

A Syntactic Approach to Type Soundness

COMP3610 – Principles of Programming Languages

Ben Lippmeier

Australian National University

Semester 2, 2009

Progress

If $\emptyset \vdash e :: \tau$ then $e \in \text{Value}$ or $e \longrightarrow e'$

A closed, well typed term is either a value, or can be reduced to a new term.

Preservation

If $\Gamma \vdash e :: \tau$ and $e \longrightarrow e'$ then $\Gamma \vdash e' :: \tau$

If we reduce a well typed term, then the result is also well typed.

Language

Expressions $e ::= x \mid \lambda x.e \mid e_1 e_2 \mid n \mid n + n'$

Values $v ::= x \mid \lambda x.e \mid n$

Types $\tau ::= Int \mid \tau \rightarrow \tau'$

$$\boxed{e \longrightarrow e'}$$

$$(\lambda x.e_1) e_2 \longrightarrow e_1[e_2/x] \quad (\text{EApp})$$

$$\frac{e_1 \longrightarrow e'_1}{e_1 e_2 \longrightarrow e'_1 e_2} \quad (\text{EAppL})$$

$$n_1 + n_2 \longrightarrow n_3$$

where $n_3 = n_1 + n_2$ (EAdd)

$$\frac{e_1 \longrightarrow e'_1}{e_1 + e_2 \longrightarrow e'_1 + e_2} \quad (\text{EAddL})$$

$$\frac{e_2 \longrightarrow e'_2}{e_1 + e'_2 \longrightarrow e_1 + e'_2} \quad (\text{EAddR})$$

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

$$\frac{x : \tau \in \Gamma}{\Gamma \vdash x :: \tau} \quad (\text{TVar})$$

$$\frac{\Gamma, x : \tau_1 \vdash e :: \tau_2}{\Gamma \vdash \lambda x.e :: \tau_1 \rightarrow \tau_2} \quad (\text{TAbs})$$

$$\frac{\Gamma \vdash e_1 :: \tau_{11} \rightarrow \tau_{12} \quad \Gamma \vdash e_2 :: \tau_{11}}{\Gamma \vdash e_1 e_2 :: \tau_{12}} \quad (\text{TApp})$$

$$\overline{\Gamma \vdash n :: \text{Int}} \quad (\text{TNum})$$

$$\frac{\Gamma \vdash e_1 :: \text{Int} \quad \Gamma \vdash e_2 :: \text{Int}}{\Gamma \vdash e_1 + e_2 :: \text{Int}} \quad (\text{TAdd})$$

Progress

If $\emptyset \vdash e :: \tau$ then $e \in \text{Value}$ or $e \longrightarrow e'$

Proof by rule induction over the derivation of $\emptyset \vdash e :: \tau$

(1) **Case** e one of $x, \lambda x.e', n$

(2) $e \in \text{Value}$

(3) **Case** $e = e_1 e_2$ and last rule of derivation is TApp.

(IH) Progress holds for all subterms of e (Assume)

(4) $\emptyset \vdash e_1 e_2 :: \tau$ (Assume)

(5) $\emptyset \vdash e_1 :: \tau_{11} \rightarrow \tau$ (Inversion of TApp 4)

(6) $\emptyset \vdash e_2 :: \tau_{11}$ (Inversion of TApp 4 5)

(7) $e_1 \in \text{Value}$ or $e_1 \longrightarrow e'_1$ (IH 3 5)

(8) Case $e_1 \in \text{Value}$

(9) $e_1 = \lambda y. e_{12}$

(Forms of Terms 8 5)

(10) $(\lambda y. e_{12}) e_2 \longrightarrow e_{12}[e_2/x]$

(EApp 2 9)

(11) Case $e_1 \longrightarrow e'_1$

(12) $e_1 e_2 \longrightarrow e'_1 e_2$

(EAppL 11)

Exercise: Complete this proof.

Preservation

If $\Gamma \vdash e :: \tau$ and $e \longrightarrow e'$ then $\Gamma \vdash e' :: \tau$

Proof by rule induction over the derivation of $\Gamma \vdash e :: \tau$

- (1) **Case** e one of $x, \lambda x.e', n$
- (2) Can't happen. No rule of form $e \rightarrow e'$
- (3) **Case** $e = e_1 e_2$ and last rules of derivations are TApp and EApp
- (IH) Progress holds for all subterms of e (Assume)
- (4) $\Gamma \vdash (\lambda x.e_{12}) e_2 :: \tau$ (Assume)
- (5) $(\lambda x.e_{12}) e_2 \longrightarrow e_{12}[e_2/x]$ (Assume)
- (6) $\Gamma \vdash \lambda x.e_{12} :: \tau_{11} \rightarrow \tau$ (Inversion of TApp 4)
- (7) $\Gamma \vdash e_2 :: \tau_{11}$ (Inversion of TApp 4 6)
- (8) $\Gamma, x : \tau_{11} \vdash e_{12} :: \tau$ (Inversion of TAbs 6)
- (9) $\Gamma \vdash e_{12}[e_2/x] :: \tau$ (Stability Theorem 7 8)

(10) **Case** $e = e_1 e_2$ and last rules of derivations are TApp and EAppL

(11) $\Gamma \vdash e_1 e_2 :: \tau$ (Assume)

(12) $e_1 e_2 \longrightarrow e'_1 e_2$ (Assume)

(13) ...

Exercise: Complete this proof.

Stability of Types under Substitution

If $\Gamma, x : \tau_1 \vdash e_2 :: \tau_2$ and $\Gamma \vdash e_1 :: \tau_1$ then $\Gamma \vdash e_2[e_1/x] :: \tau_2$

Proof by rule induction over the derivation of $\Gamma, x : \tau_1 \vdash e_2 :: \tau_2$

(1) **Case** $e_2 \equiv x$

(2) $\Gamma, x : \tau_1 \vdash x :: \tau_2$

(Assume)

(3) $\Gamma \vdash e_1 :: \tau_1$

(Assume)

(4) $x : \tau_2 \in \Gamma, x : \tau_1$

(Inversion of TVar 2)

(5) $\tau_1 \equiv \tau_2$

(Def of Type Environment 4)

(6) $\Gamma \vdash e_2 :: \tau_2$

(3 5)

(7) $\Gamma \vdash x[e_1/x] :: \tau_2$

(Def of Substitution 6)

- (8) **Case** $e \equiv \lambda y.e_{12}$
- (IH) Substitution holds for all subterms of e (Assume)
- (10) $\Gamma, x : \tau_1 \vdash \lambda y.e_{12} :: \tau_{11} \rightarrow \tau_{12}$
- $\tau_2 = \tau_{11} \rightarrow \tau_{12}$ (Assume)
- (11) $\Gamma \vdash e_1 :: \tau_1$ (Assume)
- (12) $\Gamma, x : \tau_1, y : \tau_{11} \vdash e_{12} :: \tau_{12}$ (Inversion of TAbs 10)
- (13) $\Gamma, y : \tau_{11} \vdash e_{12}[e_1/x] :: \tau_{12}$ (IH 12 11)
- (14) $\Gamma \vdash \lambda y.e_{12}[e_1/x] :: \tau_{11} \rightarrow \tau_{12}$ (TAbs 13)
- (15) $\Gamma \vdash (\lambda y.e_{12})[e_1/x] :: \tau_{11} \rightarrow \tau_{12}$ (Def of Substitution 14)

Exercise: Complete this proof.