1 Introduction

This note expands on Chapters 28 and 29 of PFPL by considering both a by-name and a by-value stack machine, and proving safety for both cases.

2 By-Name Stack Machine

The abstract syntax of the by-name stack machine for PCF is given by the following grammar:

Types
\( \tau ::= \text{nat} \mid \tau_1 \rightarrow \tau_2 \)

Stacks
\( k ::= \varepsilon \mid k ; f \)

Frames
\( f ::= \text{ap}(\neg;e_2) \mid \text{ifz}(\tau)(\neg;e_0;x.e_1) \)

Expr’s
\( e ::= x \mid z \mid s(e) \mid \text{ifz}(\tau)(e;e_0;x.e_1) \mid \lambda(\tau)(x.e) \mid \text{ap}(e_1;e_2) \mid \text{fix}(\tau)(x.e) \)

States
\( s ::= k \# e \)

The statics for the by-name stack machine is given in Figure 1; the typing rules for PCF-by-name expressions are omitted, as they can be found in the text. The dynamics for the by-name stack machine is defined in Figure 2.

The safety theorem for the by-name stack machine is stated according to the familiar pattern.

Theorem 2.1 (Safety). The by-name stack machine enjoys these properties:

1. If \( s \xrightarrow{\cdot} s' \) then \( s \text{ ok} \) implies \( s' \text{ ok} \).

2. If \( s \text{ ok} \), then either \( s \text{ done} \) or \( s \xrightarrow{\cdot} s' \) for some state \( s' \).

To prove these requires two auxiliary lemmas, the canonical forms lemma and the stack lemma.

Lemma 2.2 (Canonical Forms By Name). If \( e : \tau \) and \( e \text{ val} \), then

1. if \( \tau = \text{nat} \), then either \( e = z \) or \( e = s(e') \) for some \( e' : \text{nat} \);

2. if \( \tau = \tau_1 \rightarrow \tau_2 \), then \( e = \lambda(\tau_1)(x.e_2) \) with \( x : \tau_1 \vdash e_2 : \tau_2 \).

Lemma 2.3 (Stacks By Name). If \( k \div \tau \) is non-empty, then

1. if \( \tau = \text{nat} \), then \( k = k' ; \text{ifz}(\tau)(\neg;e_0;x.e_1) \) for some \( k' \div \tau \), \( e_0 : \tau \), and \( x : \text{nat} \vdash e_1 : \tau \).

2. if \( \tau = \tau_2 \rightarrow \tau' \), then \( k = k' ; \text{ap}(\neg;e_2) \) for some \( k' \div \tau_2 \rightarrow \tau' \) and \( e_2 : \tau_2 \).
\[
\begin{align*}
\varepsilon & \vdash \tau \\
k & \vdash \tau & f : \tau & \leadsto \tau' \quad (1a) \\
k & \vdash \tau & f & \vdash \tau' \\
k & \vdash \tau & \text{ap}(-;e_2) : \tau_2 & \leadsto \tau & \leadsto \tau & \quad (1b) \\
e_0 : \tau & x : \text{nat} & \vdash e_1 : \tau & \quad (1c) \\
\text{ifz}\{\tau\}(-; e_0; x. e_1) : \text{nat} & \leadsto \tau \\
k & \vdash \tau & e : \tau & \quad (1d) \\
k & \vdash \tau & e & \text{ok} \\
k & \vdash \tau & e_0 \\
k & \vdash \tau & e_1 \\
\end{align*}
\]

Figure 1: Statics of By-Name Stack Machine

\[
\begin{align*}
\varepsilon & \# e \text{ ready} \\
e & \text{ val} \\
\varepsilon & \# e \text{ done} \\
k & \vdash \tau & e_0; x. e_1 & \# z & \rightarrow & k & \# e_0 & \quad (2) \\
k & \vdash \tau & e_0; x. e_1 & \# s(e) & \rightarrow & k & \# [e/x]e_1 & \quad (3) \\
k & \# \text{ifz}\{\tau\}(-; e_0; x. e_1) & \# e & \rightarrow & k & \# [e/x]e_1 & \quad (4a) \\
k & \# \text{ifz}\{\tau\}(-; e_0; x. e_1) & \# \text{ifz}\{\tau\}(-; e_0; x. e_1) & \# e & \quad (4b) \\
k & \# \text{ap}(-; e_2) & \# \lambda\tau_2(x. e) & \rightarrow & k & \# [e_2/x]e & \quad (4c) \\
k & \# \text{ap}(e_1; e_2) & \rightarrow & k & \# \text{ap}(-; e_2) & \# e_1 & \quad (4d) \\
k & \# \text{fix}\{\tau\}(x. e) & \rightarrow & k & \# \text{fix}\{\tau\}(x. e)/x & e & \quad (4e) \\
k & \# \text{fix}\{\tau\}(x. e) & \rightarrow & k & \# \text{fix}\{\tau\}(x. e)/x & e & \quad (4f) \\
\end{align*}
\]

Figure 2: Dynamics of By-Name Stack Machine
Both of these lemmas are proved by induction on the relevant typing judgments. Now, on to the proof the safety theorem.

Proof. 1. Preservation is proved by induction on the transitions of the state machine. Because the transitions are defined by rules free of premises, the induction reduces to a case analysis on each of the rules, with no appeal to any inductive hypothesis. Assume that \( s \) ok, and that \( s \mapsto s' \) for some \( s' \), with the intention to show that \( s' \) ok. By inversion on the first assumption, \( s = k \# e \) for some \( k \) and \( e \) such that \( k \div \sigma \) and \( e : \sigma \) for some mediating type \( \sigma \). Consider the possible transitions from \( s \):

(a) Rule 4a: The mediating type \( \sigma \) must be \( \text{nat} \), and so \( k' \div \tau \) where \( e_0 : \tau \) and \( x : \text{nat} \vdash e_1 : \tau \). But then \( k' \# e_0 \) ok, taking the mediating type to be \( \tau \).

(b) Rule 4b Similar, using inversion to obtain the type of the predecessor.

(c) Rule 4c: The mediating type \( \sigma \) is the type \( \tau \) of the conditional, and so \( k \div \tau \), \( e_0 : \tau \), and \( x : \text{nat} \vdash e_1 : \tau \). But then \( k ; \text{ifz}\{\tau\}(\neg ; e_0 ; x.e_1) \div \text{nat} \), which is enough to ensure \( k ; \text{ifz}\{\tau\}(\neg ; e_0 ; x.e_1) \# e \) ok.

(d) Rules 4d and Rule 4e: Similar.

(e) Rule 4f: immediate by inversion of typing.

2. Progress is proved by analysis of the assumption \( s \) ok. By inversion \( s \) must be \( k \# e \) for some \( k \) and \( e \) such that \( k \div \sigma \) and \( e : \sigma \) for some mediating type \( \sigma \). Proceed by cases on whether \( e \) is a value or not.

(a) If \( e \) \text{val} , then consider whether \( k \) is empty or not. If \( k = \varepsilon \), then \( s \) done, which completes the proof. If \( k \) is non-empty, then the stack lemma applies, according to the mediating type \( \sigma \).

i. If \( \sigma = \text{nat} \), then by the stack lemma \( k = k' ; \text{ifz}\{\tau'\}(\neg ; e_0 ; x.e_1) \), where \( k' \div \tau' \), \( e_0 : \tau' \), and \( x : \text{nat} \vdash e_1 : \tau' \). By the canonical forms lemma either \( e = z \) or \( e = s(e') \) with \( e' : \text{nat} \). In the former case, apply Rule 4a, in the latter apply Rule 4b.

ii. If \( \sigma = \sigma_1 \rightarrow \sigma_2 \), then by canonical forms \( e = \lambda{\sigma_1}(x.e_2) \), and by the stack lemma \( k = k' ; \text{ap}(\neg ; e_2) \), where \( k' \div \sigma_2 \) and \( x : \sigma_1 \vdash e_2 : \tau_2 \). Then apply Rule 4e to ensure progress.

(b) If \( e \) is not a value, then either \( e = \text{ap}(e_1 ; e_2) \) or \( e = \text{ifz}\{\tau\}(e' ; e_0 ; x.e_1) \) or \( e = \text{fix}\{\tau\}(x.e) \). Rules 4c, 4e, and 4f ensure progress in the respective cases.

The proof is not all that different from the usual one for \( \text{PCF} \), but for the explicit manipulation of the stack.

3 By-Value Stack Machine

The by-value stack machine is defined in \( \text{PFPL} \) using states of the form \( k \triangleright e \) and \( k \triangleleft e \) where \( e \) \text{val}. The by-value dynamics is given in Figure 3 for convenient reference. Observe that the successor operation is strict (evaluates its argument) and that applications evaluate their argument before calling the specified (recursive) function.
Figure 3: Dynamics of the By-Value Stack Machine
The proof of the safety theorem for the by-value stack machine proceeds along similar lines to the proof for the by-name case, with the significant difference being the statements of the canonical forms and stack lemmas. With regard to stacks, the type of the stack no longer uniquely determines the topmost frame, because of the eager successor and call-by-value application.

**Lemma 3.1 (Canonical Forms By Value).** If \( e : \tau \) and \( e \text{ val} \), then

1. if \( \tau = \text{nat} \), then \( e = \overline{n} \) for some \( n \in \mathbb{N} \).

2. if \( \tau = \tau_1 \rightarrow \tau_2 \), then \( e = \text{fun}\{\tau_1;\tau_2\}(f.x.e_2) \) with \( f : \tau_1 \rightarrow \tau_2, x : \tau_1 \vdash e_2 : \tau_2 \).

**Lemma 3.2 (Stacks By Value).** If \( k \div \tau \) for some non-empty stack \( k = k'; f \), then

1. if \( \tau = \text{nat} \), then \( k' \div \tau' \), and either
   
   (a) \( f = \text{ifz}\{\tau'\}(\_;e_0;x.e_1) \) with \( e_0 : \tau' \) and \( x : \text{nat} \vdash e_1 : \tau' \), or
   
   (b) \( f = \text{s}(\_\_\_) \) and \( \tau' = \text{nat} \), or
   
   (c) \( f = \text{ap}(e_1;\_\_) \) with \( e_1 \text{ val} \) and \( e_1 : \text{nat} \rightarrow \tau' \).

2. if \( \tau = \tau_2 \rightarrow \tau' \), then \( k' \div \tau' \) and either
   
   (a) \( f = \text{ap}(\_\_;e_2) \) with \( e_2 : \tau_2 \), or
   
   (b) \( f = \text{ap}(e_1;\_\_) \) with \( e_1 \text{ val} \) and \( e_1 : \tau \rightarrow \tau' \), or
   
   (c) \( f = \text{ifz}\{\tau'\}(\_;e_0;x.e_1) \) with \( e_0 : \tau' \) and \( x : \text{nat} \vdash e_1 : \tau' \).

The by-value dynamics introduces many more possibilities for a stack of a given type! This complicates the safety proof by requiring further case analyses according to the stacks lemma, applying the appropriate rule in each case to established progress.

**References**