A Structural Approach to Operational Semantics

Gordon D. Plotkin

Laboratory for Foundations of Computer Science, School of Informatics, University of Edinburgh, King's Buildings, Edinburgh EH9 3JZ, Scotland

Contents

Email address: `gdp@inf.ed.ac.uk` (Gordon D. Plotkin).

1 Transition Systems and Interpreting Automata

1.1 Introduction

It is the purpose of these notes to develop a simple and direct method for specifying the semantics of programming languages. Very little is required in the way of mathematical background; all that will be involved is "symbol-pushing" of one kind or another of the sort which will already be familiar to readers with experience of either the non-numerical aspects of programming languages or else formal deductive systems of the kind employed in mathematical logic.

Apart from a simple kind of mathematics the method is intended to produce concise comprehensible semantic definitions. Indeed the method is even intended as a direct formalisation of (many aspects of) the usual informal natural language descriptions. I should really confess here that while I have some experience what has been expressed above is rather a pious hope than a statement of fact. I would therefore be most grateful to readers for their comments and particularly their criticisms.

I will follow the approach to programming languages taken by such authors as Gordon [Gor] and Tennent [Ten] considering the main syntactic classes – expressions, commands and declarations – and the various features found in each. The linguistic approach is that developed by the Scott-Strachey school (together with Landin and McCarthy and others) but within an operational rather than a denotational framework. These notes should be considered as an attempt at showing the feasibility of such an approach. Apart from various inadequacies of the treatment as presented many topics of importance are omitted. These include data structures and data types; various forms of control structure from jumps to exceptions and coroutines; concurrency including semaphores, monitors and communicating process.

Many thanks are due to the Department of Computer Science at Aarhus University at whose invitation I was enabled to spend a very pleasant six months developing this material. These notes partially cover a series of lectures given at the department. I would like also to thank the staff and students whose advice and criticism had a strong influence and also Jette Milwertz whose typing skills made the work look better than it should.

1.2 Transition Systems

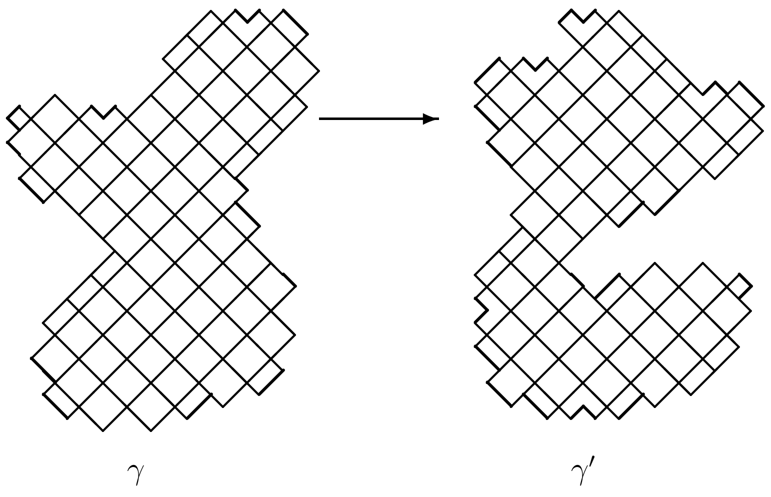
The announced "symbol-pushing" nature of our method suggests what is the truth; it is an *operational* method of specifying semantics based on *syntactic* transformations of programs and *simple* operations on discrete data. The idea is that in general one should be interested in computer *systems* whether hardware or software and for semantics one thinks of systems whose *configurations* are a mixture of syntactical objects – the programs and data – such as stores or environments. Thus in these notes we have

$$\text{SYSTEM} = \text{PROGRAM} + \text{DATA}$$

One wonders if this study could be generalised to other kinds of systems, especially hardware ones.

Clearly systems have some behaviour and it is that which we wish to describe. In an operational semantics one focuses on the operations the system can perform – whether internally or interactively with some supersystem or the outside world. For in our discrete (digital) computer systems behaviour consists of elementary steps which are occurrences of operations. Such elementary steps are called here, (and also in many other situations in Computer Science) *transitions* (= *moves*). Thus a transition steps from one configuration to another and as a first idea we take it to be a binary relation between configurations.

Definition 1 *A Transition System (ts) is (just!) a structure $\langle \Gamma, \longrightarrow \rangle$ where Γ is a set (of elements, γ, called configurations) and $\longrightarrow \subseteq \Gamma \times \Gamma$ is a binary relation (called the transition relation). Read $\gamma \longrightarrow \gamma'$ as saying that there is a transition from the configuration γ to the configuration γ'. (Other notations sometimes seen are $\vdash$, $\Rightarrow$ and $\rhd$).*



A Transition

Of course this idea is hardly new and examples can be found in any book on automata or formal languages. Its application to the definition of programming languages can be found in the work of Landin and the Vienna Group [Lan,Oll,Weg].

Structures of the form, $\langle \Gamma, \longrightarrow \rangle$ are rather simple and later we will consider several more elaborate variants, tailored to individual circumstances. For example it is often helpful to have an idea of *terminal* (= *final* = *halting*) configurations.

Definition 2 *A Terminal Transition System (tts) is a structure $\langle \Gamma, \longrightarrow, T \rangle$ where $\langle \Gamma, \longrightarrow \rangle$ is a ts, and $T \subseteq \Gamma$ (the set of final configurations) satisfies $\forall \gamma \in T\ \forall \gamma' \in \Gamma\, .\, \gamma \not\longrightarrow \gamma'$.*

A point to watch is to make a distinction between *internal* and *external* behaviour. Internally a system's behaviour is nothing but the sum of its transitions. (We ignore here the fact that often these transitions make sense only at a certain level; what counts as one transition for one purpose may in fact consist of many steps when viewed in more detail. Part of the spirit of our method is to choose steps of the appropriate "size".) However externally many of the transitions produce no detectable effect. It is a matter of experience to choose the right definition of external behaviour. Often two or more definitions of behaviour (or of having the same behaviour) are possible for a given transition system. Indeed on occasion one must turn the problem around and look for a transition system which makes it possible to obtain an expected notion of behaviour.

1.3 Examples of Transition Systems

We recall a few familiar and not so familiar examples from computability and formal languages.

1.3.1 Finite Automata

A *finite automaton* is a quintuplet $M = \langle Q, \Sigma, \delta, q_0, F \rangle$ where

- Q is a finite set (of *states*)
- Σ is a finite set (the *input* alphabet)
- $\delta : Q \times \Sigma \longrightarrow \mathcal{P}(Q)$ (is the *state transition relation*)
- $q_0 \in Q$ (is the *initial state*)
- $F \subseteq Q$ (is the set of *final states*)

To obtain a transition system we set

$$\Gamma = Q \times \Sigma^*$$

So any configuration, $\gamma = \langle q, w \rangle$ has a *state* component, q, and a *control* component, w, for data.

For the transitions we put whenever $q' \in \delta(q, a)$:

$$\langle q, aw \rangle \vdash \langle q', w \rangle$$

(More formally, $\vdash = \{\langle \langle q, aw \rangle, \langle q', w \rangle \rangle \mid q, q' \in Q, a \in \Sigma, w \in \Sigma^*, q' \in \delta(q, a)\}$).

The behaviour of a finite automaton is just the set $L(M)$ of strings it accepts:

$$L(M) = \{w \in \Sigma^* \mid \exists q \in F\ \langle q_0, w \rangle \vdash^* \langle q, \varepsilon \rangle\}$$

Of course we could also define the terminal configurations by:

$$T = \{\langle q, \varepsilon\rangle \mid q \in F\}$$

and then

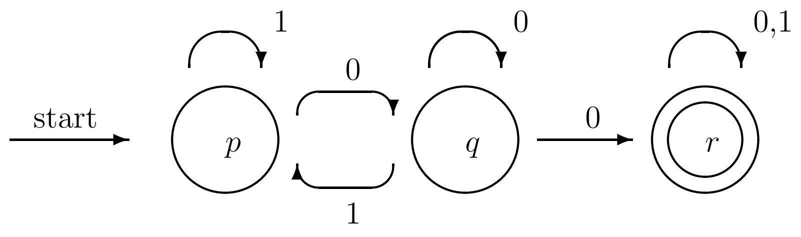
$$L(M) = \{w \in \Sigma^* \mid \exists \gamma \in T\ \langle q_0, w\rangle \vdash^* \gamma\}$$

In fact we can even get a little more abstract. Let $\langle \Gamma, \longrightarrow, T\rangle$ be a tts. An input function for it is any mapping in: $I \longrightarrow \Gamma$ and the *language* it accepts is then $L(\Gamma) \subseteq I$ where:

$$L(\Gamma) = \{i \in I \mid \exists \gamma \in T \,.\, \mathrm{in}(i) \longrightarrow^* \gamma\}$$

(For finite automata as above we take $I = \Sigma^*$, and $\mathrm{in}(w) = \langle q_0, w\rangle$). Thus we can easily formalise at least one general notion of behaviour.

Example 3 *The machine:*



A transition sequence:

$$\begin{aligned}
\langle p, 01001\rangle &\vdash \langle q, 1001\rangle \vdash \langle p, 001\rangle\\
&\vdash \langle q, 01\rangle \quad \vdash \langle r, 1\rangle\\
&\vdash \langle r, \varepsilon\rangle
\end{aligned}$$

1.3.2 Three Counter Machines

We have three counters, C, namely I, J and K. There are instructions, O, of the following four types:

- **Increment**: **inc** $C : m$
- **Decrement**: **dec** $C : m$
- **Zero Test**: **zero** $C : m/n$
- **Stop**: **stop**

Then *programs* are just sequences $P = O_1, \ldots, O_l$ of instructions. Now, fixing P, the set of *configurations* is:

$$\Gamma = \{\langle m, i, j, k\rangle \mid 1 \leq m \leq l;\ i, j, k \in \mathrm{N}\}$$

Then the transition relation is defined in terms of the various possibilities by:

- Case II: $O_m = \textbf{inc}\ \mathrm{I} : m'$

$$\langle m, i, j, k\rangle \vdash \langle m', i+1, j, k\rangle$$

- Case ID: $O_m = \textbf{dec}\ \mathrm{I} : m'$

$$\langle m, i+1, j, k\rangle \vdash \langle m', i, j, k\rangle$$

- Case IZ: $O_m = \textbf{zero}\ \mathrm{I} : m'/m''$

$$\begin{array}{l}\langle m, 0, j, k\rangle \vdash \langle m', 0, j, k\rangle \\ \langle m, i+1, j, k\rangle \vdash \langle m'', i+1, j, k\rangle\end{array}$$

and similarly for J and K.

Note 1 There is no case for the stop instruction.
Note 2 In case m' or m'' are 0 or $> k$ the above definitions do not (of course!) apply.
Note 3 The transition relation is *deterministic*, that is:

$$\forall \gamma, \gamma', \gamma'' \cdot \gamma \longrightarrow \gamma' \wedge \gamma \longrightarrow \gamma'' \Rightarrow \gamma' = \gamma''$$

or, diagrammatically:

$$\begin{tikzcd} & \gamma \arrow[dl] \arrow[dr] & \\ \gamma' \arrow[rr, equal] & & \gamma'' \end{tikzcd}$$

(*Exercise* – prove this).

Now the set of *terminal* configurations is defined by:

$$T = \{\langle m, 0, j, 0\rangle \mid O_m = \textbf{stop}\}$$

and the behaviour is a partial function $f : \mathrm{N} \underset{P}{\longrightarrow} \mathrm{N}$ where:

$$f(i) = j \quad \overset{def}{=} \quad \langle 1, i, 0, 0\rangle \longrightarrow^* \langle m, 0, j, 0\rangle \in T$$

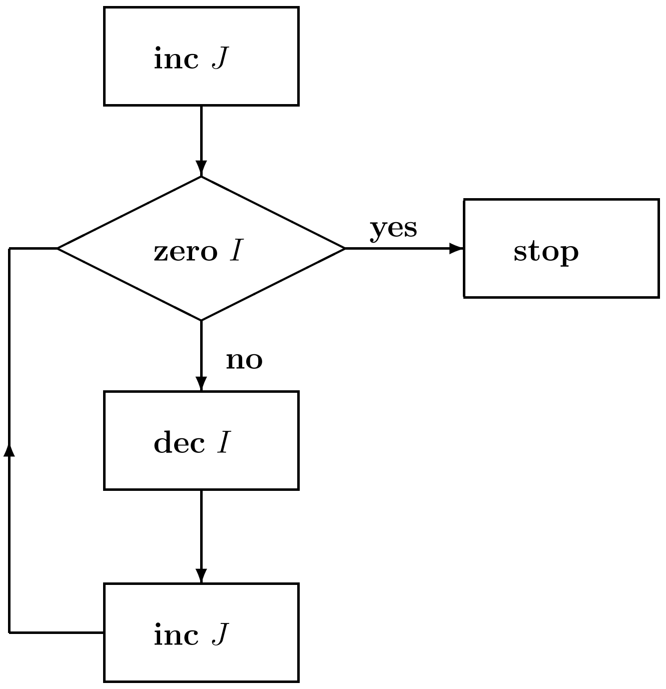
This can be put a little more abstractly, if we take for any tts $\langle \Gamma, \longrightarrow, T\rangle$ an *input* function, in : $I \longrightarrow \Gamma$ as before and also an *output* function, out : $T \longrightarrow O$ and define a partial function $f_\Gamma : I \underset{P}{\longrightarrow} O$ by

$$f_\Gamma(i) = o \quad \equiv \quad \exists \gamma\ \mathrm{in}(i) \longrightarrow^* \gamma \in T \wedge o = \mathrm{out}(\gamma)$$

Of course for this to make sense the tts must be *deterministic* (why?). In the case of a three-counter machine we have

$$\begin{cases} I = O = \mathrm{N} \\ \mathrm{in}(i) = \langle 1, i, 0, 0\rangle \\ \mathrm{out}(\langle m, i, j, k\rangle) = j \end{cases}$$

Example 4 *A program for the successor function,* $n \mapsto n + 1$



1.3.3 Context-Free Grammars

A *context-free grammar* is a quadruple, $G = \langle N, \Sigma, P, S\rangle$ where

- N is a finite set (of *non-terminals*)
- Σ is a finite set (the *input alphabet*)
- $P \subseteq N \times (N \cup \Sigma)^*$ (is the set of *productions*)
- $S \in N$ (is the *start symbol*)

Then the configurations are given by:

$$\Gamma = (N \cup \Sigma)^*$$

and the *transition relation* $\Rightarrow$ is given by:

$$wXv \Rightarrow wxv \qquad \text{(when } X \to x \text{ is in } P\text{)}$$

Now the *behaviour* is just

$$L(G) = \{w \mid S \Rightarrow^* w\}$$

Amusingly, this already does not fit into our abstract idea for behaviours as sets (the one which worked for finite automata). The problem is that was intended for *acceptance* where here we have to do with *generation* (by leftmost derivations).

Exercise: Write down an abstract model of generation.

Example 5 *The grammar is:*

$$\begin{array}{l} S \rightarrow \\ S \rightarrow (S) \\ S \rightarrow SS \end{array}$$

and a transition sequence could be

$$\begin{array}{l} S \Rightarrow SS \Rightarrow (S)S \Rightarrow ()S \Rightarrow ()(S) \\ \quad \Rightarrow ()(SS) \Rightarrow^2 ()(()S) \Rightarrow^2 ()(()()) \end{array}$$

1.3.4 Labelled Transition Systems

Transition systems in general do not give the opportunity of saying very much about any individual transition. By adding the possibility of such information we arrive at a definition.

Definition 6 *A Labelled Transition System (lts) is a structure $\langle \Gamma, A, \longrightarrow \rangle$ where Γ is a set (of configurations) and A is a set (of actions (= labels = operations)) and*

$$\longrightarrow \subseteq \Gamma \times A \times \Gamma$$

is the transition relation.

We write a transition as: $\gamma \xrightarrow{a} \gamma'$ where γ, γ' are configurations and a is an action. The idea is that an action can give information about what went on in the configuration during the transition (*internal* actions) or about the interaction between the system and its environment (external actions) (or both). The labels are particularly useful for specifying distributed systems where the actions may relate to the communications between sub-systems. The idea seems to originate with Keller [Kel].

The idea of *Labelled Terminal Transition Systems* $\langle \Gamma, A, \longrightarrow, T \rangle$ should be clear to the reader who will also expect the following generalisation of reflexive (resp. transitive) closure. For any lts let γ and γ' be configurations and take $x = a_1 \dots a_k$ in A^+ (resp. A^*) then:

$$\gamma \xrightarrow{x}^{+\,(\text{resp. } *)} \gamma' \quad \overset{def}{=} \quad \exists \gamma_1, \dots, \gamma_k.\ \gamma \xrightarrow{a_1} \gamma_1 \dots \xrightarrow{a_k} \gamma_k = \gamma'$$

where $k > 0$ (resp. $k \geq 0$).

Example 7 (Finite Automata (continued)) *This time define a tts by taking*

- $\Gamma = Q$
- $A = \Sigma$
- $q \xrightarrow{a} q' \equiv q' \in \delta(q, a)$
- $T = F$

Then we have $L(M) = \{w \in A^* \mid \exists q \in T.\ q_0 \xrightarrow{w}^* q\}$. *The example transition sequence given above now becomes simply:*

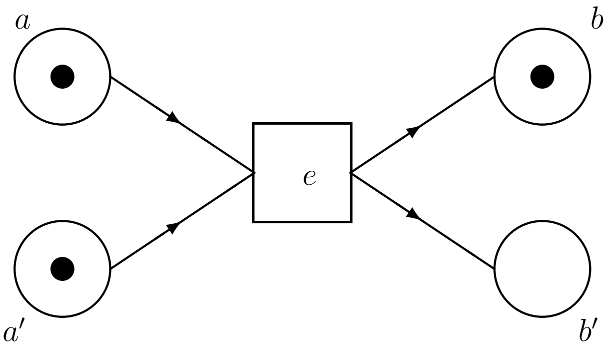
$$p \xrightarrow{0} q \xrightarrow{1} p \xrightarrow{0} q \xrightarrow{0} r \xrightarrow{1} r \in F$$

Example 8 (Petri Nets) *One idea of a Petri Net is just a quadruple* $N = \langle B, E, F, m \rangle$ *where*

- B *is a finite set (of conditions)*
- E *is a finite set (of events)*
- $F \subseteq (B \times E) \cup (E \times B)$ *(is the flow relation)*
- $m \subseteq B$ *(is the initial case)*

A configuration, m, is contact-free if

$$\neg \exists e \in E.\ (F^{-1}(e) \subseteq m \wedge F(e) \cap m \neq \emptyset)$$



A contact situation for $m = a, a', b$

The point of this definition is that the occurrence of an event, e, is nothing more than the ceasing-to-hold of its preconditions ($= F^{-1}(e)$) *and the starting-to-hold of its postconditions* ($= F(e)$) *in any given case. Here a case is a set of conditions (those that hold in the case). A* *contact-situation is one where this idea does not make sense. Often one excludes this possibility axiomatically (and imposes also other intuitively acceptable axioms). We will just (somewhat arbitrarily) regard them as "runtime errors" and take*

$$\Gamma = \{m \subseteq B \mid m \textit{ is contact-free}\}$$

If two different events share a precondition in a case, then according to the above intentions they cannot both occur at once. Accordingly we define a conflict relation between events by:

$$e \sharp e' \quad \equiv \quad (F^{-1}(e) \cap F^{-1}(e') \neq \emptyset \wedge e \neq e')$$

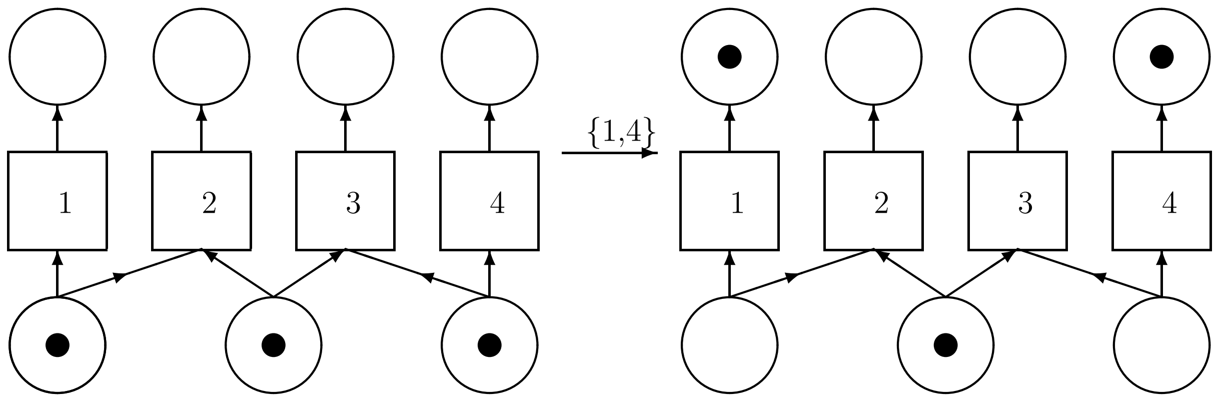
An event can occur from a given case if all its preconditions hold in the case. What is (much) more, Petri Nets model concurrency in that several events (not in conflict) can occur together in a given case. So we put

$$A = \{X \subseteq E \mid \neg \exists e, e' \in X.\ e \sharp e'\}$$

and define

$$m \xrightarrow{X} m' \quad \equiv \quad F^{-1}(X) \subseteq m \wedge m' = [m \backslash F^{-1}(X)] \cup F(X)$$

Here is a pictorial example of such a transition

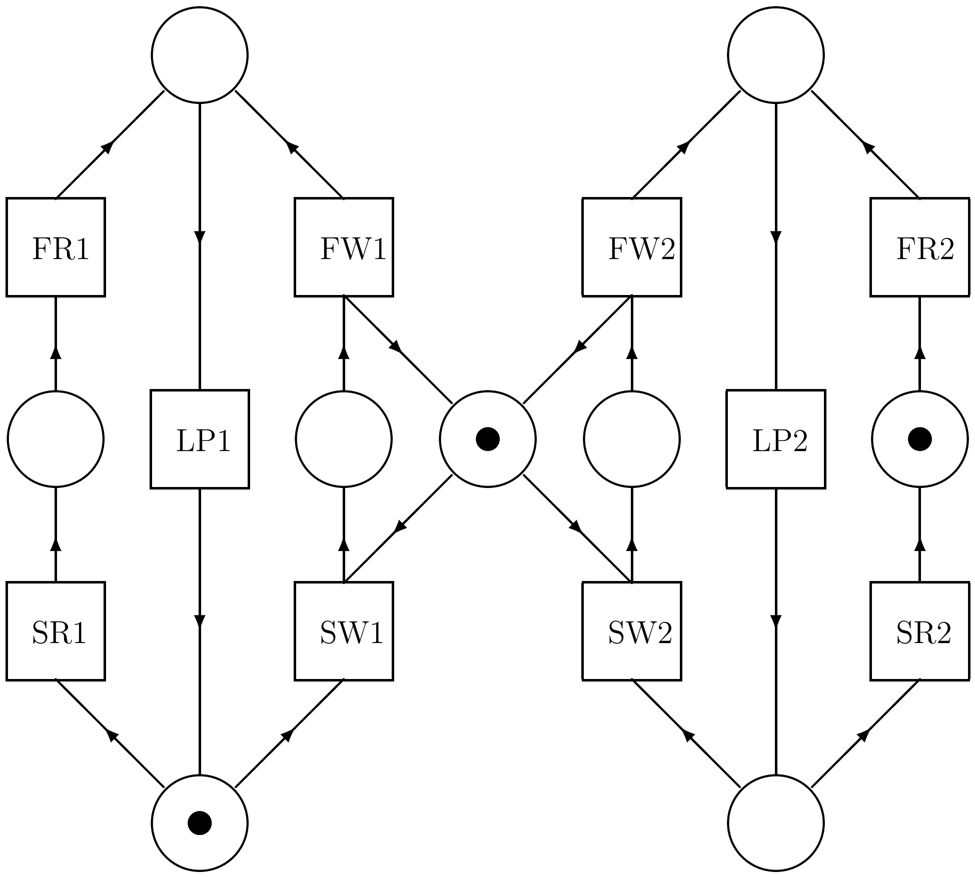


A Transition

We give no definition of behaviour as there does not seem to be any generally accepted one in the literature. For further information on Petri Nets see [Bra,Pet].

Of course our transitions with their actions must also be thought of as kinds of events; even more so when we are discussing the semantics of languages for concurrency. We believe there are very strong links between our ideas and those in Net Theory, but, alas, do not have time here to pursue them.

Example 9 (Readers and Writers) *This is a (partial) specification of a Readers and Writers problem with two agents each of whom can read and write (and do some local processing) but where the writes should not overlap.*



SWi	*is Start Writing*	i	
FWi	*is Finish Writing*	i	
SRi	*is Start Reading*	i	
FRi	*is Finish Reading*	i	
LRi	*is Local Processing*	i	*where* $1 \leq i \leq 2$

1.4 Interpreting Automata

To finish Chapter 1 we give an example of how to define the operational semantics of a language by an interpreting automaton. The reader should obtain some feeling for what is possible along these lines (see the references given above for more information), as well as a feeling that the method is somehow a little too indirect thus paving the way for the approach taken in the next chapter.

1.4.1 The Language L

We begin with the *Abstract Syntax* of a very simple programming language called L. What is abstract about it will be discussed a little here and later at greater length. For us syntax is a collection of syntactic sets of phrases; each set corresponds to a different type of phrase. Some of these sets are very simple and can be taken as given:

- Basic Syntactic Sets
  Truth-values This is the set $\mathrm{T} = \{\mathrm{tt}, \mathrm{ff}\}$ and is ranged over by (the metavariable) t (and we also happily employ for this (and any other) metavariable sub- and super-scripts to generate other metavariables: t', t_0, t'''_{1k}).
  Numbers m, n are the metavariables over $\mathrm{N} = \{0, 1, 2, \ldots\}$.
  Variables $v \in \mathrm{Var} = \{a, b, c, \ldots, z\}$
  Note how we have progressed to a fairly spare style of specification in the above.
- Derived Syntactic Sets
  Expressions $e \in \mathrm{Exp}$ given by

$$e ::= m \mid v \mid e + e' \mid e - e' \mid e * e'$$

  Boolean Expressions $b \in \mathrm{BExp}$ given by

$$b ::= t \mid e = e' \mid b \textbf{ or } b' \mid {\sim}b$$

  Commands $c \in \mathrm{Com}$ given by

$$c ::= \textbf{nil} \mid v := e \mid c; c' \mid \textbf{ if } b \textbf{ then } c \textbf{ else } c' \mid \textbf{while } b \textbf{ do } c$$

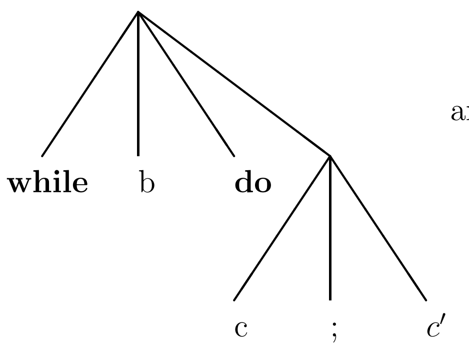
This specification can be taken, roughly speaking, as a context-free grammar if the reader just ignores the use of the infinite set N and the use of primes. It can also (despite appearances!) be taken as *unambiguous* if the reader just regards the author as having lazily omitted brackets as in:

$$b ::= t \mid e = e' \mid b \textbf{ or } b' \mid {\sim}b$$

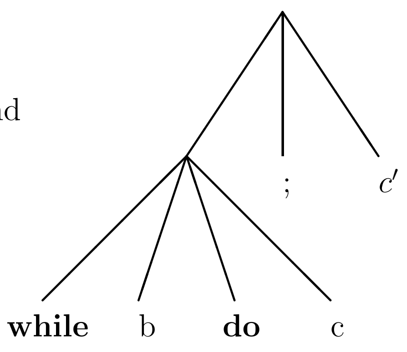
specifying parse trees so that rather than saying ambiguously that (for example):

$$\textbf{while } b \textbf{ do } c;\ c'$$

is a program what is being said is that both



and



are trees.

So we are abstract in not worrying about some lexical matters and just using for example integers rather than numerals and in not worrying about the exact specification of phrases. What we are really trying to do is abstract away from the problems of parsing the token strings that really came into the computer and considering instead the "deep structure" of programs. Thus the syntactic categories we choose are supposed to be those with *independent semantic significance*; the various program constructs – such as semicolon or **while** . . . **do** . . . – are the constructive operations on phrases that possess semantic significance.

For example contrast the following concrete syntax for (some of) our expressions (taken from [Ten]):

$$\begin{array}{lll}
\langle\text{expression}\rangle & ::= & \langle\text{term}\rangle \ \mid \ \langle\text{expression}\rangle\ \langle\text{addop}\rangle\ \langle\text{term}\rangle \\
\langle\text{term}\rangle & ::= & \langle\text{factor}\rangle \ \mid \ \langle\text{term}\rangle\ \langle\text{multop}\rangle\ \langle\text{factor}\rangle \\
\langle\text{factor}\rangle & ::= & \langle\text{variable}\rangle \ \mid \ \langle\text{literal}\rangle \ \mid \ (\langle\text{expression}\rangle) \\
\langle\text{addop}\rangle & ::= & + \mid - \\
\langle\text{multop}\rangle & ::= & * \\
\langle\text{variable}\rangle & ::= & a \mid b \mid c \mid \ldots \mid z \\
\langle\text{literal}\rangle & ::= & 0 \mid 1 \mid \ldots \mid 9
\end{array}$$

Now, however convenient it is for a parser to distinguish between ⟨expression⟩, ⟨term⟩ and ⟨factor⟩ it does not make much semantic sense!

Thus we will never give semantics directly to token strings but rather to their real structure. However, we can always obtain the semantics of token strings via *parsers* which we regard as essentially just maps:

$$\text{Parser: Concrete Syntax} \longrightarrow \text{Abstract Syntax}$$

Of course it is not really so well-defined what the abstract syntax for a given language is, and we shall clearly make good use of the freedom of choice available.

Returning to our language L we observe the following "dependency diagram":

$$\begin{tikzcd}
C \arrow[d] \arrow[dr] & \\
B \arrow[r] & E
\end{tikzcd}$$

1.4.2 The SMC-Machine

Now we define a suitable transition system whose configurations are those of the SMC-machine.

- Value Stacks is ranged over by S and is the set $(\mathrm{T} \cup \mathrm{N} \cup \mathrm{Var} \cup \mathrm{BExp} \cup \mathrm{Com})^*$
- Memories is ranged over by M and is $\mathrm{Var} \longrightarrow \mathrm{N}$
- Control Stacks is ranged over by C and is

$$(\mathrm{Com} \cup \mathrm{BExp} \cup \mathrm{Exp} \cup \{+, -, *, =, \mathbf{or}, \sim, :=, \mathbf{if}, \mathbf{while}\})^*$$

The set of configurations is

$$\Gamma = \text{Value Stacks} \times \text{Memories} \times \text{Control Stacks}$$

and so a typical configuration is $\gamma = \langle S, M, C \rangle$. The idea is that we *interpret* commands and produce as our interpretation proceeds, stacks C, of control information (initially a command but later bits of commands). Along the way we accumulate partial results (when evaluating expressions), and bits of command text which will be needed later; this is all put (for some reason) on the value stack, S. Finally we have a model of the *store* (= *memory*) as a function $M : \mathrm{Var} \longrightarrow \mathrm{N}$ which given a variable, v, says what its value $M(v)$ is in the store.

Notation: In order to discuss updating variables, we introduce for a memory, M, natural number, m, and variable v the memory $M' = M[m/v]$ where

$$M'(v') = \begin{cases} m & (\text{if } v' = v) \\ M(v') & (\text{otherwise}) \end{cases}$$

So $M[m/v]$ is the memory resulting from updating M by changing the value of v from $M(v)$ to m.

The *transition relation*, $\Rightarrow$, is defined by cases according to what is on the top of the control stack.

- Expressions

En	$\langle S, M, n\ C\rangle$	$\Rightarrow \langle n\ S, M, C\rangle$
Ev	$\langle S, M, v\ C\rangle$	$\Rightarrow \langle M(v)\ S, M, C\rangle$
$E\underset{*}{\overset{+}{-}}I$	$\langle S, M, e \underset{*}{\overset{+}{-}} e'\ C\rangle$	$\Rightarrow \langle S, M, e\ e'\ \underset{*}{\overset{+}{-}}\ C\rangle$
$E\underset{*}{\overset{+}{-}}E$	$\langle m'\ m\ S, M, \underset{*}{\overset{+}{-}}\ C\rangle$	$\Rightarrow \langle n\ S, M, C\rangle$
		(where $n = m \underset{*}{\overset{+}{-}} m'$)

Note 1 *The symbols $+$, $-$, $*$, are being used both as symbols of L and to stand for the functions addition, subtraction and multiplication.*

- Boolean Expressions

$B\ t$	$\langle S, M, t\ C\rangle$	$\Rightarrow \langle t\ S, M, C\rangle$
$B = I$	$\langle S, M, e = e'\ C\rangle$	$\Rightarrow \langle S, M, e\ e' = C\rangle$
$B = E$	$\langle m'\ m\ S, M, = C\rangle$	$\Rightarrow \langle t\ S, M, C\rangle$
		(where $t = (m = m')$)
B **or** I	$\langle S, M, b$ **or** $b'\ C\rangle$	$\Rightarrow \langle S, M, b\ b'$ **or** $C\rangle$
B **or** E	$\langle t'\ t\ S, M,$ **or** $C\rangle$	$\Rightarrow \langle t''\ S, M, C\rangle$
		(where $t'' = (t \vee t')$)
$B \sim I$	$\langle S, M, \sim b\ C\rangle$	$\Rightarrow \langle S, M, b \sim C\rangle$
$B \sim E$	$\langle t\ S, M, \sim C\rangle$	$\Rightarrow \langle t'\ S, M, C\rangle$
		(where $t' = \sim t$)

- Commands

C **nil**	$\langle S, M, \textbf{nil}\ C\rangle$	$\Rightarrow \langle S, M, C\rangle$
$C := I$	$\langle S, M, v := e\ C\rangle$	$\Rightarrow \langle v\ S, M, e := C\rangle$
$C := E$	$\langle m\ v\ S, M, := C\rangle$	$\Rightarrow \langle S, M[m/v], C\rangle$
$C;$	$\langle S, M, c; c'\ C\rangle$	$\Rightarrow \langle S, M, c\ c'\ C\rangle$
C **if** I	$\langle S, M, \textbf{if}\ b\ \textbf{then}\ c\ \textbf{else}\ c'\ C\rangle$	$\Rightarrow \langle c\ c'\ S, M, b\ \textbf{if}\ C\rangle$
C **if** E	$\langle t\ c\ c'\ S, M, \textbf{if}\ C\rangle$	$\Rightarrow \langle S, M, c''\ C\rangle$
	(where if $t = \mathrm{tt}$ then $c'' = c$ else $c'' = c'$)	
C **while** I	$\langle S, M, \textbf{while}\ b\ \textbf{do}\ c\ C\rangle$	$\Rightarrow \langle b\ c\ S, M, b\ \textbf{while}\ C\rangle$
C **while** $E1$	$\langle \mathrm{tt}\ b\ c\ S, M, \textbf{while}\ C\rangle$	$\Rightarrow \langle S, M, c\ \textbf{while}\ b\ \textbf{do}\ c\ C\rangle$
C **while** $E2$	$\langle \mathrm{ff}\ b\ c\ S, M, \textbf{while}\ C\rangle$	$\Rightarrow \langle S, M, C\rangle$

Now that we have at some length defined the transition relation, the terminal configurations are defined by:

$$T = \{\langle \varepsilon, M, \varepsilon\rangle\}$$

and an input function in : Commands $\times$ Memories $\longrightarrow \Gamma$ is defined by:

$$\mathrm{in}(C, M) = \langle \varepsilon, M, C\rangle$$

and out : $T \longrightarrow$ Memories by:

$$\mathrm{out}(\langle \varepsilon, M, \varepsilon\rangle) = M$$

The behaviour of the SMC-machine is then a partial function, Eval : Commands$\times$Memories $\underset{P}{\longrightarrow}$ Memories and clearly:

$$\mathrm{Eval}(C, M) = M' \qquad \equiv \qquad \langle \varepsilon, M, C\rangle \Rightarrow^* \langle \varepsilon, M', \varepsilon\rangle$$

Example 10 (Factorial)

$$y := 1;\ \underbrace{\textbf{while}\ {\sim}(x = 0)\ \textbf{do}\ \overbrace{y := y * x; x := x - 1}^{C'}}_{C}$$

$\langle \varepsilon, \langle 3, 5\rangle, y := 1; C\rangle$
$\Rightarrow \langle \varepsilon, \langle 3, 5\rangle, y := 1\ C\rangle$ *by $C;$*
$\Rightarrow \langle y, \langle 3, 5\rangle, 1\ :=\ C\rangle$ *by $C := I$*

$$\begin{array}{ll}
\quad \Rightarrow \langle 1\ y, \langle 3,5\rangle, :=\ C\rangle & \textit{by } Em \\
\Rightarrow \langle \varepsilon, \langle 3,1\rangle, C\rangle & \textit{by } C := E \\
\Rightarrow \langle {\sim}(x=0)\ C', \langle 3,1\rangle, {\sim}(x=0)\ \textbf{while}\rangle & \textit{by } C\ \textbf{while}\ I \\
\quad \Rightarrow \langle {\sim}(x=0)\ C', \langle 3,1\rangle, (x=0) \sim \textbf{while}\rangle & \textit{by } E \sim I \\
\quad\quad \Rightarrow \langle {\sim}(x=0)\ C', \langle 3,1\rangle, x\ 0\ =\ \sim \textbf{while}\rangle & \textit{by } E = I \\
\quad\quad\quad \Rightarrow \langle 3 \sim(x=0)\ C', \langle 3,1\rangle, 0\ =\ \sim \textbf{while}\rangle & \textit{by } Ev \\
\quad\quad\quad \Rightarrow \langle 0\ 3 \sim(x=0)\ C', \langle 3,1\rangle, =\ \sim \textbf{while}\rangle & \textit{by } Em \\
\quad\quad \Rightarrow \langle \mathrm{ff} \sim(x=0)\ C', \langle 3,1\rangle, \sim \textbf{while}\rangle & \textit{by } E = E \\
\quad \Rightarrow \langle \mathrm{tt} \sim(x=0)\ C', \langle 3,1\rangle, \textbf{while}\rangle & \textit{by } E \sim E \\
\Rightarrow \langle \varepsilon, \langle 3,1\rangle, C'\ C\rangle & \textit{by } C\ \textbf{while}\ E1 \\
\Rightarrow \langle \varepsilon, \langle 3,1\rangle, y := y * x\ x := x - 1\ C\rangle & \textit{by } C; \\
\Rightarrow^* \langle \varepsilon, \langle 3,3\rangle, x := x - 1\ C\rangle & \\
\Rightarrow^* \langle \varepsilon, \langle 2,3\rangle, C\rangle & \\
\Rightarrow^* \langle \varepsilon, \langle 1,6\rangle, C\rangle & \\
\Rightarrow^* \langle \varepsilon, \langle 0,6\rangle, C\rangle & \\
\Rightarrow \langle {\sim}(x=0)\ C', \langle 0,6\rangle, {\sim}(x=0)\ \textbf{while}\rangle & \textit{by } C\ \textbf{while}\ I \\
\Rightarrow^* \langle \mathrm{ff} \sim(x=0)\ C', \langle 0,6\rangle, \textbf{while}\rangle & \\
\Rightarrow \langle \varepsilon, \langle 0,6\rangle, \varepsilon\rangle & \textit{by } C\ \textbf{while}\ E2
\end{array}$$

Many other machines have been proposed along these lines. It is, perhaps, fair to say that none of them can be considered as *directly formalising* the *intuitive* operational semantics to be found in most language definitions. Rather they are more or less clearly correct on the *basis* of this intuitive understanding. Further, although this is of less importance, they all have a tendency to pull the syntax to pieces or at any rate to wander around the syntax creating various complex symbolic structures which do not seem particularly forced by the demands of the language itself. Finally, they do not in general have any great claim to being *syntax-directed* in the sense of defining the semantics of compound phrases in terms of the semantics of their components, although the definition of the transition relation does fall into natural cases following the various syntactical possibilities.

1.5 Exercises

Finite Automata

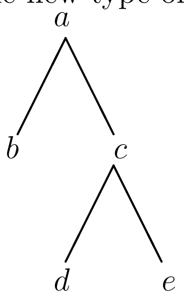
Let $M = \langle Q, \Sigma, \delta, q_0, F\rangle$ be a finite automaton.

1. Redefine the behaviour of M so that it accepts *infinite* strings $a_1a_2 \ldots a_n \ldots$, that is so that $L(M) \subseteq \Sigma^\omega$. [Hint: There are actually two answers, which can with difficulty be proved equivalent.]

2. Suppose that δ were changed so that the labelled transition relation had instead the form:

$$q \xrightarrow{a} q_1, q_2$$

and F so that $F \subseteq Q \times \Sigma$. What is the new type of δ? How can *binary trees* like



now be accepted by M?

3. Suppose instead transitions occurred with *probability* so that we had

$$q \xrightarrow[p]{a} q'$$

with $0 \leq p \leq 1$ and for any q and a:

$$\Sigma\{p \mid q \xrightarrow[p]{a} q' \text{ for some } q'\} \leq 1$$

What is a good definition of behaviour now?

4. Finite automata can be turned into *transducer* by taking δ to be a finite set of *transitions* of the form:

$$q \xrightarrow[w]{v} q'$$

with v, $w \in \Sigma^*$. Define the relation $q \xrightarrow[w]{v} q'$ and the appropriate notion of behaviour. Show any finite-state transducer can be turned into an equivalent one, where we have in any transition that $0 \leq |v| \leq 1$.

Various Machines

5. Define k counter machines. Show that any function computable by a k counter machine is computable by a 3-counter machine. [Hint: First program elementary functions on the 3-counter machine including pairing, pair : $\mathrm{N}^2 \longrightarrow \mathrm{N}$, and selection functions, $\mathrm{fst}, \mathrm{snd} : \mathrm{N} \longrightarrow \mathrm{N}$ such that:

$$\mathrm{fst}(\mathrm{pair}(m, n)) = m$$

$$\mathrm{snd}(\mathrm{pair}(m, n)) = n$$

Then simulate by coding all the registers of the k counter machine by a big tuple held in one of the registers of the 3-counter machine.]

Show that any partial-recursive function (= one computable by a Turing Machine) can be computed by some 3-counter machine (and vice-versa).

6. Consider stack machines where the registers hold stacks and operations on a stack (= element of Σ^*) are push_a, pop, ishd_a (for each $a \in \Sigma$) given by:

$$\mathrm{push}_a(w) = aw$$
$$\mathrm{pop}(aw) = w$$
$$\mathrm{ishd}_a(w) = \begin{cases} \text{true} & (\text{if } w = aw' \text{ for some } w') \\ \text{false} & (\text{otherwise}) \end{cases}$$

Show stack machines compute the same functions as Turing Machines. How many stacks are needed at most?

7. Define and investigate queue machines.

8. See how your favourite machines (Turing Machines, Push-Down Automata) fit into our framework. For a general view of machines, consult the eminently readable: [Bir] or [Sco]. Look too at [Gre].

Grammars

9. For CF grammars our notion of behaviour is adapted to *generation*. Define a notion that is good for *acceptance*. What about mixed generation/acceptance? Change the definitions so that you get parse trees as behaviour. What is the nicest way you can find to handle syntax-directed translation schemes?

10. Show that for LL(1) grammars you can obtain *deterministic* labelled (with Σ) transitions of the form

$$w \xrightarrow{a} w'$$

with w strings of terminals and non-terminals. What can you say about LL(k), LR(k)?

11. Have another look at other kinds of grammar too, e.g., Context-Sensitive, Type 0 (= arbitrary) grammars. Discover other ideas for Transition Systems in the literature. Examples include: Tag, Semi-Thue Systems, Markov Algorithms, λ-Calculus, Post Systems, L-Systems, Conway's Game of Life and other forms of Cell Automata, Kleene's Nerve Nets . . .

Petri Nets

12. Show that if we have

$$\begin{tikzcd} & m \arrow[dl, "X"'] \arrow[dr, "X'"] & \\ m' & & m'' \end{tikzcd}$$

where $F^{-1}(X) \cap F^{-1}(X') = \emptyset$ (i.e., no *conflict* between X and X') then for some m''' we have:

$$\begin{tikzcd} & m \arrow[dl, "X"'] \arrow[dr, "X'"] \arrow[dd, "Y"] & \\ m' \arrow[dr, "X'"'] & & m'' \arrow[dl, "X"] \\ & m''' & \end{tikzcd}$$

where $Y = X \cup X'$

This is a so-called *Church-Rosser Property.*

13. Show that if we have $m \xrightarrow{X} m'$ where $X = \{e_1, \ldots, e_k\}$ then for some $m_1, \ldots, m_k$ we have:

$$m \xrightarrow{\{e_1\}} m_1 \xrightarrow{\{e_2\}} \cdots \xrightarrow{\{e_k\}} m_k = m$$

What happens if we remove the restrictions on finiteness?

14. Write some Petri Nets for a parallel situation you know well (e.g., for something you knew at home or some computational situation).

15. How can nets accept languages (= subsets of Σ^*)? Are they always regular?

16. Find, for the Readers and Writers net given above, all the cases you can reach by transition sequences starting at the initial case. Draw (nicely!) the graph of cases and transitions (this is a so-called case graph).

Interpreting Automata

17. Let $G = \langle N, \Sigma, P, S \rangle$ be a context-free grammar. It is *strongly unambiguous* if there are no two leftmost derivations of the same word in Σ^*, even possibly starting from different non-terminals. Find suitable conditions on the productions of P which ensure that $G' =$

$\langle N, \Sigma', P', S \rangle$ is strongly unambiguous where $\Sigma' = \Sigma \cup \{(,)\}$ where the parentheses are assumed not to be in N or Σ and where

$$T \longrightarrow (w) \text{ is in } P' \text{ if } T \longrightarrow w \text{ is in } P.$$

18. See what changes you should make in the definition of the interpreting automaton when some of the following features are added:

$$e \ ::= \ \textbf{if } b \textbf{ then } e \textbf{ else } e \ \mid \ \textbf{begin } c \textbf{ result } e$$

$$\begin{array}{lll} c \ ::= & \multicolumn{2}{l}{\textbf{if } b \textbf{ then } c \ \mid} \\ & \textbf{case } e \textbf{ of } & e_1 \ : \ c \\ & & \vdots \\ & & e_k \ : \ c \\ & \textbf{end} \ \mid & \\ & \multicolumn{2}{l}{\textbf{for } v := e, e \textbf{ do } c \ \mid} \\ & \multicolumn{2}{l}{\textbf{repeat } c \textbf{ until } b} \end{array}$$

19. Can you handle constructions that drastically change the flow of control such as:

$$c ::= \ \textbf{stop} \ \mid m : c \mid \ \textbf{goto } m$$

(Here **stop** just stops everything!)

20. Can you handle elementary read/write instructions such as:

$$c ::= \textbf{read}(v) \mid \textbf{write}(e)$$

[Hint: Consider an analogy with finite automata – especially transducers.]

21. Can you add facilities to the automaton to handle run-time errors?

22. Can you produce measures of time/space complexity by adding extra components to the automaton?

23. Can you treat diagnostic (debugging, tracing) facilities?

24. What about real-time? That is suppose we had the awful expression:

$$e ::= \ \textbf{time}$$

which delivers the correct time.

25. Treat the following PASCAL subset. The basic sets are T, N and $x \in \mathrm{I} \times \{\mathrm{i}, \mathrm{r}, \mathrm{b}\}$ – the set of typical *identifiers* (which is *infinite*) and $o \in \mathrm{O}$ – the set { =, <>, <, <=, >, >=,

+, −, ∗, /, **div**, **mod**, **and** } of operations. The idea for typical identifiers is that i, r, b are *type symbols* for integer, real and boolean respectively and so $\langle \mathrm{FRED}, r\rangle$ is the real identifier FRED.

The derived sets are expressions and commands where:

$$e ::= m \mid t \mid v \mid -e \mid \mathbf{not}\, e \mid e\, o\, e$$
$$c ::= \mathbf{nil} \mid v := e \mid c;\, c' \mid \mathbf{if}\, e\, \mathbf{then}\, c\, \mathbf{else}\, c' \mid \mathbf{while}\, e\, \mathbf{do}\, c$$

The point of the question is that you must think about compile-time type-checking and the memories used in the $\langle S, M, C\rangle$ machine should be finite (even although there are potentially infinitely many identifiers).

26. Can you treat the binding mechanism

$$s ::= i \mid r \mid b$$
$$c ::= \mathbf{var}\, v : s\, \mathbf{begin}\, c\, \mathbf{end}$$

so that you must now incorporate symbol tables?

2 Bibliography

[Bir] Bird, R. (1976) *Programs and Machines*, Wiley and Sons.

[Bra] Brauer, W., ed. (1980) *Net Theory and Applications*, LNCS 84, Springer.

[Gor] Gordon, M.J. (1979) *The Denotational Description of Programming Languages*, Springer.

[Gre] Greibach, S.A. (1975) *Theory of Program Structures: Schemes, Semantics, Verification*, LNCS 36, Springer.

[Kel] Keller, R.M. (1976) *Formal Verification of Parallel Programs*, Communications of the ACM 19(7):371–384.

[Lan] Landin, P.J. (1966) *A Lambda-calculus Approach*, Advances in Programming and Non-numerical Computation, ed. L. Fox, Chapter 5, pp. 97–154, Pergamon Press.

[Oll] Ollengren, A. (1976) *Definition of Programming Languages by Interpreting Automata*, Academic Press.

[Pet] Peterson, J.L. (1977) *Petri Nets*, ACM Computing Surveys 9(3):223–252.

[Sco] Scott, D.S. (1967) *Some Definitional Suggestions for Automata Theory*, Journal of Computer and System Sciences 1(2):187–212.

[Ten] Tennent, R.D. (1981) *Principles of Programming Languages*, Prentice-Hall.

[Weg] Wegner, P. (1972) *The Vienna Definition Language*, ACM Computing Surveys 4(1):5–63.

3 Simple Expressions and Commands

The $\langle S, M, C \rangle$ machine emphasises the idea of computation as a sequence of transitions involving simple data manipulations; further the definition of the transitions falls into simple cases according to the syntactic structure of the expression or command on top of the control stack. However, many of the transitions are of little intuitive importance, contradicting our idea of the right choice of the "size" of the transitions. Further the definition of the transitions is not syntax-directed so that, for example, the transitions of $c; c'$ are not directly defined in terms of those for c and those for c'. Finally but really the most important, the $\langle S, M, C \rangle$ machine is not a formalisation of intuitive operational ideas but is rather, fairly clearly, correct *given* these intuitive ideas.

In this chapter we develop a method designed to answer these objections, treating simple expressions and commands as illustrated by the language L. We consider run-time errors and say a little on how to establish properties of transition relations. Finally we take a first look at simple type-checking.

3.1 Simple Expressions

Let us consider first the very simple subset of expressions given by:

$$e ::= m \mid e_0 + e_1$$

and how the $\langle S, M, C\rangle$ machine deals with them. For example we have the transition sequence for the expression $(1 + (2 + 3)) + (4 + 5)$:

$$\begin{aligned}
\langle \varepsilon, M, (1+(2+3))+(4+5)\rangle &\longrightarrow \langle \varepsilon, M, (1+(2+3))\ (4+5)\ +\rangle \\
&\longrightarrow \langle \varepsilon, M, 1\ (2+3)\ +\ (4+5)\ +\rangle \\
&\longrightarrow \langle 1, M, (2+3)\ +\ (4+5)\ +\rangle \\
&\longrightarrow \langle 1, M, 2\ 3\ +\ +\ (4+5)\ +\rangle \\
&\longrightarrow \langle 2\ 1, M, 3\ +\ +\ (4+5)\ +\rangle \\
&\longrightarrow \langle 3\ 2\ 1, M, +\ +\ (4+5)\ +\rangle \qquad (*) \\
&\longrightarrow \langle 5\ 1, M, +\ (4+5)\ +\rangle \qquad (*) \\
&\longrightarrow \langle 6, M, (4+5)\ +\rangle \\
&\longrightarrow^3 \langle 5\ 4\ 6, M, +\ +\rangle \qquad (*) \\
&\longrightarrow \langle 9\ 6, M, +\rangle \qquad (*) \\
&\longrightarrow \langle 15, M, \varepsilon\rangle
\end{aligned}$$

In these 13 transitions only the 4 additions marked $(*)$ are of any real interest as system events. Further the intermediate structures generated on the stacks are also of little interest. Preferable would be a sequence of 4 transitions on the expression itself thus:

$$\begin{aligned}
(1 + (2 \overset{\triangledown}{+} 3)) + (4 + 5)) &\longrightarrow (1 \overset{\triangledown}{+} 5) + (4 + 5) \\
&\longrightarrow 6 + (4 \overset{\triangledown}{+} 5) \\
&\longrightarrow 6 \overset{\triangledown}{+} 9 \\
&\longrightarrow 15
\end{aligned}$$

where we are ignoring the memory and we have marked the occurrences of the additions in each transition. (These transition sequences of expressions are often called *reduction* sequences (= *derivations*) and the occurrences are called *redexes*; this notation originates in the λ-calculus (see, e.g., [Hin]).)

Now consider an informal specification of this kind of expression *evaluation*. Briefly one might just say one evaluates from left-to-right. More pedantically one could say:

Constants Any constant, m, is already evaluated with itself as value.
Sums To evaluate $e_0 + e_1$
(1) Evaluate e_0 obtaining m_0, say, as result.
(2) Evaluate e_1 obtaining m_1, say, as result.

(3) Add m_0 to m_1 obtaining m_2, say, as result.
This finishes the evaluation and m_2 is the result of the evaluation.

Note that this specification is syntax-directed, and we use it to obtain *rules* for describing steps (= transitions) of evaluation which we think of as nothing else than a derivation of the form:

$$e = e_1 \longrightarrow e_2 \longrightarrow \ldots \longrightarrow e_{n-1} \longrightarrow e_n = m$$

(where m is the result). Indeed if we just look at the first step we see from the above specification that

(1) If e_0 is not a constant the first step of the evaluation of $e_0 + e_1$ is the first step of the evaluation of e_0.
(2) If e_0 is a constant, but e_1 is not, the first step of the evaluation of $e_0 + e_1$ is the first step of the evaluation of e_1.
(3) If e_0 and e_1 are constants the first (and last!) step of the evaluation of $e_0 + e_1$ is the addition of e_0 and e_1.

Clearly too the first step of evaluating an expression, e, can be taken as resulting in an expression e' with the property that the evaluation of e is the first step followed by the evaluation of e'. We now put all this together to obtain rules for the first step. These are rules for establishing binary relationships of the form:

$$e \longrightarrow e' \quad \equiv \quad e' \text{ is the result of the first step of the evaluation of } e.$$

Rules: Sum

(1) $$\frac{e_0 \longrightarrow e_0'}{e_0 + e_1 \longrightarrow e_0' + e_1}$$

(2) $$\frac{e_1 \longrightarrow e_1'}{m_0 + e_1 \longrightarrow m_0 + e_1'}$$

(3) $m_0 + m_1 \longrightarrow m_2$ (if m_2 is the sum of m_0 and m_1)

Thus, for example, rule 1 states what is obvious from the above discussion:

If e_0' is the result of the first step of the evaluation of e_0 then $e_0' + e_1$ is the result of the first step of the evaluation of $e_0 + e_1$.

We now take these rules as a *definition* of what relationships hold – namely exactly these we can establish from the rules. We take the above discussion as showing why this *mathematical* definition makes sense from an *intuitive view*; it is the *direct* formalisation referred to above.

As an example consider the step:

$$(1 + (2 + 3)) + (4 + 5) \longrightarrow (1 + 5) + (4 + 5)$$

To establish this step we have

1.	$2+3$	$\longrightarrow$	5	(By rule 3)
2.	$1+(2+3)$	$\longrightarrow$	$1+5$	(By rule 2)
3.	$(1+(2+3))+(4+5)$	$\longrightarrow$	$(1+5)+(4+5)$	(By rule 1)

Rather than this unnatural "bottom-up" method we usually display these little proofs in the "top-down" way they are actually "discovered". The arrow is supposed to show the "direction" of discovery:

$$\begin{tikzcd}
(1+(2+3))+(4+5) \arrow[r, "\text{Sum 1}"] \arrow[rr, bend right=90, looseness=1.5, phantom] & (1+5)+(4+5)) \\
1 + (2+3) \arrow[r, "\text{Sum 2}"] & 1 + 5 \\
2 + 3 \arrow[r, "\text{Sum 3}"] & 5
\end{tikzcd}$$

Thus, while the evaluation takes four steps, the justification (proof) of each step has a certain size of its own (which need not be displayed). In this light the $\langle S, M, C\rangle$ machine can be viewed as mixing-up the additions with the reasons why they should be performed into one long linear sequence.

It could well be argued that our formalisation is not really that direct. A more direct approach would be to give rules for the transition sequences themselves (the evaluations). For the intuitive specification refers to these evaluations rather than any hypothetical atomic actions from which they are composed. However, axiomatising a step is intuitively simpler, and we prefer to follow a simple approach until it leads us into such difficulties that it is better to consider whole derivations.

Another point concerns the lack of formalisation of our ideas. The above rules are easily turned into a formal system of formulae, axioms and rules. What we would want is a sufficiently elastic conception of a *range* of such formal systems which on the one hand allows the natural expression of all the systems of rules we wish, and on the other hand returns some profit in the form of interesting theorems about such systems or interesting computer systems based on such systems. However, the present work is too exploratory for us to fix our ideas, although we may later try out one or two possibilities. We also fear that introducing such formalities could easily lead us into obscurities in the presentation of otherwise natural ideas.

Now we try out more expressions. To evaluate variables we need the memory component of the $\langle S, M, C\rangle$ machines – indeed that is the only "natural" component they have! It is convenient here to change our notation to a more generally accepted one:

OLD	NEW
Memory	Store
Memories = (Var $\longrightarrow$ N) = S	
M	σ
$M[m/v]$	$\sigma[m/v]$

3.1.1 L-Expressions

Now for the expression language of L:

$$e ::= m \mid v \mid (e + e') \mid (e - e') \mid (e * e')$$

we introduce the configurations

$$\Gamma = \{\langle e, \sigma \rangle\}$$

and the relation

$$\langle e, \sigma \rangle \longrightarrow \langle e', \sigma \rangle$$

meaning one step of the evaluation of e (with store σ) results in the expression e' (with store σ). The rules are just those we already have, adapted to take account of stores plus an obvious rule for printing the value of a variable in a store.

Rules: Sum

$$(1)\quad \frac{\langle e_0, \sigma \rangle \longrightarrow \langle e_0', \sigma \rangle}{\langle e_0 + e_1, \sigma \rangle \longrightarrow \langle e_0' + e_1, \sigma \rangle}$$

$$(2)\quad \frac{\langle e_1, \sigma \rangle \longrightarrow \langle e_1', \sigma \rangle}{\langle m + e_1, \sigma \rangle \longrightarrow \langle m + e_1', \sigma \rangle}$$

(3) $\langle m + m', \sigma \rangle \longrightarrow \langle n, \sigma \rangle$ (where $n = m + m'$)

Minus

1,2. Exercise for the reader.

3. $\langle m - m', \sigma \rangle \longrightarrow \langle n, \sigma \rangle$ (if $m \geq m'$ and $n = m - m'$)

Times

1,2,3. Exercise for the reader.

Variable

(1) $\langle v, \sigma \rangle \longrightarrow \langle \sigma(v), \sigma \rangle$

Note the two uses of the symbol, +, in rule Sum 3: one as a syntactic construct and one for the addition function. We will often overload symbols in this way relying on the context for disambiguation. So here, for example, to make sense of $n = m+m'$ we must be meaning addition as the left-hand-side of the equation denotes a natural number.

Of course the terminal configurations are those of the form $\langle m, \sigma \rangle$, and m is the result of the evaluation. Note that there are configurations such as:

$$\gamma = \langle 5 + (7 - 11), \sigma \rangle$$

which are not terminal but for which there is no γ' with $\gamma \longrightarrow \gamma'$.

Definition 11 *Let $\langle \Gamma, T, \longrightarrow \rangle$ be a tts. A configuration γ is stuck if $\gamma \notin T$ and $\neg \exists \gamma'.\ \gamma \longrightarrow \gamma'$.*

In most programming languages these stuck configurations result in run-time errors. These will be considered below.

The behaviour of expressions is the result of their evaluation and is defined by:

$$\text{eval}(e, \sigma) = m \quad \Leftrightarrow \quad \langle e, \sigma \rangle \longrightarrow^* \langle m, \sigma \rangle$$

The reader will see (from 2.3 below, if needed) that eval is a well-defined partial function.

One can also define the *equivalence* of expressions by:

$$e \equiv e' \quad \Leftrightarrow \quad \forall \sigma.\ \text{eval}(e, \sigma) = \text{eval}(e', \sigma)$$

3.1.2 Boolean Expressions

Now we turn to the Boolean expressions of the language L given by:

$$b := t \mid b \textbf{ or } b' \mid e = e' \mid {\sim} b$$

Here we take $\Gamma = \{\langle b, \sigma \rangle\}$ and consider the rules for the transition relation. There are clearly none for truth-values, t, but there are several possibilities for disjunctions, b **or** b'. These possibilities differ not only in the order of the transitions, but even on which transitions occur. The configurations are pairs $\langle b, \sigma \rangle$.

A. **Complete Evaluation**: This is just the Boolean analogue of our rules for expressions and corresponds to the method used by our SMC-machine.

(1) $\dfrac{\langle b_0, \sigma\rangle \longrightarrow \langle b_0', \sigma\rangle}{\langle b_0 \textbf{ or } b_1, \sigma\rangle \longrightarrow \langle b_0' \textbf{ or } b_1, \sigma\rangle}$

(2) $\dfrac{\langle b_1, \sigma\rangle \longrightarrow \langle b_1', \sigma\rangle}{\langle t \textbf{ or } b_1, \sigma\rangle \longrightarrow \langle t \textbf{ or } b_1' , \sigma\rangle}$

(3) $t \textbf{ or } t' \longrightarrow t''$ (where $t'' = t \vee t'$)

B. **Left-Sequential Evaluation**: This takes advantage of the fact that it is not needed to evaluate b, in tt **or** b, as the result will be tt independently of the result of evaluating b,

(1) $\dfrac{\langle b_0, \sigma\rangle \longrightarrow \langle b_0', \sigma\rangle}{\langle b_0 \textbf{ or } b_1, \sigma\rangle \longrightarrow \langle b_0' \textbf{ or } b_1, \sigma\rangle}$

(2) $\langle \mathrm{tt} \textbf{ or } b_1, \sigma\rangle \longrightarrow \langle \mathrm{tt}, \sigma\rangle$

(3) $\langle \mathrm{ff} \textbf{ or } b_1, \sigma\rangle \longrightarrow \langle b_1, \sigma\rangle$

C. **Right-Sequential Evaluation**: Like B but "backwards".

D. **Parallel Evaluation**: This tries to combine the advantages of B and C by evaluating b_0 and b_1 in parallel. In practice that would mean having two processors, one for b_0 and one for b_1, or using one but interleaving, somehow, the evaluations of b_0 and b_1. This idea is therefore not found in the usual sequential programming languages (as opposed to these making explicit provisions for concurrency). However, it may be useful for hardware specification.

(1) $\dfrac{\langle b_0, \sigma\rangle \longrightarrow \langle b_0', \sigma\rangle}{\langle b_0 \textbf{ or } b_1, \sigma\rangle \longrightarrow \langle b_0' \textbf{ or } b_1, \sigma\rangle}$

(2) $\dfrac{\langle b_1, \sigma\rangle \longrightarrow \langle b_1', \sigma\rangle}{\langle b_0 \textbf{ or } b_1, \sigma\rangle \longrightarrow \langle b_0 \textbf{ or } b_1', \sigma\rangle}$

(3) $\langle \mathrm{tt} \textbf{ or } b_1, \sigma\rangle \longrightarrow \langle \mathrm{tt}, \sigma\rangle$

(4) $\langle b_0 \textbf{ or } \mathrm{tt}, \sigma\rangle \longrightarrow \langle \mathrm{tt}, \sigma\rangle$

(5) $\langle \mathrm{ff} \textbf{ or } b_1, \sigma\rangle \longrightarrow \langle b_1, \sigma\rangle$

(6) $\langle b_0 \textbf{ or } \mathrm{ff}, \sigma\rangle \longrightarrow \langle b_0, \sigma\rangle$

The above evaluation mechanisms are very different when subexpressions can have non-terminating evaluations, when we have the following relationships:

$$\begin{tikzcd}
\mathrm{B} \arrow[d, Leftarrow, ""] & \mathrm{A} \arrow[l, Rightarrow] \arrow[d, Rightarrow] \\
\mathrm{D} & \mathrm{C} \arrow[l, Rightarrow]
\end{tikzcd}$$

where X $\Rightarrow$ Y means that if method X terminates with result t, so does method Y. We take method A for the semantics of our example language L.

For Boolean expressions of the form $e = e'$ our rules depend on those for expressions, but otherwise are normal (and for brevity we omit the σ's).

- **Equality**

(1) $\dfrac{e_0 \longrightarrow e_0'}{e_0 = e_1 \longrightarrow e_0' = e_1}$

(2) $\dfrac{e_1 \longrightarrow e_1'}{m = e_1 \longrightarrow m = e_1'}$

(3) $m = n \longrightarrow t$ (where t is tt if $m = n$ and ff otherwise)

For negations $\sim b$ we have, again omitting the σ's:

- **Negation**

(1) $\dfrac{b \longrightarrow b'}{\sim b \longrightarrow \sim b'}$

(2) $\sim t \longrightarrow t'$ $(\textit{where } t' = \neg t)$

The *behaviour* of Boolean expressions is defined by:

$$\text{eval}(b, \sigma) = t \Leftrightarrow \langle b, \sigma \rangle \longrightarrow^* \langle t, \sigma \rangle$$

One can also define *equivalence* of Boolean expressions by:

$$b \equiv b' \quad \Leftrightarrow \quad \forall \sigma.\ \text{eval}(b, \sigma) = \text{eval}(b', \sigma)$$

3.2 Simple Commands

Again we begin with a trivial language of commands,

$$c ::= \textbf{nil} \mid v := e \mid c;\ c'$$

and see how the SMC-machine behaves on an example:

$$\begin{aligned}
\langle \varepsilon, abc, z := x; (x := y; y := z)\rangle &\longrightarrow \langle \varepsilon, abc, z := x\ x := y; y := z\rangle \\
&\longrightarrow \langle z, abc, x :=\ \ x := y; y := z\rangle \\
&\longrightarrow \langle a\ z, abc, :=\ \ x := y; y := z\rangle \quad (*) \\
&\longrightarrow \langle \varepsilon, aba, x := y; y := z\rangle \\
&\longrightarrow \langle \varepsilon, aba, x := y\ y := z\rangle \\
&\longrightarrow^2 \langle b\ x, aba, :=\ \ y := z\rangle \quad (*) \\
&\longrightarrow \langle \varepsilon, bba, y := z\rangle \\
&\longrightarrow^2 \langle a\ y, bba, :=\rangle \quad (*) \\
&\longrightarrow \langle \varepsilon, baa, \varepsilon\rangle
\end{aligned}$$

And we see that of the eleven transitions only three – the assignments – are of interest as system events.

Preferable here would be a sequence of three transitions on configurations of the form $\langle c, \sigma\rangle$, thus:

$$\begin{aligned}
\langle z \overset{\triangledown}{:=} x;\ (x := y;\ y := z), abc\rangle &\longrightarrow \langle (x \overset{\triangledown}{:=} y;\ y := z), aba\rangle \\
&\longrightarrow \langle y \overset{\triangledown}{:=} z\ , bba\rangle \\
&\longrightarrow baa
\end{aligned}$$

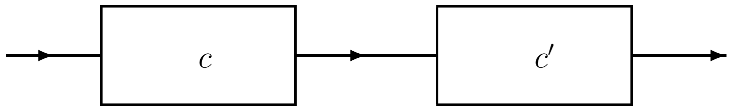
where we have marked the assignments occurring in transitions.

Now informally one can specify such command *executions* as follows:

- **Nil**: To execute **nil** from store σ take no action and terminate with σ as the final store of the execution.
- **Assignment**: To execute $v := e$ from store σ evaluate e, and if the result is m, change σ to $\sigma[m/v]$ (the final store of the execution).
- **Composition**: To execute $c; c'$ from store σ

(1) Execute c from store σ obtaining a final store, σ', say, if this execution terminates.
(2) Execute c' from the store σ'. The final store of this execution is also the final store of the execution of $c; c'$.

Sometimes the execution of $c; c'$ is pictured in terms of a little flowchart:



As in the case of expressions one sees that this description is syntax-directed. We formalise it considering terminating executions of a command c from a store σ to be transition sequences of the form:

$$\langle c, \sigma\rangle = \langle c_0, \sigma_0\rangle \longrightarrow \langle c_1, \sigma_1\rangle \longrightarrow \ldots \longrightarrow \langle c_{n-1}, \sigma_{n-1}\rangle \longrightarrow \sigma_n$$

Here we take the configurations to be:

$$\Gamma = \{\langle c, \sigma\rangle\} \cup \{\sigma\}$$

and the terminal configurations to be

$$T = \{\sigma\}$$

where the transition relation $\langle c, \sigma\rangle \longrightarrow \langle c', \sigma'\rangle$ (resp. σ') is read as:

> One step of execution of the command c from the store σ results in the store σ' and the rest of the execution of c is the execution of c' from σ' (resp. and the execution terminates).

Thus we choose c' to represent, in as simple a way as is available, the remainder of the execution of c after its first step. The rules are

- Nil: $\langle \mathbf{nil}, \sigma\rangle \longrightarrow \sigma$
- Assignment:

(1) $$\frac{\langle e, \sigma\rangle \longrightarrow^* \langle m, \sigma\rangle}{\langle v := e, \sigma\rangle \longrightarrow \sigma[m/v]}$$

- Composition:

(1) $$\frac{\langle c_0, \sigma\rangle \longrightarrow \langle c_0', \sigma'\rangle}{\langle c_0;\ c_1, \sigma\rangle \longrightarrow \langle c_0';\ c_1, \sigma'\rangle}$$

(2) $$\frac{\langle c_0, \sigma\rangle \longrightarrow \sigma'}{\langle c_0;\ c_1, \sigma\rangle \longrightarrow \langle c_1, \sigma'\rangle}$$

Note: In formulating the rule for assignment we have considered the *entire evaluation* of the right-hand-side as part of *one* execution step. This corresponds to a change in view of the size of our step when considering commands, but we could just as well have chosen otherwise.

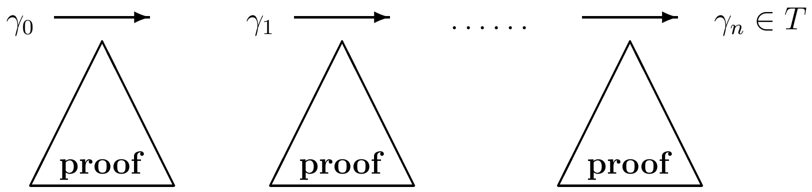
As an example consider the first transition desired above for the execution

$$\langle z := x; (x := y;\ y := z), abc\rangle$$

It is presented in the top-down way

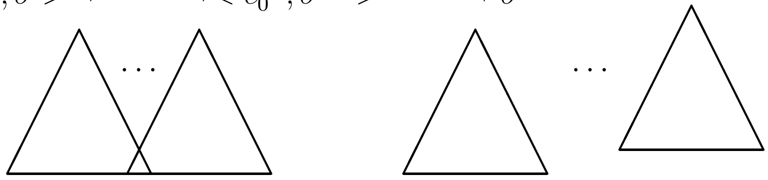
$$\langle z := x;\ (x := y;\ y := z), abc\rangle \overset{\text{Comp 2}}{\longrightarrow} \langle (x := y;\ y := z), aba\rangle$$
$$\langle z := x, abc\rangle \overset{\text{Ass 1}}{\longrightarrow} aba$$
$$\langle x, abc\rangle \overset{\text{Var 1}}{\longrightarrow} \langle a, abc\rangle$$

Again we see, as in the case of expressions a “two-dimensional” structure consisting of a “horizontal” transition sequence of the events of system significance and for each transition a “vertical” explanation of why and how it occurs.



For terminating executions of $c_0; c_1$ this will have the form:

$$\frac{< c_0; c_1, \sigma > \overset{c1}{\rightarrow} \cdots}{< c_0, \sigma > \rightarrow} \frac{\overset{c1}{\rightarrow} < c_0^{\prime \cdot\cdot \prime}; c_1, \sigma^{\prime \cdot\cdot \prime} >}{\rightarrow < c_0^{\prime \cdot\cdot \prime}, \sigma^{\prime \cdot\cdot \prime} >} \frac{\overset{c2}{\rightarrow} < c_1, \sigma^{\prime \cdot\cdot \prime\prime} >}{\rightarrow \sigma^{\prime \cdot\cdot \prime\prime}} \cdots \rightarrow \sigma^{\prime \cdot\cdot \prime\prime \cdot\cdot \prime}$$



Again we see that the SMC-machine transition sequences are more-or-less linearisations of these structures. Note the appearance of rules for binary relations (with additional data components) such as:

$$\mathrm{R}(c, c', \sigma, \sigma') \overset{def}{=} \langle c, \sigma \rangle \longrightarrow \langle c', \sigma' \rangle$$
$$\mathrm{S}(e, e', \sigma) \quad \overset{def}{=} \langle e, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle$$

Later we shall make extensive use of predicates to treat the context-sensitive aspects of syntax (= the static aspects of semantics). As far as we can see there is no particular need for *ternary* relations, although the above discussion on the indirectness of our formalisation does suggest the possibility of needing relations of *variable* degree for dealing with execution sequences.

3.3 L-commands

Recalling the syntax of L-commands,

$c ::=$ **nil** $\mid v := e \mid c; c' \mid$ **if** b **then** c **else** $c' \mid$ **while** b **do** c

we see that it remains only to treat conditionals and repetitions.

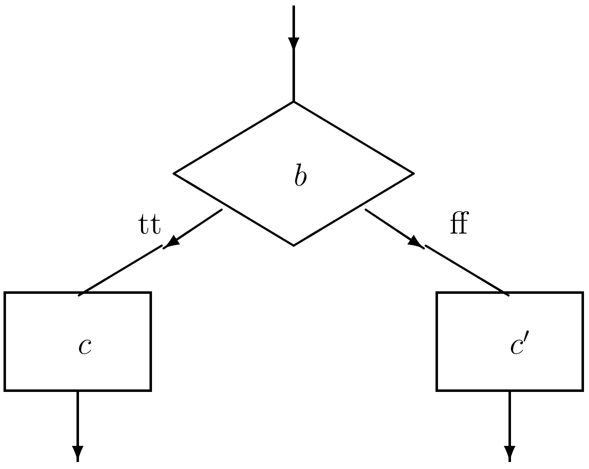
- **Conditionals:** To execute **if** b **then** c **else** c' from σ

1. Evaluate b in σ

2.1 If result was tt execute c from σ.

2.2 If result was ff execute c' from σ.

In pictures we have:



And the rules are:

(1) $$\frac{\langle b, \sigma\rangle \longrightarrow^* \langle \mathrm{tt}, \sigma\rangle}{\langle \mathbf{if}\ b\ \mathbf{then}\ c\ \mathbf{else}\ c', \sigma\rangle \longrightarrow \langle c, \sigma\rangle}$$

(2) $$\frac{\langle b, \sigma\rangle \longrightarrow^* \langle \mathrm{ff}, \sigma\rangle}{\langle \mathbf{if}\ b\ \mathbf{then}\ c\ \mathbf{else}\ c', \sigma\rangle \longrightarrow \langle c', \sigma\rangle}$$

Note: Again we are depending on the transition relation of another syntactic class – here Boolean expressions – and a whole computation from that class becomes one step of the computation.

Note: No rules for $T(\mathbf{if}\ b\ \mathbf{then}\ c\ \mathbf{else}\ c')$ are given as that predicate never applies. For a conditional is never terminal as one always has at least one action – namely evaluating the condition.

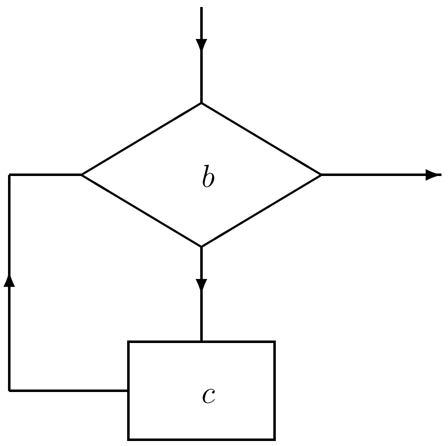
- **While**: To execute **while** b **do** c from σ

1. Evaluate b

2.1 If the result is tt, execute c from σ. If that terminates with final state σ', execute **while** b **do** c from σ'.

2.2 If the result is ff, the execution is finished and the final state is σ.

In pictures we have the familiar flowchart:



The rules are:

$$(1)\quad \frac{\langle b,\sigma\rangle \longrightarrow^* \langle \mathrm{tt},\sigma\rangle}{\langle \textbf{while}\ b\ \textbf{do}\ c,\sigma\rangle \longrightarrow \langle c;\ \textbf{while}\ b\ \textbf{do}\ c,\sigma\rangle}$$

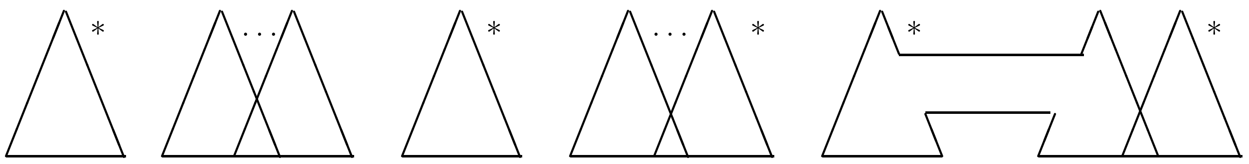
$$(2)\quad \frac{\langle b,\sigma\rangle \longrightarrow^* \langle \mathrm{ff},\sigma\rangle}{\langle \textbf{while}\ b\ \textbf{do}\ c,\sigma\rangle \longrightarrow \sigma}$$

Example 12 *Consider the factorial example* $y := 1; w$ *from Chapter 1, where* $w =$ **while** $\sim(x = 0)$ **do** c *where* $c = (y := y * x;\ x := x - 1)$*. We start from the state* $\langle 3, 5\rangle$*.*

$$\begin{array}{lll}
\langle y\langle 3,5\rangle\rangle \overset{ASS1}{\longrightarrow} & \langle w,\langle 3,1\rangle\rangle\rangle & \\
\overset{COMP2}{\longrightarrow} & \langle c;w,\langle 3,1\rangle\rangle & \textit{(via WHI)}\\
\overset{COMP1}{\longrightarrow} & \langle x := x-1;w,\langle 3,3\rangle\rangle & \textit{(via COMP2 and ASS1)}\\
\overset{COMP2}{\longrightarrow} & \langle w,\langle 2,3\rangle\rangle & \\
\overset{COMP2}{\longrightarrow} & \langle c;w,\langle 2,3\rangle\rangle & \textit{(WHI)}\\
\overset{COMP1}{\longrightarrow} & \langle x := x-1;w,\langle 2,6\rangle\rangle & \textit{(via COMP2 and ASS1)}\\
\overset{COMP1}{\longrightarrow} & \langle w,\langle 1,6\rangle\rangle & \\
\longrightarrow & \langle c;w,\langle 1,6\rangle\rangle & \\
\longrightarrow & \langle x := x-1;w,\langle 1,6\rangle\rangle & \\
\longrightarrow & \langle w,\langle 0,6\rangle\rangle & \\
\overset{COMP2}{\longrightarrow} & \langle 0,6\rangle & \textit{(via WHI2)}
\end{array}$$

A terminating execution sequence of a while-loop $w =$ **while** b **do** c looks like this (omitting σ's):

$$\begin{array}{l}
w \longrightarrow c;w \longrightarrow \ldots \longrightarrow w \longrightarrow c;w \longrightarrow \ldots \longrightarrow w - - - - - - - \ldots \longrightarrow w \longrightarrow \cdot\\
b \longrightarrow^* \mathrm{tt}\ c \longrightarrow \ldots \longrightarrow \cdot b \longrightarrow^* \mathrm{tt}\ c \longrightarrow \ldots \longrightarrow \cdot b - - - - - - - \ldots \longrightarrow \cdot; b \longrightarrow^* \mathrm{ff}
\end{array}$$



One can now define the behaviour and equivalence of commands by:

$$\text{exec}(c, \sigma) = \sigma' \quad \Leftrightarrow \quad \langle c, \sigma \rangle \longrightarrow^* \sigma'$$

and

$$c \simeq c' \quad \Leftrightarrow \quad \forall \sigma.\ \text{exec}(c, \sigma) = \text{exec}(c', \sigma)$$

where we are using *Kleene equality*, which means that one side is defined iff the other is, and in that case they are both equal.

3.4 Structural Induction

Although we have no particular intention of proving very much either about or with our operational semantics, we would like to introduce enough mathematical apparatus to enable us to establish the truth of such obvious statements as:

if $\gamma \notin T$ then for some γ' we have $\gamma \longrightarrow \gamma'$

The standard tool is the principle of *Structural Induction* (SI). It enables us to prove properties $P(p)$ of syntactic phrases, and it takes on different forms according to the abstract syntax of the language. For L we have three such principles, one for expressions, one for Boolean expressions and one for commands.

Structural Induction for Expressions

Let $P(e)$ be a property of expressions. Suppose that:

(1) For all m in N it is the case that $P(m)$ holds, and
(2) For all v in Var it is the case that $P(v)$ holds, and
(3) For all e and e' in E if $P(e)$ and $P(e')$ holds so does $P(e + e')$, and
(4) As 3 but for $-$, and
(5) As 3 but for $*$

Then for all expressions e, it is the case that $P(e)$ holds.

We take this principle as being intuitively obvious. It can be stated more compactly by using standard logical notation:

$$
\begin{aligned}
&[(\forall m \in \mathrm{N}.\ P(m)) \wedge (\forall v \in \mathrm{Var}.\ P(v)) \\
&\quad \wedge (\forall e, e' \in \mathrm{E}.\ P(e) \wedge P(e') \supset P(e + e')) \\
&\quad \wedge (\forall e, e' \in \mathrm{E}.\ P(e) \wedge P(e') \supset P(e - e')) \\
&\quad \wedge (\forall e, e' \in \mathrm{E}.\ P(e) \wedge P(e') \supset P(e * e'))] \\
&\quad \supset \forall e \in \mathrm{E}.\ P(e)
\end{aligned}
$$

As an example we prove

Fact 13 *The transition relation for expressions is deterministic.*

PROOF. We proceed by SI on the property $P(e)$ where

$$P(e) \equiv \forall \sigma, \gamma', \gamma''(\langle e, \sigma\rangle \longrightarrow \gamma' \wedge \langle e, \sigma\rangle \longrightarrow \gamma'') \supset \gamma' = \gamma''$$

Now there are five cases according to the hypotheses necessary to establish the conclusion by SI.

1. $e = m \in \mathrm{N}$ Suppose $\langle m, \sigma\rangle \longrightarrow \gamma', \gamma''$. But this cannot be the case as $\langle m, \sigma\rangle$ is stuck. Thus $P(e)$ holds vacuously.
2. $e = v \in \mathrm{Var}$ Suppose $\langle v, \sigma\rangle \longrightarrow \gamma', \gamma''$. Then as there is only one rule for variables, we have $\gamma' = \langle \sigma(v), \sigma\rangle = \gamma''$.
3. $e = e_0 + e_1$ Suppose $\langle e_0 + e_1, \sigma\rangle \longrightarrow \gamma', \gamma''$. There are three subcases according to why $\langle e_0 + e_1, \sigma\rangle \longrightarrow \gamma'$.
3.1 Rule 1 For some e_0' we have $\langle e_0, \sigma\rangle \longrightarrow \langle e_0', \sigma\rangle$ and $\gamma' = \langle e_0' + e_1, \sigma\rangle$. Then e_0 is not in N (otherwise $\langle e_0, \sigma\rangle$ would be stuck) and so for some e_0'' we have $\langle e_0, \sigma\rangle \longrightarrow \langle e_0'', \sigma\rangle$ and so $\gamma'' = \langle e_0'' + e_1, \sigma\rangle$. But by the induction hypothesis applied to e_0 we therefore have $e_0' = e_0''$ and so $\gamma' = \gamma''$.
3.2 Rule 2 We have $e_0 = m \in \mathrm{N}$ and for some e_1' we have $\langle e_1, \sigma\rangle \longrightarrow \langle e_1', \sigma\rangle$ and $\gamma' = \langle m + e_1', \sigma\rangle$. Then e_1 is not in N and for some e_1'' we have $\langle e_1, \sigma\rangle \longrightarrow \langle e_1'', \sigma\rangle$ and $\gamma'' = \langle m + e_1'', \sigma\rangle$. But applying the induction hypothesis to e_1, we see that $e_1' = e_1''$ and so $\gamma' = \gamma''$.
3.3 Rule 3 We have $e_0 = m_0, e_1 = m_1$. Then clearly $\gamma' = \gamma''$.
4. $e = e_0 - e_1$
5. $e = e_0 * e_1$ These cases are similar to the third case and are left to the reader. ■

In the above we did not need such a strong induction hypothesis. Instead we could choose a fixed σ and proceed by SI on $Q(e)$ where:

$$Q(e) \equiv \forall \gamma', \gamma''.\ (\langle e, \sigma\rangle \longrightarrow \gamma \wedge \langle e, \sigma\rangle \longrightarrow \gamma'') \supset \gamma' = \gamma''$$

However, this is just a matter of luck (here that the evaluation of expressions does not side effect the state). Generally it is wise to choose one's induction hypothesis as strong as possible.

The point is that if one's hypothesis has the form (for example)

$$P(e) \equiv \forall\sigma.\ Q(e,\sigma)$$

then when proving $P(e_0 + e_1)$ given $P(e_0)$ and $P(e_1)$ one fixes σ and tries to prove $Q(e,\sigma)$. But in this proof one is at liberty to use the facts $Q(e_0,\sigma)$, $Q(e_0,\sigma'), Q(e_1,\sigma), Q(e_1,\sigma'')$ for *any* σ' and σ''.

SI for Boolean Expressions

We just write down the symbolic version for a desired property $P(b)$ of Boolean expressions.

$$\begin{aligned}&[(\forall t \in \mathrm{T}.\ P(t)) \wedge (\forall e, e' \in E.\ P(e = e'))\\ &\qquad \wedge (\forall b, b' \in \mathrm{B}.\ P(b) \wedge P(b') \supset P(b\ \mathbf{or}\ b'))\\ &\qquad \wedge (\forall b \in \mathrm{B}.\ P(b) \supset P(\sim b))]\\ &\qquad \supset \forall b \in B.P(b)\end{aligned}$$

In general when applying this principle one may need further structural inductions on expressions. For example:

Fact 14 *If b is not in T and contains no occurrence of an expression of the form $(m-n)$ where $m < n$, then no $\langle b,\sigma\rangle$ is stuck.*

PROOF. We fix σ and proceed by SI on Boolean expressions on the property:

$$\begin{aligned}Q(b) \equiv\ &[b \notin \mathrm{T} \wedge (\forall m < n.(m-n) \text{ does not occur in } b)]\\ &\quad \supset \langle b,\sigma\rangle \text{ is not stuck}\end{aligned}$$

Case 1 $b = \mathrm{tt}$ This holds vacuously.
Case 2 $b = (e = e')$ Here there are three subcases depending on the forms of e and e'.
Case 2.1 If e is not in N, then for some e'' we have $\langle e,\sigma\rangle \longrightarrow \langle e'',\sigma\rangle$
Lemma For any expression e not in N if e has no subexpressions of the form, $m-n$, where $m<n$, then no $\langle e,\sigma\rangle$ is stuck.
Proof By SI on expressions and left to the reader. ⌧

Continuing with case 2.1 we see that $\langle e = e',\sigma\rangle \longrightarrow \langle e'' = e',\sigma\rangle$ so $\langle b,\sigma\rangle$ is not stuck.
Case 2.2 Here e is in N but e' is not; the proof is much like case 2.1 and also uses the lemma.
Case 2.3 Here e, e' are in N and we an use rule EQU. 3.
Case 3 $b = (b_0\ \mathbf{or}\ b_1)$ This is like case 3 of the proof of fact 1.
Case 4 $b = \sim b_0$ If b_0 is not in T we can easily apply the induction hypothesis. Otherwise use rule NEG. 2.

This concludes all the cases and hence the proof. ■

SI for Commands

We just write down the symbolic version for a (desired) property $P(c)$ of commands:

$$\begin{aligned}
&[P(\mathbf{nil}) \wedge \forall v \in \mathrm{Var},\ e \in \mathrm{E}.\ P(v := e)\\
&\quad \wedge (\forall c, c' \in \mathrm{C}.\ P(c) \wedge P(c') \supset P(c; c'))\\
&\quad \wedge (\forall b \in \mathrm{B}. \forall c, c' \in C.\ P(c) \wedge P(c') \supset P(\mathbf{if}\ b\ \mathbf{then}\ c\ \mathbf{else}\ c'))\\
&\quad \wedge (\forall b \in \mathrm{B}.\ \forall c \in C.\ P(c) \supset P(\mathbf{while}\ b\ \mathbf{do}\ c))]\\
&\quad \supset \forall c \in \mathrm{C}.\ P(c)
\end{aligned}$$

For an example we prove:

Fact 15 *If v does not occur on the left-hand-side of an assignment in c, then the execution of c cannot affect its value. That is if $\langle c, \sigma \rangle \longrightarrow^* \sigma'$ then $\sigma(v) = \sigma'(v)$.*

PROOF. By SI on commands. The statement of the hypothesis should be apparent from the proof, and is left to the reader.

Case 1 $c = \mathbf{nil}$ Clear.
Case 2 $c = (v' := e)$ Here $v' \neq v$ and we just use the definition of $\sigma[m/v']$.
Case 3 $c = (c_0;\ c_1)$ Here if $\langle c_0; c_1, \sigma \rangle \longrightarrow^* \sigma'$ then for some σ'' we have $\langle c_0, \sigma \rangle \longrightarrow^* \sigma''$ and $\langle c_1, \sigma'' \rangle \longrightarrow^* \sigma'$. (This requires a lemma for proof by the reader).
Then by the induction hypothesis applied first to c_1 and then to c_0 we have:

$$\sigma'(v) = \sigma''(v) = \sigma(v)$$

Case 4 $c = \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1$ Here we easily use the induction hypothesis on c_0 and c_1 (according to the outcome of the evaluation of b).
Case 5 $c = \mathbf{while}\ b\ \mathbf{do}\ c'$ Here we argue on the *length* of the transition sequence $\langle c, \sigma \rangle \longrightarrow \ldots \longrightarrow \sigma'$. This is just an ordinary mathematical induction. In case the sequence has length 0, we have $\sigma' = \sigma$. Otherwise there are two cases according to the result of evaluating b. We just look at the harder one.
Case 5.1 $\langle c, \sigma \rangle \longrightarrow \langle c'; c, \sigma \rangle \longrightarrow \ldots \longrightarrow \sigma_1$. Here we see that $\langle c', \sigma \rangle \longrightarrow^* \sigma_2$ (and apply the main SI hypothesis) and also that $\langle c, \sigma_2 \rangle \longrightarrow^* \sigma_1$ and a shorter transition sequence to which the induction hypothesis can therefore be applied. ■

This particular lemma shows that on occasion we will use other induction principles such as induction on the length of a derivation sequence.

Another possibility is to use induction on some measure of the *size* of the proof of an assertion $\gamma \longrightarrow \gamma'$ (which would, strictly speaking, require a careful definition of the size measure).

Anyway we repeat that we will not develop too much "technology" for making these proofs, but would like the reader to be able, in principle, to check out simple facts.

3.5 Dynamic Errors

In the definition of the operational semantics of L-expressions we allowed configurations of the kind $\langle (5+7)*(10-16), \sigma\rangle$ to stick. Thus, although we did ensure:

$$\gamma \in T \supset \neg\exists\gamma'.\gamma \longrightarrow \gamma'$$

we did not ensure the converse. Implementations of real programming languages will ensure the converse generally by issuing a run-time (= dynamic) error report and forcibly terminating the computation. It would therefore be pleasant if we could also specify dynamic errors.

As a first approximation we add an **error** configuration to the possible configurations of each of the syntactic classes of L. Then we add some **error** rules.

- Expressions
  - · Sum
    4. $\dfrac{\langle e_0, \sigma\rangle \longrightarrow \mathbf{error}}{\langle e_0 + e_1, \sigma\rangle \longrightarrow \mathbf{error}}$
    5. $\dfrac{\langle e_1, \sigma\rangle \longrightarrow \mathbf{error}}{\langle m + e_1, \sigma\rangle \longrightarrow \mathbf{error}}$
  - · Minus
    4,5 as for Sum
    6. $\langle m - m', \sigma\rangle \longrightarrow \mathbf{error}$ (if $m < m'$)
  - · Times
    4,5 as for Sum
- Boolean Expressions
  - · Disjunction
    4,5 as for Sum
  - · Equality
    4,5 as for Sum
  - · Negation
    3. $\dfrac{\langle b, \sigma\rangle \longrightarrow \mathbf{error}}{\langle \sim b, \sigma\rangle \longrightarrow \mathbf{error}}$
- Commands
  - · Assignment
    2. $\dfrac{\langle e, \sigma\rangle \longrightarrow \mathbf{error}}{\langle v := e, \sigma\rangle \longrightarrow \mathbf{error}}$
  - · Composition
    3. $\dfrac{\langle c_0, \sigma\rangle \longrightarrow \mathbf{error}}{\langle c_0; c_1, \sigma\rangle \longrightarrow \mathbf{error}}$

· Conditional

3. $$\frac{\langle b, \sigma\rangle \longrightarrow^* \textbf{error}}{\langle \textbf{if } b \textbf{ then } c \textbf{ else } c', \sigma\rangle \longrightarrow \textbf{error}}$$

· Repetition

3. $$\frac{\langle b, \sigma\rangle \longrightarrow^* \textbf{error}}{\langle \textbf{while } b \textbf{ do } c, \sigma\rangle \longrightarrow \textbf{error}}$$

So the *only* possibility of dynamic errors in L arises from the subtraction of a greater from a smaller. Of course other languages can provide many other kinds of dynamic errors: division by zero, overflow, taking the square root of a negative number, failing dynamic type-checking tests, overstepping array bounds, missing a dangling reference or reaching an uninitialised location etc. etc. But the above simple example does at least indicate a possibility.

Fact 16 *No L-configuration sticks (with the above rules added).*

PROOF. Left to the reader as an exercise. ■

3.6 Simple Type-Checking

We consider a variant, L′, of L in which expressions and Boolean expressions are amalgamated into one syntactic class and have to be sorted out again by type-checking. Here is the language L′.

- Basic Syntactic Sets
  - **Truth-values**: $t \in \mathrm{T}$
  - **Numbers**: $m, n \in \mathrm{N}$
  - **Variables**: $v \in \mathrm{Var} = \{a, b, x, x', x_1, x_2, \ldots\}$
  - **Binary Operations**: $bop \in \mathrm{Bop} = \{+, -, *, =, \textbf{or}\}$
- Derived Syntactic Sets
  - **Expressions**: $e \in \mathrm{Exp}$ where:

$$e ::= m \mid t \mid v \mid e_0 \; bop \; e_1 \mid \sim e$$

  - **Commands**: $c \in \mathrm{Com}$ where:

$$c ::= \textbf{nil} \mid v := e \mid c_0;\ c_1 \mid \textbf{if } e \textbf{ then } c_0 \textbf{ else } c_1 \mid \textbf{while } e \textbf{ do } c$$

Note: We have taken Var to be infinite in the above in order to raise a little problem (later) on how to avoid infinite memories.

Many expressions such as $(\mathrm{tt}+5)$ or ~ 6 now have no sense to them, and nor do such commands as **if** x **or** 5 **then** c_0 **else** c_1. To make sense an expression must have a type, and in L′ there are exactly two possibilities:

- **Types**: $\tau \in \text{Types} = \{\text{nat}, \text{bool}\}$

To see which expressions have types and what they are we will just give some rules for assertions:

$$e : \tau \quad \equiv \quad e \text{ has type } \tau$$

Note first that the basic syntactic sets have, in a natural way, associated type information. Clearly we will have truth-values having type bool, numbers having type nat, variables having type nat and for each binary operation, *bop*, we have a *partial binary function* τ_{bop} on Types:

$+, -, *$	bool	nat
bool	?	?
nat	?	nat

$=$	bool	nat
bool	?	?
nat	?	bool

or	bool	nat
bool	bool	?
nat	?	?

- Rules

Truth-values: $t : \text{bool}$

Numbers: $m : \text{nat}$

Variables: $v : \text{nat}$

Binary Operations: $\dfrac{e_0 : \tau_0 \quad e_1 : \tau_1}{e_0 \; bop \; e_1 : \tau_2}$ (where $\tau_2 = \tau_{bop}(\tau_0, \tau_1)$)

Negation: $\dfrac{e : \text{bool}}{\sim e : \text{bool}}$

Now for commands we need to sort out those commands which are *well-formed* in the sense that all subexpressions have a type and are Boolean when they ought to be. The rules for commands involve assertions:

$$\text{Wfc}(c) \equiv c \text{ is a well-formed command.}$$

Nil: $\text{Wfc}(\mathbf{nil})$

Assignment: $\dfrac{e : \text{nat}}{\text{Wfc}(v := e)}$

Sequencing: $\dfrac{\text{Wfc}(c_0) \quad \text{Wfc}(c_1)}{\text{Wfc}(c_0; c_1)}$

Conditional: $\dfrac{e : \text{bool} \quad \text{Wfc}(c_0) \quad \text{Wfc}(c_1)}{\text{Wfc}(\mathbf{if} \; e \; \mathbf{then} \; c_0 \; \mathbf{else} \; c_1)}$

While: $\dfrac{e : \text{bool} \quad \text{Wfc}(c)}{\text{Wfc}(\mathbf{while} \; e \; \mathbf{do} \; c)}$

Of course all of this is really quite trivial and one could have separated out the Boolean expressions very easily in the first place, as was done with L. However, we will see that the method generalises to the *context-sensitive* aspects, also referred to in the literature as the *static semantics.*

Turning to the dynamic semantics we want now to avoid configurations $\langle c, \sigma\rangle$ with $\sigma : \mathrm{Var} \longrightarrow \mathrm{N}$, as such stores are infinite objects. For we have more or less explicitly indicated that we are doing (hopefully nice) finitary mathematics. The problem is easily overcome by noting that we only need σ to give values for all the variables in C, and there are certainly only finitely many such variables. Consequently for any *finite* subset V of Var we set:

$$\mathrm{Stores}_V = V \longrightarrow \mathrm{N}$$

and take the configurations also to be indexed by V

$$\Gamma_{E,V} = \{\langle e, \sigma\rangle \mid \exists\tau.\ e : \tau, \mathrm{Var}(e) \subseteq V,\ \sigma \in \mathrm{Stores}_V\}$$
$$\Gamma_{C,V} = \{\langle c, \sigma\rangle \mid \mathrm{Wfc}(c), \mathrm{Var}(c) \subseteq V, \sigma \in \mathrm{Stores}_V\} \cup \{\sigma \mid \sigma \in \mathrm{Stores}_V\}$$

where $\mathrm{Var}(e)$ is the set of variables occurring in e. The rules are much the same as before, formally speaking. That is they are the same as before but with the variables and metavariables ranging over the appropriate sets and an added index. So for example in the rule

$$\textbf{Comp 2}\qquad \frac{\langle c_0, \sigma\rangle \longrightarrow_V \sigma'}{\langle c_0;\ c_1, \sigma\rangle \longrightarrow_V \langle c_1, \sigma'\rangle}$$

it is meant that c_0, c_1 (and hence $c_0; c_1$) are well formed commands with their variables all in V and all of the configurations mentioned in the rule are in $\Gamma_{C,V}$.

Equally in the rule

$$\textbf{Sum 1}\qquad \frac{\langle e_0, \sigma\rangle \longrightarrow_V \langle e_0', \sigma\rangle}{\langle e_0 + e_1, \sigma\rangle \longrightarrow_V \langle e_0' + e_1, \sigma\rangle}$$

it is meant that all the expressions $e_0, e_0', e_0 + e_1, e_0' + e_1$ have a type (which must here be nat) and all their variables are in V and all the configurations mentioned in the rule are in $\Gamma_{E,V}$. Thus the rules define families of transition relations, $\longrightarrow_V \subseteq \Gamma_{E,V} \times \Gamma_{E,V}$ for expressions, $\longrightarrow_V \subseteq \Gamma_{C,V} \times \Gamma_{C,V}$ for commands.

In the above we have taken the definition of $\mathrm{Var}(e)$, the variables occurring in e and also of $\mathrm{Var}(c)$ for granted as it is rather obvious what is meant. However, it is easily given by a so-called *definition by structural induction.*

$$\begin{aligned}
\mathrm{Var}(t) &= \mathrm{Var}(m) = \emptyset \\
\mathrm{Var}(v) &= \{v\} \\
\mathrm{Var}(e_0\ \mathit{bop}\ e_1) &= \mathrm{Var}(e_0) \cup \mathrm{Var}(e_1) \\
\mathrm{Var}(\sim e) &= \mathrm{Var}(e)
\end{aligned}$$

With this kind of syntax-directed definition what is meant is that it can easily be shown by SI that the above equations ensure that for any e there is only one V with $\mathrm{Var}(e) = V$. The definition for commands is similar and is left to the reader, the only point of (very slight) interest is the definition of Var($v := e$).

The definition can also be cast in the form of rules for assertions of the form Var(t) = V.

Truth-values: $\mathrm{Var}(t) = \emptyset$

Numbers: $\mathrm{Var}(m) = \emptyset$

Variables $\mathrm{Var}(v) = \{v\}$

Binary Operations: $$\frac{\mathrm{Var}(e_0) = V_0 \quad \mathrm{Var}(e_1) = V_1}{\mathrm{Var}(e_0\ bop\ e_1) = V_0 \cup V_1}$$

Negation: $$\frac{\mathrm{Var}(e) = V}{\mathrm{Var}({\sim} e) = V}$$

Exercise: Give rules for the assertion Var(e) $\subseteq V$.

Finally we have a parametrical form of behaviour. For example for commands we have a partial function:

$$\mathrm{Exec} : C_V \times \mathrm{Stores}_V \longrightarrow \mathrm{Stores}_V$$

where $C_V = \{c \in C \mid \mathrm{Wfc}(c) \wedge \mathrm{Var}(c) \subseteq V\}$, given by:

$$\mathrm{Exec}(c, \sigma) = \sigma' \quad \equiv \quad \langle c, \sigma\rangle \longrightarrow^* \sigma'$$

3.7 Static Errors

The point here is to specify failures in the type-checking mechanism. Here are some rules for a very crude specification where one just adds a new predicate Error.

- Binary Operations

(1) $$\frac{\mathrm{Error}(e_0)}{\mathrm{Error}(e_0\ bop\ e_1)}$$

(2) $$\frac{\mathrm{Error}(e_1)}{\mathrm{Error}(e_0\ bop\ e_1)}$$

(3) $$\frac{e_0 : \tau_0 \quad e_1 : \tau_1}{\mathrm{Error}(e_0\ bop\ e_1)}$$ (if $\tau_{bop}(\tau_0, \tau_1)$ is undefined)

- Negation

$$\frac{\mathrm{Error}(e)}{\mathrm{Error}({\sim} e)}$$

- Assignment

(1) $$\frac{\mathrm{Error}(e)}{\mathrm{Error}(v := e)}$$

(2) $$\frac{e : \mathrm{bool}}{\mathrm{Error}(v := e)}$$

- Sequencing

(1) $$\frac{\text{Error}(c_0)}{\text{Error}(c_0;\ c_1)}$$

(2) $$\frac{\text{Error}(c_1)}{\text{Error}(c_0;\ c_1)}$$

- Conditional

(1) $$\frac{\text{Error}(e)}{\text{Error}(\textbf{if}\ e\ \textbf{then}\ c_0\ \textbf{else}\ c_1)}$$

(2) $$\frac{\text{Error}(c_0)}{\text{Error}(\textbf{if}\ e\ \textbf{then}\ c_0\ \textbf{else}\ c_1)}$$

(3) $$\frac{\text{Error}(c_1)}{\text{Error}(\textbf{if}\ e\ \textbf{then}\ c_0\ \textbf{else}\ c_1)}$$

(4) $$\frac{e : \text{nat}}{\text{Error}(\textbf{if}\ e\ \textbf{then}\ c_0\ \textbf{else}\ c_1)}$$

- While

(1) $$\frac{\text{Error}(e)}{\text{Error}(\textbf{while}\ e\ \textbf{do}\ c)}$$

(2) $$\frac{\text{Error}(c)}{\text{Error}(\textbf{while}\ e\ \textbf{do}\ c)}$$

(3) $$\frac{e : \text{nat}}{\text{Error}(\textbf{while}\ e\ \textbf{do}\ c)}$$

3.8 Exercises

Expressions

1. Try out a few example evaluations.

2. Write down rules for the right-to-left evaluation of expressions, as opposed to the left-to-right evaluation described above.

3. Write down rules for the *parallel* evaluation of expressions, so that the following kind of transition sequence is possible:

$$(1 + (2 + 3)) + ((4 + 5) + 6) \longrightarrow (1 + (2 + 3)) + (9 + 6) \longrightarrow (1 + 5) + (9 + 6)$$
$$\longrightarrow 6 + (9 + 6) \longrightarrow 6 + 15 \longrightarrow 21$$

Here one transition is one action of imaginary processors situated just above the leaves of the expressions (considered as a tree).

4. Note that in the rules if $\langle e, \sigma\rangle \longrightarrow \langle e', \sigma'\rangle$ then $\sigma' = \sigma$. This is the mathematical counterpart of the fact that evaluation of L-expressions produces no side-effects. Rephrase the rules for L-expressions in terms of relations $\sigma \vdash e \longrightarrow e'$ where $\sigma \vdash e \longrightarrow e'$ means that $\langle e, \sigma\rangle \longrightarrow \langle e', \sigma\rangle$ and can be read as "given σ, e reduces to e'".

5. Give rules for "genuine" parallel evaluation where one or more processors as imagined in 3 can perform an action during the same transition. [Hint: Use the idea of exercise 4.]

6. ** Try to develop a method of axiomatising entire derivation sequences. Can you find any advantages for this idea?

Boolean Expressions

7. Can you find various kinds of rules analogous to those for **or** for conjunctions b **and** b'? By the way, the left-sequential construct is often advantageous to avoid array subscripts going out of range as in:

$\textbf{while}\,(i <= n)$ **and** $a[i] <> x$

do $\quad i := i + 3;\ c$

8. Treat the following additions to the syntax

$e ::= \textbf{if } b \textbf{ then } e_0 \textbf{ else } e_1$
$b ::= \textbf{if } b_0 \textbf{ then } b_1 \textbf{ else } b_2$

Presumably you will have given rules for the usual sequential conditional. Can you find and give rules for a parallel conditional analogous to parallel disjunction?

9. Treat the following additions to the syntax which introduce the possibilities of side-effects in the evaluation of expressions:

$e ::= \textbf{begin } c \textbf{ result } e$

(meaning: execute c then evaluate e) and the assignment expression:

$e ::= (v := e)$

where the intention is that the value of $(v := e)$ is the value of e but the assignment also occurs, producing a side-effect in general.

10. Show that the equivalence relations on expressions and boolean expressions are *respected* by the program constructs discussed above so that for example:

a) $e_0 \equiv e_0' \ \wedge\ e_1 \equiv e_1' \quad \supset \quad (e_0 + e_1) \equiv (e_0' + e_1')$

b) $e_0 \equiv e_0' \ \wedge\ e_1 \equiv e_1' \quad \supset \quad (e_0 - e_1) \equiv (e_0' - e_1')$

c) $e_0 \equiv e_0' \ \wedge\ e_1 \equiv e_1' \quad \supset \quad (e_0 = e_1) \equiv (e_0' = e_1')$

d) $b \equiv b' \quad \supset \quad {\sim}b \equiv {\sim}b'$

Commands

11. Give a semantics for the "desk calculator" command

$$v+ := e$$

so that the equivalence

$$(v+ := e) \quad \equiv \quad (v := v + e)$$

holds (and you can prove it!)

12. Give a semantics for the ALGOL-60 assignment command

$$v_1 := (v_2 := \ldots (v_n := e) \ldots)$$

so that (see exercise 9) the equivalence

$$(v_1 := (v_2 := \ldots (v_n := e) \ldots)) \quad \equiv \quad (v_1 := e)$$

where $e = (v_2 := \ldots (v_n := e) \ldots)$ holds, and you can prove it.

13. Treat the simultaneous assignment

$$v_1 := e_1 \textbf{ and } \ldots \textbf{ and } v_n := e_n$$

where the v_i must all be different. Execution of this command consists of first evaluating all the expressions and then performing the assignments.

14. Treat the following variations on the conditional command:

```
if $b$ then $c$ | unless $b$ then $c$ |
        if $b_1$ then $c_1$
        else if $b_2$ then $c_2$
        ⋮
        else if $b_n$ then $c_n$
        else $c_{n+1}$
```

and show they can all be eliminated (to within equivalence) in favour of the ordinary conditional.

15. Treat the simple iteration command

$$\textbf{do } e \textbf{ times } c$$

and the following variations on repetitive commands like **while** b **do** c:

$$\textbf{repeat } c \textbf{ until } b \;\mid\; \textbf{until } b \textbf{ repeat } c \;\mid\; \textbf{repeat } c \textbf{ unless } b \;\mid$$

```
loop
$c_1$
when $b_1$ do $c'_1$ exit
$c_2$
⋮
when $b_n$ do $c'_n$ exit
$c_{n+1}$
repeat
```

where the last construct has n possible exits from the loop.

16. Show that equivalence is respected by the above constructs on commands so that, for example

a) $e \equiv e' \quad \supset \quad (v := e) \equiv (v := e')$

b) $c_0 \equiv c'_0 \wedge c_1 \equiv c'_1 \quad \supset \quad c_0;\ c_1 \equiv c'_0;\ c'_1$

c) $b \equiv b' \wedge c_0 \equiv c'_0 \wedge c_1 \equiv c'_1 \quad \supset \quad$ **if** b **then** c_0 **else** $c_1 \equiv$ **if** b' **then** c'_0 **else** c'_1

d) $b \equiv b' \wedge c \equiv c' \quad \supset \quad$ **while** b **do** $c \equiv$ **while** b' **do** c'

17. Redefine behaviour and equivalence to take account of run-time errors. Do the statements of exercise 16 remain valid?

18. ** Try time and space complexity in the present setting. [Hint: Consider configurations of the form, say, $\langle c, \sigma, t, s \rangle$ where

$t =$ "the total time used so far"
$s =$ "the maximum space used so far"]

There is lots to do. Try finding fairly general definitions, define behaviour and equivalence (approximate equivalence?) and see which program equivalences preserve equivalence. Try looking at measures for the parallel evaluation of expressions. Try to see what is reasonable to incorporate from complexity literature. Can you use the benefits of our structured languages to make standard simulation results easier/nicer for students?

19. ** Try exercises 23 and 24 from Chapter 1 again.

20. Give an operational semantics for L, but where only 1 step of the evaluation of an expression or Boolean expression is needed for 1 step of execution of a command. Which of the two possibilities – the "big steps" of the main text or the "little steps" of the exercise – do you prefer and why?

Proof

21. Let c be any command not involving subexpressions of the form $(e - e')$ or **while** loops but allowing the simple iteration command of exercise 15. Show that any execution sequence $\langle c, \sigma\rangle \longrightarrow^* \ldots$ terminates.

22. Establish (for L) the following "arithmetic" equivalences:

$$\begin{array}{lcl} e_0 + 0 & \equiv & e_0 \\ e_0 + e_1 & \equiv & e_1 + e_0 \\ e_0 + (e_1 + e_2) & \equiv & (e_0 + e_1) + e_2 \\ \text{etc} & & \end{array}$$

Which ones fail if side-effects are allowed in expressions?
Establish the equivalences:

a) **if** b **then** c **else** $c \quad \equiv \quad c$
b) **if** b **then if** b **then** c_0 **else** c' **else if** b **then** c_1 **else** $c_1' \quad \equiv \quad$ **if** b **then** c_0 **else** c_1'
c) **if** b **then if** b' **then** c_0 **else** c_1 **else if** b' **then** c_2 **else** $c_3 \quad \equiv$
if b' **then if** b **then** c_0 **else** c_2 **else if** b **then** c_1 **else** c_3.

Which ones remain true if Boolean expressions have side-effects/need not terminate?

23. Establish or refute each of the following suggested equivalences for the language L (and slight extensions, as indicated):

a) **nil**; $c \quad \equiv \quad c \quad \equiv \quad c$; **nil**

b) c; **if** b **then** c_0 **else** $c_1 \quad \equiv \quad$ **if begin** c **result** b **then** c_0 **else** c_1

c) (**if** b **then** c_0 **else** c_1); $c \quad \equiv \quad$ **if** b **then** $c_0; c$ **else** $c_1; c$

d) **while** b **do** $c \quad \equiv \quad$ **if** b **then** (c; **while** b **do** c) **else nil**

e) **repeat** c **until** $b \quad \equiv \quad c$; **while** $\sim b$ **do** c

Type-Checking

24. Make L′ a little more realistic by adding a type real, decimals, variables of all three types, and a variety of operators. Allow nat to real conversion, but not vice-versa.

25. Show that if $\langle c, \sigma\rangle \longrightarrow \langle c', \sigma'\rangle$ and $x \in Dom(\sigma)\backslash Var(c)$ then $\sigma(x) = \sigma'(x)$.

26. Show that if $\langle c, \sigma\rangle \longrightarrow \langle c', \sigma'\rangle$ is a transition within $\Gamma_{C,V}$ and $\langle c, \overline{\sigma}\rangle \longrightarrow \langle c', \overline{\sigma}'\rangle$ is a transition within $\Gamma_{C,V'}$ where $V \subseteq V'$ then, if $\sigma = \overline{\sigma} \restriction V$, it follows that $\sigma' = \overline{\sigma}' \restriction V$.

27. The static error specification is far too crude. Instead one should have a set M of *messages* and a relation:

$$\text{Error}(e, m) \equiv m \text{ is a report on an error in } e$$

and similarly for commands. Design a suitable M and a specification of Error for L$'$. Try to develop a philosophy of what a nice error message should be. See [Hor] for some ideas.

28. How would you treat dynamic type-checking in L$'$? What would be the new ideas for error messages (presumably one adds an M (see exercise 27) to the configurations).

3.9 Bibliographical Remarks

The idea of reduction sequences originates in the λ-calculus [Hin] as does the present method of specifying steps axiomatically where I was motivated by Barendregt's thesis [Bar1]. I applied the idea to λ-calculus-like programming languages in [Plo1], [Plo2] and Milner saw how to extend it to simple imperative languages in [Mil1]. More recently the idea has been applied to languages for concurrency and distributed systems [Hen1], [Mil2], [Hen2]. The present course is a systematic attempt to apply the idea as generally as possible. A good deal of progress has been made on other aspects of reduction and the λ-calculus, a partial survey and further references can be found in [Ber] and see [Bar2].

Related ideas can be found in work by de Bakker and de Roever. A direct precursor of our method can be found in the work by Lauer and Hoare [Hoa], who use configurations which have the rough form $\langle s_1, \ldots, s_n, \sigma\rangle$ where the s_i are statements (includes commands). They define a next-configuration function and the definition is to some extent syntax-directed. The idea of a syntax-directed approach was independently conceived and mentioned all too briefly in the work of Salwicki [Sal].

Somewhat more distantly various grammatical (= symbol-pushing too) approaches have been tried. For example W-grammars [Cle] and attribute grammars [Mad]; although these definitions are not syntax-directed definitions of single transitions it should be perfectly possible to use the formalisms to write definitions which are. The question is rather how appropriate the formalisms would be with regard to such issues as completeness, clarity (= readability), naturalness, realism, modularity (= modifiability + extensionality). One good discussion of some of these issues can be found in [Mar]. For concern with modularity consult the course notes of Peter Mosses. Our method is clearly intended to be complete and natural and realistic, and we try to be clear; the only point is that it is quite informal, being normal finite mathematics. There must be many questions on good choices of formalism. As regards modularity we just hope that if we get the other things in a reasonable state, then current ideas for imposing modularity on specifications will prove useful.

For examples of good syntax-directed English specifications consult the excellent article by

Ledgard on ten mini-languages [Led]. These languages will provide you with mini-projects which you should find very useful in understanding the course, and which could very well be the basis for more extended projects. For a much more extended example see the ALGOL 68 Report [Wij]. Structural Induction seems to have been introduced to Computer Science by Burstall in [Bur]; for a system which performs automatic proofs by Structural Induction on lists see [Boy]. For discussions of what error messages should be see [Hor] and for remarks on how and whether to specify them see [Mar].

4 Bibliography

[Bar1] Barendregt, H. (1971) *Some Extensional Term Models for Combinatory Logic and Lambda-calculi*, PhD thesis, Department of Mathematics, Utrecht University.

[Bar2] Barendregt, H. (1981) *The Lambda Calculus*, Studies in Logic 103, North-Holland.

[Ber] Berry, G. and Lévy, J-J. *A Survey of Some Syntactic Results in the Lambda-calculus*, Proc. MFCS'79, ed. J. Becvár, LNCS 74, pp. 552–566.

[Boy] Boyer, R.S. and Moore, J.S. (1979) *A Computational Logic*, Academic Press.

[Bur] Burstall, R.M.B. (1969) *Proving Properties of Programs by Structural Induction*, Computer Journal 12(1):41–48.

[Cle] Cleaveland, J.C. and Uzgalis, R.C. (1977) *Grammars for Programming Languages*, Elsevier.

[Hen1] Hennessy, M.C.B. and Plotkin, G.D. (1979) *Full Abstraction for a Simple Parallel Programming Language*, Proc. MFCS'79, ed. J. Becvár, LNCS 74, pp. 108–120.

[Hen2] Hennessy, M.C.B., Li, Wei and Plotkin, G.D. (1981) *A First Attempt at Translating CSP into CCS*, Proc. ICDCS'81, pp. 105–115, IEEE.

[Hin] Hindley, J.R., Lercher, B. and Seldin, J.P. (1972) *Introduction to Combinatory Logic*, Cambridge University Press.

[Hoa] Hoare, C.A.R. and Lauer, P.E. (1974) *Consistent and Complementary Formal Theories of the Semantics of Programming Languages*, Acta Informatica 3:135–153.

[Hor] Horning, J.J. (1974) *What the Compiler Should Tell The User*, Compiler Construction: An Advanced Course, eds F.L. Bauer and J. Eickel, LNCS 21, pp. 525–548.

[Lau] Lauer, P.E. (1971) *Consistent Formal Theories of The Semantics of Programming Languages*, PhD thesis, Queen's University of Belfast, IBM Laboratories Vienna TR 25.121.

[Led] Ledgard, H.F. (1971) *Ten Mini-Languages: A Study of Topical Issues in Programming Languages*, ACM Computing Surveys 3(3):115–146.

[Mad] Madsen, O.L. (1980) *On Defining Semantics by Means of Extended Attribute Grammars*, Semantics-Directed Compiler Generation, ed. N.D. Jones, LNCS 94, pp. 259–299.

[Mar] Marcotty, M., Ledgard, H.F. and von Bochmann, G. (1976) *A Sampler of Formal Definitions*, ACM Computing Surveys 8(2):191-276

[Mil1] Milner, A.J.R.G. (1976) *Program Semantics and Mechanized Proof*, Foundations of Computer Science II, eds K.R. Apt and J.W. de Bakker, Mathematical Centre Tracts 82, pp. 3–44.

[Mil2] Milner, A.J.R.G. (1980) *A Calculus of Communicating Systems*, LNCS 92.

[Plo1] Plotkin, G.D. (1975) *Call-by-name, Call-by-value and the Lambda-calculus*, Theoretical Computer Science 1(2):125–159.

[Plo2] Plotkin, G.D. (1977) *LCF Considered as a Programming Language*, Theoretical Computer Science 5(3):223–255.

[Sal] Salwicki, A. (1976) *On Algorithmic Logic and its Applications*, Mathematical Institute, Polish Academy of Sciences.

[Wij] van Wijngaarden, A., Mailloux, B.J., Peck, J.E.L., Koster, C.H.A., Sintzoff, M., Lindsey, C.H., Meertens, L.G.T. and Fisker, R.G. (1975) *Revised Report on the Algorithmic Language ALGOL 68*, Acta Informatica 5:1–236.

5 Definitions and Declarations

5.1 Introduction

In this chapter we begin the journey towards realistic programming languages by considering binding mechanisms which enable the introduction of new names in local contexts. This leads to definitions of local variables in applicative languages and declarations of constant and variable identifiers in imperative languages. We will distinguish the semantic concepts of environments and stores. The former concerns those aspects of identifiers which do not change throughout the evaluation of expressions or the execution of commands and so on; the latter concerns those aspects which do as in side-effects in the evaluation of expressions or the effects of the execution of commands. In the static semantics context-free methods no longer suffice, and we show how our rules enable the context-sensitive aspects to be handled in a natural and syntax-directed way.

5.2 Simple Definitions in Applicative Languages

We consider a little applicative (= functional) language with simple local definitions of variables. It can be considered as a first step towards full-scale languages like ML [Gor].

- **Syntax Basic Sets**
  Numbers: $m, n \in \mathrm{N}$
  Binary Op.: $bop \in \mathrm{Bop} = \{+, -, *\}$
  Variables: $x, y, z \in \mathrm{Var} = \{x_1, x_2, \ldots\}$
- **Derived Sets**
  Expressions: $e \in \mathrm{Exp}$ where

$$e ::= m \mid x \mid e_0 \ bop \ e_1 \mid \ \mathbf{let} \ x = e_0 \ \mathbf{in} \ e_1$$

Note: Sometimes **let** $x = e_0$ **in** e_1 is written instead as e_1 **where** $x = e_0$. From the point of view of readability the first form is preferable when a bottom-up style is appropriate, and the second where a top-down style is appropriate. For in the first case one first defines x and then uses it, and in the second it is used before being defined.

Clearly any expression contains various occurrences of variables, and in our language there are two kinds of these occurrences. First we have *defining* occurrences where variables are introduced; second we have *applied* occurrences where variables are used. For example, considering the figure below the defining occurrences are 2, 6, 9 and the others are applied. In some languages - but not ours! - one finds other occurrences which can fairly be termed *useless.*

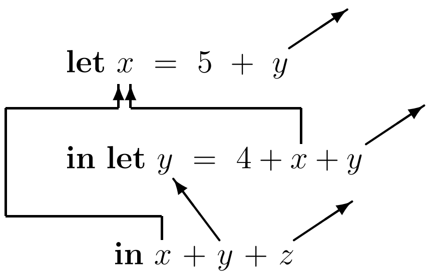
$$\begin{aligned}
&x^1 * (\,\mathbf{let}\ x^2 = 5 * y^3 * x^4\\
&\qquad \mathbf{in}\ x^5 + (\,\mathbf{let}\ y^6 = 14 - x^7\\
&\qquad\qquad \mathbf{in}\ y^8 + (\,\mathbf{let}\ x^9 = 3 + x^{10} + x^{11}\\
&\qquad\qquad\qquad \mathbf{in}\ x^{12} * y^{13})))
\end{aligned}$$

Some Variable Occurrences

Now the region of program text over which defining occurrences have an influence is known as their *scope*. One often says, a little loosely, that, for example, the scope of the first occurrence of x in $e = \mathbf{let}\ x = e_0\ \mathbf{in}\ e_1$ is the expression e_1. But then one considers examples such as that of the above figure, where occurrence 12 is not in the scope of 2 (as it is instead in the scope of 9), this is called a *hole* in the scope of 2. It is more accurate to say that the scope of a defining occurrence is a set of applied occurrences. In the case of $\mathbf{let}\ x = e_0\ \mathbf{in}\ e_1$ the scope of x is all those applied occurrences of x in e_1, which are not in the scope of any defining occurrence of x in e_1. Thus in the case of figure 1 we have the following table showing which applied occurrences are in the scope of which defining occurrences (equivalently which defining occurrences bind which applied occurrences).

Defining Occurrence	Applied Occurrences
2	{5, 7, 10, 11}
6	{8, 13}
9	{12}

Note that each applied occurrence is in the scope of at most one defining occurrence. Those not in any scope are termed *free* (versus *bound*); for example occurrences 1, 3, 4 above are free. One can picture the bindings and the free variables by means of a drawing with arrows such as:



From the point of view of semantics it is irrelevant which identifiers are chosen just so long as the same set of bindings is generated. (Of course a sensible choice of identifiers greatly affects *readability*, but that is not a semantic matter.) All we really need are the arrows, but it is hard to accommodate then into our one-dimensional languages. In the literature on λ-calculus one does find direct attempts to formalise the arrows and also attempts to eliminate variables altogether; as in *Combinatory Logic* [Hin]; in *Dataflow* one sees graphical languages where the graphs display the arrows [Ack].

Static Semantics

Free Variables: The following definition by structural induction is of $\mathrm{FV}(e)$, the set of free variables (= variables with free occurrences) of e:

	m	x	$e_0\ bop\ e_1$	$\mathbf{let}\ x = e_0\ \mathbf{in}\ e_1$
FV	$\emptyset$	$\{x\}$	$\mathrm{FV}(e_0) \cup \mathrm{FV}(e_1)$	$\mathrm{FV}(e_0) \cup (\mathrm{FV}(e_1) \backslash \{x\})$

Example 17

$$\begin{aligned}
&\mathrm{FV}(\mathbf{let}\ x = 5 + y\ \mathbf{in}\ (\ \mathbf{let}\ y = 4 + y + z\ \mathbf{in}\ x + y + z))\\
&= \mathrm{FV}(5 + y) \cup (\mathrm{FV}(\ \mathbf{let}\ y = 4 + x + y\ \mathbf{in}\ x + y + z) \backslash \{x\})\\
&= \{y\} \cup ((\{x, y\} \cup (\{x, y, z\} \backslash \{y\})) \backslash \{x\})\\
&= \{y\} \cup (\{x, y, z\} \backslash \{x\})\\
&= \{y, z\}
\end{aligned}$$

Dynamic Semantics

For the most part applicative languages have no concept of state; there is only the evaluation of expressions in different environments (= semantic contexts). We take:

$$\mathrm{Env}_V = (V \longrightarrow \mathrm{N})$$

for any finite subset of V of the set Var of variables and let ρ range over $\mathrm{Env} = \sum_V \mathrm{Env}_V$ and write $\rho : V$ to mean that ρ is in Env_V. Of course $\mathrm{Env}_V = \mathit{Store}_V$, but we introduce a new notation in order to emphasise the new idea.

The set of configurations is also parameterised on V and

$$\Gamma_V = \{e \in \mathrm{Exp} \mid \mathrm{FV}(e) \subseteq V\}$$
$$\mathrm{T}_V = \mathrm{N}$$

The transition relation is now relative to an environment and for any $\rho : V$ and e, e' in Γ_V we write

$$\rho \vdash_V e \longrightarrow e'$$

and read that in (= given) environment ρ one step of the evaluation of the expression e results in the expression e'. The use of the turnstile is borrowed from formal logic as we wish to think of the above as an assertion of $e \longrightarrow e'$ conditional on ρ which in turn is thought of as an assertion supplied by the environment on the values of the free variables of e and e'. As this environment will not change from step to step of the evaluation of an expression, we will often use, fixing ρ in the transition relation, the transitive reflexive closure $\rho \vdash_V e \longrightarrow^* e'$. It is left to the reader to define *relative* transition systems.

Rules:

Variables:	$\rho \vdash_V x \longrightarrow \rho(x)$
Binary Operations:	(1) $\rho \vdash_V e_0 \longrightarrow e_0' \Rightarrow \rho \vdash_V e_0 \ bop \ e_1 \longrightarrow e_0' \ bop \ e_1$
	(2) $\rho \vdash_V e_1 \longrightarrow e_1' \Rightarrow \rho \vdash_V m \ bop \ e_1 \longrightarrow m \ bop \ e_1'$
	(3) $\rho \vdash_V m \ bop \ m' \longrightarrow n \qquad (\text{where } n = m \ bop \ m')$

Note: To save space we are using an evident horizontal lay-out for our rules. That is the rule:

$$\frac{A_1 \ \ldots\ldots \ A_k}{A}$$

can alternatively be written in the form

$$A_1, \ldots\ldots, A_k \Rightarrow A.$$

Definition 18 *Informally, to evaluate $e =$* **let** $x = e_0$ **in** e_1 *given ρ*

(1) Evaluate e_0 given ρ to get the value m_0.
(2) Change from ρ to $\rho' = \rho[m_0/x]$.
(3) Evaluate e_1 given ρ' to get the value m.

Then m is the value of e given ρ.

The rules for one step of the evaluation are:

$$(1) \quad \frac{\rho \vdash_V e_0 \longrightarrow e_0'}{\rho \vdash_V \ \mathbf{let}\ x = e_0 \ \mathbf{in}\ e_1 \longrightarrow \ \mathbf{let}\ x = e_0' \ \mathbf{in}\ e_1}$$

$$(2) \quad \frac{\rho[m/x] \vdash_{V \cup \{x\}} e_1 \longrightarrow e_1'}{\rho \vdash_V \ \mathbf{let}\ x = m \ \mathbf{in}\ e_1 \longrightarrow \ \mathbf{let}\ x = m \ \mathbf{in}\ e_1'}$$

$$(3) \quad \rho \vdash_V \ \mathbf{let}\ x = m \ \mathbf{in}\ n \longrightarrow \ n$$

Of course these rules are just a clearer version of those given in Chapter 2 for expressions (as suggested in exercise 4). Continuing the logical analogy our rules look like a Gentzen system of natural deduction [Pra] written in a linear way. Possible definitions of behaviour are left to the reader.

5.3 Compound Definitions

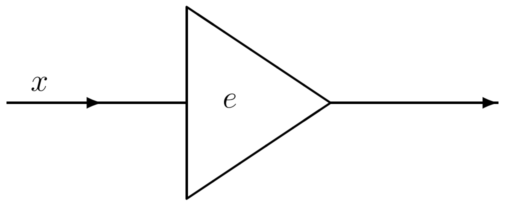
In general it is not convenient just to repeat simple definitions, and so we consider several ways of putting definitions together. The category of expressions is now:

$$e ::= m \mid x \mid e_0 \ bop \ e_1 \mid \textbf{let} \ d \ \textbf{in} \ e$$

where d ranges over the category Def of *definitions* where:

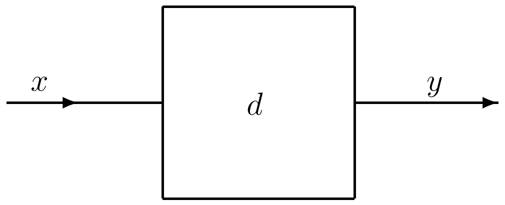
$$d ::= \textbf{nil} \mid x = e \mid d_0; d_1 \mid d_0 \ \textbf{and} \ d_1 \mid d_0 \ \textbf{in} \ d_1$$

To understand this it is convenient to think in terms of *import* and *export*. An *expression*, e, *imports* values for its free variables from its environment (and produces a value). This can be pictured as:



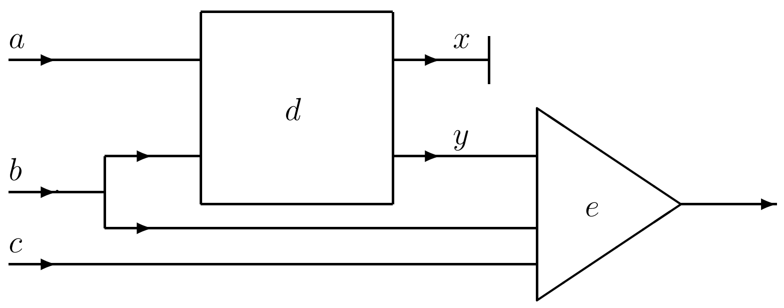
An Expression

where x is a typical free variable of e. A *definition*, d, *imports* values for its free variables and exports values for its defining variables (those with defining occurrences). This can be pictured as:



A Definition

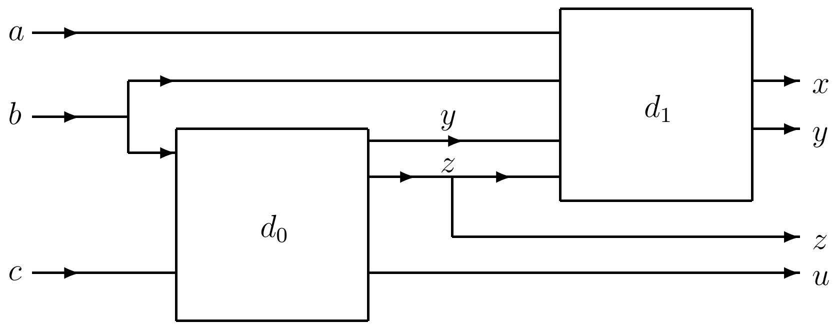
These are *dataflow diagrams* and they also help explain compound expressions and definition. For example a *definition block* **let** d **in** e imports from its environment into d and then d exports into e with any other needed imports of e coming from the block environment. Pictorially



A Definition Block

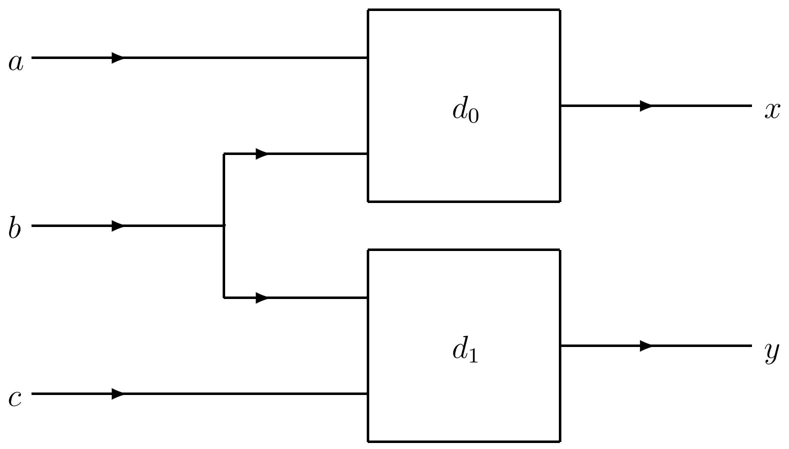
Here a is a typical variable imported by d but not e, and b is one imported by d and e, and c is one imported by e and not d; again x is a variable exported by d and not imported by e (useless but logically possible), and y is a variable exported by d and imported by e. Of course we later give a precise explanation of all this by formal rules of an operational semantics.

Turning to compound definitions we have *sequential* definition, $d_0; d_1$, and *simultaneous* definitions, d_0 **and** d_1, and *private* definitions, d_0 **in** d_1. What $d_0; d_1$ does is import from the environment into d_0 and export from d_0 into d_1 (with any additional exports needed for d_1 being taken from the environment); then $d_0; d_1$ exports from both d_0 and d_1 with the latter taking precedence for common exports. Pictorially (and we need a picture!):



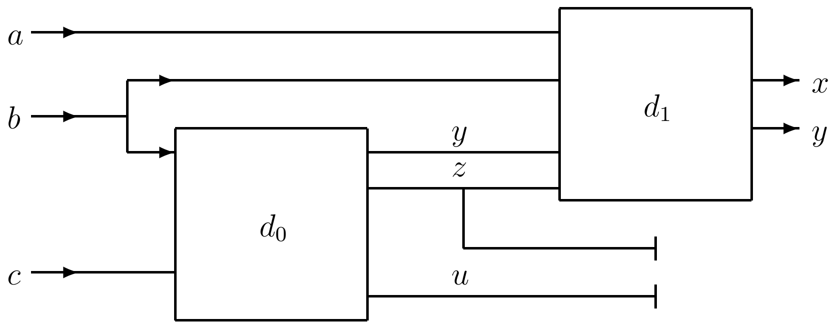
Sequential Definition

Simultaneous definition is much simpler; d_0 **and** d_1 imports into both d_0 and d_1 from the environment and then exports from both (and there must be no common defined variable). Pictorially



Simultaneous Definition

Finally, a private definition d_0 **in** d_1 is just like a sequential one, except that the *only* exports are from d_1. It can be pictured as:



Private Definition

We may write also d_0 **in** d_1 as **let** d_0 **in** d_1 or as **private** d_0 **within** d_1. Private definitions provide examples of blocks where the body is a definition. We have already seen blocks with expression bodies and will see ones with command bodies. Tennent's *Principle of Qualification* says that in principle any semantically meaningful syntactic class can be the body of a block [Ten]. We shall later encounter other examples of helpful organisational principles.

As remarked in [Ten] many programming languages essentially force one construct to do jobs better done by several; for instance it is common to try to get something of the effect of both sequential and simultaneous definition. A little thought should convince the reader that there are essentially just the three interesting ways of putting definitions together.

Example 19 *Consider the expression*

let $x = 3$

in let $x = 5 \,\&\, y = 6 * x$

  in $x + y$

Depending on whether & is ; or **and** *or* **in**, *the expression has the values* $35 = 5 + (6 * 5)$ *or* $23 = 5 + (6 * 3)$ *or* $33 = 3 + (6 * 5)$.

Static Semantics

We will define the set $\mathrm{DV}(d)$ of *defined variables* of a definition d and also $\mathrm{FV}(d/e)$, the set of *free variables* of a definition d or expression e.

	nil	$x = e$	$d_0; d_1$	d_0 **and** d_1	d_0 **in** d_1
DV	$\emptyset$	$\{x\}$	$\mathrm{DV}(d_0) \cup \mathrm{DV}(d_1)$	$\mathrm{DV}(d_0) \cup \mathrm{DV}(d_1)$	$\mathrm{DV}(d_1)$
FV	$\emptyset$	$\mathrm{FV}(e)$	$\mathrm{FV}(d_0) \cup (\mathrm{FV}(d_1) \backslash \mathrm{DV}(d_0))$	$\mathrm{FV}(d_0) \cup \mathrm{FV}(d_1)$	$\mathrm{FV}(d_0) \cup (\mathrm{FV}(d_1) \backslash \mathrm{DV}(d_0))$

For expressions the definition of free variables is the same as before except for the case

$$\mathrm{FV}(\textbf{let } d \textbf{ in } e) = \mathrm{FV}(d) \cup (\mathrm{FV}(e) \backslash \mathrm{DV}(d))$$

Because of the restriction on simultaneous definitions not all expressions or definitions are well-formed - for example consider **let** $x = 3$ **and** $x = 6$ **in** x. So we also define the well-formed ones by means of rules for a predicate $\mathrm{W}(d/e)$ on definitions and expressions.

Rules:

- **Definitions**

Nil:	$\mathrm{W}(\textbf{nil})$	
Simple:	$\mathrm{W}(e) \Rightarrow \mathrm{W}(x = e)$	
Sequential:	$\mathrm{W}(d_0), \mathrm{W}(d_1) \Rightarrow \mathrm{W}(d_0; d_1)$	
Simultaneous:	$\mathrm{W}(d_0), \mathrm{W}(d_1) \Rightarrow \mathrm{W}(d_0 \textbf{ and } d_1)$	(if $\mathrm{DV}(d_0) \cap \mathrm{DV}(d_1) = \emptyset$)
Private:	$\mathrm{W}(d_0), \mathrm{W}(d_1) \Rightarrow \mathrm{W}(d_0 \textbf{ in } d_1)$	

- **Expressions**

Constants:	$\mathrm{W}(m)$
Variables:	$\mathrm{W}(x)$
Binary Op.:	$\mathrm{W}(e_0), \mathrm{W}(e_1) \Rightarrow \mathrm{W}(e_0 \textit{ bop } e_1)$

Definitions: $\quad \mathrm{W}(d), \mathrm{W}(e) \Rightarrow \mathrm{W}(\textbf{let } d \textbf{ in } e)$

Dynamic Semantics

It is convenient to introduce some new notation to handle environments. For purposes of displaying environments consider, for example, $\rho : \{x, y, z\}$, where $\rho(x) = 1$, $\rho(y) = 2$, $\rho(z) = 3$. We will also write ρ as $\{x = 1, y = 2, z = 3\}$ and drop the set brackets when desired; this situation makes it clearer that environments can be thought of as assertions.

Next for any V_0, V_1 and $\rho_0{:}V_0$, $\rho_1{:}V_1$ we define $\rho = \rho_0[\rho_1]{:}V_0 \cup V_1$ by:

$$\rho(x) = \begin{cases} \rho_1(x) & (x \in V_1) \\ \rho_0(x) & (x \in V_0 \backslash V_1) \end{cases}$$

We now have the nice $\rho[x = m]$ to replace the less readable $\rho[m/x]$. Finally for any $\rho_0{:}V_0$, $\rho_1{:}V_1$ with $V_0 \cap V_1 = \emptyset$ we write ρ_0, ρ_1 for $\rho_0 \cup \rho_1$. Of course this is equal to $\rho_0[\rho_1]$, and also to $\rho_1[\rho_0]$, but the extra notation makes it clear that it is required that $V_0 \cap V_1 = \emptyset$.

The expression configurations are parameterised on V by:

$$\Gamma_V = \{e \mid \mathrm{W}(e),\ \mathrm{FV}(e) \subseteq V\}$$

and of course

$$\mathrm{T}_V = \mathrm{N}$$

And our transition relation, $\rho \vdash_V e \longrightarrow e'$, is defined only for $\rho : V$, and e, e' in Γ_V.

For definitions the idea is that just as an expression is evaluated to yield values so is a definition *elaborated* to yield a "little" environment (for its defined variables). For example, given $\rho = \{x = 1, y = 2, z = 3\}$ the definition $x = 5 + x + z$; $y = x + y + z$ is elaborated to yield $\{x = 9, y = 14\}$. In order to make this work we add another clause to the definition of Def

$$d ::= \rho$$

What this means is that the abstract syntax of declaration configurations allows environments; it does not mean that the abstract syntax of declarations does so.

In a sense we slipped a similar trick in under the carpet when we allowed numbers as expressions. Strictly speaking we should only have allowed literals and then allowed natural numbers as part of the configurations and given rules for evaluating literals to numbers. Similar statements hold for other kinds of literals. However, there seemed little point in forcing the reader through this tedious procedure.

Returning to definitions we now add clauses for free and defined variables:

$$\begin{aligned}&\mathrm{FV}(\rho) = \emptyset\\ &\mathrm{DV}(\rho) = V \qquad (\text{if } \rho : V)\end{aligned}$$

and also add for any ρ that $\mathrm{W}(\rho)$ holds, and for any V that

$$\Gamma_V = \{d \mid \mathrm{W}(d),\ \mathrm{FV}(d) \subseteq V\}$$

and

$$\mathrm{T}_V = \{\rho\}$$

and consider for V and $\rho : V$ and $d, d' \in \Gamma_V$ the transition relation

$$\rho \vdash_V d \longrightarrow d'$$

which means that, given ρ, one step of the elaboration of d yields d'.

Example 20 *We shall expect to see that:*

$$\begin{aligned}x = 1, y = 2, z = 3 \vdash x = (5 + x) + z; y = (x + y) + z\\ \longrightarrow^* \{x = 9\}; y = (x + y) + z\\ \longrightarrow^* \{x = 9\}; \{y = 14\}\\ \longrightarrow \ \{x = 9, y = 14\}\end{aligned}$$

Rules:

- **Expressions**: As before but with a change for definitions:
  Definitions: Informally, to evaluate $e_1 = \mathbf{let}\ d\ \mathbf{in}\ e_0$ in the environment ρ

(1) Elaborate d in ρ yielding ρ_0.
(2) Change from ρ to $\rho' = \rho[\rho_0]$.
(3) Evaluate e_0 in ρ' yielding m.
Then the evaluation of e_1 yields m. Formally we have:

(1) $$\frac{\rho \vdash_V d \longrightarrow d'}{\rho \vdash_V \ \mathbf{let}\ d\ \mathbf{in}\ e \longrightarrow \ \mathbf{let}\ d'\ \mathbf{in}\ e}$$

(2) $$\frac{\rho[\rho_0] \vdash_{V \cup V_0} e \longrightarrow e'}{\rho \vdash_V \ \mathbf{let}\ \rho_0\ \mathbf{in}\ e \longrightarrow \ \mathbf{let}\ \rho_0\ \mathbf{in}\ e'} \qquad (\text{where } \rho_0 : V_0)$$

(3) $\rho \vdash_V \ \mathbf{let}\ \rho_0\ \mathbf{in}\ m \longrightarrow m$

- **Definitions**: The first two cases are self-explanatory.

Nil:	$\rho \vdash_V \mathbf{nil} \longrightarrow \emptyset$
Simple:	(1) $\rho \vdash_V e \longrightarrow e' \quad \Rightarrow \quad \rho \vdash_V x = e \longrightarrow x = e'$
	(2) $\rho \vdash_V x = m \longrightarrow \{x = m\}$

Sequential: Informally to elaborate $d_0; d_1$ given ρ

(1) Elaborate d_0 in ρ yielding ρ_0

(2) Elaborate d_1 in $\rho[\rho_0]$ yielding ρ_1

Then the elaboration of $d_0; d_1$ yields $\rho_0[\rho_1]$. Formally we have:

(1) $$\frac{\rho \vdash_V d_0 \longrightarrow d_0'}{\rho \vdash_V d_0; d_1 \longrightarrow d_0'; d_1}$$

(2) $$\frac{\rho[\rho_0] \vdash_{V \cup V_0} d_1 \longrightarrow d_1'}{\rho \vdash_V \rho_0; d_1 \longrightarrow \rho_0; d_1'} \qquad \text{(where } \rho_0 : V_0\text{)}$$

(3) $\rho \vdash_V \rho_0; \rho_1 \longrightarrow \rho_0[\rho_1]$

Simultaneous: Informally to elaborate d_0 **and** d_1 given ρ

(1) Elaborate d_0 in ρ yielding ρ_0.

(2) Elaborate d_1 in ρ yielding ρ_1.

Then the elaboration of d_0 **and** d_1 yields ρ_0, ρ_1 if that is defined. Formally

(1) $\rho \vdash_V d_0 \longrightarrow d_0' \quad \Rightarrow \quad \rho \vdash_V d_0 \textbf{ and } d_1 \longrightarrow d_0' \textbf{ and } d_1$

(2) $\rho \vdash_V d_1 \longrightarrow d_1' \quad \Rightarrow \quad \rho \vdash_V \rho_0 \textbf{ and } d_1 \longrightarrow \rho_0 \textbf{ and } d_1'$

(3) $\rho \vdash_V \rho_0 \textbf{ and } \rho_1 \longrightarrow \rho_0, \rho_1$

Private: Informally to elaborate d_0 **in** d_1 given ρ

(1) Elaborate d_0 in ρ yielding ρ_0.

(2) Elaborate d_1 in $\rho[\rho_0]$ yielding ρ_1.

Then the elaboration of d_0 **in** d_1 yields ρ_1. Formally

(1) $\rho \vdash_V d_0 \longrightarrow d_0' \quad \Rightarrow \quad \rho \vdash_V d_0 \textbf{ in } d_1 \longrightarrow d_0' \textbf{ in } d_1$

(2) $\rho[\rho_0] \vdash_{V \cup V_0} d_1 \longrightarrow d_1' \quad \Rightarrow \quad \rho \vdash_V \rho_0 \textbf{ in } d_1 \longrightarrow \rho_0 \textbf{ in } d_1'$
(where $\rho_0 : V_0$)

(3) $\rho \vdash_V \rho_0 \textbf{ in } \rho_1 \longrightarrow \rho_1$

Example 21

$$\begin{aligned}
x = 1, y = 2, z = 3 \vdash x = (5 + x) + z; y = (x + y) + z & \\
\overset{SEQ1}{\longrightarrow}\ x = (5 + 1) + z; y = (x + y) + z & \quad \textit{(using SIM1)} \\
\overset{SEQ1}{\longrightarrow}\ x = 9; y = (x + y) + z & \quad \textit{(using SIM1)} \\
\overset{SEQ1}{\longrightarrow}\ \{x = 9\}; y = (x + y) + z & \quad \textit{(using SIM2)} \\
\overset{SEQ2}{\longrightarrow}\ \{x = 9\}; y = (9 + y) + z & \\
\overset{SEQ2}{\longrightarrow}\ \{x = 9\}; \{y = 14\} & \\
\overset{SEQ3}{\longrightarrow}\ \{x = 9, y = 14\}. &
\end{aligned}$$

The reader is encouraged here (and generally too) to work out examples for all the other constructs.

New problems arise in static semantics when we consider type-checking and definitions. For example one cannot tell whether or not such an expression as x **or** tt or $x + x$ is well-typed without knowing what the type of x is and that depends on the context of its occurrence. We will be able to solve these problems by introducing static environments α to give this type information and giving rules to establish properties of the form

$$\alpha \vdash_V e : \tau$$

As usual we work by considering an example language.

- **Basic Sets**

Types:	$\tau \in \text{Types} = \{\text{nat}, \text{bool}\}$
Numbers:	$m, n \in \text{N}$;
Truth-values:	$t \in \text{T}$;
Variables:	$x, y, z \in \text{Var}$;
Binary Operations:	$\mathit{bop} \in \text{Bop} = \{+, -, *, =, \textbf{or}\}$.

- **Derived Sets**

Constants: $\mathit{con} \in \text{Con}$ where $\mathit{con} ::= m \mid t$

Definitions: $d \in \text{Def}$ where

$$d ::= \textbf{nil} \mid x : \tau = e \mid d_0; d_1 \mid d_0 \textbf{ and } d_1 \mid d_0 \textbf{ in } d_1$$

Expressions: $e \in \text{Exp}$ where

$$e ::= \mathit{con} \mid x \mid {\sim}e \mid e_0 \; \mathit{bop} \; e_1 \mid \textbf{if } e_0 \textbf{ then } e_1 \textbf{ else } e_2 \mid \textbf{let } d \textbf{ in } e$$

Static Semantics

The definitions of DV(d) and FV(d) are as before as is FV(e) just adding that

$$\text{FV}(\textbf{if } e_0 \textbf{ then } e_1 \textbf{ else } e_2) = \text{FV}(e_0) \cup \text{FV}(e_1) \cup \text{FV}(e_2)$$

We now need *type environments* over V. These form the set

$$\text{TEnv}_V = V \longrightarrow \text{Types}$$

and the set $\text{TEnv}_V = \sum_V \text{TEnv}_V$ is ranged over by α and β and we write $\alpha : V$ for $\alpha \in \text{TEnv}_V$. Of course all the notation $\alpha[\beta]$ and α, β extends without change from ordinary environments to type environments.

Now for every V and $\alpha{:}V$, τ and e with $\mathrm{FV}(e) \subseteq V$ we give rules for the relation

$$\alpha \vdash_V e : \tau$$

meaning that given α the expression e is well-formed and has type τ. This will involve us in giving similar rules for constants and also for every V and $\alpha : V$, β and definition d with $\mathrm{FV}(d) \subseteq V$, for the relation

$$\alpha \vdash_V d : \beta$$

meaning that given α the definition d is well-formed and yields the type environment β.

Example 22 *(1)* $y = \mathrm{bool} \vdash (\textbf{let } x : \mathrm{nat} = 1 \textbf{ in } (x = x) \textbf{ or } y) : \mathrm{bool}$
(2) $y = \mathrm{bool} \vdash (x : \mathrm{nat} = \textbf{if } y \textbf{ then } 0 \textbf{ else } 1; y : \mathrm{nat} = x + 1) : \{x = \mathrm{nat}, y = \mathrm{nat}\}$

Rules:

- **Constants:**
  - **Numbers:** $\alpha \vdash_V m : \mathrm{nat}$
  - **Truth-values:** $\alpha \vdash_V t : \mathrm{bool}$
- **Expressions:**
  - **Constants:** $\alpha \vdash_V \mathit{con} : \tau \quad \Rightarrow \quad \alpha \vdash_V \mathit{con} : \tau$ (this makes sense!)
  - **Variables:** $\alpha \vdash_V x : \alpha(x)$
  - **Negation:** $\alpha \vdash_V e : \mathrm{bool} \quad \Rightarrow \quad \alpha \vdash_V {\sim} e : \mathrm{bool}$
  - **Binary Operations:** $\dfrac{\alpha \vdash_V e_0 : \tau_0 \quad \alpha \vdash_V e_1 : \tau_1}{\alpha \vdash_V e_0 \; \mathit{bop} \; e_1 : \tau}$ (if $\tau = \tau_0 \; \tau_{bop} \tau_1$)
  - **Conditional:** $\alpha \vdash_V e_0 : \mathrm{bool}, \alpha \vdash_V e_1 : \tau, \alpha \vdash_V e_2 : \tau$

    $\Rightarrow \quad \alpha \vdash_V \textbf{ if } e_0 \textbf{ then } e_1 \textbf{ else } e_2 : \tau$
  - **Definition:** $\dfrac{\alpha \vdash_V d : \beta \quad \alpha[\beta] \vdash_{V \cup V_0} e : \tau}{\alpha \vdash_V \textbf{let } d \textbf{ in } e : \tau}$ (where $\beta : V_0$)

Note that this allows the type of variables to be redefined.

Definition 23

Nil: $\alpha \vdash_V \textbf{nil} : \emptyset$

Simple: $\alpha \vdash_V e : \tau \quad \Rightarrow \quad \alpha \vdash_V (x : \tau = e) : \{x = \tau\}$

Sequential: $\dfrac{\alpha \vdash_V d_0 : \beta_0 \quad \alpha[\beta_0] \vdash_{V \cup V_0} d_1 : \beta_1}{\alpha \vdash_V (d_0; d_1) : \beta_0[\beta_1]}$ *(where $\beta_0 : V_0$)*

Simultaneous: $\dfrac{\alpha \vdash_V d_0 : \beta_0 \quad \alpha \vdash_V d_1 : \beta_1}{\alpha \vdash_V (d_0 \textbf{ and } d_1) : \beta_0, \beta_1}$ *(if* $\mathrm{DV}(d_0) \cap \mathrm{DV}(d_1) = \emptyset$)

Private: $\dfrac{\alpha \vdash_V d_0 : \beta_0 \quad \alpha[\beta_0] \vdash_{V \cup V_0} d_1 : \beta_1}{\alpha \vdash_V (d_0 \textbf{ in } d_1) : \beta_1}$ *(where $\beta_0 : V_0$)*

It is hoped that these rules are self-explanatory. It is useful to define for any V and $\alpha : V$ and e with $\mathrm{FV}(e) \subseteq V$ the property of being well-formed

$$\mathrm{W}_V(e, \alpha) \equiv \exists \tau.\ \alpha \vdash_V e : \tau$$

and also for any V, $\alpha : V$ and d with $\mathrm{FV}(d) \subseteq V$ the property of being well-formed

$$\mathrm{W}_V(d, \alpha) \equiv \exists \beta.\ \alpha \vdash_V d : \beta.$$

Dynamic Semantics

If x has type τ in environment α then in the corresponding ρ it should be the case that $\rho(x)$ also has type τ; that is if $\tau = \text{nat}$, then we should have $\rho(x) \in \mathrm{N}$ and otherwise $\rho(x) \in \mathrm{T}$. To this end for any V and $\alpha : V$ and $\rho : V \longrightarrow \mathrm{N} + \mathrm{T}$ we define:

$$\begin{aligned}\rho : \alpha \equiv \forall x \in V.\ &(\alpha(x) = \text{nat} \ \supset \rho(x) \in \mathrm{N}) \\ &\wedge (\alpha(x) = \text{bool} \ \supset \rho(x) \in \mathrm{T})\end{aligned}$$

and put $\mathrm{Env}_\alpha = \{\rho : V \longrightarrow \mathrm{N} + \mathrm{T} \mid \rho : \alpha\}$. Note that if $\rho_0 : \alpha_0$ and $\rho_1 : \alpha_1$ then $\rho_0[\rho_1] : \alpha_0[\alpha_1]$ and so too that (if it makes sense) $(\rho_0, \rho_1) : (\alpha_0, \alpha_1)$.

Configurations: We separate out the various syntactic categories according to the possible type environments.

- **Expressions:** For every $\alpha : V$ we put $\Gamma_\alpha = \{e \mid W_V(e, \alpha)\}$ and $\mathrm{T}_\alpha = \mathrm{N} + \mathrm{T}$.
- **Definitions:** We add the production $d ::= \rho$ as before (but with ρ ranging over the Env_α) and then for every $\alpha : V$ we put $\Gamma_\alpha = \{d \mid \mathrm{W}_V(d, \alpha)\}$ and $\mathrm{T}_\alpha = \{\rho\}$.

Transition Relations:

- **Expressions:** For every $\alpha : V$ we have the relation where $\rho : \alpha$ and $e, e' \in \Gamma_\alpha$:

$$\rho \vdash_\alpha e \longrightarrow e'$$

- **Definitions:** For every $\alpha : V$ we have the relation where $\rho : \alpha$ and $d, d' \in \Gamma_\alpha$:

$$\rho \vdash_\alpha d \longrightarrow d'$$

Rules: The rules are much as usual but with the normal constraints that all mentioned expressions and definitions be configurations and environments be of the right type-environment. Here are three examples which should make the others obvious.

- **Expressions**:

Definition 2: $$\frac{\rho[\rho_0] \vdash_{\alpha[\alpha_0]} e \longrightarrow e'}{\rho \vdash_\alpha \ \textbf{let}\ \rho_0\ \textbf{in}\ e \longrightarrow \textbf{let}\ \rho_0\ \textbf{in}\ e'} \qquad (\text{where } \rho_0 : \alpha_0)$$

- **Definitions**:

  Simple 2: $\rho \vdash_\alpha x = con \longrightarrow \{x = con\}$

  Sequential 2: $\dfrac{\rho[\rho_0] \vdash_{\alpha[\alpha_0]} d_1 \longrightarrow d_1'}{\rho \vdash_\alpha \rho_0; d_1 \longrightarrow \rho_0; d_1'}$ (where $\rho_0 : \alpha_0$)

Example 24

$$\begin{aligned}
\{x = \mathrm{tt}, y = 5\} \vdash_{\{x=\mathrm{bool}, y=\mathrm{nat}\}} & \ \mathbf{let\ private}(x : \mathrm{nat} = 1 \ \mathbf{and}\ y : \mathrm{nat} = 2) \\
& \ \mathbf{within}\ z : \mathrm{nat} = x + y \\
& \ \mathbf{in\ if}\ x\ \mathbf{then}\ y + z\ \mathbf{else}\ y \\
\longrightarrow^3 & \ \mathbf{let\ private}\ \{x = 1, y = 2\} \\
& \ \mathbf{within}\ z : \mathrm{nat} = x + y \\
& \ \mathbf{in\ if}\ x\ \mathbf{then}\ y + z\ \mathbf{else}\ y \\
\longrightarrow^4 & \ \mathbf{let\ private}\ \{x = 1, y = 2\} \\
& \ \mathbf{within}\ \{z = 3\} \\
& \ \mathbf{in\ if}\ x\ \mathbf{then}\ y + z\ \mathbf{else}\ y \\
\longrightarrow & \ \mathbf{let}\ \{z = 3\}\ \mathbf{in\ if}\ x\ \mathbf{then}\ y + z\ \mathbf{else}\ y \\
\longrightarrow^2 & \ \mathbf{let}\ \{z = 3\}\ \mathbf{in}\ y + z \\
\longrightarrow^4 & \ 8.
\end{aligned}$$

Declarations in Imperative Languages

The ideas so far developed transfer to imperative languages where we will speak of declarations (of identifiers) rather than definitions (of variables). Previously we have used stores for imperative languages and environments for applicative ones, although mathematically they are the same - associations of values to identifiers/variables. It now seems appropriate, however, to use both environments and stores; the former shows what does not vary and the latter what does vary when commands are executed.

It is also very convenient to change the definitions of stores by introducing an (arbitrary) infinite set, Loc, of locations (= references = cells) and taking for any $L \subseteq \mathrm{Loc}$

$$\mathrm{Stores}_L = L \longrightarrow \mathrm{Values}$$

and

$$\mathrm{Stores} = \sum_L \mathrm{Stores}_L \qquad (= \mathrm{Loc} \longrightarrow_{\mathrm{fin}} \mathrm{Values})$$

and putting

$$\mathrm{Env} = \mathrm{Id} \longrightarrow_{\mathrm{fin}} (\mathrm{Values} + \mathrm{Loc})$$

The idea is that if in some environment ρ we have an identifier x whose values should not vary then $\rho(x)$ = that value; otherwise $\rho(x)$ is a location, l, and given a store $\sigma : L$ (with l in L) then $\sigma(l)$ is the value held in the location l (its *contents*). In the first case we talk of *constant* identifiers and in the second we talk of *variable* identifiers. The former are introduced by constant declarations like

$$\mathbf{const}\ \ x = 5$$

and the latter by variable declarations like

$$\mathbf{var}\ \ x = 5$$

In all cases declarations will produce new (little) environments, just as before. The general form of transitions will be:

$$\rho \vdash_l \langle d, \sigma\rangle \longrightarrow \langle d', \sigma'\rangle$$

where ρ is the elaboration environment and σ, σ' are the *stores*. So, for example we will have

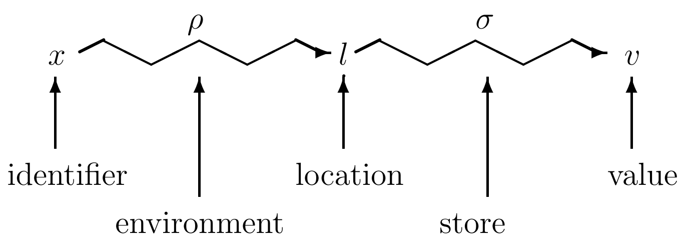
$$\rho \vdash_l \langle \mathbf{const}\ x = 5, \sigma\rangle \longrightarrow \langle \{x = 5\}, \sigma\rangle$$

and

$$\rho \vdash_l \langle \mathbf{var}\ x = 5, \sigma\rangle \longrightarrow \langle \{x = l\}, \sigma[l = 5]\rangle \qquad (*)$$

where l is a certain "new" location.

Locations can be thought of as "abstract addresses" where we do not really want to commit ourselves to any machine architecture, but only to the needed logical properties. A better way to think of a location is as an *individual* or *object* which has *lifetime* (= extent); it is created in a transition such as $(*)$ and its lifetime continues either throughout the entire computation (execution sequence) or until it is *deleted* (= disposed of) (the deletion being achieved either through such mechanisms as block exit or through explicit storage management primitives in the language). Throughout its lifetime it has a (varying) contents, generally an ordinary mathematical value (or perhaps other locations). It is generally referred to by some identifier and is then said to be the *L-value* (or left-hand value) of the identifier and its contents, in some state, is the *R-value* (right-hand value) of the identifier, in that state. The lifetime of the location is related to, but logically distinct from the scope of the identifier. Thus we have a two-level picture



The L/R value terminology comes from considering assignment statements

$$x := y$$

where on the left we think of the variable as referring to a location and on the right as referring to a value. Indeed we analyse the effect of assignment as changing the contents of the location to the R-value of y:

$$\rho \vdash \langle x := y, \sigma\rangle \longrightarrow \sigma[\rho x = \sigma(\rho y)]$$

This is of course a more complicated analysis of assignment than in Chapter 2. The L/R terminology is a little inappropriate in that some programming languages write their assignments in the opposite order and also in that not all occurrences on the left of an assignment are references to L-values.

The general idea of locations and separation of environments and stores comes from the Scott-Strachey tradition (e.g., [Gor,Ten,Led]); it is also reminiscent of ideas of individuals in modal logic [Hug]. In fact we do not need locations for most of the problems we encounter in the rest of this chapter (see exercise 26) but they will provide a secure foundation for later concepts such as

- Static binding of the same global variables in different procedure bodies (storage sharing).
- Call-by-reference (aliasing problems).
- Arrays (location expressions).
- Reference types (anonymous references).

On the other hand it would be interesting to see how far one can get without locations and to what extent programming languages would suffer from their excision (see [Don][Rey]). One can argue that it is the concept of location that distinguishes imperative from applicative languages.

We now make all this precise by considering a suitable mini-language.

Syntax:

- **Basic Sets**:

Types:	$\tau \in Types = \{\text{bool}, \text{nat}\}$
Numbers:	$m, n \in \mathrm{N}$
Truth-values:	$t \in \mathrm{T}$

Binary Operations: $bop \in$ Bop

- **Derived Sets**

Constants: $con \in$ Con where $con ::= m \mid t$

Expressions: $e \in$ Exp where

$$e ::= con \mid x \mid \sim e \mid e_0 \; bop \; e_1 \mid \textbf{if } e_0 \textbf{ then } e_1 \textbf{ else } e_2$$

Declarations: $d \in$ Dec where

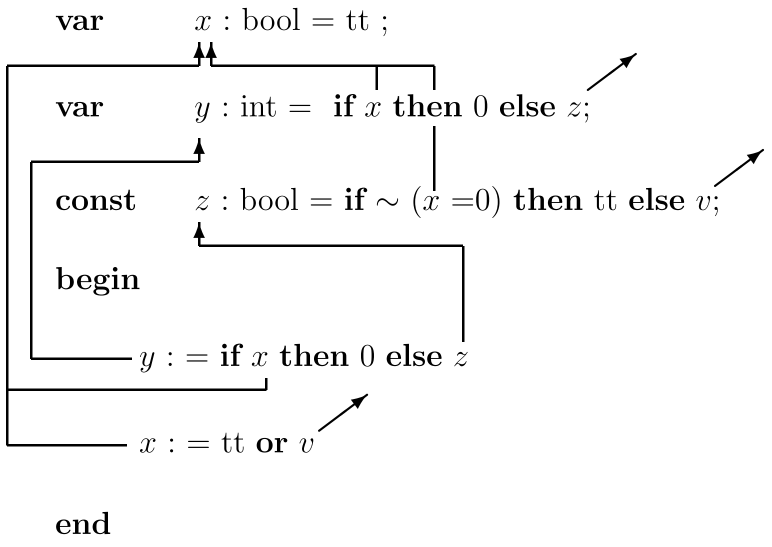
$$\begin{aligned} d ::= \textbf{nil} \mid \textbf{const } x : \tau = e \mid \textbf{var } x : \tau = e \mid d_0; d_1 \mid \\ d_0 \textbf{ and } d_1 \mid d_0 \textbf{ in } d_1 \end{aligned}$$

Commands: $c \in$ Com where

$$\begin{aligned} c ::= \textbf{nil} \mid x := e \mid c_0; c_1 \mid \textbf{if } e \textbf{ then } c_0 \textbf{ else } c_1 \mid \\ \textbf{while } e \textbf{ do } c \mid d; c \end{aligned}$$

Note: On occasion we write **begin** c **end** for (c). That is **begin** … **end** act as command parentheses, and have no particular semantic significance. However, their use can make scopes more apparent.

The whole of our discussion of defining, applied, and free and bound occurrences carries over to commands and is illustrated by the command in figure 2.



var x : bool = tt ;
var y : int = **if** x **then** 0 **else** z;
const z : bool = **if** ∼ (x =0) **then** tt **else** v;
begin
y : = **if** x **then** 0 **else** z
x : = tt **or** v
end

Bindings

Note that left-hand variable occurrences in assignments are applied, not binding.

Identifiers: For *expressions* we need the set, FI(e), of identifiers occurring freely in e (defined as usual). For *declarations* we need the sets FI(d) and DI(d) of identifiers with free and defining occurrences in d; they are defined just like in the case of definitions and of course

$$\mathrm{FI}(\mathbf{const}\ x : \tau = e) = \mathrm{FI}(\mathbf{var}\ x : \tau = e) = \mathrm{FI}(e)$$
$$\mathrm{DI}(\mathbf{const}\ x : \tau = e) = \mathrm{DI}(\mathbf{var}\ x : \tau = e) = \{x\}$$

For commands we only need FI(c) defined as usual plus $\mathrm{FI}(d; c) = \mathrm{FI}(c)\backslash\mathrm{DI}(d)$.

Type-Checking: We take

$$\mathrm{TEnv} = \mathrm{Id} \longrightarrow_{\mathrm{fin}} (\mathrm{Types} + \mathrm{Types} \times \{\mathbf{loc}\})$$

and write $\alpha : I$ for any α in TEnv with domain $I \subseteq Id$. The idea is that $\alpha(x) = \tau$ means that x denotes a value of type τ, whereas $\alpha(x) = \tau\ \mathbf{loc}$ ($\overset{def}{=} \langle\tau, \mathbf{loc}\rangle$) means that x denotes a location which holds a value of type τ.

Assertions:

- **Expressions**: For each I and expression e with $\mathrm{FI}(e) \subseteq I$ and type-environment $\alpha : I$ we define

  $$\alpha \vdash_I e : \tau$$

  meaning that given α the expression e is well-formed and of type τ.
- **Declarations**: Here for each I and declaration d with $\mathrm{FI}(d) \subseteq I$ and type-environment $\alpha : I$ we define

  $$\alpha \vdash_I d : \beta$$

  meaning that given α the declaration d is well-formed and yields the type-environment β.
- **Commands**: Here for each I and command c with $\mathrm{FI}(c) \subseteq I$ and type-environment $\alpha : I$ we define:

  $$\alpha \vdash_I c$$

  meaning that given α the command c is well-formed.

Rules:

- **Expressions**: As usual except for identifiers where:
  Identifiers: $\alpha \vdash_I x : \tau$ (if $\alpha(x) = \tau$ or $\alpha(x) = \tau\ \mathbf{loc}$)
- **Declarations**: Just like definitions before, except for simple ones:

Constants: $$\frac{\alpha \vdash_I e : \tau}{\alpha \vdash_I \textbf{const}\ x : \tau = e : \{x = \tau\}}$$

Variables: $$\frac{\alpha \vdash_I e : \tau}{\alpha \vdash_I \textbf{var}\ x : \tau = e : \{x = \tau\ \textbf{loc}\}}$$

- **Commands**: The rules are similar to those in Chapter 2. We give an illustrative sample.

Nil: $\alpha \vdash_I \textbf{nil}$

Assignment: $$\frac{\alpha \vdash_I e : \tau}{\alpha \vdash_I x := e} \quad (\text{if } \alpha(x) = \tau \text{ loc})$$

Sequencing: $$\frac{\alpha \vdash_I c_0 \qquad \alpha \vdash_I c_1}{\alpha \vdash_I c_0; c_1}$$

Blocks: $$\frac{\alpha \vdash_I d : \beta \quad \alpha[\beta] \vdash_{I \cup I_0} c}{\alpha \vdash_I d; c} \qquad (\text{where } \beta : I_0)$$

Dynamic Semantics

Following the ideas on environments and stores we consider suitably typed locations and assume we have for each τ infinite sets

$$\text{Loc}_\tau$$

which are disjoint and that (in order to create new locations) we have for each $I \subseteq \text{Loc}_\tau$ a location $\text{New}_\tau(I) \in \text{Loc}_\tau$ with $\text{New}_\tau(I) \notin I$ (the *new* property).

Note: It is very easy to arrange these matters. Just put $\text{Loc}_\tau = \text{N} \times \{\tau\}$ and $\text{New}_\tau(I) = \langle \mu m. \langle m, \tau \rangle \notin I, \tau \rangle$.

Now putting $\text{Loc} = \bigcup_\tau \text{Loc}_\tau$ we take for

$$\begin{aligned}\text{Stores} = \{\sigma : L \subseteq \text{Loc} \longrightarrow_{\text{fin}} \text{Con} \mid & \forall l \in \text{Loc}_{\text{nat}} \cap L.\ \sigma(l) \in \text{N} \\ & \wedge \forall l \in \text{Loc}_{\text{bool}} \cap L.\ \sigma(l) \in \text{T}\}\end{aligned}$$

(as Con is the set of values). And we also take

$$\text{Env} = \text{Id} \longrightarrow_{\text{fin}} \text{Con} + \text{Loc}$$

For any $\rho : I$ and $\alpha : I$ we define $\rho : \alpha$ by:

$$\begin{aligned}\rho : \alpha \equiv \forall x \in I.\ (\alpha(x) = \text{bool} \wedge \rho(x) \in \text{T})\ & \vee (\alpha(x) = \text{nat} \wedge \rho(x) \in \text{N}) \\ & \vee \exists \tau.\ (\alpha(x) = \tau\ \textbf{loc}\ \wedge \rho(x) \in \mathit{Loc}_\tau)\end{aligned}$$

Transition Relations:

- **Expressions:** For any $\alpha : I$ we set

  $$\Gamma_\alpha = \{\langle e, \sigma\rangle \mid \exists\tau.\ \alpha \vdash_I e : \tau\}$$
  $$\mathrm{T}_\alpha = \{\langle con, \sigma\rangle\}$$

  and for any $\alpha : I$ we will define transition relations of the form

  $$\rho \vdash_\alpha \langle e, \sigma\rangle \longrightarrow \langle e', \sigma'\rangle$$

  where $\rho : \alpha$ and $\langle e, \sigma\rangle$ and $\langle e', \sigma'\rangle$ are in Γ_α.
- **Declarations**: We extend Dec by adding the production

  $$d ::= \rho$$

  and putting $\mathrm{FI}(\rho) = \emptyset$ and $\mathrm{DI}(\rho) = I$ (where $\rho : I$), and putting $\alpha \vdash_I \rho : \beta$ (where $\rho : \beta$). Now for any $\alpha : I$ we take

  $$\Gamma_\alpha = \{\langle d, \sigma\rangle \mid \exists\beta.\ \alpha \vdash_I d : \beta\} \cup \{\rho\} \qquad \text{and} \qquad \mathrm{T}_\alpha = \{\rho\}$$

  and the transition relation has the form

  $$\rho \vdash_\alpha \langle d, \sigma\rangle \longrightarrow \langle d', \sigma'\rangle \text{ (or } \rho')$$

  where $\rho : \alpha$ and $\langle d, \sigma\rangle$ and $\langle d', \sigma'\rangle$ (or ρ') are in Γ_α.
- **Commands**: For any $\alpha : I$ we take

  $$\Gamma_\alpha = \{\langle c, \sigma\rangle \mid \alpha \vdash_I c\} \cup \{\sigma\} \qquad \text{and} \qquad \mathrm{T}_\alpha = \{\sigma\}$$

  and the transition relation has the form

  $$\rho \vdash_\alpha \langle c, \sigma\rangle \longrightarrow \langle c', \sigma'\rangle \qquad \text{(or } \sigma')$$

  where $\rho : \alpha$ and $\langle c, \sigma\rangle$ and $\langle c', \sigma'\rangle$ (or σ') are in Γ_α.

Rules:

- **Expressions:** These should be fairly obvious and we just give some examples.

  Identifiers: (1) $\rho \vdash_\alpha \langle x, \sigma\rangle \longrightarrow \langle con, \sigma\rangle$ (if $\rho(x) = con$)

  (2) $\rho \vdash_\alpha \langle x, \sigma\rangle \longrightarrow \langle con, \sigma\rangle$ (if $\rho(x) = l$ and $\sigma(l) = con$)

  Conditional: (1) $$\frac{\rho \vdash_\alpha \langle e_0, \sigma\rangle \longrightarrow \langle e_0', \sigma\rangle}{\rho \vdash_\alpha \langle \mathbf{if}\ e_0\ \mathbf{then}\ e_1\ \mathbf{else}\ e_2, \sigma\rangle \longrightarrow \langle \mathbf{if}\ e_0'\ \mathbf{then}\ e_1\ \mathbf{else}\ e_2, \sigma\rangle}$$

  (2) $\rho \vdash_\alpha \langle \mathbf{if}\ \mathrm{tt}\ \mathbf{then}\ e_1\ \mathbf{else}\ e_2, \sigma\rangle \longrightarrow \langle e_1, \sigma\rangle$

  (3) $\rho \vdash_\alpha \langle \mathbf{if}\ \mathrm{ff}\ \mathbf{then}\ e_1\ \mathbf{else}\ e_2, \sigma\rangle \longrightarrow \langle e_2, \sigma\rangle$
- **Declarations:**

  Nil: $\rho \vdash_\alpha \langle \mathbf{nil}, \sigma\rangle \longrightarrow \langle \emptyset, \sigma\rangle$

Constants: (1) $$\frac{\rho \vdash_\alpha \langle e, \sigma\rangle \longrightarrow \langle e', \sigma'\rangle}{\rho \vdash_\alpha \langle \mathbf{const}\ x : \tau\ = e, \sigma\rangle \longrightarrow \langle \mathbf{const}\ x : \tau = e', \sigma'\rangle}$$

(2) $\rho \vdash_\alpha \langle \mathbf{const}\ x : \tau\ = con, \sigma\rangle \longrightarrow \langle \{x = con\}, \sigma\rangle$

Variables: Informally to elaborate **var** $x : \tau = e$ from state σ given ρ

(1) Evaluate e from state σ given ρ yielding *con*.

(2) Get a new location l and change σ to $\sigma[l = con]$ and yield $\{x = l\}$.

Formally

(1) $$\frac{\rho \vdash_\alpha \langle e, \sigma\rangle \longrightarrow \langle e', \sigma'\rangle}{\rho \vdash_\alpha \langle \mathbf{var}\ x : \tau\ = e, \sigma\rangle \longrightarrow \langle \mathbf{var}\ x : \tau = e', \sigma'\rangle}$$

(2) $\rho \vdash_\alpha \langle \mathbf{var}\ x : \tau\ = con, \sigma\rangle \longrightarrow \langle \{x = l\}, \sigma[l = con]\rangle$

(where $\sigma : L$ and $l = \mathrm{New}_\tau(L \cap Loc_\tau)$)

Sequential: (1) $$\frac{\rho \vdash_\alpha \langle d_0, \sigma\rangle \longrightarrow \langle d_0', \sigma'\rangle}{\rho \vdash_\alpha \langle d_0; d_1, \sigma\rangle \longrightarrow \langle d_0'; d_1, \sigma'\rangle}$$

(2) $$\frac{\rho[\rho_0] \vdash_{\alpha[\alpha_0]} \langle d_1, \sigma\rangle \longrightarrow \langle d_1', \sigma'\rangle}{\rho \vdash_\alpha \langle \rho_0; d_1, \sigma\rangle \longrightarrow \langle \rho_0; d_1', \sigma'\rangle} \qquad \text{(where } \rho_0 : \alpha_0)$$

(3) $\rho \vdash_\alpha \langle \rho_0; \rho_1, \sigma\rangle \longrightarrow \langle \rho_0[\rho_1], \sigma\rangle$

Private: 1./2. Like Sequential.

3. $\rho \vdash_\alpha \langle \rho_0\ \mathbf{in}\ \rho_1, \sigma\rangle \longrightarrow \langle \rho_1, \sigma\rangle$

Simultaneous: (1) Like Sequential.

(2) $$\frac{\rho \vdash_\alpha \langle d_1, \sigma\rangle \longrightarrow \langle d_1', \sigma'\rangle}{\rho \vdash_\alpha \langle \rho_0\ \mathbf{and}\ d_1, \sigma\rangle \longrightarrow \langle \rho_0\ \mathbf{and}\ d_1', \sigma'\rangle}$$

(3) $\rho \vdash_\alpha \langle \rho_0\ \mathbf{and}\ \rho_1, \sigma\rangle \longrightarrow \langle \rho_0, \rho_1, \sigma\rangle$

Note: These definitions follow those for definitions very closely.

- **Commands:** On the whole the rules for commands are much like those we have already seen in Chapter 2.

Nil: $\rho \vdash_\alpha \langle \mathbf{nil}, \sigma\rangle \longrightarrow \sigma$

Assignment: $$\frac{\rho \vdash_\alpha \langle e, \sigma\rangle \longrightarrow^* \langle con, \sigma'\rangle}{\rho \vdash_\alpha \langle x := e, \sigma\rangle \longrightarrow \sigma'[l = con]}$$

(where $\rho(x) = l$, and if $l \in L$ where $\sigma : L$)

Composition: 1./2. Like Chapter 2, but with ρ.

Conditional While: Like Chapter 2, but with ρ.

Blocks: Informally to execute $d; c$ from σ given ρ

(1) Elaborate d from σ given ρ yielding ρ_0 and a store σ'.

(2) Execute c from σ' given $\rho[\rho_0]$ yielding σ''. Then σ'' is the result of the execution.

(1) $$\frac{\rho \vdash_\alpha \langle d, \sigma\rangle \longrightarrow \langle d', \sigma'\rangle}{\rho \vdash_\alpha \langle d; c, \sigma\rangle \longrightarrow \langle d'; c, \sigma'\rangle}$$

(2) $$\frac{\rho[\rho_0] \vdash_{\alpha[\alpha_0]} \langle c, \sigma\rangle \longrightarrow \langle c', \sigma'\rangle}{\rho \vdash_\alpha \langle \rho_0; c, \sigma\rangle \longrightarrow \langle \rho_0; c', \sigma'\rangle} \qquad (\rho_0 : \alpha_0)$$

$$(3)\quad \frac{\rho[\rho_0] \vdash_{\alpha[\alpha_0]} \langle c, \sigma\rangle \longrightarrow \sigma'}{\rho \vdash_\alpha \langle \rho_0; c, \sigma\rangle \longrightarrow \sigma'}$$

In the above we have not connected up ρ and σ. In principle it could happen either that

(1) There is an l in the range of ρ but not in the domain of σ. This is an example of a *dangling* reference. They are also possible in relation to a configuration such as $\langle c, \sigma\rangle$ where l occurs in c (via some ρ) but not in the domain of σ.
(2) There is an l not in the range of ρ but in the domain of σ. And similarly wrt c and σ, etc. This is an example of an *inaccessible* reference.

However, we easily show that if for example we have no dangling references in ρ and σ, or c and σ and if $\rho \vdash \langle c, \sigma\rangle \longrightarrow^* \langle c', \sigma'\rangle$ then there are none either in ρ and σ' or c and σ'. One says that the language has no *storage insecurities*. An easy way to obtain a language which is not secure is to add the command

$$c ::= \mathbf{dispose}(x)$$

with the dynamic semantics

$$\rho \vdash_\alpha \langle \mathbf{dispose}(x), \sigma\rangle \longrightarrow \sigma\backslash l \qquad (\text{where } l = \rho(x))$$

(and $\sigma\backslash l = \sigma\backslash\{\langle l, \sigma(l)\rangle\}$) (and obvious static semantics). One might wish to add an error rule for attempted assignments to dangling references.

On the other hand according to out semantics we do have inaccessible references. For example a block exit

$$\begin{aligned}\rho \vdash \langle \mathbf{var}\ x : \text{bool} = \text{tt},\ \mathbf{begin\ nil\ end}, \sigma\rangle &\longrightarrow \langle \{x = l\}; \mathbf{nil}, \sigma[l = \text{tt}]\rangle \\ &\longrightarrow \sigma[l = \text{tt}]\end{aligned}$$

Another example is provided by sequential or private definitions, e.g.,

$$\begin{aligned}\rho \vdash \langle \mathbf{var}\ x : \text{bool} = \text{tt}; \mathbf{var}\ x : \text{bool} = \text{tt}, \sigma\rangle &\longrightarrow \langle \{x = l_1\}; \mathbf{var}\ x : \text{bool} = \text{tt}, \sigma[l_1 = \text{tt}]\rangle \\ &\longrightarrow \langle \{x = l_1\}; \{x = l_2\}, \sigma[l_1 = \text{tt}, l_2 = \text{tt}]\rangle \\ &\longrightarrow \langle \{x = l_2\}, \sigma[l_1 = \text{tt}, l_2 = \text{tt}]\rangle\end{aligned}$$

and again

$$\begin{aligned}\rho \vdash \langle \mathbf{var}\ x : \text{bool} = \text{tt}\ \mathbf{in}\ \mathbf{var}\ y : \text{bool} = \text{tt}, \sigma\rangle &\longrightarrow^* \langle \{x = l_1\ \mathbf{in}\ y = l_2\}, \sigma[l_1 = \text{tt}, l_2 = \text{tt}]\rangle \\ &\longrightarrow \langle \{y = l_2\}, \sigma[l_1 = \text{tt}, l_2 = \text{tt}]\rangle\end{aligned}$$

It is not clear whether inaccessible references should be allowed. They can easily be avoided, at the cost of complicating the definitions, by "pruning" them away as they are created, a kind of logical garbage collection. We prefer here to leave them in, for the sake of simple definitions; they do not, unlike dangling references, cause any harm.

The semantics for expressions is a little more complicated than necessary in that if $\rho \vdash \langle e, \sigma\rangle \longrightarrow \langle e', \sigma'\rangle$ then $\sigma = \sigma'$; that is there are no *side-effects*. However, the extra generality will prove useful. For example suppose we had a production:

$$\begin{aligned} e ::= {}&\mathbf{begin}\ c\\ &\mathbf{result}\ e\end{aligned}$$

To evaluate **begin** c **result** e from σ given ρ one first executes c from σ given ρ yielding σ' and then evaluates e from σ' given ρ. The transition rules would, of course, be:

$$\frac{\rho \vdash_\alpha \langle c, \sigma\rangle \longrightarrow \langle c', \sigma'\rangle}{\rho \vdash_\alpha \langle \mathbf{begin}\ c\ \mathbf{result}\ e, \sigma\rangle \longrightarrow \langle \mathbf{begin}\ c'\ \mathbf{result}\ e, \sigma'\rangle}$$

$$\frac{\rho \vdash_\alpha \langle c, \sigma\rangle \longrightarrow \sigma'}{\rho \vdash_\alpha \langle \mathbf{begin}\ c\ \mathbf{result}\ e, \sigma\rangle \longrightarrow \langle e, \sigma'\rangle}$$

(and the static semantics is obvious).

With this construct one also has now the possibility of side-effects during the elaboration of definitions; previously we had instead that if

$$\rho \vdash_\alpha \langle d, \sigma\rangle \longrightarrow \langle d', \sigma'\rangle$$

then $\sigma' \upharpoonright L = \sigma$ where $\sigma : L$.

We note some other important constructs. The principle of qualification suggests we include expression blocks:

$$\begin{aligned} e ::= {}&\mathbf{let}\ d\\ &\mathbf{in}\ e\end{aligned}$$

with evident static semantics and the rules

$$\frac{\rho \vdash_\alpha \langle d, \sigma\rangle \longrightarrow \langle d', \sigma'\rangle}{\rho \vdash_\alpha \langle \mathbf{let}\ d\ \mathbf{in}\ e, \sigma\rangle \longrightarrow \langle \mathbf{let}\ d'\ \mathbf{in}\ e, \sigma'\rangle}$$

$$\frac{\rho[\rho_0] \vdash_{\alpha[\alpha_0]} \langle e, \sigma\rangle \longrightarrow \langle e', \sigma'\rangle}{\rho \vdash_\alpha \langle \mathbf{let}\ \rho_0\ \mathbf{in}\ e, \sigma\rangle \longrightarrow \langle \mathbf{let}\ \rho_0\ \mathbf{in}\ e', \sigma'\rangle} \qquad \text{(where } \rho_0 : \alpha_0)$$

$$\rho \vdash_\alpha \langle \mathbf{let}\ \rho_0\ \mathbf{in}\ con, \sigma\rangle \longrightarrow \langle con, \sigma\rangle$$

As another kind of atomic declaration consider

$$d ::= x == y$$

meaning that x should refer to the location referred to by y (in ρ). The relevant static semantics will, of course, be:

$$\begin{array}{l}\mathrm{DI}(x == y) = \{x\};\ \mathrm{FI}(x == y) = \{y\} \\ \alpha \vdash_I x == y : \{x = \tau\ \mathbf{loc}\} \qquad (\text{if } \alpha(y) = \tau\ \mathbf{loc})\end{array}$$

and the dynamic semantics is:

$$\rho \vdash_\alpha \langle x == y, \sigma\rangle \longrightarrow \langle x = l, \sigma\rangle \qquad (\text{if } \rho(y) = l)$$

This construct is an example where it is hard to do without locations; more complex versions allowing the evaluation of expressions to references will be considered in the next chapter.

It can be important to allow initialisation commands in declarations such as

$$\begin{array}{l} d ::= d \\ \qquad \mathbf{initial} \\ \qquad\qquad c \\ \qquad \mathbf{end} \end{array}$$

and the static semantics is:

$$\mathrm{DI}(d\ \mathbf{initial}\ c\ \mathbf{end}\ ) = \mathrm{DI}(d); \qquad \mathrm{FI}(d\ \mathbf{initial}\ c\ \mathbf{end}) = \mathrm{FI}(d) \cup (\mathrm{FI}(c)\backslash\mathrm{DI}(d))$$

and

$$\frac{\alpha \vdash_I d : \beta \qquad \alpha[\beta] \vdash_{I \cup I_0} c}{\alpha \vdash_I d\ \mathbf{initial}\ c\ \mathbf{end}} \qquad (\text{if } \beta : I_0)$$

However, we may wish to add other conditions (like the drastic $\mathrm{FI}(c) \subseteq \mathrm{DI}(d)$) to avoid side-effects. The dynamic semantics is:

$$\frac{\rho \vdash_\alpha \langle d, \sigma\rangle \longrightarrow \langle d', \sigma'\rangle}{\rho \vdash_\alpha \langle d\ \mathbf{initial}\ c\ \mathbf{end}, \sigma\rangle \longrightarrow \langle d'\ \mathbf{initial}\ c\ \mathbf{end}, \sigma'\rangle}$$

$$\frac{\rho \vdash_{\alpha[\alpha_0]} \langle c, \sigma\rangle \longrightarrow \langle c', \sigma'\rangle}{\rho \vdash_\alpha \langle \rho_0\ \mathbf{initial}\ c\ \mathbf{end}, \sigma\rangle \longrightarrow \langle \rho_0\ \mathbf{initial}\ c'\ \mathbf{end}, \sigma'\rangle} \qquad (\text{where } \rho_0 : \alpha_0)$$

$$\frac{\rho[\rho_0] \vdash_{\alpha[\alpha_0]} \langle c, \sigma\rangle \longrightarrow \sigma'}{\rho \vdash_\alpha \langle \rho_0\ \mathbf{initial}\ c\ \mathbf{end}, \sigma\rangle \longrightarrow \langle \rho_0, \sigma'\rangle}$$

In the exercises we consider a dual idea of *declaration finalisation* commands which are executed after the actions associated with the scope rather than before the scope of the declaration.

Finally, we stand back a little and look at the various classes of *values* associated with our language.

- **Expressible Values:** These are the values of expressions. In our language this set, EVal, is just the set, Con, of constants.
- **Denotable Values:** These are the values of identifiers in environments. Here the set, DVal, is the set Con + Loc of constants and locations. Note, that $\mathrm{Env} = \mathrm{Id} \longrightarrow_{\mathrm{fin}} \mathrm{DVal}$.
- **Storeable Values:** These are the values of locations in the store. Here, the set, SVal, is the set Con of constants. Note, that Stores is the set of type-respecting finite maps from Loc to SVal.

Thus we can consider the sets EVal, DVal, SVal of expressible, denotable and storeable values; languages can differ greatly in what they are and their relationship to each other [Str]. Other classes of values – e.g., writeable ones – may also be of interest.

5.5 *Exercises*

1. It is possible to formalise the notion of occurrence. An occurrence is a sequence $l = m_1 \ldots m_n$ $(n \geq 0)$ of non-zero natural numbers. For any expression, e, (say in the first language of Chapter 3) and occurrence, l, one has the expression $e' = \mathrm{Occ}(e, l)$ occurring in e at l (it may not be defined). For example

$$\mathrm{Occ}(e, \varepsilon) = e$$

$$\mathrm{Occ}(\mathbf{let}\ x = e_0\ \mathbf{in}\ e_1, m \frown l) = \begin{cases} \mathrm{Occ}(x, l) & (m = 1) \\ \mathrm{Occ}(e_0, l) & (m = 2) \\ \mathrm{Occ}(e_1, l) & (m = 3) \\ \text{undefined} & (\text{otherwise}) \end{cases}$$

Define $\mathrm{Occ}(e, l)$ in general. Define $\mathrm{FO}(x, e)$ = the set of free occurrences of x in e and also the sets $\mathrm{AO}(x, e)$ and $\mathrm{BO}(x, e)$ of applied and binding occurrences of x in e. For any l in $\mathrm{BO}(x, e)$ define $\mathrm{Scope}(l)$ = the set of applied occurrences of x in the scope of l; for any bound occurrence, l, of x in e (i.e., l in $[\mathrm{AO}(x, e) \cup \mathrm{BO}(x, e)] \backslash \mathrm{FO}(x, e)$, define $\mathrm{binder}(l)$ the unique occurrence in whose scope l is.

2. Repeat exercise 1 for the other languages in Chapter 3 (and later chapters!).

3. Ordinary mathematical language also has binding constructions. Notable are such examples as integration and summation.

$$\int_0^y \int_1^x f(y)\, dy\, dx \qquad \text{and} \qquad \sum_{n \geq 0} a_n x^n$$

Define mathematical expression language with these constructs and then define free variables and occurrences etc, just as in exercise 1.

4. The language of predicate logic also contains binders. Given a syntax for arithmetic expressions (say) we can define formulae by:

$$F ::= e = e \mid e > e \mid \ldots \mid \neg F \mid F \vee F \mid F \wedge F \mid F \supset F \mid \forall x.\ F \mid \exists x F$$

where $\wedge, \vee, \supset$ mean logical and, or and implies and to assert $\forall x.\ F$ means that for all x we have F and to assert $\exists x.\ F$ means that we have F for some x. Repeat the work of exercise 3 for predicate logic. To what extent is it feasible to construct an operational semantics for the languages of exercise 3 and 4? How would it help to only consider finite sums, $\sum\limits_{a \le n \le b} e$ and quantifications $\forall x.\ \le b.F$ and piecewise approximation?

5. Can you specify the location of dynamic errors? Thus starting from c, σ suppose we reach c', σ' and the next action is (for example) division by zero; then we want to specify an error occurred as some occurrence in the original command c. [Hint: Add a labelling facility, $c ::= L :: c$ and transition rules for it, and start not from c but a labelled version in which the occurrences are used for labels.]

6. Define the behaviour and equivalence of definitions and expressions of the second language of this chapter; prove that the program constructs respect equivalence. Establish or refute each of the following suggested equivalences

$$\begin{array}{lcl} d_0 \textbf{ and } (d_1 \textbf{ and } d_2) & \equiv & (d_0 \textbf{ and } d_1) \textbf{ and } d_2 \\ d_0 \textbf{ and } d_1 & \equiv & d_1 \textbf{ and } d_0 \\ d_0 \textbf{ and nil} & \equiv & d_0 \\ d_0 \textbf{ and nil} & \equiv & \textbf{nil} \end{array}$$

and similar ones for private and sequential definition.

7. Show that the following right-distributive law

$$d_0 \textbf{ in } (d_1 \textbf{ and } d_2) \quad \equiv \quad (d_0 \textbf{ in } d_1) \textbf{ and } (d_0 \textbf{ and } d_2)$$

holds. What about the left-distributive law? What about other such laws? Show that d_0 **in** $(x = e) \equiv x =$ **let** d_0 **in** e. Show that $d_0; d_1 \equiv d_0$ **in** $(d_1$ **and** $d_V)$ where $V = \mathrm{DV}(d_0) \backslash \mathrm{DV}(d_1)$ and where for any $V = \{x_1, \ldots, x_n\}$ we put $d_V = x_1 = x_1$ **and** $\ldots$ **and** $x_n = x_n$. Conclude that any d can be put, to within equivalence, in the form $x_1 = e_1$ **and** $\ldots$ **and** $x_n = e_n$.

8. Show that **let** $d_0; d_1$ **in** $e \equiv$ **let** d_0 **in** (**let** d_1 **in** e). Under what general conditions do we have $d_0; d_1 \equiv d_1; d_0$? When do we have $d_0; d_1 \equiv d_0$ **in** d_1? When do we have **let** $d_0; d_1$ **in** $e \equiv$ **let** d_0 **in** d_1 **in** $d_0; e$?

9. It has been said that in blocks like **let** d_0 **in** e all free variables of e should be bound by d for reasons of programming readability. Introduce *strict* blocks **let** d_0 **in** e and d_0 **in** d_1 where it is required that $\mathrm{FV}(e)$ (resp. $\mathrm{FV}(d_1)) \subseteq \mathrm{DV}(d_0)$. Show that the non-strict blocks are easily defined in terms of the strict ones. [Hint: Use simultaneous definitions and the d_V of exercise 7.] Investigate equivalences for the strict constructions.

10. Two expressions (of the first language of the present chapter) e and e' are α-equivalent - written $e \equiv_\alpha e'$ - if they are identical "up to renaming of bound variables". For example

$$\textbf{let } x = e \textbf{ in let } y = e' \textbf{ in } x + y \equiv_\alpha \textbf{let } y = e \textbf{ in let } x = e' \textbf{ in } y + x$$

if $x, y \notin \mathrm{FV}(e')$, but $\textbf{let } x = e \textbf{ in } x + y \not\equiv_\alpha \textbf{let } y = e \textbf{ in } y + y$. Define α-equivalence. [Hint: For a definition by structural induction to show $\textbf{let } x = e_0 \textbf{ in } e_1 \equiv_\alpha \textbf{let } y = e'_0 \textbf{ in } e'_1$ it is necessary to show some relation between e_1 and e'_1. So define $\pi : e \equiv_\alpha e'$ where $\pi : \mathrm{FV}(e) \cong \mathrm{FV}(e')$ is a bijection; this relation means e is α-equivalent to e' up to the renaming, π, of the free variables.] Show that $e \equiv_\alpha e'$ implies $e \equiv e'$. Show that for any e there is an e' with $e \equiv_\alpha e'$ and no bound variable of e' in some specified finite set and no variable of e' has more than one binding occurrence.

11. Define for the first language of the present chapter the substitution of an expression e for a variable x in the expression e' - written $[e/x]e'$; in the substitution process no free variable of e' should be captured by a binding occurrence in e', so that some systematic renaming of bound variables will be needed. For example we could not have

$$[x/y] \textbf{ let } x = e \textbf{ in } x + y = \textbf{let } x = [x/y]\, e \textbf{ in } x + x$$

but could have

$$[x/y] \textbf{ let } x = e \textbf{ in } x + y = \textbf{let } z = [x/y]\, e \textbf{ in } z + x$$

where $z \neq x$. Show the following

$$\begin{aligned}
&\textbf{let } x = e \textbf{ in } e' \equiv_\alpha \textbf{let } y = e \textbf{ in } [y/x]e' \text{ (if } y \notin \mathrm{FV}(e')) \\
&[e/x][e'/y]e'' \equiv_\alpha [[e/x]e'/y][e/x]e'' && \text{(if } x \neq y) \\
&[e/x][e'/x]e'' \equiv_\alpha [[e/x]e'/x]e'' \\
&[e/x]e' \equiv_\alpha e' && \text{(if } x \notin \mathrm{FV}(e')) \\
&\mathrm{FV}([e/x]e') = \mathrm{FV}(e) \cup (\mathrm{FV}(e') \backslash \{x\}) \\
&[e/x]e' \equiv \textbf{let } x = e \textbf{ in } e'.
\end{aligned}$$

12. By using substitution we could avoid the use of environments in the dynamic semantics of the first language of the present chapter. The transition relation would have the form $e \longrightarrow e'$ for *closed* e, e' (no free variables) and the rules would be as usual for binary operations, none (needed) for identifiers, and $\textbf{let } x = e_0 \textbf{ in } e_1 \longrightarrow [e_0/x]e_1$. Show this gives the same notion of behaviour for closed expressions as the usual semantics.

13. Extend the work of exercises 10, 11 and 12 to the second language of the present chapter.

14. It is possible to have iterative constructs in applicative languages. Tennent has suggested the construct

$$e = \textbf{ for } x = e_0 \textbf{ to } e_1 \textbf{ op } \textit{bop} \textbf{ on } e_2$$

So that, for example, if $e_0 = 0$ and $e_1 = n$ and $\textit{bop} = +$ and $e_2 = x{*}x$ then $e = \sum_{0 \le x \le n} x{*}x$. Give the operational semantics of this construct.

15. It is even possible to use definitions to obtain analogues of while loops. Consider the definition construct

$$d = \textbf{while } e \textbf{ do } d$$

So that

$$\begin{array}{l} \textbf{let } \textbf{ private}\, x = 1 \textbf{ and } y = 1 \\ \quad \textbf{within } \textbf{ while } y \neq n \\ \qquad\qquad \textbf{do } x = x * y \textbf{ and } y = y + 1 \\ \textbf{in } x \end{array}$$

computes $n!$ for $n \geq 1$. Give this construct a semantics; show that the construct of exercise 14 can be defined in terms of it. Is the new construct a "good idea"?

16. Consider the third language of the present chapter. Show that the type-environments generated by definitions are *determined* by defining by Structural Induction a partial function DTE: Definitions $\longrightarrow$ TEnv and then proving that for any α, V, d, β:

$$\alpha \vdash_V d : \beta \ \Rightarrow \text{DTE}(d) \text{ is defined and equal to } \beta.$$

17. Give a semantics to a variant of the third language in which the types of variables are not declared and type-checking is dynamic.

18. Change the fourth language of the present chapter so that the atomic declarations have the more usual forms:

$$\textbf{const } x = e \qquad \text{and} \qquad \textbf{var } x : \tau$$

Can you type-check the resulting language? To what extent can you impose in the static semantics the requirement that variables should be initialised before use? Give an operational semantics following one of the obvious alternatives regarding initialisation at declaration:

(1) The variable is initialised to a conventional value (e.g., 0/ff), or an unlikely one (e.g., the maximum natural number available/?).

(2) The variable is not initialised at declaration. [Hint: Use undefined maps for stores or (equivalently) introduce a special UNDEF value into the natural numbers (and another for truth-values).] In this case show how to specify the error of access before initialisation. Which alternative do you prefer?

19. In PL/I identifiers can be declared to be "EXTERNAL"; as such they take their value from an external environment - and so the declaration is an applied occurrence - but they have local scope - and so the declaration is also a binding occurrence. For example consider the following fragment in an extension of our fourth mini-language (not PL/I!) (where we allow $d ::= \textbf{external}\ x : \tau$):

```
external x : nat;
begin
        x := 2;
        var x : nat;
        begin
                x := 1;
                external        x : nat;
                begin y := x end
        end
end
```

This sets y equal to 2. Give a semantics to external declarations.

20. In PL/I variables can be declared without storage allocation being made until explicitly requested. Thus a program fragment like

```
var    x : nat
begin
       x := 1; allocate(x)
end
```

would result in a dynamic error under that interpretation of variable declaration. Give a semantics to this idea.

21. In the programming language EUCLID it is possible to declare identifiers as *pervasive*, meaning that no holes are allowed in their scope - they cannot be redeclared within their scope. Formulate an extension of the imperative language of this chapter which allows pervasive declarations and give it a static semantics. Are there any problems with its dynamic semantics?

22. Formalise Dijkstra's ideas on scope as presented in Section 10 of his book, A Discipline of Programming (Prentice-Hall, 1976). To do this define and give a semantics to a variant of the fourth mini-language which incorporates his ideas in as elegant a way as you can manage.

23. Suppose we have two flavours of variable declaration

local var $x : \tau$ and **heap var** $x : \tau$

(cf PL/I, ALGOL 68). From an implementation point of view local variables are allocated space on the stack and heap ones on the heap; from a semantical point of view the locations are disposed of on block exit (i.e., they live until the end of the variable's scope is reached) or never (unless explicitly disposed of). Formalise the semantics for these ideas. Does replacing local by heap make any difference to a program's behaviour? If not, find some language extensions for which it does.

24. Add to the considerations of exercise 23 the possibility

static var $x : \tau$

Here, the locations are allocated as part of the static semantics (of FORTRAN, COBOL, PL/I).

25. Consider the *finalisation* construct $d = d_0$ **final** c. Informally to elaborate this from an environment ρ one elaborates d_0 obtaining ρ_0 but then *after* the actions (whether elaboration, execution or evaluation) involved in the scope of d one executes c in the environment $\rho' = \rho[\rho_0]$ (equivalently, one executes $\rho'; c$). Give an operational semantics for an extension of the imperative language of the present chapter by a finalisation construct. [Hint: The elaboration of declarations should result in an environment and a command (with no free identifiers).] Justify your treatment of the interaction of finalisation and the various compound definition forms.

26. How far can you go in treating the constructs of the imperative language of this chapter (or later ones) without using locations? One idea would be for declarations to produce couples $< \rho, \sigma >$ of environments and stores (in the sense of Chapter 2) where $\rho : I_1, \sigma : I_2$ and $I_1 \cap I_2 = \phi$. What problems arise with the declaration $x == y$?

27. Formalise the notion of accessibility of a location and of a *dangling* location by defining when given an environment ρ and a configuration $\langle c, \sigma \rangle$ (or $\langle d, \sigma \rangle$ or $\langle e, \sigma \rangle$) a location, l, is accessible. Define the notion of *lifetime* with respect to the imperative language of the present chapter. Would it be best to define it so that the lifetime of a location ended exactly when it was no longer accessible or dangling? Using your definition formulate and prove a theorem, for the imperative language, relating scope and lifetime.

28. Locations can be considered as “dynamic place holders” (in the execution sequence) just as we considered identifiers as “static place holders” (in program text). Draw some arrow diagrams for locations in execution sequences to show their creation occurrences analogous to those drawn in this chapter to show binding occurrences.

29. Define α-equivalence for the imperative programming language of the present chapter (see exercise 10). One can consider $c \;\equiv_\alpha\; c'$ as saying that c and c' are equivalent up to choice of static place holders. Define a relation of *location equivalence* between couples of environments and configurations, written $\rho,\ \gamma \;\equiv_l\; \rho',\ \gamma'$ (where γ is an expression, command or declaration configuration); it should mean that the couples are equivalent up to choice of locations (dynamic place holders). For example

$$\begin{array}{l}\{x = l_1\}, \langle\{y = l_2\}; x := x + y, \{l_1 = 3, l_2 = 4\}\rangle \quad \equiv_l \\ \qquad\qquad \{x = l_2\}, \langle\{y = l_1\}; x := x + y, \{l_2 = 3, l_1 = 4\}\rangle\end{array}$$

holds.

30. Define the behaviour of commands, expressions and declarations and define an equivalence relation $\equiv_l$ between behaviours which should reflect equality of behaviours up to choice of dynamic place holders. Prove, for example, that

$$(\mathbf{var}\ x : \mathrm{nat} = 1; \mathbf{var}\ y : \mathrm{nat} = 1) \quad \equiv_l \quad (\mathbf{var}\ y : \mathrm{nat} = 1; \mathbf{var}\ x : \mathrm{nat} = 1)$$

even though the two sides do not have identical behaviours. Investigate the issues of exercises 10, 11, and 12 using $\equiv_l$.

5.6 Remarks

The ideas of structuring definitions and declarations seem to go back to Landin [Lan] and Milne and Strachey [Mil]. The idea of separating environments and stores, via locations, can also be found in [Mil]. The concepts of scope, extent, environments, stores and their mathematical formulations seem to be due to Burstall, Landin, McCarthy, Scott and Strachey. [I do not want to risk exact credits, or exclude others . . .] For another account of these matters see [Sto].

The ideas of Section 5.4 on static semantics where the constraints are clearly context-sensitive in general were formulated in line with the general ideas on dynamic semantics. In fact, they are simpler as it is only needed to establish properties of phrases rather than having relations between them. lt is hoped that the method is easy to read and in line with one’s intuition. There are many other methods for the purpose and for a survey with references, see [Wil]. It is also possible to use the techniques of denotational semantics for this purpose [Gor,Sto]. Our method seems particularly close to the production systems of Ledgard and the extended attribute grammars used by Watt; one can view, in such formulae as $\alpha \vdash_V d : \beta$, the turnstile symbols α and V as inherited attributes and β as a synthesized attribute of the definition d; obviously too the type-environments α and β are nothing but symbol tables. It would be interesting to compare the methods on a formal basis.

As pointed out in exercise 26 one can go quite far without using locations. Donahue also tries to avoid them in [Don]. In a first version of our ideas we also avoided them, but ran into unpleasantly complicated systems when considering shared global variables of function bodies.

As pointed out in exercise 12 one can try to avoid environments by using substitutions; it is not clear how far one can go in this direction (which is the usual one in syntactic studies of the λ-calculus). However, we have made a definite decision in these notes to stick to the Scott-Strachey tradition of environments. Note that in such rules as

$$\mathbf{let}\ x = e_0\ \mathbf{in}\ e_1 \longrightarrow [e_0/x]e_1$$

there is no offence against the idea of syntax-directed operational semantics. It is just that substitution is a rather “heavy” primitive and one can argue that the use of environments is closer to the intuitions normally used for understanding programming languages. (One awful exception is the ALGOL 60 call-by-name mechanism.)

6 Bibliography

[Ack] Ackerman, W.B. (1982) *Data Flow Languages*, IEEE Computer 15(2):15–25.

[Don] Donahue, J.E. (1977) *Locations Considered Unnecessary*, Acta Informatica 8:221–242.

[Gor1] Gordon, M.J., Milner, A.J.R.G. and Wadsworth, C.P. (1979) *Edinburgh LCF*, LNCS 78, Springer.

[Gor2] Gordon, M.J. (1979) *The Denotational Description of Programming Languages*, Springer.

[Hin] Hindley, J.R., Lercher, B. and Seldin, J.P. (1972) *Introduction to Combinatory Logic*, Cambridge University Press.

[Hug] Hughes, G.E. and Cresswell, M.J. (1968) *An Introduction to Modal Logic*, Methuen.

[Lan1] Landin, P.J. (1964) *The Mechanical Evaluation of Expressions*, Computer Journal 6(4):308–320.

[Lan2] Landin, P.J. (1965) *A Correspondence between ALGOL 60 and Church’s Lambda-notation*, Communications of the ACM 8(2):89–101 and 8(3):158–165.

[Led] Ledgard, H.F. and Marcotty, M. (1981) *The Programming Language Landscape*, Science Research Associates.

[Mil] Milne, R.E. and Strachey, C. (1976) *A Theory of Programming Language Semantics*, Chapman and Hall.

[Pra] Prawitz, D. (1971) *Ideas and Results in Proof Theory*, Proc. 2nd Scandinavian Logic Symposium, ed. J.E. Fenstad, p. 237–309, North Holland.

[Rey] Reynolds, J.C. (1978) *Syntactic Control of Interference*, Proc. POPL’78, pp. 39–46.

[Str] Strachey, C. (1973) *The Varieties of Programming Language*, Technical Monograph PRG-10, Programming Research Group, Oxford University.

[Sto] Stoy, J.E. (1977) *Denotational Semantics: The Scott-Strachey Approach to Programming Language Theory*, MIT Press.

[Wil] M.H. Williams (1981) *Methods for Specifying Static Semantics*, Computer Languages 6(1):1–17.

7 Functions, Procedures and Classes

In this chapter we consider various mechanisms allowing various degrees of abbreviation and abstraction in programming languages. The idea of abbreviating the repeated use of some expressions by using definitions or declarations of identifiers was considered in Chapter 3; if we apply the same choice to commands we arrive at (parameterless) procedures (= subroutines). It is very much more useful to abstract many similar computations together, different ones being obtained by varying the values of *parameters*. In this way we obtain functions from expressions and procedures from commands.

Tennent's *Principle of Abstraction* declares that the same thing can be done with any semantically meaningful category of phrases. Applying the idea to definitions of declarations we obtain a version of the *class* concept, introduced by SIMULA and recently taken up in many modern programming languages. (If we just use identifiers to stand for definitions or declarations we obtain the simpler but still most useful idea of *module*.)

Calling (= invoking) abstractions with *actual* parameters (their *arguments*) for the *formal* ones appearing in their definition results in appropriate computations whether evaluations, executions or elaborations of the *bodies* of their definitions. We will explain this by allowing abstraction identifiers to denote *closures* which record their formal parameters and bodies. Invocations will be explained in terms of computations of blocks chosen in terms of Tennent's Principle of Correspondence which declares that in principle to every parameter mechanism there corresponds an appropriate definition or declaration mechanism. For example if we define

$$f(x : \mathrm{nat}) : \mathrm{nat} = x + 1$$

then the elaboration results in the environment

$$f = \lambda x : \mathrm{nat}.\ x + 1 : \mathrm{nat}$$

To invoke f in an expression, say $f(5)$, we just evaluate the expression block

$$\begin{array}{l} \mathbf{let}\, x : \mathrm{nat} = 5 \\ \mathbf{in}\ \ x + 1 \end{array}$$

Note that this block exists by virtue of Tennent's Principle of Qualification.

Below we use these ideas to consider an applicative programming language with (possibly recursive) definitions of functions of several arguments. We then consider an imperative language where we consider both functions and procedures and use the Principle of Correspondence to obtain the parameter mechanisms of call-by-constant and call-by-value. Other parameter mechanisms are easily handled using the same ideas (some explicitly in the text and others in exercises); let us mention call-by-reference, call-by-result, call-by-value-result, call-by-name and call-by-text. Next we consider higher order functions and procedures. Finally we use the Principles of Abstraction and Correspondence to handle modules and classes; this needs no new ideas although some of the type-checking issues are interesting.

7.1 Functions in Applicative Languages

We begin with the simplest case where it is possible to define functions of one argument (unary) functions. Let us consider throughout extensions of the second applicative language of Chapter 3. Add the following kind of function definitions:

$$d ::= f(x : \tau_0) : \tau_1 = e$$

and function calls

$$e ::= f(e)$$

where f is another letter we will use to range over variables (but reserving its use to contexts where functions are expected).

Static Semantics

This is just as before as regards free and defining variables with the extensions

$$\begin{aligned}&\mathrm{FV}(f(x : \tau_0) : \tau_1 = e) = \mathrm{FV}(e)\backslash\{x\}\\&\mathrm{DV}(f(x : \tau_0) : \tau_1 = e) = \{f\}\\&\mathrm{FV}(f(e)) = \{f\} \cup \mathrm{FV}(e)\end{aligned}$$

It is convenient to consider types a little more systematically than before. Just as we have expressible and denotable values (EVal and DVal) we now introduce the sets of ETypes and DTypes, *expressible and denotable types* (ranged over by et and dt respectively) where

$$\begin{aligned}&et ::= \tau\\&dt ::= \tau \mid \tau_0 \to \tau_1\end{aligned}$$

More complex expressible types will be needed later; denotable types of the form $\tau_0 \to \tau_1$ will be used for functions which take arguments of type τ_0 and deliver *results* of type τ_1. Later we will want also sets of *storeable* types and other such sets. Now we take

$$\mathrm{TEnv} = \mathrm{Var} \longrightarrow_{\mathrm{fin}} \mathrm{DTypes}$$

ranged over, as before, by α and β and give rules for the predicates

$$\alpha \vdash_V e : et$$

where $\alpha : V$ and $\mathrm{FV}(e) \subseteq V$, and

$$\alpha \vdash_V d : \beta$$

where $\alpha : V$ and $\mathrm{FV}(d) \subseteq V$. These rules are just as before with the evident extensions for function calls and definitions:

Function Calls: $$\frac{\alpha \vdash_V e : et_0}{\alpha \vdash_V f(e) : et_1} \quad (\text{if } \alpha(f) = et_0 \rightarrow et_1)$$

Function Definitions: $$\frac{\alpha \vdash_V e : \tau_1}{\alpha \vdash_V f(x : \tau_0) : \tau_1 = e : \{\tau_0 \rightarrow \tau_1\}}$$

Dynamic Semantics

We introduce the set, Closures, of closures

$$\mathrm{Closures} = \{\lambda x : et_0.\ e : et_1 \mid \{x = et_0\} \vdash_{\{x\}} e : et_1\}$$

and define the set of denotable values by

$$\mathrm{DVal} = \mathrm{Con} + \mathrm{Closures}$$

and then we define, as usual,

$$\mathrm{Env} = \mathrm{Var} \longrightarrow_{\mathrm{fin}} \mathrm{DVal}$$

and add the following production to the definition of the category of definitions

$$d ::= \rho$$

(and put for $\rho : V$, $\mathrm{DV}(\rho) = V$ and $\mathrm{FV}(\rho) = \emptyset$).

It is important to note that what is meant here is that the sets Dec, Exp, Closures, DVal and Env are being defined mutually recursively. For example the following is an expression of type nat

$$\begin{array}{l} \textbf{let}\ f = \lambda x : \mathrm{nat} \\ \qquad\quad (\textbf{let}\{y = 3, g = \lambda y : \mathrm{bool}.\ {\sim}y : \mathrm{bool}\}\ \textbf{in if}\ g(\mathrm{ff})\ \textbf{then}\ x\ \textbf{else}\ y) : \mathrm{nat} \\ \quad \textbf{and}\ w = 5 \\ \textbf{in}\ \ f(2) + w \end{array}$$

There is no more harm in such recursions than in those found in context-free grammars; a detailed discussion is left to Appendix B.

Note too that closures have in an obvious sense no free variables. This raises the puzzle of what we intend to do about the free variable in function definitions. In fact in elaborating such definitions we will bind the free variables to their values in the elaboration environment. This is known as *static binding* (= binding of free variables determined by their textual occurrence), and will be followed throughout these notes. The alternative of delaying binding until the function is called, and then using the calling environment, is known as *dynamic binding*, and is considered in the exercises.

To extend the static semantics we type denotable values defining the predicate for *dval* in DVal and *dt* in DTypes

$$dval : dt$$

and for $\rho : V$ in Env and $\alpha : V$ in TEnv define

$$\rho : \alpha$$

by the rules

Constants: $m : \mathrm{nat} \qquad t : \mathrm{bool}$

Closures: $(\lambda x : et_0.\ e : et_1) : et_0 \rightarrow et_1$

Environments: $\dfrac{\forall x \in V.\ \rho(x) : \alpha(x)}{\rho : \alpha}$ (where $\rho : V$, $\alpha : V$)

and add the rule for environments considered as definitions

Environments: $\dfrac{\rho : \alpha}{\beta \vdash_V \rho : \alpha}$

With all this we now easily extend the old dynamic semantics with the usual transition relations

$$\rho \vdash_\alpha e \longrightarrow e'$$
$$\rho \vdash_\alpha d \longrightarrow d'$$

by rules for function calls and definition.

- **Function Calls**:

  $$\rho \vdash_\alpha f(e_0) \longrightarrow \mathbf{let}\ x : et_0 = e_0\ \mathbf{in}\ e \qquad (\text{if } \rho(f) = \lambda x : et_0.\ e : et_1\ )$$

  This rule is just a formal version of the Principle of Correspondence for the language under consideration.
- **Function Definitions**:

  $$\rho \vdash_\alpha f(x : \tau_0) : \tau_1 = e \longrightarrow \{f = \lambda x : \tau_0.\ (\mathbf{let}\ \rho \upharpoonright V\ \mathbf{in}\ e) : \tau_1\} \quad (\text{where } V = \mathrm{FV}(e) \backslash \{x\})$$

Example 25 *We write $f(x:\tau_0):\tau_1 = e$ for the less readable $f = \lambda x:\tau_0.\, e:\tau_1$ (and miss out τ_0 and/or τ_1 when they are obvious). Consider the expression*

$$\begin{aligned} e \overset{def}{=} & \ \textbf{let}\,\mathrm{double}(x:\mathrm{nat}):\mathrm{nat} = 2*x \\ & \ \textbf{in}\ \mathrm{double}(\mathrm{double}(2)) \end{aligned}$$

We have

$$\emptyset \vdash_\emptyset e \longrightarrow \textbf{let}\ \rho\ \textbf{in}\ \mathrm{double}(\mathrm{double}(2))$$

where $\rho \overset{def}{=} \{\mathrm{double}(x) = 2*x\}$ *and now note the computation*

$$\begin{aligned} \rho \vdash \mathrm{double}(\mathrm{double}(2)) & \longrightarrow \textbf{let}\ x:\mathrm{nat} = \mathrm{double}(2)\ \textbf{in}\ \mathrm{double}(2) \\ & \longrightarrow\ \textbf{let}\ x:\mathrm{nat} = (\textbf{let}\ x:\mathrm{nat} = 2\ \textbf{in}\ 2*x)\ \textbf{in}\ 2*x \\ & \longrightarrow^3 \textbf{let}\ x:\mathrm{nat} = 4\ \textbf{in}\ 2*x \\ & \longrightarrow^3 8 \end{aligned}$$

and so

$$\emptyset \vdash e \longrightarrow^* 8$$

Our function calls are call-by-value in the sense that the argument is evaluated before the body of the function. On the other hand it is evaluated just after the function call; a slight variant effects the evaluation before.

- **Function Call (Amended)**

(1) $\dfrac{\rho \vdash_V e \longrightarrow e'}{\rho \vdash_V f(e) \longrightarrow f(e')}$

(2) $\rho \vdash_V f(con) \longrightarrow \textbf{let}\ x:\tau_0 = con\ \textbf{in}\ e$ (if $f(x:\tau_0) = e$ is in ρ)

This variant has no effect on the result of our computations (prove this!) although it is not hard to define imperative languages where there could be a difference (because of side-effects). Another important possibility – call-by-name – is considered below and in the exercises.

We now consider how to extend the above to definitions of functions of several arguments such as

$$\max(x:\mathrm{nat}, y:\mathrm{nat}):\mathrm{nat} = \textbf{if}\ x \geq y\ \textbf{then}\ x\ \textbf{else}\ y$$

Intending to use the Principle of Correspondence to account for function calls we expect such transitions as

$$\rho \vdash \max(3,5) \longrightarrow \begin{array}{l} \mathbf{let}\ x : \mathrm{nat}, y : \mathrm{nat} = 3, 5 \\ \mathbf{in\ if}\ x \geq y\ \mathbf{then}\ x\ \mathbf{else}\ y \end{array}$$

and therefore simultaneous simple definitions. To this end we adopt a "minimalist" approach adding two syntactic classes to the applicative language of the last chapter.

Formals: This is the set Forms ranged over by *form* and given by

$$\mathit{form} ::= \cdot \ \mid\ x : \tau, \mathit{form}$$

Actual Expressions: This is the set AcExp ranged over by *ae* where

$$\mathit{ae} ::= \cdot \ \mid\ e, \mathit{ae}$$

Then we extend the category of definitions allowing more simple definitions and function definitions

$$d ::= \mathit{form} = \mathit{ae} \ \mid\ f(\mathit{form}) : \tau = e$$

and adding function calls to the stock of expressions

$$e ::= f(\mathit{ae})$$

To obtain a conventional notation $x : \tau,\ \cdot$ and $e,\ \cdot$ are written $x : \tau$ and e respectively and $f()$ replaces $f(\cdot)$. In a "maximalist" solution we could include actual expressions as expressions and allow corresponding "tuple" types as types of identifiers and function results; see exercise 2.

Static Semantics

Formals give rise to defining variable occurrences

$$\mathrm{DV}(\cdot) = \emptyset \qquad \mathrm{DV}(x : \tau, \mathit{form}) = \{x\} \cup \mathrm{DV}(\mathit{form})$$

Then we have free variables in actual expressions

$$\mathrm{FV}(\cdot) = \emptyset \qquad \mathrm{FV}(e, \mathit{ad}) = \mathrm{FV}(e) \cup \mathrm{FV}(\mathit{ae})$$

and for the new kinds of definitions

$$\begin{array}{ll} \mathrm{FV}(\mathit{form} = \mathit{ae}) = \mathrm{FV}(\mathit{ae}) & \mathrm{DV}(\mathit{form} = \mathit{ae}) = \mathrm{DV}(\mathit{form}) \\ \mathrm{FV}(f(\mathit{form}) : \tau = e) = \mathrm{FV}(e) \backslash \mathrm{DV}(\mathit{form}) & \mathrm{DV}(f(\mathit{form}) : \tau = e) = \{f\} \end{array}$$

and for function calls, $\mathrm{FV}(f(ae)) = \{f\} \cup \mathrm{FV}(ae)$.

Turning to types we now have ETypes, AcETypes (ranged over by *aet*) and DTypes where

$$et ::= \tau \qquad aet ::= \cdot \mid \tau, aet \qquad dt ::= et \mid aet \to et$$

Then with $\mathrm{TEnv} = \mathrm{Var} \longrightarrow_{\mathrm{fin}} \mathrm{DTypes}$ as always we have the evident predicates

$$\alpha \vdash_V e : et \qquad \alpha \vdash_V ae : aet \qquad \alpha \vdash_V d : \beta$$

Formals give positional information and type environments. So we define $T : \mathrm{Formals} \longrightarrow \mathrm{AcETypes}$ by

$$T(\cdot) = \cdot \qquad T(x : \tau, \mathit{form}) = \tau, T(\mathit{form})$$

and give rules for the predicate $\mathit{form} : \beta$

(1) $\cdot : \emptyset$
(2) $\mathit{form} : \beta \quad \Rightarrow \quad (x : \tau, \mathit{form}) : \{x = \tau\}, \beta$ (if $x \notin \mathrm{DV}(\mathit{form})$)

Note that it is here the natural restriction of no variable occurring twice in a formal is made.

Here are the rules for the other predicates:

Function Calls: $\dfrac{\alpha \vdash_V ae : aet}{\alpha \vdash_V f(ae) : et}$ (if $\alpha(f) = aet \to et$)

Definitions: $\dfrac{\mathit{form} : \beta \quad \alpha \vdash_V ae : aet}{\alpha \vdash_V (\mathit{form} = ae) : \beta}$ (where $aet = T(\mathit{form})$)

$$\frac{\mathit{form} : \beta \quad \alpha[\beta] \vdash_{V \cup V_0} e}{\alpha \vdash_V (f(\mathit{form}) : \tau = e) : \{f = aet \longrightarrow \tau\}}$$

(where $\beta : V_0$ and $aet = T(\mathit{form})$)

Actual Expr.: $\alpha \vdash_V \cdot : \cdot$

$$\frac{\alpha \vdash_V e : et \quad \alpha \vdash_V ae : aet}{\alpha \vdash_V e, ae : et, aet}$$

Dynamic Semantics

We proceed much as before as regards closures, denotable values and environments

$\mathrm{Closures} = \{\lambda \mathit{form}.\ e : et \mid \exists \beta, V.\ \mathit{form} : \beta \text{ and } \beta : V \text{ and } \beta \vdash_V e : et\}$
$\mathrm{DVal} = \mathrm{Con} + \mathrm{Closures}$
$\mathrm{Env} = \mathrm{Var} \longrightarrow_{\mathrm{fin}} \mathrm{DVal}$
$d ::= \rho$

with the free and defining variables of ρ as usual and extend the static semantics by defining the predicates $dval : dt$ and $\rho : \alpha$ much as before.

As regards transition rules we will naturally define $\rho \vdash_V e \longrightarrow e'$ and $\rho \vdash_V d \longrightarrow d'$ and, for actuals, $\rho \vdash_V ae \longrightarrow ae'$. The terminal actual configurations are the "actual constants"-tuples of constants given by the rules

$$acon ::= \cdot \mid con, acon$$

As for formals they give rise to environments in the content of a value for the corresponding actuals and so we begin with rules for the predicate

$$acon \vdash form : \rho$$

(1) $\cdot \vdash \cdot : \emptyset$

(2) $\dfrac{acon \vdash form : \rho}{con, acon \vdash (x : \tau, form) : \rho \cup \{x = con\}}$

While this is formally adequate enough it does seem odd to use values rather than environments as dynamic contexts.

The other rules should now be easy to understand.

Function Calls: $\rho \vdash_\alpha f(ae) \longrightarrow \mathbf{let}\ form = ae\ \mathbf{in}\ e \qquad (\text{if } \rho(f) = \lambda form.\ e : et)$

Definitions Simple: $\dfrac{\rho \vdash_\alpha ae \longrightarrow ae'}{\rho \vdash form = ae \longrightarrow form = ae'}$

$$\frac{acon \vdash form : \rho_0}{\rho \vdash form = acon \longrightarrow \rho_0}$$

Function: $\rho \vdash_\alpha f(form) : \tau = e \longrightarrow \{f = \lambda form.\ \mathbf{let}\ \rho \upharpoonright V\ \mathbf{in}\ e : \tau\}$

(where $V = \mathrm{FV}(e) \backslash \mathrm{DV}(form)$)

Actual Expr.: $\rho \vdash_\alpha e \longrightarrow e' \quad \Rightarrow \quad \rho \vdash_\alpha e, ae \longrightarrow e', ae$

$\rho \vdash_\alpha ae \longrightarrow ae' \quad \Rightarrow \quad \rho \vdash_\alpha con, ae \longrightarrow con, ae'$

Example 26 *We calculate the maximum of* $2+3$ *and* $2*3$*. Let* ρ_0 *be the environment* $\{\max = \lambda x : \mathrm{nat}, y : \mathrm{nat}.\ \mathbf{let}\ \emptyset\ \mathbf{in}\ \mathbf{if}\ x \geq y\ \mathbf{then}\ x\ \mathbf{else}\ y : \mathrm{nat}\}$*. Then we have*

$$\begin{aligned}
\emptyset \vdash \{&\mathbf{let}\ \max(x : \mathrm{nat}, y : \mathrm{nat}) : \mathrm{nat} = \ \mathbf{if}\ x \geq y\ \mathbf{then}\ x\ \mathbf{else}\ y\}\ \mathbf{in}\ \max(2+3, 2*3) \\
&\longrightarrow \mathbf{let}\ \rho_0\ \mathbf{in}\ \max(2+3, 2*3) \\
&\longrightarrow \mathbf{let}\ \rho_0\ \mathbf{in}\ \mathbf{let}\ x : \mathrm{nat}, y : \mathrm{nat} = 2+3, 2*3\ \mathbf{in}\ \mathbf{let}\ \emptyset\ \mathbf{in}\ (\mathbf{if}\ x \geq y\ \mathbf{then}\ x\ \mathbf{else}\ y) \\
&\longrightarrow^* \mathbf{let}\ \rho_0\ \mathbf{in}\ \mathbf{let}\ \{x = 5, y = 6\}\ \mathbf{in}\ \mathbf{let}\ \emptyset\ \mathbf{in}\ (\mathbf{if}\ x \geq y\ \mathbf{then}\ x\ \mathbf{else}\ y) \\
&\longrightarrow^* \mathbf{let}\ \rho_0\ \mathbf{in}\ \mathbf{let}\ \{x = 5, y = 6\}\ \mathbf{in}\ \mathbf{let}\ \emptyset\ \mathbf{in}\ 6 \\
&\longrightarrow^3 6.
\end{aligned}$$

as one sees that

$$\rho_0 \vdash x : \mathrm{nat}, y : \mathrm{nat} = 2+3, 2*3 \longrightarrow^* \{x = 5, y = 6\}$$

Recursion

It will not have escaped the readers attention that no matter how interesting our applicative language may be it is useless as there is no ability to prescribe interesting computations. For example we do not succeed in defining the factorial function by

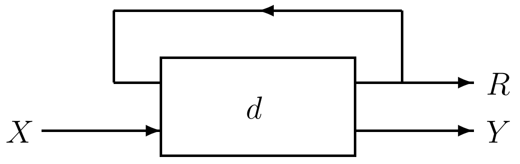
$$d \overset{def}{=} \mathit{fact}(n : \mathrm{nat}) : \mathrm{nat} = \mathbf{if}\ n = 0\ \mathbf{then}\ 1\ \mathbf{else}\ n * \mathit{fact}(n-1)$$

as the *fact* on the right will be taken from the environment of d_{fact} and not understood recursively. (Of course the imperative languages are interesting owing to the possibility of loops; note too exercise 3, 14, 15.)

Clearly we need to introduce recursion. Syntactically we just postulate a unary operator on definitions (and later on declarations)

$$d ::= \mathbf{rec}\ d$$

Thus **rec** d_{fact} will define the factorial function. In terms of imports and exports **rec** d imports all imports of d other than exports which provide the rest of the imports to d; the exports of **rec** d are those of d. In other words define X to be $\mathrm{FV}(d)\backslash\mathrm{DV}(d)$, Y to be $\mathrm{DV}(d)$ and R to be $\mathrm{FV}(d) \cap \mathrm{DV}(d)$. Then X is the set of imports of **rec** d and Y is the set of its exports with R being defined recursively. Diagrammatically we have



A Recursive Declaration: **rec** d

The unary recursion operator gives a very flexible way to make recursive definitions since the d in **rec** d can take many forms other than simple function definitions like $f(x : \tau_1 \ldots) : \tau = e$. *Simultaneous recursive* definitions are written

$$\begin{aligned} \mathbf{rec}\ \ & f(\ldots) = \ldots f \ldots g \ldots \mathbf{and} \ldots \mathbf{and} \\ & g(\ldots) = \ldots f \ldots g \ldots \end{aligned}$$

A *narrow scope* form of sequential recursive definitions is

$$\begin{aligned} &\mathbf{rec}\ f(\ldots) = \ldots f \ldots g \ldots\ ;\ \ldots\ ; \\ &\mathbf{rec}\ g(\ldots) = \ldots f \ldots g \ldots\ ; \end{aligned}$$

where the g in the definition of f is taken from the environment but the f in the definition of

g is the recursively defined one. A *wide scope* form is obtained by writing

$$\begin{array}{l}\mathbf{rec}\ \ f(\ldots) = \ldots f \ldots g \ldots\ ; \ldots\ ; \\ \qquad g(\ldots) = \ldots f \ldots g \ldots\end{array}$$

which is equivalent to the simultaneous definition unless $f = g$ for example.

Static Semantics

For free and defining variables we note that

$$\begin{array}{l}\mathrm{FV}(\mathbf{rec}\ d) = \mathrm{FV}(d)\backslash\mathrm{DV}(d) \\ \mathrm{DV}(\mathbf{rec}\ d) = \mathrm{DV}(d)\end{array}$$

We keep TEnv and DTypes, ETypes and AcETypes as before. The natural rule for recursive declarations is

$$\frac{\alpha[\beta \restriction R] \vdash_{V \cup R} d : \beta}{\alpha \vdash_V \mathbf{rec}\ d : \beta} \qquad (\text{where } R = \mathrm{FV}(d) \cap \mathrm{DV}(d))$$

However, this is not easy to use in a top-down fashion as given **rec** d and α one would have to guess β. But, as covered by exercise 11, it would work. It is more convenient to use the fact that in $\alpha \vdash_V d : \beta$ the elaborated β does not depend on α but is uniquely determined by d, the α only being used to check the validity of β. We make this explicit by defining *two* predicates for definitions. First for any V and d with $\mathrm{FV}(d) \subseteq V$ and β we define

$$\vdash_V d : \beta$$

and secondly for any $\alpha : V$ and d with $\mathrm{FV}(d) \subseteq V$ we define

$$\alpha \vdash_V d$$

The first predicate can be read as saying that if d is a valid definition then it will have type β; the second says that given α then d is valid. The other predicates will be as before

$$\alpha \vdash_V e : et \qquad \alpha \vdash_V ae : aet \qquad form : \beta$$

Rules:

- **Definitions:**

  Nil: (1) $\vdash_V \mathbf{nil} : \emptyset$

  (2) $\alpha \vdash_V \mathbf{nil}$

  Simple: (1) $\dfrac{form : \beta}{\vdash_V form = ae : \beta}$

(2) $\dfrac{\mathit{form} : \beta \quad \alpha \vdash_V ae : T(\mathit{form})}{\alpha \vdash_V \mathit{form} = ae}$

Function: (1) $\vdash_V f(\mathit{form}) : \tau = e : T(\mathit{form} \longrightarrow \tau)$

(2) $\dfrac{\mathit{form} : \beta \quad \alpha[\beta] \vdash_{V \cup V_0} e : \tau}{\alpha \vdash_V f(\mathit{form}) : \tau = e}$ (where $\beta : V_0$)

Sequential: (1) $\dfrac{\vdash_V d_0 : \beta_0 \quad \vdash_V d_1 : \beta_1}{\vdash_V d_0; d_1 : \beta_0[\beta_1]}$

(2) $\dfrac{\alpha \vdash_V d_0 \quad \vdash_V d_0 : \beta \quad \alpha[\beta] \vdash_{V \cup V_0} d_1}{\alpha \vdash_V d_0; d_1}$ (where $\beta : V_0$)

Simultaneous: (1) $\dfrac{\vdash_V d_0 : \beta_0 \quad \vdash_V d_1 : \beta_1}{\vdash_V d_0 \textbf{ and } d_1 : \beta_0, \beta 1}$

(2) $\dfrac{\alpha \vdash_V d_0 \quad \alpha \vdash_V d_1}{\alpha \vdash_V d_0 \textbf{ and } d_1}$ (if $\mathrm{DV}(d_0) \cap \mathrm{DV}(d_1) = \emptyset$)

Private: (1) $\dfrac{\vdash_V d_1 : \beta_1}{\vdash_V d_0 \textbf{ in } d_1 : \beta_1}$

(2) $\dfrac{\alpha \vdash_V d_0 \quad \vdash_V d_0 : \beta_0 \quad \alpha[\beta_0] \vdash_{V \cup V_0} d_1}{\alpha \vdash_V d_0 \textbf{ in } d_1}$ (where $\beta_0 : V_0$)

Recursion: (1) $\dfrac{\vdash_V d : \beta}{\vdash_V \textbf{rec } d : \beta}$

(2) $\dfrac{\vdash_V d : \beta \quad \alpha[\beta \restriction R] \vdash_{V \cup R} d}{\alpha \vdash_V \textbf{rec } d}$ (where $R = \mathrm{FV}(d) \cap \mathrm{DV}(d)$)

The other rules are as before except for expression blocks:

$$\frac{\vdash_V d : \beta \quad \alpha \vdash_V d \quad \alpha[\beta] \vdash_{V \cup V_0} e}{\alpha \vdash_V \textbf{let } d \textbf{ in } e} \qquad \text{(where } \beta : V_0\text{)}$$

Example 27 *Consider the definition*

$$d = \textbf{rec } f(x : \mathrm{nat}) : \mathrm{nat} = g(x) \textbf{ and } g(x : \mathrm{nat}) : \mathrm{nat} = f(x)$$

Here as $\vdash_\emptyset f(x : \mathrm{nat}) : \mathrm{nat} = g(x) : \{f = \mathrm{nat} \to \mathrm{nat}\}$*, etc. we have*

$$\vdash_\emptyset d : \{f = \mathrm{nat} \to \mathrm{nat}, g = \mathrm{nat} \longrightarrow \mathrm{nat}\}.$$

Then to see that $\emptyset \vdash_\emptyset d$ *one just shows that* $\{f = \mathrm{nat} \to \mathrm{nat}, g = \mathrm{nat} \to \mathrm{nat}\} \vdash_{f,g} d_0$ *(where* **rec** $d_0 = d$*). This example also shows why it is needed to explicitly mention the result (= output) of functions.*

Dynamic Semantics

Before discussing our specific proposal we should admit that this seems, owing to a certain clumsiness and its somewhat unnatural approach, to be a possible weak point in our treatment of operational semantics.

At first sight one wants to get something of the following effect with recursive definitions

$$\frac{\rho[\rho_0 \upharpoonright V_0] \vdash_{\alpha \cup \alpha_0} d \longrightarrow^* \rho_0}{\rho \vdash_\alpha \mathbf{rec}\ d \longrightarrow^* \rho_0} \qquad \text{(where } \rho_0 : \mathrm{DV}(d) \text{ and for suitable } \alpha_0 : V_0\text{)}$$

Taken literally this is not possible. For example put $d = f(x : \mathrm{nat}) : \mathrm{nat} = f(x)$ and suppose $\rho_0(f) = d$. Then for $V = \emptyset$ and $\rho = \emptyset$ we would have

$$\rho_0 \vdash_{\{f\}} f(x : \mathrm{nat}) : \mathrm{nat} = f(x) \longrightarrow \{f = \lambda x : \mathrm{nat}.\ (\mathbf{let}\ \rho_0\ \mathbf{in}\ f(x)) : \mathrm{nat}\}$$

and so we would have $d = \lambda x : \mathrm{nat}.\ (\mathbf{let}\ \rho_0\ \mathbf{in}\ f(x)) : \mathrm{nat}$ which is clearly impossible as d cannot occur in itself (via ρ_0). Of course it is just in finding solutions to suitable analogues of this equation that the Scott-Strachey approach finds one of its major achievements.

Let us try to overcome the problem by not trying to guess ρ_0 but trying to elaborate d without any knowledge of the values of the recursively defined identifiers. Thus in our example we first elaborate the body

$$\emptyset \vdash_\emptyset f(x : \mathrm{nat}) : \mathrm{nat} = f(x) \longrightarrow \{f = \lambda x : \mathrm{nat}.\ (\mathbf{let}\ \emptyset\ \mathbf{in}\ f(x)) : \mathrm{nat}\}$$

and let ρ_0 be the resulting "environment". Note that we no longer have closures as there can be free variables in the abstractions. So we know that for any imported value of f that ρ_0 gives the corresponding export. But in **rec** d the imports and the exports must be the same, that is $f = \rho(f)$ in some recursive sense and we can take $f \overset{def}{=} \mathbf{rec}\ \rho_0$. To get a closure we now take the all important step of binding f to **rec** ρ_0 in ρ_0 and take the elaboration of **rec** d to be

$$\rho_1 = \{f(x : \mathrm{nat}) : \mathrm{nat} = \mathbf{let\ rec}\ \rho_0\ \mathbf{in}\ (\mathbf{let}\ \emptyset\ \mathbf{in}\ f(x) : \mathrm{nat})\}$$

What we have done is unwound the recursive definition by one step and bound into the body instructions for further unwinding. Indeed it will be the case that

$$\vdash \mathbf{rec}\ \rho_0 \longrightarrow \rho_1$$

and so when we *call* $f(e)$ we will arrive at the expression

$$\mathbf{let}\ x : \mathrm{nat} = e\ \mathbf{in\ let\ rec}\ \rho_0\ \mathbf{in\ let}\ \emptyset\ \mathbf{in}\ f(x) : \mathrm{nat}$$

Then we will evaluate the argument e, then we will unwind the definition once more (in preparation for the next call!), then we will evaluate the body. This is perhaps not too bad; in the usual operational semantics of recursive definitions (see exercise 7) one first evaluates the argument, then unwinds the definition for the *present* call and then evaluates the body. Thus we have simply performed in advance one step of the needed unwindings during the elaboration.

Let us now turn our attention to the formal details, the changes from previously mostly concern allowing free variables in closures, and we define

$$\mathrm{Abstracts} = \{\lambda \mathit{form}.\ e : \mathit{et}\}$$

and put

$$\text{DVal} = \text{Con} + \text{Abstracts}$$

and

$$\text{Env} = \text{Var} \longrightarrow_{\text{fin}} \text{DVal}$$

and add

$$d ::= \rho$$

To extend the static semantics we define $\text{FV}(\mathit{dval})$ by

$$\text{FV}(\mathit{con}) = \emptyset \qquad \text{FV}(\lambda \mathit{form}.\ e : \mathit{et}) = \text{FV}(e) \backslash \text{DV}(\mathit{form})$$

and then for $\rho : V$

$$\text{DV}(\rho) = V \qquad \text{and} \qquad \text{FV}(\rho) = \bigcup_{x \in V} \text{FV}(\rho(x))$$

Now we define predicates $\vdash_V \mathit{dval} : \mathit{dt}$ and $\alpha \vdash_V \mathit{dval}$ by

Constants: (1) $\vdash_V m : \text{nat}$
(2) $\alpha \vdash_V m$
(3) $\vdash_V t : \text{bool}$
(4) $\alpha \vdash_V t$

Abstracts: (1) $\vdash_V \lambda \mathit{form}.e : \mathit{et} : T(\mathit{form}) \to \mathit{et}$
(2) $$\frac{\mathit{form} : \beta \quad \alpha[\beta] \vdash_{V \cup V_0} e}{\alpha \vdash_V \lambda \mathit{form}.\ e : \mathit{et}} \qquad (\text{where } \beta : V_0)$$

Then the rules for environments $\rho : V$

(1) $$\frac{\forall x \in V.\ \vdash_W \rho(x) : \beta(x)}{\vdash_W \rho : \beta}$$

(2) $$\frac{\forall x \in V.\ \alpha \vdash_W \rho(x)}{\alpha \vdash_W \rho}$$

Turning to the transition relations we define for $\alpha : V$ and $\beta : W$, with $W \subseteq V$ and $\rho : \alpha \upharpoonright W$, and e, e' in Γ_α (as before)

$$\rho \vdash_\alpha e \longrightarrow e'$$

and keep the same set Γ_α of terminal expressions. Similarly we define $\rho \vdash_\alpha ae \longrightarrow ae'$ and $\rho \vdash_\alpha d \longrightarrow d'$.

The rules are formally the same as before except that for $\rho : W$ conditions of the form $\rho(f) = \ldots$ are understood to mean that $f \in W$ and $\rho(f) = \ldots$ and similarly for $\rho(x) = \ldots$ (this affects looking up the values of variables and function calls).

We need rules for recursion:

(1) $$\frac{\rho \restriction X \vdash_{\alpha[\alpha_0]} d \longrightarrow d'}{\rho \vdash_\alpha \mathbf{rec}\ d \longrightarrow \mathbf{rec}\ d'}$$

(where $X = \mathrm{FV}(d) \backslash \mathrm{DV}(d)$ and taking β from the requirement that $\vdash d : \beta$ we have $\alpha_0 = \beta \restriction R$ where $R = \mathrm{FV}(d) \cap \mathrm{DV}(d)$)

(2) $$\rho \vdash_\alpha \mathbf{rec}\ \rho_0 \longrightarrow \{x = con \mid x = con\ \mathbf{in}\ \rho_0\} \cup \{f(form) : \tau = \mathbf{let\ rec}\ \rho_0 \backslash \mathrm{DV}(form)\ \mathbf{in}\ e \mid f(form) : \tau = e\ \mathbf{in}\ \rho_0\}$$

In other words we first elaborate d without knowing anything about the values of recursively defined variables and then from the resulting ρ_0 we yield ρ_0 altered to bind its free variables by **rec** ρ_0. Here are a couple of examples. More can be found in the exercises.

Example 28 *Consider the traditional definition of factorial*

$$d = \mathbf{rec}\ fact(x : \mathrm{nat}) : \mathrm{nat} = \mathbf{if}\ x = 0\ \mathbf{then}\ 1\ \mathbf{else}\ x * fact(x - 1)$$

Then for any suitable ρ and α we have

$$\rho \vdash_{\alpha[\alpha_0]} fact(x : \mathrm{nat}) : \mathrm{nat} = \ldots \longrightarrow \rho_0 \qquad \textit{(with } \alpha_0 \textit{ as given above)}$$

where $\rho_0 = \{fact(x : \mathrm{nat}) : \mathrm{nat} = \mathbf{let}\ \emptyset\ \mathbf{in} \ldots\}$ *(and from now on we omit the tedious "***let** $\emptyset$ **in***"). Then we have*

$$\rho \vdash_\alpha \mathbf{rec}\ d \longrightarrow \mathbf{rec}\ \rho_0 \longrightarrow \rho_1$$

where $\rho_1 = \{fact(x) = \mathbf{let\ rec}\ \rho_0\ \mathbf{in} \ldots\}$

To compute $fact(0)$ *we look at the derivation*

$$\begin{aligned}\emptyset \vdash_\emptyset \mathbf{let\ rec}\ d\ \mathbf{in}\ fact(0) &\longrightarrow^* \mathbf{let}\ \rho_1\ \mathbf{in}\ fact(0)\\ &\longrightarrow \mathbf{let}\ x : \mathrm{nat} = 0\ \mathbf{in\ let\ rec}\ \rho_0\ \mathbf{in}\ \ldots\\ &\longrightarrow^* \mathbf{let}\ \{x = 0\}\ \mathbf{in\ let}\ \rho_1\ \mathbf{in\ if}\ x = 0\ \mathbf{then}\ 1\ \mathbf{else}\ \ldots\\ &\longrightarrow^3 1\end{aligned}$$

Equally for $fact(1)$ *we have*

$$\begin{aligned}\emptyset \vdash_\emptyset \mathbf{let}\ d\ \mathbf{in}\ fact(1) &\longrightarrow^* \mathbf{let}\ \{x = 1\}\ \mathbf{in\ let}\ \rho_1\ \mathbf{in}\\ &\qquad \mathbf{if}\ x = 0\ \mathbf{then}\ 1\ \mathbf{else}\ x * fact(x - 1)\\ &\longrightarrow^* \mathbf{let}\ \{x = 1\}\ \mathbf{in\ let}\ \rho_1\ \mathbf{in}\ x * fact(x - 1)\\ &\longrightarrow^* \mathbf{let}\ \{x = 1\}\ \mathbf{in\ let}\ \rho_1\ \mathbf{in}\ 1 * [\mathbf{let}\ x : \mathrm{nat} = x - 1\ \mathbf{in\ rec}\ \rho_0\ \mathbf{in} \ldots]\end{aligned}$$

$$\begin{array}{l}\longrightarrow^* \textbf{let } \{x=1\} \textbf{ in let } \rho_1 \textbf{ in } 1 * [\textbf{let } x = 0 \textbf{ in let } \rho_1 \textbf{ in} \ldots] \\ \longrightarrow 1\end{array}$$

Example 29 *It is allowed to define natural numbers or truth-values recursively. For example consider $d = (\textbf{rec}\ x = x + 1)$. To elaborate d given $\rho = \{x = 1\}$ we must elaborate $x = x + 1$ from $\rho\backslash\{x\} = \emptyset$ and that elaboration sticks as we must evaluate $x+1$ in the empty environment. It could be helpful to specify a dynamic error in this case. Again the elaboration of*

$$d = \textbf{rec}\ x = \mathit{fact}(0)\ \textbf{and}\ \mathit{fact}(x : \mathrm{nat}) : \mathrm{nat} = \ldots$$

does not succeed as, intuitively, we need to know the value of fact before the elaboration – which produces this value – has finished. On the other hand simple things like the elaboration of **rec** $x = 5$ *do succeed. If desired we could have specified in the static semantics that only recursive function definitions were allowed.*

7.2 Procedures and Functions

We now consider abstractions in imperative languages. Abstracts of expressions give rise to functions, as before, but now with the possibility of side-effects as in:

$$\begin{array}{l}\textbf{function}\ f(\textbf{var}\ x : \mathrm{nat}) : \mathrm{nat} = \\ \quad \textbf{begin} \\ \quad\quad y := y + 1 \\ \quad \textbf{result}\ x + y\end{array}$$

In several programming languages the bodies of functions are commands, but are treated, via special syntactic devices, as expressions – see exercise 12. We take a straightforward view where the bodies are (clearly) expressions. Abstracts of commands give rise to procedures as in:

$$\begin{array}{l}\textbf{procedure}\ p(\textbf{var}\ x : \mathrm{nat}) \\ \quad \textbf{begin} \\ \quad\quad y := x + y \\ \quad \textbf{end}\end{array}$$

which may also have side-effects and indeed are often executed for their side-effects. To see why we write **var** in the formal parameter let us see how the Principle of Correspondence allows us to treat a procedure call. First the above declaration, d, will be elaborated thus

$$\rho \vdash_\alpha \langle d, \sigma\rangle \longrightarrow \langle\{p(\textbf{var}\ x : \mathrm{nat}) = \{y = l\};\ y := x + y\}, \sigma\rangle$$

where $l = \rho(y)$. Then the procedure call $p(e)$ in the resulting environment ρ' will look like this

$$\rho' \vdash_\alpha \langle p(e), \sigma\rangle \longrightarrow \langle \textbf{var}\ x : \mathrm{nat} = e;\ \textbf{begin}\ \{y = l\};\ y := x + y\ \textbf{end}, \sigma\rangle$$

And we see the reason for writing **var** ... is to get an easy correspondence with our previous declaration mechanism. The computation now proceeds by evaluating e, finding a new location l', making l' refer to the value of e in the state and then executing the body of the procedure with x bound to l'. This is very clearly nothing else but the classical call-by-value. Constant declarations will give rise to a call-by-constant parameter mechanism.

We begin by working these ideas out in the evident extension of the imperative language of Chapter 3. Then we proceed to other parameter mechanisms by considering the corresponding declaration mechanisms. (Many real languages will not possess such a convenient correspondence; one way to deal with their parameter mechanisms would be to add the corresponding declaration mechanisms when defining the set of possible configurations.)

For the extension we drop the **const** $x : \tau = e$ and **var** $x : \tau = e$ productions and add:

Expressions:	$e ::= \mathbf{let}\ d\ \mathbf{in}\ e \mid f(ae) \mid \mathbf{begin}\ c\ \mathbf{result}\ e$
Actual Expr.:	$ae ::= \cdot \mid e, ae$
Declarations:	$d ::= \mathit{form} = ae \mid \mathbf{function}\ f(\mathit{form}) : \tau = e \mid \mathbf{procedure}\ p(\mathit{form})\ c \mid \mathbf{rec}\ d$
Formals:	$\mathit{form} ::= \cdot \mid \mathbf{const}\ x : \tau, \mathit{form} \mid \mathbf{var}\ x : \tau, \mathit{form}$
Commands:	$c ::= p(ae)$

Static Semantics

We have the following sets of identifiers with the evident definitions and meanings: FI(e), FI(ae), FI(d), DI(d), DI(form), FI(c). For example

$$\mathrm{FI}(\mathbf{procedure}\ p(\mathit{form})\ c) = \mathrm{FI}(c) \backslash \mathrm{DI}(\mathit{form})$$
$$\mathrm{DI}(\mathbf{procedure}\ p(\mathit{form})\ c) = \{p\}$$
$$\mathrm{FI}(p(ae)) = \{p\} \cup \mathrm{FI}(ae)$$

Turning to types we define ETypes, AcETypes and DTypes; these are as before except that both locations and procedures are denotable, causing a change in DTypes

$$et ::= \tau$$

$$aet ::= \cdot \mid \tau, aet$$

$$dt ::= et \mid et\ \mathbf{loc} \mid aet \longrightarrow et \mid aet\ \mathbf{proc}$$

and of course TEnv = Id $\longrightarrow_{\mathrm{fin}}$ DTypes. We also need $T(\mathit{form}) \in$ AcETypes with the evident definition

	$\cdot$	**const** $x : \tau, \mathit{form}$	**var** $x : \tau, \mathit{form}$
T	$\cdot$	τ, aet	τ, aet

Then we define the expected predicates

$$\alpha \vdash_I e : et \qquad \alpha \vdash_I ae : aet \qquad \vdash_I d : \beta \qquad \alpha \vdash_I d\, form : \beta \qquad \alpha \vdash_I c$$

We give some representative rules:

Procedure Declarations: (1) $\vdash_I \textbf{procedure}\ p(form)\ c : \{p = T(form)\ \textbf{proc}\}$

(2) $\dfrac{form : \beta \quad \alpha[\beta] \vdash_{I \cup I_0} c}{\alpha \vdash_I c}$ (where $\beta : I_0$)

Formals: (1) $\cdot : \emptyset$

(2) $\dfrac{form : \beta}{\textbf{const}\ x : \tau, form : \{x = \tau\}, \beta}$ (if $x \notin I_0$ where $\beta : I_0$)

(3) $\dfrac{form : \beta}{\textbf{var}\ x : \tau, form : \{x = \tau\ \textbf{loc}\}, \beta}$ (if $x \notin I_0$ where $\beta : I_0$)

Procedure Calls: (1) $\dfrac{\alpha \vdash_I ae : aet}{\alpha \vdash_I p(ae)}$ (if $\alpha(p) = aet\ \textbf{proc}$)

Dynamic Semantics

We begin with environments, abstracts and denotable values. First the set, Abstracts (ranged over by *abs*), is

$$\text{Abstracts} = \{\lambda form.\ e : et\} \cup \{\lambda form.\ c\}$$

then

$$\text{DVal} = \text{Con} + \text{Loc} + \text{Abstracts}$$

where Loc is the set $\text{Loc}_{\text{nat}} \cup \text{Loc}_{\text{bool}}$ of Chapter 3 and

$$\text{Env} = \text{Id} \longrightarrow_{\text{fin}} \text{DVal}$$

and we add the production

$$d ::= \rho$$

and all the above is to be interpreted recursively as usual.

Then FI(*dval*) is defined in the obvious way; for example

$$\text{FI}(\lambda form.\ c) = \text{FI}(c) \backslash \text{DI}(form)$$

Then $\text{DI}(\rho)$ and $\text{FI}(\rho)$ are defined. Next we define the evident predicates

$$\vdash_I dval : dt \qquad \alpha \vdash_I dval \qquad \vdash_I \rho : \beta \qquad \alpha \vdash_I \rho : \beta$$

as expected; for example

Procedure Abstracts: (1) $\vdash_I \lambda \mathit{form}.\ c : T(\mathit{form})$ **proc**

$$(2)\quad \frac{\mathit{form} : \beta \qquad \alpha[\beta] \vdash_{I \cup I_0} c}{\alpha \vdash_I \lambda \mathit{form}.\ c} \qquad \text{(where } \beta : I_0\text{)}$$

Transition Relations: Turning to the transition relations we first need the set of stores

$$\text{Stores} = \{\sigma : L \in \text{Loc} \longrightarrow_{\text{fin}} \text{Con} \mid \sigma \text{ respects types}\}$$

– the same as in Chapter 3.

- **Expressions:** We have

  $$\Gamma_\alpha = \{\langle e, \sigma\rangle \mid \exists et.\ \alpha \vdash_I e : et\} \qquad (\text{for } \alpha : I)$$

  and

  $$\mathrm{T}_\alpha = \{\langle con, \sigma\rangle\}$$

  and the evident relation

  $$\rho \vdash_\alpha \langle e, \sigma\rangle \longrightarrow \langle e', \sigma'\rangle$$

- **Actual Expressions:** We have

  $$\Gamma_\alpha = \{\langle ae, \sigma\rangle \mid \exists aet.\ \alpha \vdash_I ae : aet\} \qquad (\text{for } \alpha : I)$$

  and

  $$\mathrm{T}_\alpha = \{\langle acon, \sigma\rangle\}$$

  where *acon* is in AeCon, as before. And we have the relation

  $$\rho \vdash_\alpha \langle ae, \sigma\rangle \longrightarrow \langle ae', \sigma'\rangle$$

- **Declarations:** We have

  $$\Gamma_\alpha = \{\langle d, \sigma\rangle \mid \alpha \vdash_I d\} \qquad (\text{for } \alpha : I)$$

  and

  $$\mathrm{T}_\alpha = \{\langle \rho, \sigma\rangle \mid \langle \rho, \sigma\rangle \in \Gamma_\alpha\}$$

  and the relation

  $$\rho \vdash_\alpha \langle d, \sigma\rangle \longrightarrow \langle d', \sigma'\rangle$$

- **Formals:** We define

  $$acon, L \vdash \mathit{form} : \rho, \sigma$$

  meaning that in the context of an actual expression constant *acon* and given an existing set, L, of locations the formal (part of a declaration) form yields a new (little) environment ρ and store σ.
- **Commands:** We have

  $$\Gamma_\alpha, \mathrm{T}_\alpha$$

  and

  $$\rho \vdash_\alpha \langle c, \sigma\rangle \longrightarrow \langle c', \sigma'\rangle \qquad \text{(or } \sigma'\text{)}$$

  as usual.

Rules: The rules are generally just those we already know and only the new points are covered.

- **Declarations:**

  Simple: (1) $$\frac{\rho \vdash_\alpha \langle ae, \sigma\rangle \longrightarrow \langle ae', \sigma'\rangle}{\rho \vdash_\alpha \langle \mathit{form} = ae, \sigma\rangle \longrightarrow \langle \mathit{form} = ae', \sigma'\rangle}$$

  (2) $$\frac{acon, L \vdash \mathit{form} : \rho_0, \sigma_0}{\rho \vdash_\alpha \langle \mathit{form} = ae, \sigma\rangle \longrightarrow \langle \rho_0, \sigma \cup \sigma_0\rangle} \qquad \text{(where } \sigma : L\text{)}$$

  Procedure: $$\rho \vdash_\alpha \langle \textbf{procedure}\ p(\mathit{form})\ c, \sigma\rangle \longrightarrow \langle \{p = \lambda \mathit{form}.\ \rho \backslash I; c\}, \sigma\rangle$$

  (where $I = \mathrm{FI}(c) \backslash \mathrm{DI}(\mathit{form})$)

  Recursive: (1) $$\frac{\rho \backslash R \vdash_{\alpha[\alpha_0]} d \longrightarrow d'}{\rho \vdash_\alpha \textbf{rec}\ d \longrightarrow \textbf{rec}\ d'}$$

  (where if $\vdash_{\mathrm{FI}(d)} d : \beta$ then $R = \mathrm{FI}(d) \cap \mathrm{DI}(d)$ and $\alpha = \beta \restriction R$)

  (2) $\rho \vdash_\alpha \textbf{rec}\ \rho_0 \longrightarrow \rho_1$

  $$\begin{aligned}
  \text{(where } \rho_1 = {} & \{x = con \mid x = con \text{ in } \rho_0\} \cup \\
  & \{x = l\ \textbf{loc} \mid x = l\ \textbf{loc} \text{ in } \rho_0\} \cup \\
  & \{f(\mathit{form}) : et = \textbf{let rec}\ \rho_0 \backslash I\ \textbf{in}\ e \mid \\
  & \quad f(\mathit{form}) : et = e \text{ in } \rho_0 \text{ and } I = \mathrm{DI}(\mathit{form})\} \cup \\
  & \{p(\mathit{form}).\ \textbf{rec}\ \rho_0 \backslash I;\ c \mid \\
  & \quad p(\mathit{form})\ c \text{ in } \rho_0 \text{ and } I = \mathrm{DI}(\mathit{form})\})
  \end{aligned}$$

- **Formals:**

  Empty: $\cdot, L \vdash \cdot : \emptyset, \emptyset$
- **Declarations**

  Empty: $$\frac{acon, L \vdash \mathit{form} : \rho_0, \sigma_0}{(con, acon), L \vdash \textbf{const}\ x : \tau, \mathit{form} : \rho_0 \cup \{x = con\}, \sigma_0}$$

Variable: $$\frac{\mathit{acon}, L \cup \{l\} \vdash \mathit{form} : \rho_0, \sigma_0}{(\mathit{con}, \mathit{acon}), L \vdash \mathbf{var}\ x : \tau, \mathit{form} : \{x = l\} \cup \rho_0, \{l = \mathit{con}\} \cup \sigma_0}$$
$$(\text{where } l = \text{New}_\tau(L \cap \text{Loc}_\tau))$$

Example 30 *The following program demonstrates the use of private variables shared between several procedures. This provides a nice version of ALGOL's own variables and anticipates the facilities provided by classes and abstract data types. Consider the command*

$c =$ **private var** x : nat $= 1$

  within procedure inc() $x := x + 1$

    procedure dec() **if** $x > 0$ **then** $x := x - 1$ **else nil**;

  begin

   inc(); dec()

  end

First look at the declaration part, d:

$$\begin{aligned}
&\rho \vdash \langle d, \sigma\rangle \longrightarrow \langle \mathbf{private}\ \{x = l\}\ \mathbf{within\ procedure}\ \text{inc}()-;\ \mathbf{procedure}\ \text{dec}()\ldots, \sigma[l = 1]\rangle\\
&\longrightarrow \langle \mathbf{private}\ \{x = l\}\ \mathbf{within}\{\text{inc}() = \{x = l\}; -\}; \mathbf{procedure}\ \text{dec}()\ldots, \sigma[l = 1]\rangle\\
&\longrightarrow^3 \langle \mathbf{private}\ \{x = l\}\ \mathbf{within}\ \{\text{inc}() = \{x = l\}; -, \text{dec}()\{x = l\}; \ldots, \sigma[l = 1]\rangle\\
&\longrightarrow \langle \{\text{inc}()\{x = l\}; -, \text{dec}()\{x = l\}; \ldots, \sigma[l = 1]\rangle\\
&\quad = \langle \rho, \sigma[l = 1]\rangle, \text{say}
\end{aligned}$$

So we see that

$$\rho \vdash \langle c, \sigma\rangle \longrightarrow^* \langle \rho_0; (\text{inc}(); \text{dec}()), \sigma[l = 1]\rangle$$

and so we should examine the computation:

$$\begin{aligned}
&\rho[\rho_0] \vdash \langle \text{inc}(); \text{dec}(), \sigma[l = 1]\rangle\\
&\qquad\longrightarrow \langle (\{x = l\}; x := x + 1); \text{dec}(), \sigma[l = 1]\rangle\\
&\qquad\longrightarrow^* \langle \text{dec}(), \sigma[l = 2]\rangle\\
&\qquad\longrightarrow \langle \{x = l\}; \mathbf{if}\ x > 0\ \mathbf{then}\ x := x - 1\ \mathbf{else\ nil}, \sigma[l = 2]\rangle\\
&\qquad\longrightarrow^* \langle \sigma[l = 1]\rangle.
\end{aligned}$$

7.3 Other Parameter Mechanisms

Other parameter mechanisms can be considered in the same manner. The general principle is to admit more ways to declare identifiers (as discussed above) and to admit more ways of evaluating expressions (and/or actual expressions). The latter is needed because actual expressions can be evaluated to various degrees when abstracts are called. One extreme is absolutely no evaluation (see exercise 16 for this call-by-text mechanism). We shall first consider call-by-name in the context of our applicative language which we regard as evaluating the argument to the extent of binding the call-time environment to it; this well-known idea differs from the official ALGOL-60 definition and is discussed further in exercise 15.

Then we consider call-by-reference in the context of our imperative language where the argument is evaluated to produce a reference. Other mechanisms are considered in the exercises. Note that in call-by-name for example the actual parameter may be further evaluated during computation of the body of the abstract. It is even possible to have mechanisms (e.g., variants of call-by-result) where some or all of the evaluation is delayed until *after* the computation of the body of the abstract.

Call-by-Name

Syntactically it is only necessary to add another possibility for the formal parameters to the syntax of our applicative language

$$\mathit{form} ::= \mathbf{name}\ x : \tau, \mathit{form}$$

Static Semantics

The sets of defining variables of **name** $x : \tau$, *form* is clearly $\{x\} \cup \mathrm{DV}(\mathit{form})$. Regarding types we add

$$\mathit{aet} ::= \tau\ \mathbf{name},\ \mathit{aet}$$
$$\mathit{dt} ::= \mathit{et}\ \mid\ \tau\ \mathbf{name}\ \mid\ \mathit{aet} \rightarrow \mathit{et}$$

The definition of the type $T(\mathit{form})$ of a formal needs the new clause

$$T(\mathbf{name}\ x : \tau, \mathit{form}) = \tau\ \mathbf{name},\ T(\mathit{form})$$

Here are the new predicate rules

- **Formals:** $\mathit{form} : \beta \Longrightarrow (\mathbf{name}\ x : \tau, \mathit{form}) : \{x = \tau\ \mathbf{name}\} \cup \beta \quad (\text{if } x \notin \mathrm{DV}(\mathit{form}))$
- **Expressions:**
  Variables: $\alpha \vdash_V x : \tau \qquad (\text{if } \alpha(x) = \tau\ \mathbf{name})$
  This rule expresses the fact that if x is a call-by-name formal parameter as in **name** $x : \tau$ then in the calling environment its denotation can be evaluated to a value of type τ.
- **Actual Expr.:** $\dfrac{\alpha \vdash_V e : \mathit{et} \qquad \alpha \vdash_V \mathit{ae} : \mathit{aet}}{\alpha \vdash_V e, \mathit{ae} : \mathit{et}\ \mathbf{name}, \mathit{aet}}$
  It is important to note that this rule is in *addition* to the previous rule. So given α an actual expression can have several different types; these are needed as the same expression can correspond to formals of different types, and that will require different kinds of evaluation.

Example 31 *Consider these two expressions*

$$\begin{array}{l}\textbf{let function}\ \mathit{fred}(x:\mathrm{nat}, \textbf{name}\ y:\mathrm{nat}):\mathrm{nat} = x+y\\ \textbf{in}\ \mathit{fred}(u+v, u-v)\end{array}$$

and

$$\begin{array}{l}\textbf{let function}\ \mathit{fred}(\textbf{name}\ x:\mathrm{nat}, y:\mathrm{nat}):\mathrm{nat} = x+y\\ \textbf{in}\ \mathit{fred}(u+v, u-v)\end{array}$$

In the first case we need the fact that $\alpha \vdash u+v, u-v : \mathrm{nat}, \mathrm{nat}\ \textbf{name}$ *and in the second that* $\alpha \vdash u+v, u-v : \mathrm{nat}\ \textbf{name}, \mathrm{nat}$ *(where* $\alpha = \{u = \mathrm{nat}, v = \mathrm{nat}\}$*).*

Dynamic Semantics

Clearly we must add a new component to the set of denotable values, corresponding to the new denotable types τ **name**

$$\mathrm{DVal} = \mathrm{Con} + \mathrm{NExp} + \mathrm{Abstracts}$$

where we need $\mathrm{NExp} = \{e : \textbf{name}\ \tau\}$ to allow free variables in the expressions because of the possibility of recursive definitions. For example consider

$$\begin{array}{rcl}\textbf{rec name}\ x:\mathrm{nat} & = & f(5)\ \textbf{and}\\ f(x:\mathrm{nat}) & = & \ldots f \ldots\end{array}$$

The extension to the definition of FV(*dval*) is, of course, clear

$$\mathrm{FV}(e : \textbf{name}\ \tau) = \mathrm{FV}(e)$$

For the predicates $\vdash_V \mathit{dval} : \mathit{dt}$ and $\alpha \vdash_V \mathit{dval}$ we add the rules

$$\vdash_V (e : \tau\ \textbf{name}) : \textbf{name}\ \tau \qquad \frac{\alpha \vdash e : \tau}{\alpha \vdash e : \tau\ \textbf{name}}$$

Transition Relations: For expressions and definitions we refine the usual $\rho \vdash_\alpha e \longrightarrow e'$ and $\rho \vdash_\alpha d \longrightarrow d'$ a little, parameterising also on the set of variables whose definition is currently available in the environment (the others will be in the process of being recursively defined). So for $\alpha : V$ and $W \subseteq V$ we will define the relations

$$\rho \vdash_{\alpha,W} e \longrightarrow e' \qquad \text{and} \qquad \rho \vdash_{\alpha,W} d \longrightarrow d'$$

where $\rho : \alpha \upharpoonright W$ and $e, e' \in \Gamma^{\mathrm{exp}}_{\alpha,W}$ and $d, d' \in \Gamma^{\mathrm{def}}_{\alpha,W}$ where

$$\Gamma^{\mathrm{exp}}_{\alpha,W} = \{e \mid \exists et.\ \alpha \vdash_V e : et\}$$

$$\Gamma^{\text{def}}_{\alpha,W} = \{d \mid \alpha \vdash_V d\}$$

We also have the evident $\mathrm{T}^{\text{exp}}_{\alpha,W}$ and $\mathrm{T}^{\text{def}}_{\alpha,W}$.

For formals we have the predicate

$$ae \vdash_{\mu,W} \mathit{form} : \rho_0$$

where $ae \in \mathrm{T}_{\mu,W}$ and $\mu = M(T(\mathit{form}))$.

For actual expressions the result desired will depend on the context and we introduce an apparatus of different *evaluation modes*. The set Modes of modes is ranged over by μ given by

$$\mu ::= \cdot \mid \mathbf{value}, \mu \mid \mathbf{name}, \mu$$

Each actual expression type, *aet*, has a mode, $M(aet)$ where

$$M(\cdot) = \cdot$$
$$M(\tau, aet) = \mathbf{value}, M(aet)$$
$$M(\tau\ \mathbf{name},\ aet) = \mathbf{name}, M(aet)$$

We define transition relations $\rho \vdash_{\alpha,W,\mu} ae \longrightarrow ae'$ which are also parameterised on modes. The set of configurations is, for $\alpha : V$, $W \subseteq V$ and mode μ

$$\Gamma_{\alpha,W,\mu} = \{ae \mid \exists aet.\ \alpha \vdash_V ae : aet \text{ and } M(aet) = \mu\}$$

and we define the set $\mathrm{T}_{\alpha,W,\mu}$ of terminal actual expressions by some rules of the form $\vdash_{\mu,W} T(ae)$

(1) $\vdash_{\cdot,W} T(\cdot)$

(2) $\dfrac{\vdash_{\mu,W} T(ae)}{\vdash_{(\mathbf{value},\mu),W} T(con, ae)}$

(3) $\dfrac{\vdash_{\mu,W} T(ae)}{\vdash_{(\mathbf{name},\mu),W} T(e, ae)}$ (if $\mathrm{FV}(e) \cap W = \emptyset$)

It is rule 3 which introduces the need for W, insisting that all variables are bound, except, possibly, for those being recursively defined.

The transition relation is defined for $\rho : \alpha \upharpoonright W$ and $ae, ae' \in \Gamma_{\alpha,W,\mu}$ and has the form $\rho \vdash_{\alpha,W,\mu} ae \longrightarrow ae'$. The apparatus of modes gives types what might also be called metatypes and this may be a useful general idea. The reader should not confuse this with one normal usage of the term mode as synonymous with type.

Transition Rules:

- **Expressions:** These are the same as before except for identifiers:
  Identifiers: (1) $\rho \vdash x \longrightarrow con$ (if $\rho(x) = con$)

(2) $\rho \vdash x \longrightarrow e \qquad$ (if $\rho(x) = e : \tau$ **name**)

- **Actual Expr.**

Value Mode: (1) $\dfrac{\rho \vdash_{\alpha,W} e \longrightarrow e'}{\rho \vdash_{\alpha,(\mathbf{value},\mu),W} e, ae \longrightarrow e', ae}$

(2) $\dfrac{\rho \vdash_{\alpha,\mu,W} ae \longrightarrow ae'}{\rho \vdash_{\alpha,(\mathbf{value},\mu),W} con, ae \longrightarrow con, ae'}$

Name Mode: (1) $\rho \vdash_{\alpha,(\mathbf{name},\mu),W} e, ae \longrightarrow (\mathbf{let}\ \rho \upharpoonright \mathrm{FV}(e)\ \mathbf{in}\ e), ae$

(2) $\dfrac{\rho \vdash_{\alpha,\mu,W} ae \longrightarrow ae'}{\rho \vdash_{\alpha,(\mathbf{name},\mu),W} e, ae \longrightarrow e, ae'} \qquad$ (if $\mathrm{FV}(e) \cap W = \emptyset$)

- **Definitions:** Here we need a rule which ensures that the actual expressions are evaluated in the right mode. Otherwise the rules are as before.

Simple: (1) $\dfrac{\rho \vdash_{\alpha,\mu,W} ae \longrightarrow ae'}{\rho \vdash_{\alpha,W} \mathit{form} = ae \longrightarrow \mathit{form} = ae'} \qquad$ (where $\mu = M(T(\mathit{form}))$)

(2) $\dfrac{ae \vdash \mathit{form} : \rho_0}{\rho \vdash_{\alpha,W} \mathit{form} = ae \longrightarrow \rho_0}$

(if $ae \in \mathrm{T}_{\alpha,\mu,W}$ where $\mu = M(T(\mathit{form}))$

Formals: (1) $\cdot \vdash_{\cdot,W} \cdot : \emptyset$

(2) $\dfrac{ae \vdash_{\mu,W} \mathit{form} : \rho}{con, ae \vdash_{(\mathbf{value},\mu),W} (x : \tau, \mathit{form}) : \{x = con\} \cup \rho}$

(3) $\dfrac{ae \vdash_{\mu,W} \mathit{form} : \rho}{e, ae \vdash_{(\mathbf{name},\mu),W} (x : \tau\ \mathbf{name}, \mathit{form}) : \{x = e : \tau\ \mathbf{name}\} \cup \rho}$

Example 32 *The main difference between call-by-name and call-by-value in applicative languages is that call-by-name may terminate where call-by-value need not. For example consider the expression*

$$e = \mathbf{let}\ f(x : \mathrm{nat}\ \mathbf{name}) : \mathrm{nat} = 1\ \mathbf{and\ rec}\ g(x : \mathrm{nat}) : \mathrm{nat} = g(x)\ \mathbf{in}\ f(g(2))$$

Then $\rho \vdash e \longrightarrow^* \mathbf{let}\ \rho_0\ \mathbf{in}\ f(g(2))$ *where* $\rho_0 = \{f(x : \mathrm{nat}\ \mathbf{name}) : \mathrm{nat} = 1, g(x : \mathrm{nat}) : \mathrm{nat} = \ldots\}$*. So we look at*

$$\begin{aligned} \rho_0 \vdash f(g(2)) &\longrightarrow \mathbf{let}\ x : \mathrm{nat}\ \mathbf{name} = g(2)\ \mathbf{in}\ 1 \\ &\longrightarrow^* \mathbf{let}\ \{x = \mathbf{let}\ g(x : \mathrm{nat}) : \mathrm{nat} = \ldots\}\ \mathbf{in}\ 1 \\ &\longrightarrow 1 \end{aligned}$$

On the other hand if we change the formal parameter of f *to be call-by-value instead, then, as the reader may care to check, the evaluation does not terminate.*

Call-by-Reference

We consider a variant (the simplest one!) where the actual parameter must be a variable (identifier denoting a location). In other languages the actual parameter could be any of a wide variety of expressions which are evaluated to produce a location; these might include conditionals and function calls. This would require a number of design decisions on the permitted expressions and on how the type-checking should work. For lack of time rather than any intrinsic difficulty we leave such variants to exercise 17. Just note that it will certainly be necessary to rethink expression evaluation; this should either be changed so that evaluation yields a natural value (be it location or primitive value) or else different evaluation modes should be introduced.

Syntactically we consider an extension to our imperative language

$$form ::= \mathbf{loc}\ x : \tau, form.$$

Static Semantics

Clearly we have $\mathrm{DI}(\mathbf{loc} x : \tau, form) = \{x\} \cup \mathrm{DI}(form)$. For types we add another actual expression type

$$aet ::= \tau\ \mathbf{loc}, aet$$

and

$$T(\mathbf{ref}\ x : \tau, form) = \tau\ \mathbf{ref}, aet$$

and we have the rule

$$\frac{form : \beta}{\mathbf{ref}\ x : \tau, form : \{x = \tau\ \mathbf{ref}\}, \beta} \qquad (\text{if } x \notin I \text{ where } \beta : I)$$

- **Actual Expressions**: These are as before with the addition

$$\frac{\alpha \vdash_V ae : aet}{\alpha \vdash_V x, et : \tau\ \mathbf{loc}, aet} \qquad (\text{if } \alpha(x) = \tau\ \mathbf{loc})$$

It is here that we insist that actual reference parameters must be variables. As in the case of call-by-name the type of an actual expression is not determined by its environment alone, but by its context as well. (A more honest notation might be $\alpha, aet \vdash_V ae$ rather than $\alpha \vdash_V ae : aet$.)

Dynamic Semantics

It is not necessary to change the definitions of DVal (or Env or Dec) as locations are already included. However, we allow locations in AcExp and AeCon

$$ae ::= l, ae$$

$$acon ::= l, acon$$

and clearly $\mathrm{FV}(l, ae) = \mathrm{FV}(ae)$ and we have the rule

$$\frac{\alpha \vdash_I ae : aet}{\alpha \vdash_I l, ae : \tau\ \mathbf{loc}, aet} \qquad (l \in Loc_\tau)$$

Transition Rules: We have relations $\rho \vdash_\alpha \langle e, \sigma\rangle \longrightarrow \langle e', \sigma'\rangle$, $\rho \vdash_\alpha \langle d, \sigma\rangle \longrightarrow \langle d', \sigma'\rangle$ and $\rho \vdash_\alpha \langle c, \sigma\rangle \longrightarrow \langle c', \sigma'\rangle$ (or σ') and a predicate $acon, L \vdash form : \rho, \sigma$ as before. For actual expressions we proceed as with call-by-name and introduce a set, Mode, of evaluation modes

$$\mu ::= \cdot \mid \mathbf{val}, \mu \mid \mathbf{loc}, \mu$$

with the evident definition of $M(aet) \in$ Mode and put for $\alpha : I$ and μ,

$$\Gamma_{\alpha,\mu} = \{\langle ae, \sigma\rangle \mid \exists aet.\ \alpha \vdash_I ae : aet \text{ and } \mu = M(aet)\}$$
$$\mathrm{T}_{\alpha,\mu} = \{\langle acon, \sigma\rangle \in \Gamma_{\alpha,\mu}\}$$

and will define the transition relation for $\rho : \alpha$ and μ

$$\rho \vdash_{\alpha,\mu} \langle ae, \sigma\rangle \longrightarrow \langle ae', \sigma'\rangle$$

Rules:

- **Actual Expressions:**

  Value Mode: (1) $$\frac{\rho \vdash_\alpha \langle e, \sigma\rangle \longrightarrow \langle e', \sigma'\rangle}{\rho \vdash_{\alpha,(\mathbf{val},\mu)} \langle (e, ae), \sigma\rangle \longrightarrow \langle (e', ae), \sigma'\rangle}$$

  (2) $$\frac{\rho \vdash_\alpha \langle ae, \sigma\rangle \longrightarrow \langle ae', \sigma'\rangle}{\rho \vdash_{\alpha,(\mathbf{val},\mu)} \langle (con, ae), \sigma\rangle \longrightarrow \langle (con, ae'), \sigma'\rangle}$$

  Ref. Mode: (1) $\rho \vdash_{\alpha,(\mathbf{ref},\mu)} \langle (x, ae), \sigma\rangle \longrightarrow \langle (l, ae), \sigma\rangle$ (if $\rho(x) = l$)

  (2) $$\frac{\rho \vdash_{\alpha,\mu} \langle ae, \sigma\rangle \longrightarrow \langle ae', \sigma'\rangle}{\rho \vdash_{\alpha,(\mathbf{ref},\mu)} \langle (l, ae), \sigma\rangle \longrightarrow \langle (l, ae'), \sigma'\rangle}$$

- **Definitions:**

  Simple: (1) $$\frac{\rho \vdash_{\alpha,\mu} \langle ae, \sigma\rangle \longrightarrow \langle ae', \sigma'\rangle}{\rho \vdash_\alpha \langle form = ae, \sigma\rangle \longrightarrow \langle form = ae', \sigma'\rangle} \qquad (\text{if } \mu = M(T(form)))$$

  (2) $$\frac{acon, L \vdash form : \rho_0, \sigma_0}{\rho \vdash_\alpha \langle form = acon, \sigma\rangle \longrightarrow \langle \rho_0, \sigma \cup \sigma_0\rangle} \qquad (\text{where } \sigma : L)$$

  Formals: We just add a rule for declaration-by-reference (= location)

  $$\frac{acon, L \vdash form : \rho_0, \sigma_0}{(l, acon), L \vdash \mathbf{loc}\ x : \tau, form : \{x = l\} \cup \rho_0, \sigma_0}$$

  Note: All we have done is to include the construct $x == y$ of Chapter 3 in our simple declarations.

- **Commands:** No new rules are needed.

Clearly our discussion of binding mechanisms is only a start, even granting the ground covered in the exercises. I hope the reader will have been led to believe that a more extensive coverage is feasible. What is missing is a good guiding framework to permit a systematic coverage.

7.4 Higher Types

Since we can define or declare abstractions, such as functions and procedures, Tennent's Principle of Correspondence tells us that we can allow abstractions themselves as parameters of (other) abstractions. The resulting abstractions are said to be of *higher types* (the resulting functions are often called *functionals*). For example the following recursive definition is of a function to apply a given function, f, to a given argument, x, a given number, t, of times:

$$\begin{array}{l}\textbf{rec}\ \text{Apply}(f : \text{nat} \longrightarrow \text{nat}, x : \text{nat}, t : \text{nat}) : \text{nat} = \\ \quad \textbf{if}\ t = 0\ \textbf{then}\ x\ \textbf{else}\ \text{Apply}(f, f(x), t - 1)\end{array}$$

We will illustrate this idea by considering a suitable extension of the imperative language of this chapter (but neglecting call-by-reference). Another principle would be to allow any denotable type to be an expressible type; this principle would allow locations or functions and procedures as expressions and, in particular, as results of functions (by the Principle of Abstraction). For example we could define an expression (naturally, called an *abstraction*)

$$\lambda \mathit{form}.\ e$$

that would be an abbreviation for the expression **let** $f(\mathit{form}) : \tau = e$ **in** f. For a suitable τ, depending on the context, it might, more naturally, be written as: **function** *form. e*; such functions (and other similar abstractions) are often termed anonymous. Then the following function would output the composition of two given functions

$$\text{Compose}(f : \text{nat} \to \text{nat}, g : \text{nat} \to \text{nat}) : \text{nat} \to \text{nat} = \lambda x : \text{nat}.\ f(g(x))$$

In this way we obtain (many) versions of the typed λ-calculus. A number of problems arise in imperative languages where functions are not denotable, but only references to them. In the definition of Compose one will have locally declared references to functions as the denotations of f and g; if these are disposed of upon termination of the function call one will have a dangling reference. Just the same thing happens, but in an even more bare-faced way, if we allow locations as outputs

$$\textbf{function}\ f() : \text{nat}\ \textbf{loc}\ =\ \textbf{let var}\ x : \text{nat} = 5\ \textbf{in}\ x$$

At any rate we will leave these issues to exercises, being moderately confident they can be handled along the lines we have developed.

Now, let us turn to our language with higher types. We extend the syntax by including the category AcETypes of actual expression types:

$$aet ::= \cdot \mid \tau, aet \mid (aet \longrightarrow \tau), aet \mid aet\ \mathbf{proc}, aet$$

and then add to the stock of formals

$$form ::= \mathbf{function}\ f : aet \to \tau, form \mid \mathbf{procedure}\ p : aet, form$$

It is clear how this allows functions and procedures of higher type to be defined; they are passed as arguments via identifiers that denote them.

Static Semantics

Clearly

$$\mathrm{DI}(\mathbf{function}\ f : aet \longrightarrow \tau, form) = \{f\} \cup \mathrm{DI}(form) \qquad \text{and}$$
$$\mathrm{DI}(\mathbf{procedure}\ p : aet, form) = \{p\} \cup \mathrm{DI}(form)$$

The definition of $T(form)$ in AcETypes is also evident and we note

$$T(\mathbf{function}\ f : aet \to \tau, form) = (aet \to \tau), T(form)$$
$$T(\mathbf{procedure}\ p : aet, form) = aet\ \mathbf{proc}, T(form)$$

As for the predicate $form : \beta$ we first note the definition of the set, DTypes, of denotable types:

$$dt ::= et \mid et\ \mathbf{loc} \mid aet \longrightarrow et \mid aet\ \mathbf{proc}$$

The rules are fairly clear and we just note the procedure case:

$$\frac{form : \beta}{\mathbf{procedure}\ p : aet, form : \{p = aet\ \mathbf{proc}\}, \beta} \qquad (\text{if } p \notin I \text{ where } \beta : I)$$

Turning to the other predicates we only need to add a rule for actuals:

$$\frac{\alpha \vdash_I ae : aet}{\alpha \vdash_I x, ae : dt, aet} \qquad (\text{where } dt = \alpha(x) \text{ is either of the form } aet \to et \text{ or } aet\ \mathbf{proc})$$

Example 33 *Try type-checking the following imperative version of Apply in the environment* $\{x = \mathrm{nat}\}$

```
function double(x : nat) : nat = 2 ∗ x
rec function apply(function f : nat → nat, x : nat, t : nat) : nat =
    let var result : nat = x in
    begin while t > 0 do begin x := f(x); t := t − 1 end
    result result; end
x := apply(double, x, x)
```

Once more there is no need to change (the form of) the definitions of DVal or Env or Dec. We must now allow abstracts within actual expressions and also AcCon

$$\begin{aligned} &ae ::= (\lambda form.\ e : \tau), ae \ \mid\ (\lambda form.\ c), ae \\ &acon ::= (\lambda form.\ e : \tau), acon \ \mid\ (\lambda form.\ c), acon \end{aligned}$$

with the evident extensions to the definitions of $\mathrm{FV}(ae)$ and $\alpha \vdash_I ae : aet$.

Transition Relations: In the following $\alpha : I$ and $J \subseteq I$.

- **Expressions:** We define configurations and terminal configurations as usual; for the transition relation we define for $\rho : \alpha \upharpoonright J$

  $$\rho \vdash_{\alpha,J} \langle e, \sigma\rangle \longrightarrow \langle e', \sigma'\rangle$$

- **Actual Expressions:** We take

  $$\Gamma_{\alpha,J} = \{\langle ae, \sigma\rangle \ \mid\ \mathrm{FI}(ae) \subseteq I\}$$

  and

  $$\mathrm{T}_{\alpha,J} = \{\langle acon, \sigma\rangle \ \mid\ \mathrm{FI}(acon) \cap J = \emptyset\}$$

  and for $\rho : \alpha \upharpoonright J$ the relation

  $$\rho \vdash_{\alpha,J} \langle ae, \sigma\rangle \longrightarrow \langle ae', \sigma'\rangle$$

- **Declarations:** We define $\Gamma_{\alpha,J}$, $\mathrm{T}_{\alpha,J}$ in the evident way, and the transition relation $\rho \vdash_{\alpha,J} \langle d, \sigma\rangle \longrightarrow \langle d', \sigma'\rangle$ is of the evident form.
- **Commands:** Again the configurations, the terminal configurations and the transition relation are of the evident forms.
- **Formals:** We will define the predicate $acon, L \vdash_J form : \rho_0, \sigma_0$ where $\mathrm{FI}(acon) \cap J = \emptyset$.

Rules: **Expressions**, **Declarations**, **Commands** as before.

- **Actual Expressions:** As before, plus

  $$\rho \vdash_{\alpha,J} \langle (x, ae), \sigma\rangle \longrightarrow \langle (abs, ae), \sigma\rangle \qquad (\text{if } \rho(x) = abs \in \text{Abstracts})$$

  $$\frac{\rho \vdash_{\alpha,J} \langle ae, \sigma\rangle \longrightarrow \langle ae', \sigma'\rangle}{\rho \vdash_{\alpha,J} \langle (abs, ae), \sigma\rangle \longrightarrow \langle (abs, ae'), \sigma'\rangle}$$

- **Formals:** We just need two more rules

  $$\frac{acon, L \vdash_J form : \beta}{((\lambda form.\ e : \tau), acon), L \vdash_J \ \mathbf{function}\ f : aet \to \tau, form : \{f = \lambda form.\ e : \tau\}, \beta}$$

(if $f \notin I$ where $\beta : I$)

$$\frac{acon, L \vdash_J form : \beta}{((\lambda form.\ e), acon), L \vdash_J \mathbf{procedure}\ p : aet, form : \{p = \lambda form.\ e\}, \beta}$$

(if $p \notin I$ where $\beta : I$)

As a matter of fact the J's are not needed, but we obtain finer control over the allowable actual expression configurations. This can be useful in extensions of our language where abstractions are allowed.

7.5 Modules and Classes

There is a certain confusion of terminology in the area of modules and classes. Rather than enumerate the possibilities let me say what I mean here. First there is a *Principle of Denotation* which says that one can in principle use an identifier to denote the value of any syntactic phrase – where "value" is deliberately ambiguous and may indicate various degrees of "evaluation". For expressions this says we can declare constants (in imperative languages) but also allows declaration by name or by text and so on; for commands it means we can have parameterless subroutines. For declarations we take it as meaning one can declare identifiers as modules, and they will denote the environment resulting from the elaboration. (There is a corresponding *Principle of Storeability* which the reader will spot for himself; it is anything but clear how useful these principles are!)

Applying the Principle of Abstraction to declarations on the other hand we obtain what we call classes. Applying a class to actual arguments gives a declaration which can be used to supply a denotation to a module identifier; then we say the module is an instance of the class. (Of course everything we say here applies just as well to applicative languages; by now, however, it is enough just to consider one case!)

A typical example is providing a random natural number facility. Let d_{rand} be the declaration

```
private
    var $a = seed$ mod $d$
within
    function $draw()$ : nat
    begin $a := a * m$ mod $d$
    result $a/d$ end
```

where *seed*, d and m are assumed declared previously. This would declare a function, *draw*, providing a random natural number with its own private variable – inaccessible from the outside. If one wanted to declare and use two random natural numbers, just declare two modules

module X : $draw : \cdot \to \text{nat} = d_{\text{rand}}$

module Y : *draw* : $\cdot \to$ nat $= d_{\text{rand}}$
begin . . . X.*draw*() . . . Y.*draw*() . . . **end**

Thus *draw* is an *attribute* of both X and Y and the syntax X.*draw* selects the attribute (in general there is more than one).

When one wants some parameterisation and/or desires to avoid writing out d_{rand} several times, one can declare and use a *class*

```
class random(const seed : nat, const d : nat) : draw : · → nat; d_rand;
begin
    ⋮
    module X : draw : · → nat = random(5, 2);
    module Y : draw : · → nat = random(2, 3);
    begin . . . X.draw() . . . Y.draw() . . . end
    ⋮
end
```

Finally we note that it is possible to use the compound forms of declarations to produce similar effects on classes. For example a version of the SIMULA class-prefixing idea is available.

```
class CLASS1(form1) . . . ; . . . ;
class CLASS2(form2)—; —;
class PREFIXCLASS(form1, form2) . . . —;
        CLASS1(form1); CLASS2(form2)
```

Naturally we will also be able to use simultaneous and private and recursive class declarations (can you tell me some good examples of the use of these?). One can also easily envisage classes of higher types (classicals?), but we do not investigate this idea.

Here is our extension of the syntax of the imperative language of the present chapter (but no call-by-reference, or higher types).

- **Types:** We need the categories DTSpecs, AcETypes and DecTSpecs of denotable type specifications, actual expression types and declaration type specifications

  $$dts ::= \tau \mid \tau\ \mathbf{loc} \mid aet \to \tau \mid aet\ \mathbf{proc} \mid dects \mid aet \to dects$$
  $$aet ::= \cdot \mid \tau, aet$$
  $$dects ::= x : dts \mid x : dts, dects$$

  Clearly *dect* will be the type of a module identifier and *aet* $\to$ *dect* will be the type of a class identifier.
- **Expressions:** We add five(!!) new categories of expressions, function, procedure, variable, module and class expressions, called FExp, PExp, VExp, MExp, CExp and ranged over by

fe, pe, ve, me, cle and given by the following productions (where we also allow f, p, v, m, cl as metavariables over the set, Id, of identifiers)

$$\begin{aligned}
&fe ::= f \mid me.f\\
&pe ::= p \mid me.p\\
&ve ::= v \mid me.v\\
&me ::= m \mid me.m \mid cle(ae)\\
&cle ::= cl \mid me.cl
\end{aligned}$$

The definition of the set of expressions is extended by

$$e ::= me.x \mid fe(ae)$$

(and the second possibility generalises expressions of the form $f(ae)$). The set of actual expressions is defined as before.

- **Commands:** We generalize commands of the forms $p(ae)$ and $x := e$ (i.e., procedure calls and assignment statements) by

  $$c ::= pe(ae) \mid ve := e$$

- **Declarations:** We add the following productions to the definition

  $$d ::= \textbf{module}\ m : dects = d \mid \textbf{class}\ cl(form) : dects; d$$

  Note that declaration types are used here to specify the types of the attributes of modules and classes. If we except recursive declarations this information is redundant, but it could be argued that it increases readability as the attribute types may be buried deep inside the declarations.
- **Formals:** The definition of these remains the same as we do not want class or module parameters.

Note: In this chapter we have essentially been following a philosophy of different expressions for different uses. This is somewhat inconsistent with previous chapters where we have merged different kinds of expressions (e.g., natural number and boolean) and been content to separate them out again via the static semantics. By now the policy of this chapter looks a little ridiculous and it could well be better to merge everything together. However, the reader may have appreciated the variation.

Static Semantics

For the definitions of $\mathrm{FI}(fe), \ldots, \mathrm{FI}(cle)$ we do not regard the attribute identifiers as free (but rather as a different use of identifiers from all previous ones; their occurrences are the same as constant occurrences and they are thought of as standing for themselves). So for example

FI(me) is given by the table

	m	$me.m$	$cle(ae)$
FI	$\{m\}$	FI(me)	FI(cle) $\cup$ FI(ae)

For the definitions of FI(e), FI(c) we put

$$\begin{aligned}
\mathrm{FI}(me.x) &= \mathrm{FI}(me)\\
\mathrm{FI}(fe(ae)) &= \mathrm{FI}(fe) \cup \mathrm{FI}(ae)\\
\mathrm{FI}(pe(ae)) &= \mathrm{FI}(pe) \cup \mathrm{FI}(ae)\\
\mathrm{FI}(ve := e) &= \mathrm{FI}(ve) \cup \mathrm{FI}(e)
\end{aligned}$$

and for FI(d) and DI(d) we have

	module $m : dect = d$	**class** $cl(form) : dect; d$
FI	FI(d)	FI(d)\DI($form$)
DI	$\{m\}$	$\{d\}$

(We are really cheating somewhere here. For example the above scheme would not work if we added the reasonable production

$d ::= me$

as then with, for example, a command m; **begin** $\ldots x \ldots$ **end** the x can be in the scope of the m if the command is in the scope of a declaration of the form **module** $m : dect =$ **var** x : nat $= \ldots ; \ldots$

Thus it is no longer possible to define the free identifiers of a phrase in a context-free way. Let us agree to ignore the problem.)

- **Types:** We define (mutually recursively) the sets ETypes, FETypes, . . . , ClETypes, DTypes, TEnv of expression types, function expression types, . . . , class expression types, denotable types and type environments by

$$\begin{aligned}
&et ::= \tau\\
&fet ::= aet \to \tau\\
&pet ::= aet\ \mathbf{proc}\\
&vet ::= \tau\ \mathbf{loc}\\
&met ::= \alpha\\
&clet ::= aet \longrightarrow \alpha\\
&dt ::= et \mid vet \mid fet \mid pet \mid met \mid clet
\end{aligned}$$

$$\text{TEnv} = \text{Id} \longrightarrow_{\text{fin}} \text{DTypes} \qquad (\text{with } \alpha \text{ ranging over TEnv})$$

To see how the sets DTSpecs and DecTSpecs of denotable and declaration type specifications specify denotable and declaration types respectively, we define predicates

$$\mathit{dts} : \mathit{dt} \qquad \text{and} \qquad \mathit{dects} : \mathit{dect}$$

by the formulae

- **DTSpecs:**

(1) $\tau : \tau$

(2) $\tau\ \mathbf{loc} : \tau\ \mathbf{loc}$

(3) $\mathit{aet} \to \tau : \mathit{aet} \to \tau$

(4) $\mathit{aet}\ \mathbf{proc} : \mathit{aet}\ \mathbf{proc}$

(5) $\dfrac{\mathit{dects} : \alpha}{\mathit{dects} : \alpha}$ (where the premise means proved from the rules for DecTSpecs)

(6) $\dfrac{\mathit{dects} : \alpha}{\mathit{aet} \to \mathit{dects} : \mathit{aet} \to \alpha}$

- **DecTSpecs:**

(1) $\dfrac{\mathit{dts} : \alpha}{(x : \mathit{dts}) : \{x = \alpha\}}$

(2) $\dfrac{\mathit{dts} : \alpha \qquad \mathit{dects} : \beta}{(x : \mathit{dts}, \mathit{dets}) : \{x = \alpha\} \cup \beta}$ (if $x \notin I$ for $\beta : I$)

Next $T(\mathit{form}) \in$ AcETypes is defined as before. Now we must define the predicates

$$\alpha \vdash_I e : \mathit{et} \qquad \alpha \vdash_I \mathit{fe} : \mathit{fet}, \ldots, \alpha \vdash_I \mathit{cle} : \mathit{clet}, \alpha \vdash_I c,$$
$$\vdash_I d : \beta \qquad \alpha \vdash_I d\,\mathit{form} : \beta$$

The old rules are retained and we add new ones as indicated by the following examples.

- **Expressions:**

(1) $\dfrac{\alpha \vdash_I \mathit{me} : \beta}{\alpha \vdash_I \mathit{me}.x : \mathit{dt}}$ (if $\beta(x) = \mathit{dt}$)

(2) $\dfrac{\alpha \vdash_I \mathit{fe} : \mathit{aet} \to \mathit{et} \quad \alpha \vdash_I \mathit{ae} : \mathit{aet}}{\alpha \vdash_I \mathit{fe}(\mathit{ae}) : \mathit{et}}$

- **Function Expressions:**

(1) $\alpha \vdash_I f : \mathit{ft}$ (if $\alpha(f) = \mathit{ft} \in$ FTypes)

(2) $\dfrac{\alpha \vdash_I \mathit{me} : \beta}{\alpha \vdash_I \mathit{me}.f : \mathit{ft}}$ (if $\beta(f) = \mathit{ft} \in$ FTypes)

- **Class Expressions:**

(1) $\alpha \vdash_I \mathit{cle} : \mathit{clet}$ (if $\alpha(\mathit{cl}) = \mathit{clet} \in$ ClETypes)

(2) $\dfrac{\alpha \vdash_I \mathit{me} : \beta}{\alpha \vdash_I \mathit{me}.\mathit{cl} : \mathit{clet}}$ (if $\beta(\mathit{cl}) = \mathit{clet} \in$ ClETypes)

- **Commands:**

(1) $\dfrac{\alpha \vdash_I pe : aet\ \mathbf{proc} \quad \alpha \vdash_I ae : clet}{\alpha \vdash_I pe(ae)}$

(2) $\dfrac{\alpha \vdash_I vet : \tau\ \mathbf{loc} \quad \alpha \vdash_I e : \tau}{\alpha \vdash_I (vet := e)}$

• **Declarations:**

- **Modules:**

(1) $\dfrac{dects : \beta}{(\mathbf{module}\ m : dects = d) : \{m = \beta\}}$

(2) $\dfrac{dects : \beta \quad \alpha \vdash_I d : \beta}{\alpha \vdash_I \mathbf{module}\ m : dects = d}$

- **Classes:**

(1) $\dfrac{dects : \beta}{(\mathbf{class}\ cl(form) : dects; d) : \{cl = T(form) \longrightarrow \beta\}}$

(2) $\dfrac{dects : \beta\ form : \alpha_0 \quad \alpha[\alpha_0] \vdash_{I \cup I_0} d : \beta}{\alpha \vdash_I \mathbf{class}\ cl(form) : dects : d}$ (where $\alpha_0 : I_0$)

Dynamic Semantics

First we define the sets FECon, ... , ClECon of function expression constants, ... , class expression constants by

$fecon ::= \lambda form.\ e : et$
$pecon ::= \lambda form.\ c$
$vecon ::= l$
$mecon ::= \rho$
$clecon ::= \lambda form.\ d : \beta$

and also add the productions

$fe ::= fecon, \ldots, cle ::= clean \mid d$

and define the sets DVal and Env of denotable values and environments by

$dval ::= con \mid vecon \mid fecon \mid pecon \mid clecon \mid mecon$
$\mathrm{Env} = \mathrm{Id} \longrightarrow_{\mathrm{fin}} \mathrm{DVal}$

and extend the definition of declarations by the production

$d ::= \rho$

These are mutually recursive definitions of a harmless kind. The extensions to the definition of $\mathrm{FI}(fe), \ldots, \mathrm{FI}(de), \mathrm{FI}(d), \mathrm{DI}(d)$ are evident; for example $\mathrm{FI}(\lambda form.\ d : \beta) = \mathrm{FI}(d) \backslash \mathrm{DI}(form)$.

We must also extend the definitions of $\alpha \vdash_I fe : fet, \ldots, \alpha \vdash_I cle : clet$ and $\vdash_I d : \beta$ and $\alpha \vdash_I d$ (the latter two in the case $d = \rho$). The former extensions are obvious; for example

- **Class Abstracts:**

$$\frac{\mathit{form} : \alpha_0 \quad \alpha[\alpha_0] \vdash_{I \cup I_0} d : \beta}{\alpha \vdash_I (\lambda \mathit{form}.\ d : \beta)} \qquad \text{(where } \alpha_0 : I_0\text{)}$$

For the latter we have to define $\vdash_I \mathit{decon} : \mathit{dt}$ and this also presents little difficulty; for example

- **Class Abstracts:**

$$\vdash_I (\lambda \mathit{form}.\ d : \beta) : T(\mathit{form}) \to \beta$$

Then we have the two rules

$$(1) \quad \frac{\forall x \in I_0 \quad \vdash_I \rho(x) : \beta(x)}{\vdash_I \rho : \beta} \qquad \text{(where } \rho : I_0\text{)}$$

$$(2) \quad \frac{\forall x \in I_0 \quad \alpha \vdash_I \rho(x) : \beta(x)}{\alpha \vdash_I \rho}$$

Transition Relations: The set, Stores, is as before.

The configurations, final configurations and the transition relations for expressions, actual expressions and declarations are as before; for formals we have the same predicate as before. Now fix $\alpha : I$ and $\rho : \alpha \restriction J$ (for some $J \subseteq I$).

- **Function Expressions:** We take $\Gamma_\alpha = \{\langle fe, \sigma\rangle \mid \exists fet.\ \alpha \vdash_I fe : fet\}$, $T_\alpha = \{\langle fecon, \sigma\rangle \mid \exists fet.\ \alpha \vdash_I fecon : fet\}$ and the transition relation has the form $\rho \vdash_I \gamma \longrightarrow \gamma'$

The definitions for PExp, ... , CExp are the analogues of that for function expressions

Rules:

- **Class Expressions:**

(1) $\rho \vdash_\alpha \langle \mathit{cl}, \sigma\rangle \longrightarrow \langle \mathit{clecon}, \sigma\rangle \qquad$ (if $\rho(\mathit{cl}) = \mathit{clecon}$)

$$(2) \quad \frac{\rho \vdash_\alpha \langle \mathit{me}, \sigma\rangle \longrightarrow \langle \mathit{me}', \sigma'\rangle}{\rho \vdash_\alpha \langle \mathit{me}.\mathit{cl}, \sigma\rangle \longrightarrow \langle \mathit{me}'.\mathit{cl}, \sigma\rangle}$$

(3) $\rho \vdash_\alpha \langle \rho_0.\mathit{cl}, \sigma\rangle \longrightarrow \langle \mathit{clecon}, \sigma\rangle \qquad$ (if $\rho_0(\mathit{cl}) = \mathit{clecon}$)

The rules for FExp, ... , MExp are similar except that in the last case we need also

$$(1) \quad \frac{\rho \vdash_\alpha \langle \mathit{cle}, \sigma\rangle \longrightarrow \langle \mathit{cle}', \sigma'\rangle}{\rho \vdash_\alpha \langle \mathit{cle}(\mathit{ae}), \sigma\rangle \longrightarrow \langle \mathit{cle}'(\mathit{ae}), \sigma'\rangle}$$

(2) $\rho \vdash_\alpha \langle (\lambda \mathit{form}.\ d : \beta)(\mathit{ae}), \sigma\rangle \longrightarrow \langle \textbf{private}\ \mathit{form} = \mathit{ae}\ \textbf{within}\ d, \sigma\rangle$

$$(3) \quad \frac{\rho \vdash_\alpha \langle d, \sigma\rangle \longrightarrow \langle d', \sigma'\rangle}{\rho \vdash_\alpha \langle d, \sigma\rangle \longrightarrow \langle d', \sigma'\rangle} \qquad \text{(where in the top line we mean a transition of Decl)}$$

The new rules for expressions and commands should be clear; for example

- **Assignment:**

(1) $$\frac{\rho \vdash_\sigma \langle ve, \sigma\rangle \longrightarrow \langle ve', \sigma'\rangle}{\rho \vdash_\alpha \langle ve := e, \sigma\rangle \longrightarrow \langle ve' := e, \sigma'\rangle}$$

(2) $$\frac{\rho \vdash_\alpha \langle e, \sigma\rangle \longrightarrow \langle e', \sigma'\rangle}{\rho \vdash_\alpha \langle l := e, \sigma\rangle \longrightarrow \langle l := e', \sigma'\rangle}$$

(3) $\rho \vdash_\alpha \langle l := \mathit{con}, \sigma\rangle \longrightarrow \sigma[l = \mathit{con}]$

For declarations the new rules are

- **Modules:**

(1) $$\frac{\rho \vdash_\alpha \langle d, \sigma\rangle \longrightarrow \langle d', \sigma'\rangle}{\rho \vdash_\alpha \langle \textbf{module}\ m : \mathit{dects} = d, \sigma\rangle \longrightarrow \langle \textbf{module}\ m : \mathit{dects} = d', \sigma'\rangle}$$

(2) $\rho \vdash_\alpha \langle \textbf{module}\ m : \mathit{dects} = \rho_0, \sigma\rangle \longrightarrow \langle \{m = \rho_0\}, \sigma\rangle$

- **Classes:**

$\rho \vdash_\alpha$ $\textbf{class}\ \mathit{cl}(\mathit{form}) : \mathit{dects};\ d \longrightarrow \{\mathit{cl} = \lambda \mathit{form}.\ (\rho \backslash I)\ \textbf{in}\ d\}$ (where $I = \mathrm{DI}(\mathit{form})$)

7.6 Exercises

1. Consider dynamic binding in the context of a simple applicative language so that, for example,

$\textbf{let}\ x = 1;\ f(y) = x + y$
$\textbf{in let}\ x = 2\ \textbf{in}\ f(3)$

has value 5. What issues arise with type-checking? Can you program iterations (e.g., factorial) without using recursive function definitions?

2. In a maximalist solution to the problem (in the applicative language) of neatly specifying functions of several arguments one could define the class of formal parameters by

$\mathit{form} ::= \cdot \mid x : \tau \mid \mathit{form}, \mathit{form}$

and merge expressions and actual expressions, putting

$e ::= \cdot \mid e, e \mid f(e)$

and amending the definition of definitions

$d ::= \mathit{form} = e \mid f(\mathit{form}) : \tau = e$

a) Do this, but effectively restrict the extension to the minimalist case by a suitable choice of static semantics.

b) Allow the full extension.
c) Go further and extend the types available in the language by putting

$$\tau ::= \mathrm{nat} \mid \mathrm{bool} \mid \tau, \tau \mid \cdot$$

thus allowing tuples to be denotable.

3. Consider the maximalist position in a simple imperative programming language.

4. Consider in a simple imperative language how to allow expressions on the left-hand of assignments:

$$e_0 := e_1$$

and even the boolean expression $e_0 \equiv e_1$ which is true precisely when e_0 and e_1 evaluate to the same reference. As well as discussing type-checking issues, try the two following approaches to expression evaluation:
a) Expressions are evaluated to their natural values which will be either locations or basic values.
b) Modes of evaluation are introduced, as in the text.
Extend the work to the maximalist position where actual expressions and expressions are merged, thus allowing simultaneous assignments.

5. Just as expressions are evaluated, and so on, formals are matched (to given actual values) to produce environments (= matchings). The semantics given above can be criticised as not being dynamic enough as the matching *process* is not displayed. Provide an answer to this; you may find configurations of the form

$$\langle \mathit{form}, \mathit{con}, \rho \rangle$$

useful where *form* is the formal being matched, *con* is the actual value and ρ is the matching produced so far. A typical rule could be

$$\langle x : \tau, \mathit{con}\ \rho \rangle \longrightarrow \rho \cup \{x = \mathit{con}\}$$

This is all for the applicative case; what about the imperative one? Investigate dynamic errors, allowing constants and repeated variables in the formals (dynamic error = matching failure).

6. In the phrase **rec** d all identifiers in $R = \mathrm{FV}(d) \cap \mathrm{DV}(d)$ are taken to be recursively defined. Investigate the alternative **rec** $x_1, \ldots, x_n.d$ where $\{x_1, \ldots x_n\} \subseteq R$.

7. In some treatments of recursion to evaluate an expression of the form

$$\textbf{let rec}\ (f(x) = \ldots f \ldots g \ldots\ \textbf{and}\ g(x) = \text{---}\ f\ \text{---}\ g\ \text{---})\ \textbf{in}\ f(5)$$

one evaluates $f(5)$ in the environment

$$\rho = \{f(x) = \ldots f \ldots g \ldots, g(x) = \text{—}\, f \,\text{—}\, g \,\text{—}\}$$

(ignoring free variables) and uses the simple transition:

$$\rho \vdash f(5) \longrightarrow \textbf{let } x = 5 \textbf{ in } \ldots f \ldots g \ldots$$

I could not see how to make this simple and nice idea (leave the recursively defined variables free) work in the present setting where one has nested definitions and binary operations on declarations. Can you make it work?

8. Try some examples of the form

$$\textbf{let rec } (f(x) = \ldots f \ldots g \ldots \;\&\; g(x) = \text{—}\, f \,\text{—}\, g \,\text{—}) \textbf{ in } e$$

where & is any of ;, **and** or **in**.

9. Consider the following recursive definitions of constants:

a) $\textbf{rec } x : \text{nat} = 1$

b) $\textbf{rec } (y : \text{nat} = 1 \textbf{ and } x : \text{nat} = y)$

c) $\textbf{rec } (x : \text{nat} = y \textbf{ and } y : \text{nat} = 1)$

d) $\textbf{rec } (x : \text{nat} = x)$

e) $\textbf{rec } (x : \text{nat} = y \textbf{ and } y : \text{nat} = x)$

How are these treated using the above static and dynamic semantics? What do you think should happen? Specify suitable static and dynamic semantics with any needed error rules. Justify your decisions, considering how your ideas will extend to imperative languages with side-effects (which might result in non-determinism).

10 Find definitions d_0 and d_1 to make different as many as possible of the following definitions:

a) $(\textbf{rec } d_0;\ d_1)$

b) $(\textbf{rec})\ (\textbf{rec } d_0;\ d_1)$

c) $(\textbf{rec})\ (d_0;\ \textbf{rec } d_1)$

d) $(\textbf{rec})\ (\textbf{rec } d_0;\ \textbf{rec } d_1)$

where (**rec**) d indicates the two possibilities with and without **rec**.

11. Check that the first alternative for type-checking recursive definitions would work in the sense that

$$\alpha \vdash_V d : \beta \quad \text{iff} \quad \vdash_V d : \beta \textbf{ and } \alpha \vdash_V d$$

12. Programming languages like PASCAL often adopt the following idea for function definition:

```
**function** $f(form) : \tau$
**begin**
    $c$
**end**
```

where within c the identifier f as well as possibly denoting a function also denotes a location, created on function entry and destroyed on exit; the result of a function call is the final value of this location on exit. For example the following is an obscure definition of the identity function:

```
rec function $f(x : \text{nat}) : \text{nat}$
    begin
        $f := 1$;
        if $x = 0$ then $f := 0$
        else $f := f + f(x - 1)$
    end
```

Give this idea a semantics.

13. *Call-by-need.* In applicative languages this is a "delayed evaluation" version of call-by-name. As in call-by-name the formal is bound to the unevaluated actual, with the local environment bound in the closure. However, when it is necessary for the first time to evaluate the actual, the formal is then bound to the result of the evaluation. Give this idea a semantics. One possibility is to put (some of) the environment into the configurations, treating it like a store. Another is to bind the actual to a new location and make the actual the value of that location in a store. Prove call-by-need equivalent to call-by-name. Consider delayed evaluation variants of parameter mechanisms found in imperative languages.

14. *Call-by-name.* Consider (minimalist & maximalist) versions of call-by-name in imperative programming languages. Look out for the dangers inherent in

```
procedure $f(x : \mathrm{nat}\ \mathbf{name}) =$
begin
    ⋮
    $x := \cdots$
    ⋮
end
```

15. Discover the official ALGOL 60 definition of call-by-name (it works via a substitution process); give a semantics following the idea and prove it equivalent to one following the idea in these notes (substitution = binding a closure).

16. *Call-by-text.* Give a semantics for call-by-text where the formal is bound to the actual (not binding in the current environment); when a value is desired the actual is evaluated in the then current environment. Consider also more "concrete" languages in which the abstract syntax (of the text) is available to the programmer, or even the concrete syntax: does the latter possibility lead to any alteration of the current framework?

17. *Call-by-reference.* Give a maximalist discussion of call-by-reference, still only allowing actual reference parameters to be variables. Extend this to allow a wider class of expressions which (must) evaluate to a reference. Extend that in turn to allow *any* expression as an actual; if it does not evaluate to a reference the formal should be bound to a new reference and that should have the value of the actual.

18. *Call-by-result.* Discuss this mechanism where first the actual is evaluated to a reference, l; second the formal is bound to a new reference l' (not initialised); third, *after* computation of the body of the abstract, the value of l is set to the value of l' in the then current store. Discuss too a variant where the actual is not evaluated at all until after the body for the abstract. [Hint: Use declaration finalisation.]

19. *Call-by-value-result.* Discuss this mechanism where first the actual is evaluated to a reference l; second the formal is bound to a new reference l' which is initialised to the current value of l; third, *after* the computation of the abstract of the body, the value of l is set to the value of l' in the then current store.

20. Discuss *selectors* which are really just functions returning references. A suitable syntax might be

selector $f(\mathit{form}) : \tau = e$

which means that f returns a reference to a τ value. First consider the case where all lifetimes are semi-infinite (extending beyond block execution). Second consider the case where lifetimes do not persist beyond the block where they were created; in this case interesting questions arise in the static semantics.

21. Consider higher-order functions in programming languages which may return abstracts such as functions or procedures. Thus we add the syntax:

$$e ::= \lambda \mathit{form}.\ e \mid \lambda \mathit{form}.\ c$$

The issues that arise include those of lifetime addressed in exercise 20.

22. Here is a version of the typed λ-calculus

$$\tau ::= \mathrm{nat} \mid \mathrm{bool} \mid \tau \longrightarrow \tau$$

$$e ::= m \mid t \mid x \mid e\ \mathit{bop}\ e \mid \mathbf{if}\ e\ \mathbf{then}\ e\ \mathbf{else}\ e \mid$$
$$\mathbf{let}\ x : \tau = e\ \mathbf{in}\ e \mid e(e) \mid \lambda x : \tau.\ e$$

Give a static semantics and two dynamic semantics where the first one is a standard one using environments and where the second one is for closed expressions only and uses substitutions as discussed in the exercises of Chapter 3. Prove these equivalent. Add a recursion operator expression

$$e ::= Y$$

with the static semantics $\alpha \vdash_V Y : (\tau \longrightarrow \tau) \longrightarrow \tau\ (\tau \neq \mathrm{nat}, \mathrm{bool})$ and a rule something like $\rho \vdash Ye_0 \longrightarrow e_0(Ye_0)$. What does this imply about formals which are of functional type and their evaluation, and why is that important?

A A Guide to the Notation

Syntactic Categories	
Truthvalues	$t \in \mathrm{T}$
Numbers	$m, n \in \mathrm{N}$
Constants	$con \in \mathrm{Con}$
Actual Constants	$acon \in \mathrm{ACon}$
Unary Operations	$uop \in \mathrm{Uop}$
Binary Operations	$bop \in \mathrm{Bop}$
Variables	$v, f \in \mathrm{Var} \qquad V \subseteq_{\mathrm{fin}} \mathrm{Var}$
Identifiers	$x, f, p, m, cl \in \mathrm{Id} \qquad I \subseteq_{\mathrm{fin}} \mathrm{Id}$
Expressions	$e \in \mathrm{Exp}$
Boolean	$b \in \mathrm{BExp}$
Actual	$ae \in \mathrm{AExp}$
Variable	$ve \in \mathrm{VExp}$
Function	$fe \in \mathrm{FExp}$
Procedure	$pe \in \mathrm{PExp}$
Module	$me \in \mathrm{MExp}$
Class	$cle \in \mathrm{CExp}$
Commands (=Statements)	$c \in \mathrm{Com}$
Definitions/ Declarations	$d \in \mathrm{Def/Dec}$
Formals	$form \in \mathrm{Forms}$
Types	$\tau \in \mathrm{Types}$
Expression	$et \in \mathrm{ETypes}$
Actual Expr.	$aet \in \mathrm{AETypes}$
Denotable Type Spec.	$dts \in \mathrm{DTSpecs}$
Declaration Type Spec.	$dects \in \mathrm{DecTSpecs}$
Static Semantics	
Free Variables/ Identifiers	$\mathrm{FV/I}(e), \mathrm{FI}(c), \mathrm{FV/I}(d)$ etc.
Defined Variables/ Identifiers	$\mathrm{DV/I}(d) \ \ \mathrm{DV/I}(form)$

Denotable Types	$dt \in$ DTypes
Type Environments	$\alpha, \beta \in$ TEnv (e.g., = Id $\longrightarrow_{\text{fin}}$ DTypes)
Example Formulae	$\alpha \vdash_V e : et \quad \alpha \vdash_I c \quad \alpha \vdash_I d : \beta$
	$form : \beta \;\; T(form) = aet$
Dynamic Semantics	
Denotable Values	$dval \in$ DVal
Environments	$\rho \in$ Env (e.g., = Id $\longrightarrow_{\text{fin}}$ DVal)
Storeable Types	$st \in$ STypes
Locations	$l \in \text{Loc} = \sum_{st} \text{Loc}_{st} \qquad L \subseteq_{\text{fin}} \text{Loc}$
Storeable Values	$sval \in \text{SVal} = \sum_{st} \text{Val}_{st}$
Stores	$\sigma \in Stores$ (e.g., $= \{\sigma \in \text{Loc} \longrightarrow_{\text{fin}} \text{SVal} \mid \forall st \in \text{STypes}.\ \sigma(\text{Loc}_{st}) \subseteq \text{SVal}_{st}\}$)
Evaluation Modes	$\mu \in$ Modes
Transition Systems	$\langle \Gamma, T, \longrightarrow \rangle \qquad \gamma \in \Gamma$
	where Γ is the set of configurations
	$T \subseteq \Gamma$ is the set of *final* configurations
	$\gamma \longrightarrow \gamma'$ is the *transition* relation
Example Configurations	$\langle e, \sigma \rangle$; $\langle c, \sigma \rangle, \sigma$; $\langle d, \sigma \rangle$
Example Final Configurations	$\langle con, \sigma \rangle; \sigma; \langle \rho, \sigma \rangle$
Example Transition Relations	$\rho \vdash_{I,\mu} \langle e, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle$
	$\rho \vdash_I \langle c, \sigma \rangle \longrightarrow \langle c', \sigma' \rangle / \sigma'$
	$\rho \vdash_I \langle d, \sigma \rangle \longrightarrow \langle d', \sigma' \rangle / \rho'$

B Notes on Sets

We use several relations over and operations on sets as well as the (very) standard ones. For example $X \subseteq_{\text{fin}} Y$ means X is finite and a subset of Y.

Definition 34 *Let $Op(X_1, \ldots, X_n)$ be an operation on sets. It is monotonic if whenever $X_1 \subseteq X_1', \ldots, X_n \subseteq X_n'$ we have $Op(X_1, \ldots, X_n) \subseteq Op(X_1', \ldots, X_n')$. It is continuous if whenever $X_1^1 \subseteq X_1^2 \ldots \subseteq X_1^m \subseteq \ldots$ is an increasing sequence and $\ldots$ and $X_n^1 \subseteq X_n^2 \subseteq \ldots \subseteq X_n^m \subseteq \ldots$ is an increasing sequence then*

$$(*) \quad Op(\bigcup_m X_1^m, \ldots, \bigcup_m X_n^m) = \bigcup_m Op(X_1^m, \ldots, X_n^m)$$

Note: Continuity implies monotonicity. Conversely to prove continuity, first prove monotonicity. This establishes the $''\supseteq''$ half of $(*)$; then prove the $''\subseteq''$ half.

Example 35

- **Cartesian Product:**

$$X_1 \times \ldots \times X_n = \{\langle x_1, \ldots, x_n\rangle \mid x_1 \in X_1 \textit{ and } \ldots \textit{ and } x_n \in X_n\}$$

  is monotonic and continuous. Prove this yourself.
- **Disjoint Sum:**

$$\begin{aligned} X_1 + \ldots + X_n &\overset{def}{=} (\{1\} \times X_1) \cup \ldots \cup (\{n\} \times X_n) \\ \textstyle\sum_{i\in A} X_i &\overset{def}{=} \textstyle\bigcup_{i\in A} \{i\} \times X_i \end{aligned}$$

  Show that the finite sum operation is continuous. (Finite Sum is just union, but forced to be disjoint.)
- **Finite Functions:** *The class of finite functions from X to Y is*

$$X \to_{\text{fin}} Y = \sum_{A \subseteq_{\text{fin}} X} A \to Y$$

  Note that the union is necessarily disjoint. Show that $\to_{\text{fin}}$ is continuous.

For $A \subseteq_{\text{fin}} X$ if $f \in A \to Y \subseteq X \to_{\text{fin}} Y$ (we identify f with $\langle A, f\rangle$) we write $f : A$. This is used for environments (including type environments) and stores. There are two useful unary operations on finite functions. Suppose that $f : A$ and $B \subseteq A$. Then the *restriction* of f to B is written $f \restriction B$, and defined by:

$$(f \restriction B)(b) = f(b) \text{ (for } b \text{ in } B)$$

Note that $f \restriction B : B$. For any $C \subseteq X$ we also define f
$C = f \restriction (A \cap C)$.

There are also two useful binary operations. For $f : A$ and $g : B$ in $X \to_{\text{fin}} Y$ we define $f[g] : A \cup B$ by

$$f[g](c) = \begin{cases} g(c) & (c \in B) \\ f(c) & (c \in A \backslash B) \end{cases}$$

and in case $A \cap B = \emptyset$ we define $f, g : A, B$ (also written $f \cup g$) by:

$$f, g(c) = \begin{cases} f(c) & (c \in A) \\ g(c) & (c \in B) \end{cases}$$

Note this is a special case of the first definition, but it is very useful and worth separate mention.

Suppose $Op(X)$ is continuous and we want to find an X solving the equation

$$X = Op(X)$$

Put $X^0 = \emptyset$ and $X^{m+1} = Op(X^m)$. Then (by induction on m) we have for all m, $X^m \subseteq X^{m+1}$ and putting $X = \bigcup_m X^m$

$$\begin{aligned} Op(X) &= Op(\textstyle\bigcup_m X^m) \\ &= \textstyle\bigcup_m Op(X^m) \qquad \text{(by continuity)} \\ &= \textstyle\bigcup_m X^{m+1} \\ &= X \end{aligned}$$

And one can show (do so!) that X is the least solution – that is if Y is any other than $X \subseteq Y$. Indeed X is even the least set such that $Op(X) \subseteq X$.

This can be generalised, suppose $Op_1(X_1, \ldots, X_n), \ldots, Op_n(X_1, \ldots, X_n)$ are all continuous and we want to solve the n equations

$$\begin{aligned} X_1 &= Op_1(X_1, \ldots, X_n) \\ &\vdots \\ X_n &= Op_n(X_1, \ldots, X_n) \end{aligned}$$

Put $X_i^0 = \emptyset$ for $i = 1, \ldots, n$ and define

$$X_i^{m+1} = Op_i(X_1^m, \ldots, X_n^m)$$

Then for all m and i, $X_i^m \subseteq X_i^{m+1}$ (prove this) and putting

$$X_i = \bigcup_m X_i^m$$

we obtain the least solutions to the equations – if Y_i are also solutions then for all i, $X_i \subseteq Y_i$. Indeed the X_i are even the least sets such that $Op_i(X_i, \ldots, X_n) \subseteq X_i$ $(i = 1, \ldots, n)$. This is used in the example below. Prove this.

Example 36 *Suppose we are given sets Num, Id, Bop and wish to define sets Exp and Com by the abstract syntax*

$$e ::= m \mid x \mid e_0 \; bop \; e_1$$

$$e ::= x := e \mid c_0;\ c_1 \mid \textbf{if } e_0 = e_1 \textbf{ then } c_0 \textbf{ else } c_1 \mid \textbf{while } e_0 = e_1 \textbf{ do } c$$

Then we regard this definition as giving us set equations

$$\begin{aligned}
&\mathrm{Exp} = \mathrm{Num} + \mathrm{Id} + (\mathrm{Exp} \times \mathrm{Bop} \times \mathrm{Exp})\\
&\mathrm{Com} = (\mathrm{Id} \times \mathrm{Exp}) + \mathrm{Com} \times \mathrm{Com} + (\mathrm{Exp} \times \mathrm{Exp} \times \mathrm{Com} \times \mathrm{Com}) + (\mathrm{Exp} \times \mathrm{Exp} \times \mathrm{Com})
\end{aligned}$$

and also giving us a notation for working with the solution to the equations. First m *is identified with* $\langle 1, m\rangle \in \mathrm{Exp}$ *and* x *is identified with* $\langle 2, x\rangle$ *in Exp. Next*

$$\begin{aligned}
&e_0\ bop\ e_1 && = \langle 3, \langle e_0, bop, e_1\rangle\rangle\\
&x := e && = \langle 1, \langle x, e\rangle\rangle\\
&c_0;\ c_1 && = \langle 2, \langle c_0, c_1\rangle\rangle\\
&\mathbf{if}\ e_0 = e_1\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1 && = \langle 3, \langle e_0, e_1, c_0, c_1\rangle\rangle\\
&\mathbf{while}\ e_0 = e_1\ \mathbf{do}\ c_0 && = \langle 4, \langle e_0, e_1, c_0\rangle\rangle
\end{aligned}$$

Now the set equations are easily solved using the above techniques as they are in the form

$$\begin{aligned}
&Exp\ = Op_1(\mathrm{Exp}, \mathrm{Com})\\
&Com = Op_2(\mathrm{Exp}, \mathrm{Com})
\end{aligned}$$

where $Op_1(\mathrm{Exp}, \mathrm{Com}) = \mathrm{Num} + \mathrm{Id} + (\mathrm{Exp} \times \mathrm{Bop} \times \mathrm{Exp})$ *and* Op_2 *is defined similarly. Clearly* Op_1 *and* Op_2 *are continuous as they are built up out of (composed from) the continuous disjoint sum and product operations (prove they are continuous). Therefore we can apply the above techniques to find a least solution Exp, Com. Note that Exp and Com are therefore the least sets such that*

1. $\mathrm{Num} \subseteq \mathrm{Exp}$ *and* $\mathrm{Id} \subseteq \mathrm{Exp}$ *(using the above identifications).*

2. If e_0, e_1 *are in Exp and bop is in Bop then* $e_0\ bop\ e_1$ *is in Exp.*

3. If x *is in Id and* e *is in Exp then* $x := e$ *is in Com.*

4. . . . $\vdots$

5. . . . $\vdots$

6. If e_0, e_1 *are in Exp and* c *is in Com then* **while** $e_0 = e_1$ **do** c *is in Com.*

At some points in the text environments (and similar things) were mutually recursively defined with commands and so on. This is justified using our apparatus of continuous set operators employing, in particular, the finite function operator.