

1 Formal Development

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

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

Lemma 2 (Consistency of source type and target type). *If $\psi \sim \tau$, then one of the following holds:*

1. $\psi = \sigma$ and $\tau = \sigma^\ell$.
2. $\psi = \sigma[n]$ and $\tau = \sigma^\ell[n]$.

Lemma 3 (Consistency of type environment and source runtime environment). *If $\Gamma \sim \rho$ and $\Gamma(x) = \tau$, then $\rho(x) = v$ s.t. $v : \psi$ and $\psi \sim \tau$.*

Lemma 4 (Compilation of source environment). *If $\Gamma \vdash \rho \hookrightarrow \tilde{\rho}; \hat{\rho}_1, \hat{\rho}_2$ and $\Gamma(x) = \tau$, then one of the following holds:*

1. $\tau = \sigma^{\mathcal{P}}$, $\rho(x) = c$, and $\tilde{\rho}(x) = c$.
2. $\tau = \sigma^m$, $\rho(x) = c$, $\tilde{\rho}(x) = r$, and $(\hat{\rho}_1[r], \hat{\rho}_2[r]) = \mathcal{E}_m(c)$.
3. $\tau = \sigma^{\mathcal{P}}[n]$, $\rho(x) = [c_i]_n$, and $\tilde{\rho}(x) = [c_i]_n$.
4. $\tau = \sigma^m[n]$, $\rho(x) = [c_i]_n$, $\tilde{\rho}(x) = [r_i]_n$, $(\hat{\rho}_1[r_i], \hat{\rho}_2[r_i]) = \mathcal{E}_m(c_i)$

Lemma 5 (Soundness of scalar expressions). *If*

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

Then

- (a) $\rho \vdash e \Downarrow v$
- (b) $v : \sigma$
- (c) $\tilde{\rho} \vdash \tilde{e} \Downarrow \tilde{v}; \kappa$

where either $\ell = \mathcal{P}$, $\tilde{v} = v$, and $\kappa = \cdot$

or $\exists r, m. \ell = m$, $\tilde{v} = r$, $\hat{\rho}_1, \hat{\rho}_2 \vdash \kappa \mapsto \hat{\rho}'_1, \hat{\rho}'_2; \cdot$, and $\mathcal{D}_m(\hat{\rho}'_1[r], \hat{\rho}'_2[r]) = v$.

Proof. Proof by induction on the derivation (1), case analysis on the last rule.

Case S_CONS: $e = c$, $\sigma = \delta(c)$, $\ell = \mathcal{P}$, $\tilde{e} = c$.

(a) follows from SE_CONST.

(b) follows from V_CONST.

(c) follows from EE_CONST with $\kappa = \cdot$.

And first case of either holds.

Case S_VAR: $e = x$, $\sigma^\ell = \tau$, $\tilde{e} = x$.

□

Lemma 6 (Soundness of array expressions). *If*

$$1. \Gamma \vdash e : \sigma^\ell[n] \rightsquigarrow \tilde{e}$$

$$2. \Gamma \sim \rho$$

$$3. \Gamma \vdash \rho \hookrightarrow \tilde{\rho}; \hat{\rho}_1, \hat{\rho}_2$$

Then

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

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

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

where either $\tilde{v} = [c_i]_n$ and $\kappa = \cdot$

or $\exists r_i, m. \tilde{v} = [r_i]_n, \hat{\rho}_1, \hat{\rho}_2 \vdash \kappa \mapsto \tilde{\rho}'_1, \tilde{\rho}'_2; \cdot$, and $\forall i. \mathcal{D}_m(\tilde{\rho}'_1[r_i], \tilde{\rho}'_2[r_i]) = c_i$.

Proof. Proof by Induction on (1). □

Lemma 7 (Target semantics correspondence). *If:*

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

$$2. \Gamma \sim \rho$$

$$3. \Gamma \vdash \rho \hookrightarrow \tilde{\rho}; \hat{\rho}_1, \hat{\rho}_2$$

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

then:

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

$$(b) \hat{\rho}_1, \hat{\rho}_2 \vdash \kappa \mapsto \tilde{\rho}'_1, \tilde{\rho}'_2; O$$

Lemma 8 (Soundness of source semantics). *If:*

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

$$2. \Gamma \sim \rho$$

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

Theorem 9 (Soundness). *If:*

1. $\Gamma \vdash s \rightsquigarrow \tilde{s} \mid \Gamma'$
2. $\Gamma \sim \rho$
3. $\Gamma \vdash \rho \hookrightarrow \tilde{\rho}; \hat{\rho}_1, \hat{\rho}_2$

then:

- (a) $\rho \vdash s \downarrow \rho'; O$
- (b) $\tilde{\rho} \vdash \tilde{s} \Longrightarrow \tilde{\rho}'; \kappa$
- (c) $\hat{\rho}_1, \hat{\rho}_2 \vdash \kappa \longmapsto \tilde{\rho}'_1, \tilde{\rho}'_2; O$

Proof. Follows from Lemma 7 and 8. □