COMP 523: Language-based security
Assignment 1 (100 points total)

Prof. B. Pientka
McGill University

Due: Thursday, 20 Sept, 2:35pm

Exercise 1 (20 pts): In the lecture and in Pierce's book, we define the following operational semantics for a small language of terms. For convenience, we repeat the evaluation rules here.

$$\frac{}{\texttt{pred (succ } nv\texttt{)} \longrightarrow nv}\ \text{E-PRED-SUCC} \qquad \frac{}{\texttt{pred z} \longrightarrow \texttt{z}}\ \text{E-PRED-ZERO}$$

$$\frac{t \longrightarrow t'}{\texttt{succ t} \longrightarrow \texttt{succ t}'}\ \text{E-SUCC} \qquad \frac{t \longrightarrow t'}{\texttt{pred t} \longrightarrow \texttt{pred t}'}\ \text{E-PRED}$$

$$\frac{}{\texttt{if true then t}_1\texttt{ else t}_2 \longrightarrow \texttt{t}_1}\ \text{E-IF-TRUE} \qquad \frac{}{\texttt{if false then t}_1\texttt{ else t}_2 \longrightarrow \texttt{t}_2}\ \text{E-IF-FALSE}$$

$$\frac{t \longrightarrow t'}{\texttt{if t then t}_1\texttt{ else t}_2 \longrightarrow \texttt{if t}'\texttt{ then t}_1\texttt{ else t}_2}\ \text{E-IF}$$

$$\frac{}{\texttt{iszero z} \longrightarrow \texttt{true}}\ \text{E-ISZERO-ZERO} \qquad \frac{}{\texttt{iszero (succ } nv\texttt{)} \longrightarrow \texttt{false}}\ \text{E-ISZERO-SUCC}$$

$$\frac{t \longrightarrow t'}{\texttt{iszero t} \longrightarrow \texttt{iszero t}'}\ \text{E-ISZERO}$$

A friend of yours suggests to replace the evaluation rule E-PRED-SUCC with the rule

$$\frac{}{\texttt{succ (pred t)} \longrightarrow \texttt{t}}$$

and the rule E-ISZERO-SUCC with

$$\frac{}{\texttt{iszero (succ t)} \longrightarrow \texttt{false}}\ \text{E-ISZERO-SUCC}$$

Is this a good idea? What would you say to her or him? Which basic property discussed in Ch 3 breaks down? – If you think the above rule is good, verify that all the theorems in Ch 3 still hold. If you think the rule is bad, then give a counterexample and explain which theorem does not hold.

Exercise 2 (20pts): Show that for the small-step semantics, we have that all values evaluate to themselves.

$$\text{If } v \text{ is a value and } v \longrightarrow^* v' \text{ then } v = v'.$$

Use the following rules for the multi-step relation $t \longrightarrow^* t'$.

$$\frac{}{t \longrightarrow^* t}\ \text{refl} \qquad \frac{t \longrightarrow^* s \quad s \longrightarrow^* t'}{t \longrightarrow^* t'}\ \text{trans} \qquad \frac{t \longrightarrow t'}{t \longrightarrow^* t'}\ \text{single}$$

Consider only the cases for numerical values.

Exercise 3 (20 pts) An alternative formulation of the multi-step rules

$$\frac{}{t \Longrightarrow^* t}\ \text{m-refl} \qquad \frac{t \longrightarrow s \quad s \Longrightarrow^* t'}{t \Longrightarrow^* t'}\ \text{m-step}$$

Show that the two formulations are equivalent, i.e. $t \longrightarrow^* s$ iff $t \Longrightarrow^* s$. State and prove any additional lemmas you might need.

Exercise 4 (40pts): Extend the language for booleans and arithmetic expressions we have seen in class (see also Ch 3, CH 8 in Pierce) with an expression `leq` t t′ which allows us to check whether `t` is less than or equal to `t'`.

1. (5 pts) Define small-step evaluation rules for `leq` t t′.
2. (16 pts) Prove that the rules are deterministic. Justify which cases are impossible and why.
3. (4 pts) Define a typing rule for `leq` t t′.
4. (15 pts) Prove that type preservation holds for this extension.

Exercise 5 (optional) : An alternative style to the small-step semantics seen in class is the *big-step* semantics. The judgment $e \Downarrow v$ describes the complete evaluation of the expression e to some final value v. We concentrate here on the fragment for natural numbers. The rules for big-step evaluation for the small fragment consisting of `z`, `succ` e, `pred` e, and `iszero` e are given below.

$$\frac{}{\texttt{z} \Downarrow \texttt{z}}\ \text{B-Z} \qquad \frac{e \Downarrow v}{\texttt{succ}\ e \Downarrow \texttt{succ}\ v}\ \text{B-SUCC}$$

$$\frac{e \Downarrow \texttt{z}}{\texttt{pred}\ e \Downarrow \texttt{z}}\ \text{B-PRED-ZERO} \qquad \frac{e \Downarrow \texttt{succ}\ v}{\texttt{pred}\ e \Downarrow v}\ \text{B-PRED-SUCC}$$

$$\frac{e \Downarrow \texttt{z}}{\texttt{iszero}\ e \Downarrow \texttt{true}}\ \text{B-ISZERO} \qquad \frac{e \Downarrow \texttt{succ}\ v}{\texttt{iszero}\ e \Downarrow \texttt{false}}\ \text{B-ISSUCC}$$

Prove that the small-step and big-step semantics coincide, i.e. $e \Downarrow v$ iff $e \longrightarrow^* v$. In your proofs, you should show the case for handling the predecessor in detail; in particular, state and prove all necessary lemmas. You can sketch the remaining cases for successor and iszero-expression.

Hint: Read Exercise 3.5.17 in TAPL page 42 and the corresponding solution page 498.