Sample Solution to COMP 523 Homework 2

Brigitte Pientka
McGill University
Montréal, Canada

September 28, 2010

1 Exercise 1

Extend the language for booleans and arithmetic expressions we have seen in class (see also Ch 3, CH 8 in Pierce) with an expression $\texttt{leq}\ \texttt{t}\ \texttt{t}'$ which allows us to check whether $\texttt{t}$ is less than or equal to $\texttt{t'}$.

Small-step semantics

$$\frac{V \text{ numerical value}}{\texttt{leq}\ \texttt{z}\ V \longrightarrow \texttt{true}}\ \text{E-LEQ-Z} \qquad \frac{V \text{ numerical value}}{\texttt{leq}\ (\texttt{succ}\ \ V)\ \texttt{z} \longrightarrow \texttt{false}}\ \text{E-LEQ-SUCC-Z}$$

$$\frac{V_1 \text{ numerical value} \quad V_2 \text{ numerical value} \quad \texttt{leq}\ V_1\ V_2 \longrightarrow V}{\texttt{leq}\ (\texttt{succ}\ \ V_1)\ (\texttt{succ}\ \ V_2) \longrightarrow V}\ \text{E-LEQ-SUCC-SUCC}$$

$$\frac{M \longrightarrow M'}{\texttt{leq}\ \ M\ N \longrightarrow \texttt{leq}\ M'\ N}\ \text{E-LEQ-1} \qquad \frac{V \text{ numerical value} \quad N \longrightarrow N'}{\texttt{leq}\ \ V\ N \longrightarrow \texttt{leq}\ V\ N'}\ \text{E-LEQ-2}$$

Theorem 1 (Determinacy of small-step rules)**.** *If* $M \longrightarrow N_1$ *and* $M \longrightarrow N_2$ *then* $N_1 = N_2$.

Proof. Induction on $M \longrightarrow N_1$.

Case $\quad \mathcal{S}_1 = \dfrac{V \text{ numerical value}}{\texttt{leq}\ \texttt{z}\ V \longrightarrow \texttt{true}}\ \text{E-LEQ-Z}$

We note that we cannot have used the rule E-LEQ-1 nor the rule E-LEQ-2 to derive $\mathcal{S}_2 : \texttt{leq}\ \texttt{z}\ V \longrightarrow N_2$, since there are no small-step rules for values. Hence, the only possible rule we could have used is E-LEQ-Z. Therefore:

$$\mathcal{S}_2 = \frac{V \text{ numerical value}}{\texttt{leq}\ \texttt{z}\ V \longrightarrow \texttt{true}}\ \text{E-LEQ-Z}$$

and clearly $\texttt{true} = \texttt{true}$ by reflexivity of equality.

Case $\quad \mathcal{S}_1 = \dfrac{V \text{ numerical value}}{\texttt{leq}\ (\texttt{succ}\ \ V)\ \texttt{z} \longrightarrow \texttt{false}}\ \text{E-LEQ-SUCC-Z}$

We note that we cannot have used the rule E-LEQ-1 nor the rule E-LEQ-2 to derive $\mathcal{S}_2 : \texttt{leq}\ (\texttt{succ}\ \ V)\ \texttt{z} \longrightarrow N_2$, since there are no small-step rules for values. Hence, the only possible rule we could have used is E-LEQ-SUCC-Z. Therefore:

$$\mathcal{S}_2 = \frac{V \text{ numerical value}}{\texttt{leq}\ (\texttt{succ}\ \ V)\ \texttt{z} \longrightarrow \texttt{false}}\ \text{E-LEQ-SUCC-Z}$$

and clearly $\texttt{false} = \texttt{false}$ by reflexivity of equality.

Case $\mathcal{S}_1 = \dfrac{\mathsf{V}_1 \text{ numerical value} \quad \mathsf{V}_2 \text{ numerical value} \quad \overset{\mathcal{S}_1'}{\texttt{leq}\ \mathsf{V}_1\ \mathsf{V}_2 \longrightarrow \mathsf{V}}}{\texttt{leq}\ (\texttt{succ}\ \ \mathsf{V}_1)\ (\texttt{succ}\ \ \mathsf{V}_2) \longrightarrow \mathsf{V}}$ E-LEQ-SUCC-SUCC

We again note that we cannot have used the rule E-LEQ-1 nor the rule E-LEQ-2 to derive $\mathcal{S}_2 : \texttt{leq}\ (\texttt{succ}\ \ \mathsf{V})\ \texttt{z} \longrightarrow \mathsf{N}_2$, since there are no small-step rules for values. Hence, the only possible rule we could have used is E-LEQ-SUCC-SUCC. Therefore:

$$\mathcal{S}_2 = \dfrac{\mathsf{V}_1 \text{ numerical value} \quad \mathsf{V}_2 \text{ numerical value} \quad \overset{\mathcal{S}_2'}{\texttt{leq}\ \mathsf{V}_1\ \mathsf{V}_2 \longrightarrow \mathsf{V}'}}{\texttt{leq}\ (\texttt{succ}\ \ \mathsf{V}_1)\ (\texttt{succ}\ \ \mathsf{V}_2) \longrightarrow \mathsf{V}'}\ \text{E-LEQ-SUCC-SUCC}$$

By i.h. using $\mathcal{S}_1'$ and $\mathcal{S}_2'$, we know that $\mathsf{V} = \mathsf{V}'$.

Case $\mathcal{S}_1 = \dfrac{\overset{\mathcal{S}_1'}{\mathsf{M} \longrightarrow \mathsf{M}'}}{\texttt{leq}\ \ \mathsf{M}\ \mathsf{N} \longrightarrow \texttt{leq}\ \mathsf{M}'\ \mathsf{N}}$ E-LEQ-1

The only possible rule we could have used on $\mathcal{S}_2$ to derive $\texttt{leq}\ \ \mathsf{M}\ \mathsf{N} \longrightarrow \mathsf{N}_2$ is the rule E-LEQ-1. If we would have used any other rule, then M would need to be a value, but since values don't step there would be no derivation for $\mathsf{M} \longrightarrow \mathsf{M}'$ and hence these cases are impossible. Hence, we only consider the case where we have use E-LEQ-2 to derive $\mathcal{S}_2$.

$$\mathcal{S}_2 = \dfrac{\overset{\mathcal{S}_2'}{\mathsf{M} \longrightarrow \mathsf{M}''}}{\texttt{leq}\ \ \mathsf{M}\ \mathsf{N} \longrightarrow \texttt{leq}\ \mathsf{M}''\ \mathsf{N}}\ \text{E-LEQ-1}$$

By i.h. $\mathcal{S}_1'$ and $\mathcal{S}_2'$, we have that $\mathsf{M}' = \mathsf{M}''$ and therefore we have $\texttt{leq}\ \mathsf{M}'\ \mathsf{N} = \texttt{leq}\ \mathsf{M}''\ \mathsf{N}$.

Case $\mathcal{S}_1 = \dfrac{\mathsf{V} \text{ numerical value} \quad \overset{\mathcal{S}_1'}{\mathsf{N} \longrightarrow \mathsf{N}'}}{\texttt{leq}\ \ \mathsf{V}\ \mathsf{N} \longrightarrow \texttt{leq}\ \mathsf{V}\ \mathsf{N}'}$ E-LEQ-2

The only possible rule we could have used on $\mathcal{S}_2$ to derive $\texttt{leq}\ \ \mathsf{M}\ \mathsf{N} \longrightarrow \mathsf{N}_2$ is the rule E-LEQ-1. We could not have used the rule E-LEQ-2, since M is a value and values don't step. We also could not have used any other rule such as E-LEQ-Z, E-LEQ-SUCC-Z, or E-LEQ-SUCC-SUCC, since then N would need to be a value; but since values don't step there would be no derivation for $\mathsf{N} \longrightarrow \mathsf{N}'$ and hence these cases are impossible. Hence, we only consider the case where we have use E-LEQ-2 to derive $\mathcal{S}_2$.

$$\mathcal{S}_2 = \dfrac{\mathsf{V} \text{ numerical value} \quad \overset{\mathcal{S}_2'}{\mathsf{N} \longrightarrow \mathsf{N}''}}{\texttt{leq}\ \ \mathsf{V}\ \mathsf{N} \longrightarrow \texttt{leq}\ \mathsf{V}\ \mathsf{N}''}\ \text{E-LEQ-2}$$

By i.h. $\mathcal{S}_1'$ and $\mathcal{S}_2'$, we have that $\mathsf{N}' = \mathsf{N}''$ and therefore we have $\texttt{leq}\ \mathsf{V}\ \mathsf{N}' = \texttt{leq}\ \mathsf{V}\ \mathsf{N}''$.

$\square$

Typing rules, preservation and progress

$$\frac{M : \text{NAT} \quad N : \text{NAT}}{\texttt{leq}\ M\ N : \text{BOOL}}\ \text{T-LEQ}$$

We fold the preservation and progress proof into one statement here. It is equally fine to prove both statements separately.

Theorem 2 (Preservation and progress)**.**
If $M : T$ *then either* M *numerical value or there exists a term* N *s.t.* $M \longrightarrow N$ *and* $N : T$.

Proof. By induction on the typing derivation $M : T$.

Case $\mathcal{D} = \dfrac{\begin{array}{c}\mathcal{D}_1\\ M : \text{NAT}\end{array} \qquad \begin{array}{c}\mathcal{D}_2\\ N : \text{NAT}\end{array}}{\texttt{leq}\ M\ N : \text{BOOL}}$

either M numerical value or there exists a term M' s.t. $M \longrightarrow M'$ and $M' : \text{NAT}$ by i.h. $\mathcal{D}_1$
either N numerical value or there exists a term N' s.t. $N \longrightarrow N'$ and $N' : \text{NAT}$ by i.h. $\mathcal{D}_2$

Sub-case 1 M numerical value and N numerical value

By the canonical forms lemma, we need to distinguish the following combinations

1. If $M = \texttt{z}$, then we can use the rule E-LEQ-Z and $\texttt{leq z}\ N \longrightarrow \texttt{true}$; moreover, by the typing rule T-TRUE, we know that $\texttt{true} : \text{BOOL}$.
2. If $M = \texttt{succ}\ \ V$ and $N = \texttt{z}$, then we can use the rule E-LEQ-SUCC-Z and $\texttt{leq}\ (\texttt{succ}\ \ V)\texttt{z} \longrightarrow \texttt{false}$; moreover, by the typing rule T-FALSE, we know that $\texttt{false} : \text{BOOL}$.
3. If $M = \texttt{succ}\ \ V$ and $N = \texttt{succ}\ \ V'$, we have by assumption $\mathcal{D}_1 :: \texttt{succ}\ \ V : \text{NAT}$ and $\mathcal{D}_2 :: \texttt{succ}\ \ V' : \text{NAT}$. By inversion on the typing rule for T-SUCC, we know that $\mathcal{D}_1' :: V : \text{NAT}$ and $\mathcal{D}_2' :: V' : \text{NAT}$. Using $\mathcal{D}_1'$ and $\mathcal{D}_2'$, we know there exists a typing derivation $\mathcal{D}' :: \texttt{leq}\ V\ V' : \text{BOOL}$ and that $\mathcal{D}'$ is smaller than $\mathcal{D}$. By i.h. on $\mathcal{D}'$, we know that there exists a term M_0 s.t. $\texttt{leq}\ V\ V' \longrightarrow M_0$ and $M_0 : \text{BOOL}$. By the rule E-LEQ-SUCC-SUCC, we have that there exists a term, namely M_0, where $\texttt{leq}\ (\texttt{succ}\ \ V)\ (\texttt{succ}\ \ V') \longrightarrow M_0$.

Sub-case 2 M numerical value and there exists a term N' s.t. $N \longrightarrow N'$ and $N' : \text{NAT}$

$\texttt{leq}\ M\ N \longrightarrow \texttt{leq}\ M N'$ by rule E-LEQ-2
$\texttt{leq}\ M\ N' : \text{BOOL}$ by typing rule using $\mathcal{D}_1 : M : \text{NAT}$ and $N' : \text{NAT}$

Sub-case 3 There exists a term M' s.t. $M \longrightarrow M'$ and $M' : \text{NAT}$

$\texttt{leq}\ M\ N \longrightarrow \texttt{leq}\ M' N$ by rule E-LEQ-1
$\texttt{leq}\ M'\ N : \text{BOOL}$ by typing rule using $M' : \text{NAT}$ and $\mathcal{D}_2 : N : \text{NAT}$

$\square$