TD: Logical Relations for Type Systems Safety

Jacques-Henri Jourdan, MPRI 2-4

2023/02/21

We are interested in the logical relations approach to proving type system safety. We focus on a very simple setting: the safety of system F, extended with integers and some arithmetic operations.

All the definitions, including that of the logical relation, are given in Figure 1. Note that division by 0 is considered safe, but non-deterministically returns an arbitrary integer (this is an excuse to introduce non-determinism in the calculus).

Moreover, note that the definition of the logical relation uses a predicate $\mathit{Safe}(e)$, meaning that e cannot reduce in a stuck state, in any number of steps.

Exercise 1. State and prove *adequacy* of the logical relation.

Exercise 2. State and establish lemmas for proving $e \in \mathcal{E}^\rho(\tau)$ in the following cases:

- e is a value;
- e is of the form $E[e']$;
- the set of direct reducts of e (i.e., $\{e' \mid e \longrightarrow e'\}$) is known.

Exercise 3. State and prove the fundamental theorem of the logical relation.

Exercise 4. Conclude the safety of the type system.

Exercise 5. Discuss difficulties arising with extensions of this proof: what if we added tuples to the type system? Subtyping? Recursive types? References?

Syntax:

$$
\begin{aligned}
\tau &::= \alpha \mid \tau \to \tau \mid \forall \alpha.\, \tau \mid \texttt{int} \\
e &::= x \mid e\, e \mid \lambda x.\, e \mid n \mid e + e \mid e/e \\
v &::= \lambda x.\, e \mid n \\
E &::= \Box \mid E\, e \mid v\, E \mid E + e \mid v + e \mid E/e \mid v/e
\end{aligned}
$$

Operational semantics:

$$\frac{e_1 \longrightarrow e_2}{E[e_1] \longrightarrow E[e_2]} \qquad (\lambda x.\, e)\, v \longrightarrow e[x/v] \qquad \frac{n_1 + n_2 = n \text{ (as an arithmetic operation)}}{n_1 + n_2 \longrightarrow n}$$

$$\frac{n_2 \neq 0 \qquad \lfloor n_1/n_2 \rfloor = n \text{ (as an arithmetic operation)}}{n_1/n_2 \longrightarrow n} \qquad n/0 \longrightarrow n'$$

Typing rules:

$$\textsc{Var}\ \frac{x : \tau \in \Gamma}{\Gamma \vdash x : \tau} \qquad \textsc{Lam}\ \frac{\Gamma, x : \tau_1 \vdash e : \tau_2}{\Gamma \vdash \lambda x.\, e : \tau_1 \to \tau_2} \qquad \textsc{App}\ \frac{\Gamma \vdash e_1 : \tau_1 \to \tau_2 \qquad \Gamma \vdash e_2 : \tau_1}{\Gamma \vdash e_1\, e_2 : \tau_2}$$

$$\textsc{AllIntro}\ \frac{\Gamma \vdash e : \tau \qquad \alpha \notin \mathcal{FV}(\Gamma)}{\Gamma \vdash e : \forall \alpha.\, \tau} \qquad \textsc{AllElim}\ \frac{\Gamma \vdash e : \forall \alpha.\, \tau_1}{\Gamma \vdash e : \tau_1[\alpha/\tau_2]} \qquad \textsc{Int}\ \frac{n \in \mathbb{Z}}{\Gamma \vdash n : \texttt{int}}$$

$$\textsc{Add}\ \frac{\Gamma \vdash e_1 : \texttt{int} \qquad \Gamma \vdash e_2 : \texttt{int}}{\Gamma \vdash e_1 + e_2 : \texttt{int}}$$

Logical relation:

$$
\begin{aligned}
\mathcal{V}^\rho(\alpha) &\triangleq \rho(\alpha) \\
\mathcal{V}^\rho(\texttt{int}) &\triangleq \mathbb{Z} \\
\mathcal{V}^\rho(\tau_1 \to \tau_2) &\triangleq \{v \mid \forall v_1 \in \mathcal{V}^\rho(\tau_1).\ (v\, v_1) \in \mathcal{E}^\rho(\tau_2)\} \\
\mathcal{V}^\rho(\forall \alpha.\, \tau) &\triangleq \{v \mid \forall A.\ v \in \mathcal{V}^{\rho[\alpha \leftarrow A]}(\tau)\} \\
\mathcal{E}^\rho(\tau) &\triangleq \{e \mid \mathit{Safe}(e) \wedge \forall v.\ e \longrightarrow^* v \Longrightarrow v \in \mathcal{V}^\rho(\tau)\} \\
\mathcal{G}^\rho(\Gamma) &\triangleq \{\gamma \mid \forall (x : \tau) \in \Gamma.\ \gamma(x) \in \mathcal{V}^\rho(\tau)\} \\
\Gamma \vDash e : \tau &\triangleq \forall \rho.\ \forall \gamma \in \mathcal{G}^\rho(\Gamma).\ \gamma(e) \in \mathcal{E}^\rho(\tau)
\end{aligned}
$$

Figure 1: Definitions