Chapter 1

Evaluation contexts

This chapter presents an alternative formulation of the operational semantics for the simply typed λ-calculus. Compared with the operational semantics in Chapter ??, the new formulation is less complex, yet better reflects reductions of expressions in a concrete implementation. The new formulation is a basis for an abstract machine for the simply typed λ-calculus, which, like the Java virtual machine, is capable of running a program independently of the underlying hardware platform.

1.1 Evaluation contexts

Consider the simply typed λ-calculus given in Chapter ??:

| type     | A ::= P | A → A |
| base type | P ::= bool |
| expression| e ::= x | λx:A. e | e e | true | false | if e then e else e |
| value    | v ::= λx:A. e | true | false |

A reduction judgment \( e \mapsto e' \) for the call-by-value strategy is defined inductively by the following reduction rules:

\[
\begin{align*}
\frac{\text{Lam}}{e_1 \mapsto e'_1} & \quad \frac{\text{Arg}}{e_2 \mapsto (\lambda x:A. e) e_2} & \quad \frac{\text{App}}{(\lambda x:A. e) v \mapsto [v/x]e} \\
\frac{\text{If}}{\text{if } e \text{ then } e_1 \text{ else } e_2 \mapsto e'} & \quad \frac{\text{If true}}{\text{if true then } e_1 \text{ else } e_2 \mapsto e_1} & \quad \frac{\text{If false}}{\text{if false then } e_1 \text{ else } e_2 \mapsto e_2}
\end{align*}
\]

Since only the rules App, If true, and If false have no premise, every derivation tree for a reduction judgment \( e \mapsto e' \) must end with an application of one of these rules:

\[
\begin{align*}
\frac{(\lambda x:A. e'') v \mapsto [v/x]e''}{\text{App}} & \quad \frac{\text{If true}}{\text{if true then } e_1 \text{ else } e_2 \mapsto e_1} & \quad \frac{\text{If false}}{\text{if false then } e_1 \text{ else } e_2 \mapsto e_2}
\end{align*}
\]
Thus the reduction of an expression \( e \) amounts to locating an appropriate subexpression \( (\lambda x : A. e') \) \( v \), if true then \( e_1 \) else \( e_2 \), or if false then \( e_1 \) else \( e_2 \) of \( e \) and applying a corresponding reduction rule.

As an example, let us reduce the following expression:

\[
e = (\text{if } (\lambda x : A. e') v \text{ then } e_1 \text{ else } e_2) e'
\]

The reduction of \( e \) cannot proceed without first reducing the underlined subexpression \( (\lambda x : A. e') \) \( v \) by the rule \( \text{App} \), as shown in the following derivation tree:

\[
\begin{align*}
(\lambda x : A. e'') v & \mapsto [v/x]e'' \quad \text{App} \\
\quad v & \mapsto [v/x]e'' \quad \text{If} \\
(\text{if } (\lambda x : A. e'') v \text{ then } e_1 \text{ else } e_2) e' & \mapsto \ldots \quad \text{Lam}
\end{align*}
\]

Then we may think of \( e \) as consisting of two parts: a subexpression, or a redex, \( (\lambda x : A. e'') \) \( v \) which actually reduces to another expression \([v/x]e''\) by the rule \( \text{App} \), and the rest which remains intact during the reduction. Note that the second part is not an expression because it is obtained by erasing the redex from \( e \). We write the second part as \( (\text{if } \Box \text{ then } e_1 \text{ else } e_2) e' \) where the hole \( \Box \) indicates the position of the redex.

We refer to an expression with a hole in it, such as \( (\text{if } \Box \text{ then } e_1 \text{ else } e_2) e' \), as an evaluation context. The hole indicates the position of the redex (to be reduced by one of the rules \( \text{App} \), \( \text{If} \), and \( \text{If} \)) for the next step. Note that we may not use the rule \( \text{Lam} \), \( \text{Arg} \), or \( \text{If} \) to reduce the redex, since none of these rules reduces the whole redex in a single step.

Since the hole in an evaluation context indicates the position of a redex, every expression is decomposed into a unique evaluation context and a unique redex under a particular reduction strategy. For the same reason, not every expression with a hole in it is a valid evaluation context. For example, \((e_1 e_2) \Box \) is not a valid evaluation context under the call-by-value strategy because given an expression \((e_1 e_2) e' \), we have to reduce \( e_1 e_2 \) before we reduce \( e' \). These two observations show that a particular reduction strategy specifies a unique inductive definition of evaluation contexts. The call-by-value strategy results in the following definition:

\[
\text{evaluation context} \quad \kappa ::= \Box | \kappa e | (\lambda x : A. e) \kappa | \text{if } \kappa \text{ then } e_1 \text{ else } e_2
\]

\( \kappa e \) is an evaluation context for \( e' \) \( e \) where \( e' \) needs to be further reduced; \( (\lambda x : A. e) \kappa \) is an evaluation context for \( (\lambda x : A. e) e' \) where \( e' \) needs to be further reduced. Similarly if \( \kappa \) then \( e_1 \) else \( e_2 \) is an evaluation context for \( e' \) then \( e_1 \) else \( e_2 \) where \( e' \) needs to be further reduced.

Let us write \( \kappa[e] \) for an expression obtained by filling the hole in \( \kappa \) with \( e \). Here are a few examples:

\[
\begin{align*}
\Box[(\lambda x : A. e'') v] & = (\lambda x : A. e'') v \\
(\text{if } \Box \text{ then } e_1 \text{ else } e_2)[(\lambda x : A. e'') v] & = (\text{if } (\lambda x : A. e'') v \text{ then } e_1 \text{ else } e_2) \\
((\text{if } \Box \text{ then } e_1 \text{ else } e_2) e')[(\lambda x : A. e'') v] & = (\text{if } (\lambda x : A. e'') v \text{ then } e_1 \text{ else } e_2) e'
\end{align*}
\]

A formal definition of \( \kappa[e] \) is given as follows:

\[
\begin{align*}
\Box[e] & = e \\
(\kappa e')[e] & = \kappa[e] e' \\
((\lambda x : A. e') \kappa)[e] & = (\lambda x : A. e') \kappa[e] \\
(\text{if } \kappa \text{ then } e_1 \text{ else } e_2)[e] & = \kappa[e] \text{ if } e_1 \text{ else } e_2
\end{align*}
\]

Now consider an expression which is known to reduce to another expression. We can write it as \( \kappa[e] \) for a unique evaluation context \( \kappa \) and a unique redex \( e \). Since \( \kappa[e] \) is known to reduce to another expression, \( e \) must also reduce to another expression \( e' \). We write \( e \rightarrow_\beta e' \) to indicate that the reduction of \( e \) to \( e' \) uses the rule \( \text{App} \), \( \text{If_true} \), or \( \text{If_false} \). Then the following reduction rule alone is enough to completely specify a reduction strategy because the order of reduction is implicitly determined by the definition of evaluation contexts:

\[
\begin{align*}
e & \rightarrow_\beta e' \\
\kappa[e] & \rightarrow \kappa[e']
\end{align*}
\]

April 16, 2009
evaluation context \( \kappa ::= \emptyset | \kappa \cdot e | (\lambda x : A \cdot e) \kappa \) if \( \kappa \) then \( e \) else \( e \)

\[
(\lambda x : A \cdot e) v \quad \rightsquigarrow_{\beta} \quad [v/x]e
\]

if true then \( e_1 \) else \( e_2 \) \quad \rightsquigarrow_{\beta} \quad e_1

if false then \( e_1 \) else \( e_2 \) \quad \rightsquigarrow_{\beta} \quad e_2

\[
\frac{e \rightsquigarrow_{\beta} e'}{\kappa[e] \rightsquigarrow_{\beta} \kappa[e']}
\]

\( \text{Red}_{\beta} \)

Figure 1.1: Call-by-value operational semantics using evaluation contexts

evaluation context \( \kappa ::= \emptyset | \kappa \cdot e | (\lambda x : A \cdot e) \kappa \) if \( \kappa \) then \( e \) else \( e \)

\[
(\lambda x : A \cdot e) e' \quad \rightsquigarrow_{\beta} \quad [e'/x]e
\]

if true then \( e_1 \) else \( e_2 \) \quad \rightsquigarrow_{\beta} \quad e_1

if false then \( e_1 \) else \( e_2 \) \quad \rightsquigarrow_{\beta} \quad e_2

\[
\frac{e \rightsquigarrow_{\beta} e'}{\kappa[e] \rightsquigarrow_{\beta} \kappa[e']}
\]

\( \text{Red}_{\beta} \)

Figure 1.2: Call-by-name operational semantics using evaluation contexts

The reduction relation \( \rightsquigarrow_{\beta} \) is defined by the following equations:

\[
(\lambda x : A \cdot e) v \quad \rightsquigarrow_{\beta} \quad [v/x]e
\]

if true then \( e_1 \) else \( e_2 \) \quad \rightsquigarrow_{\beta} \quad e_1

if false then \( e_1 \) else \( e_2 \) \quad \rightsquigarrow_{\beta} \quad e_2

Figure 1.1 summarizes how to use evaluation contexts to specify the call-by-value operational semantics. An example of a reduction sequence is shown below. In each step, we underline the redex and show how to decompose a given expression into a unique evaluation context and a unique redex.

\[
(\text{if} (\text{if} \lambda y : \text{bool} \cdot y \text{ else} \lambda z : \text{bool} \cdot z) \text{ true} \text{ then} \lambda y : \text{bool} \cdot y \text{ else} \lambda z : \text{bool} \cdot z) \text{ true} \quad \rightsquigarrow_{\beta} \quad (\text{if} \text{ true} \text{ then} \lambda y : \text{bool} \cdot y \text{ else} \lambda z : \text{bool} \cdot z) \text{ true} \\
= \quad (\text{if} \text{ true} \text{ then} \lambda y : \text{bool} \cdot y \text{ else} \lambda z : \text{bool} \cdot z) \text{ true} \\
\cdot \quad (\lambda y : \text{bool} \cdot y) \text{ true} \\
= \quad \emptyset \text{ true} \\
\rightsquigarrow_{\beta} \quad \text{true}
\]

In order to obtain the call-by-name operational semantics, we only have to change the inductive definition of evaluation contexts and the reduction relation \( \rightsquigarrow_{\beta} \), as shown in Figure 1.2. With a proper understanding of evaluation contexts, it should also be straightforward to incorporate those reduction rules in Chapter ?? into the definition of evaluation contexts and the reduction relation \( \rightsquigarrow_{\beta} \). The reader is encouraged to try to augment the definition of evaluation contexts and the reduction relation \( \rightsquigarrow_{\beta} \). See Figures 1.3 and 1.4 for the result.

Exercise 1.1. Give a definition of evaluation contexts corresponding to the weird reduction strategy specified in Exercise ??.

1.2 Type safety

As usual, type safety consists of progress and type preservation:

April 16, 2009
Proof.

Case

\[\begin{align*}
\text{evaluation context} \quad \kappa & := \cdots | (\kappa, \epsilon) | (v, \kappa) | \text{fst} \, \kappa | \text{snd} \, \kappa | \\
& \quad \text{inl}_A \, \kappa | \text{inr}_A \, \kappa | \text{case} \, \kappa \text{ of } \text{inl} \, x. \, e | \text{inr} \, x. \, e
\end{align*}\]

\[\begin{align*}
\text{fst} \, (v_1, v_2) & \mapsto_\beta v_1 \\
\text{snd} \, (v_1, v_2) & \mapsto_\beta v_2
\end{align*}\]

\[\begin{align*}
\text{case } \text{inl}_A \, v \text{ of } \text{inl} \, x_1, e_1 & \mapsto_\beta [v/x_1]e_1 \\
\text{case } \text{inr}_A \, v \text{ of } \text{inl} \, x_1, e_1 & \mapsto_\beta [v/x_2]e_2 \\
\text{fix } x : A. \, e & \mapsto_\beta \text{[fix } x : A, e/x]e
\end{align*}\]

\[\begin{align*}
\text{The proof of Theorem } 1.2 & \text{ is similar to the proof of Theorem } 0.0. \\
\text{The proof of Theorem } 1.3 & \text{ uses the following lemma whose proof uses Lemma } 0.0:
\end{align*}\]

\[\begin{align*}
\text{Lemma } 1.5. & \text{ If } \Gamma \vdash \kappa | e : C, \text{ then } \Gamma \vdash e : A \text{ and } \Gamma \vdash \kappa : A \Rightarrow C \text{ for some type } A.
\end{align*}\]
1.3 Abstract machine C

The concept of evaluation context leads to a concise formulation of the operational semantics, but it is not suitable for an actual implementation of the simply typed λ-calculus. The main reason is that the rule Red_3 tacitly assumes an automatic decomposition of a given expression into a unique evaluation context and a unique redex, but it may in fact require an explicit analysis of the given expression in several steps. For example, in order to rewrite

\[
e = \text{(if } (\lambda x : A. e'') \; v \text{ then } e_1 \text{ else } e_2) \; e'
\]

as \((\text{(if } \Box \text{ then } e_1 \text{ else } e_2) \; e')[(\lambda x : A. e'') \; v]\), we would analyze \(e\) in several steps:

\[
e = \Box[(\text{(if } (\lambda x : A. e'') \; v \text{ then } e_1 \text{ else } e_2) \; e')]
\]

\[= (\Box \; e')[(\text{(if } (\lambda x : A. e'') \; v \text{ then } e_1 \text{ else } e_2) \; e')]
\]

\[= ((\text{if } \Box \text{ then } e_1 \text{ else } e_2) \; e')[(\lambda x : A. e'') \; v]
\]

The abstract machine C is another formulation of the operational semantics in which such an analysis is explicit.

Roughly speaking, the abstract machine C replaces an evaluation context by a stack of frames such that each frame corresponds to a specific step in the analysis of a given expression:

\[
\text{frame} \quad \phi \quad ::= \quad \Box \; e \mid (\lambda x : A. e) \; \Box \mid \text{if } \Box \text{ then } e_1 \text{ else } e_2
\]

\[
\text{stack} \quad \sigma \quad ::= \quad \Box \mid \sigma \mid \phi
\]

Frames are special cases of evaluation contexts which are not defined inductively. Thus we may write \(\phi[e]\) for an expression obtained by filling the hole in \(\phi\) with \(e\). A stack of frames also represents an evaluation context in that given an expression, it determines a unique expression. To be specific, a stack \(\sigma\) and an expression \(e\) determine a unique expression \(\sigma[e]\) defined inductively as follows:

\[
\Box[e] = e
\]

\[\sigma[\phi[e]] = \sigma[\phi[e]]\]

If we write \(\sigma\) as \(\Box; \phi_1; \phi_2; \cdots; \phi_n\) for \(n \geq 0\), \(\sigma[e]\) may be written as

\[\Box[\phi_1[\phi_2[\cdots[\phi_n[e]]]]]
\]

Now, for example, an implicit analysis of \(e = \text{(if } (\lambda x : A. e'') \; v \text{ then } e_1 \text{ else } e_2) \; e'\) shown above can be made explicit by using a stack of frames:

\[
e = (\Box; \Box e'; \text{if } \Box \text{ then } e_1 \text{ else } e_2)[(\lambda x : A. e'') \; v]
\]

Note that the top frame of a stack \(\sigma; \phi\) is \(\phi\) and that the bottom of a stack is always \(\Box\).

A state of the abstract machine C is specified by a stack \(\sigma\) and an expression \(e\), in which case the machine can be thought of as reducing an expression \(\sigma[e]\). In addition, the state includes a flag to indicate whether \(e\) needs to be further analyzed or has already been reduced to a value. Thus we use the following definition of states:

\[
\text{state} \quad s \quad ::= \quad \sigma \triangleright e \mid \sigma \triangleleft v
\]
• $\sigma \triangleright e$ means that the machine is currently reducing $\sigma[e]$, but has yet to analyze $e$.

• $\sigma \triangleright v$ means that the machine is currently reducing $\sigma[v]$ and has already analyzed $v$. That is, it is returning $v$ to the top frame of $\sigma$.

Thus, if an expression $e$ evaluates to a value $v$, a state $\sigma \triangleright e$ will eventually lead to another state $\sigma \triangleright v$. As a special case, the initial state of the machine evaluating $e$ is always $\square \triangleright e$ and the final state $\square \triangleright v$ if $e$ evaluates to $v$.

A state transition in the abstract machine $C$ is specified by a reduction judgment $s \xrightarrow{s'}$; we write $\xrightarrow{c}$ for the reflexive and transitive closure of $\xrightarrow{c}$ . The guiding principle for state transitions is to maintain the invariant that $e \xrightarrow{*} v$ holds if and only if $\sigma \xrightarrow{c} \sigma \triangleright v$ holds for any stack $\sigma$. The rules for the reduction judgment $s \xrightarrow{c} s'$ are as follows:

| $\sigma \triangleright e_1 \xrightarrow{c} \sigma \triangleright e_2$ | $\sigma ; e_2 \triangleright \lambda x : A . e \xrightarrow{c} \sigma ; (\lambda x : A . e) \square \triangleright e_2$ |
| $\sigma ; (\lambda x : A . e) \square \triangleright v \xrightarrow{c} \sigma \triangleright [v/x] e$ | $\sigma \triangleright e_1 \xrightarrow{c} \sigma ; e_2 \triangleright e$ |

An example of a reduction sequence is shown below. Note that it begins with a state $\square \triangleright e$ and ends with a state $\square \triangleright v$.

$\xrightarrow{c}$ $\square \triangleright (\lambda x :\text{bool} . x)$ true then $\lambda y :\text{bool} . y$ else $\lambda z :\text{bool} . z$ true $\xrightarrow{c}$ $\square ; \square \triangleright (\lambda x :\text{bool} . x)$ true then $\lambda y :\text{bool} . y$ else $\lambda z :\text{bool} . z$ $\xrightarrow{c}$ $\square ; \square \triangleright \lambda y :\text{bool} . y$ else $\lambda z :\text{bool} . z$ $\xrightarrow{c}$ $\square ; \square \triangleright \lambda x :\text{bool} . x$ $\square \triangleright \lambda x :\text{bool} . x$ true $\xrightarrow{c}$ $\square \triangleright \lambda y :\text{bool} . y$

1.4 Correctness of the abstract machine $C$

This section presents a proof of the correctness of the abstract machine $C$ as stated in the following theorem:

**Theorem 1.6.** $e \xrightarrow{*} v$ if and only if $\square \triangleright e \xrightarrow{c} \square \triangleright v$.

A more general version of the theorem allows any stack $\sigma$ in place of $\square$, but we do not prove it here. For the sake of simplicity, we also do not consider expressions of type bool altogether. It is a good and challenging exercise to prove the theorem. The main difficulty lies in finding several lemmas necessary for proving the theorem, not in constructing their proofs. The reader is encouraged to guess these lemmas without having to write their proofs.

The proof uses a generalization of $\kappa[\cdot]$ and $\sigma[\cdot]$ over evaluation contexts:

$$\square[\kappa'] = \kappa'$$
$$\square[\lambda x : A . e][\kappa'] = (\lambda x : A . e)[\kappa']$$
$$\square[\sigma ; \phi][\kappa] = \sigma[\phi[\kappa]]$$

April 16, 2009
Note that $\kappa[\kappa']$ and $\sigma[\kappa]$ are evaluation contexts.

**Proposition 1.7.** $\kappa[\kappa'[e]] = \kappa[\kappa'][e]$.

**Proof.** By structural induction on $\kappa$. We show two cases.

Case $\kappa = \Box$:

$\Box[\kappa'[e]] = \kappa'[e] = \Box[\kappa'][e]$

Case $\kappa = \kappa'' \epsilon''$:

$(\kappa'' \epsilon'')[\kappa'[e]] = \kappa''[\kappa'[e]] \epsilon'' = \kappa''[\kappa'][e] \epsilon'' = (\kappa''[\kappa'][\epsilon''])[e] = (\kappa'' \epsilon'')[\kappa'][e]$.

**Proposition 1.8.** $\sigma[\kappa[e]] = \sigma[\kappa][e]$.

**Proof.** By structural induction on $\kappa$. The second case uses Proposition 1.7.

Case $\sigma = \Box$:

$\Box[\kappa[e]] = \kappa[e] = \Box[\kappa][e]$.

Case $\sigma = \sigma'; \phi$:

$(\sigma'; \phi)[\kappa[e]] = \sigma'[\phi[\kappa][e]] = \sigma'[\phi[\kappa][e]] = \sigma'[\phi[\kappa][e]] = (\sigma'; \phi)[\kappa][e]$.

**Lemma 1.9.** For $\sigma$ and $\kappa$, there exists $\sigma'$ such that $\sigma \triangleright \kappa[e] \rightarrow_\varsigma \sigma' \triangleright e$ and $\sigma[\kappa] = \sigma'[\Box]$ for any expression $e$.

**Proof.** By structural induction on $\kappa$. We show two cases.

Case $\kappa = \Box$:

We let $\sigma' = \sigma$.

Case $\kappa = \kappa' \epsilon'$:

$\sigma \triangleright (\kappa' \epsilon')[\kappa[e]] = \sigma \triangleright \kappa'[\kappa[e]] \epsilon' \rightarrow_\varsigma \sigma; \Box \epsilon' \triangleright \kappa'[e]$ by the rule $\text{Lam}_{\varsigma}$

$\sigma; \Box \epsilon' \triangleright \kappa'[e] \rightarrow_\varsigma \sigma' \triangleright e$ and $\sigma; \Box \epsilon' \triangleright \kappa'[\kappa][e] = \sigma' \triangleright \Box$ by induction hypothesis

$\sigma[\kappa] = \sigma[\kappa' \epsilon'][e] = \sigma[\Box \epsilon'][\kappa][e] = (\sigma; \Box \epsilon' \triangleright \kappa')[\kappa] = \sigma'[\Box]$.

**Lemma 1.10.** Suppose $\sigma[e] = \kappa[f v]$ where $f$ is a lambda abstraction. Then one of the following cases holds:

1. $\sigma \triangleright e \rightarrow_\varsigma \sigma' \triangleright \kappa'[f v]$ and $\sigma' \triangleright \kappa$.
2. $\sigma = \sigma'; \Box v$ and $e = f$ and $\sigma'[\Box] = \kappa$.
3. $\sigma = \sigma'; f \Box$ and $e = v$ and $\sigma'[\Box] = \kappa$.

**Proof.** By structural induction on $\sigma$. We show two cases.

Case $\sigma = \Box$:

$\sigma[e] = e = \kappa[f v]$ assumption

$\sigma \triangleright e = \Box \triangleright \kappa[f v]$ (1) $\sigma \triangleright e \rightarrow_\varsigma \Box \triangleright \kappa[f v]$ and $\Box[\kappa] = \kappa$

Case $\sigma = \sigma'; \Box v'$:

$\sigma[e] = (\sigma'; \Box v')[e] = \sigma'[\Box v'][e] = \sigma'[e v'] = \kappa[f v]$.

Subcase (1) $\sigma' \triangleright e v' \rightarrow_\varsigma \sigma'' \triangleright \kappa'[f v]$ and $\sigma''[\kappa'] = \kappa$ by induction hypothesis on $\sigma'$

$\sigma' \triangleright e v' \rightarrow_\varsigma \sigma'' \triangleright \kappa' \triangleright \kappa'[f v]$ assumption

(1) $\sigma \triangleright e v' \rightarrow_\varsigma \kappa'' \triangleright \kappa'[f v]$ and $\sigma''[\kappa'] = \kappa$

$\sigma' = \sigma''$ and $e v' = \kappa'[f v]$, and $\kappa' = \Box$ assumption

$e = f$ and $\epsilon' = v$

(2) $\sigma = \sigma'; \Box v$ and $e = f$ and $\sigma'[\Box] = \sigma''[\kappa'] = \kappa$

April 16, 2009 7
\[ \sigma' = \sigma'' \text{ and } e \ e' = \kappa'[f \ v], \text{ and } \kappa' = \kappa'' e' \]

assumption

\[ e = \kappa'[f \ v] \]

\( (1) \sigma \triangleright e \mapsto \_ \sigma \triangleright \kappa''[f \ v] \text{ and} \]

\[ \sigma[\kappa''] = (\sigma''; \sqcap e')[v] = \sigma''[\kappa''][e'] = \sigma''[\kappa'] = \kappa \]

\[ \sigma' = \sigma'' \text{ and } e \ e' = \kappa'[f \ v], \text{ and } \kappa' = e \kappa'' \]

assumption

\[ e \text{ is a } \lambda\text{-abstraction and } e' = \kappa''[f \ v] \]

\( (1) \sigma \triangleright e \mapsto \_ \sigma' \triangleright e \mapsto \_ \sigma' \triangleright e \mapsto \_ \sigma' \triangleright e' = \sigma' \triangleright e \square \triangleright \kappa''[f \ v] \]

and \( (\sigma'; e \square)[\kappa''] = \sigma'[e \kappa''] = \sigma''[\kappa'] = \kappa \)

Subcases (2) and (3) impossible \( e e' \neq f \text{ and } e e' \neq v \)

\[ \Box \]

**Lemma 1.11.** Suppose \( \sigma[e] = \kappa[f \ v] \) where \( f \) is a \( \lambda \)-abstraction and \( f v \mapsto_{\beta} e' \). Then \( \sigma \triangleright e \mapsto \_ \sigma' \triangleright e' \text{ and } \sigma'[e'] = \kappa[e'] \).

**Proof.** By Lemma 1.10, we need to consider the following three cases:

\( (1) \sigma \triangleright e \mapsto \_ \sigma' \triangleright \kappa'[f \ v] \text{ and } \sigma'[\kappa'] = \kappa \)

\[ \sigma \triangleright e \mapsto \_ \sigma' \triangleright \kappa'[f \ v] \]

where \( \sigma'[\kappa'] = \sigma''[\square] \) by Lemma 1.9

\[ \rightarrow \sigma''; \square v \triangleright f \]

\[ \rightarrow \sigma' \triangleright e' \]

\[ \sigma'[e'] = \sigma''[\square[e']] = \sigma''[\square][e'] = \sigma'[\kappa'][e'] = \kappa[e'] \]

by Proposition 1.8

We let \( \sigma'' = \sigma' \).

\( (2) \sigma = \sigma'; \square v \text{ and } e = f \text{ and } \sigma'[\square] = \kappa \)

\[ \sigma \triangleright e = \sigma'; \square v \triangleright f \]

\[ \rightarrow \sigma' \triangleright e' \]

\[ \sigma'[e'] = \sigma'[[\square][e']] = \sigma'[[\square]][e'] = \kappa[e'] \]

by Proposition 1.8

We let \( \sigma'' = \sigma' \).

\( (3) \sigma = \sigma'; f \square \text{ and } e = v \text{ and } \sigma'[\square] = \kappa \)

\[ \sigma \triangleright e = \sigma'; f \square \triangleright v \]

\[ \rightarrow \sigma' \triangleright e' \]

\[ \sigma'[e'] = \sigma'[[\square][e']] = \sigma'[[\square]][e'] = \kappa[e'] \]

by Proposition 1.8

We let \( \sigma'' = \sigma' \). \( \Box \)

**Corollary 1.12.** Suppose \( e_1 \mapsto e_2 \text{ and } \sigma[e] = e_1 \). Then there exist \( \sigma' \text{ and } e' \text{ such that } \sigma \triangleright e \mapsto \_ \sigma' \triangleright e' \text{ and } \sigma'[e'] = e_2 \).

We leave it to the reader to prove all results given below.

**Proposition 1.13.** Suppose \( e \mapsto v \text{ and } \sigma[e'] = e \). Then \( \sigma \triangleright e' \mapsto \_ \square \triangleright v \).

**Corollary 1.14.** If \( e \mapsto v \), then \( \square \triangleright e \mapsto \_ \square \triangleright v \).

**Proposition 1.15.**

If \( \sigma \triangleright e \mapsto \_ \sigma' \triangleright e' \), then \( \sigma[e] \mapsto \sigma'[e'] \).

If \( \sigma \triangleright e \mapsto \_ \sigma' \triangleright v' \), then \( \sigma[e] \mapsto \sigma'[v'] \).

**Corollary 1.16.**

If \( \sigma \triangleright e \mapsto \_ \sigma' \triangleright e' \), then \( \sigma[e] \mapsto \sigma'[e'] \).

If \( \sigma \triangleright e \mapsto \_ \sigma' \triangleright v' \), then \( \sigma[e] \mapsto \sigma'[v'] \).

**Corollary 1.17.** If \( \square \triangleright e \mapsto \_ \square \triangleright v \), then \( e \mapsto v \).

Corollaries 1.12 and 1.17 prove Theorem 1.6
1.5 Safety of the abstract machine $C$

The safety of the abstract machine $C$ is proven independently of its correctness. We use two judgments to describe the state of $C$ with three inference rules given below:

- $s$ okay means that $s$ is an “okay” state. That is, $C$ is ready to analyze a given expression.
- $s$ stop means that $s$ is a “stop” state. That is, $C$ has finished reducing a given expression.

\[
\begin{align*}
\frac{\sigma[\emptyset] : A \Rightarrow C ~ \vdash e : A}{\sigma \triangleright e \ stackrel{\text{Okay}}{\Rightarrow} s} \quad \frac{\sigma[\emptyset] : A \Rightarrow C ~ \vdash v : A}{\sigma \triangleright v \ stackrel{\text{Okay}}{\Rightarrow} s} \\
\sigma \triangleright v \ stackrel{\text{Stop}}{\Rightarrow} s
\end{align*}
\]

The first clause in the following theorem may be thought of as the progress property of the abstract machine $C$; the second clause may be thought of as the “state” preservation property.

**Theorem 1.18 (Safety of the abstract machine $C$).**

If $s$ okay, then either $s$ stop or there exists $s'$ such that $s \mapsto_C s'$.

If $s$ okay and $s \mapsto_C s'$, then $s'$ okay.

1.6 Exercises

**Exercise 1.19.** Prove Theorems 1.2 and 1.3.

**Exercise 1.20.** Consider the simply typed $\lambda$-calculus extended with product types, sum types, and the fixed point construct.

\[
\begin{align*}
\text{expression} \quad e & ::= \ x \mid \lambda x : A. e \mid e \ e \mid (e, e) \mid \text{fst} e \mid \text{snd} e \mid () \\
& \mid \text{inl}_A e \mid \text{inr}_A e \mid \text{case} \ e \ \text{of} \ \text{inl} x. e \mid \text{inr} x. e \mid \text{fix} x : A. e \\
& \mid \text{true} \mid \text{false} \mid \text{if} \ e \ \text{then} \ e \ \text{else} \ e
\end{align*}
\]

\[
\begin{align*}
\text{value} \quad v & ::= \ \lambda x : A. e \mid (v, v) \mid () \mid \text{inl}_A v \mid \text{inr}_A v \mid \text{true} \mid \text{false}
\end{align*}
\]

Assuming the call-by-value strategy, extend the definition of frames and give additional rules for the reduction judgment $s \mapsto_C s'$ for the abstract machine $C$. See Figure 1.5 for an answer.

**Exercise 1.21.** Prove Theorem 1.18.
Figure 1.5: Abstract machine C for product types, sum types, and the fixed point construct