1 Syntax

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

2 Abstract Semantics

2.1 Expressions

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

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

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

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

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

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

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

$$\textsc{red-add-1}(e_2)\quad \frac{(- \mid \phi, \eta_e, \eta_c), e_2 \Downarrow \left(M \mid \phi', r^\sharp\right) \qquad \left(M \mid \phi', M\left(v_1^\sharp\right), r^\sharp\right), \cdot +_2 \cdot \Downarrow \Phi}{\left(- \mid \phi, \eta_c, \left(\eta_e, v_1^\sharp\right)\right), \cdot +_1 e_2 \Downarrow \Phi}$$

$$\textsc{red-add-2}\quad \frac{}{\left(- \mid \mathit{emp}, v_1^\sharp, \left(\eta_e, v_2^\sharp\right)\right), \cdot +_2 \cdot \Downarrow \left(- \mid \mathit{emp}, \eta_e, v_1^\sharp +^\sharp v_2^\sharp\right)}$$

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

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

$$\textsc{red-app-1}(e_2)\quad \frac{(- \mid \phi, \eta_e, \eta_c), e_2 \Downarrow \left(M \mid \phi', r^\sharp\right) \qquad \left(M \mid \phi', M\left(v_1^\sharp\right), \mathsf{x}, s, r^\sharp\right), @_2 \Downarrow \Phi}{(- \mid \phi, \eta_c, (\eta_e, (\eta_c', \lambda \mathsf{x}.s)))\, @_1(e_2) \Downarrow \Phi}$$

$$\textsc{red-app-2}(s)\quad \frac{\begin{array}{c}\eta_c' \text{ fresh} \\ \left(-, \bullet \to \eta_c' \mid \eta_c' \mapsto E^\sharp\left[\mathsf{x} \leftarrow v^\sharp\right] \star \eta \mapsto E^\sharp \star \phi, \eta_e, \eta_c'\right), s \Downarrow \Phi \qquad \Phi, @_3 \Downarrow \Phi'\end{array}}{\left(- \mid \eta \mapsto E^\sharp \star \phi, \eta_e, \eta_c, \mathsf{x}, s, v^\sharp\right), @_2 \Downarrow \Phi'}$$

$$\textsc{red-app-3-ret}\quad \frac{}{\left(- \mid \mathit{emp}, \mathit{ret}\left(\eta_e, v^\sharp\right)\right), @_3 \Downarrow \left(- \mid \mathit{emp}, \eta_e, v^\sharp\right)}$$

$$\textsc{red-app-3-no-ret}\quad \frac{}{(- \mid \mathit{emp}, \eta_e, \eta_c), @_3 \Downarrow (- \mid \mathit{emp}, \mathit{err})}$$

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

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

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

$$\textsc{red-in}(\mathtt{f}, e)\quad \frac{(- \mid \phi, \eta_e, \eta_c), e \Downarrow \Phi \qquad \Phi, \mathtt{f}\ \mathit{in}_1 \cdot \Downarrow \Phi'}{(- \mid \phi, \eta_e, \eta_c), \mathtt{f}\ \mathit{in}\ e \Downarrow \Phi'}$$

$$\textsc{red-in-1-true}(\mathtt{f})\quad \frac{}{\left(- \mid l \mapsto \left\{\mathtt{f} : u^\sharp\right\}, \eta_e, l\right), \mathtt{f}\ \mathit{in}_1 \cdot \Downarrow \left(- \mid l \mapsto \left\{\mathtt{f} : u^\sharp\right\}, \eta_e, +\right)} \quad u^\sharp|_{\mathit{Val}^\sharp} \neq \bot$$

$$\textsc{red-in-1-false}(\mathtt{f})\quad \frac{}{\left(- \mid l \mapsto \left\{\mathtt{f} : u^\sharp\right\}, \eta_e, l\right), \mathtt{f}\ \mathit{in}_1 \cdot \Downarrow \left(- \mid l \mapsto \left\{\mathtt{f} : u^\sharp\right\}, \eta_e, 0\right)} \quad \boxtimes \sqsubseteq u^\sharp$$

2.2 Statements

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

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

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

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

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

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

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

$$\textsc{red-if}(e, s_1, s_2)\quad \frac{(- \mid \phi, \eta_e, \eta_c), e \Downarrow \left(M \mid \phi', x^\sharp\right) \qquad \left(M \mid \phi', M(\eta_c), x^\sharp\right), \mathit{if}_1\ s_1\ s_2 \Downarrow \Phi}{(- \mid \phi, \eta_e, \eta_c), \mathit{if}\ (e > 0)\ s_1\ s_2 \Downarrow \Phi}$$

$$\textsc{red-if-1-pos}(s_1, s_2)\quad \frac{(- \mid \phi, \eta_c, \eta_e), s_1 \Downarrow \Phi}{\left(- \mid \phi, \eta_c, \left(\eta_e, v^\sharp\right)\right), \mathit{if}_1\ s_1\ s_2 \Downarrow \Phi} \quad v^\sharp \sqcap + \neq \bot$$

$$\textsc{red-if-1-neg}(s_1, s_2)\quad \frac{(- \mid \phi, \eta_c, \eta_e), s_2 \Downarrow \Phi}{\left(- \mid \phi, \eta_c, \left(\eta_e, v^\sharp\right)\right), \mathit{if}_1\ s_1\ s_2 \Downarrow \Phi} \quad v^\sharp \sqcap -_0 \neq \bot$$

$$\textsc{red-while}(e, s)\quad \frac{(- \mid \phi, \eta_e, \eta_c), e \Downarrow \left(M \mid \phi', x^\sharp\right) \qquad \left(M \mid \phi', M(\eta_c), x^\sharp\right), \mathit{while}_1\ (e > 0)\ s \Downarrow \Phi}{(- \mid \phi, \eta_e, \eta_c), \mathit{while}\ (e > 0)\ s \Downarrow \Phi}$$

$$\textsc{red-while-1-neg}(e, s)\quad \frac{}{\left(- \mid \phi, \eta_c, \left(\eta_e, v^\sharp\right)\right), \mathit{while}_1\ (e > 0)\ s \Downarrow (- \mid \phi, \eta_e, \eta_c)} \quad v^\sharp \sqcap -_0 \neq \bot$$

$$\textsc{red-while-1-pos}(e, s)\quad \frac{(- \mid \phi, \eta_e, \eta_c), s \Downarrow \Phi \qquad \Phi, \mathit{while}_2\ (e > 0)\ s \Downarrow \Phi'}{\left(- \mid \phi, \eta_c, \left(\eta_e, v^\sharp\right)\right), \mathit{while}_1\ (e > 0)\ s \Downarrow \Phi'} \quad v^\sharp \sqcap + \neq \bot$$

$$\textsc{red-while-2}(e, s)\quad \frac{(- \mid \phi, \eta_e, \eta_c), \mathit{while}\ (e > 0)\ s \Downarrow \Phi}{(- \mid \phi, \eta_e, \eta_c), \mathit{while}_2\ (e > 0)\ s \Downarrow \Phi}$$

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

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

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

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

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

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

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

2.3 Aborting Rules

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

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