Logical relations: safety of system F (Quick Reference)

Amin Timany

October 9, 2023

Syntax

$$\begin{array}{rl} \textit{variables}(\mathsf{Var}) & \quad x, y, z, \ldots \\ \textit{expressions}(\mathsf{E}) & e ::= x \mid tt \mid (e, e) \mid \textit{fst}\ e \mid \textit{snd}\ e \mid \lambda x.\ e \mid e\ e \mid \Lambda\ e \mid e\ \_ \\ \textit{values}(\mathsf{Val}) & v ::= tt \mid (v, v) \mid \lambda x.\ e \mid \Lambda\ e \end{array}$$

Types and typing

$$\begin{array}{rl} \textit{type variables}(\mathsf{TVar}) & \quad \alpha, \delta, \zeta, \ldots \\ \textit{types}(\mathsf{Typ}) & \tau ::= \alpha \mid () \mid \tau \times \tau \mid \tau \to \tau \mid \forall \alpha.\ \tau \\ \textit{typing context}\ (\mathsf{TCtx}) & \Gamma ::= \cdot \mid x : \tau, \Gamma \\ \textit{context of typing variables}\ (\mathsf{TCtx}) & \Delta ::= \cdot \mid \alpha, \Delta \end{array}$$

$$\textsc{T-Unit}\ \ \Delta; \Gamma \vdash tt : () \qquad \textsc{T-Var}\ \frac{x : \tau \in \Gamma}{\Delta; \Gamma \vdash x : \tau} \qquad \textsc{T-Prod}\ \frac{\Delta; \Gamma \vdash e_1 : \tau_1 \qquad \Delta; \Gamma \vdash e_2 : \tau_2}{\Delta; \Gamma \vdash (e_1, e_2) : \tau_1 \times \tau_2} \qquad \textsc{T-Fst}\ \frac{\Delta; \Gamma \vdash e : \tau_1 \times \tau_2}{\Delta; \Gamma \vdash \textit{fst}\ e : \tau_1}$$

$$\textsc{T-Snd}\ \frac{\Delta; \Gamma \vdash e : \tau_1 \times \tau_2}{\Delta; \Gamma \vdash \textit{snd}\ e : \tau_2} \qquad \textsc{T-Lam}\ \frac{\Delta; x : \tau_1, \Gamma \vdash e : \tau_2}{\Delta; \Gamma \vdash \lambda x.\ e : \tau_1 \to \tau_2} \qquad \textsc{T-App}\ \frac{\Delta; \Gamma \vdash e : \tau_1 \to \tau_2 \qquad \Delta; \Gamma \vdash e' : \tau_1}{\Delta; \Gamma \vdash e\ e' : \tau_2}$$

$$\textsc{T-TLam}\ \frac{\alpha, \Delta; \Gamma \vdash e : \tau \qquad \alpha\ \text{ does not appear freely in }\ \Gamma}{\Delta; \Gamma \vdash \Lambda\ e : \forall \alpha.\ \tau} \qquad \textsc{T-TApp}\ \frac{\Delta; \Gamma \vdash e : \forall \alpha.\ \tau}{\Delta; \Gamma \vdash e\ \_ : \tau[\tau'/\alpha]}$$

Operational semantics (CBV)

$$\textit{fst}\ (v_1, v_2) \leadsto_h v_1 \qquad \textit{snd}\ (v_1, v_2) \leadsto_h v_2 \qquad (\lambda x.\ e)\ v \leadsto_h e[v/x] \qquad (\Lambda\ e)\ \_ \leadsto_h e$$

$$\frac{e \leadsto_h e'}{\mathbf{K}[e] \leadsto \mathbf{K}[e']}$$

$$\textit{evaluation contexts}\ (\mathsf{ECtx}) \quad \mathbf{K} ::= [] \mid \textit{fst}\ \mathbf{K} \mid \textit{snd}\ \mathbf{K} \mid (\mathbf{K}, e) \mid (v, \mathbf{K}) \mid \mathbf{K}\ e \mid v\ \mathbf{K} \mid \mathbf{K}\ \_$$

Type safety

$$\forall e, \tau.\ \cdot; \cdot \vdash e : \tau \implies \mathbf{Safe}(e)$$

where

$$\mathbf{Safe}(e) \triangleq \forall e'.\ e \rightsquigarrow^* e' \implies e' \in \mathsf{Val} \vee \exists e''.\ e \rightsquigarrow e''$$

Parameterized Safety

$$\mathbf{Safe}_P(e) \triangleq \forall e'.\ e \rightsquigarrow^* e' \implies (e' \in \mathsf{Val} \wedge P(e')) \vee \exists e''.\ e \rightsquigarrow e''$$

Parameterized safety implies safety: $\mathbf{Safe}_P(e) \implies \mathbf{Safe}(e)$

Safe-Mono. $(\forall v.\ P(v) \implies Q(v)) \implies \boldsymbol{Safe}_P(e) \implies \boldsymbol{Safe}_Q(e)$

Safe-Val. $P(v) \implies \boldsymbol{Safe}_P(v)$

Safe-Bind. $\boldsymbol{Safe}_Q(e) \wedge (\forall v.\ Q(v) \implies \boldsymbol{Safe}_P(\mathbf{K}[v])) \implies \boldsymbol{Safe}_P(\mathbf{K}[e])$

Safe-Step. $e \rightsquigarrow e' \wedge \boldsymbol{Safe}_P(e') \implies \boldsymbol{Safe}_P(e)$

Logical Relations

$$\begin{aligned}
[\![\Delta \vdash \alpha]\!]_\xi &\triangleq \xi(\alpha) \\
[\![\Delta \vdash ()]\!]_\xi (v) &\triangleq v = tt \\
[\![\Delta \vdash \tau_1 \times \tau_2]\!]_\xi (v) &\triangleq \exists v_1, v_2.\ v = (v_1, v_2) \wedge [\![\Delta \vdash \tau_1]\!]_\xi (v_1) \wedge [\![\Delta \vdash \tau_1]\!]_\xi (v_2) \\
[\![\Delta \vdash \tau_1 \to \tau_2]\!]_\xi (v) &\triangleq \exists x, e.\ v = \lambda x.\ e \wedge \forall v'.\ [\![\Delta \vdash \tau_1]\!]_\xi (v') \implies [\![\Delta \vdash \tau_2]\!]^{\mathbf{E}}_\xi (e[v'/x]) \\
[\![\Delta \vdash \forall \alpha.\ \tau]\!]_\xi (v) &\triangleq \exists e.\ v = \Lambda\ e \wedge \forall P \in 2^{\mathsf{Val}}.\ [\![\alpha, \Delta \vdash \tau]\!]^{\mathbf{E}}_{[\alpha \mapsto P]\xi} (e)
\end{aligned}$$

$$\begin{aligned}
[\![\Delta \vdash \cdot]\!]_\xi (vs) &\triangleq |vs| = 0 \\
[\![\Delta \vdash x : \tau, \Gamma]\!]_\xi (vs) &\triangleq \exists v, vs'.\ vs = v, vs' \wedge [\![\Delta \vdash \tau]\!]_\xi (v) \wedge [\![\Delta \vdash \Gamma]\!]_\xi (vs')
\end{aligned}$$

LogRel-Subst. $[\![\Delta \vdash \tau[\tau'/\alpha]]\!]_\xi (v) \iff [\![\alpha, \Delta \vdash \tau]\!]_{[\alpha \mapsto [\![\Delta \vdash \tau']\!]_\xi]\xi} (v)$

LogRel-Weaken. *When α the **does not** appear freely in τ,* $[\![\Delta \vdash \tau]\!]_\xi (v) \iff [\![\alpha, \Delta \vdash \tau]\!]_{[\alpha \mapsto P]\xi} (v)$

LogRel-Seq-Weaken. *When α the **does not** appear freely in Γ,*

$$[\![\Delta \vdash \Gamma]\!]_\xi (vs) \iff [\![\alpha, \Delta \vdash \Gamma]\!]_{[\alpha \mapsto P]\xi} (vs)$$

Fundamental Theorem (of logical relations)**.** *For any e, Δ, Γ and τ such that $\Delta; \Gamma \vdash e : \tau$ we have:*

$$\forall \xi, vs.\ [\![\Delta \vdash \Gamma]\!]_\xi (vs) \implies [\![\Delta \vdash \tau]\!]^{\boldsymbol{E}}_\xi (e[vs/xs])$$

where xs is the sequence of variables of Γ and $e[vs/xs]$ is a shorthand for $e[v_1, \ldots, v_n/x_1, \ldots, x_n]$ which is the term e where x_i's are substituted with v_i's simultaneously.