CS101 (Fall 2005) Special Topics in Computer Science

Language-Based Security

Substitution Lemma (Partial Proof)

Last Update: October 12, 2005 20:51

Lemma. If $\Gamma; x : t_1; \Delta \vdash e_1 \in t_2$ and $\Gamma; \Delta \vdash e_2 \in t_1$, then $\Gamma; \Delta \vdash e_1[e_2/x] \in t_2$.

Proof. First we formulate the lemma more precisely, as follows:

> For any variable x, expression e_2, and type t_1, for any derivation $D_1, D_2 \in \mathbb{D}$ (where $\mathbb{D}$ is the set of all well-formed λ-Calculus typing derivations that we have defined inductively in class), for any variable contexts Γ and Δ, for any expressions e_1, and type t_2,
>
> > If D_1 ends with $\Gamma; x : t_1; \Delta \vdash e_1 \in t_2$ and D_2 ends with $\Gamma; \Delta \vdash e_2 \in t_1$, then $\Gamma; \Delta \vdash e_1[e_2/x] \in t_2$ is derivable.

Now, given a variable x, expression e_2, and type t_1, we prove the statement of the Lemma by structural induction on derivation D_1 (the statement that we are proving by induction is "for any D_2, Γ, Δ, e_1, and t_2, ..."). There are 5 cases to consider (one case for each of the derivation rules in the λ-Calculus type system). Here we present the case that corresponds to the *(Fun)* rule.

Case (Fun). D_1 has a form

$$\dfrac{\left.\dfrac{\cdots}{\Sigma; y : \tau_1 \vdash f \in \tau_2}\right\} D_1'}{\Sigma \vdash \lambda y : \tau_1 . f \in \tau_1 \to \tau_2}\ (\mathit{Fun})$$

where $D_1' \in \mathbb{D}$ is a subderivation of D_1. (Note — since we can alpha-rename y without affecting x, we can assume that x and y are distinct without loss of generality).

The statement that we are trying to prove requires us to assume that for some Γ, Δ, e_1, e_2, and t_2, D_1 ends with $\Gamma; x : t_1; \Delta \vdash e_1 \in t_2$. Since a derivation can only end with a single formula, this means that $\Gamma; x : t_1; \Delta \vdash e_1 \in t_2 = \Sigma \vdash \lambda y : \tau_1 . f \in \tau_2$. From that we conclude that

$$\begin{aligned} \Sigma &= \Gamma; x : t_1; \Delta \\ e_1 &= \lambda y : \tau_1 . f \\ t_2 &= \tau_1 \to \tau_2 \end{aligned}$$

Now, by using the inductive hypothesis for D_1 with the appropriate D_2, Γ, Δ, e_1, and t_2 (namely, we take $\Gamma' := \Gamma$, $\Delta' := \Delta; y : \tau_1$, $e_1' := f$, $t_2' := \tau 2$, and D_2' to be the result of taking the original D_2 and adding an extra hypothesis $y : \tau_1$ as needed[1]) we get that $\Gamma; \Delta; y : \tau_1 \vdash f[e_2/x] \in t_2$ is derivable. Using the same *(Fun)* rule

$$\dfrac{\Gamma; \Delta; y : \tau_1 \vdash f[e_2/x] \in \tau_2}{\Gamma; \Delta \vdash \lambda y : \tau_1 . f[e_2/x] \in \tau_1 \to \tau_2}\ (\mathit{Fun}) \quad ,$$

we can conclude that $\Gamma; \Delta \vdash \lambda y : \tau_1 . f[e_2/x] \in t_2$ is derivable. This is almost exactly what we needed to prove, except we needed $(\lambda y : \tau_1 . f)[e_2/x]$ and instead we got $\lambda y : \tau_1 . (f[e_2/x])$. Fortunately, the from the properties of substitution it follows that the two expressions are the same[2] (as before, we assume that all variable names are distinct and there are no issues with variable naming during substitution).

---

[1] Strictly speaking, we need to prove a separate lemma by induction on D_2 — "if D_2 is a valid derivation, we can add an extra hypothesis $y : \tau_1$ to it and the result will be a valid derivation". The proof of such lemma is very straightforward, so we label it as "obvious" and do not provide it here.

[2] Again, strictly speaking, this should be proven by structural induction on f. And again we pretend that it's "obvious".