Intro. to Step-Indexed Logical Relations: Type Safety for STLC + fix

Jeremy G. Siek
Indiana University, Bloomington

PL Wonks
November 2023

Outline

- Review of
  - STLC + fix
  - Type Safety via Progress and Preservation
- The Logical Relations Recipe
- Strawman Logical Relation for Type Safety
- Step-indexed Logical Relation for Type Safety
- A Step-indexed Logic
- Proof of the Fundamental Lemma
- Proof of Type Safety

Review: STLC + fix

$$
\begin{array}{llll}
\text{types} & A, B & ::= & \mathbb{N} \mid A \to B \\
\text{terms} & L, M, N & ::= & \texttt{zero} \mid \texttt{suc}(M) \mid \texttt{case}\, L\, M\, N \mid \\
 & & & i \mid \lambda N \mid L\ \ M \mid \mu N \\
\text{values} & V, W & ::= & \texttt{zero} \mid \texttt{suc}(V) \mid \lambda N \mid \mu V \\
\text{frames} & F & ::= & \texttt{suc}(\square) \mid \texttt{case}\, \square\, M\, N \mid \square\ \ M \mid V\ \ \square
\end{array}
$$

Substitution: $N[M]$ (Replace 0 with M in N, decrement free vars.)
Plug: $F(\!|M|\!)$ (Replace $\square$ with M in F.)
Reduction

$$
\begin{array}{rcll}
(\mu V)\ \ W & \longrightarrow & V[\mu V]\ \ W & \\
(\lambda N)\ \ W & \longrightarrow & N[W] & \\
\texttt{case}\,\texttt{zero}\, M\, N & \longrightarrow & M & \\
\texttt{case}\,\texttt{suc}(V)\, M\, N & \longrightarrow & N[V] & \\
F(\!|M|\!) & \longrightarrow & F(\!|N|\!) & \text{if } M \longrightarrow N
\end{array}
$$

Review: STLC + fix

$\boxed{\Gamma \vdash^{\mathcal{V}} V : A}$

$$\frac{}{\Gamma \vdash^{\mathcal{V}} \texttt{zero} : \mathbb{N}} \qquad \frac{\Gamma \vdash^{\mathcal{V}} V : \mathbb{N}}{\Gamma \vdash^{\mathcal{V}} \texttt{suc}(V) : \mathbb{N}}$$

$$\frac{\Gamma, A \vdash^{\mathcal{V}} N : B}{\Gamma \vdash^{\mathcal{V}} \lambda N : A \to B} \quad \frac{\Gamma, A \to B \vdash^{\mathcal{V}} V : A \to B}{\Gamma \vdash^{\mathcal{V}} \mu V : A \to B}$$

$\boxed{\Gamma \vdash M : A}$

$$\frac{\Gamma \vdash^{\mathcal{V}} V : A}{\Gamma \vdash V : A} \qquad \frac{}{\Gamma \vdash i : \Gamma_i}$$

$$\frac{\Gamma \vdash L : A \to B \qquad \Gamma \vdash M : A}{\Gamma \vdash L\ M : B}$$

$$\frac{\Gamma \vdash M : \mathbb{N}}{\Gamma \vdash \texttt{suc}(M) : \mathbb{N}} \qquad \frac{\begin{array}{c}\Gamma \vdash L : \mathbb{N} \\ \Gamma \vdash M : A \qquad \mathbb{N}, \Gamma \vdash N : A\end{array}}{\Gamma \vdash \texttt{case}\, L\, M\, N : A}$$

Review: Type Safety via Progress & Preservation

Lemma (Progress)

If $\Gamma \vdash M : A$ *then either* M *is a value or* $M \longrightarrow N$ *for some* N.

Lemma (Presevation)

If $\Gamma \vdash M : A$ *and* $M \longrightarrow N$ *then* $\Gamma \vdash N : A$.

Theorem (Type Safety)

If $\vdash M : A$ *then either* $M \longrightarrow^* V$ *for some* V *or* M *diverges.*

Aside: de Bruijn variables and substitutions

A substitution σ is a mapping of variables to terms.

We use de Bruijn variables, so they are numbers: 0, 1, 2, ...

We represent a substitution as a sequence of terms:

$$\sigma = M_0, M_1, M_2, \ldots$$

Applying a substitution to a term: $\boxed{\sigma(M)}$

$$\begin{aligned}
\sigma(\texttt{zero}) &= \texttt{zero} \\
\sigma(\texttt{suc}(M)) &= \texttt{suc}(\sigma(M)) \\
\sigma(\texttt{case}\, L\, M\, N) &= \texttt{case}\, \sigma(L)\, \sigma(M)\, \mathsf{ext}(\sigma)(N) \\
&\quad \text{where } \mathsf{ext}(\sigma) = 0, \uparrow \sigma_0, \uparrow \sigma_1, \ldots \\
\sigma(i) &= \sigma_i \\
\sigma(\lambda N) &= \lambda\, \mathsf{ext}(\sigma)(N) \\
\sigma(L\ M) &= \sigma(L)\ \ \sigma(M) \\
\sigma(\mu N) &= \mu\, \mathsf{ext}(\sigma)(N)
\end{aligned}$$

The Logical Relations Recipe

- Define two functions that generalize the theorem you'd like to prove: one maps types to a predicate on closed values $\mathcal{V}(A)(V)$ and the other maps types to a predicate on closed terms $\mathcal{E}(A)(M)$.
- Extend the $\mathcal{V}$ and $\mathcal{E}$ functions to open terms:

$$
\begin{aligned}
\mathcal{G}(\Gamma)(\sigma) &= \forall A_i \in \Gamma, \mathcal{V}(A_i)(\sigma_i) \\
\Gamma \models^{\mathcal{V}} V : A &= \forall \sigma, \mathcal{G}(\Gamma)(\sigma) \text{ implies } \mathcal{V}(A)(\sigma(V)) \\
\Gamma \models M : A &= \forall \sigma, \mathcal{G}(\Gamma)(\sigma) \text{ implies } \mathcal{E}(A)(\sigma(M))
\end{aligned}
$$

- Prove the Fundamental Lemma, that
  (1) $\Gamma \vdash^{\mathcal{V}} V : A$ implies $\Gamma \models^{\mathcal{V}} V : A$ and
  (2) $\Gamma \vdash M : A$ implies $\Gamma \models M : A$.
- Prove that $\mathcal{E}(A)(M)$ implies your theorem.

Strawman Logical Relation for Type Safety

$\boxed{\mathcal{E}(A)(M) : \mathbb{B}}$ "Progress and Preservation"

$$\mathcal{E}(A)(M) = \begin{array}{l} \mathcal{V}(A)(M) \text{ or } \exists M', M \longrightarrow M' \\ \text{and } \forall M', M \longrightarrow M' \Rightarrow \mathcal{E}(A)(M') \end{array}$$

$\boxed{\mathcal{V}(A)(V) : \mathbb{B}}$

$$\begin{aligned} \mathcal{V}(\mathbb{N})(\texttt{zero}) &= \text{true} \\ \mathcal{V}(\mathbb{N})(\texttt{suc}(V)) &= \mathcal{V}(\mathbb{N})(V) \\ \mathcal{V}(A \to B)(\lambda N) &= \forall W, \mathcal{V}(A)(W) \Rightarrow \mathcal{E}(B)(N[W]) \\ \mathcal{V}(A \to B)(\mu V) &= \mathcal{V}(A \to B)(V[\mu V]) \\ \mathcal{V}(A)(V) &= \text{false} \qquad \text{otherwise} \end{aligned}$$

Argument of recursion is not smaller.

Step-indexed Logical Relation for Type Safety

$$\boxed{\mathcal{E}(A)(M) : \mathbb{N} \to \mathbb{B}}$$

$$\mathcal{E}(A)(M) = \begin{array}{l} \mathcal{V}(A)(M) \text{ or}^\circ \exists^\circ M', M \longrightarrow M' \\ \text{and}^\circ \forall^\circ M', M \longrightarrow M' \Rightarrow^\circ \triangleright^\circ \mathcal{E}(A)(M') \end{array}$$

$$\boxed{\mathcal{V}(A)(V) : \mathbb{N} \to \mathbb{B}}$$

$$\begin{aligned} \mathcal{V}(\mathbb{N})(\mathtt{zero}) &= \text{true}^\circ \\ \mathcal{V}(\mathbb{N})(\mathtt{suc}(V)) &= \mathcal{V}(\mathbb{N})(V) \\ \mathcal{V}(A \to B)(\lambda N) &= \forall^\circ W, \triangleright^\circ \mathcal{V}(A)(W) \Rightarrow^\circ \triangleright^\circ \mathcal{E}(B)(N[W]) \\ \mathcal{V}(A \to B)(\mu V) &= \triangleright^\circ \mathcal{V}(A \to B)(V[\mu V]) \\ \mathcal{V}(A)(V) &= \text{false}^\circ \qquad \text{otherwise} \end{aligned}$$

The $\mathcal{E}$ and $\mathcal{V}$ functions terminate because the step-index gets smaller in the recursive calls thanks to $\triangleright^\circ$.

A Step-indexed Logic (SIL)

$\boxed{\phi, \psi : \mathbb{N} \to \mathbb{B}}$

$$
\begin{aligned}
\mathsf{true}^\circ(k) &= \mathsf{true} \\
\mathsf{false}^\circ(k) &= \mathsf{false} \\
(\phi \,\mathsf{and}^\circ\, \psi)(k) &= \phi(k) \text{ and } \psi(k) \\
(\phi \,\mathsf{or}^\circ\, \psi)(k) &= \phi(k) \text{ or } \psi(k) \\
(\forall^\circ x, P(x))(k) &= \forall x, P(x)(k) \\
(\rhd^\circ \phi)(k) &= \forall j, j < k \Rightarrow \phi(j) \\
&\vdots
\end{aligned}
$$

$\boxed{\psi_1, \ldots, \psi_n \vdash^\circ \phi}$

$$\psi_1, \ldots, \psi_n \vdash^\circ \phi \quad = \quad \forall k, \psi_1(k) \text{ and } \cdots \ \psi_n(k) \Rightarrow \phi(k)$$

A Step-indexed Logic (SIL)

Proof rules regarding the “later“ operator $\triangleright^\circ$:

$$\frac{\mathcal{P} \vdash^\circ \phi}{\mathcal{P} \vdash^\circ \triangleright^\circ \phi} \qquad \frac{\mathcal{P} \vdash^\circ \triangleright^\circ (\phi \Rightarrow^\circ \psi)}{\mathcal{P} \vdash^\circ \triangleright^\circ \phi \Rightarrow^\circ \triangleright^\circ \psi} \qquad \ldots$$

$$\frac{\mathcal{P} \vdash^\circ \triangleright^\circ \phi \qquad \phi, \mathcal{P} \vdash^\circ \psi}{\mathcal{P} \vdash^\circ \triangleright^\circ \psi}$$

Löb Induction:

$$\frac{\triangleright^\circ \phi, \mathcal{P} \vdash^\circ \phi}{\mathcal{P} \vdash^\circ \phi}$$

Recipe: extend $\mathcal{V}$ and $\mathcal{E}$ to open terms

$$
\begin{aligned}
\mathcal{G}(A_1, \ldots, A_n)(\sigma) &= \mathcal{V}(A_1)(\sigma_0), \ldots, \mathcal{V}(A_n)(\sigma_n) \\
\Gamma \models^{\mathcal{V}} V : A &= \forall \sigma, \mathcal{G}(\Gamma)(\sigma) \vdash^{\circ} \mathcal{V}(A)(\sigma(V)) \\
\Gamma \models M : A &= \forall \sigma, \mathcal{G}(\Gamma)(\sigma) \vdash^{\circ} \mathcal{E}(A)(\sigma(M))
\end{aligned}
$$

Recipe: prove the Fundamental Lemma

Lemma (Fundamental)

(1) $\Gamma \vdash^{\mathcal{V}} V : A$ implies $\Gamma \models^{\mathcal{V}} V : A$ and
(2) $\Gamma \vdash M : A$ implies $\Gamma \models M : A$.

Proceed by mutual induction on $\Gamma \vdash^{\mathcal{V}} V : A$ and $\Gamma \vdash M : A$.
By tradition, each case of the proof is proved by a separate lemma. These lemmas are called the "compatibility" lemmas.

Compatibility Lemmas

Lemma (Compatibility for `zero`)
$\Gamma \models^{\mathcal{V}} \texttt{zero} : \mathbb{N}$.

Proof.
Let σ be a substitution. We need to show that

$$\mathcal{G}(\Gamma)(\sigma) \vdash^{\circ} \mathcal{V}(\mathbb{N})(\sigma(\texttt{zero}))$$

which is equivalent to

$$\mathcal{G}(\Gamma)(\sigma) \vdash^{\circ} \mathsf{true}^{\circ}$$

which is trivial to prove. $\square$

Some compatibility lemmas are easy.

Compatibility Lemmas, continued

Lemma (Compatibility for suc(V))

If $\Gamma \models^{\mathcal{V}} V : \mathbb{N}$, *then* $\Gamma \models^{\mathcal{V}} \mathtt{suc}(V) : \mathbb{N}$.

Proof.

Let σ be a substitution. We need to show that

$$\mathcal{G}(\Gamma)(\sigma) \vdash^{\circ} \mathcal{V}(\mathbb{N})(\sigma(\mathtt{suc}(V)))$$

which is equivalent to

$$\mathcal{G}(\Gamma)(\sigma) \vdash^{\circ} \mathcal{V}(\mathbb{N})(\sigma(V))$$

which we obtain from the premise. □

Compatibility Lemmas, continued

Lemma (Compatibility for λN)

If $A, \Gamma \models N : B$, *then* $\Gamma \models^{\mathcal{V}} \lambda N : A \to B$.

Proof.

Let σ be a substitution. We need to show that

$$\mathcal{G}(\Gamma)(\sigma) \vdash^{\circ} \forall^{\circ} W, \rhd^{\circ} \mathcal{V}(A)(W) \Rightarrow^{\circ} \rhd^{\circ} \mathcal{E}(B)(\mathsf{ext}(\sigma)(N)[W])$$

Let W be a value and assume $\rhd^{\circ} \mathcal{V}(A)(W)$.
From the premise $A, \Gamma \models N : B$ we have
$\mathcal{V}(A)(W), \mathcal{G}(\Gamma)(\sigma) \vdash^{\circ} \mathcal{E}(B)((W, \sigma)(N))$.
With the assumption, we have $\rhd^{\circ} \mathcal{E}(B)((W, \sigma)(N))$. We conclude via the following equality

$$\begin{aligned} \mathsf{ext}(\sigma)(N)[W] &= (W, \downarrow\uparrow \sigma_0, \downarrow\uparrow \sigma_1, \ldots)(N) \\ &= (W, \sigma)(N) \end{aligned}$$

Compatibility Lemmas, continued

Lemma (Compatibility for μV)

If $A \to B, \Gamma \models^{\mathcal{V}} V : A \to B$, *then* $\Gamma \models^{\mathcal{V}} \mu V : A \to B$.

Proof.

Let σ be a substitution. We need to show that
$\mathcal{G}(\Gamma)(\sigma) \vdash^{\circ} \mathcal{V}(A \to B)(\mu\, V')$ where $V' = \mathsf{ext}(\sigma)(V)$.
We proceed by Löb induction, so we may assume
$\rhd^{\circ} \mathcal{V}(A \to B)(\mu\, V')$ (IH)
From the premise of this lemma we have
$\mathcal{G}(A \to B, \Gamma)(\sigma') \vdash^{\circ} \mathcal{V}(A \to B, \sigma'(V))$ where $\sigma' = (\mu\, V', \sigma)$,
and therefore
$\mathcal{G}(\Gamma)(\sigma) \vdash^{\circ} \mathcal{V}(A \to B)(\mu\, V') \Rightarrow \mathcal{V}(A \to B)(\sigma'(V))$.
Together with (IH), we have
$\mathcal{G}(\Gamma)(\sigma) \vdash^{\circ} \rhd^{\circ} \mathcal{V}(A \to B)(\sigma'(V))$
which is equivalent to our goal. $\square$

Bind Lemma

Many of the compatibility lemmas involve terms that have subterms. For example, the term $\mathtt{suc}(M)$ has subterm M. We'll know that $\mathcal{E}(\mathbb{N})(M)$ and want to show $\mathcal{E}(\mathbb{N})(\mathtt{suc}(M))$. From $\mathcal{E}(\mathbb{N})(M)$ we can deduce that either M diverges or $M \longrightarrow^* V$ where $\mathcal{V}(\mathbb{N})(V)$ for some V. If M diverges, so does $\mathtt{suc}(M)$. If M reduces to V, then to prove $\mathcal{E}(\mathbb{N})(\mathtt{suc}(M))$ it suffices to prove $\mathcal{E}(\mathbb{N})(\mathtt{suc}(V))$.
Generalizing this reasoning to any frame F with subterm M gives us the following Bind lemma.

Lemma (Bind)

If $\mathcal{P} \vdash^\circ \mathcal{E}(B)(M)$
and $\mathcal{P} \vdash^\circ \forall^\circ V, M \longrightarrow^* V \Rightarrow^\circ \mathcal{V}(B)(V) \Rightarrow^\circ \mathcal{E}(A)(F(\!|V|\!))$
then $\mathcal{P} \vdash^\circ \mathcal{E}(A)(F(\!|M|\!))$.

Compatibility Lemmas, continued

Lemma

If $\mathcal{V}(A{\to}B)(V)$ *and* $\mathcal{V}(A)(W)$*, then* $\mathcal{E}(B)(V\ \ W)$*.*

Proof.

We proceed by Löb induction, so we may assume
$\forall^\circ VW, \rhd^\circ\mathcal{V}(A{\to}B)(V)\ \mathsf{and}^\circ\ \rhd^\circ\mathcal{V}(A)(W) \Rightarrow^\circ\ \rhd^\circ\mathcal{E}(B)(V\ \ W)$.
From $\mathcal{V}(A{\to}B)(V)$ we know that either $V = \lambda N$ or $V = \mu\, V'$.
Suppose $V = \lambda N$. We have progress because $(\lambda N)\, W \longrightarrow N[W]$.
We have preservation because $\mathcal{V}(A{\to}B)(\lambda N)$ with premise
$\mathcal{V}(A)(W)$ tells us that $\rhd^\circ\mathcal{E}(B)(N[W])$.
Suppose $V = \mu\, V'$. We have progress: $(\mu\, V')\, W \longrightarrow V'[\mu\, V']\ W$.
For preservation we need to show $\rhd^\circ\mathcal{E}(B)(V'[\mu\, V']\ W)$.
From $\mathcal{V}(A{\to}B)(\mu\, V')$ we have $\rhd^\circ\mathcal{V}(A{\to}B)(V'[\mu\, V'])$ and from
$\mathcal{V}(A)(W)$ we have $\rhd^\circ\mathcal{V}(A)(W)$. So the induction hypothesis gives
us $\rhd^\circ\mathcal{E}(B)(V'[\mu\, V']\ W)$. $\square$

Compatibility Lemmas, continued

Lemma (Compatibility for application)

If $\Gamma \models L : A \to B$ *and* $\Gamma \models M : A$, *then* $\Gamma \models L \; M : B$.

Proof.

Let σ be a substitution. We need to prove that $\mathcal{G}(\Gamma)(\sigma) \vdash^{\circ} \mathcal{E}(B)(\sigma(L) \;\; \sigma(M))$.

We apply the Bind Lemma to $\sigma(L)$ and $\sigma(M)$ to obtain $\sigma(L) \longrightarrow^{*} V$, $\sigma(M) \longrightarrow^{*} W$, $\mathcal{V}(A{\to}B)(V)$, $\mathcal{V}(A)(W)$, and it remains to prove $\mathcal{E}(B)(V \;\; W)$, which we obtain by the previous lemma. $\square$

Recipe: $\mathcal{E}(A)(M)$ implies Type Safety

Lemma (Multi-step Preservation)

If $M \longrightarrow^* N$ and $\mathcal{E}(A)(M)$, then $\mathcal{E}(A)(N)$.

Proof.

Proceed by induction on the reduction sequence, using the preservation part of $\mathcal{E}$ at each step. $\square$

Theorem (Type Safety)

If $\emptyset \vdash M : A$ and $M \longrightarrow^* N$,
then N is a value or $N \longrightarrow N'$ for some N'.

Proof.

Apply the Fundamental Lemma to obtain $\mathcal{E}(A)(M)$. Then by Multi-step Preservation, we have $\mathcal{E}(A)(N)$. We conclude using the progress part of $\mathcal{E}(A)(N)$. $\square$

Conclusion

- Logical Relations Recipe:
  Define $\mathcal{V}(A)(V)$ and $\mathcal{E}(A)(M)$.
  Extend $\mathcal{V}$ and $\mathcal{E}$ to open terms.
  Prove the Fundamental Lemma.
  Prove that $\mathcal{E}$ implies your theorem.
- A Step-Indexed Logic:
  Enables the definition of recursive predicates ($\mathcal{V}$ and $\mathcal{E}$) on full-featured programming languages.
  Hides the bookkeeping of the step indexing.
  Automates the proofs of monotonicity of $\mathcal{V}$ and $\mathcal{E}$.