1 Syntax

$$
\begin{array}{lll}
e ::= c \in \mathbb{Z} & e_e ::= \cdot +_1 e & s \in stat ::= skip \\
\quad \mid \mathtt{x} \in Var & \quad \mid \cdot +_2 \cdot & \quad \mid s_1; s_2 \\
\quad \mid e_1 + e_2 & \quad \mid @_1 (e_2) & \quad \mid \mathtt{x} := e \\
\quad \mid \lambda \mathtt{x}.s & \quad \mid @_2 & \quad \mid if\ (e > 0)\ s_1\ s_2 \\
\quad \mid e_1\,(e_2) & \quad \mid @_3 & \quad \mid while\ (e > 0)\ s \\
\quad \mid alloc & \quad \mid \mathtt{.f} & \quad \mid return\, e \\
\quad \mid e.\mathtt{f} & \quad \mid \mathtt{f}\ in_1 \cdot & \quad \mid e_1.\mathtt{f} := e_2 \\
\quad \mid \mathtt{f}\ in\ e & & \quad \mid delete\ e.\mathtt{f}
\end{array}
$$

$$
\begin{array}{l}
s_e ::= \mathtt{x} :=_1 \cdot \\
\quad \mid \cdot ;_1 s_2 \\
\quad \mid if_1\, s_1\, s_2 \\
\quad \mid while_1\ (e > 0)\ s \\
\quad \mid while_2\ (e > 0)\ s \\
\quad \mid return_1 \cdot \\
\quad \mid \mathtt{.f} :=_1 e_2 \\
\quad \mid \mathtt{.f} :=_2 \cdot \\
\quad \mid delete_1\ \mathtt{.f}
\end{array}
$$

2 Abstract Semantics

2.1 Expressions

$$\textsc{red-const}(c)\quad \frac{}{(- \mid emp, \eta_e, \eta_c), c \Downarrow (- \mid emp, \eta_e, \alpha(c))}$$

$$\textsc{red-var-local}(\mathtt{x})\quad \frac{}{\left(- \mid \eta_e \mapsto E_e^\sharp \star \eta_c \mapsto E_c^\sharp, \eta_e, \eta_c\right), \mathtt{x} \Downarrow \left(- \mid \eta_e \mapsto E_e^\sharp \star \eta_c \mapsto E_c^\sharp, \eta_e, E_c^\sharp[\mathtt{x}]\right)} \quad \mathtt{x} \in dom\left(E_c^\sharp\right)$$

$$\textsc{red-var-local}(\mathtt{x})\quad \frac{}{\left(- \mid \eta \mapsto E^\sharp, \eta, \eta\right), \mathtt{x} \Downarrow \left(- \mid \eta \mapsto E^\sharp, \eta, E^\sharp[\mathtt{x}]\right)} \quad \mathtt{x} \in dom\left(E^\sharp\right)$$

$$\textsc{red-var-global}(x)\quad \frac{}{\left(- \mid \eta_e \mapsto E_e^\sharp \star \eta_c \mapsto E_c^\sharp, \eta_e, \eta_c\right), \mathtt{x} \Downarrow \left(- \mid \eta_e \mapsto E_e^\sharp \star \eta_c \mapsto E_c^\sharp, \eta_e, E_e^\sharp[\mathtt{x}]\right)} \quad \mathtt{x} \in dom\left(E_e^\sharp\right) \wedge \mathtt{x} \notin dom\left(E_c^\sharp\right)$$

$$\textsc{red-var-undef}(x)\quad \frac{}{\left(- \mid \eta_e \mapsto E_e^\sharp \star \eta_c \mapsto E_c^\sharp, \eta_e, \eta_c\right), \mathtt{x} \Downarrow \left(- \mid \eta_e \mapsto E_e^\sharp \star \eta_c \mapsto E_c^\sharp, err^\sharp\right)} \quad \mathtt{x} \notin dom\left(E_e^\sharp\right) \wedge \mathtt{x} \notin dom\left(E_c^\sharp\right)$$

$$\textsc{red-var-undef}(x)\quad \frac{}{\left(- \mid \eta \mapsto E^\sharp, \eta, \eta\right), \mathtt{x} \Downarrow \left(- \mid \eta \mapsto E^\sharp, err^\sharp\right)} \quad \mathtt{x} \notin dom\left(E^\sharp\right)$$

RED-ADD(e_1, e_2)

$$\frac{(- \mid \phi, \eta_e, \eta_c), e_1 \Downarrow \left(M \mid \phi', r^\sharp\right) \qquad \left(M \mid \phi', M(\eta_c), r^\sharp\right), \cdot +_1 e_2 \Downarrow \Phi}{(- \mid \phi, \eta_e, \eta_c), e_1 + e_2 \Downarrow \Phi}$$

RED-ADD-1(e_2)

$$\frac{(- \mid \phi, \eta_e, \eta_c), e_2 \Downarrow \left(M \mid \phi', r^\sharp\right) \qquad \left(M \mid \phi', M\left(v_1^\sharp\right), r^\sharp\right), \cdot +_2 \cdot \Downarrow \Phi}{\left(- \mid \phi, \eta_c, \left(\eta_e, v_1^\sharp\right)\right), \cdot +_1 e_2 \Downarrow \Phi}$$

RED-ADD-2

$$\frac{}{\left(- \mid emp, v_1^\sharp, \left(\eta_e, v_2^\sharp\right)\right), \cdot +_2 \cdot \Downarrow \left(- \mid emp, \eta_e, v_1^\sharp +^\sharp v_2^\sharp\right)}$$

RED-LAMBDA(x, s)

$$\frac{}{(- \mid emp, \eta_e, \eta_c), \lambda \mathsf{x}.s \Downarrow (- \mid emp, \eta_e, (\eta_c, \lambda \mathsf{x}.s))}$$

RED-APP(e_1, e_2)

$$\frac{(- \mid \phi, \eta_e, \eta_c), e_1 \Downarrow \left(M \mid \phi', r^\sharp\right) \qquad \left(M \mid \phi', M(\eta_c), r^\sharp\right), @_1(e_2) \Downarrow \Phi}{(- \mid \phi, \eta_e, \eta_c), e_1 + e_2 \Downarrow \Phi}$$

RED-APP-1(e_2)

$$\frac{(- \mid \phi, \eta_e, \eta_c), e_2 \Downarrow \left(M \mid \phi', r^\sharp\right) \qquad \left(M \mid \phi', M\left(v_1^\sharp\right), \mathsf{x}, s, r^\sharp\right), @_2 \Downarrow \Phi}{(- \mid \phi, \eta_c, (\eta_e, (\eta_c', \lambda \mathsf{x}.s))) @_1(e_2) \Downarrow \Phi}$$

RED-APP-2(s)

$$\frac{\begin{array}{c}\eta_c' \text{ fresh} \\ \left(-, \bullet \to \eta_c' \mid \eta_c' \mapsto E^\sharp\left[\mathsf{x} \leftarrow v^\sharp\right] \star \eta \mapsto E^\sharp \star \phi, \eta_e, \eta_c'\right), s \Downarrow \Phi \qquad \Phi, @_3 \Downarrow \Phi'\end{array}}{\left(- \mid \eta \mapsto E^\sharp \star \phi, \eta_e, \eta_c, \mathsf{x}, s, v^\sharp\right), @_2 \Downarrow \Phi'}$$

RED-APP-3-RET

$$\frac{}{\left(- \mid emp, ret\left(\eta_e, v^\sharp\right)\right), @_3 \Downarrow \left(- \mid emp, \eta_e, v^\sharp\right)}$$

RED-APP-3-NO-RET

$$\frac{}{(- \mid emp, \eta_e, \eta_c), @_3 \Downarrow (- \mid emp, err)}$$

$$\textsc{red-new-obj}\quad \frac{}{(- \mid \mathit{emp}, \eta_e, \eta_c)\,, \mathit{alloc} \Downarrow (-, \bullet \to l \mid l \mapsto \{\_ : \boxtimes\}, \eta_e, l)}$$

$$\textsc{red-field}(e, \mathtt{f})\quad \frac{(- \mid \phi, \eta_e, \eta_c)\,, e \Downarrow \Phi \qquad \Phi, .\mathtt{f} \Downarrow \Phi'}{(- \mid \phi, \eta_e, \eta_c)\,, e.\mathtt{f} \Downarrow \Phi'}$$

$$\textsc{red-field-1}(\mathtt{f})\quad \frac{}{\left(- \,\middle|\, l \mapsto \left\{\mathtt{f} : u^\sharp\right\}, \eta_e, \eta_c\right).\mathtt{f} \Downarrow \left(- \,\middle|\, l \mapsto \left\{\mathtt{f} : u^\sharp\right\}, \eta_e, u^\sharp\big|_{Val^\sharp}\right)}$$

$$\textsc{red-in}(\mathtt{f}, e)\quad \frac{(- \mid \phi, \eta_e, \eta_c)\,, e \Downarrow \Phi \qquad \Phi, \mathtt{f}\ in_1 \cdot \Downarrow \Phi'}{(- \mid \phi, \eta_e, \eta_c)\,, \mathtt{f}\ in\ e \Downarrow \Phi'}\ \frac{}{\left(- \,\middle|\, l \mapsto \left\{\mathtt{f} : u^\sharp\right\}, \eta_e, l\right), \mathtt{f}\ in_1 \cdot \Downarrow \left(- \,\middle|\, l \mapsto \left\{\mathtt{f} : u^\sharp\right\}, \eta_e, +\right)}\ \textsc{red-in-1-true}(\mathtt{f})\quad u^\sharp\big|_{Val^\sharp} \neq \bot$$

$$\textsc{red-in-1-false}(\mathtt{f})\quad \frac{}{\left(- \,\middle|\, l \mapsto \left\{\mathtt{f} : u^\sharp\right\}, \eta_e, l\right), \mathtt{f}\ in_1 \cdot \Downarrow \left(- \,\middle|\, l \mapsto \left\{\mathtt{f} : u^\sharp\right\}, \eta_e, 0\right)}\quad \boxtimes \sqsubseteq u^\sharp$$

2.2 Statements

$$\textsc{red-skip}\quad \frac{}{(- \mid \mathit{emp}, \eta_e, \eta_c)\,, \mathit{skip} \Downarrow (- \mid \mathit{emp}, \eta_e, \eta_c)}$$

$$\textsc{red-seq}(s_1, s_2)\quad \frac{(- \mid \phi, \eta_e, \eta_c)\,, s_1 \Downarrow \Phi \qquad \Phi, \cdot ;_1 s_2 \Downarrow \Phi'}{(- \mid \phi, \eta_e, \eta_c)\,, s_1; s_2 \Downarrow \Phi'} \qquad \textsc{red-seq-1}(s_2)\quad \frac{(- \mid \phi, \eta_e, \eta_c)\,, s_2 \Downarrow \Phi}{(- \mid \phi, \eta_e, \eta_c)\,, \cdot ;_1 s_2 \Downarrow \Phi}$$

$$\textsc{red-asn}(\mathsf{x}, e)\quad \frac{(-\mid \phi, \eta_e, \eta_c), e \Downarrow \left(M \mid \phi', x^\sharp\right) \qquad \left(M \mid \phi', M(\eta_c), x^\sharp\right), \mathsf{x} :=_1 \cdot \Downarrow \Phi}{(-\mid \phi, \eta_e, \eta_c), \mathsf{x} := e \Downarrow \Phi}$$

$$\textsc{red-asn-1}(\mathsf{x})\quad \frac{\eta_e' \text{ fresh}}{\left(- \;\middle|\; \eta_e \mapsto E_e^\sharp \star \eta_c \mapsto E_c^\sharp, \eta_c, \left(\eta_e, v^\sharp\right)\right), \mathsf{x} :=_1 \cdot \Downarrow \left(-, \bullet \to \eta_e' \;\middle|\; \eta_e \mapsto E_e^\sharp \star \eta_c \mapsto E_c^\sharp \star \eta_e' \mapsto E_e^\sharp\left[\mathsf{x} \leftarrow v^\sharp\right], \eta_e', \eta_c\right)} \quad \mathsf{x} \notin dom\left(E_c^\sharp\right)$$

$$\textsc{red-asn-1}(\mathsf{x})\quad \frac{\eta_e \text{ fresh}}{\left(- \;\middle|\; \eta \mapsto E^\sharp, \eta, \left(\eta, v^\sharp\right)\right), \mathsf{x} :=_1 \cdot \Downarrow \left(-, \bullet \to \eta_e \;\middle|\; \eta \mapsto E^\sharp \star \eta_e \mapsto E^\sharp\left[\mathsf{x} \leftarrow v^\sharp\right], \eta_e, \eta\right)} \quad \mathsf{x} \notin dom\left(E^\sharp\right)$$

$$\textsc{red-asn-1-local}(\mathsf{x})\quad \frac{\eta_c' \text{ fresh}}{\left(- \;\middle|\; \eta_e \mapsto E_e^\sharp \star \eta_c \mapsto E_c^\sharp, \eta_c, \left(\eta_e, v^\sharp\right)\right), \mathsf{x} :=_1 \cdot \Downarrow \left(-, \bullet \to \eta_c' \;\middle|\; \eta_e \mapsto E_e^\sharp \star \eta_c \mapsto E_c^\sharp \star \eta_c' \mapsto E_c^\sharp\left[\mathsf{x} \leftarrow v^\sharp\right], \eta_e, \eta_c'\right)} \quad \mathsf{x} \in dom\left(E_c^\sharp\right)$$

$$\textsc{red-asn-1-local}(\mathsf{x})\quad \frac{\eta_c \text{ fresh}}{\left(- \;\middle|\; \eta \mapsto E^\sharp, \eta, \left(\eta, v^\sharp\right)\right), \mathsf{x} :=_1 \cdot \Downarrow \left(-, \bullet \to \eta_c \;\middle|\; \eta \mapsto E^\sharp \star \eta_c \mapsto E^\sharp\left[\mathsf{x} \leftarrow v^\sharp\right], \eta, \eta_c\right)} \quad \mathsf{x} \in dom\left(E^\sharp\right)$$

$$\textsc{red-if}(e, s_1, s_2)\quad \frac{(-\mid \phi, \eta_e, \eta_c), e \Downarrow \left(M \mid \phi', x^\sharp\right) \qquad \left(M \mid \phi', M(\eta_c), x^\sharp\right), if_1\, s_1\, s_2 \Downarrow \Phi}{(-\mid \phi, \eta_e, \eta_c), if\ (e > 0)\ s_1\, s_2 \Downarrow \Phi}$$

$$\textsc{red-if-1-pos}(s_1, s_2)\quad \frac{(-\mid \phi, \eta_c, \eta_e), s_1 \Downarrow \Phi}{\left(- \mid \phi, \eta_c, \left(\eta_e, v^\sharp\right)\right), if_1\, s_1\, s_2 \Downarrow \Phi} \quad v^\sharp \sqcap + \neq \bot$$

$$\textsc{red-if-1-neg}(s_1, s_2)\quad \frac{(-\mid \phi, \eta_c, \eta_e), s_2 \Downarrow \Phi}{\left(- \mid \phi, \eta_c, \left(\eta_e, v^\sharp\right)\right), if_1\, s_1\, s_2 \Downarrow \Phi} \quad v^\sharp \sqcap -_0 \neq \bot$$

$$\textsc{red-while}(e, s)\quad \frac{(-\mid \phi, \eta_e, \eta_c), e \Downarrow \left(M \mid \phi', x^\sharp\right) \qquad \left(M \mid \phi', M(\eta_c), x^\sharp\right), while_1\ (e > 0)\ s \Downarrow \Phi}{(-\mid \phi, \eta_e, \eta_c), while\ (e > 0)\ s \Downarrow \Phi}$$

$$\textsc{red-while-1-neg}(e, s)\quad \frac{}{\left(- \mid \phi, \eta_c, \left(\eta_e, v^\sharp\right)\right), while_1\ (e > 0)\ s \Downarrow (-\mid \phi, \eta_e, \eta_c)} \quad v^\sharp \sqcap -_0 \neq \bot$$

$$\textsc{red-while-1-pos}(e, s)\quad \frac{(-\mid \phi, \eta_e, \eta_c), s \Downarrow \Phi \qquad \Phi, while_2\ (e > 0)\ s \Downarrow \Phi'}{\left(- \mid \phi, \eta_c, \left(\eta_e, v^\sharp\right)\right), while_1\ (e > 0)\ s \Downarrow \Phi'} \quad v^\sharp \sqcap + \neq \bot$$

$$\textsc{red-while-2}(e, s)\quad \frac{(-\mid \phi, \eta_e, \eta_c), while\ (e > 0)\ s \Downarrow \Phi}{(-\mid \phi, \eta_e, \eta_c), while_2\ (e > 0)\ s \Downarrow \Phi}$$

$$\textsc{red-return}(e)\quad \frac{(-\mid \phi,\eta_e,\eta_c),e \Downarrow \Phi \qquad \Phi, return_1\cdot \Downarrow \Phi'}{(-\mid \phi,\eta_e,\eta_c),return\, e \Downarrow \Phi'}$$

$$\textsc{red-return-1}\quad \frac{}{\left(-\;\middle|\; emp,\eta_e,v^\sharp\right),return_1\cdot \Downarrow \left(-\;\middle|\; emp, ret\left(\eta_e,v^\sharp\right)\right)}$$

$$\textsc{red-field-asn}(e_1,\mathtt{f},e_2)\quad \frac{(-\mid \phi,\eta_e,\eta_c),e_1 \Downarrow \left(M\;\middle|\;\phi',r^\sharp\right) \qquad \left(M\;\middle|\;\phi',M\left(\eta_c\right),r^\sharp\right),.\mathtt{f} :=_1 e_2 \Downarrow \Phi}{(-\mid \phi,\eta_e,\eta_c),e_1.\mathtt{f} := e_2 \Downarrow \Phi}$$

$$\textsc{red-field-asn-1}(\mathtt{f},e_2)\quad \frac{(-\mid \phi,\eta_e,\eta_c),e_2 \Downarrow \left(M\;\middle|\;\phi',r^\sharp\right) \qquad \left(M\;\middle|\;\phi',M\left(\eta_c\right),M\left(l\right),r^\sharp\right),.\mathtt{f} :=_2 \cdot \Downarrow \Phi}{(-\mid \phi,\eta_c,(\eta_e,l)),.\mathtt{f} :=_1 e_2 \Downarrow \Phi}$$

$$\textsc{red-field-asn-2}(\mathtt{f})\quad \frac{}{\left(-\;\middle|\; l\mapsto\left\{\mathtt{f}:u^\sharp\right\},\eta_c,l,\left(\eta_e,v^\sharp\right)\right),.\mathtt{f} :=_2 \cdot \Downarrow \left(-\;\middle|\; l\mapsto\left\{\mathtt{f}:v^\sharp\right\},\eta_e,\eta_c\right)}$$

$$\textsc{red-delete}(e,\mathtt{f})\quad \frac{(-\mid \phi,\eta_e,\eta_c),e \Downarrow \left(M\;\middle|\;\phi',r^\sharp\right) \qquad \left(M\;\middle|\;\phi',M\left(\eta_c\right),r^\sharp\right),delete_1\ .\mathtt{f} \Downarrow \Phi}{(-\mid \phi,\eta_e,\eta_c),delete\ e.\mathtt{f} \Downarrow \Phi}$$

$$\textsc{red-delete-1}(\mathtt{f})\quad \frac{}{\left(-\;\middle|\; l\mapsto\left\{\mathtt{f}:u^\sharp\right\},\eta_c,(\eta_e,l)\right),delete_1\ .\mathtt{f} \Downarrow (-\mid l\mapsto\{\mathtt{f}:\boxtimes\},\eta_c,\eta_e)}$$

2.3 Aborting Rules

$$\textsc{red-error-expr}(e)\quad \frac{}{\Phi,e \Downarrow \Phi}\ \mathbf{abort}\,\Phi \wedge \neg \mathbf{intercept}_e\,\Phi \qquad \textsc{red-error-stat}(s)\quad \frac{}{\Phi,s \Downarrow \Phi}\ \mathbf{abort}\,\Phi$$

$$\frac{x^\sharp = C\left[err^\sharp\right]}{\mathbf{abort}\,\left(M\;\middle|\;\phi,x^\sharp\right)} \qquad \frac{}{\mathbf{intercept}_{@_3}\,\left(M\;\middle|\;\phi,ret\left(\eta_e,v^\sharp\right)\right)}$$