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

Prof. B. Pientka
McGill University

September 10, 2010—**Due: Wednesday, 15 September 2010 at 2:35pm**

Exercise 1 (20pts): 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.

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

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

$$\frac{}{\texttt{if true then } t_1 \texttt{ else } t_2 \rightarrow t_1}\ \text{E-IF-TRUE} \qquad \frac{}{\texttt{if false then } t_1 \texttt{ else } t_2 \rightarrow t_2}\ \text{E-IF-FALSE}$$

$$\frac{t \rightarrow t'}{\texttt{if } t \texttt{ then } t_1 \texttt{ else } t_2 \rightarrow \texttt{if } t' \texttt{ then } t_1 \texttt{ else } t_2}\ \text{E-IF}$$

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

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

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

$$\frac{}{\texttt{succ (pred (}nv\texttt{))} \rightarrow nv}$$

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 (30pts): Show that for the small-step semantics, we have that all values evaluate to themselves.

If v is a value and $v \rightarrow^* v'$ then $v = v'$.

Exercise 3 (50pts) : 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 $\mathtt{z}$, $\mathtt{succ}\ e$, $\mathtt{pred}\ e$, and $\mathtt{iszero}\ e$ are given below.

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

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

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

Prove that the small-step and big-step semantics for this language coincide, i.e. $e \Downarrow v$ iff $e \rightarrow^* v$. 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.