CS101

Special Topics in Computer Science

Language-Based Security

Lecture 3: Type Preservation in λ-Calculus

Aleksey Nogin

October 12, 2005

Reminder: λ-Calculus Typing Rules

Here Γ and Δ stand for arbitrary number of *hypotheses* in a sequent.

$$\frac{}{\Gamma \vdash n \in \texttt{int}}\ (\textit{Number}) \qquad \frac{}{\Gamma; x : t; \Delta \vdash x \in t}\ (\textit{Var})$$

$$\frac{\Gamma \vdash e_1 \in \texttt{int} \quad \Gamma \vdash e_2 \in \texttt{int}}{\Gamma \vdash e_1\ op\ e_2 \in \texttt{int}}\ (\textit{Binop})$$

$$\frac{\Gamma \vdash e_1 \in t_1 \rightarrow t_2 \quad \Gamma \vdash e_2 \in t_1}{\Gamma \vdash (e_1\ e_2) \in t_2}\ (\textit{Apply})$$

$$\frac{\Gamma; x : t_1 \vdash e \in t_2}{\Gamma \vdash \lambda x : t_1 . e \in (t_1 \rightarrow t_2)}\ (\textit{Fun})$$

Substitution Lemma

Lemma.
If $\Gamma; x : t_1; \Delta \vdash e \in t_2$ and $\Gamma; \Delta \vdash e' \in t_1$, then $\Gamma; \Delta \vdash e[e'/x] \in t_2$.

Substitution Lemma

Lemma.
If $\Gamma; x : t_1; \Delta \vdash e \in t_2$ and $\Gamma; \Delta \vdash e' \in t_1$, then $\Gamma; \Delta \vdash e[e'/x] \in t_2$.

Proof. By induction on the derivation of $\Gamma; x : t_1; \Delta \vdash e \in t_2$

Substitution Lemma

Lemma.
If $\Gamma; x : t_1; \Delta \vdash e \in t_2$ and $\Gamma; \Delta \vdash e' \in t_1$, then
$\Gamma; \Delta \vdash e[e'/x] \in t_2$.

Proof. By induction on the derivation of $\Gamma; x : t_1; \Delta \vdash e \in t_2$

Case $\dfrac{}{\Gamma \vdash n \in \mathtt{int}}$ *(Number)* .

Substitution Lemma

Lemma.
If $\Gamma; x : t_1; \Delta \vdash e \in t_2$ and $\Gamma; \Delta \vdash e' \in t_1$, then
$\Gamma; \Delta \vdash e[e'/x] \in t_2$.

Proof. By induction on the derivation of $\Gamma; x : t_1; \Delta \vdash e \in t_2$

Case $\dfrac{}{\Gamma \vdash n \in \mathtt{int}}$ *(Number)* . Here e is n, t_2 is $\mathtt{int}$, $e[e'/x]$ is also n, $\Gamma; \Delta \vdash e[e'/x] \in t_2$ can be proven using *(Number)*.

Substitution Lemma

Lemma.
If $\Gamma; x : t_1; \Delta \vdash e \in t_2$ and $\Gamma; \Delta \vdash e' \in t_1$, then
$\Gamma; \Delta \vdash e[e'/x] \in t_2$.

Proof. By induction on the derivation of $\Gamma; x : t_1; \Delta \vdash e \in t_2$

Case $\dfrac{}{\Gamma \vdash n \in \mathtt{int}}$ *(Number)* . Here e is n, t_2 is $\mathtt{int}$, $e[e'/x]$ is also n, $\Gamma; \Delta \vdash e[e'/x] \in t_2$ can be proven using *(Number)*.

Case $\dfrac{}{\Gamma; x : t; \Delta \vdash x \in t}$ *(Var)* .

Substitution Lemma

Lemma.
If $\Gamma; x : t_1; \Delta \vdash e \in t_2$ and $\Gamma; \Delta \vdash e' \in t_1$, then
$\Gamma; \Delta \vdash e[e'/x] \in t_2$.

Proof. By induction on the derivation of $\Gamma; x : t_1; \Delta \vdash e \in t_2$

Case $\dfrac{}{\Gamma \vdash n \in \mathtt{int}}$ *(Number)* . Here e is n, t_2 is $\mathtt{int}$, $e[e'/x]$ is also n, $\Gamma; \Delta \vdash e[e'/x] \in t_2$ can be proven using *(Number)*.

Case $\dfrac{}{\Gamma; x : t; \Delta \vdash x \in t}$ *(Var)* . e is x, $e[e'/x]$ is e', $t_1 = t_2$.

Substitution Lemma

Lemma.
If $\Gamma; x : t_1; \Delta \vdash e \in t_2$ and $\Gamma; \Delta \vdash e' \in t_1$, then
$\Gamma; \Delta \vdash e[e'/x] \in t_2$.

Proof. By induction on the derivation of $\Gamma; x : t_1; \Delta \vdash e \in t_2$

Case $\dfrac{}{\Gamma \vdash n \in \mathtt{int}}$ *(Number)* . Here e is n, t_2 is `int`, $e[e'/x]$ is also n, $\Gamma; \Delta \vdash e[e'/x] \in t_2$ can be proven using *(Number)*.

Case $\dfrac{}{\Gamma; x : t; \Delta \vdash x \in t}$ *(Var)* . e is x, $e[e'/x]$ is e', $t_1 = t_2$.

Case $\dfrac{}{\Gamma; y : t; \Delta \vdash y \in t}$ *(Var)* .

Reminder: λ-Calculus Evaluation

Numbers and functions are values:

$$\dfrac{}{n \longrightarrow n} \qquad \dfrac{}{\lambda x : t.e \longrightarrow \lambda x : t.e}$$

Binary operations: $\dfrac{e_1 \longrightarrow n_1 \quad e_2 \longrightarrow n_2 \quad n = n_1\, op\, n_2}{e_1\, op\, e_2 \longrightarrow n}$

Function applications:

$$\dfrac{e_1 \longrightarrow \lambda x : t.e_1' \quad e_2 \longrightarrow v \quad e_1'[v/x] \longrightarrow v'}{e_1\ e_2 \longrightarrow v'}$$

Homework I

Reminder:
Homework I due Friday in class.

λ-Calculus: "Small-Step" Evaluation

Binary operations:

$$\dfrac{}{n_1\, op\, n_2 \rightarrow n} \quad (n = n_1\, op\, n_2)$$

λ-Calculus: "Small-Step" Evaluation

Binary operations:

$$\frac{}{n_1 \; op \; n_2 \rightarrow n} \quad (n = n_1 \; op \; n_2)$$

$$\frac{}{e_1 \; op \; e_2 \rightarrow}$$

λ-Calculus: "Small-Step" Evaluation

Binary operations:

$$\frac{}{n_1 \; op \; n_2 \rightarrow n} \quad (n = n_1 \; op \; n_2)$$

$$\frac{e_1 \rightarrow e_1'}{e_1 \; op \; e_2 \rightarrow}$$

λ-Calculus: "Small-Step" Evaluation

Binary operations:

$$\frac{}{n_1 \; op \; n_2 \rightarrow n} \quad (n = n_1 \; op \; n_2)$$

$$\frac{e_1 \rightarrow e_1'}{e_1 \; op \; e_2 \rightarrow e_1' \; op \; e_2}$$

λ-Calculus: "Small-Step" Evaluation

Binary operations:

$$\frac{}{n_1 \; op \; n_2 \rightarrow n} \quad (n = n_1 \; op \; n_2)$$

$$\frac{e_1 \rightarrow e_1'}{e_1 \; op \; e_2 \rightarrow e_1' \; op \; e_2} \qquad \frac{e_2 \rightarrow e_2'}{v \; op \; e_2 \rightarrow v \; op \; e_2'}$$

λ-Calculus: "Small-Step" Evaluation

Binary operations:

$$\frac{}{n_1 \; op \; n_2 \rightarrow n} \quad (n = n_1 \; op \; n_2)$$

$$\frac{e_1 \rightarrow e_1'}{e_1 \; op \; e_2 \rightarrow e_1' \; op \; e_2} \qquad \frac{e_2 \rightarrow e_2'}{v \; op \; e_2 \rightarrow v \; op \; e_2'}$$

Applications:

$$\frac{}{\lambda x : t.e \; v \rightarrow e[v/x]}$$

λ-Calculus: "Small-Step" Evaluation

Binary operations:

$$\frac{}{n_1 \; op \; n_2 \rightarrow n} \quad (n = n_1 \; op \; n_2)$$

$$\frac{e_1 \rightarrow e_1'}{e_1 \; op \; e_2 \rightarrow e_1' \; op \; e_2} \qquad \frac{e_2 \rightarrow e_2'}{v \; op \; e_2 \rightarrow v \; op \; e_2'}$$

Applications:

$$\frac{}{\lambda x : t.e \; v \rightarrow e[v/x]} \qquad \frac{e_1 \rightarrow e_1'}{e_1 \; e_2 \rightarrow e_1' \; e_2} \qquad \frac{e_2 \rightarrow e_2'}{v \; e_2 \rightarrow v \; e_2'}$$

Type Preservation Theorem

Theorem. If $\vdash e \in t$ and $e \rightarrow e'$, then $\vdash e' \in t$.

Proof. By induction on derivation of $e \rightarrow e'$.