Chapter 1

Extensions to the simply typed \(\lambda\)-calculus

This chapter presents three extensions to the simply typed \(\lambda\)-calculus: product types, sum types, and the fixed point construct. Product types account for pairs, tuples, records, and units in SML. Sum types are sometimes (no pun intended!) called disjoint unions and can be thought of as special cases of datatypes in SML. Like the fixed point combinator for the untyped \(\lambda\)-calculus, the fixed point construct enables us to encode recursive functions in the simply typed \(\lambda\)-calculus. Unlike the fixed point combinator, however, it is not syntactic sugar: it cannot be written as another expression and its addition strictly increases the expressive power of the simply typed \(\lambda\)-calculus.

1.1 Product types

The idea behind product types is that a value of a product type \(A_1 \times A_2\) contains a value of type \(A_1\) and also a value of type \(A_2\). In order to create an expression of type \(A_1 \times A_2\), therefore, we need two expressions: one of type \(A_1\) and another of type \(A_2\); we use a pair \((e_1, e_2)\) to pair up two expressions \(e_1\) and \(e_2\). Conversely, given an expression of type \(A_1 \times A_2\), we may need to extract its individual components. We use projections \(\text{fst}\ e\) and \(\text{snd}\ e\) to retrieve the first and the second component of \(e\), respectively.

\[
\text{type} \quad A ::= \cdots | A \times A
\]
\[
\text{expression} \quad e ::= \cdots | (e, e) | \text{fst}\ e | \text{snd}\ e
\]

As with function types, a typing rule for product types is either an introduction rule or an elimination rule. Since there are two kinds of projections, we need two elimination rules (\(\times E_1\) and \(\times E_2\)):

\[
\begin{array}{c}
\Gamma \vdash e_1 : A_1 \\
\Gamma \vdash e_2 : A_2
\end{array}
\quad\Rightarrow
\begin{array}{c}
\Gamma \vdash (e_1, e_2) : A_1 \times A_2
\end{array}
\]
\[
\begin{array}{c}
\Gamma \vdash e : A_1 \times A_2
\end{array}
\quad\Rightarrow
\begin{array}{c}
\Gamma \vdash \text{fst}\ e : A_1
\end{array}
\]
\[
\begin{array}{c}
\Gamma \vdash e : A_1 \times A_2
\end{array}
\quad\Rightarrow
\begin{array}{c}
\Gamma \vdash \text{snd}\ e : A_2
\end{array}
\]

As for reduction rules, there are two alternative strategies which differ in the definition of values of product types (just like there are two reduction strategies for function types). If we take an eager approach, we do not regard \((e_1, e_2)\) as a value; only if both \(e_1\) and \(e_2\) are values do we regard it as a value, as stated in the following definition of values:

\[
\text{value} \quad v ::= \cdots | (v, v)
\]

Here the ellipsis \(\cdots\) denotes the previous definition of values which is irrelevant to the present discussion of product types. Then the eager reduction strategy is specified by the following reduction rules:
we give the specification of the eager reduction strategy; the lazy reduction strategy is left as an exercise.

\[
\begin{align*}
& e_1 \mapsto e'_1 \\
& (e_1, e_2) \mapsto (e'_1, e'_2) \\
& e \mapsto e'
\end{align*}
\]

\[
\begin{align*}
& \text{Fst} \quad \text{fst} \ e \mapsto \text{fst} \ e' \\
& \text{snd} \quad \text{snd} \ e \mapsto \text{snd} \ e' \\
& \text{Fst}' \quad \text{fst} \ (v_1, v_2) \mapsto v_1 \\
& \text{snd}' \quad \text{snd} \ (v_1, v_2) \mapsto v_2
\end{align*}
\]

Alternatively we may take a lazy approach which regards \((e_1, e_2)\) as a value:

\[
\text{value} \quad v \ ::= \ \cdots \ | \ (e, e)
\]

The lazy reduction strategy reduces \((e_1, e_2)\) "lazily" in that it postpones the reduction of \(e_1\) and \(e_2\) until the result is explicitly requested. It is specified by the following reduction rules:

\[
\begin{align*}
& e \mapsto e' \\
& \text{Fst} \quad \text{fst} \ e \mapsto \text{fst} \ e' \\
& \text{snd} \quad \text{snd} \ e \mapsto \text{snd} \ e'
\end{align*}
\]

Exercise 1.1. Why is it a bad idea to reduce \(\text{fst} \ (e_1, e_2)\) to \(e_1\) (and similarly for \(\text{snd} \ (e_1, e_2)\)) under the eager reduction strategy?

In order to incorporate these reduction rules into the operational semantics, we extend the definition of \(FV(e)\) and \([e'/x]e\) accordingly:

\[
\begin{align*}
& FV((e_1, e_2)) = FV(e_1) \cup FV(e_2) \\
& FV(\text{fst} \ e) = FV(e) \\ & FV(\text{snd} \ e) = FV(e)
\end{align*}
\]

\[
\begin{align*}
& [e'/x](e_1, e_2) = ([e'/x]e_1, [e'/x]e_2) \\
& \text{fst} \ [e'/x]e = \text{fst} \ [e'/x]e \\
& \text{snd} \ [e'/x]e = \text{snd} \ [e'/x]e
\end{align*}
\]

1.2 General product types and unit type

Product types are easily generalized to \(n\)-ary cases \(A_1 \times A_2 \times \cdots \times A_n\). A tuple \((e_1, e_2, \cdots, e_n)\) has a general product type \(A_1 \times A_2 \times \cdots \times A_n\) if \(e_i\) has type \(A_i\) for \(1 \leq i \leq n\). A projection \(\text{proj}_i \ e\) now uses an index \(i\) to indicate which component to retrieve from \(e\).

\[
\begin{align*}
\text{type} & \quad A ::= \cdots \mid A_1 \times A_2 \times \cdots \times A_n \\
\text{expression} & \quad e ::= \cdots \mid (e_1, e_2, \cdots, e_n) \mid \text{proj}_i \ e
\end{align*}
\]

As in binary cases, eager and lazy reduction strategies are available for general product types. Below we give the specification of the eager reduction strategy; the lazy reduction strategy is left as an exercise.

\[
\begin{align*}
& \text{value} \quad v ::= \cdots \mid (v_1, v_2, \cdots, v_n)
\end{align*}
\]

\[
\begin{align*}
& e_i \mapsto e'_i \\
& (v_1, v_2, \cdots, v_{i-1}, e_i, \cdots, e_n) \mapsto (v_1, v_2, \cdots, v_{i-1}, e'_i, \cdots, e_n) \\
& \text{proj}_i \ e \mapsto \text{proj}_i \ e' \\
& 1 \leq i \leq n
\end{align*}
\]

Of particular importance is the special case \(n = 0\) in a general product type \(A_1 \times A_2 \times \cdots \times A_n\). To better understand the ramifications of setting \(n\) to \(0\), let us interpret the rules \(\times 1\) and \(\times E_i\) as follows:
• The rule \( \times 1 \) says that in order to build a value of type \( A_1 \times A_2 \times \cdots \times A_n \), we have to provide \( n \) different values of types \( A_1 \) through \( A_n \) in the premise.

• The rule \( \times E \), says that since we have already provided \( n \) different values of types \( A_1 \) through \( A_n \), we may retrieve any of these values individually in the conclusion.

Now let us see what happens when we set \( n \) to 0:

• In order to build a value of type \( A_1 \times A_2 \times \cdots \times A_0 \), we have to provide 0 different values. That is, we do not have to provide any value in the premise at all!

• Since we have provided 0 different values, we cannot retrieve any value in the conclusion at all. That is, the rule \( \times E \) never applies if \( n = 0 \! \right)

The type unit is a general product type \( A_1 \times A_2 \times \cdots \times A_n \) with \( n = 0 \). It has an introduction rule with no premise (because we do not have to provide any value), but has no elimination rule (because there is no way to retrieve a value after providing no value). An expression \( () \) is called a unit and is the only value belonging to type unit. The typing rule unit below is the introduction rule for unit:

\[
\begin{align*}
\text{type} & : \quad A \ ::= \ \cdots \ | \ \text{unit} \\
\text{expression} & : \quad e \ ::= \ \cdots \ | \ () \\
\text{value} & : \quad v \ ::= \ \cdots \ | \ ()
\end{align*}
\]

\[\Gamma \vdash () : \text{unit} \]

The type unit is useful when we introduce computational effects such as input/output and mutable references. For example, a function returning a character typed by the user does not need an argument of particular meaning. Hence it may use unit as the type of its arguments.

### 1.3 Sum types

The idea behind sum types is that a value of a sum type \( A_1 + A_2 \) contains a value of type \( A_1 \) or else a value of type \( A_2 \), but not both. Therefore there are two ways to create an expression of type \( A_1 + A_2 \): using an expression \( e_1 \) of type \( A_1 \) and using an expression \( e_2 \) of type \( A_2 \). In the first case, we use a left injection, or inleft for short, \( \text{inl}_{A_2} \; e_1 \); in the second case, we use a right injection, or inright for short, \( \text{inr}_{A_1} \; e_2 \).

Then how do we extract back a value from an expression of type \( A_1 + A_2 \)? In general, it is unknown which of the two types \( A_1 \) and \( A_2 \) has been used in creating a value of type \( A_1 + A_2 \). For example, in the body \( e \) of a \( \lambda \)-abstraction \( \lambda x : A_1 + A_2. \; e \), nothing is known about variable \( x \) except that its value can be created from a value of either type \( A_1 \) or type \( A_2 \). In order to examine the value associated with an expression of type \( A_1 + A_2 \), therefore, we have to provide for two possibilities: when a left injection has been used and when a right injection has been used. We use a case expression case \( e \) of \( \text{inl} \; x_1 \; e_1 \) \( \mid \; \text{inr} \; x_2 \; e_2 \) to perform a case analysis on expression \( e \) which must have a sum type \( A_1 + A_2 \). Informally speaking, if \( e \) has been created with a value \( v_1 \) of type \( A_1 \), the case expression takes the first branch, reducing \( e_1 \) after binding \( x_1 \) to \( v_1 \); otherwise it takes the second branch, reducing \( e_2 \) in an analogous way.

\[
\begin{align*}
\text{type} & : \quad A \ ::= \ \cdots \ | \ A + A \\
\text{expression} & : \quad e \ ::= \ \cdots \ | \ \text{inl}_A \; e \ | \ \text{inr}_A \; e \ | \ \text{case} \; e \; \text{of} \; \text{inl} \; x \; e \ | \ \text{inr} \; x \; e
\end{align*}
\]

As is the case with function types and product types, a typing rule for sum types is either an introduction rule or an elimination rule. Since there are two ways to create an expression of type \( A_1 + A_2 \), there are two introduction rules \( (+L \; \text{for inl}_A \; e \; \text{and} \; +R \; \text{for inr}_A \; e) \):

May 15, 2007
Then the eager reduction strategy is specified by the following reduction rules:

\[
\begin{align*}
\Gamma \vdash e : A_1 & \quad \Gamma \vdash \text{inl}_A e : A_1 + A_2 \\ +L & \quad \Gamma \vdash \text{inr}_A e : A_1 + A_2 \\ +R & \quad \Gamma \vdash \text{case} e \text{ of } \text{inl} x_1, e_1 \mid \text{inr} x_2, e_2 : C \\
\end{align*}
\]

In the rule +E, expressions \( e_1 \) and \( e_2 \) must have the same type; otherwise we cannot statically determine the type of the whole case expression.

As with product types, reduction rules for sum types depend on the definition of values of sum types. An eager approach uses the following definition of values:

\[
\text{value } v ::= \cdots \mid \text{inl}_A v \mid \text{inr}_A v
\]

Then the eager reduction strategy is specified by the following reduction rules:

\[
\begin{align*}
\text{inl}_A e & \mapsto \text{inl}_A e' \quad \text{Inl} \\
\text{inr}_A e & \mapsto \text{inr}_A e' \quad \text{Inr}
\end{align*}
\]

\[
\begin{align*}
\text{case } e & \text{ of } \text{inl} x_1, e_1 \mid \text{inr} x_2, e_2 \mapsto \text{case } e' \text{ of } \text{inl} x_1, e_1 \mid \text{inr} x_2, e_2 \quad \text{Case}\' \\
\text{case } \text{inl}_A v & \text{ of } \text{inl} x_1, e_1 \mid \text{inr} x_2, e_2 \mapsto \text{[v/x]e}_1 \quad \text{Case}\'\prime \\
\text{case } \text{inr}_A v & \text{ of } \text{inl} x_1, e_1 \mid \text{inr} x_2, e_2 \mapsto \text{[v/x]e}_2 \quad \text{Case}\''
\end{align*}
\]

A lazy approach regards \( \text{inl}_A e \) and \( \text{inr}_A e \) as values regardless of the form of expression \( e \):

\[
\text{value } v ::= \cdots \mid \text{inl}_A e \mid \text{inr}_A e
\]

Then the lazy reduction strategy is specified by the following reduction rules:

\[
\begin{align*}
\text{case } e & \text{ of } \text{inl} x_1, e_1 \mid \text{inr} x_2, e_2 \mapsto \text{case } e' \text{ of } \text{inl} x_1, e_1 \mid \text{inr} x_2, e_2 \quad \text{Case} \\
\text{case } \text{inl}_A e & \text{ of } \text{inl} x_1, e_1 \mid \text{inr} x_2, e_2 \mapsto \text{[e/x]e}_1 \quad \text{Case}' \\
\text{case } \text{inr}_A e & \text{ of } \text{inl} x_1, e_1 \mid \text{inr} x_2, e_2 \mapsto \text{[e/x]e}_2 \quad \text{Case}''
\end{align*}
\]

In extending the definition of \( FV(e) \) and \( [e'/x]e \) for sum types, we have to be careful about case expressions. Intuitively \( x_1 \) and \( x_2 \) in case \( e \) of \( \text{inl} x_1, e_1 \mid \text{inr} x_2, e_2 \) are bound variables, just like \( x \) in \( \lambda x : A. e \) is a bound variable. Thus \( x_1 \) and \( x_2 \) are not free variables in case \( e \) of \( \text{inl} x_1, e_1 \mid \text{inr} x_2, e_2 \), and may have to be renamed to avoid variable captures in a substitution \( [e'/x]e \) case \( e \) of \( \text{inl} x_1, e_1 \mid \text{inr} x_2, e_2 \).

\[
\begin{align*}
FV(\text{inl}_A e) &= FV(e) \\
FV(\text{inr}_A e) &= FV(e) \\
FV(\text{case } e \text{ of } \text{inl} x_1, e_1 \mid \text{inr} x_2, e_2) &= FV(e) \cup (FV(e_1) - \{x_1\}) \cup (FV(e_2) - \{x_2\}) \\
[e'/x]FV(\text{inl}_A e) &= \text{inl}_A [e'/x]e \\
[e'/x]FV(\text{inr}_A e) &= \text{inr}_A [e'/x]e \\
[e'/x]\text{case } e \text{ of } \text{inl} x_1, e_1 \mid \text{inr} x_2, e_2 &= \text{case } [e'/x]e \text{ of } \text{inl} x_1, [e'/x]e_1 \mid \text{inr} x_2, [e'/x]e_2 \\
\text{if } x \neq x_1, x \notin FV(e') \\
\end{align*}
\]

As an example of using sum types, let us encode the type bool. The inherent capability of a boolean value is to choose one of two different options, as mentioned in Section 7. Hence a sum type unit + unit is sufficient for encoding the type bool because the left unit corresponds to the first option and the right
unit to the second option. Then true, false, and if \( e \) then \( e_1 \) else \( e_2 \) are encoded as follows, where \( x_1 \) and \( x_2 \) are dummy variables of no significance:

\[
\begin{align*}
\text{true} &\equiv \text{inl}_\text{unit}() \\
\text{false} &\equiv \text{inr}_\text{unit}() \\
\text{if } e \text{ then } e_1 \text{ else } e_2 &\equiv \text{case } e \text{ of } \text{inl} \ x_1, e_1 | \text{inr} \ x_2, e_2
\end{align*}
\]

Sum types are easily generalized to \( n \)-ary cases \( A_1 + A_2 + \cdots + A_n \). Here we discuss the special case \( n = 0 \).

Consider a general sum type \( A = A_1 + A_2 + \cdots + A_n \). We have \( n \) different ways of creating a value of type \( A \): by providing a value of type \( A_1 \), a value of type \( A_2 \), \ldots, and a value of type \( A_n \). Now what happens if \( n = 0 \)? We have 0 different ways of creating a value of type \( A \), which is tantamount to saying that there is no way to create a value of type \( A \). Therefore it is impossible to create a value of type \( A \).

Next suppose that an expression \( e \) has type \( A = A_1 + A_2 + \cdots + A_n \). In order to examine the value associated with \( e \) and obtain an expression of another type \( C \), we have to consider \( n \) different possibilities. (See the rule +E for the case \( n = 2 \)) Now what happens if \( n = 0 \)? We have to consider 0 different possibilities, which is tantamount to saying that we do not have to consider anything at all. Therefore we can obtain an expression of an arbitrary type \( C \) for free!

The type \( \text{void} \) is a general sum type \( A_1 + A_2 + \cdots + A_n \) with \( n = 0 \). It has no introduction rule because a value of type \( \text{void} \) is impossible to create. Consequently there is no value belonging to type \( \text{void} \). The typing rule \text{Abort} below is the elimination rule for \( \text{void} \); \text{abort}_A \ e \ is called an \text{abort} expression.

\[
\begin{array}{c}
type \quad A ::= \cdots | \text{void} \\
expression \quad e ::= \cdots | \text{abort}_A \ e
\end{array}
\]

\[
\frac{\Gamma \vdash e : \text{void}}{\Gamma \vdash \text{Abort}_{\text{C}} e : C} \text{ Abort}
\]

There is no reduction rule for an abort expression \( \text{abort}_A \ e \): if we keep reducing expression \( e \), we will eventually obtain a value of type \( \text{void} \), which must never happen because there is no value of type \( \text{void} \). So we stop!

The rule \text{Abort} may be a bit disquieting because its premise appears to contradict the fact that there is no value of type \( \text{void} \). That is, if there is no value of type \( \text{void} \), how can we possibly create an expression of type \( \text{void} \)? The answer is that we can never create a value of type \( \text{void} \), but we may still “assume” that there is a value of type \( \text{void} \). For example, \( \lambda x : \text{void} . \text{abort}_x x \) is a well-typed expression of type \( \text{void} \rightarrow A \) in which we “assume” that variable \( x \) has type \( \text{void} \). In essence, there is nothing wrong with making an assumption that something impossible has actually happened.

### 1.4 Fixed point construct

In the untyped \( \lambda \)-calculus, the fixed point combinator is syntactic sugar which is just a particular expression. We may hope, then, that encoding recursive functions in the simply typed \( \lambda \)-calculus boils down to finding a type for the fixed point combinator from the untyped \( \lambda \)-calculus. Unfortunately the fixed point combinator is untypable in the sense that we cannot assign a type to it by annotating all bound variables in it with suitable types. Thus the fixed point combinator cannot be an expression in the simply typed \( \lambda \)-calculus.

It is not difficult to see why the fixed point combinator is untypable. Consider the fixed point combinator for the call-by-value strategy in the untyped \( \lambda \)-calculus:

\[
\lambda F . (\lambda f : A. F (\lambda x. f f x)) (\lambda f : A. F (\lambda x. f f x))
\]

Let us assign a type \( A \) to variable \( f \):

\[
\lambda F . (\lambda f : A. F (\lambda x. f f x)) (\lambda f : A. F (\lambda x. f f x))
\]
Since \( f \) in \( f f x \) is applied to \( f \) itself which is an expression of type \( A \), it must have a type \( A \to B \) for some type \( B \). Since \( f \) can have only a single unique type, \( A \) and \( A \to B \) must be identical, which is impossible.

Thus we are led to introduce a fixed point construct \( \text{fix} \, x : A. e \) as a primitive construct (as opposed to syntactic sugar) which cannot be rewritten as an existing expression in the simply typed \( \lambda \)-calculus:

\[
\begin{align*}
\text{expression} & \quad e \ ::= \quad \cdots \mid \text{fix} \, x : A. e \\
\text{fix} \, x : A. e \text{ is intended to find a fixed point of a } \lambda \text{-abstraction } \lambda x : A. e. \text{ The typing rule } \text{Fix} \text{ states that a fixed point is defined on a function of type } A \to A \text{ only, in which case it has also type } A:
\end{align*}
\]

Since \( \text{fix} \, x : A. e \) is intended as a fixed point of a \( \lambda \)-abstraction \( \lambda x : A. e \), the definition of fixed point justifies the following (informal) equation:

\[
\text{fix} \, x : A. e = (\lambda x : A. e) \, \text{fix} \, x : A. e
\]

As \((\lambda x : A. e) \, \text{fix} \, x : A. e\) reduces to \([\text{fix} \, x : A. e/x]e\) by the \( \beta \)-reduction, we obtain the following reduction rule for the fixed point construct:

\[
\text{fix} \, x : A. e \mapsto [\text{fix} \, x : A. e/x]e \quad \text{Fix}
\]

In extending the definition of \( \text{FV}(e) \) and \([e'/x]e\), we take into account the fact that \( y \) in \( \text{fix} \, y : A. e \) is a bound variable:

\[
\begin{align*}
\text{FV}(\text{fix} \, x : A. e) &= \text{FV}(e) - \{x\} \\
[\text{e'}/x]\text{fix} \, y : A. e &= \text{fix} \, y : A. [\text{e'}/x]e \quad \text{if } x \neq y, y \notin \text{FV}(e')
\end{align*}
\]

In the case of the call-by-name strategy, the rule \( \text{Fix} \) poses no particular problem. In the case of the call-by-value strategy, however, a reduction by the rule \( \text{Fix} \) may fall into an infinite loop because \([\text{fix} \, x : A. e/x]e\) needs to be further reduced unless \( e \) is already a value:

\[
\text{fix} \, x : A. e \mapsto [\text{fix} \, x : A. e/x]e \mapsto \cdots
\]

For this reason, a typical functional language based on the call-by-value strategy requires that \( e \) in \( \text{fix} \, x : A. e \) be a \( \lambda \)-abstraction (among all those values including integers, booleans, \( \lambda \)-abstractions, and so on). Hence it allows the fixed point construct of the form \( \text{fix} \, f : A \to B. \, \lambda x : A. e \) only, which implies that it uses the fixed point construct only to define recursive functions. For example, \( \text{fix} \, f : A \to B. \, \lambda x : A. e \) may be thought of as a recursive function \( f \) of type \( A \to B \) whose formal argument is \( x \) and whose body is \( e \). Note that its reduction immediately returns a value:

\[
\text{fix} \, f : A \to B. \, \lambda x : A. e \mapsto \lambda x : A. \, [\text{fix} \, f : A \to B. \, \lambda x : A. e/f]e
\]

One important question remains unanswered: how do we encode mutually recursive functions? For example, how do we encode two mutually recursive functions \( f_1 \) of type \( A_1 \to B_1 \) and \( f_2 \) of type \( A_2 \to B_2 \)? The trick is to find a fixed point of a product type \((A_1 \to B_1) \times (A_2 \to B_2)\):

\[
\text{fix} \, f_{12} : (A_1 \to B_1) \times (A_2 \to B_2). (\lambda x_1 : A_1. e_1, \lambda x_2 : A_2. e_2)
\]

In expressions \( e_1 \) and \( e_2 \), we use \( \text{fst} \, f_{12} \) and \( \text{snd} \, f_{12} \) to refer to \( f_1 \) and \( f_2 \), respectively. To be precise, therefore, \( e \) in \( \text{fix} \, x : A. e \) can be not only a \( \lambda \)-abstraction but also a pair/tuple of \( \lambda \)-abstractions.
Theorem 1.3 (Type preservation).

Theorem 1.2 (Progress).

calculus:

There is no expression of type \((A \rightarrow A) \rightarrow A\) because Pierce's Law. Note that it is not Pierce's Law!

May 15, 2007 7

1.5 Type inhabitation

We say that a type \(A\) is inhabited if there exists an expression of type \(A\). For example, the function type \(A \rightarrow A\) is inhabited for any type \(A\) because \(\lambda x. A\) is an example of such an expression. Interestingly not every type is inhabited in the simply typed \(\lambda\)-calculus without the fixed point construct. For example, there is no expression of type \((A \rightarrow B) \rightarrow A\). Consequently, in order to use an expression of type \((A \Rightarrow B) \Rightarrow A\), we have to introduce it as a primitive construct which then strictly increases the expressive power of the simply typed \(\lambda\)-calculus. (callcc in Chapter ?? can be thought of such a primitive construct.)

The presence of the fixed point construct, however, completely defeats the purpose of introducing the concept of type inhabitation, since every type is now inhabited: \(\text{fix } x : A. x\) has type \(A\)! In this regard, the fixed point construct is not a welcome guest to type theory.

1.6 Type safety

This section proves type safety, i.e., progress and type preservation, of the extended simply typed \(\lambda\)-calculus:

Theorem 1.2 (Progress). If \(\Gamma \vdash e : A\) for some type \(A\), then either \(e\) is a value or there exists \(e'\) such that \(e \mapsto e'\).

Theorem 1.3 (Type preservation). If \(\Gamma \vdash e : A\) and \(e \mapsto e'\), then \(\Gamma \vdash e' : A\).

We assume the eager reduction strategy and do not consider general product types and general sum types. Figure 1.1 shows the typing rules and the reduction rules to be considered in the proof. Note that the extended simply typed \(\lambda\)-calculus does not include an abort expression \(\text{abort}_A e\) which destroys the progress property. (Why?)

The proof of progress extends the proof of Theorem ?? First we extend the canonical forms lemma (Lemma ??).
Lemma 1.4 (Canonical forms).

If \( v \) is a value of type \( A_1 \times A_2 \), then \( v \) is a pair \((v_1, v_2)\) of values.
If \( v \) is a value of type unit, then \( v \) is \( () \).
If \( v \) is a value of type \( A_1 + A_2 \), then \( v \) is either \( \text{inl}_{A_1} v' \) or \( \text{inr}_{A_1} v' \).
There is no value of type void.

Proof. By case analysis of \( v \).

Suppose that \( v \) is a value of type \( A_1 \times A_2 \). The only typing rule that assigns a product type \( A_1 \times A_2 \) to a value is the rule \( \times \). Therefore \( v \) must be a pair. Since \( v \) is a value, it must be a pair \((v_1, v_2)\) of values. Note that other typing rules may assign a product type, but never to a value.

Suppose that \( v \) is a value of type unit. The only typing rule that assigns type unit to a value is the rule Unit. Therefore \( v \) must be \( () \).

Suppose that \( v \) is a value of type \( A_1 + A_2 \). The only typing rules that assign a sum type \( A_1 \times A_2 \) to a value are the rules \(+_{L} \) and \(+_{R} \). Therefore \( v \) must be either \( \text{inl}_{A_1} e \) or \( \text{inr}_{A_1} e \). Since \( v \) is a value, it must be either \( \text{inl}_{A_1} v' \) or \( \text{inr}_{A_1} v' \).

There is no value of type void because there is no typing rule assigning type void to a value. \( \square \)

Proof of Theorem 1.2. By rule induction on the judgment \( \cdot \vdash e : A \). If \( e \) is already a value, we need no further consideration. Therefore we assume that \( e \) is not a value. Then there are eight cases to consider.

Case 1: \( \cdot \vdash e_1 : A_1 \quad \cdot \vdash e_2 : A_2 \quad \times 1 \) where \( e = (e_1, e_2) \) and \( A = A_1 \times A_2 \):

\( e_1 \) is a value or there exists \( e'_1 \) such that \( e_1 \rightarrow e'_1 \) by induction hypothesis on \( \cdot \vdash e_1 : A_1 \)
\( e_2 \) is a value or there exists \( e'_2 \) such that \( e_2 \rightarrow e'_2 \) by induction hypothesis on \( \cdot \vdash e_2 : A_2 \)

Both \( e_1 \) and \( e_2 \) cannot be values simultaneously because \( e = (e_1, e_2) \) is assumed not to be a value.

Subcase: \( e_1 \) is a value and there exists \( e'_2 \) such that \( e_2 \rightarrow e'_2 \) by the rule Pair.

We let \( e' = (e_1, e'_2) \).

Subcase: there exists \( e'_1 \) such that \( e_1 \rightarrow e'_1 \)
\( (e_1, e_2) \rightarrow (e'_1, e_2) \) by the rule Pair.

We let \( e' = (e'_1, e_2) \).

Case 2: \( \cdot \vdash e_0 : A_1 \times A_2 \quad \times E \) where \( e = \text{fst} e_0 \) and \( A = A_1 \):

\( e_0 \) is a value or there exists \( e'_0 \) such that \( e_0 \rightarrow e'_0 \) by induction hypothesis on \( \cdot \vdash e_0 : A_1 \times A_2 \)
\( e_0 \) cannot be a value because \( e = \text{fst} e_0 \) is assumed not to be a value.

\( \text{fst} e_0 \rightarrow \text{fst} e'_0 \) by the rule Fst.

We let \( e' = \text{fst} e'_0 \).

(The cases for the rules \( \times E_2, +_{L}, \) and \( +_{R} \) are all similar.)

Case 3: \( \cdot \vdash e_s : A_1 + A_2 \quad x_1 : A_1 \vdash e_1 : A \quad x_2 : A_2 \vdash e_2 : A \quad +E \) where \( e = \text{case } e_s \text{ of } \text{inl } x_1. e_1 \mid \text{inr } x_2. e_2 \):

\( e_s \) is a value or there exists \( e'_s \) such that \( e_s \rightarrow e'_s \) by induction hypothesis on \( \cdot \vdash e_s : A_1 + A_2 \)

Subcase: \( e_s \) is a value
\( e_s \rightarrow [v/x_1] e_1 \) or \( e_s \rightarrow [v/x_2] e_2 \)

We let \( e' = [v/x_1] e_1 \) or \( e' = [v/x_2] e_2 \).

Subcase: there exists \( e'_s \) such that \( e_s \rightarrow e'_s \)
\( \text{case } e_s \text{ of } \text{inl } x_1. e_1 \mid \text{inr } x_2. e_2 \rightarrow \text{case } e'_s \text{ of } \text{inl } x_1. e_1 \mid \text{inr } x_2. e_2 \)

We let \( e' = \text{case } e'_s \text{ of } \text{inl } x_1. e_1 \mid \text{inr } x_2. e_2 \).
Case $x : A \vdash e_0 : A$ Fix where $e = \text{fix } x : A. e_0$.

$\text{fix } x : A. e_0 \rightarrow [\text{fix } x : A. e_0/x]e_0$

We let $e' = [\text{fix } x : A. e_0/x]e_0$.

The proof of type preservation extends the proof of Theorem 3. First we extend the substitution lemma (Lemma 5) and the inversion lemma (Lemma 6).

**Lemma 1.5 (Substitution).** If $\Gamma \vdash e : A$ and $\Gamma, x : A \vdash e' : C$, then $\Gamma \vdash [e/x]e' : C$.

**Proof of Lemma 1.5.** By rule induction on the judgment $\Gamma, x : A \vdash e' : C$. The proof extends the proof of Lemma 5.

The case for the rule $\times 1$ is similar to the case for the rule $\rightarrow E$. The cases for the rules $\times E_1$, $\times E_2$, $\rightarrow L$, and $\Rightarrow$ are also similar to the case for the rule $\rightarrow E$ except that $e'$ contains only one smaller subexpression (e.g., $e' = \text{fst } e_0$). The case for the rule $\text{Fix}$ is similar to the case for the rule $\rightarrow l$.

\[ \Gamma, x : A \vdash e_0 : A_1 + A_2 \quad \Gamma, x : A, x_1 : A_1 \vdash e_1 : C \quad \Gamma, x : A, x_2 : A_2 \vdash e_2 : C \]  
\[ \Gamma, x : A \vdash \text{case } e_0 \text{ of inl } x_1, e_1 \mid \text{inr } x_2, e_2 : C \]  
\[ \text{where } e' = \text{case } e_0 \text{ of inl } x_1, e_1 \mid \text{inr } x_2, e_2 : C \]

Without loss of generality, we may assume $x_1 \neq x, x_1 \notin FV(e), x_2 \neq x$, and $x_2 \notin FV(e)$ because we can apply $\alpha$-conversions to $x_1$ and $x_2$ if necessary. This case is similar to the case for the rule $\rightarrow l$.

\[ \Gamma \vdash [e/x]e_0 : A_1 + A_2 \]  
by induction hypothesis on $\Gamma, x : A \vdash e_0 : A_1 + A_2$

\[ \Gamma, x_1 : A_1 \vdash [e/x]e_1 : C \]  
by induction hypothesis on $\Gamma, x : A, x_1 : A_1 \vdash e_1 : C$

\[ \Gamma, x_2 : A_2 \vdash [e/x]e_2 : C \]  
by induction hypothesis on $\Gamma, x : A, x_2 : A_2 \vdash e_2 : C$

\[ \Gamma \vdash \text{case } [e/x]e_0 \text{ of inl } x_1, [e/x]e_1 \mid \text{inr } x_2, [e/x]e_2 : C \]  
\[ \text{by the rule } + E \]

\[ \Gamma \vdash [e/x]\text{case } e_0 \text{ of inl } x_1, e_1 \mid \text{inr } x_2, e_2 : C \]  
\[ \text{from } x_1 \neq x, x_1 \notin FV(e), x_2 \neq x, x_2 \notin FV(e) \]

**Lemma 1.6 (Inversion).** Suppose $\Gamma \vdash e : C$.

If $e = (e_1, e_2)$, then $C = A_1 \times A_2$ and $\Gamma \vdash e_1 : A_1$ and $\Gamma \vdash e_2 : A_2$ for some types $A_1$ and $A_2$.

If $e = \text{fst } e'$, then $\Gamma \vdash e' : C \times A_2$ for some type $A_2$.

If $e = \text{snd } e'$, then $\Gamma \vdash e' : A_1 \times C$ for some type $A_1$.

If $e = ()$, then $C = \text{unit}$.

If $e = \text{inl } A_1 e'$, then $C = A_1 + A_2$ and $\Gamma \vdash e' : A_1$ for some type $A_1$.

If $e = \text{inr } A_1 e'$, then $C = A_1 + A_2$ and $\Gamma \vdash e' : A_2$ for some type $A_2$.

If $e = \text{case } e_0 \text{ of inl } x_1, e_1 \mid \text{inr } x_2, e_2$, then $\Gamma \vdash e_0 : A_1 + A_2$, $\Gamma, x_1 : A_1 \vdash e_1 : C$, and $\Gamma, x_2 : A_2 \vdash e_2 : C$ for some types $A_1$ and $A_2$.

If $e = \text{fix } x : A. e'$, then $C = A$ and $\Gamma, x : A \vdash e' : A$.

**Proof.** By the syntax-directedness of the type system.

The proof of Theorem 1.3 extends the proof of Theorem 5.

**Proof of Theorem 1.3.** By rule induction on the judgment $e \Rightarrow e'$. We consider two cases that use Lemma 1.5. All other cases use a simple pattern (as in the case for the rule Lam): apply Lemma 1.6 to $\Gamma \vdash e : A$, apply induction hypothesis, and apply a typing rule to deduce $\Gamma \vdash e' : A$.

Case $\text{case } \text{inl}_C v \text{ of inl } x_1, e_1 \mid \text{inr } x_2, e_2 \rightarrow [v/x_1]e_1$ Case $'$

\[ \Gamma \vdash \text{case } \text{inl}_C v \text{ of inl } x_1, e_1 \mid \text{inr } x_2, e_2 : A \]  
\[ \text{assumption} \]

\[ \Gamma \vdash \text{inl}_C v : A_1 + A_2 \]  
by Lemma 1.6

\[ \Gamma, x_1 : A_1 \vdash e_1 : A \]  
\[ \Gamma, x_2 : A_2 \vdash e_2 : A \text{ for some types } A_1 \text{ and } A_2 \]

\[ \Gamma \vdash [v/x_1]e_1 : A \]  
by applying Lemma 1.5 to $\Gamma \vdash v : A_1$ and $\Gamma, x_1 : A_1 \vdash e_1 : A$.

May 15, 2007
(The case for the rule $\text{Case''}$ is similar.)

$\text{Case } \text{fix}_{x:C. e_0} \mapsto [\text{fix}_{x:C. e_0/x}]e_0$ 

$\Gamma \vdash \text{fix}_{x:C. e_0 : A}$ 

$A = C$ and $\Gamma, x : C \vdash e_0 : C$ 

$\Gamma \vdash \text{fix}_{x:C. e_0 : C}$ 

$\Gamma \vdash [\text{fix}_{x:C. e_0/x}]e_0 : C$ 

by applying Lemma 1.5 to $\Gamma \vdash \text{fix}_{x:C. e_0 : A}$ and $\Gamma, x : C \vdash e_0 : C$ 

$\square$