CSE-433 Midterm - Fall 2024

gla@postech

Out: 01:01am, Nov 29
Due: 11:59pm, Dec 1

1 Definition of the simple language

The simple language uses the following definition of terms:

$$t \quad ::= \quad \textbf{true} \mid \textbf{false} \mid \textbf{if}\ t\ \textbf{then}\ t\ \textbf{else}\ t \mid \textbf{0} \mid \textbf{S}\ t \mid \textbf{P}\ t \mid \textbf{iszero}\ t$$

A judgment *bvalue* t means that t is a boolean value (which cannot be further reduced):

$$\frac{}{\mathit{bvalue}\ \textbf{true}}\ \textsf{btrue} \qquad \frac{}{\mathit{bvalue}\ \textbf{false}}\ \textsf{bfalse}$$

A judgment *nvalue* t means that t is a natural number value:

$$\frac{}{\mathit{nvalue}\ \textbf{0}}\ \textsf{nzero} \qquad \frac{\mathit{nvalue}\ t}{\mathit{nvalue}\ \textbf{S}\ t}\ \textsf{nsucc}$$

A judgment *value* t means that t is a value (either a natural number value or a boolean value):

$$\frac{\mathit{nvalue}\ t}{\mathit{value}\ t}\ \textsf{natv} \qquad \frac{\mathit{bvalue}\ t}{\mathit{value}\ t}\ \textsf{booleanv}$$

The small-step semantics uses a reduction judgment $t \mapsto t'$ which means that term t reduces to term t' in a single step. Reduction rules for the small-step semantics are given as follows:

$$\frac{}{\textbf{if true then}\ t_2\ \textbf{else}\ t_3 \mapsto t_2}\ \textsf{iftrue} \qquad \frac{}{\textbf{if false then}\ t_2\ \textbf{else}\ t_3 \mapsto t_3}\ \textsf{iffalse}$$

$$\frac{t_1 \mapsto t_1'}{\textbf{if}\ t_1\ \textbf{then}\ t_2\ \textbf{else}\ t_3 \mapsto \textbf{if}\ t_1'\ \textbf{then}\ t_2\ \textbf{else}\ t_3}\ \textsf{if}$$

$$\frac{t \mapsto t'}{\textbf{S}\ t \mapsto \textbf{S}\ t'}\ \textsf{succ} \qquad \frac{}{\textbf{P}\ \textbf{0} \mapsto \textbf{0}}\ \textsf{predzero} \qquad \frac{\mathit{nvalue}\ t}{\textbf{P}\ (\textbf{S}\ t) \mapsto t}\ \textsf{predsucc} \qquad \frac{t \mapsto t'}{\textbf{P}\ t \mapsto \textbf{P}\ t'}\ \textsf{pred}$$

$$\frac{}{\textbf{iszero}\ \textbf{0} \mapsto \textbf{true}}\ \textsf{iszerozero} \qquad \frac{\mathit{nvalue}\ t}{\textbf{iszero}\ (\textbf{S}\ t) \mapsto \textbf{false}}\ \textsf{iszerosucc} \qquad \frac{t \mapsto t'}{\textbf{iszero}\ t \mapsto \textbf{iszero}\ t'}\ \textsf{iszero}$$

We say that a term t is in normal form if it does not reduce to another term, and use a judgment *normal* t:

$$\mathit{normal}\ t \quad \iff \quad \text{There exists no term } t' \text{ such that } t \mapsto t'.$$

All the above definitions are given in the Coq script.

2 Deterministic reduction

We want to prove that the reduction of a term is always deterministic.

Lemma 2.1. *If bvalue t, then normal t.*

Lemma 2.2. *If nvalue t, then normal t.*

Lemma 2.3. *If value t, then normal t.*

Theorem 2.4. *If $t \mapsto t'$ and $t \mapsto t''$, then $t' = t''$.*

Prove Theorem 2.4 in Coq.

3 Verifying the interpreter

We write $\mapsto^*$ for the reflexive and transitive closure of $\mapsto$:

$$\frac{}{t \mapsto^* t}\ \mathsf{refl} \qquad \frac{t \mapsto t' \quad t' \mapsto^* u}{t \mapsto^* u}\ \mathsf{step}$$

The definition of the interpreter **interp** is given in the Coq script. The specification for the interpreter **interp** is as follows:

- **interp** t returns t' if and only if $t \mapsto^* t'$ and there is no term t'' such that $t' \mapsto t''$.

We want to formally verify the definition of **interp**.

Theorem 3.1. *For every term t, we have $t \mapsto^*$* **interp** *t.*

Theorem 3.2. *For every term t,* **interp** *t is in normal form,* i.e., *normal* **interp** *t holds.*

Prove Theorems 3.1 and 3.2 in Coq.