1 Formal Development

Lemma 1 (Value inversion)**.** *Inversion lemma for values:*

1. *If* $v : \mathsf{uint}$*, then* $v = n$
2. *If* $v : \mathsf{bool}$*, then* $v = \top$ *or* $v = \bot$
3. *If* $v : \sigma[n]$*, then* $v = [c_i]_n$ *and* $c_i : \sigma$

Lemma 2 (Soundness of scalar expressions)**.** *If*

1. $\Gamma \vdash e : \sigma^\ell \rightsquigarrow \widetilde{e}$
2. $\Gamma \sim \rho$
3. $\Gamma \vdash \rho \hookrightarrow \widetilde{\rho}; \widehat{\rho}_1, \widehat{\rho}_2$

Then

(a) $\rho \vdash e \downarrow v$

(b) $v : \sigma$

(c) $\widetilde{\rho} \vdash \widetilde{e} \Downarrow \widetilde{v}; \kappa$

where either $\ell = \mathcal{P}$*,* $\widetilde{v} = v$*, and* $\kappa = \cdot$
or $\exists r, m.\ \ell = m$*,* $\widetilde{v} = r$*,* $\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa \longmapsto \widehat{\rho}'_1, \widehat{\rho}'_2; \cdot$*, and* $\mathcal{D}_m(\widehat{\rho}'_1[r], \widehat{\rho}'_2[r]) = v$*.*

Proof. Proof by Induction on (1). □

Lemma 3 (Soundness of array expressions)**.** *If*

1. $\Gamma \vdash e : \sigma^\ell[n] \rightsquigarrow \widetilde{e}$
2. $\Gamma \sim \rho$
3. $\Gamma \vdash \rho \hookrightarrow \widetilde{\rho}; \widehat{\rho}_1, \widehat{\rho}_2$

Then

(a) $\rho \vdash e \downarrow [c_i]_n$

(b) $[c_i]_n : \sigma[n]$

(c) $\widetilde{\rho} \vdash \widetilde{e} \Downarrow \widetilde{v}; \kappa$

where either $\widetilde{v} = [c_i]_n$ *and* $\kappa = \cdot$
or $\exists r_i, m.\ \widetilde{v} = [r_i]_n$*,* $\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa \longmapsto \widehat{\rho}'_1, \widehat{\rho}'_2; \cdot$*, and* $\forall i.\ \mathcal{D}_m(\widehat{\rho}'_1[r_i], \widehat{\rho}'_2[r_i]) = c_i$*.*

Proof. Proof by Induction on (1). □

Lemma 4 (Target semantics correspondence)**.** *If:*

1. $\Gamma \vdash s \rightsquigarrow \widetilde{s} \mid \Gamma'$

2. $\Gamma \sim \rho$

3. $\Gamma \vdash \rho \hookrightarrow \widetilde{\rho}; \widehat{\rho}_1, \widehat{\rho}_2$

4. $\rho \vdash s \downarrow \rho'; O$

then:

(a) $\widetilde{\rho} \vdash \widetilde{s} \Longrightarrow \widetilde{\rho}'; \kappa$

(b) $\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa \longmapsto \widehat{\rho}'_1, \widehat{\rho}'_2; O$

Lemma 5 (Soundness of source semantics)**.** *If:*

1. $\Gamma \vdash s \rightsquigarrow \widetilde{s} \mid \Gamma'$

2. $\Gamma \sim \rho$

then, $\rho \vdash s \downarrow \rho'; O$

Theorem 6 (Soundness)**.** *If:*

1. $\Gamma \vdash s \rightsquigarrow \widetilde{s} \mid \Gamma'$

2. $\Gamma \sim \rho$

3. $\Gamma \vdash \rho \hookrightarrow \widetilde{\rho}; \widehat{\rho}_1, \widehat{\rho}_2$

then:

(a) $\rho \vdash s \downarrow \rho'; O$

(b) $\widetilde{\rho} \vdash \widetilde{s} \Longrightarrow \widetilde{\rho}'; \kappa$

(c) $\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa \longmapsto \widehat{\rho}'_1, \widehat{\rho}'_2; O$

Proof. Follows from Lemma 4 and 5. $\square$