

# COMP 617 RAP Seminar, Fall 2006

Presenter: Walid Taha

Scribe: Angela Zhu

October 14, 2006

## Type Safety of a Simply Typed System

Last class, we introduced a simple type system for pure lambda-calculus. An important property of type system is that it ensures type safety. We summarize type system of the pure simply typed lambda-calculus as below:

$$\frac{\Gamma(x) = t}{\Gamma \vdash x : t} \quad (\text{TVar})$$

$$\frac{\Gamma \vdash e_1 : t_1 \rightarrow t_2 \quad \Gamma \vdash e_2 : t_1}{\Gamma \vdash e_1 e_2 : t_2} \quad (\text{TApp})$$

$$\frac{\Gamma, x : t_1 \vdash e : t_2}{\Gamma \vdash \lambda x. e : t_1 \rightarrow t_2} \quad (\text{TAbs})$$

This lambda-calculus has semantic rules for evaluation as:

$$\frac{e_1 \mapsto e'_1}{e_1 e_2 \mapsto e'_1 e_2} \quad (\text{EApp1})$$

$$\overline{(\lambda x. e_1) e_2 \mapsto e_1[x = e_2]} \quad (\text{EApp2})$$

This class, we will prove this property. Before doing the proof, we will introduce an important lemma which will be used in our proof and will be proved later.

**Lemma 1** (Substitution).  $\forall e_1, e_2 \in E, x \in \mathbb{V}, t_1, t \in T,$

$$x : t_1 \vdash e_1 : t \wedge \cdot \vdash e_2 : t_1 \Rightarrow \cdot \vdash e_1[x = e_2] : t$$

**Lemma 1.** ' (Substitution) *The following rule is admissible:*

$$\frac{x : t_1 \vdash e_1 : t \quad \cdot \vdash e_2 : t_1}{\cdot \vdash e_1[x = e_2] : t}$$

**Theorem 1** (Type-Safety for  $\lambda_{\rightarrow}$ ).

$$\forall e, t, \cdot \vdash e : t \wedge e \notin \mathbb{V} \Rightarrow \exists e', e \mapsto e' \wedge \cdot \vdash e' : t$$

*Proof.* By case analysis on  $e$ .  $e$  has the form:

$$e ::= x \mid \lambda x.e \mid ee$$

**Case 1.**  $e \equiv x$ ,  $e : t$  From (TVar),  $\cdot \vdash x : t$  need  $\cdot(x) = t$ , which is not true, case1 cannot happen.

**Case 2.**  $e \equiv \lambda x.e_1$ ,  $e : t$  The precondition of theorem said that  $e \notin \mathbb{V}$ , but  $\lambda x.e_1 \in \mathbb{V}$ . We don't need to consider it.

**Case 3.**  $e \equiv e_1e_2$ ,  $e : t$

By case analysis on the structure of  $e_1$ .  $e_1$  has the form  $\lambda x.e_3$  or not, thus we have two cases:

- case 3.1:  $e \equiv (\lambda x.e_3)e_2 : t$

The first part we need to prove is that  $\exists e'$ ,  $e \mapsto e'$ . From (EApp2) comes directly:

$$(\lambda x.e_3)e_2 \mapsto e_3[x = e_2]$$

The second part we need to prove is that  $\cdot \vdash e' : t$ . This comes from the following derivation:

$$\vdash \uparrow \frac{\vdash \uparrow \frac{x : t_1 \vdash e_3 : t \quad \cdot \vdash e_2 : t_1}{\cdot \vdash \lambda x.e_3 : t_1 \rightarrow t} \quad \cdot \vdash e_2 : t_1}{\cdot \vdash (\lambda x.e_3)e_2 : t} \quad \xrightarrow{\text{Lemma1}} \cdot \vdash e_3[x = e_2] : t$$

- case 3.2:  $e \equiv e_1e_2 : t$ ,  $e_1 \neq \lambda x.e_3$

The first part we need to prove is that  $\exists e'$ ,  $e \mapsto e'$ . From (EApp1) comes directly:

$$\frac{e_1 \mapsto e'_1}{e_1e_2 \mapsto e'_1e_2}$$

The second part we need to prove is that  $\cdot \vdash e' : t$ . This comes from the following derivation:

$$\vdash \uparrow \frac{\cdot \vdash e_1 : t_2 \rightarrow t \quad \cdot \vdash e_2 : t_2}{\cdot \vdash e_1 e_2 : t} \xrightarrow{IH} \frac{\cdot \vdash e'_1 : t_2 \rightarrow t \quad \cdot \vdash e_2 : t_2}{\cdot \vdash e'_1 e_2 : t} \vdash, :=, \Downarrow$$

□

Now let's recall the Substitution Lemma (Lemma1) and prove it. The following definition of substitution will be used in our proof:

**Definition 1** (Substitution).

$$\begin{aligned} x[x = e_2] &= e_2 && (Sub1) \\ y[x = e_2] &= y && (Sub2) \\ (\lambda y. e_1)[x = e_2] &= \lambda y. (e_1[x = e_2]) && y \neq x \quad (Sub3) \\ (e_1 e'_1)[x = e_2] &= (e_1[x = e_2])(e'_1[x = e_2]) && y \notin FV(e_2) \quad (Sub4) \end{aligned}$$

(Lemma1) says that:

$$\frac{x : t_1 \vdash e_1 : t \quad \cdot \vdash e_2 : t_1}{\cdot \vdash e_1[x = e_2] : t}$$

*Proof.* We prove it by induction on the structure of  $e_1$ <sup>1</sup>. Suppose for every  $e_1$ , where  $e_1$  is sub-expression of  $e_3$ , (Lemma 1) holds:

$$\frac{x : t_1 \vdash e_1 : t \quad \cdot \vdash e_2 : t_1}{\cdot \vdash e_1[x = e_2] : t}$$

We will argue that (Lemma 1) also holds for  $e_3$ :

---

<sup>1</sup>In next class we will see that induction on  $e_1$  doesn't work for some case. And actually We redo the proof in a similar way using induction on the derivation

$$\frac{x : t_1 \vdash e_3 : t \quad \cdot \vdash e_2 : t_1}{\cdot \vdash e_3[x = e_2] : t}$$

**Case 1.**  $e_3 \equiv x$

*Reproduce the assumption for  $e_3 = x$ , we get:*

$$x : t_1 \vdash x : t \wedge \cdot \vdash e_2 : t_1$$

*since  $x : t_1 \vdash x : t \Rightarrow t_1 = t$ , we have  $\frac{\cdot \vdash e_2 : t_1}{\cdot \vdash e_2 : t}$*

*From (Sub1) we have:  $x[x = e_2] = e_2$ . Thus  $e_3[x = e_2] : t$*

**Case 2.**  $e_3 \equiv y, y \neq x$

*Reproduce the assumptions for  $e_3 = y$ , we get:*

$$x : t_1 \vdash y : t$$

*This is vacuously true.*

**Case 3.**  $e_3 \equiv e_1 e'_1$

$$\vdash \uparrow \frac{x : t_1 \vdash e_1 : t_3 \rightarrow t \quad x : t_1 \vdash e'_1 : t_3}{\cdot \vdash e_1 e'_1 : t} \begin{array}{c} \xrightarrow{IH} \\ \xrightarrow{IH} \end{array} \frac{\cdot \vdash e_1[x = e_2] : t_3 \rightarrow t \quad \cdot \vdash e'_1[x = e_2] : t_3}{\cdot \vdash e_1 e'_1[x = e_2] : t} \vdash, := \Downarrow$$

**Case 4.**  $e_3 \equiv \lambda x. e_1$  (To be continued)

□