_2, u_2$
  - $(\mathbf{u}_1, u_2) \in \triangleright\mathcal{V}[\tau]\rho(W^5)$

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

$$(\Phi^6, \text{kpc}), \quad (M^6.h, K[u_2])$$

such that

- $\mathbf{M}^6 := \mathbf{M}^5[\text{wk}_5 \mapsto \mathbf{u}_1]_{\text{reg}}[-1]_{\text{stk}}$ ,
- $\mathbf{M}^6 \text{ repr } \Phi^6$ ,
- $M^6 := M^5$ .

- 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  $((\Phi^6, \text{kpc}), (M^6.h, K[u_2])) \in \mathcal{O}(W^6)$ .
- As  $W^6 \sqsupseteq_{\text{pub}} W^3$  and  $((\text{kpc}, [\text{wk}_5]), K) \in \mathcal{K}[\tau]\rho(W^3)$ , 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

$$(\Gamma \vdash e_1 == e_2) ::= \text{Prefeq}((\Gamma \vdash e_1), (\Gamma \vdash e_2))$$

$$\text{Prefeq}(p_1, p_2) ::= \lambda \text{ alloc, bg.}$$

$$\text{let instrs}_1 := p_1(\text{alloc, bg} + 4), \quad c_1 := |\text{instrs}_1|,$$

$$\text{instrs}_2 := p_2(\text{alloc, bg} + c_1 + 6), \quad c_2 := |\text{instrs}_2| \quad \text{in } [$$

bg	plus	$[\text{sp}]$	$[\text{sp}]$	<u>2</u>
	move	$\langle \text{sp} - 2 \rangle_s$	$[\text{wk}_0]$	
	move	$\langle \text{sp} - 1 \rangle_s$	<u>0</u>	
	move	$[\text{wk}_0]$	<u><math>\text{bg} + c_1 + 4</math></u>	
		instrs <sub>1</sub>		
bg + c <sub>1</sub> + 4	move	$\langle \text{sp} - 1 \rangle_s$	$[\text{wk}_5]$	
	move	$[\text{wk}_0]$	<u><math>\text{bg} + c_1 + c_2 + 6</math></u>	
		instrs <sub>2</sub>		
bg + c <sub>1</sub> + c <sub>2</sub> + 6	jneq	<u><math>\text{bg} + c_1 + c_2 + 9</math></u>	$\langle \text{sp} - 1 \rangle_s$	$[\text{wk}_5]$
	move	$[\text{wk}_5]$	<u>1</u>	
	jmp	<u><math>\text{bg} + c_1 + c_2 + 10</math></u>		
bg + c <sub>1</sub> + c <sub>2</sub> + 9	move	$[\text{wk}_5]$	<u>0</u>	
bg + c <sub>1</sub> + c <sub>2</sub> + 10	minus	$[\text{sp}]$	$[\text{sp}]$	<u>2</u>
	jmp	$\langle \text{sp} - 0 \rangle_s$		

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

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

*Proof.*

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

- Goal: find  $W^{pe}$  such that
  - $W^{pe} \sqsupseteq W \wedge \text{lev}(W^{pe}) = \text{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^{pe})$
  - $\Delta; \Gamma \vdash \text{bg} \approx_{W^{pe}} e_1 == e_2 : \text{unit}$
- 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  $\mathbf{M}^2 := \mathbf{M}^1 \uplus \{\text{code}^{p_1}\}_{\text{code}}$ .  
From  $\Delta; \Gamma \vdash p_1 \approx e_1 : \text{ref } \tau$ , we have  $W^2$  such that
  - $W^2 \sqsupseteq W^1 \wedge \text{lev}(W^2) = \text{lev}(W^1)$
  - $(\mathbf{M}^2, M) \in \mathcal{M}(W^2)$
  - $(*) \Delta; \Gamma \vdash \text{bg} + 4 \approx_{W^2} e_1 : \text{ref } \tau$
- Let  $\mathbf{M}^3 := \mathbf{M}^2 \uplus \{\text{code}^{p_2}\}_{\text{code}}$ .  
From  $\Delta; \Gamma \vdash p_2 \approx e_2 : \text{ref } \tau$ , we have  $W^3$  such that
  - $W^3 \sqsupseteq W^2 \wedge \text{lev}(W^3) = \text{lev}(W^2)$
  - $(\mathbf{M}^3, M) \in \mathcal{M}(W^3)$
  - $(**) \Delta; \Gamma \vdash \text{bg} + c_1 + 6 \approx_{W^3} e_2 : \text{ref } \tau$
- We now choose  $W^{pe}$  to be  $W^3$  and show the required properties.
- $W^3 \sqsupseteq W \wedge \text{lev}(W^3) = \text{lev}(W) \wedge (\mathbf{M}', M) \in \mathcal{M}(W^3)$  holds vacuously.
- To show:  $\forall W^4 \sqsupseteq W^3. \forall \rho \in \mathcal{D}[\Delta]. \forall (\mathbf{v}, \gamma) \in \mathcal{G}[\Gamma]\rho(W^4)$ .  
 $((\text{bg}, \lfloor \text{wk}_0 \rfloor, \lfloor \text{wk}_5 \rfloor, \{ \mathbf{M} \mid \mathbf{M}.\text{reg}(\text{sv}_0) = \mathbf{v} \}), \gamma\rho(e_1 == e_2)) \in \mathcal{E}[\text{unit}]\rho(W^4)$
- By definition of  $\mathcal{E}[\text{unit}]\rho(W^4)$  and plugc, we suppose
  - $((\text{kpc}, \lfloor \text{wk}_5 \rfloor), K) \in \mathcal{K}[\text{unit}]\rho(W^4)$ ,
  - $(\mathbf{M}^4, M^4) \in \mathcal{M}(W^4)$ ,
  - $\mathbf{M}^4 \text{ repr } \Phi^4$ ,
  - $\mathbf{M}^4.\text{reg}(\text{wk}_0) = \text{kpc}$ ,
  - $\mathbf{M}^4.\text{reg}(\text{sv}_0) = \mathbf{v}$ .
- To show:  $((\Phi^4, \text{bg}), (M^4.h, K[\gamma\rho(e_1 == e_2)])) \in \mathcal{O}(W^4)$
- As  $W^4$  includes  $\iota^{\text{code}}(\text{code}^\bullet)$ , we execute the four instructions from  $\text{bg}$  on the low side and get the configurations

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

such that

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

- Let  $W^5 := W^4[ ++ \text{kpc}, \underline{0}]_1$ .  
Then  $(\mathbf{M}^5, M^4) \in \mathcal{M}(W^5)$ .  
By Theorem 9, it suffices to show that  $((\Phi^5, \text{bg} + 4), (M^4.h, K[\gamma\rho e_1 == \gamma\rho e_2])) \in \mathcal{O}(W^5)$ .
- By  $(*)$ , it suffices to show that  $((\text{bg} + c_1 + 4, \lfloor \text{wk}_5 \rfloor), K[- == \gamma\rho e_2]) \in \mathcal{K}[\text{ref } \tau]\rho(W^5)$ .

- Suppose
  - $W^6 \sqsupseteq_{\text{pub}} W^5$ ,
  - $(\mathbf{v}_1, v_2) \in \mathcal{V}[\llbracket \text{ref } \tau \rrbracket \rho](W^6)$ ,
  - $(\mathbf{M}^6, M^6) \in \mathcal{M}(W^6)$ ,
  - $\mathbf{M}^6.\text{reg}(\text{wk}_5) = \mathbf{v}_1$ ,
  - $\mathbf{M}^6 \text{ repr } \Phi^6$ .
- To show:  $((\Phi^6, \text{bg} + c_1 + 4), (M^6.h, K[v_2 == \gamma \rho e_2])) \in \mathcal{O}(W^6)$
- As  $W^6$  includes  $\iota^{\text{code}}(\text{code}^\bullet)$ , we execute the two instructions from  $\text{bg} + c_1 + 4$  on the low side and get the configurations

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

such that

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

- Let  $W^7 := W^6[|\mathbf{M}^7.\text{stk}| - 1 \mapsto \mathbf{v}_1]_1$ .  
Then  $(\mathbf{M}^7, M^6) \in \mathcal{M}(W^7)$ .  
By Theorem 9, it suffices to show that  $((\Phi^7, \text{bg} + c_1 + 6), (M^6.h, K[v_2 == \gamma \rho e_2])) \in \mathcal{O}(W^7)$ .
- By (\*\*), it suffices to show that  $((\text{bg} + c_1 + c_2 + 6, \lfloor \text{wk}_5 \rfloor), K[v_2 == -]) \in \mathcal{K}[\llbracket \text{ref } \tau \rrbracket \rho](W^7)$ .

- Suppose
  - $W^8 \sqsupseteq_{\text{pub}} W^7$ ,
  - $(\mathbf{v}_3, v_4) \in \mathcal{V}[\llbracket \text{ref } \tau \rrbracket \rho](W^8)$ ,
  - $(\mathbf{M}^8, M^8) \in \mathcal{M}(W^8)$ ,
  - $\mathbf{M}^8.\text{reg}(\text{wk}_5) = \mathbf{v}_3$ ,
  - $\mathbf{M}^8 \text{ repr } \Phi^8$ .
- To show:  $((\Phi^8, \text{bg} + c_1 + c_2 + 6), (M^8.h, K[v_2 == v_4])) \in \mathcal{O}(W^8)$
- As  $(\mathbf{v}_1, v_2) \in \mathcal{V}[\llbracket \text{ref } \tau \rrbracket \rho](W^6)$  and  $W^8 \sqsupseteq W^6$ ,
  - $(\mathbf{v}_1, v_2) \in \mathcal{B}(W^8)$
  - $v_2$  is a location
- As  $(\mathbf{v}_3, v_4) \in \mathcal{V}[\llbracket \text{ref } \tau \rrbracket \rho](W^8)$ ,
  - $(\mathbf{v}_3, v_4) \in \mathcal{B}(W^8)$
  - $v_4$  is a location
- As  $W^8$  includes  $\iota^{\text{code}}(\text{code}^\bullet)$ , we execute the instructions from  $\text{bg} + c_1 + c_2 + 6$  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.

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

such that

- $\mathbf{M}^9 := \mathbf{M}^8[\text{wk}_5 \mapsto \underline{1}]_{\text{reg}}[-2]_{\text{stk}}$
- $\mathbf{M}^9 \text{ repr } \Phi^9$
- $M^9 := M^8$



- 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  $((\Phi^9, \text{kpc}), (M^9.h, K[\text{tt}])) \in \mathcal{O}(W^9)$ .
- As  $W^9 \sqsupseteq_{\text{pub}} W^4$  and  $((\text{kpc}, [\text{wk}_5]), K) \in \mathcal{K}[\![\text{bool}]\!] \rho(W^4)$ , it suffices to show that

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

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.

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

such that

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

- 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  $((\Phi^9, \text{kpc}), (M^9.h, K[\text{ff}])) \in \mathcal{O}(W^9)$ .
- As  $W^9 \sqsupseteq_{\text{pub}} W^4$  and  $((\text{kpc}, [\text{wk}_5]), K) \in \mathcal{K}[\![\text{bool}]\!] \rho(W^4)$ , it suffices to show that

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

which trivially holds by definition.

□

## 9.18 If

$$(\Gamma \vdash \text{if } e_1 \text{ then } e_2 \text{ else } e_3) ::= \text{Pif}((\Gamma \vdash e_1), (\Gamma \vdash e_2), (\Gamma \vdash e_3))$$

$$\text{Pif}(p_1, p_2, p_3) ::= \lambda \text{ alloc, bg.}$$

$$\text{let instrs}_1 := p_1(\text{alloc, bg} + 3), \quad c_1 := |\text{instrs}_1|,$$

$$\text{instrs}_2 := p_2(\text{alloc, bg} + c_1 + c_3 + 5), \quad c_2 := |\text{instrs}_2|,$$

$$\text{instrs}_3 := p_3(\text{alloc, bg} + c_1 + 5), \quad c_3 := |\text{instrs}_3| \quad \text{in } [$$

bg	<b>plus</b>	[sp]	[sp]	<u>1</u>
	<b>move</b>	$\langle \text{sp} - 1 \rangle_s$	[wk <sub>0</sub> ]	
	<b>move</b>	[wk <sub>0</sub> ]	<u>bg + c<sub>1</sub> + 3</u>	
		instrs <sub>1</sub>		
bg + c <sub>1</sub> + 3	<b>move</b>	[wk <sub>0</sub> ]	<u>bg + c<sub>1</sub> + c<sub>2</sub> + c<sub>3</sub> + 5</u>	
	<b>jnz</b>	bg + c <sub>1</sub> + c <sub>3</sub> + 5	[wk <sub>5</sub> ]	
		instrs <sub>3</sub>		
		instrs <sub>2</sub>		
bg + c <sub>1</sub> + c <sub>2</sub> + c <sub>3</sub> + 5	<b>minus</b>	[sp]	[sp]	<u>1</u>
	<b>jmp</b>	$\langle \text{sp} - 0 \rangle_s$		

]

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

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

*Proof.*

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

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

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

such that

- $\mathbf{M}^6 := \mathbf{M}^5[+\text{kpc}]_{\text{stk}}[\text{wk}_0 \mapsto \text{bg} + c_1 + 3]_{\text{reg}}$ ,
- $\mathbf{M}^6$  repr  $\Phi^6$ .

- Let  $W^6 := W^5[+\text{kpc}]_1$ .  
Then  $(\mathbf{M}^6, M^5) \in \mathcal{M}(W^6)$ .  
By Theorem 9, it suffices to show that  $((\Phi^6, \text{bg} + 3), (M^5.h, K[\gamma\rho(\text{if } e_1 \text{ then } e_2 \text{ else } e_3)])) \in \mathcal{O}(W^6)$ .
- By (\*), it suffices to show that

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

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

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

- As  $W^7$  includes  $\iota^{\text{code}}(\text{code}^\bullet)$ , we execute the two instructions from `bg + c1 + 3` on the low side, take one step on the high side, and get the configurations

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

such that

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

- Still,  $(\mathbf{M}^8, M^7) \in \mathcal{M}(W^7)$ .

By Theorem 9, it suffices to show that

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

- By  $(***)$ , it suffices to show that  $((\text{bg} + c_1 + c_2 + c_3 + 5, [\text{wk}_5]), K[-]) \in \mathcal{K}[\tau]\rho(W^7)$ .

- Suppose

$$\begin{aligned} W^9 &\sqsupseteq_{\text{pub}} W^7, \\ (\mathbf{v}_3, v_4) &\in \mathcal{V}[\tau]\rho(W^9), \\ (\mathbf{M}^9, M^9) &\in \mathcal{M}(W^9), \\ \mathbf{M}^9.\text{reg}(\text{wk}_5) &= \mathbf{v}_3, \\ \mathbf{M}^9 &\text{repr } \Phi^9. \end{aligned}$$

- To show:  $((\Phi^9, \text{bg} + c_1 + c_2 + c_3 + 5), (M^9.h, K[v_4])) \in \mathcal{O}(W^9)$

- As  $W^9$  includes  $\iota^{\text{code}}(\text{code}^\bullet)$ , we execute the instructions from  $\text{bg} + c_1 + c_2 + c_3 + 5$  on the low side and get the following

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

such that

$$\begin{aligned} - \mathbf{M}^{10} &:= \mathbf{M}^9[-1]_{\text{stk}} \\ - \mathbf{M}^{10} &\text{repr } \Phi^{10} \end{aligned}$$

- 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  $((\Phi^{10}, \text{kpc}), (M^9.h, K[v_4])) \in \mathcal{O}(W^{10})$ .

- As  $W^{10} \sqsupseteq_{\text{pub}} W^5$  and  $((\text{kpc}, [\text{wk}_5]), K) \in \mathcal{K}[\tau]\rho(W^5)$ , 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  $v_2 = \text{ff}$

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

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

such that

$$\begin{aligned} - \mathbf{M}^8 &:= \mathbf{M}^7[\text{wk}_0 \mapsto \underline{\text{bg} + c_1 + c_2 + c_3 + 5}]_{\text{reg}}, \\ - \mathbf{M}^8 &\text{repr } \Phi^8. \end{aligned}$$

- Still,  $(\mathbf{M}^8, M^7) \in \mathcal{M}(W^7)$ .

By Theorem 9, it suffices to show that

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

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

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

such that

- $\mathbf{M}^{10} := \mathbf{M}^9[-1]_{\text{stk}}$
- $\mathbf{M}^{10} \text{ repr } \Phi^{10}$

- 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  $((\Phi^{10}, \text{kpc}), (M^9.h, K[v_4])) \in \mathcal{O}(W^{10})$ .
- As  $W^{10} \sqsupseteq_{\text{pub}} W^5$  and  $((\text{kpc}, \lfloor \text{wk}_5 \rfloor), K) \in \mathcal{K}[\tau]\rho(W^5)$ , 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.

□

⋮