CS 4110

Programming Languages & Logics

Lecture 20
Proving Type Soundness

20 October 2014

Announcements

- Today: Foster office hours 4-5pm
- PS 5 starter code updated last night

Simply-Typed Lambda Calculus

Syntax

expressions	$e ::= x \mid \lambda x{:}\tau.\, e \mid e_1\ e_2 \mid n \mid e_1 + e_2 \mid ()$
values	$v ::= \lambda x{:}\tau.\, e \mid n \mid ()$
types	$\tau ::= \mathbf{int} \mid \mathbf{unit} \mid \tau_1 \to \tau_2$

Simply-Typed Lambda Calculus

Syntax

expressions	$e ::= x \mid \lambda x{:}\tau.\, e \mid e_1\ e_2 \mid n \mid e_1 + e_2 \mid ()$
values	$v ::= \lambda x{:}\tau.\, e \mid n \mid ()$
types	$\tau ::= \mathbf{int} \mid \mathbf{unit} \mid \tau_1 \to \tau_2$

Dynamic Semantics

$$E ::= [\cdot] \mid E\ e \mid v\ E \mid E + e \mid v + E$$

$$\frac{e \to e'}{E[e] \to E[e']} \qquad \frac{}{(\lambda x{:}\tau.\, e)\ v \to e\{v/x\}} \qquad \frac{n = n_1 + n_2}{n_1 + n_2 \to n}$$

Simply-Typed Lambda Calculus

Static Semantics

Simply-Typed Lambda Calculus

Static Semantics

$$\frac{}{\Gamma \vdash n : \mathbf{int}}\ \text{T-Int}$$

Simply-Typed Lambda Calculus

Static Semantics

$$\frac{}{\Gamma \vdash n : \mathbf{int}}\ \text{T-Int} \qquad \frac{}{\Gamma \vdash () : \mathbf{unit}}\ \text{T-Unit}$$

Simply-Typed Lambda Calculus

Static Semantics

$$\frac{}{\Gamma \vdash n : \mathbf{int}}\ \text{T-Int} \qquad \frac{}{\Gamma \vdash () : \mathbf{unit}}\ \text{T-Unit}$$

$$\frac{\Gamma \vdash e_1 : \mathbf{int} \quad \Gamma \vdash e_2 : \mathbf{int}}{\Gamma \vdash e_1 + e_2 : \mathbf{int}}\ \text{T-Add}$$

Simply-Typed Lambda Calculus

Static Semantics

$$\frac{}{\Gamma \vdash n : \mathbf{int}}\ \text{T-Int} \qquad \frac{}{\Gamma \vdash () : \mathbf{unit}}\ \text{T-Unit}$$

$$\frac{\Gamma \vdash e_1 : \mathbf{int} \quad \Gamma \vdash e_2 : \mathbf{int}}{\Gamma \vdash e_1 + e_2 : \mathbf{int}}\ \text{T-Add}$$

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

Simply-Typed Lambda Calculus

Static Semantics

$$\frac{}{\Gamma \vdash n : \mathbf{int}}\ \text{T-Int} \qquad \frac{}{\Gamma \vdash () : \mathbf{unit}}\ \text{T-Unit}$$

$$\frac{\Gamma \vdash e_1 : \mathbf{int} \quad \Gamma \vdash e_2 : \mathbf{int}}{\Gamma \vdash e_1 + e_2 : \mathbf{int}}\ \text{T-Add}$$

$$\frac{\Gamma(x) = \tau}{\Gamma \vdash x : \tau}\ \text{T-Var} \qquad \frac{\Gamma, x : \tau \vdash e : \tau'}{\Gamma \vdash \lambda x : \tau.\, e : \tau \to \tau'}\ \text{T-Abs}$$

Simply-Typed Lambda Calculus

Static Semantics

$$\frac{}{\Gamma \vdash n : \mathbf{int}}\ \text{T-Int} \qquad \frac{}{\Gamma \vdash () : \mathbf{unit}}\ \text{T-Unit}$$

$$\frac{\Gamma \vdash e_1 : \mathbf{int} \quad \Gamma \vdash e_2 : \mathbf{int}}{\Gamma \vdash e_1 + e_2 : \mathbf{int}}\ \text{T-Add}$$

$$\frac{\Gamma(x) = \tau}{\Gamma \vdash x : \tau}\ \text{T-Var} \qquad \frac{\Gamma, x : \tau \vdash e : \tau'}{\Gamma \vdash \lambda x : \tau.\, e : \tau \to \tau'}\ \text{T-Abs}$$

$$\frac{\Gamma \vdash e_1 : \tau \to \tau' \quad \Gamma \vdash e_2 : \tau}{\Gamma \vdash e_1\ e_2 : \tau'}\ \text{T-App}$$

Properties

Theorem (Type soundness)

If $\vdash e : \tau$ *and* $e \to^* e'$ *and* $e' \not\to$ *then* e' *is a value and* $\vdash e' : \tau$.

Properties

Theorem (Type soundness)

If $\vdash e : \tau$ *and* $e \to^* e'$ *and* $e' \not\to$ *then* e' *is a value and* $\vdash e' : \tau$.

Lemma (Preservation)

If $\vdash e : \tau$ *and* $e \to e'$ *then* $\vdash e' : \tau$.

Properties

Theorem (Type soundness)

If $\vdash e : \tau$ *and* $e \to^* e'$ *and* $e' \not\to$ *then* e' *is a value and* $\vdash e' : \tau$.

Lemma (Preservation)

If $\vdash e : \tau$ *and* $e \to e'$ *then* $\vdash e' : \tau$.

Lemma (Progress)

If $\vdash e : \tau$ *then either* e *is a value or there exists an* e' *such that* $e \to e'$.