Type safety of Simply Typed Lambda Calculus

Maud van de Lockant
Susan Withaar

Table of contents

Definition simple typed lambda environment

$$\tau ::= \text{bool} \mid \tau \to \tau$$

$$e ::= x \mid \text{true} \mid \text{false} \mid \text{if } e \text{ then } e \text{ else } e \mid \lambda x : \tau.\ e \mid e\ e$$

$$v ::= \text{true} \mid \text{false} \mid \lambda x : \tau.\ e$$

$$E ::= [] \mid \text{if E then } e \text{ else } e \mid \text{E } e \mid v \text{ E}$$

Type safety

- “well-typed programs do not go wrong.” -Robin Milner
- “well-typed programs do not get stuck.”

$$\mathrm{safe}(e) := \forall e'.\ e \mapsto^* e' \Rightarrow \mathrm{val}(e') \vee \exists e''.\ e' \mapsto e''$$

Type safety theorem

Theorem (Type safety): $\cdot \vdash e : \tau \Rightarrow \mathrm{safe}(e)$.

A) $\cdot \vdash e : \tau \Rightarrow \cdot \models e : \tau$ (Theorem)

B) $\cdot \models e : \tau \Rightarrow \mathrm{safe}(e)$

$$\mathrm{safe}(e) := \forall e'.\ e \mapsto^* e' \Rightarrow \mathrm{val}(e') \vee \exists e''.\ e' \mapsto e''$$

Logical relations for type safety

$$\tau ::= \text{bool} \mid \tau \to \tau$$
$$e ::= x \mid \text{true} \mid \text{false} \mid \text{if } e \text{ then } e \text{ else } e \mid \lambda x : \tau.\ e \mid e\ e$$
$$v ::= \text{true} \mid \text{false} \mid \lambda x : \tau.\ e$$

$$\mathcal{V}[\![\text{bool}]\!] := \{\text{true, false}\}$$

$$\mathcal{V}[\![\tau_1 \to \tau_2\ ]\!] := \{\lambda x : \tau_1.\ e \mid \forall v \in \mathcal{V}[\![\tau_1]\!].\ e[v/x] \in \mathcal{E}[\![\tau_2]\!]\}$$

$$\mathcal{E}[\![\tau]\!] := \{e \mid \forall e'.\ e \mapsto^* e' \wedge \text{irred}(e') \Rightarrow e' \in \mathcal{V}[\![\tau]\!]\}$$

$$\text{irred}(e) := \nexists e'.\ e \mapsto e'$$

$$\text{safe}(e) := \forall e'.\ e \mapsto^* e' \Rightarrow \text{val}(e') \vee \exists e''.\ e' \mapsto e''$$

Semantic well-typedness

Theorem (Type safety): $\cdot \vdash e : \tau \Rightarrow \mathrm{safe}(e)$.

A) $\cdot \vdash e : \tau \Rightarrow \cdot \models e : \tau$ (Theorem)

B) $\cdot \models e : \tau \Rightarrow \mathrm{safe}(e)$

$$\mathcal{G}[\![\cdot]\!] := \{\emptyset\}$$

$$\mathcal{G}[\![\Gamma, x : \tau]\!] := \{\gamma[x \mapsto v] \mid \gamma \in \mathcal{G}[\![\Gamma]\!] \land v \in \mathcal{V}[\![\tau]\!]\}$$

Semantic type safety / well-typedness: $\Gamma \models e : \tau := \forall \gamma \in \mathcal{G}[\![\Gamma]\!].\ \gamma(e) \in \mathcal{E}[\![\tau]\!]$

Proof of part B

$\mathrm{safe}(e) := \forall e'.\ e \mapsto^* e' \Rightarrow \mathrm{val}(e') \vee \exists e''.\ e' \mapsto e''$

$\mathrm{irred}(e) := \nexists e'.\ e \mapsto e'$

$\Gamma \models e : \tau := \forall \gamma \in \mathcal{G}[\![\Gamma]\!].\ \gamma(e) \in \mathcal{E}[\![\tau]\!]$

$\mathcal{G}[\![\cdot]\!] := \{\emptyset\}$

$\mathcal{E}[\![\tau]\!] := \{e \mid \forall e'.\ e \mapsto^* e' \wedge \mathrm{irred}(e') \Rightarrow e' \in \mathcal{V}[\![\tau]\!]\}$

B) $\cdot \models e : \tau \Rightarrow \mathrm{safe}(e)$

Proof. Suppose $e \mapsto^* e'$. To show: $\mathrm{val}(e')$ or $\exists e''.\ e' \mapsto e''$.
Either $\mathrm{irred}(e')$ or $\neg\mathrm{irred}(e')$.

1. Case $\neg\mathrm{irred}(e')$. Then $\exists e''.\ e' \mapsto e''$ ✓
2. Case $\mathrm{irred}(e')$. From $\cdot \models e : \tau$ we have $e \in \mathcal{E}[\![\tau]\!]$. Therefore, $e' \in \mathcal{V}[\![\tau]\!]$. Thus $\mathrm{val}(e')$ ✓

□

Fundamental Property/Basic Lemma Theorem (A)

$$\text{A)}\quad \cdot \vdash e : \tau \Rightarrow \cdot \models e : \tau \text{ (Theorem)}$$

Proof. Suppose $\cdot \vdash e : \tau$ we have to show $\cdot \models e : \tau$. We proceed by induction on the typing judgement

$$\boxed{\Gamma \vdash e : \tau}$$

$$\textsc{T-True}\ \frac{}{\Gamma \vdash \text{true} : \text{bool}} \qquad \textsc{T-False}\ \frac{}{\Gamma \vdash \text{false} : \text{bool}} \qquad \textsc{T-Var}\ \frac{\Gamma(x) = \tau}{\Gamma \vdash x : \tau}$$

$$\textsc{T-IfThenElse}\ \frac{\Gamma \vdash e : \text{bool} \qquad \Gamma \vdash e_1 : \tau \qquad \Gamma \vdash e_2 : \tau}{\Gamma \vdash \text{if } e \text{ then } e_1 \text{ else } e_2 : \tau}$$

$$\textsc{T-Abs}\ \frac{\Gamma, x : \tau_1 \vdash e : \tau_2}{\Gamma \vdash \lambda x : \tau_1.\ e : \tau_1 \to \tau_2} \qquad \textsc{T-App}\ \frac{\Gamma \vdash e_1 : \tau_2 \to \tau_1 \qquad \Gamma \vdash e_2 : \tau_2}{\Gamma \vdash e_1\ e_2 : \tau_1}$$

Fundamental Property/Basic Lemma Theorem (A)

$$\Gamma \models e : \tau := \forall \gamma \in \mathcal{G}[\![\Gamma]\!].\ \gamma(e) \in \mathcal{E}[\![\tau]\!]$$

Case $\dfrac{\textsc{T-True}}{\Gamma \vdash \text{true} : \text{bool}}$

$$\mathcal{E}[\![\tau]\!] := \{e \mid \forall e'.\ e \mapsto^* e' \wedge \text{irred}(e') \Rightarrow e' \in \mathcal{V}[\![\tau]\!]\}$$

$$\text{irred}(e) := \nexists e'.\ e \mapsto e'$$

A) $\cdot \vdash e : \tau \Rightarrow \cdot \models e : \tau$

Case to show $\Gamma \models \mathit{true} : \mathit{bool}$

Proof. Suppose $\gamma \in \mathcal{G}[\![\Gamma]\!]$ to show: $\gamma(\mathit{true}) \in \mathcal{E}[\![\mathit{bool}]\!]$.

Since $\text{irred}(\mathit{true})$ therefore to show: $\mathit{true} \in \mathcal{V}[\![\mathit{bool}]\!]$.

$$\mathcal{V}[\![\text{bool}]\!] := \{\text{true}, \text{false}\}$$

$\square$

Fundamental Property/Basic Lemma Theorem (A)

$$\boxed{\Gamma \vdash e : \tau}$$

$$\textsc{T-True}\ \frac{}{\Gamma \vdash \text{true} : \text{bool}}$$

$$\textsc{T-False}\ \frac{}{\Gamma \vdash \text{false} : \text{bool}}$$

$$\textsc{T-Var}\ \frac{\Gamma(x) = \tau}{\Gamma \vdash x : \tau}$$

$$\textsc{T-IfThenElse}\ \frac{\Gamma \vdash e : \text{bool} \qquad \Gamma \vdash e_1 : \tau \qquad \Gamma \vdash e_2 : \tau}{\Gamma \vdash \text{if } e \text{ then } e_1 \text{ else } e_2 : \tau}$$

$$\textsc{T-Abs}\ \frac{\Gamma, x : \tau_1 \vdash e : \tau_2}{\Gamma \vdash \lambda x : \tau_1.\ e : \tau_1 \to \tau_2}$$

$$\textsc{T-App}\ \frac{\Gamma \vdash e_1 : \tau_2 \to \tau_1 \qquad \Gamma \vdash e_2 : \tau_2}{\Gamma \vdash e_1\ e_2 : \tau_1}$$

Fundamental Property/Basic Lemma Theorem (A)

$\Gamma \models e : \tau := \forall \gamma \in \mathcal{G}[\![\Gamma]\!].\ \gamma(e) \in \mathcal{E}[\![\tau]\!]$

$\mathcal{E}[\![\tau]\!] := \{e \mid \forall e'.\ e \mapsto^* e' \wedge \text{irred}(e') \Rightarrow e' \in \mathcal{V}[\![\tau]\!]\}$

$\mathcal{V}[\![\tau_1 \to \tau_2\ ]\!] := \{\lambda x : \tau_1.\ e \mid \forall v \in \mathcal{V}[\![\tau_1]\!].\ e[v/x] \in \mathcal{E}[\![\tau_2]\!]\}$

Case $\dfrac{\Gamma, x : \tau_1 \vdash e : \tau_2}{\Gamma \vdash \lambda x : \tau_1.\ e : \tau_1 \to \tau_2}$ T-ABS

A) $\cdot \vdash e : \tau \Rightarrow \cdot \models e : \tau$
Case to show $\Gamma \models \lambda x : \tau_1.e : \tau_1 \to \tau_2$

Proof. Suppose $\gamma \in \mathcal{G}[\![\Gamma]\!]$to show: $\gamma(\lambda x : \tau_1.e) \in \mathcal{E}[\![\tau_1 \to \tau_2]\!]$.
To show $\equiv (\lambda x : \tau_1.\gamma(e)) \in \mathcal{E}[\![\tau_1 \to \tau_2]\!]$.

Suppose $\lambda x : \tau_1.\gamma(e) \mapsto^* e' \wedge irred(e')$ To show: $e' \in \mathcal{V}[\![\tau_1 \to \tau_2]\!]$.
Since $\lambda x : \tau_1.\gamma(e)$ is a value $e' = \lambda x : \tau_1.\gamma(e)$
Therefore to show: $\lambda x : \tau_1.\gamma(e) \in \mathcal{V}[\![\tau_1 \to \tau_2]\!]$.

$v ::= \text{true} \mid \text{false} \mid \lambda x : \tau.\ e$

Suppose $v \in \mathcal{V}[\![\tau_1]\!]$to show: $\gamma(e)[v/x] \in \mathcal{E}[\![\tau_2]\!]$.

$\text{irred}(e) := \nexists e'.\ e \mapsto e'$

Fundamental Property/Basic Lemma Theorem (A)

To show: $\gamma(e)[v/x] \in \mathcal{E}[\![\tau_2]\!]$

Case $\dfrac{\Gamma, x : \tau_1 \vdash e : \tau_2}{\Gamma \vdash \lambda x : \tau_1.\ e : \tau_1 \to \tau_2}$ T-ABS

$\mathcal{G}[\![\Gamma, x : \tau]\!] := \{\gamma[x \mapsto v] \mid \gamma \in \mathcal{G}[\![\Gamma]\!] \wedge v \in \mathcal{V}[\![\tau]\!]\}$

$\Gamma \models e : \tau := \forall \gamma \in \mathcal{G}[\![\Gamma]\!].\ \gamma(e) \in \mathcal{E}[\![\tau]\!]$

Induction Hypothesis $\Gamma, x : \tau_1 \models e : \tau_2$
Instantiate $\gamma[x \mapsto v] \in \mathcal{G}[\![\Gamma, x : \tau_1]\!]$with conditions $\gamma \in \mathcal{G}[\![\Gamma]\!] \wedge v \in \mathcal{V}[\![\tau_1]\!]$.
Gives $\gamma[x \mapsto v](e) \in \mathcal{E}[\![\tau_2]\!] \equiv \gamma(e)[v/x] \in \mathcal{E}[\![\tau_2]\!]$ $\square$