Preface

This is a working draft of a book on the foundations of programming languages. The central organizing principle of the book is that programming language features may be seen as manifestations of an underlying type structure that governs its syntax and semantics. The emphasis, therefore, is on the concept of type, which codifies and organizes the computational universe in much the same way that the concept of set may be seen as an organizing principle for the mathematical universe. The purpose of this book is to explain this remark.

This is very much a work in progress, with major revisions made nearly every day. This means that there may be internal inconsistencies as revisions to one part of the book invalidate material at another part. Please bear this in mind!

Corrections, comments, and suggestions are most welcome, and should be sent to the author at rwh@cs.cmu.edu. I am grateful to the following people for their comments, corrections, and suggestions to various versions of this book: Arbob Ahmad, Andrew Appel, Zena Ariola, Guy E. Blelloch, William Byrd, Luca Cardelli, Iliano Cervesato, Manuel Chakravarti, Richard C. Cobbe, Karl Crary, Daniel Dantas, Anupam Datta, Jake Donham, Derek Dreyer, Matthias Felleisen, Frank Pfenning, Dan Friedman, Maia Ginsburg, Kevin Hely, Cao Jing, Gabriele Keller, Danielle Kramer, Akiva Leffert, Dan Licata, Dave MacQueen, Greg Morrisett, Tom Murphy, Aleksandar Nanevski, Georg Neis, David Neville, Doug Perkins, Frank Pfenning, Benjamin C. Pierce, Andrew M. Pitts, Gordon D. Plotkin, Carter T. Schonwald, Dale Schumacher, Dana Scott, Zhong Shao, Robert Simmons, Pawel Sobocinski, Daniel Spoonhower, Michael Tschantz, Kami Vaniea, Carsten Varming, David Walker, Dan Wang, Jack Wileden, Todd Wilson, Luke Zarko, Yu Zhang.
Contents

Preface iii

I Judgements and Rules 1

1 Inductive Definitions 3
   1.1 Objects and Judgements ................................. 3
   1.2 Inference Rules ............................................ 4
   1.3 Derivations .................................................. 6
   1.4 Rule Induction .............................................. 7
   1.5 Iterated and Simultaneous Inductive Definitions ...... 10
   1.6 Defining Functions by Rules ............................. 12
   1.7 Modes .......................................................... 13
   1.8 Foundations .................................................. 14
   1.9 Exercises ..................................................... 15

2 Hypothetical Judgements 17
   2.1 Derivability .................................................. 17
   2.2 Admissibility ............................................... 20
   2.3 Hypothetical Inductive Definitions ...................... 22
   2.4 Exercises ..................................................... 23

3 Parametric Judgements 25
   3.1 Parameters and Objects .................................... 25
   3.2 Rule Schemes ................................................ 26
   3.3 Parametric Derivability ................................... 27
   3.4 Parametric Inductive Definitions ....................... 28
   3.5 Exercises ..................................................... 30
## CONTENTS

### 4 Transition Systems  
4.1 Transition Systems ........................................ 31  
4.2 Iterated Transition ........................................ 32  
4.3 Simulation and Bisimulation ................................. 33  
4.4 Exercises .................................................. 34

### II Levels of Syntax  

#### 5 Concrete Syntax  
5.1 Strings Over An Alphabet ................................. 37  
5.2 Lexical Structure .......................................... 38  
5.3 Context-Free Grammars ..................................... 42  
5.4 Grammatical Structure ..................................... 43  
5.5 Ambiguity .................................................. 45  
5.6 Exercises .................................................. 46

#### 6 Abstract Syntax Trees  
6.1 Abstract Syntax Trees ....................................... 47  
6.2 Variables and Substitution .................................. 48  
6.3 Exercises .................................................. 51

#### 7 Binding and Scope  
7.1 Abstract Binding Trees ..................................... 54  
  7.1.1 Structural Induction With Binding and Scope ....... 56  
  7.1.2 Apartness ............................................. 57  
  7.1.3 Renaming of Bound Parameters ......................... 57  
  7.1.4 Substitution ........................................... 58  
7.2 Exercises .................................................. 59

#### 8 Parsing  
8.1 Parsing Into Abstract Syntax Trees ....................... 61  
8.2 Parsing Into Abstract Binding Trees ...................... 64  
8.3 Syntactic Conventions ...................................... 66  
8.4 Exercises .................................................. 66

### III Static and Dynamic Semantics  

#### 9 Static Semantics  
9.1 Type System ................................................ 69
<table>
<thead>
<tr>
<th>CONTENTS</th>
<th>vii</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2 Structural Properties</td>
<td>72</td>
</tr>
<tr>
<td>9.3 Exercises</td>
<td>74</td>
</tr>
<tr>
<td>10 Dynamic Semantics</td>
<td>75</td>
</tr>
<tr>
<td>10.1 Structural Semantics</td>
<td>75</td>
</tr>
<tr>
<td>10.2 Contextual Semantics</td>
<td>78</td>
</tr>
<tr>
<td>10.3 Equational Semantics</td>
<td>80</td>
</tr>
<tr>
<td>10.4 Exercises</td>
<td>84</td>
</tr>
<tr>
<td>11 Type Safety</td>
<td>85</td>
</tr>
<tr>
<td>11.1 Preservation</td>
<td>86</td>
</tr>
<tr>
<td>11.2 Progress</td>
<td>86</td>
</tr>
<tr>
<td>11.3 Run-Time Errors</td>
<td>88</td>
</tr>
<tr>
<td>11.4 Exercises</td>
<td>90</td>
</tr>
<tr>
<td>12 Evaluation Semantics</td>
<td>91</td>
</tr>
<tr>
<td>12.1 Evaluation Semantics</td>
<td>91</td>
</tr>
<tr>
<td>12.2 Relating Transition and Evaluation Semantics</td>
<td>92</td>
</tr>
<tr>
<td>12.3 Type Safety, Revisited</td>
<td>94</td>
</tr>
<tr>
<td>12.4 Cost Semantics</td>
<td>95</td>
</tr>
<tr>
<td>12.5 Exercises</td>
<td>96</td>
</tr>
<tr>
<td>IV Function Types</td>
<td>97</td>
</tr>
<tr>
<td>13 Function Definitions and Values</td>
<td>99</td>
</tr>
<tr>
<td>13.1 First-Order Functions</td>
<td>100</td>
</tr>
<tr>
<td>13.2 Higher-Order Functions</td>
<td>101</td>
</tr>
<tr>
<td>13.3 Evaluation Semantics and Definitional Equivalence</td>
<td>103</td>
</tr>
<tr>
<td>13.4 Dynamic Scope</td>
<td>105</td>
</tr>
<tr>
<td>13.5 Exercises</td>
<td>107</td>
</tr>
<tr>
<td>14 Gödel's System T</td>
<td>109</td>
</tr>
<tr>
<td>14.1 Statics</td>
<td>109</td>
</tr>
<tr>
<td>14.2 Dynamics</td>
<td>111</td>
</tr>
<tr>
<td>14.3 Definability</td>
<td>112</td>
</tr>
<tr>
<td>14.4 Non-Definability</td>
<td>114</td>
</tr>
<tr>
<td>14.5 Exercises</td>
<td>116</td>
</tr>
</tbody>
</table>

DECEMBER 18, 2009  DRAFT  14:36
## CONTENTS

### 15 Plotkin’s PCF
- 15.1 Statics ........................................... 119
- 15.2 Dynamics ........................................ 120
- 15.3 Definability ........................................ 122
- 15.4 Co-Natural Numbers ............................. 124
- 15.5 Exercises ........................................... 124

### V Finite Data Types

#### 16 Product Types
- 16.1 Nullary and Binary Products ..................... 127
- 16.2 Finite Products .................................... 129
- 16.3 Primitive and Mutual Recursion .................. 131
- 16.4 Exercises ........................................... 132

#### 17 Sum Types
- 17.1 Binary and Nullary Sums ......................... 133
- 17.2 Finite Sums ....................................... 135
- 17.3 Uses for Sum Types .............................. 137
  - 17.3.1 Void and Unit ................................ 137
  - 17.3.2 Booleans .................................... 137
  - 17.3.3 Enumerations ................................ 138
  - 17.3.4 Options ...................................... 138
- 17.4 Exercises ........................................... 140

#### 18 Pattern Matching
- 18.1 A Pattern Language .............................. 142
- 18.2 Statics ........................................... 143
- 18.3 Dynamics ........................................... 144
- 18.4 Exhaustiveness and Redundancy .................. 147
- 18.5 Exercises ........................................... 150

### VI Infinite Data Types

#### 19 Inductive and Co-Inductive Types
- 19.1 Motivating Examples ............................. 153
- 19.2 Generic Programming ............................. 156
  - 19.2.1 Positive Type Operators ..................... 157
  - 19.2.2 Action of a Positive Type Operator .......... 158
# CONTENTS

- 28.5 Exercises .............................................. 250

## 29 Continuations

- 29.1 Informal Overview ................................. 251
- 29.2 Semantics of Continuations ...................... 253
- 29.3 Coroutines ........................................... 255
- 29.4 Exercises ............................................ 259

## X Types and Propositions

## 30 Constructive Logic

- 30.1 Constructive Semantics ......................... 264
- 30.2 Constructive Logic ................................ 265
  - 30.2.1 Rules of Provability ........................... 266
  - 30.2.2 Rules of Proof ................................... 268
- 30.3 Propositions as Types ............................ 269
- 30.4 Exercises ............................................ 271

## 31 Classical Logic

- 31.1 Classical Logic ........................................ 274
  - 31.1.1 Provability and Refutability ................ 274
  - 31.1.2 Proofs and Refutations ....................... 276
- 31.2 Deriving Elimination Forms ...................... 278
- 31.3 Proof Dynamics ....................................... 280
- 31.4 Law of the Excluded Middle ...................... 281
- 31.5 Exercises ............................................ 283

## XI Subtyping

## 32 Subtyping

- 32.1 Subsumption ........................................... 288
- 32.2 Varieties of Subtyping ............................ 288
  - 32.2.1 Numeric Types ................................... 288
  - 32.2.2 Product Types .................................. 289
  - 32.2.3 Sum Types ....................................... 291
- 32.3 Variance .............................................. 292
  - 32.3.1 Product Types .................................. 292
  - 32.3.2 Sum Types ....................................... 292
  - 32.3.3 Function Types ................................. 293
## CONTENTS

32.3.4 Recursive Types ............................................ 294  
32.4 Safety for Subtyping ........................................... 296  
32.5 Exercises ...................................................... 299  

33 Singleton and Dependent Kinds ................................. 301  
33.1 Informal Overview ............................................. 302  

XII Symbols .................................................................. 305  

34 Symbols ................................................................... 307  
34.1 Statics ............................................................... 307  
34.2 Scoped Dynamics ................................................ 309  
34.3 Unscoped Dynamics ............................................ 310  
34.4 Safety ............................................................... 311  
34.5 Exercises .......................................................... 312  

35 Fluid Binding .......................................................... 313  
35.1 Statics ............................................................... 313  
35.2 Dynamics ........................................................... 314  
35.3 Type Safety ......................................................... 316  
35.4 Subtleties of Fluid Binding .................................... 317  
35.5 Fluid References ................................................ 319  
35.6 Exercises .......................................................... 321  

36 Dynamic Classification ............................................. 323  
36.1 Statics ............................................................... 324  
36.2 Dynamics ........................................................... 325  
36.3 Definability of Classification ................................... 326  
36.4 Classifying Secrets .............................................. 327  
36.5 Exercises .......................................................... 328  

XIII Storage Effects .................................................... 329  

37 Reynolds’s IA .......................................................... 331  
37.1 Commands .......................................................... 332  
37.1.1 Statics ............................................................ 333  
37.1.2 Dynamics ........................................................ 334  
37.1.3 Safety ............................................................ 336  
37.2 Some Programming Idioms ................................. 337
## Futures and Speculation

42 Futures and Speculation

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>42.1 Futures</td>
<td>396</td>
</tr>
<tr>
<td>42.1.1 Statics</td>
<td>396</td>
</tr>
<tr>
<td>42.1.2 Dynamics</td>
<td>397</td>
</tr>
<tr>
<td>42.2 Speculation</td>
<td>400</td>
</tr>
<tr>
<td>42.3 Exercises</td>
<td>401</td>
</tr>
</tbody>
</table>

## Concurrency

XVI Concurrency

43 Process Calculus

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>43.1 Actions and Events</td>
<td>406</td>
</tr>
<tr>
<td>43.2 Concurrent Interaction</td>
<td>407</td>
</tr>
<tr>
<td>43.3 Replication</td>
<td>409</td>
</tr>
<tr>
<td>43.4 Private Channels</td>
<td>411</td>
</tr>
<tr>
<td>43.5 Synchronous Communication</td>
<td>412</td>
</tr>
<tr>
<td>43.6 Polyadic Communication</td>
<td>413</td>
</tr>
<tr>
<td>43.7 Mutable Cells as Processes</td>
<td>414</td>
</tr>
<tr>
<td>43.8 Asynchronous Communication</td>
<td>415</td>
</tr>
<tr>
<td>43.9 Exercises</td>
<td>417</td>
</tr>
</tbody>
</table>

44 Concurrency

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>44.1 Framework</td>
<td>419</td>
</tr>
<tr>
<td>44.2 Input/Output</td>
<td>421</td>
</tr>
<tr>
<td>44.3 Mutable Cells</td>
<td>422</td>
</tr>
<tr>
<td>44.4 Futures</td>
<td>425</td>
</tr>
<tr>
<td>44.5 Fork and Join</td>
<td>427</td>
</tr>
<tr>
<td>44.6 Synchronization</td>
<td>427</td>
</tr>
<tr>
<td>44.7 Exercises</td>
<td>430</td>
</tr>
</tbody>
</table>

## Modularity

XVII Modularity

45 Separate Compilation and Linking

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>45.1 Linking and Substitution</td>
<td>433</td>
</tr>
<tr>
<td>45.2 Exercises</td>
<td>433</td>
</tr>
</tbody>
</table>

46 Basic Modules

47 Parameterized Modules

14:36 Draft December 18, 2009
## XVIII Equivalence

48 Equational Reasoning for T 441  
48.1 Observational Equivalence 442  
48.2 Extensional Equivalence 446  
48.3 Extensional and Observational Equivalence Coincide 447  
48.4 Some Laws of Equivalence 450  
48.4.1 General Laws 451  
48.4.2 Extensionality Laws 451  
48.4.3 Induction Law 452  
48.5 Exercises 452

49 Equational Reasoning for PCF 453  
49.1 Observational Equivalence 453  
49.2 Extensional Equivalence 454  
49.3 Extensional and Observational Equivalence Coincide 455  
49.4 Compactness 459  
49.5 Co-Natural Numbers 462  
49.6 Exercises 464

50 Parametricity 465  
50.1 Overview 465  
50.2 Observational Equivalence 466  
50.3 Logical Equivalence 468  
50.4 Parametricity Properties 474  
50.5 Exercises 477

## XIX Working Drafts of Chapters 479
Part I

Judgements and Rules
Chapter 1

Inductive Definitions

Inductive definitions are an indispensable tool in the study of programming languages. In this chapter we will develop the basic framework of inductive definitions, and give some examples of their use.

1.1 Objects and Judgements

We start with the notion of a judgement, or assertion, about an object of study. We shall make use of many forms of judgement, including examples such as these:

\begin{align*}
  n \text{ nat} & \quad n \text{ is a natural number} \\
  n = n_1 + n_2 & \quad n \text{ is the sum of } n_1 \text{ and } n_2 \\
  a \text{ ast} & \quad a \text{ is an abstract syntax tree} \\
  \tau \text{ type} & \quad \tau \text{ is a type} \\
  e : \tau & \quad \text{expression } e \text{ has type } \tau \\
  e \downarrow v & \quad \text{expression } e \text{ has value } v
\end{align*}

A judgement states that one or more objects have a property or stand in some relation to one another. The property or relation itself is called a judgement form, and the judgement that an object or objects have that property or stand in that relation is said to be an instance of that judgement form. A judgement form is also called a predicate, and the objects constituting an instance are its subjects.

We will use the meta-variable $P$ to stand for an unspecified judgement form, and the meta-variables $a$, $b$, and $c$ to stand for unspecified objects. We write $a \ P$ for the judgement asserting that $P$ holds of $a$. When it is not important to stress the subject of the judgement, we write $J$ to stand for
an unspecified judgement. For particular judgement forms, we freely use
prefix, infix, or mixfix notation, as illustrated by the above examples, in
order to enhance readability.

We are being intentionally vague about the universe of objects that may
be involved in an inductive definition. The rough-and-ready rule is that
any sort of finite construction of objects from other objects is permissible.
In particular, we shall make frequent use of the construction of compos-
itive objects of the form $o(a_1, \ldots, a_n)$, where $a_1, \ldots, a_n$ are objects and $o$ is
an $n$-argument operator. This construction includes as a special case the
formation of $n$-tuples, $(a_1, \ldots, a_n)$, in which the tupling operator is left im-
licit. (In Chapters 6 and 7 we will formalize these and richer forms of
objects, called abstract syntax trees.)

1.2 Inference Rules

An inductive definition of a judgement form consists of a collection of rules
of the form

$$
\frac{J_1 \quad \cdots \quad J_k}{J}
$$

(1.1)
in which $J$ and $J_1, \ldots, J_k$ are all judgements of the form being defined. The
judgements above the horizontal line are called the premises of the rule,
and the judgement below the line is called its conclusion. If a rule has no
premises (that is, when $k$ is zero), the rule is called an axiom; otherwise it is
called a proper rule.

An inference rule may be read as stating that the premises are sufficient
for the conclusion: to show $J$, it is enough to show $J_1, \ldots, J_k$. When
$k$ is zero, a rule states that its conclusion holds unconditionally. Bear in
mind that there may be, in general, many rules with the same conclusion,
each specifying sufficient conditions for the conclusion. Consequently, if
the conclusion of a rule holds, then it is not necessary that the premises
hold, for it might have been derived by another rule.

For example, the following rules constitute an inductive definition of
the judgement $a$ nat:

$$
\frac{}{\text{zero nat}}
$$

(1.2a)

$$
\frac{a \text{ nat}}{\text{succ}(a) \text{ nat}}
$$

(1.2b)

These rules specify that $a$ nat holds whenever either $a$ is zero, or $a$ is
succ($b$) where $b$ nat. Taking these rules to be exhaustive, it follows that
1.2 Inference Rules

\( a \text{ nat} \iff a \) is a natural number written in unary.

Similarly, the following rules constitute an inductive definition of the judgement \( a \text{ tree} \):

\[
\begin{align*}
\text{empty} & \quad \text{tree} \\
\frac{a_1 \text{ tree} \quad a_2 \text{ tree}}{\text{node}(a_1; a_2) \text{ tree}}
\end{align*}
\]

(1.3a)

(1.3b)

These rules specify that \( a \) tree holds if either \( a \) is \( \text{empty} \), or \( a \) is \( \text{node}(a_1; a_2) \), where \( a_1 \) tree and \( a_2 \) tree. Taking these to be exhaustive, these rules state that \( a \) is a binary tree, which is to say it is either empty, or a node consisting of two children, each of which is also a binary tree.

The judgement \( a = b \text{ nat} \) defining equality of \( a \text{ nat} \) and \( b \text{ nat} \) is inductively defined by the following rules:

\[
\begin{align*}
\frac{}{\text{zero} = \text{zero} \text{ nat}}
\end{align*}
\]

(1.4a)

\[
\begin{align*}
\frac{a = b \text{ nat}}{\text{succ}(a) = \text{succ}(b) \text{ nat}}
\end{align*}
\]

(1.4b)

In each of the preceding examples we have made use of a notational convention for specifying an infinite family of rules by a finite number of patterns, or rule schemes. For example, Rule (1.2b) is a rule scheme that determines one rule, called an instance of the rule scheme, for each choice of object \( a \) in the rule. We will rely on context to determine whether a rule is stated for a specific object, \( a \), or is instead intended as a rule scheme specifying a rule for each choice of objects in the rule. (In Chapter 3 we will remove this ambiguity by introducing parameterization of rules by objects.)

A collection of rules is considered to define the strongest judgement that is closed under, or respects, those rules. To be closed under the rules simply means that the rules are sufficient to show the validity of a judgement: \( J \) holds if there is a way to obtain it using the given rules. To be the strongest judgement closed under the rules means that the rules are also necessary: \( J \) holds only if there is a way to obtain it by applying the rules. The sufficiency of the rules means that we may show that \( J \) holds by deriving it by composing rules. Their necessity means that we may reason about it using rule induction.
1.3 Derivations

To show that an inductively defined judgement holds, it is enough to exhibit a derivation of it. A derivation of a judgement is a finite composition of rules, starting with axioms and ending with that judgement. It may be thought of as a tree in which each node is a rule whose children are derivations of its premises. We sometimes say that a derivation of \( J \) is evidence for the validity of an inductively defined judgement \( J \).

We usually depict derivations as trees with the conclusion at the bottom, and with the children of a node corresponding to a rule appearing above it as evidence for the premises of that rule. Thus, if

\[
\frac{I_1 \ldots I_k}{J}
\]

is an inference rule and \( \nabla_1, \ldots, \nabla_k \) are derivations of its premises, then

\[
\frac{\nabla_1 \ldots \nabla_k}{J}
\]

is a derivation of its conclusion. In particular, if \( k = 0 \), then the node has no children.

For example, this is a derivation of \( \text{succ}(\text{succ}(\text{succ}(\text{zero}))) \text{ nat} \):

\[
\frac{\text{zero nat}}{\text{succ(zero) nat}} \quad \frac{\text{succ(zero) nat}}{\text{succ(succ(zero)) nat}} \quad \frac{\text{succ(succ(zero)) nat}}{\text{succ(succ(succ(zero))) nat}}.
\]

(1.6)

Similarly, here is a derivation of \( \text{node}((\text{node}(\text{empty}; \text{empty}); \text{empty}); \text{empty}) \text{ tree} \):

\[
\frac{\text{empty tree}}{\text{node}(\text{empty}; \text{empty}) \text{ tree}} \quad \frac{\text{empty tree}}{\text{empty tree}} \quad \frac{\text{node}(\text{empty}; \text{empty}) \text{ tree}}{\text{node}(\text{node}(\text{empty}; \text{empty}); \text{empty}) \text{ tree}}.
\]

(1.7)

To show that an inductively defined judgement is derivable we need only find a derivation for it. There are two main methods for finding derivations, called forward chaining, or bottom-up construction, and backward chaining, or top-down construction. Forward chaining starts with the axioms and works forward towards the desired conclusion, whereas backward...
1.4 Rule Induction

chaining starts with the desired conclusion and works backwards towards the axioms.

More precisely, forward chaining search maintains a set of derivable judgements, and continually extends this set by adding to it the conclusion of any rule all of whose premises are in that set. Initially, the set is empty; the process terminates when the desired judgement occurs in the set. Assuming that all rules are considered at every stage, forward chaining will eventually find a derivation of any derivable judgement, but it is impossible (in general) to decide algorithmically when to stop extending the set and conclude that the desired judgement is not derivable. We may go on and on adding more judgements to the derivable set without ever achieving the intended goal. It is a matter of understanding the global properties of the rules to determine that a given judgement is not derivable.

Forward chaining is undirected in the sense that it does not take account of the end goal when deciding how to proceed at each step. In contrast, backward chaining is goal-directed. Backward chaining search maintains a queue of current goals, judgements whose derivations are to be sought. Initially, this set consists solely of the judgement we wish to derive. At each stage, we remove a judgement from the queue, and consider all rules whose conclusion is that judgement. For each such rule, we add the premises of that rule to the back of the queue, and continue. If there is more than one such rule, this process must be repeated, with the same starting queue, for each candidate rule. The process terminates whenever the queue is empty, all goals having been achieved; any pending consideration of candidate rules along the way may be discarded. As with forward chaining, backward chaining will eventually find a derivation of any derivable judgement, but there is, in general, no algorithmic method for determining in general whether the current goal is derivable. If it is not, we may futilely add more and more judgements to the goal set, never reaching a point at which all goals have been satisfied.

1.4 Rule Induction

Since an inductive definition specifies the strongest judgement closed under a collection of rules, we may reason about them by rule induction. The principle of rule induction states that to show that a property $P$ holds of a judgement $J$ whenever $J$ is derivable, it is enough to show that $P$ is closed under, or respects, the rules defining $J$. Writing $P(J)$ to mean that the prop-
1.4 Rule Induction

Property \( P \) holds of the judgement \( J \), we say that \( P \) respects the rule

\[
\begin{array}{c}
J_1 \ldots J_k \\
\hline
J
\end{array}
\]

if \( P(J) \) holds whenever \( P(J_1), \ldots, P(J_k) \). The assumptions \( P(J_1), \ldots, P(J_k) \) are called the *inductive hypotheses*, and \( P(J) \) is called the *inductive conclusion*, of the inference.

In practice the premises and conclusion of the rule involve objects that are universally quantified in the inductive step corresponding to that rule. Thus to show that a property \( P \) is closed under a rule of the form

\[
\begin{array}{c}
a_1 J_1 \ldots a_k J_k \\
\hline
a J
\end{array}
\]

we must show that for every \( a, a_1, \ldots, a_k \), if \( P(a_1 J_1), \ldots, P(a_k J_k) \), then \( P(a J) \).

The principle of rule induction is simply the expression of the definition of an inductively defined judgement form as the *strongest* judgement form closed under the rules comprising the definition. This means that the judgement form is both (a) closed under those rules, and (b) sufficient for any other property also closed under those rules. The former property means that a derivation is evidence for the validity of a judgement; the latter means that we may reason about an inductively defined judgement form by rule induction.

If \( P(J) \) is closed under a set of rules defining a judgement form, then so is the conjunction of \( P \) with the judgement itself. This means that when showing \( P \) to be closed under a rule, we may inductively assume not only that \( P(J_i) \) holds for each of the premises \( J_i \), but also that \( J_i \) itself holds as well. We shall generally take advantage of this without explicit mentioning that we are doing so.

When specialized to Rules (1.2), the principle of rule induction states that to show \( P(a \text{ nat}) \) whenever \( a \text{ nat} \), it is enough to show:

1. \( P(\text{zero nat}) \).
2. for every \( a \), if \( P(a \text{ nat}) \), then \( P(\text{succ}(a) \text{ nat}) \).

This is just the familiar principle of *mathematical induction* arising as a special case of rule induction. The first condition is called the *basis* of the induction, and the second is called the *inductive step*.

Similarly, rule induction for Rules (1.3) states that to show \( P(a \text{ tree}) \) whenever \( a \text{ tree} \), it is enough to show
1.4 Rule Induction

1. \( \mathcal{P}(\text{empty tree}) \).

2. For every \( a_1 \) and \( a_2 \), if \( \mathcal{P}(a_1 \text{ tree}) \) and \( \mathcal{P}(a_2 \text{ tree}) \), then \( \mathcal{P}(\text{node}(a_1;a_2) \text{ tree}) \).

This is called the principle of tree induction, and is once again an instance of rule induction.

As a simple example of a proof by rule induction, let us prove that natural number equality as defined by Rules (1.4) is reflexive:

**Lemma 1.1.** If \( a \text{ nat} \), then \( a = a \text{ nat} \).

**Proof.** By rule induction on Rules (1.2): 

**Rule (1.2a)** Applying Rule (1.4a) we obtain \( \text{zero} = \text{zero nat} \).

**Rule (1.2b)** Assume that \( a = a \text{ nat} \). It follows that \( \text{succ}(a) = \text{succ}(a) \text{ nat} \) by an application of Rule (1.4b). 

□

As another example of the use of rule induction, we may show that the predecessor of a natural number is also a natural number. While this may seem self-evident, the point of the example is to show how to derive this from first principles.

**Lemma 1.2.** If \( \text{succ}(a) \text{ nat} \), then \( a \text{ nat} \).

**Proof.** It is instructive to re-state the lemma in a form more suitable for inductive proof: if \( b \text{ nat} \) and \( b \) is \( \text{succ}(a) \) for some \( a \), then \( a \text{ nat} \). We proceed by rule induction on Rules (1.2).

**Rule (1.2a)** Vacuously true, since \( \text{zero} \) is not of the form \( \text{succ}(-) \).

**Rule (1.2b)** We have that \( b \) is \( \text{succ}(b') \), and we may assume both that the lemma holds for \( b' \) and that \( b' \text{ nat} \). The result follows directly, since if \( \text{succ}(b') = \text{succ}(a) \) for some \( a \), then \( a \) is \( b' \). 

□

Similarly, let us show that the successor operation is injective.

**Lemma 1.3.** If \( \text{succ}(a_1) = \text{succ}(a_2) \text{ nat} \), then \( a_1 = a_2 \text{ nat} \).
Proof. It is instructive to re-state the lemma in a form more directly amenable to proof by rule induction. We are to show that if \( b_1 = b_2 \) nat then if \( b_1 \) is \( \text{succ}(a_1) \) and \( b_2 \) is \( \text{succ}(a_2) \), then \( a_1 = a_2 \) nat. We proceed by rule induction on Rules (1.4):

**Rule (1.4a)** Vacuously true, since \( \text{zero} \) is not of the form \( \text{succ}(\cdot) \).

**Rule (1.4b)** Assuming the result for \( b_1 = b_2 \) nat, and hence that the premise \( b_1 = b_2 \) nat holds as well, we are to show that if \( \text{succ}(b_1) \) is \( \text{succ}(a_1) \) and \( \text{succ}(b_2) \) is \( \text{succ}(a_2) \), then \( a_1 = a_2 \) nat. Under these assumptions we have \( b_1 = a_1 \) and \( b_2 = a_2 \), and so \( a_1 = a_2 \) nat is just the premise of the rule. (We make no use of the inductive hypothesis to complete this step of the proof.)

Both proofs rely on some natural assumptions about the universe of objects; see Section 1.8 on page 14 for further discussion.

### 1.5 Iterated and Simultaneous Inductive Definitions

Inductive definitions are often *iterated*, meaning that one inductive definition builds on top of another. In an iterated inductive definition the premises of a rule

\[
\begin{array}{c}
I_1 \quad \cdots \quad I_k \\
\hline
J
\end{array}
\]

may be instances of either a previously defined judgement form, or the judgement form being defined. For example, the following rules, define the judgement \( a \) list stating that \( a \) is a list of natural numbers.

\[
\begin{array}{c}
\text{nil} \text{ list} \quad (1.8a)
\end{array}
\]

\[
\begin{array}{c}
\text{cons}(a; b) \text{ list} \\
\quad \text{a nat} \quad \text{b list} \quad (1.8b)
\end{array}
\]

The first premise of Rule (1.8b) is an instance of the judgement form \( a \) nat, which was defined previously, whereas the premise \( \text{b list} \) is an instance of the judgement form being defined by these rules.

Frequently two or more judgements are defined at once by a *simultaneous inductive definition*. A simultaneous inductive definition consists of a
set of rules for deriving instances of several different judgement forms, any of which may appear as the premise of any rule. Since the rules defining each judgement form may involve any of the others, none of the judgement forms may be taken to be defined prior to the others. Instead one must understand that all of the judgement forms are being defined at once by the entire collection of rules. The judgement forms defined by these rules are, as before, the strongest judgement forms that are closed under the rules. Therefore the principle of proof by rule induction continues to apply, albeit in a form that allows us to prove a property of each of the defined judgement forms simultaneously.

For example, consider the following rules, which constitute a simultaneous inductive definition of the judgements $a$ \textit{even}, stating that $a$ is an even natural number, and $a$ \textit{odd}, stating that $a$ is an odd natural number:

\begin{align*}
\text{zero} & \text{ even} \quad \text{(1.9a)} \\
\text{a odd} & \quad \text{succ}(a) \text{ even} \quad \text{(1.9b)} \\
\text{a even} & \quad \text{succ}(a) \text{ odd} \quad \text{(1.9c)}
\end{align*}

The principle of rule induction for these rules states that to show simultaneously that $\mathcal{P}(a \text{ even})$ whenever $a$ \textit{even} and $\mathcal{P}(a \text{ odd})$ whenever $a$ \textit{odd}, it is enough to show the following:

1. $\mathcal{P}(\text{zero even})$;
2. if $\mathcal{P}(a \text{ odd})$, then $\mathcal{P}(\text{succ}(a) \text{ even})$;
3. if $\mathcal{P}(a \text{ even})$, then $\mathcal{P}(\text{succ}(a) \text{ odd})$.

As a simple example, we may use simultaneous rule induction to prove that (1) if $a$ even, then $a$ nat, and (2) if $a$ odd, then $a$ nat. That is, we define the property $\mathcal{P}$ by (1) $\mathcal{P}(a \text{ even})$ iff $a$ nat, and (2) $\mathcal{P}(a \text{ odd})$ iff $a$ nat. The principle of rule induction for Rules (1.9) states that it is sufficient to show the following facts:

1. $\text{zero}$ nat, which is derivable by Rule (1.2a).
2. If $a$ nat, then $\text{succ}(a)$ nat, which is derivable by Rule (1.2b).
3. If $a$ nat, then $\text{succ}(a)$ nat, which is also derivable by Rule (1.2b).
1.6 Defining Functions by Rules

A common use of inductive definitions is to define a function by giving an inductive definition of its graph relating inputs to outputs, and then showing that the relation uniquely determines the outputs for given inputs. For example, we may define the addition function on natural numbers as the relation \( \text{sum}(a; b; c) \), with the intended meaning that \( c \) is the sum of \( a \) and \( b \), as follows:

\[
\begin{align*}
\text{sum}(a; b; c) & \quad \text{sum}(\text{succ}(a); b; \text{succ}(c)) \\
\text{sum}(\text{zero}; b) & \quad \text{sum}(b; b)
\end{align*}
\]  

(1.10a)

(1.10b)

The rules define a ternary (three-place) relation, \( \text{sum}(a; b; c) \), among natural numbers \( a \), \( b \), and \( c \). We may show that \( c \) is determined by \( a \) and \( b \) in this relation.

**Theorem 1.4.** For every \( a \) nat and \( b \) nat, there exists a unique \( c \) nat such that \( \text{sum}(a; b; c) \).

**Proof.** The proof decomposes into two parts:

1. (Existence) If \( a \) nat and \( b \) nat, then there exists \( c \) nat such that \( \text{sum}(a; b; c) \).
2. (Uniqueness) If \( a \) nat, \( b \) nat, \( c \) nat, \( c' \) nat, \( \text{sum}(a; b; c) \), and \( \text{sum}(a; b; c') \), then \( c = c' \) nat.

For existence, let \( P(a \) nat) be the proposition if \( b \) nat then there exists \( c \) nat such that \( \text{sum}(a; b; c) \). We prove that if \( a \) nat then \( P(a \) nat) by rule induction on Rules (1.2). We have two cases to consider:

**Rule (1.2a)** We are to show \( P(\text{zero} \) nat). Assuming \( b \) nat and taking \( c \) to be \( b \), we obtain \( \text{sum}(\text{zero}; b; c) \) by Rule (1.10a).

**Rule (1.2b)** Assuming \( P(a \) nat), we are to show \( P(\text{succ}(a) \) nat). That is, we assume that if \( b \) nat then there exists \( c \) nat such that \( \text{sum}(a; b; c) \), and are to show that if \( b' \) nat, then there exists \( c' \) such that \( \text{sum}(\text{succ}(a); b'; c') \). To this end, suppose that \( b' \) nat. Then by induction there exists \( c \) such that \( \text{sum}(a; b'; c) \). Taking \( c' = \text{succ}(c) \), and applying Rule (1.10b), we obtain \( \text{sum}(\text{succ}(a); b'; c') \), as required.

For uniqueness, we prove that if \( \text{sum}(a; b; c_1) \), then if \( \text{sum}(a; b; c_2) \), then \( c_1 = c_2 \) nat by rule induction based on Rules (1.10).
1.7 Modes

The statement that one or more arguments of a judgement is (perhaps uniquely) determined by its other arguments is called a mode specification for that judgement. For example, we have shown that every two natural numbers have a sum according to Rules (1.10). This fact may be restated as a mode specification by saying that the judgement \( \text{sum}(a; b; c) \) has mode \( (\forall, \forall, \exists) \). The notation arises from the form of the proposition it expresses: for all \( a \text{ nat} \) and for all \( b \text{ nat} \), there exists \( c \text{ nat} \) such that \( \text{sum}(a; b; c) \). If we wish to further specify that \( c \) is uniquely determined by \( a \) and \( b \), we would say that the judgement \( \text{sum}(a; b; c) \) has mode \( (\forall, \forall, \exists!) \), corresponding to the proposition for all \( a \text{ nat} \) and for all \( b \text{ nat} \), there exists a unique \( c \text{ nat} \) such that \( \text{sum}(a; b; c) \). If we wish only to specify that the sum is unique, if it exists, then we would say that the addition judgement has mode \( (\forall, \forall, \exists^{\leq 1}) \), corresponding to the proposition for all \( a \text{ nat} \) and for all \( b \text{ nat} \) there exists at most one \( c \text{ nat} \) such that \( \text{sum}(a; b; c) \).

As these examples illustrate, a given judgement may satisfy several different mode specifications. In general the universally quantified arguments are to be thought of as the inputs of the judgement, and the existentially quantified arguments are to be thought of as its outputs. We usually try to arrange things so that the outputs come after the inputs, but it is not essential that we do so. For example, addition also has the mode \( (\forall, \exists^{\leq 1}, \forall) \), stating that the sum and the first addend uniquely determine the second addend, if there is any such addend at all. Put in other terms, this says that addition of natural numbers has a (partial) inverse, namely subtraction. We could equally well show that addition has mode \( (\exists^{\leq 1}, \forall, \forall) \), which is just another way of stating that addition of natural numbers has a partial inverse.
Often there is an intended, or principal, mode of a given judgement, which we often foreshadow by our choice of notation. For example, when giving an inductive definition of a function, we often use equations to indicate the intended input and output relationships. For example, we may re-state the inductive definition of addition (given by Rules (1.10)) using equations:

\[
\begin{align*}
\frac{a \text{ nat}}{a + \text{zero} = a \text{ nat}} \\
\frac{a + b = c \text{ nat}}{a + \text{succ}(b) = \text{succ}(c) \text{ nat}}
\end{align*}
\] (1.11a)

(1.11b)

When using this notation we tacitly incur the obligation to prove that the mode of the judgement is such that the object on the right-hand side of the equations is determined as a function of those on the left. Having done so, we abuse notation, writing \(a + b\) for the unique \(c\) such that \(a + b = c \text{ nat}\).

1.8 Foundations

An inductively judgement form, such as \(a \text{ nat}\), may be seen as isolating a class of objects, \(a\), satisfying criteria specified by a collection of rules. While intuitively clear, this description is vague in that it does not specify what sorts of things may appear as the subjects of a judgement. Just what is \(a\)? And what, exactly, are the objects \(\text{zero}\) and \(\text{succ}(a)\) used in the definition of the judgement \(a \text{ nat}\)? More generally, what sorts of objects are permissible in an inductive definition?

One answer to these questions is to fix in advance a particular set, \(U\), to serve as the universe of discourse over which all judgements are defined. The universe must be rich enough to contain all objects of interest, and must be specified clearly enough to avoid concerns about its existence. Standard practice is to define \(U\) to be a particular set that can be shown to exist using the standard axioms of set theory, and to specify how the various objects of interest are constructed as elements of this set.

But what should we demand of \(U\) to serve as a suitable universe of discourse? At the very least it should include labeled finitary trees, which are trees of finite height each of whose nodes has finitely many children and is labeled with an operator drawn from some infinite set. An object such as \(\text{succ}(\text{succ}(\text{zero}))\) is a finitary tree with nodes labeled \(\text{zero}\) having no children and nodes labeled \(\text{succ}\) having one child. Similarly, a finite tuple \((a_1, \ldots, a_n)\) may be thought of as a tree whose node is labeled by an \(n\)-tuple operator. Finitary trees will suffice for our work, but it is common
to consider also regular trees, which are finitary trees in which a child of a node may also be an ancestor of it, and infinitary trees, which admit nodes with infinitely many children.

The standard way to show that the universe, $\mathcal{U}$, exists (that is, is properly defined) is to construct it explicitly from the axioms of set theory. This requires that we fix the representation of trees as particular sets, using well-known, but notoriously unenlightening, methods.\textsuperscript{1} Instead we shall simply take it as given that this can be done, and take $\mathcal{U}$ to be a suitably rich universe including at least the finitary trees. In particular we assume that $\mathcal{U}$ comes equipped with operations that allow us to construct finitary trees as elements of $\mathcal{U}$, and to deconstruct such elements of $\mathcal{U}$ into an operator and finitely many children.

The advantage of working within set theory is that it settles any worries about the existence of the universe, $\mathcal{U}$. However, it is important to keep in mind that accepting the axioms of set theory is far more dubious, foundationally speaking, than just accepting the existence of finitary trees without recourse to encoding them as sets. Moreover, there is a significant disadvantage to working with sets, namely that abstract sets have no intrinsic computational content, and hence are of no use to implementation. Yet it is intuitively clear that finitary trees can be readily implemented on a computer by means that have nothing to do with their set-theoretic encodings. Thus we are better off just taking $\mathcal{U}$ as our starting point, from both a foundational and computational perspective.

\section*{1.9 Exercises}

1. Give an inductive definition of the judgement $\text{max}(a; b; c)$, where $a$ nat, $b$ nat, and $c$ nat, with the meaning that $c$ is the larger of $a$ and $b$. Prove that this judgement has the mode $(\forall, \forall, \exists!)$.

2. Consider the following rules, which define the height of a binary tree as the judgement $\text{hgt}(a; b)$.

\[
\begin{align*}
\text{hgt}(\text{empty}; \text{zero}) & \quad (1.12a) \\
\text{hgt}(a_1; b_1) & \quad \text{hgt}(a_2; b_2) \quad \text{max}(b_1; b_2; b) \\
\frac{\text{hgt}(\text{node}(a_1; a_2); \text{succ}(b))}{\text{hgt}(a_1; b_1) \quad \text{hgt}(a_2; b_2) \quad \text{max}(b_1; b_2; b) \quad \text{hgt}(\text{node}(a_1; a_2); \text{succ}(b))} & \quad (1.12b)
\end{align*}
\]

\textsuperscript{1}Perhaps you have seen the definition of the natural number 0 as the empty set, $\emptyset$, and the number $n + 1$ as the set $n \cup \{ n \}$, or the definition of the ordered pair $\langle a, b \rangle$ as the set $\{ a, \{ a, b \} \}$. Similar coding tricks can be used to represent any finitary tree.
1.9 Exercises

Prove by tree induction that the judgement $\text{hgt}$ has the mode $(\forall, \exists)$, with inputs being binary trees and outputs being natural numbers.

3. Give an inductive definition of the judgement "$\nabla$ is a derivation of $J$" for an inductively defined judgement $J$ of your choice.

4. Give an inductive definition of the forward-chaining and backward-chaining search strategies.
Chapter 2

Hypothetical Judgements

A *categorical* judgement is an unconditional assertion about some object of the universe. The inductively defined judgements given in Chapter 1 are all categorical. A *hypothetical judgement* expresses an *entailment* between one or more *hypotheses* and a *conclusion*. We will consider two notions of entailment, called *derivability* and *admissibility*. Derivability expresses the stronger of the two forms of entailment, namely that the conclusion may be deduced directly from the hypotheses by composing rules. Admissibility expresses the weaker form, that the conclusion is derivable from the rules whenever the hypotheses are also derivable. Both forms of entailment enjoy the same *structural* properties that characterize conditional reasoning. One consequence of these properties is that derivability is stronger than admissibility (but the converse fails, in general). We then generalize the concept of an inductive definition to admit rules that have not only categorical, but also hypothetical, judgements as premises. Using these we may enrich the rules with new axioms that are available for use within a specified premise of a rule.

2.1 Derivability

For a given set, \( \mathcal{R} \), of rules, we define the *derivability* judgement, written \( J_1, \ldots, J_k \vdash \mathcal{R} K \), where each \( J_i \) and \( K \) are categorical, to mean that we may derive \( K \) from the expansion \( \mathcal{R}[J_1, \ldots, J_k] \) of the rules \( \mathcal{R} \) with the additional axioms

\[
J_1 , \ldots , J_k .
\]
That is, we treat the hypotheses, or antecedents, of the judgement, $J_1, \ldots, J_n$ as temporary axioms, and derive the conclusion, or consequent, by composing rules in $\mathcal{R}$. That is, evidence for a hypothetical judgement consists of a derivation of the conclusion from the hypotheses using the rules in $\mathcal{R}$.

We use capital Greek letters, frequently $\Gamma$ or $\Delta$, to stand for a finite collection of basic judgements, and write $\mathcal{R}[\Gamma]$ for the expansion of $\mathcal{R}$ with an axiom corresponding to each judgement in $\Gamma$. The judgement $\Gamma \vdash_{\mathcal{R}} K$ means that $K$ is derivable from rules $\mathcal{R}[\Gamma]$. We sometimes write $\vdash_{\mathcal{R}} \Gamma$ to mean that $\vdash_{\mathcal{R}} J$ for each judgement $J$ in $\Gamma$. The derivability judgement $J_1, \ldots, J_n \vdash_{\mathcal{R}} J$ is sometimes expressed by saying that the rule

$$
\begin{array}{c}
J_1 \quad \ldots \quad J_n \\
\hline
J
\end{array}
$$

is derivable from the rules $\mathcal{R}$.

For example, consider the derivability judgement

$$
a \text{ nat} \vdash_{(1.2)} \text{ succ}(\text{ succ}(a)) \text{ nat}
$$

relative to Rules (1.2). This judgement is valid for any choice of object $a$, as evidenced by the derivation

$$
\frac{a \text{ nat}}{\text{ succ}(a) \text{ nat}} \frac{\text{ succ}(\text{ succ}(a)) \text{ nat}}
$$

which composes Rules (1.2), starting with $a$ nat as an axiom, and ending with $\text{ succ}(\text{ succ}(a))$ nat. Equivalently, the validity of (2.2) may also be expressed by stating that the rule

$$
\frac{a \text{ nat}}{\text{ succ}(\text{ succ}(a)) \text{ nat}}
$$

is derivable from Rules (1.2).

It follows directly from the definition of derivability that it is stable under extension with new rules.

**Theorem 2.1** (Uniformity). If $\Gamma \vdash_{\mathcal{R}} J$, then $\Gamma \vdash_{\mathcal{R} \cup R'} J$.

**Proof.** Any derivation of $J$ from $\mathcal{R}[\Gamma]$ is also a derivation from $(\mathcal{R} \cup \mathcal{R'})[\Gamma]$, since the presence of additional rules does not influence the validity of the derivation. \qed
2.1 Derivability

Derivability enjoys a number of structural properties that follow from its definition, independently of the rules, \( \mathcal{R} \), in question.

**Reflexivity** Every judgement is a consequence of itself: \( \Gamma, J \vdash_{\mathcal{R}} J \). Each hypothesis justifies itself as conclusion.

**Weakening** If \( \Gamma \vdash_{\mathcal{R}} J \), then \( \Gamma, K \vdash_{\mathcal{R}} J \). Entailment is not influenced by unexercised options.

**Exchange** If \( \Gamma_1, I_1, I_2, \Gamma_2 \vdash_{\mathcal{R}} J \), then \( \Gamma_1, I_2, I_1, \Gamma_2 \vdash_{\mathcal{R}} J \). The relative ordering of the axioms is immaterial.

**Contraction** If \( \Gamma, J, J \vdash_{\mathcal{R}} K \), then \( \Gamma, J \vdash_{\mathcal{R}} K \). We may use a hypothesis as many times as we like in a derivation.

**Transitivity** If \( \Gamma, K \vdash_{\mathcal{R}} J \) and \( \Gamma \vdash_{\mathcal{R}} K \), then \( \Gamma \vdash_{\mathcal{R}} J \). If we replace an axiom by a derivation of it, the result is a derivation of its consequent without that hypothesis.

These properties may be summarized by saying that the derivability hypothetical judgement is structural.

**Theorem 2.2.** For any rule set, \( \mathcal{R} \), the derivability judgement \( \Gamma \vdash_{\mathcal{R}} J \) is structural.

**Proof.** Reflexivity follows directly from the meaning of derivability. Weakening follows directly from uniformity. Exchange and contraction follow from the treatment of the rules, \( \mathcal{R} \), as a finite set, for which order does not matter and replication is immaterial. Transitivity is proved by rule induction on the first premise.

In view of the structural properties of exchange and contraction, we regard the hypotheses, \( \Gamma \), of a derivability judgement as a finite set of assumptions, so that the order and multiplicity of hypotheses does not matter. In particular, when writing \( \Gamma \) as the union \( \Gamma_1 \Gamma_2 \) of two sets of hypotheses, a hypothesis may occur in both \( \Gamma_1 \) and \( \Gamma_2 \). This is obvious when \( \Gamma_1 \) and \( \Gamma_2 \) are given, but when decomposing a given \( \Gamma \) into two parts, it is well to remember that the same hypothesis may occur in both parts of the decomposition.
2.2 Admissibility

Admissibility, written $\Gamma \models_R J$, is a weaker form of hypothetical judgement stating that $\vdash_R \Gamma$ implies $\vdash_R J$. That is, the conclusion $J$ is derivable from rules $\Gamma$ whenever the assumptions $\Gamma$ are all derivable from rules $R$. In particular if any of the hypotheses are not derivable relative to $R$, then the judgement is vacuously true. The admissibility judgement $J_1, \ldots, J_n \models_R J$ is sometimes expressed by stating that the rule,

$$
\frac{J_1 \ldots J_n}{J},
$$

(2.5)

is admissible relative to the rules in $R$.

For example, the admissibility judgement

$$
succ(a) \text{ nat} \models_{(1.2)} a \text{ nat}
$$

(2.6)

is valid, because any derivation of $succ(a) \text{ nat}$ from Rules (1.2) must contain a sub-derivation of $a \text{ nat}$ from the same rules, which justifies the conclusion. The validity of (2.6) may equivalently be expressed by stating that the rule

$$
\frac{succ(a) \text{ nat}}{a \text{ nat}}
$$

(2.7)

is admissible for Rules (1.2).

In contrast to derivability the admissibility judgement is not stable under extension to the rules. For example, if we enrich Rules (1.2) with the axiom

$$
succ(junk) \text{ nat}
$$

(2.8)

(where $junk$ is some object for which $junk \text{ nat}$ is not derivable), then the admissibility (2.6) is invalid. This is because Rule (2.8) has no premises, and there is no composition of rules deriving $junk \text{ nat}$. Admissibility is as sensitive to which rules are absent from an inductive definition as it is to which rules are present in it.

The structural properties of derivability given by Theorem 2.2 on the preceding page ensure that derivability is stronger than admissibility.

**Theorem 2.3.** If $\Gamma \vdash_R J$, then $\Gamma \models_R J$.

**Proof.** Repeated application of the transitivity of derivability shows that if $\Gamma \models_R J$ and $\vdash_R \Gamma$, then $\vdash_R J$. $\square$
2.2 Admissibility

To see that the converse fails, observe that there is no composition of rules such that
\[ \text{succ(junk) nat } \vdash_{(1.2)} \text{junk nat}, \]
yet the admissibility judgement
\[ \text{succ(junk) nat } \vdash_{(1.2)} \text{junk nat} \]
holds vacuously.

Evidence for admissibility may be thought of as a mathematical function transforming derivations \( \nabla_1, \ldots, \nabla_n \) of the hypotheses into a derivation \( \nabla \) of the consequent. Therefore, the admissibility judgement enjoys the same structural properties as derivability, and hence is a form of hypothetical judgement:

**Reflexivity** If \( J \) is derivable from the original rules, then \( J \) is derivable from the original rules: \( J \models_R J \).

**Weakening** If \( J \) is derivable from the original rules assuming that each of the judgements in \( \Gamma \) are derivable from these rules, then \( J \) must also be derivable assuming that \( \Gamma \) and also \( K \) are derivable from the original rules: if \( \Gamma \models_R J \), then \( \Gamma, K \models_R J \).

**Exchange** The order of assumptions in an iterated implication does not matter.

**Contraction** Assuming the same thing twice is the same as assuming it once.

**Transitivity** If \( \Gamma, K \models_R J \) and \( \Gamma \models_R K \), then \( \Gamma \models_R J \). If the assumption \( K \) is used, then we may instead appeal to the assumed derivability of \( K \).

**Theorem 2.4.** The admissibility judgement \( \Gamma \models_R J \) is structural.

*Proof.* Follows immediately from the definition of admissibility as stating that if the hypotheses are derivable relative to \( R \), then so is the conclusion. \( \Box \)

Just as with derivability, we may, in view of the properties of exchange and contraction, regard the hypotheses, \( \Gamma \), of an admissibility judgement as a finite set, for which order and multiplicity does not matter.
2.3 Hypothetical Inductive Definitions

It is useful to enrich the concept of an inductive definition to permit rules with derivability judgements as premises and conclusions. Doing so permits us to introduce local hypotheses that apply only in the derivation of a particular premise, and also allows us to constrain inferences based on the global hypotheses in effect at the point where the rule is applied.

A hypothetical inductive definition consists of a collection of hypothetical rules of the form

\[ \frac{\Gamma_1 \vdash J_1 \quad \ldots \quad \Gamma_n \vdash J_n}{\Gamma \vdash J}. \]  

(2.9)

The hypotheses \( \Gamma \) are the global hypotheses of the rule, and the hypotheses \( \Gamma_i \) are the local hypotheses of the \( i \)th premise of the rule. Informally, this rule states that \( J \) is a derivable consequence of \( \Gamma \) whenever each \( J_i \) is a derivable consequence of \( \Gamma \), augmented with the additional hypotheses \( \Gamma_i \). Thus, one way to show that \( J \) is derivable from \( \Gamma \) is to show, in turn, that each \( J_i \) is derivable from \( \Gamma \Gamma_i \). The derivation of each premise involves a “context switch” in which we extend the global hypotheses with the local hypotheses of that premise, establishing a new set of global hypotheses for use within that derivation.

Often a hypothetical rule is given for each choice of global context, without restriction. In that case the rule is said to be pure, because it applies irrespective of the context in which it is used. A pure rule, being stated uniformly for all global contexts, may be given in implicit form, as follows:

\[ \frac{\Gamma_1 \vdash J_1 \quad \ldots \quad \Gamma_n \vdash J_n}{J}. \]  

(2.10)

This formulation omits explicit mention of the global context in order to focus attention on the local aspects of the inference.

Sometimes it is necessary to restrict the global context of an inference, so that it applies only if a specified side condition is satisfied. Such rules are said to be impure. Impure rules generally have the form

\[ \frac{\Gamma_1 \vdash J_1 \quad \ldots \quad \Gamma_n \vdash J_n \quad \Psi}{\Gamma \vdash J}, \]  

(2.11)

where the condition, \( \Psi \), limits the applicability of this rule to situations in which it is true. For example, \( \Psi \) may restrict the global context of the inference to be empty, so that no instances involving global hypotheses are permissible.
A hypothetical inductive definition is to be regarded as an ordinary inductive definition of a formal derivability judgement $\Gamma \vdash J$ consisting of a finite set of basic judgements, $\Gamma$, and a basic judgement, $J$. A collection of hypothetical rules, $\mathcal{R}$, defines the strongest formal derivability judgement closed under rules $\mathcal{R}$, which, by a slight abuse of notation, we write as $\Gamma \vdash_\mathcal{R} J$.

Since $\Gamma \vdash_\mathcal{R} J$ is the strongest judgement closed under $\mathcal{R}$, the principle of hypothetical rule induction is valid for reasoning about it. Specifically, to show that $P(\Gamma \vdash J)$ whenever $\Gamma \vdash_\mathcal{R} J$, it is enough to show, for each rule (2.9) in $\mathcal{R}$,

if $P(\Gamma \Gamma_1 \vdash J_1)$ and \ldots and $P(\Gamma \Gamma_n \vdash J_n)$, then $P(\Gamma \vdash J)$.

This is just a restatement of the principle of rule induction given in Chapter 1, specialized to the formal derivability judgement $\Gamma \vdash J$.

In many cases we wish to ensure that the formal derivability relation defined by a collection of hypothetical rules is structural. This amounts to showing that the following structural rules be admissible:

$$\frac{\Gamma, J \vdash J}{\Gamma \vdash J} \quad \text{(2.12a)}$$

$$\frac{\Gamma \vdash J \quad \Gamma, K \vdash J}{\Gamma, K \vdash J} \quad \text{(2.12b)}$$

$$\frac{\Gamma \vdash K \quad \Gamma, K \vdash J}{\Gamma \vdash J} \quad \text{(2.12c)}$$

In the common case that the rules of a hypothetical inductive definition are pure, the structural rules (2.12b) and (2.12c) may be easily shown admissible by rule induction. However, it is typically necessary to include Rule (2.12a) explicitly, perhaps in a restricted form, to ensure reflexivity.

### 2.4 Exercises

1. Prove that if all rules in a hypothetical inductive definition are pure, then the structural rules of weakening (Rule (2.12b)) and transitivity (Rule (2.12c)) are admissible.

2. Define $\Gamma' \vdash \Gamma$ to mean that $\Gamma' \vdash J_i$ for each $J_i$ in $\Gamma$. Show that $\Gamma \vdash J$ iff whenever $\Gamma' \vdash \Gamma$, it follows that $\Gamma' \vdash J$. Hint: from left to right, appeal to transitivity of entailment; from right to left, consider the case of $\Gamma' = \Gamma$. 

DECEMBER 18, 2009 DRAFT 14:36
3. Show that it is dangerous to permit admissibility judgements in the premise of a rule. *Hint:* show that using such rules one may “define” an inconsistent judgement form \( J \) for which we have \( a J \) iff it is *not* the case that \( a J \).
Chapter 3

Parametric Judgements

Basic judgements express properties of objects of the universe of discourse. Hypothetical judgements express entailments between judgements, or reasoning under hypotheses. Parametric judgements express entailments among properties of objects involving parameters, abstract symbols serving as atomic objects in an expanded universe.

Parameters have a variety of uses: as atomic symbols with no properties other than their identity, and as variables given meaning by substitution, the replacement of a parameter by an object. We shall make frequent use of parametric judgements throughout this book. Parametric inductive definitions, which generalize hypothetical inductive definitions to permit introduction of parameters in an inference, are of particular importance in our work.

3.1 Parameters and Objects

We assume given an infinite set of parameters, which we will consider to be abstract atomic objects that are distinct from all other objects and that can be distinguished from one another (that is, we can tell whether any two given parameters are the same or different). It follows that if we are given an object possibly containing a parameter, \( x \), we can rename \( x \) to another parameter, \( x' \), within that object.

To account for parameters we consider the family \( \mathcal{U}[X] \) of expansions of the universe of discourse with parameters drawn from the finite set \( X \).

---

1Parameters are sometimes called symbols, atoms, or names to emphasize their atomic, featureless character.
The expansion $\mathcal{U}[\emptyset]$ may be identified with the universe, $\mathcal{U}$, of finitary trees discussed in Chapter 1. The elements of $\mathcal{U}[\mathcal{X}]$ are finitary trees in which the parameters, $\mathcal{X}$, may occur as leaves. We assume that parameters are distinct from operators so that there can be no confusion between a parameter and an operator that has no children.

Expansion of the universe is monotone in that if $\mathcal{X} \subseteq \mathcal{Y}$, then $\mathcal{U}[\mathcal{X}] \subseteq \mathcal{U}[\mathcal{Y}]$, for a tree possibly involving parameters from $\mathcal{X}$ is surely a tree possibly involving parameters from $\mathcal{Y}$. A bijection $\pi: \mathcal{X} \leftrightarrow \mathcal{X}'$ between parameter sets induces a renaming $\pi^+: \mathcal{U}[\mathcal{X}] \leftrightarrow \mathcal{U}[\mathcal{X}']$ that, intuitively, replaces each occurrence of $x \in \mathcal{X}$ by $\pi(x) \in \mathcal{X}'$ in any element of $\mathcal{U}[\mathcal{X}]$, yielding an element of $\mathcal{U}[\mathcal{X}']$.

### 3.2 Rule Schemes

The concept of an inductive definition extends naturally to any fixed expansion of the universe by parameters, $\mathcal{X}$. A collection of rules defined over the expansion $\mathcal{U}[\mathcal{X}]$ determines the strongest judgement over that expansion closed under these rules. Extending the notation of Chapter 2, we write $\Gamma \vdash_{\mathcal{U}[\mathcal{X}]} J$ to mean that $J$ is derivable from $\mathcal{R}[\Gamma]$ over the expansion $\mathcal{U}[\mathcal{X}]$.

It is often useful to consider rules that are defined over an arbitrary expansion of the universe by parameters. Recall Rule (1.2b) from Chapter 1:

\[
\frac{a \text{ nat}}{\text{succ}(a) \text{ nat}}
\]  

(3.1)

As discussed in Chapter 1, this is actually a rule scheme that stands for an infinite family of rules, called its instances, one for each choice of element $a$ of the universe, $\mathcal{U}$. We extend the concept of rule scheme so that it applies to any expansion of the universe by parameters, so that for each choice of $\mathcal{X}$, we obtain a family of instances of the rule scheme, one for each element $a$ of the expansion $\mathcal{U}[\mathcal{X}]$.

We will generally gloss over the distinction between a rule and a rule scheme, so that for example Rules (1.2) may be considered over any expansion of the universe by parameters without explicit mention. A collection of such rules defines the strongest judgement over a given expansion closed under all instances of the rule schemes over this expansion. Consequently, we may reason by rule induction as described in Chapter 1 over any expansion of the universe by simply reading the rules as applying to objects in that expansion.
3.3 Parametric Derivability

It will be useful to consider a generalization of the derivability judgement that specifies the parameters, as well as the hypotheses, of a judgement. To a first approximation, the *parametric derivability* judgement

\[ \mathcal{X} \mid \Gamma \vdash_{\mathcal{R}} J \]  

(3.2)

means simply that \( \Gamma \vdash_{\mathcal{R}}^{\mathcal{X}} J \). That is, the judgement \( J \) is derivable from hypotheses \( \Gamma \) over the expansion \( \mathcal{U}[\mathcal{X}] \). For example, the parametric judgement

\[ \{ x \} \mid x \text{ nat} \vdash_{(1.2)} \text{succ(succ(x)) nat} \]  

(3.3)

is valid with respect to Rules (1.2), because the judgement \( \text{succ(succ(x)) nat} \) is derivable from the assumption \( x \text{ nat} \) in the expansion of the universe with parameter \( x \).

This is the rough-and-ready interpretation of the parametric judgement. However, the full meaning is slightly stronger than that. In addition to the condition just specified, we also demand that the judgement hold for all renamings of the parameters \( \mathcal{X} \), so that the validity of the judgement cannot depend on the exact choice of parameters. To ensure this we define the meaning of the parametric judgement (3.2) to be given by the following condition:

\[ \forall \pi : \mathcal{X} \leftrightarrow \mathcal{X}' \quad \pi^+ \Gamma \vdash_{\mathcal{R}^+}^{\mathcal{X}''} \pi^+ J. \]

Evidence for the judgement (3.2) consists of a *parametric derivation*, \( \nabla_{\mathcal{X}'} \), of the judgement \( \pi^+ J \) from rules \( \pi^+ \mathcal{R}[\pi^+ \Gamma] \) for some bijection \( \pi : \mathcal{X} \leftrightarrow \mathcal{X}' \).

For example, judgement (3.3) is valid with respect to Rules (1.2) since, for every \( x' \), the judgement

\[ \text{succ(succ(x')) nat} \]

is derivable from Rules (1.2) expanded with the axiom \( x' \text{ nat} \). Evidence for this consists of the parametric derivation, \( \nabla_{x'} \),

\[
\begin{array}{c}
\hline
\text{x' nat} \\
\hline
\text{succ(x') nat} \\
\text{succ(succ(x') nat} \\
\hline
\end{array}
\]  

(3.4)

composed of Rules (1.2) and the axiom \( x' \text{ nat} \).

Parametric derivability enjoys two *structural properties* in addition to those enjoyed by the derivability judgement itself:
3.4 Parametric Inductive Definitions

**Proliferation** If $\mathcal{X} | \Gamma \vdash_R J$, then $\mathcal{X}, x | \Gamma \vdash_R J$.

**Renaming** If $\mathcal{X}, x | \Gamma \vdash_R J$ with $x \not\in \mathcal{X}$, then for every $x' \not\in \mathcal{X}$,

$$\mathcal{X}, \mathcal{X}' | [x \mapsto x']^\dagger \Gamma \vdash_R [x \mapsto x']^\dagger J,$$

and conversely.

Proliferation implies that parametric derivability is sensitive only to the presence, but not the absence, of parameters. Renaming states that parametric derivability is independent of the choice of fresh parameters.

**Theorem 3.1.** The parametric derivability judgement is structural.

**Proof.** Both properties follow directly from the definition of parametric derivability. \qed

In view of Theorem 3.1 we may tacitly assume that the fresh parameters of a judgement are disjoint from the ambient parameters. For if not, we may simply rename them to ensure that it is so, and appeal to the renaming property to obtain the desired judgement. In practice we tacitly assume that the fresh parameters have already been renamed apart from the ambient parameters, so that evidence for judgement (3.4) may be considered to be a parametric derivation $\nabla_x$ with parameter $x$.

### 3.4 Parametric Inductive Definitions

A *parametric inductive definition* is a generalization of a hypothetical inductive definition to permit expansion not only of the set of rules, but also of the set of parameters, in each premise of a rule. A *parametric rule* has the form

$$
\frac{\mathcal{X}_1 | \Gamma_1 \vdash J_1 \quad \ldots \quad \mathcal{X}_n | \Gamma_n \vdash J_n}{\mathcal{X} | \Gamma \vdash J}.
$$

(3.5)

The set, $\mathcal{X}$, is the set of *global parameters* of the inference, and, for each $1 \leq i \leq n$, the set $\mathcal{X}_i$ is the set of *fresh local parameters* of the $i$th premise. The local parameters are *fresh* in the sense that, by suitable renaming, they may be chosen to be disjoint from the global parameters of the inference. The pair $\mathcal{X} | \Gamma$ is called the *global context* of the rule, and each pair $\mathcal{X}_i | \Gamma_i$ is called the *local context* of the $i$th premise of the rule.
3.4 Parametric Inductive Definitions

A parametric rule is pure if it is stated for all choices of global context. A pure rule may be written in implicit form,

\[
\frac{X_1 \mid \Gamma_1 \vdash J_1 \ldots X_n \mid \Gamma_n \vdash J_n}{J},
\]

(3.6)

with the understanding that it stands for the infinite family of rules of the form Rule (3.5) for all choices of global context \( Y \mid \Gamma \). An impure parametric rule is one that is stated only for certain choices of global context, for example by insisting that the global parameters be empty.

A parametric inductive definition may be regarded as an ordinary inductive definition of the formal parametric judgement \( X \mid \Gamma \vdash J \). If \( R \) is a collection of parametric derivability rules, we abuse notation slightly by writing \( X \mid \Gamma \vdash_R J \) to mean that the formal parametric judgement \( X \mid \Gamma \vdash J \) is derivable from rules \( R \).

The principle of rule induction for a parametric inductive definition states that to show \( P(\beta X \mid \Gamma \vdash J) \) whenever \( \beta X \mid \Gamma \vdash_R J \), it is enough to show that \( P \) is closed under the rules \( R \). Specifically, for each rule in \( R \) of the form (3.5), we must show that

\[
\text{if } P(\beta X_1 \mid \Gamma_1 \vdash J_1) \ldots P(\beta X_n \mid \Gamma_n \vdash J_n) \text{ then } P(\beta X \mid \Gamma \vdash J).
\]

Because the meaning of the parametric judgement is independent of the choice of parameter names, any property \( P \) of a parametric judgement must not depend on the choice of local parameter names.

To ensure that a formal parametric judgement is structural, the following rules must be admissible relative to the rules that define it:

\[
\frac{}{X \mid \Gamma, \vdash \beta J} \quad (3.7a)
\]

\[
\frac{X \mid \Gamma \vdash J \quad X \mid \Gamma, J \vdash K}{X \mid \Gamma \vdash K} \quad (3.7b)
\]

\[
\frac{}{X \mid \Gamma, x \vdash J} \quad (3.7c)
\]

\[
\frac{}{X \mid \Gamma \vdash K} \quad (3.7d)
\]

\[
\frac{X, \beta x' \mid [x \mapsto x'] \Gamma \vdash [x \mapsto x']^+ J^+}{X, x \mid \Gamma \vdash J} \quad (3.7e)
\]
The admissibility of Rule (3.7a) is, in practice, ensured by explicitly including it in a limited form sufficient to ensure that it holds for the general case.

The admissibility of Rules (3.7c) and (3.7d) are assured if each of the parametric rules is pure. For then we may simply assimilate the parameter $x$ to the global parameters, and the hypothesis $J$ to the global hypotheses, without disrupting the validity of the derivation.

The admissibility of Rule (3.7e) is ensured by requiring that a rule be stated for all choices of local parameters provided that they are disjoint from the global parameters. This is called the renaming convention. In a proof by rule induction the naming convention allows us to choose the local parameters to be as fresh as required in a given situation, without explicit mention of having done so. In particular, this ensures that Rule (3.7e) is admissible. When constructing a derivation we need not provide a separate derivation for each choice of local parameters, but rather can provide only one derivation using some choice of fresh local parameters, for we may then transform this single derivation into the required family of derivations by simply renaming the chosen parameters in the given derivation.

Examples of parametric inductive definitions are given in Chapters 6 and 7, and will be used heavily throughout the book.

### 3.5 Exercises

1. Investigate parametric admissibility.

2. Prove structurality.

3. Explore identification convention.
Chapter 4

Transition Systems

Transition systems are used to describe the execution behavior of programs by defining an abstract computing device with a set, $S$, of states that are related by a transition judgement, $\rightarrow$. The transition judgement describes how the state of the machine evolves during execution.

4.1 Transition Systems

An (ordinary) transition system is specified by the following judgements:

1. $s$ state, asserting that $s$ is a state of the transition system.
2. $s$ final, where $s$ state, asserting that $s$ is a final state.
3. $s$ initial, where $s$ state, asserting that $s$ is an initial state.
4. $s \rightarrow s'$, where $s$ state and $s'$ state, asserting that state $s$ may transition to state $s'$.

We require that if $s$ final, then for no $s'$ do we have $s \rightarrow s'$. In general, a state $s$ for which there is no $s' \in S$ such that $s \rightarrow s'$ is said to be stuck, which may be indicated by writing $s \nrightarrow$. All final states are stuck, but not all stuck states need be final!

A transition sequence is a sequence of states $s_0, \ldots, s_n$ such that $s_0$ initial, and $s_i \rightarrow s_{i+1}$ for every $0 \leq i < n$. A transition sequence is maximal iff $s_n \nrightarrow$, and it is complete iff it is maximal and, in addition, $s_n$ final. Thus every complete transition sequence is maximal, but maximal sequences are not necessarily complete. A transition system is deterministic iff for every
state $s$ there exists at most one state $s'$ such that $s \rightarrow s'$, otherwise it is non-deterministic.

A labelled transition system over a set of labels, $I$, is a generalization of a transition system in which the single transition judgement, $s \rightarrow s'$ is replaced by an $I$-indexed family of transition judgements, $s \overset{i}{\rightarrow} s'$, where $s$ and $s'$ are states of the system. In typical situations the family of transition relations is given by a simultaneous inductive definition in which each rule may make reference to any member of the family.

It is often necessary to consider families of transition relations in which there is a distinguished unlabelled transition, $s \rightarrow s'$, in addition to the indexed transitions. It is sometimes convenient to regard this distinguished transition as labelled by a special, anonymous label not otherwise in $I$. For historical reasons this distinguished label is often designated by $\tau$ or $\epsilon$, but we will simply use an unadorned arrow. The unlabelled form is often called a silent transition, in contrast to the labelled forms, which announce their presence with a label.

### 4.2 Iterated Transition

Let $s \rightarrow s'$ be a transition judgement, whether drawn from an indexed set of such judgements or not.

The iteration of transition judgement, $s \rightarrow^* s'$, is inductively defined by the following rules:

\[
\begin{align*}
\frac{}{s \rightarrow^* s} \quad (4.1a) \\
\frac{s \rightarrow s' \quad s' \rightarrow^* s''}{s \rightarrow^* s''} \quad (4.1b)
\end{align*}
\]

It is easy to show that iterated transition is transitive: if $s \rightarrow^* s'$ and $s' \rightarrow^* s''$, then $s \rightarrow^* s''$.

The principle of rule induction for these rules states that to show that $P(s, s')$ holds whenever $s \rightarrow^* s'$, it is enough to show these two properties of $P$:

1. $P(s, s)$.
2. if $s \rightarrow s'$ and $P(s', s'')$, then $P(s, s'')$.

The first requirement is to show that $P$ is reflexive. The second is to show that $P$ is closed under head expansion, or converse evaluation. Using this principle, it is easy to prove that $\rightarrow^*$ is reflexive and transitive.
4.3 Simulation and Bisimulation

The \textit{n-times iterated} transition judgement, \( s \rightarrow^n s' \), where \( n \geq 0 \), is inductively defined by the following rules.

\[
\begin{align*}
  & s \rightarrow^0 s \\
  & s \rightarrow s' \quad s' \rightarrow^n s'' \\
  & s \rightarrow^{n+1} s''
\end{align*}
\]

(4.2a)

(4.2b)

\textbf{Theorem 4.1.} For all states \( s \) and \( s' \), \( s \rightarrow^* s' \) iff \( s \rightarrow^k s' \) for some \( k \geq 0 \).

Finally, we write \( s \downarrow \) to indicate that there exists some \( s' \) final such that \( s \rightarrow^* s' \).

4.3 Simulation and Bisimulation

A \textit{strong simulation} between two transition systems \( \rightarrow_1 \) and \( \rightarrow_2 \) is given by a binary relation, \( s_1 S s_2 \), between their respective states such that if \( s_1 S s_2 \), then \( s_1 \rightarrow_1 s'_1 \) implies \( s_2 \rightarrow_2 s'_2 \) for some state \( s'_2 \) such that \( s'_1 S s'_2 \). Two states, \( s_1 \) and \( s_2 \), are \textit{strongly similar} iff there is a strong simulation, \( S \), such that \( s_1 S s_2 \). Two transition systems are \textit{strongly similar} iff each initial state of the first is strongly similar to an initial state of the second. Finally, two transition systems are \textit{strongly bisimilar} iff there is a single relation \( S \) such that both \( S \) and its converse are strong simulations.

A strong simulation between two labelled transition systems over the same set, \( I \), of labels consists of a relation \( S \) between states such that for each \( i \in I \) the relation \( S \) is a strong simulation between \( \rightarrow^i_1 \) and \( \rightarrow^i_2 \). That is, if \( s_1 S s_2 \), then \( s_1 \rightarrow^i_1 s'_1 \) implies \( s_2 \rightarrow^i_2 s'_2 \) for some \( s'_2 \) such that \( s'_1 S s'_2 \). In other words, the simulation must preserve labels, not just transitions.

The requirements for strong simulation are rather stringent: every step in the first system must be mimicked by a similar step in the second, up to the simulation relation in question. This means, in particular, that a sequence of steps in the first system can only be simulated by a sequence of steps of the same length in the second—there is no possibility of performing “extra” work to achieve the simulation.

A \textit{weak simulation} between transition systems is a binary relation between states such that if \( s_1 S s_2 \), then \( s_1 \rightarrow_1 s'_1 \) implies \( s_2 \rightarrow_2 s'_2 \) for some \( s'_2 \) such that \( s'_1 S s'_2 \). That is, every step in the first may be matched by zero or more steps in the second. A \textit{weak bisimulation} is such that both
it and its converse are weak simulations. We say that states $s_1$ and $s_2$ are weakly (bi)similar iff there is a weak (bi)simulation $S$ such that $s_1 S s_2$.

The corresponding notion of weak simulation for labelled transitions involves the silent transition. The idea is that to weakly simulate the labelled transition $s_1 \xrightarrow{l} s'_1$, we do not wish to permit multiple labelled transitions between related states, but rather to permit any number of unlabelled transitions to accompany the labelled transition. A relation between states is a weak simulation iff it satisfies both of the following conditions whenever $s_1 S s_2$:

1. If $s_1 \xrightarrow{\cdot} s'_1$, then $s_2 \xrightarrow{\cdot} s'_2$ for some $s'_2$ such that $s'_1 S s'_2$.

2. If $s_1 \xrightarrow{l} s'_1$, then $s_2 \xrightarrow{\cdot} s'_2 \xrightarrow{l} \xrightarrow{\cdot} s'_2$ for some $s'_2$ such that $s'_1 S s'_2$.

That is, every silent transition must be mimicked by zero or more silent transitions, and every labelled transition must be mimicked by a corresponding labelled transition, preceded and followed by any number of silent transitions. As before, a weak bisimulation is a relation between states such that both it and its converse are weak simulations. Finally, two states are weakly (bi)similar iff there is a weak (bi)simulation between them.

### 4.4 Exercises

1. Prove that $S$ is a weak simulation for the ordinary transition system $\xrightarrow{\cdot}$ iff $S$ is a strong simulation for $\xrightarrow{\cdot\cdot}$.
Part II

Levels of Syntax
Chapter 5

Concrete Syntax

The concrete syntax of a language is a means of representing expressions as strings that may be written on a page or entered using a keyboard. The concrete syntax usually is designed to enhance readability and to eliminate ambiguity. While there are good methods for eliminating ambiguity, improving readability is, to a large extent, a matter of taste.

In this chapter we introduce the main methods for specifying concrete syntax, using as an example an illustrative expression language, called $L\{\text{num str}\}$, that supports elementary arithmetic on the natural numbers and simple computations on strings. In addition, $L\{\text{num str}\}$ includes a construct for binding the value of an expression to a variable within a specified scope.

5.1 Strings Over An Alphabet

An alphabet is a (finite or infinite) collection of characters. We write $c \text{ char}$ to indicate that $c$ is a character, and let $\Sigma$ stand for a finite set of such judgements, which is sometimes called an alphabet. The judgement $\Sigma \vdash s \text{ str}$, defining the strings over the alphabet $\Sigma$, is inductively defined by the following rules:

\[
\begin{align*}
\Sigma & \vdash \epsilon \text{ str} \quad (5.1a) \\
\Sigma & \vdash c \text{ char} \quad \Sigma \vdash s \text{ str} \quad (5.1b) \\
\Sigma & \vdash c \cdot s \text{ str}
\end{align*}
\]

Thus a string is essentially a list of characters, with the null string being the empty list. We often suppress explicit mention of $\Sigma$ when it is clear from context.
When specialized to Rules (5.1), the principle of rule induction states that to show \( s \ P \) holds whenever \( s \ \text{str} \), it is enough to show

1. \( \varepsilon \ P \), and
2. if \( s \ P \) and \( c \ \text{char} \), then \( c \cdot s \ P \).

This is sometimes called the principle of string induction. It is essentially equivalent to induction over the length of a string, except that there is no need to define the length of a string in order to use it.

The following rules constitute an inductive definition of the judgement \( s_1 \cdot s_2 = s \ \text{str} \), stating that \( s \) is the result of concatenating the strings \( s_1 \) and \( s_2 \).

\[
\begin{align*}
\varepsilon \cdot s &= s \ \text{str} \\
(\cdot s_1) \cdot s_2 &= c \cdot s \ \text{str}
\end{align*}
\]

(5.2a) (5.2b)

It is easy to prove by string induction on the first argument that this judgement has mode \((\forall, \forall, \exists!)\). Thus, it determines a total function of its first two arguments.

Strings are usually written as juxtapositions of characters, writing just \( abcd \) for the four-letter string \( a \cdot (b \cdot (c \cdot (d \cdot \varepsilon))) \), for example. Concatenation is also written as juxtaposition, and individual characters are often identified with the corresponding unit-length string. This means that \( abcd \) can be thought of in many ways, for example as the concatenations \( ab \cdot cd \), \( a \cdot bc \cdot d \), or \( abc \cdot d \), or even \( \varepsilon \cdot abcd \) or \( abcd \cdot \varepsilon \), as may be convenient in a given situation.

## 5.2 Lexical Structure

The first phase of syntactic processing is to convert from a character-based representation to a symbol-based representation of the input. This is called lexical analysis, or lexing. The main idea is to aggregate characters into symbols that serve as tokens for subsequent phases of analysis. For example, the numeral 467 is written as a sequence of three consecutive characters, one for each digit, but is regarded as a single token, namely the number 467. Similarly, an identifier such as \( \text{temp} \) comprises four letters, but is treated as
a single symbol representing the entire word. Moreover, many character-based representations include empty “white space” (spaces, tabs, newlines, and, perhaps, comments) that are discarded by the lexical analyzer.

The character representation of symbols is, in most cases, conveniently described using regular expressions. The lexical structure of $L\{\text{num str}\}$ is specified as follows:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Item</td>
<td>(\text{itm} ::= \text{kwd}</td>
</tr>
<tr>
<td>Keyword</td>
<td>(\text{kwd} ::= \text{l} \cdot \text{e} \cdot \text{t} \cdot \epsilon</td>
</tr>
<tr>
<td>Identifier</td>
<td>(\text{id} ::= \text{ltr} (\text{ltr}</td>
</tr>
<tr>
<td>Numeral</td>
<td>(\text{num} ::= \text{dig} \text{dig}^*)</td>
</tr>
<tr>
<td>Literal</td>
<td>(\text{lit} ::= \text{qum} (\text{ltr}</td>
</tr>
<tr>
<td>Special</td>
<td>(\text{spl} ::= +</td>
</tr>
<tr>
<td>Letter</td>
<td>(\text{ltr} ::= \text{a}</td>
</tr>
<tr>
<td>Digit</td>
<td>(\text{dig} ::= 0</td>
</tr>
<tr>
<td>Quote</td>
<td>(\text{qum} ::= &quot; )</td>
</tr>
</tbody>
</table>

A lexical item is either a keyword, an identifier, a numeral, a string literal, or a special symbol. There are three keywords, specified as sequences of characters, for emphasis. Identifiers start with a letter and may involve subsequent letters or digits. Numerals are non-empty sequences of digits. String literals are sequences of letters or digits surrounded by quotes. The special symbols, letters, digits, and quote marks are as enumerated. (Observe that we tacitly identify a character with the unit-length string consisting of that character.)

The job of the lexical analyzer is to translate character strings into token strings using the above definitions as a guide. An input string is scanned, ignoring white space, and translating lexical items into tokens, which are specified by the following rules:

\[
\begin{align*}
\text{s str} & \quad \overset{\text{ID}[s]}{\text{tok}} \\
\text{n nat} & \quad \overset{\text{NUM}[n]}{\text{tok}} \\
\text{s str} & \quad \overset{\text{LIT}[s]}{\text{tok}} \\
\text{LET} & \quad \overset{\text{tok}}{\text{tok}}
\end{align*}
\]

\(^1\)In some languages white space is significant, in which case it must be converted to symbolic form for subsequent processing.
Lexical analysis is inductively defined by the following judgement forms:

\[
\begin{array}{ll}
\text{s charstr} & \leftrightarrow \text{t tokstr} \quad \text{Scan input} \\
\text{s itm} & \leftrightarrow \text{t tok} \quad \text{Scan an item} \\
\text{s kwd} & \leftrightarrow \text{t tok} \quad \text{Scan a keyword} \\
\text{s id} & \leftrightarrow \text{t tok} \quad \text{Scan an identifier} \\
\text{s num} & \leftrightarrow \text{t tok} \quad \text{Scan a number} \\
\text{s spl} & \leftrightarrow \text{t tok} \quad \text{Scan a symbol} \\
\text{s lit} & \leftrightarrow \text{t tok} \quad \text{Scan a string literal} \\
\text{s whs} & \quad \text{Skip white space}
\end{array}
\]

The definition of these forms, which follows, makes use of several auxiliary judgements corresponding to the classifications of characters in the lexical structure of the language. For example, \( s \text{ whs} \) states that the string \( s \) consists only of “white space”, and \( s \text{ lord} \) states that \( s \) is either an alphabetic letter or a digit, and so forth.

\[
\epsilon \text{ charstr} \leftrightarrow \epsilon \text{ tokstr} \quad (5.4a)
\]
\[ s = s_1 \cdot s_2 \cdot s_3 \] str
(5.2)

\[ s_1 \text{ whs } s_2 \text{ itm } \leftrightarrow t \text{ tok } s_3 \text{ charstr } \leftrightarrow ts \text{ tokstr} \]
\[ s \text{ charstr } \leftrightarrow t \cdot ts \text{ tokstr} \]
(5.4b)

\[ s \text{ kwd } \leftrightarrow t \text{ tok} \]
\[ s \text{ itm } \leftrightarrow t \text{ tok} \]
(5.4c)

\[ s \text{ id } \leftrightarrow t \text{ tok} \]
\[ s \text{ itm } \leftrightarrow t \text{ tok} \]
(5.4d)

\[ s \text{ num } \leftrightarrow t \text{ tok} \]
\[ s \text{ itm } \leftrightarrow t \text{ tok} \]
(5.4e)

\[ s \text{ lit } \leftrightarrow t \text{ tok} \]
\[ s \text{ itm } \leftrightarrow t \text{ tok} \]
(5.4f)

\[ s \text{ spl } \leftrightarrow t \text{ tok} \]
\[ s \text{ itm } \leftrightarrow t \text{ tok} \]
(5.4g)

\[ s = l \cdot e \cdot t \cdot e \text{ str} \]
\[ s \text{ kwd } \leftrightarrow \text{ LET tok} \]
(5.4h)

\[ s = b \cdot e \cdot e \text{ str} \]
\[ s \text{ kwd } \leftrightarrow \text{ BE tok} \]
(5.4i)

\[ s = i \cdot n \cdot e \text{ str} \]
\[ s \text{ kwd } \leftrightarrow \text{ IN tok} \]
(5.4j)

\[ s = s_1 \cdot s_2 \cdot s_3 \text{ str } s_1 \text{ ltr } s_2 \text{ lord } s_2 \text{ lord} \]
\[ s \text{ id } \leftrightarrow \text{ ID[s] tok} \]
(5.4k)

\[ s = s_1 \cdot s_2 \text{ str } s_1 \text{ dig } s_2 \text{ dgs } s \text{ num } \leftrightarrow n \text{ nat} \]
\[ s \text{ num } \leftrightarrow \text{ NUM[n] tok} \]
(5.4l)

\[ s = s_1 \cdot s_2 \cdot s_3 \text{ str } s_1 \text{ qum } s_2 \text{ lord } s_3 \text{ qum} \]
\[ s \text{ lit } \leftrightarrow \text{ LIT[s] tok} \]
(5.4m)

\[ s = + \cdot e \text{ str} \]
\[ s \text{ spl } \leftrightarrow \text{ ADD tok} \]
(5.4n)

\[ s = * \cdot e \text{ str} \]
\[ s \text{ spl } \leftrightarrow \text{ MUL tok} \]
(5.4o)

\[ s = ^\cdot e \text{ str} \]
\[ s \text{ spl } \leftrightarrow \text{ CAT tok} \]
(5.4p)
5.3 Context-Free Grammars

The standard method for defining concrete syntax is by giving a context-free grammar for the language. A grammar consists of three components:

1. The tokens, or terminals, over which the grammar is defined.
2. The syntactic classes, or non-terminals, which are disjoint from the terminals.
3. The rules, or productions, which have the form $A ::= \alpha$, where $A$ is a non-terminal and $\alpha$ is a string of terminals and non-terminals.

Each syntactic class is a collection of token strings. The rules determine which strings belong to which syntactic classes.

When defining a grammar, we often abbreviate a set of productions,

\[
A ::= \alpha_1 \\
\vdots \\
A ::= \alpha_n,
\]

each with the same left-hand side, by the compound production

\[
A ::= \alpha_1 | \ldots | \alpha_n,
\]

which specifies a set of alternatives for the syntactic class $A$.

A context-free grammar determines a simultaneous inductive definition of its syntactic classes. Specifically, we regard each non-terminal, $A$, as
5.4 Grammatical Structure

a judgement form, $s \ A$, over strings of terminals. To each production of the form

$$A ::= s_1 \ A_1 \ s_2 \ldots \ s_n \ A_n \ s_{n+1} \quad (5.5)$$

we associate an inference rule

$$\frac{s'_1 \ A_1 \ldots \ s'_n \ A_n}{s_1 \ s'_1 \ s_2 \ldots \ s_n \ s'_n \ s_{n+1} \ A} \quad (5.6)$$

The collection of all such rules constitutes an inductive definition of the syntactic classes of the grammar.

Recalling that juxtaposition of strings is short-hand for their concatenation, we may re-write the preceding rule as follows:

$$\frac{s'_1 \ A_1 \ldots \ s'_n \ A_n}{s_1 \ ^* \ s'_1 \ ^* \ s_2 \ldots \ s_n \ ^* \ s'_n \ ^* \ s_{n+1} \ A} \quad (5.7)$$

This formulation makes clear that $s \ A$ holds whenever $s$ can be partitioned as described so that $s'_i \ A$ for each $1 \leq i \leq n$. Since string concatenation is not invertible, the decomposition is not unique, and so there may be many different ways in which the rule applies.

5.4 Grammatical Structure

The concrete syntax of $\mathcal{L}\{\text{num str}\}$ may be specified by a context-free grammar over the tokens defined in Section 5.2 on page 38. The grammar has only one syntactic class, $\exp$, which is defined by the following compound production:

<table>
<thead>
<tr>
<th>Token</th>
<th>Production</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expression</td>
<td>$\exp ::= \text{num}</td>
</tr>
<tr>
<td>Number</td>
<td>$\text{num} ::= \text{NUM}[n] \quad (n \ \text{nat})$</td>
</tr>
<tr>
<td>String</td>
<td>$\text{lit} ::= \text{LIT}[s] \quad (s \ \text{str})$</td>
</tr>
<tr>
<td>Identifier</td>
<td>$\text{id} ::= \text{ID}[s] \quad (s \ \text{str})$</td>
</tr>
</tbody>
</table>

This grammar makes use of some standard notational conventions to improve readability: we identify a token with the corresponding unit-length string, and we use juxtaposition to denote string concatenation.

Applying the interpretation of a grammar as an inductive definition, we obtain the following rules:

$$\frac{s \ \text{num}}{s \ \exp} \quad (5.8a)$$

DECEMBER 18, 2009

DRAFT 14:36
To emphasize the role of string concatenation, we may rewrite Rule (5.8e), for example, as follows:

\[ s = s_1 \text{MUL} s_2 \text{str} \]

That is, \( s \text{ exp} \) is derivable if \( s \) is the concatenation of \( s_1 \), the multiplication sign, and \( s_2 \), where \( s_1 \text{ exp} \) and \( s_2 \text{ exp} \).
5.5 Ambiguity

Apart from subjective matters of readability, a principal goal of concrete syntax design is to eliminate ambiguity. The grammar of arithmetic expressions given above is ambiguous in the sense that some token strings may be thought of as arising in several different ways. More precisely, there are token strings \( s \) for which there is more than one derivation ending with \( s \text{ exp} \) according to Rules (5.8).

For example, consider the character string \( 1+2*3 \), which, after lexical analysis, is translated to the token string

\[
\text{NUM}[1] \text{ ADD } \text{NUM}[2] \text{ MUL } \text{NUM}[3].
\]

Since string concatenation is associative, this token string can be thought of as arising in several ways, including

\[
\text{NUM}[1] \text{ ADD } \wedge \text{NUM}[2] \text{ MUL } \text{NUM}[3]
\]

and

\[
\text{NUM}[1] \text{ ADD } \wedge \text{NUM}[2] \wedge \text{MUL } \text{NUM}[3],
\]

where the caret indicates the concatenation point.

One consequence of this observation is that the same token string may be seen to be grammatical according to the rules given in Section 5.4 on page 43 in two different ways. According to the first reading, the expression is principally an addition, with the first argument being a number, and the second being a multiplication of two numbers. According to the second reading, the expression is principally a multiplication, with the first argument being the addition of two numbers, and the second being a number.

Ambiguity is a purely syntactic property of grammars; it has nothing to do with the “meaning” of a string. For example, the token string

\[
\text{NUM}[1] \text{ ADD } \text{NUM}[2] \text{ ADD } \text{NUM}[3],
\]

also admits two readings. It is immaterial that both readings have the same meaning under the usual interpretation of arithmetic expressions. Moreover, nothing prevents us from interpreting the token ADD to mean “division,” in which case the two readings would hardly coincide! Nothing in the syntax itself precludes this interpretation, so we do not regard it as relevant to whether the grammar is ambiguous.

To eliminate ambiguity the grammar of \( \mathcal{L}\{\text{num str}\} \) given in Section 5.4 on page 43 must be re-structured to ensure that every grammatical string...
has at most one derivation according to the rules of the grammar. The main method for achieving this is to introduce precedence and associativity conventions that ensure there is only one reading of any token string. Parenthesization may be used to override these conventions, so there is no fundamental loss of expressive power in doing so.

Precedence relationships are introduced by layering the grammar, which is achieved by splitting syntactic classes into several sub-classes.

Factor 
\[ fct ::= \text{num} | \text{lit} | \text{id} | \text{LP prg RP} \]

Term 
\[ trm ::= fct | fct \text{MUL} trm | \text{VB fct VB} \]

Expression 
\[ \text{exp} ::= \text{trm} | \text{trm ADD exp} | \text{trm CAT exp} \]

Program 
\[ \text{prg} ::= \text{exp} | \text{LET id BE exp IN prg} \]

The effect of this grammar is to ensure that \text{let} has the lowest precedence, addition and concatenation intermediate precedence, and multiplication and length the highest precedence. Moreover, all forms are right-associative. Other choices of rules are possible, according to taste; this grammar illustrates one way to resolve the ambiguities of the original expression grammar.

5.6 Exercises
Chapter 6

Abstract Syntax Trees

The concrete syntax of a language defines its linear representation as strings of symbols. The string representation of a program is convenient for keyboard input and network transmission, but is all-but-useless for analysis of the properties of programming languages. The abstract syntax of a language dispenses with the linear representation in favor of exposing the hierarchical structure of programs, making clear which phrases are constituents of which others. Phrases are represented as abstract syntax trees, or ast’s, that may involve variables serving as placeholders for other ast’s.

6.1 Abstract Syntax Trees

An abstract syntax tree, or ast for short, is an ordered tree in which nodes are labelled by operators. Each operator has an arity specifying the number of children of any node that it labels. A signature, $\Omega$, is a finite set of judgements of the form $ar(o) = k$, which specifies that the operator $o$ has arity $k \geq 0$. A signature may specify at most one arity for each operator.

The class of closed abstract syntax trees over a signature, $\Omega$, is inductively defined by the following rules:

$$\Omega \vdash ar(o) = k$$
$$\begin{array}{c}
a_1 \text{ ast} \\
\vdots \\
a_k \text{ ast} \\
o(a_1, \ldots, a_k) \text{ ast}
\end{array}$$

(6.1a)

One may read this as specifying one rule for each operator, $o$, such that $\Omega \vdash ar(o) = k$. When $k$ is zero, Rule (6.1a) has no premises (other than the arity judgement), and hence forms the basis for the induction. The ast $o()$ is usually abbreviated to $o$ for operators of arity zero.
The rule set $A[\Omega]$ consists of the expansion of Rules (6.1) with judgements of $\Omega$ as axioms (rules without premises).

For example, the abstract syntax of closed arithmetic expressions (without variables) may be specified by the following signature:

\[
\begin{align*}
ar(num[n]) &= 0 \quad (n \text{ nat}) \
ar(str[s]) &= 0 \quad (s \text{ str}) \
ar(plus) &= 2 \
ar(times) &= 2 \
ar(cat) &= 2 \
ar(len) &= 1
\end{align*}
\]

Accounting for the binding and scope of variables goes beyond the expressive capabilities of ast’s; this will be rectified in Chapter 7 using an enriched form of ast’s.

The principle of structural induction is the principle of rule induction specialized to $A[\Omega]$ for some signature $\Omega$. Specifically, to show that $P(a \text{ ast})$

\[
\text{if } P(a_1 \text{ ast}), \ldots, P(a_k \text{ ast}), \text{ then } P(o(a_1, \ldots, a_k) \text{ ast}).
\]

When $k$ is zero, this reduces to showing that $P(o)$.

For example, consider the following rules defining the height of a closed abstract syntax tree over some signature $\Omega$:

\[
\begin{align*}
hgt(a_1) &= h_1 \quad \ldots \quad hgt(a_k) = h_k \
\max(h_1, \ldots, h_k) &= h \quad \text{ar}(o) = k \\
hgt(o(a_1, \ldots, a_k)) &= h + 1
\end{align*}
\]

There is one rule for each $k$ such that $\Omega \vdash \text{ar}(o) = k$ for some operator $o$. Let $H[\Omega]$ consist of rules $A[\Omega]$ and Rules (6.1).

We may prove by structural induction that every ast has a unique height. For an operator $o$ of arity $k$, we may assume by induction that, for each $1 \leq i \leq k$, there is a unique $h_i$ such that $hgt(a_i) = h_i$. We may show separately that the maximum, $h$, of these is uniquely determined, and hence that the overall height, $h + 1$, is also uniquely determined.

### 6.2 Variables and Substitution
A variable in an ast is a placeholder for a fixed, but unspecified, ast. Given an ast and a designated variable, we may substitute an ast for all occurrences of that variable in that ast.

Fix a signature, $\Omega$, of operators, let $\mathcal{X} = \{x_1, \ldots, x_m\}$ be a finite set of parameters, and let $\Gamma$ be the finite set of hypotheses $x_1$ ast, $\ldots$, $x_m$ ast. The parametric judgement

$$\mathcal{X} \mid \Gamma \vdash_{A[\Omega]} a \text{ ast}$$

(6.3)

states that $a$ is an ast in which any of the parameters in $\mathcal{X}$ may be used as atomic ast’s. Once we define substitution these atomic ast’s will function as variables that may be replaced with other ast’s.

The parametric judgement (6.3) may be directly defined by the following rules:

$$\mathcal{X}, x \mid \Gamma, x \text{ ast} \vdash x \text{ ast}$$

(6.4a)

$$\begin{array}{c}
\frac{\Omega \vdash \text{ar}(o) = k \quad \mathcal{X} \mid \Gamma \vdash a_1 \text{ ast} \quad \ldots \quad \mathcal{X} \mid \Gamma \vdash a_k \text{ ast}}{
\mathcal{X} \mid \Gamma \vdash o(a_1, \ldots, a_k) \text{ ast}}
\end{array}$$

(6.4b)

It is easy to check that the judgement $\mathcal{X} \mid \Gamma \vdash a \text{ ast}$ defined by these rules is structural.

The principle of structural induction extends to ast’s with variables. To prove that $\mathcal{P}(\mathcal{X} \mid \Gamma \vdash a \text{ ast})$ holds whenever $\mathcal{X} \mid \Gamma \vdash a \text{ ast}$, it is enough to show these two facts:

1. $\mathcal{P}(\mathcal{X}, x \mid \Gamma, x \text{ ast} \vdash x \text{ ast})$ for every $\mathcal{X}$ and parameter $x \not\in \mathcal{X}$.

2. If $\Omega \vdash \text{ar}(o) = k$, and $\mathcal{P}(\mathcal{X} \mid \Gamma \vdash a_i \text{ ast})$ for each $1 \leq i \leq k$, then $\mathcal{P}(\mathcal{X} \mid \Gamma \vdash o(a_1, \ldots, a_k))$

As discussed in Chapter 3 we consider only properties $\mathcal{P}$ that are independent of the names of the parameters.

The definition of the height of an ast may be extended to ast’s with variables. Let $\mathcal{X}$ and $\Gamma$ be as above. The parametric judgement $\mathcal{X} \mid \Gamma \vdash \text{hgt}(a) = m$ is inductively defined by the following rules:

$$\mathcal{X}, x \mid \Gamma, x \text{ ast} \vdash \text{hgt}(x) = 1$$

(6.5a)

$$\begin{array}{c}
\Omega \vdash \text{ar}(o) = k \quad \text{max}(h_1, \ldots, h_k) = h \\
\mathcal{X} \mid \Gamma \vdash \text{hgt}(a_1) = h_1 \quad \ldots \quad \mathcal{X} \mid \Gamma \vdash \text{hgt}(a_k) = h_k
\end{array}
\quad \implies \quad
\mathcal{X} \mid \Gamma \vdash \text{hgt}(o(a_1, \ldots, a_n)) = h + 1$$

(6.5b)
6.2 Variables and Substitution

Let \( H[\Omega] \) be the extension of rules \( A[\Omega] \) with Rules (6.5). A simple structural induction shows that every ast with variables has a height.

**Theorem 6.1.** Let \( \mathcal{X} = \{ x_1, \ldots, x_m \} \), and \( \Gamma = x_1 \text{ ast}, \ldots, x_m \text{ ast} \). If \( \mathcal{X} \mid \Gamma \vdash A[\Omega] \text{ a ast} \), then there exists a unique \( h \) such that \( \mathcal{X} \mid \Gamma \vdash H[\Omega] \text{ hgt}(a) = h \).

**Proof.** By structural induction on \( a \), which is to say by rule induction on Rules (6.4). For Rule (6.4a) the unique \( p \) is provided by Rule (6.5a). For Rule (6.4b) the result follows by induction and the unicity of the maximum.

Substitution is the process of replacing all occurrences of a variable in an ast with another ast. Substitution is defined by a parametric inductive definition of the judgment \( \mathcal{X} \mid \Gamma \vdash [a/x]b = c \text{ ast} \), which states that the result of substituting \( a \) for \( x \) in \( b \) is \( c \).

\[
\frac{}{\mathcal{X} \mid \Gamma \vdash [a/x]x = a \text{ ast}} \quad (6.6a)
\]

\[
\frac{x \neq y}{\mathcal{X}, y \mid \Gamma, y \text{ ast} \vdash [a/x]y = y \text{ ast}} \quad (6.6b)
\]

\[
\frac{\Gamma \vdash ar(o) = k \quad \mathcal{X} \mid \Gamma \vdash [a/x]b_1 = c_1 \text{ ast} \quad \ldots \quad \mathcal{X} \mid \Gamma \vdash [a/x]b_k = c_k \text{ ast}}{\mathcal{X} \mid \Gamma \vdash [a/x]o(b_1, \ldots, b_k) = o(c_1, \ldots, c_k) \text{ ast}} \quad (6.6c)
\]

Let \( S[\Omega] \) be the expansion of rules \( A[\Omega] \) with Rules (6.6).

**Theorem 6.2.** Let \( \mathcal{X} = \{ x_1, \ldots, x_n \} \) and let \( \Gamma \) be \( x_1 \text{ ast}, \ldots, x_n \text{ ast} \). If \( \mathcal{X} \mid \Gamma \vdash A[\Omega] \text{ a ast} \), and \( \mathcal{X}, x \mid \Gamma, x \text{ ast} \vdash A[\Omega] \text{ b ast} \), where \( x \notin \mathcal{X} \), then there exists a unique \( c \) such that \( \mathcal{X} \mid \Gamma \vdash S[\Omega] [a/x]b = c \text{ ast} \).

**Proof.** By structural induction on \( b \). There are three cases to consider, corresponding to the inferences

1. \( \mathcal{X}, x \mid \Gamma, x \text{ ast} \vdash x \text{ ast} \);
2. \( \mathcal{X}, x, y \mid \Gamma, x \text{ ast}, y \text{ ast} \vdash y \text{ ast} \), where \( y \notin \mathcal{X}, x \) and so \( y \neq x \).
3. \( \mathcal{X}, x \mid \Gamma, x \text{ ast} \vdash o(b_1, \ldots, b_k) \text{ ast} \), given that \( \mathcal{X}, x \mid \Gamma, x \text{ ast} \vdash b_i \text{ ast} \) for each \( 1 \leq i \leq k \).

14:36 DRAFT DECEMBER 18, 2009
The first two cases are covered by Rules (6.6a) and (6.6b); the third is covered by induction and Rule (6.6c).

In view of this theorem we write \([a/x]b\) for the unique \(c\) given by the theorem, provided that we are in a context in which the premises of the theorem are understood to hold.

**Corollary 6.3.** The structural rule of substitution

\[
\frac{\mathcal{X} \mid \Gamma \vdash a \text{ ast} \quad \mathcal{X}, x \mid \Gamma, x \text{ ast} \vdash b \text{ ast}}{\mathcal{X} \mid \Gamma \vdash \left[a/x\right]b \text{ ast}}
\]

is admissible for Rules (6.4).

### 6.3 Exercises
Chapter 7

Binding and Scope

Abstract syntax trees expose the hierarchical structure of syntax, dispensing with the details of how one might represent pieces of syntax on a page or a computer screen. Abstract binding trees, or abt’s, enrich this representation with the concepts of binding and scope. In just about every language there is a means of associating a meaning to an identifier within a specified range of significance (perhaps the whole program, but often limited regions of it).

Abstract binding trees enrich abstract syntax trees with a means of introducing a fresh, or new, parameter within a specified scope. Uses of the parameter within that scope serve as references to the point at which the parameter is bound—it’s so-called binding site. Since bound parameters are merely references to a binding site, the name of the parameter does not matter, provided only that it does not conflict with any other parameters currently within scope. It is in this sense that a bound parameter is said to be “new” or “fresh”.

In this chapter we introduce the concept of an abstract binding tree, including the relation of $\alpha$-equivalence, which expresses the irrelevance of the choice of bound parameters, and the operation of capture-avoiding substitution, which ensures that parameters are not confused by substitution. While intuitively clear, the precise formalization of these concepts requires some care; experience has shown that it is surprisingly easy to get them wrong.

All of the programming languages that we shall study are represented as abstract binding trees. Consequently, we will re-use the machinery developed in this chapter many times, avoiding considerable redundancy and consolidating the effort required to make precise the notions of binding and
7.1 Abstract Binding Trees

The concepts of binding and scope are formalized by the concept of an abstract binding tree, or abt. An abt is an ast with an additional construct, called an abstractor, that introduces, or binds, a parameter for use within an abt, called the scope of the abstractor. Occurrences of the parameter within its scope are references to the abstractor at which it is bound. In this sense bound parameters behave like pronouns in natural language. Whenever we use a pronoun such as “it” in a sentence, it is understood to be a reference to an object that was specified in the context in which it occurs.

An abstractor has the form $x.a$, where $x$ is a parameter and $a$ is an abt. Such an abstractor binds the parameter, $x$, for use within its scope, the abt $a$. The parameter $x$ is meaningful only within $a$, and is, in a sense to be made precise shortly, distinct from any other parameters whose scope includes $a$. It is in this sense that an abstractor is said to introduce a “new” or “fresh” parameter for use within its scope. Making this precise requires some technical machinery, but the rough-and-ready rule is to consider each abstractor to bind a distinct parameter that serves as a reference to that binding site wherever it occurs.

As with abstract syntax trees, the definition of abstract binding trees is relative to a signature assigning arities to operators. However, to account for binding and scope, the concept of arity is generalized to be a finite sequence of natural numbers $(n_1, \ldots, n_k)$, where $k$ and each $n_i$ are natural numbers. The number $k$ determines the number of children of a node labelled with that operator, and, for each $1 \leq i \leq k$, the number $n_i$ specifies the number of parameters bound by that operator in the $i$th argument position. This number is called the valence of that argument. Only abstractors have positive valence; variables and operators form abt’s of valence zero. Since ast’s do not bind parameters, the abt arity $(0, 0, \ldots, 0)$ of length $k$ corresponds to the ast arity $k$—it specifies an operator with $k$ arguments that binds no variables in any argument.

A signature, $\Omega$, consists of a finite set of judgements $\text{ar}(o) = (n_1, \ldots, n_k)$ specifying the arity of some finite set of operators. The well-formed abt’s over a signature $\Omega$ are specified by a parametric judgement of the form

$$\{ x_1, \ldots, x_m \} \mid x_1 \text{ abt}^0, \ldots, x_m \text{ abt}^0 \vdash a \text{ abt}^n$$

stating that $a$ is an abt of valence $n$, with free variables $x_1, \ldots, x_m$. Let $\mathcal{X}$
range over parameter sets \( \{ x_1, \ldots, x_m \} \), and let \( \Gamma \) range over finite sets of hypotheses of the form \( x_1 \text{ abt}^0, \ldots, x_m \text{ abt}^0 \). The judgement (7.1) is inductively defined by the following rules:

\[
\begin{align*}
\frac{\mathcal{X}, x | \Gamma, \text{ x abt}^0 \vdash x \text{ abt}^0}{\mathcal{X}, \text{ x} | \Gamma, \text{ x abt}^0 \vdash x \text{ abt}^0} & \quad (7.2a) \\
\frac{\text{ar}(\alpha) = (n_1, \ldots, n_k)}{\mathcal{X} | \Gamma \vdash a_1 \text{ abt}^{n_1} \ldots \mathcal{X} | \Gamma \vdash a_k \text{ abt}^{n_k}} & \quad (7.2b) \\
\frac{\mathcal{X} | \Gamma \vdash a_1 \text{ abt}^{n_1} \ldots \mathcal{X} | \Gamma \vdash a_k \text{ abt}^{n_k}}{\mathcal{X} | \Gamma \vdash \alpha(a_1, \ldots, a_k) \text{ abt}^0} & \quad (7.2c)
\end{align*}
\]

Rule (7.2c) specifies that an abstractor, \( x \cdot a \), is an abt of valence \( n + 1 \) provided that \( a \) is an abt of valence \( n \) under the assumption that \( x \) is a “fresh” parameter of valence zero. The freshness of the parametric \( x \) is assured by the renaming convention discussed in Chapter 3. If \( x \in \mathcal{X} \), then the premise of the rule is implicitly renamed to the judgement

\[
\mathcal{X}, x' | \Gamma, x' \text{ abt}^0 \vdash [x \mapsto x'] (a) \text{ abt}^n
\]

where \( x' \notin \mathcal{X} \), ensuring freshness.

For example, the language \( L\{\text{num str}\} \) may be represented as abstract binding trees over the following signature:

\[
\begin{align*}
\text{ar}(\text{num}[n]) &= () \\
\text{ar}(\text{str}[s]) &= () \\
\text{ar}(\text{plus}) &= (0, 0) \\
\text{ar}(\text{times}) &= (0, 0) \\
\text{ar}(\text{cat}) &= (0, 0) \\
\text{ar}(\text{len}) &= (0) \\
\text{ar}(\text{let}) &= (0, 1)
\end{align*}
\]

Only the \textit{let} operator binds a parameter, and then only in its second argument. An abt formed from the operator \textit{let} must have the form

\[
\text{let}(a, x . b)
\]

where the first argument is an abt of valence zero, and the second is an abstractor of valence one. This specifies that the parameter, \( x \), is available for use within \( b \), but not within \( a \), and is distinct from all other parameters that may be within scope wherever this abt occurs.
7.1 Abstract Binding Trees

7.1.1 Structural Induction With Binding and Scope

The principle of structural induction for abstract syntax trees extends to abstract binding trees. For a fixed signature, \( \Omega \), to show that \( P(X; \Gamma \vdash a \text{ abt}^n) \) whenever \( X; \Gamma \vdash a \text{ abt}^n \), it suffices to show that \( P \) is closed under Rules (7.2). Specifically,

1. \( P(X; \Gamma, x \text{ abt}^0 \vdash x \text{ abt}^0) \).

2. If \( \Omega \vdash \text{ar}(o) = (n_1, \ldots, n_k) \) and \( P(X; \Gamma \vdash a_1 \text{ abt}^{n_1}), \ldots, P(X; \Gamma \vdash a_k \text{ abt}^{n_k}) \),
then \( P(X; \Gamma \vdash o(a_1, \ldots, a_k) \text{ abt}^0) \).

3. If \( P(X; x \mid \Gamma, x \text{ abt}^0 \vdash a \text{ abt}^n) \), then \( P(X; \Gamma \vdash x. a \text{ abt}^{n+1}) \).

By the renaming convention discussed in Chapter 3 the inductive hypothesis for abstractors holds for all choices of fresh local parameters. This means that we may tacitly choose the parameter, \( x \), to be any parameter not occurring in \( X \). In practice we simply assume that \( x \) has been so chosen, but in technical detail we must in general rename \( x \) to some other parameter \( x' \notin X \) in the case that \( x \in X \).

As an example, the following rules, \( H[\Omega] \), define the height of an abstract binding tree over a signature \( \Omega \):

\[
\frac{}{X, x \mid \Gamma, x \text{ abt}^0 \vdash \text{hgt}(x) = 1} \tag{7.3a}
\]

\[
\frac{X \mid \vdash \text{hgt}(a_1) = h_1 \ldots X \mid \vdash \text{hgt}(a_k) = h_k \quad \text{max}(h_1, \ldots, h_k) = h}{X \mid \vdash \text{hgt}(o(a_1; \ldots; a_k)) = h + 1} \tag{7.3b}
\]

\[
\frac{X, x \mid \Gamma, x \text{ abt}^0 \vdash \text{hgt}(a) = h}{X \mid \vdash \text{hgt}(x.a) = h + 1} \tag{7.3c}
\]

A straightforward structural induction shows that every well-formed abt has a height.

**Theorem 7.1.** If \( X \mid \Gamma \vdash a \text{ abt}^n \), then there exists a unique \( h \) such that \( X \mid \Gamma \vdash \text{hgt}(a) = h \).

Observe that this property respects renaming of parameters, since all are assigned unit height.
7.1 Abstract Binding Trees

7.1.2 Apartness

The parameter set, \( \mathcal{X} \), in the judgement \( \mathcal{X} \mid \Gamma \vdash a \text{ abt}^n \) \( \mathcal{X} \) implies that the only parameters that may occur in \( a \) are those in \( \mathcal{X} \). Occasionally it is useful to determine which parameters (among those that may) actually do, or do not, occur unbound in an abt.

The judgement \( \mathcal{X}, x \mid \Gamma, x \text{ abt}^0 \vdash x \notin a \text{ abt}^n \) states that \( x \) lies apart from abt \( a \). It is inductively defined by the following rules:

\[ \mathcal{X}, x, y \mid \Gamma, x \text{ abt}^0, y \text{ abt}^0 \vdash x \notin y \text{ abt}^0 \]  

\[ \mathcal{X}, x \mid \Gamma, x \text{ abt}^0 \vdash x \notin a_1 \text{ abt}^{n_1} \ldots \mathcal{X}, x \mid \Gamma, x \text{ abt}^0 \vdash x \notin a_k \text{ abt}^{n_k} \]  

\[ \mathcal{X}, x \mid \Gamma, x \text{ abt}^0 \vdash x \notin o(a_1, \ldots, a_k) \text{ abt}^0 \]  

\[ \mathcal{X}, x, y \mid \Gamma, x \text{ abt}^0, y \text{ abt}^0 \vdash x \notin a \text{ abt}^n \]  

\[ \mathcal{X}, x \mid \Gamma, x \text{ abt}^0 \vdash x \notin y \cdot a \text{ abt}^{n+1} \]  

By the renaming convention the parameters \( x \) and \( y \) in the premise Rule (7.4c) may be assumed to be distinct from each other and to not occur in \( \mathcal{X} \).

We say that a parameter, \( x \), lies within, or is free in, an abt, \( a \), written \( x \in a \text{ abt} \), iff it is not the case that \( x \notin a \text{ abt} \).

7.1.3 Renaming of Bound Parameters

Two abt\'s are said to be \( \alpha \)-equivalent iff they differ at most in the choice of bound parameter names. The judgement \( \mathcal{X} \mid \Gamma \vdash a =_\alpha b \text{ abt}^n \) is inductively defined by the following rules:

\[ \mathcal{X}, x \mid \Gamma, x \text{ abt}^0 \vdash x =_\alpha x \text{ abt}^0 \]  

\[ \mathcal{X} \mid \Gamma \vdash a_1 =_\alpha b_1 \text{ abt}^{n_1} \ldots \mathcal{X} \mid \Gamma \vdash a_k =_\alpha b_k \text{ abt}^{n_k} \]  

\[ \mathcal{X} \mid \Gamma \vdash o(a_1, \ldots, a_k) =_\alpha o(b_1, \ldots, b_k) \text{ abt}^0 \]  

\[ \mathcal{X}, z \mid \Gamma, z \text{ abt}^0 \vdash [x \mapsto z]^\dagger (a) =_\alpha [y \mapsto z]^\dagger (b) \text{ abt}^n \]  

\[ \mathcal{X} \mid \Gamma \vdash x \cdot a =_\alpha y \cdot b \text{ abt}^{n+1} \]  

In Rule (7.5c) we tacitly assume that \( z \notin \mathcal{X} \).

We write \( \Gamma \vdash a =_\alpha b \), or even just \( a =_\alpha b \), for \( \mathcal{X} \mid \Gamma \vdash a =_\alpha b \text{ abt}^n \) the parameters and valence are clear from context.
Lemma 7.2. The following instance of \( \alpha \)-equivalence, called \( \alpha \)-conversion, is derivable:

\[
\mathcal{X} \mid \Gamma \vdash x.a =_\alpha y.\left[y \mapsto \langle x \mapsto y \rangle \uparrow (a) \right] \text{abt}^{n+1} \quad (y \notin \mathcal{X})
\]

Theorem 7.3. \( \alpha \)-equivalence is reflexive, symmetric, and transitive.

Proof. Reflexivity and symmetry are immediately obvious from the form of the definition. Transitivity is proved by a simultaneous induction on the derivations of \( \mathcal{X} \mid \Gamma \vdash a =_\alpha b \text{abt}^n \) and \( \mathcal{X} \mid \Gamma \vdash b =_\alpha c \text{abt}^n \). The most interesting case is when both derivations end with Rule (7.5c). We have \( a = x.a', b = y.b', c = z.c', \) and \( n = m + 1 \) for some \( m \). By the renaming convention we also have

\[
\mathcal{X},u \mid \Gamma,u \text{abt}^{0} \vdash \left[x \mapsto u\right](a') =_\alpha \left[y \mapsto u\right](b') \text{abt}^m
\]

where \( u \notin \mathcal{X} \), and

\[
\mathcal{X},u \mid \Gamma,u \text{abt}^{0} \vdash \left[y \mapsto u\right](b') =_\alpha \left[z \mapsto u\right](c') \text{abt}^m,
\]

where \( u \notin \mathcal{X} \). The result then follows immediately by an application of Rule (7.5c). \( \square \)

7.1.4 Substitution

Substitution is the process of replacing all occurrences (if any) of a free parameter in an abt by another abt in such a way that the scopes of parameters are properly respected. The judgement \( \mathcal{X} \mid \Gamma \vdash [a/x]b = c \text{abt}^n \) is inductively defined by the following rules:

\[
\frac{
\mathcal{X} \mid \Gamma \vdash [a/x]x = a \text{abt}^0
}{\mathcal{X} \mid \Gamma \vdash [a/x]x = a \text{abt}^0}
\]

(7.6a)

\[
\frac{x \neq y}{\mathcal{X},y \mid \Gamma,y \text{abt}^{0} \vdash [a/x]y = y \text{abt}^{0}}
\]

(7.6b)

\[
\frac{
\mathcal{X} \mid \Gamma \vdash [a/x]b_1 = c_1 \text{abt}^{n_1} \ldots \mathcal{X} \mid \Gamma \vdash [a/x]b_k = c_k \text{abt}^{n_k}
}{\mathcal{X} \mid \Gamma \vdash [a/x] o(b_1, \ldots, b_k) = o(c_1, \ldots, c_k) \text{abt}^{0}}
\]

(7.6c)
\[
\begin{align*}
\frac{\mathcal{X}, y \mid \Gamma, y \text{ abt}^0 \vdash [a/x]b = c \text{ abt}^n \quad x \neq y}{\mathcal{X} \mid \Gamma \vdash [a/x](\mathcal{y}) = y \cdot c \text{ abt}^n} 
\end{align*}
\] (7.6d)

In Rule (7.6d) we may assume (by the renaming convention) that \( y \notin \mathcal{X} \), so that if the free parameters of \( a \) are drawn from \( \mathcal{X} \), then \( y \notin a \) abt. This latter condition is called avoidance of capture, for if \( y \in a \) abt, and \( x \in b \) abt, then occurrences of \( y \) in \( c \) would refer improperly to the abstractor \( y \cdot a \), rather than to the surrounding binding site.

The penalty for avoiding capture during substitution is that the result of performing a substitution is only determined up to \( \alpha \)-equivalence. To see this, let us re-state Rule (7.6d) with the use of the renaming convention made explicit:

\[
\begin{align*}
\frac{\mathcal{X}, y' \mid \Gamma, y' \text{ abt}^0 \vdash [a/x][y\rightarrow y']^\dagger(b) = [y\rightarrow y']^\dagger(c) \text{ abt}^n \quad x \neq y' \quad y' \notin \mathcal{X}}{\mathcal{X} \mid \Gamma \vdash [a/x]y \cdot b = y' \cdot [y\rightarrow y']^\dagger(c) \text{ abt}^n} 
\end{align*}
\] (7.7)

Since \( y', [y\rightarrow y']^\dagger(c) \) is \( \alpha \)-equivalent \( y \cdot c \), we see that the result of substitution is determined only up to the names of bound variables.

**Theorem 7.4.** If \( \mathcal{X} \mid \Gamma \vdash a \) abt\(^0\) and \( \mathcal{X}, x \mid \Gamma, x \text{ abt}^0 \vdash b \text{ abt}^n \), then there exists \( \mathcal{X} \mid \Gamma \vdash c \text{ abt}^n \) such that \( \mathcal{X} \mid \Gamma \vdash [a/x]b = c \text{ abt}^n \). If \( \mathcal{X} \mid \Gamma \vdash [a/x]b = c \text{ abt}^n \) and \( \mathcal{X} \mid \Gamma \vdash [a/x]b = c' \text{ abt}^n \), then \( \mathcal{X} \mid \Gamma \vdash c =_\alpha c' \text{ abt}^n \).

**Proof.** The first part is proved by rule induction on \( \mathcal{X} \mid \Gamma, x \text{ abt}^0 \vdash b \text{ abt}^n \), in each case constructing the required derivation of the substitution judgement. The second part is proved by simultaneous rule induction on the two premises, deriving the desired equivalence in each case. \( \square \)

Even though the result is not uniquely determined, we abuse notation and write \( [a/x]b \) for any \( c \) such that \( [a/x]b = c \), with the understanding that \( c \) is determined only up to choice of names of bound parameters.

### 7.2 Exercises

1. Suppose that \texttt{let} is an operator of arity \((0,1)\) and that \texttt{plus} is an operator of arity \((0,0)\). Determine whether or not each of the following
\(\alpha\)-equivalences are valid.

\[
\begin{align*}
\text{let}(x, x.x) &= \alpha \text{let}(x, y.y) \quad (7.8a) \\
\text{let}(y, x.x) &= \alpha \text{let}(y, y.y) \quad (7.8b) \\
\text{let}(x, x.x) &= \alpha \text{let}(y, y.y) \quad (7.8c) \\
\text{let}(x, x.\text{plus}(x, y)) &= \alpha \text{let}(x, z.\text{plus}(z, y)) \quad (7.8d) \\
\text{let}(x, x.\text{plus}(x, y)) &= \alpha \text{let}(x, y.\text{plus}(y, y)) \quad (7.8e)
\end{align*}
\]

2. Prove that apartness respects \(\alpha\)-equivalence.

3. Prove that substitution respects \(\alpha\)-equivalence.
Chapter 8

Parsing

The concrete syntax of a language is concerned with the linear representation of the phrases of a language as strings of symbols—the form in which we write them on paper, type them into a computer, and read them from a page. But languages are also the subjects of study, as well as the instruments of expression. As such the concrete syntax of a language is just a nuisance. When analyzing a language mathematically we are only interested in the deep structure of its phrases, not their surface representation. The abstract syntax of a language exposes the hierarchical and binding structure of the language. Parsing is the process of translation from concrete to abstract syntax. It consists of analyzing the linear representation of a phrase in terms of the grammar of the language and transforming it into an abstract syntax tree or an abstract binding tree that reveals the deep structure of the phrase.

8.1 Parsing Into Abstract Syntax Trees

The process of translation from concrete to abstract syntax is called parsing. We will define parsing as a judgement between the concrete and abstract syntax of $L\{\text{num str}\}$ given in Chapter 6. This judgement will have the mode $(\forall, \exists \leq 1)$, which states that the parser is a partial function of its input, being undefined for ungrammatical token strings, but otherwise uniquely determining the abstract syntax tree representation of each well-formed input.

The parsing judgements for $L\{\text{num str}\}$ follow the unambiguous gram-
These judgements are inductively defined simultaneously by the following rules:

\[
\begin{align*}
\text{num} & \quad \text{nat} \\
\text{NUM}[n] \text{ num} & \leftrightarrow \text{num}[n] \text{ ast} \\
\text{lit} & \quad \text{str} \\
\text{LIT}[s] \text{ lit} & \leftrightarrow \text{str}[s] \text{ ast} \\
\text{id} & \quad \text{str} \\
\text{ID}[s] \text{ id} & \leftrightarrow \text{id}[s] \text{ ast} \\
\text{term} & \quad \text{factor} \\
\text{num} & \leftrightarrow \text{a ast} \\
\text{fct} & \leftrightarrow \text{a ast} \\
\text{fct} & \leftrightarrow \text{a ast} \\
\text{fct} & \leftrightarrow \text{a ast} \\
\text{fct} & \leftrightarrow \text{a ast} \\
\text{prg} & \quad \text{fct} \\
\text{LPs RP fct} & \leftrightarrow \text{a ast} \\
\text{term} & \leftrightarrow \text{a ast} \\
\text{expression} & \leftrightarrow \text{a ast} \\
\end{align*}
\]
8.1 Parsing Into Abstract Syntax Trees

\[
\begin{align*}
\text{s} \, \text{trm} & \quad \rightarrow a \; \text{ast} & \text{s} \, \text{exp} & \quad \rightarrow a \; \text{ast} \\
\text{s} \, \text{ADD} \; \text{s} \, \text{exp} & \quad \rightarrow \text{plus}(a_1; a_2) \; \text{ast} \\
\text{s} \, \text{trm} & \quad \rightarrow a_1 \; \text{ast} & \text{s} \, \text{exp} & \quad \rightarrow a_2 \; \text{ast} \\
\text{s} \, \text{CAT} \; \text{s} \, \text{exp} & \quad \rightarrow \text{cat}(a_1; a_2) \; \text{ast} \\
\text{s} \, \text{exp} & \quad \rightarrow a \; \text{ast} \\
\text{s} \, \text{prg} & \quad \rightarrow a \; \text{ast} \\
\text{s} \, \text{id} & \quad \rightarrow \text{id}[s] \; \text{ast} & \text{s} \, \text{exp} & \quad \rightarrow a_2 \; \text{ast} & \text{s} \, \text{prg} & \quad \rightarrow a_3 \; \text{ast} \\
\text{LET} \; \text{s} \, \text{BE} \; \text{s} \, \text{2 IN} \; \text{s} \, \text{3 prg} & \quad \rightarrow \text{let}[s](a_2; a_3) \; \text{ast}
\end{align*}
\]

(8.1l)

(8.1m)

(8.1n)

(8.1o)

A successful parse implies that the token string must have been derived according to the rules of the unambiguous grammar and that the result is a well-formed abstract syntax tree.

**Theorem 8.1.** If \( s \, \text{prg} \rightarrow a \; \text{ast} \), then \( s \, \text{prg} \) and \( a \; \text{ast} \), and similarly for the other parsing judgements.

**Proof.** By rule induction on Rules (8.1). \( \Box \)

Moreover, if a string is generated according to the rules of the grammar, then it has a parse as an ast.

**Theorem 8.2.** If \( s \, \text{prg} \), then there is a unique \( a \) such that \( s \, \text{prg} \rightarrow a \; \text{ast} \), and similarly for the other parsing judgements. That is, the parsing judgements have mode \((\forall, \exists!)\) over well-formed strings and abstract syntax trees.

**Proof.** By rule induction on the rules determined by reading Grammar (5.5) as an inductive definition. \( \Box \)

Finally, any piece of abstract syntax may be formatted as a string that parses as the given ast.

**Theorem 8.3.** If \( a \; \text{ast} \), then there exists a (not necessarily unique) string \( s \) such that \( s \, \text{prg} \) and \( s \, \text{prg} \rightarrow a \; \text{ast} \). That is, the parsing judgement has mode \((\exists, \forall)\).

**Proof.** By rule induction on Grammar (5.5). \( \Box \)

The string representation of an abstract syntax tree is not unique, since we may introduce parentheses at will around any sub-expression.

**DECEMBER 18, 2009 DRAFT 14:36**
8.2 Parsing Into Abstract Binding Trees

In this section we revise the parser given in Section 8.1 on page 61 to translate from token strings to abstract binding trees to make explicit the binding and scope of identifiers in a program. We will work over the signature given in Chapter 7 defining the abt representation of \( L\{\text{num,str}\} \).

The revised parsing judgement, \( s \text{ prg} \leftrightarrow a \text{ abt} \), between strings \( s \) and abt’s \( a \), is defined by a collection of rules similar to those given in Section 8.1 on page 61. These rules take the form of a generic inductive definition (see Chapter 2) in which the premises and conclusions of the rules involve hypothetical judgments of the form

\[
\text{ID}[s_1] \text{ id} \leftrightarrow x_1 \text{ abt}, \ldots, \text{ID}[s_n] \text{ id} \leftrightarrow x_n \text{ abt} \vdash s \text{ prg} \leftrightarrow a \text{ abt},
\]

where the \( x_i \)'s are pairwise distinct variable names. The hypotheses of the judgement dictate how identifiers are to be parsed as variables, for it follows from the reflexivity of the hypothetical judgement that

\[
\Gamma, \text{ID}[s] \text{ id} \leftrightarrow x \text{ abt} \vdash \text{ID}[s] \text{ id} \leftrightarrow x \text{ abt}.
\]

To maintain the association between identifiers and variables when parsing a \( \text{let} \) expression, we update the hypotheses to record the association between the bound identifier and a corresponding variable:

\[
\Gamma \vdash s_1 \text{ id} \leftrightarrow x \text{ abt} \quad \Gamma \vdash s_2 \text{ exp} \leftrightarrow a_2 \text{ abt} \\
\Gamma, s_1 \text{ id} \leftrightarrow x \text{ abt} \vdash s_3 \text{ prg} \leftrightarrow a_3 \text{ abt} \\
\Gamma \vdash \text{LET} s_1 \text{ BE} s_2 \text{ IN} s_3 \text{ prg} \leftrightarrow \text{let}(a_2;x . a_3) \text{ abt}
\]

(8.2a)

Unfortunately, this approach does not quite work properly! If an inner \( \text{let} \) expression binds the same identifier as an outer \( \text{let} \) expression, there is an ambiguity in how to parse occurrences of that identifier. Parsing such nested \( \text{let} \)'s will introduce two hypotheses, say \( \text{ID}[s] \text{ id} \leftrightarrow x_1 \text{ abt} \) and \( \text{ID}[s] \text{ id} \leftrightarrow x_2 \text{ abt} \), for the same identifier \( \text{ID}[s] \). By the structural property of exchange, we may choose arbitrarily which to apply to any particular occurrence of \( \text{ID}[s] \), and hence we may parse different occurrences differently.

To rectify this we must resort to less elegant methods. Rather than use hypotheses, we instead maintain an explicit symbol table to record the association between identifiers and variables. We must define explicitly the procedures for creating and extending symbol tables, and for looking up an identifier in the symbol table to determine its associated variable. This
8.2 Parsing Into Abstract Binding Trees

8.2 Parsing Into Abstract Binding Trees

gives us the freedom to implement a shadowing policy for re-used identifiers, according to which the most recent binding of an identifier determines the corresponding variable.

The main change to the parsing judgement is that the hypothetical judgement

\[ \Gamma \vdash s \text{ prg } \leftrightarrow a \text{ abt} \]

is reduced to the categorical judgement

\[ s \text{ prg } \leftrightarrow a \text{ abt } [\sigma], \]

where \( \sigma \) is a symbol table. (Analogous changes must be made to the other parsing judgements.) The symbol table is now an argument to the judgement form, rather than an implicit mechanism for performing inference under hypotheses.

The rule for parsing \texttt{let} expressions is then formulated as follows:

\[
\begin{align*}
  s_1 \text{ id } & \leftrightarrow x \ [\sigma] \\
  s_2 \text{ exp } & \leftrightarrow a_2 \text{ abt } [\sigma] \\
  \sigma' = \sigma [s_1 \mapsto x] & \\
  s_3 \text{ prg } & \leftrightarrow a_3 \text{ abt } [\sigma'] \\
\end{align*}
\]

\[ \text{LET} \ s_1 \text{ BE} \ s_2 \text{ IN} \ s_3 \text{ prg } \leftrightarrow \text{let}(a_2; x.a_3) \text{ abt } [\sigma] \quad (8.3) \]

This rule is quite similar to the hypothetical form, the difference being that we must manage the symbol table explicitly. In particular, we must include a rule for parsing identifiers, rather than relying on the reflexivity of the hypothetical judgement to do it for us.

\[
\frac{\sigma(ID[s]) = x}{ID[s] \text{ id } \leftrightarrow x \ [\sigma]} \quad (8.4)
\]

The premise of this rule states that \( \sigma \) maps the identifier \( ID[s] \) to the variable \( x \).

Symbol tables may be defined to be finite sequences of ordered pairs of the form \( (ID[s], x) \), where \( ID[s] \) is an identifier and \( x \) is a variable name. Using this representation it is straightforward to define the following judgement forms:

\[
\begin{align*}
  \sigma \text{ symtab} & \quad \text{well-formed symbol table} \\
  \sigma' = \sigma[ID[s] \mapsto x] & \quad \text{add new association} \\
  \sigma(ID[s]) = x & \quad \text{lookup identifier} \\
\end{align*}
\]

We leave the precise definitions of these judgements as an exercise for the reader.
8.3 Syntactic Conventions

To specify a language we shall use a concise tabular notation for simultaneously specifying both its abstract and concrete syntax. Officially, the language is always a collection of abt’s, but when writing examples we shall often use the concrete notation for the sake of concision and clarity. Our method of specifying the concrete syntax is sufficient for our purposes, but leaves out niggling details such as precedences of operators or the use of bracketing to disambiguate.

The method is best illustrated by example. Here is a specification of the syntax of \( L\{\text{num,str}\} \) presented in the tabular style that we shall use throughout the book:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>( \tau ) ::=</td>
<td>\text{num}</td>
<td>\text{num}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\text{str}</td>
<td>\text{str}</td>
</tr>
<tr>
<td>Expr</td>
<td>( e ) ::=</td>
<td>( x )</td>
<td>( x )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\text{num}[n]</td>
<td>( n )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\text{str}[s]</td>
<td>&quot;s&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\text{plus}(e_1;e_2)</td>
<td>( e_1 + e_2 )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\text{times}(e_1;e_2)</td>
<td>( e_1 \cdot e_2 )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\text{cat}(e_1;e_2)</td>
<td>( e_1 \cdot e_2 )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\text{len}(e)</td>
<td>(</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\text{let}(e_1;x.e_2)</td>
<td>\text{let } x \text{ be } e_1 \text{ in } e_2</td>
</tr>
</tbody>
</table>

This specification is to be understood as defining two judgments, \( \tau \text{ type} \) and \( \tau \text{ exp} \), which specify two syntactic categories, one for types, the other for expressions. The abstract syntax column uses patterns ranging over abt’s to determine the arities of the operators for that syntactic category. The concrete syntax column specifies the typical notational conventions used in examples. In this manner Table (8.3) defines two signatures, \( \Omega_{\text{type}} \) and \( \Omega_{\text{expr}} \), that specify the operators for types and expressions, respectively. The signature for types specifies that \text{num} and \text{str} are two operators of arity () . The signature for expressions specifies two families of operators, \text{num}[n] and \text{str}[s], of arity (), three operators of arity (0, 0) corresponding to addition, multiplication, and concatenation, one operator of arity (0) for length, and one operator of arity (0, 1) for let-binding expressions to identifiers.

8.4 Exercises
Part III

Static and Dynamic Semantics
Chapter 9

Static Semantics

Most programming languages exhibit a phase distinction between the static and dynamic phases of processing. The static phase consists of parsing and type checking to ensure that the program is well-formed; the dynamic phase consists of execution of well-formed programs. A language is said to be safe exactly when well-formed programs are well-behaved when executed.

The static phase is specified by a static semantics comprising a collection of rules for deriving typing judgements stating that an expression is well-formed of a certain type. Types mediate the interaction between the constituent parts of a program by “predicting” some aspects of the execution behavior of the parts so that we may ensure they fit together properly at run-time. Type safety tells us that these predictions are accurate; if not, the static semantics is considered to be improperly defined, and the language is deemed unsafe for execution.

In this chapter we present the static semantics of the language $L\{\text{num str}\}$ as an illustration of the methodology that we shall employ throughout this book.

9.1 Type System
Recall that the abstract syntax of $\mathcal{L}\{\text{num str}\}$ is given by Grammar (8.3), which we repeat here for convenience:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>$\tau$</td>
<td>:= num</td>
<td>num</td>
</tr>
<tr>
<td></td>
<td></td>
<td>:= str</td>
<td>str</td>
</tr>
<tr>
<td>Expr</td>
<td>$e$</td>
<td>:= $x$</td>
<td>$x$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>:= $\text{num}[n]$</td>
<td>$n$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>:= $\text{str}[s]$</td>
<td>&quot;s&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>:= $\text{plus}(e_1; e_2)$</td>
<td>$e_1 + e_2$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>:= $\text{times}(e_1; e_2)$</td>
<td>$e_1 * e_2$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>:= $\text{cat}(e_1; e_2)$</td>
<td>$e_1 ^ e_2$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>:= $\text{len}(e)$</td>
<td>$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>:= $\text{let}(e_1; x.e_2)$</td>
<td>let $x$ be $e_1$ in $e_2$</td>
</tr>
</tbody>
</table>

According to the conventions discussed in Chapter 8, this grammar defines two judgements, $\tau$ type defining the category of types, and $e$ exp defining the category of expressions.

The role of a static semantics is to impose constraints on the formations of phrases that are sensitive to the context in which they occur. For example, whether or not the expression $\text{plus}(x; \text{num}[n])$ is sensible depends on whether or not the variable $x$ is declared to have type num in the surrounding context of the expression. This example is, in fact, illustrative of the general case, in that the only information required about the context of an expression is the type of the variables within whose scope the expression lies. Consequently, the static semantics of $\mathcal{L}\{\text{num str}\}$ consists of an inductive definition of parametric hypothetical judgements of the form

$$\mathcal{X} \mid \Gamma \vdash e : \tau,$$

where $\mathcal{X}$ is a finite set of variables, and $\Gamma$ is a typing context consisting of hypotheses of the form $x : \tau$, one for each $x \in \mathcal{X}$. We rely on typographical conventions to determine the set of parameters, using the letters $x$ and $y$ for variables that serve as parameters of the typing judgement. We write $x \notin \text{dom}(\Gamma)$ to indicate that there is no assumption in $\Gamma$ of the form $x : \tau$ for any type $\tau$, in which case we say that the variable $x$ is fresh for $\Gamma$.

The rules defining the static semantics of $\mathcal{L}\{\text{num str}\}$ are as follows:

$$\Gamma, x : \tau \vdash x : \tau$$  \hspace{1cm} (9.1a)

$$\Gamma \vdash \text{str}[s] : \text{str}$$  \hspace{1cm} (9.1b)
9.1 Type System

\[ \Gamma \vdash \text{num}[n] : \text{num} \quad (9.1c) \]

\[ \Gamma \vdash e_1 : \text{num} \quad \Gamma \vdash e_2 : \text{num} \]
\[ \Gamma \vdash \text{plus}(e_1; e_2) : \text{num} \quad (9.1d) \]

\[ \Gamma \vdash e_1 : \text{num} \quad \Gamma \vdash e_2 : \text{num} \]
\[ \Gamma \vdash \text{times}(e_1; e_2) : \text{num} \quad (9.1e) \]

\[ \Gamma \vdash e_1 : \text{str} \quad \Gamma \vdash e_2 : \text{str} \]
\[ \Gamma \vdash \text{cat}(e_1; e_2) : \text{str} \quad (9.1f) \]

\[ \Gamma \vdash e : \text{str} \]
\[ \Gamma \vdash \text{len}(e) : \text{num} \quad (9.1g) \]

\[ \Gamma \vdash e_1 : \tau_1 \quad \Gamma, x : \tau_1 \vdash e_2 : \tau_2 \]
\[ \Gamma \vdash \text{let}(e_1; x.e_2) : \tau_2 \quad (9.1h) \]

In Rule (9.1h) we tacitly assume that the variable, \( x \), is not already declared in \( \Gamma \). This condition may always be met by choosing a suitable representative of the \( \alpha \)-equivalence class of the \text{let} expression.

Rules (9.1) illustrate an important organizational principle, called the principle of introduction and elimination, for a type system. The constructs of the language may be classified into one of two forms associated with each type. The introductory forms of a type are the means by which values of that type are created, or introduced. In the case of \( L\{	ext{num str}\} \), the introductory forms for the type \text{num} are the numerals, \text{num}[n], and for the type \text{str} are the literals, \text{str}[s]. The eliminatory forms of a type are the means by which we may compute with values of that type to obtain values of some (possibly different) type. In the present case the eliminatory forms for the type \text{num} are addition and multiplication, and for the type \text{str} are concatenation and length. Each eliminatory form has one or more principal arguments of associated type, and zero or more non-principal arguments. In the present case all arguments for each of the eliminatory forms is principal, but we shall later see examples in which there are also non-principal arguments for eliminatory forms.

It is easy to check that every expression has at most one type.

**Lemma 9.1** (Unicity of Typing). For every typing context \( \Gamma \) and expression \( e \), there exists at most one \( \tau \) such that \( \Gamma \vdash e : \tau \).

**Proof.** By rule induction on Rules (9.1). \( \square \)
The typing rules are syntax-directed in the sense that there is exactly one rule for each form of expression. Consequently it is easy to give necessary conditions for typing an expression that invert the sufficient conditions expressed by the corresponding typing rule.

**Lemma 9.2 (Inversion for Typing).** Suppose that \( \Gamma \vdash e : \tau \). If \( e = \text{plus}(e_1; e_2) \), then \( \tau = \text{num} \), \( \Gamma \vdash e_1 : \text{num} \), and \( \Gamma \vdash e_2 : \text{num} \), and similarly for the other constructs of the language.

**Proof.** These may all be proved by induction on the derivation of the typing judgement \( \Gamma \vdash e : \tau \). \( \Box \)

In richer languages such inversion principles are more difficult to state and to prove.

### 9.2 Structural Properties

The static semantics enjoys the structural properties of the parametric hypothetical judgement.

**Lemma 9.3 (Weakening).** If \( \Gamma \vdash e' : \tau' \), then \( \Gamma, x : \tau \vdash e' : \tau' \) for any \( x \notin \text{dom}(\Gamma) \) and any \( \tau \) type.

**Proof.** By induction on the derivation of \( \Gamma \vdash e' : \tau' \). We will give one case here, for rule (9.1h). We have that \( e' = \text{let}(e_1; z \cdot e_2) \), where by the conventions on parameters we may assume \( z \) is chosen such that \( z \notin \text{dom}(\Gamma) \) and \( z \neq x \). By induction we have

1. \( \Gamma, x : \tau \vdash e_1 : \tau_1 \),
2. \( \Gamma, x : \tau, z : \tau_1 \vdash e_2 : \tau' \),

from which the result follows by Rule (9.1h). \( \Box \)

**Lemma 9.4 (Substitution).** If \( \Gamma, x : \tau \vdash e' : \tau' \) and \( \Gamma \vdash e : \tau \), then \( \Gamma \vdash [e/x]e' : \tau' \).

**Proof.** By induction on the derivation of \( \Gamma, x : \tau \vdash e' : \tau' \). We again consider only rule (9.1h). As in the preceding case, \( e' = \text{let}(e_1; z \cdot e_2) \), where \( z \) may be chosen so that \( z \neq x \) and \( z \notin \text{dom}(\Gamma) \). We have by induction
9.2 Structural Properties

1. \( \Gamma \vdash [e/x]e_1 : \tau_1 \),

2. \( \Gamma, z : \tau_1 \vdash [e/x]e_2 : \tau' \).

By the choice of \( z \) we have

\[
[e/x] \text{let}(e_1; z . e_2) = \text{let}(e_1; z . [e/x]e_2).
\]

It follows by Rule (9.1h) that \( \Gamma \vdash [e/x] \text{let}(e_1; z . e_2) : \tau \), as desired. \( \square \)

From a programming point of view, Lemma 9.3 on the preceding page allows us to use an expression in any context that binds its free variables: if \( e \) is well-typed in a context \( \Gamma \), then we may “import” it into any context that includes the assumptions \( \Gamma \). In other words the introduction of new variables beyond those required by an expression, \( e \), does not invalidate \( e \) itself; it remains well-formed, with the same type.\(^1\) More significantly, Lemma 9.4 on the facing page expresses the concepts of modularity and linking. We may think of the expressions \( e \) and \( e' \) as two components of a larger system in which the component \( e' \) is to be thought of as a client of the implementation \( e \). The client declares a variable specifying the type of the implementation, and is type checked knowing only this information. The implementation must be of the specified type in order to satisfy the assumptions of the client. If so, then we may link them to form the composite system, \([e/x]e'\). This may itself be the client of another component, represented by a variable, \( y \), that is replaced by that component during linking. When all such variables have been implemented, the result is a closed expression that is ready for execution (evaluation).

The converse of Lemma 9.4 on the preceding page is called decomposition. It states that any (large) expression may be decomposed into a client and implementor by introducing a variable to mediate their interaction.

**Lemma 9.5 (Decomposition).** If \( \Gamma \vdash [e/x]e' : \tau' \), then for every type \( \tau \) such that \( \Gamma \vdash e : \tau \), we have \( \Gamma, x : \tau \vdash e' : \tau' \).

**Proof.** The typing of \([e/x]e'\) depends only on the type of \( e \) wherever it occurs, if at all. \( \square \)

\(^1\)This may seem so obvious as to be not worthy of mention, but, suprisingly, there are useful type systems that lack this property. Since they do not validate the structural principle of weakening, they are called sub-structural type systems.
This lemma tells us that any sub-expression may be isolated as a separate module of a larger system. This is especially useful when the variable $x$ occurs more than once in $e'$, because then one copy of $e$ suffices for all occurrences of $x$ in $e'$.

9.3 Exercises

1. Show that the expression $e = \text{plus}(\text{num}[7];\text{str}[abc])$ is ill-typed in that there is no $\tau$ such that $e : \tau$. 

Chapter 10

Dynamic Semantics

The \textit{dynamic semantics} of a language specifies how programs are to be executed. One important method for specifying dynamic semantics is called \textit{structural semantics}, which consists of a collection of rules defining a transition system whose states are expressions with no free variables. \textit{Contextual semantics} may be viewed as an alternative presentation of the structural semantics of a language. Another important method for specifying dynamic semantics, called \textit{evaluation semantics}, is the subject of Chapter 12.

10.1 Structural Semantics

A structural semantics for \(\mathcal{L}\{\text{num \ str}\}\) consists of a transition system whose states are closed expressions, all of which are initial states. The final states are the \textit{closed values}, as defined by the following rules:

\[
\text{num}[n] \val \hspace{1cm} (10.1a)
\]

\[
\text{str}[s] \val \hspace{1cm} (10.1b)
\]

The transition judgement, \(e \mapsto e'\), is also inductively defined.

\[
\frac{n_1 + n_2 = n \text{ nat}}{\text{plus(num}[n_1];\text{num}[n_2]) \mapsto \text{num}[n]} \quad (10.2a)
\]

\[
\frac{e_1 \mapsto e'_1}{\text{plus}(e_1;e_2) \mapsto \text{plus}(e'_1;e_2)} \quad (10.2b)
\]
---

**10.1 Structural Semantics**

\[
\begin{align*}
&\text{plus}(e_1; e_2) \leftrightarrow \text{plus}(e_1; e'_2) \\
\Rightarrow\quad &\text{cat}(\text{str}[s_1];\text{str}[s_2]) \leftrightarrow \text{str}[s] \\
\Rightarrow\quad &\text{cat}(e_1; e_2) \leftrightarrow \text{cat}(e'_1; e_2) \\
\Rightarrow\quad &\text{let}(e_1; x. e_2) \leftrightarrow [e_1/x]e_2
\end{align*}
\]

(10.2c)

(10.2d)

(10.2e)

(10.2f)

(10.2g)

We have omitted rules for multiplication and computing the length of a string, which follow a similar pattern. Rules (10.2a), (10.2d), and (10.2g) are *instruction transitions*, since they correspond to the primitive steps of evaluation. The remaining rules are *search transitions* that determine the order in which instructions are executed.

Rules (10.2) exhibit structure arising from the principle of introduction and elimination discussed in Chapter 9. The instruction transitions express the *inversion principle*, which states that *eliminatory forms are inverse to introductory forms*. For example, Rule (10.2a) extracts the natural number from the introductory forms of its arguments, adds these two numbers, and yields the corresponding numeral as result. The search transitions specify that the principal arguments of each eliminatory form are to be evaluated. (When non-principal arguments are present, which is not the case here, there is discretion about whether to evaluate them or not.) This is essential, because it prepares for the instruction transitions, which expect their principal arguments to be introductory forms.

Rule (10.2g) specifies a *by-name* interpretation, in which the bound variable stands for the expression \(e_1\) itself.\(^1\) If \(x\) does not occur in \(e_2\), the expression \(e_1\) is never evaluated. If, on the other hand, it occurs more than once, then \(e_1\) will be re-evaluated at each occurrence. To avoid repeated work in the latter case, we may instead specify a *by-value* interpretation of binding by the following rules:

\[
\begin{align*}
&\text{let}(e_1; x. e_2) \leftrightarrow [e_1/x]e_2
\end{align*}
\]

(10.3a)

\(^1\)The justification for the terminology “by name” is obscure, but as it is very well-established we shall stick with it.

---

\[14:36\]  
\[\text{DRAFT} \quad \text{DECEMBER 18, 2009}\]
10.1 Structural Semantics

\[
\frac{e_1 \mapsto e'_1}{\text{let}(e_1; x \cdot e_2) \mapsto \text{let}(e'_1; x \cdot e_2)} \quad (10.3b)
\]

Rule (10.3b) is an additional search rule specifying that we may evaluate \(e_1\) before \(e_2\). Rule (10.3a) ensures that \(e_2\) is not evaluated until evaluation of \(e_1\) is complete.

A derivation sequence in a structural semantics has a two-dimensional structure, with the number of steps in the sequence being its “width” and the derivation tree for each step being its “height.” For example, consider the following evaluation sequence.

\[
\text{let}(\text{plus}(\text{num}[1]; \text{num}[2]); x \cdot \text{plus}(x; \text{num}[3]); \text{num}[4])) \\
\mapsto \text{let}(\text{num}[3]; x \cdot \text{plus}(x; \text{num}[3]); \text{num}[4])) \\
\mapsto \text{plus}(\text{plus}(\text{num}[3]; \text{num}[3]); \text{num}[4])) \\
\mapsto \text{plus}(\text{num}[6]; \text{num}[4]) \\
\mapsto \text{num}[10]
\]

Each step in this sequence of transitions is justified by a derivation according to Rules (10.2). For example, the third transition in the preceding example is justified by the following derivation:

\[
\frac{\text{plus}(\text{num}[3]; \text{num}[3]) \mapsto \text{num}[6]}{\text{plus}(\text{plus}(\text{num}[3]; \text{num}[3]); \text{num}[4]) \mapsto \text{plus}(\text{num}[6]; \text{num}[4])} \quad (10.2b)
\]

The other steps are similarly justified by a composition of rules.

The principle of rule induction for the structural semantics of \(L\{\text{num str}\}\) states that to show \(P(e \mapsto e')\) whenever \(e \mapsto e'\), it is sufficient to show that \(P\) is closed under Rules (10.2). For example, we may show by rule induction that structural semantics of \(L\{\text{num str}\}\) is determinate.

**Lemma 10.1** (Determinacy). If \(e \mapsto e'\) and \(e \mapsto e''\), then \(e'\) and \(e''\) are \(\alpha\)-equivalent.

\[\text{Proof.}\] By rule induction on the premises \(e \mapsto e'\) and \(e \mapsto e''\), carried out either simultaneously or in either order. Since only one rule applies to each form of expression, \(e\), the result follows directly in each case. \(\Box\)
10.2 Contextual Semantics

A variant of structural semantics, called contextual semantics, is sometimes useful. There is no fundamental difference between the two approaches, only a difference in the style of presentation. The main idea is to isolate instruction steps as a special form of judgement, called instruction transition, and to formalize the process of locating the next instruction using a device called an evaluation context. The judgement, $e\text{val}$, defining whether an expression is a value, remains unchanged.

The instruction transition judgement, $e_1 \rightsquigarrow e_2$, for $\mathcal{L}\{\text{num, str}\}$ is defined by the following rules, together with similar rules for multiplication of numbers and the length of a string.

$$m + n = p \text{ nat}$$
$$\frac{\text{plus}(\text{num}[m]; \text{num}[n]) \rightsquigarrow \text{num}[p]}{(10.4a)}$$

$$s^l = u \text{ str}$$
$$\frac{\text{cat}(\text{str}[s]; \text{str}[l]) \rightsquigarrow \text{str}[u]}{(10.4b)}$$

$$\text{let}(e_1; x. e_2) \rightsquigarrow [e_1/x]e_2$$
$$\frac{}{(10.4c)}$$

The judgement $E\text{ectxt}$ determines the location of the next instruction to execute in a larger expression. The position of the next instruction step is specified by a “hole”, written $\circ$, into which the next instruction is placed, as we shall detail shortly. (The rules for multiplication and length are omitted for concision, as they are handled similarly.)

$$\frac{}{(10.5a)}$$

$$\frac{E_1\text{ectxt}}{\text{plus}(E_1; e_2)\text{ectxt}}$$
$$\frac{}{(10.5b)}$$

$$\frac{e_1\text{val} \ E_2\text{ectxt}}{\text{plus}(e_1; E_2)\text{ectxt}}$$
$$\frac{}{(10.5c)}$$

The first rule for evaluation contexts specifies that the next instruction may occur “here”, at the point of the occurrence of the hole. The remaining rules correspond one-for-one to the search rules of the structural semantics. For example, Rule (10.5c) states that in an expression $\text{plus}(e_1; e_2)$, if the first principal argument, $e_1$, is a value, then the next instruction step, if any, lies at or within the second principal argument, $e_2$. 
10.2 Contextual Semantics

An evaluation context is to be thought of as a template that is instantiated by replacing the hole with an instruction to be executed. The judgement \( e' = \mathcal{E}\{e\} \) states that the expression \( e' \) is the result of filling the hole in the evaluation context \( \mathcal{E} \) with the expression \( e \). It is inductively defined by the following rules:

\[
\begin{align*}
  e &= \circ\{e\} \\
  e_1 &= \mathcal{E}_1\{e\} \\
  \text{plus}(e_1; e_2) &= \text{plus}(\mathcal{E}_1; e_2)\{e\} \\
  e_1 \text{ val } e_2 &= \mathcal{E}_2\{e\} \\
  \text{plus}(e_1; e_2) &= \text{plus}(e_1; \mathcal{E}_2)\{e\}
\end{align*}
\]

(10.6a) (10.6b) (10.6c)

There is one rule for each form of evaluation context. Filling the hole with \( e \) results in \( e' \); otherwise we proceed inductively over the structure of the evaluation context.

Finally, the dynamic semantics for \( \mathcal{L}\{\text{num \ str}\} \) is defined using contextual semantics by a single rule:

\[
\begin{align*}
  e &= \mathcal{E}\{e_0\} \\
  e_0 \rightsquigarrow e'_0 \\
  e' &= \mathcal{E}\{e'_0\}
\end{align*}
\]

(10.7)

Thus, a transition from \( e \) to \( e' \) consists of (1) decomposing \( e \) into an evaluation context and an instruction, (2) execution of that instruction, and (3) replacing the instruction by the result of its execution in the same spot within \( e \) to obtain \( e' \).

The structural and contextual semantics define the same transition relation. For the sake of the proof, let us write \( e \rightsquigarrow_s e' \) for the transition relation defined by the structural semantics (Rules (10.2)), and \( e \rightsquigarrow_c e' \) for the transition relation defined by the contextual semantics (Rules (10.7)).

**Theorem 10.2.** \( e \rightsquigarrow_s e' \) if, and only if, \( e \rightsquigarrow_c e' \).

**Proof.** From left to right, proceed by rule induction on Rules (10.2). It is enough in each case to exhibit an evaluation context \( \mathcal{E} \) such that \( e = \mathcal{E}\{e_0\} \), \( e' = \mathcal{E}\{e'_0\} \), and \( e_0 \rightsquigarrow e'_0 \). For example, for Rule (10.2a), take \( \mathcal{E} = \circ \), and observe that \( e \rightsquigarrow e' \). For Rule (10.2b), we have by induction that there exists an evaluation context \( \mathcal{E}_1 \) such that \( e_1 = \mathcal{E}_1\{e_0\} \), \( e'_1 = \mathcal{E}_1\{e'_0\} \), and \( e_0 \rightsquigarrow e'_0 \). Take \( \mathcal{E} = \text{plus}(\mathcal{E}_1; e_2) \), and observe that \( e = \text{plus}(\mathcal{E}_1; e_2)\{e_0\} \) and \( e' = \text{plus}(\mathcal{E}_1; e_2)\{e'_0\} \) with \( e_0 \rightsquigarrow e'_0 \).
From right to left, observe that if $e \rightarrow_c e'$, then there exists an evaluation context $E$ such that $e = E\{e_0\}$, $e' = E\{e'_0\}$, and $e_0 \leadsto e'_0$. We prove by induction on Rules (10.6) that $e \rightarrow_s e'$. For example, for Rule (10.6a), $e_0$ is $e$, $e'_0$ is $e'$, and $e \leadsto e'$. Hence $e \rightarrow_s e'$. For Rule (10.6b), we have that $E = \text{plus}(E_1; e_2), e_1 = E_1\{e_0\}, e'_1 = E_1\{e'_0\}$, and $e_1 \rightarrow_s e'_1$. Therefore $e$ is $\text{plus}(e_1; e_2), e'$ is $\text{plus}(e'_1; e_2)$, and therefore by Rule (10.2b), $e \rightarrow_s e'$.

Since the two transition judgements coincide, contextual semantics may be seen as an alternative way of presenting a structural semantics. It has two advantages over structural semantics, one relatively superficial, one rather less so. The superficial advantage stems from writing Rule (10.7) in the simpler form

$$\begin{align*}
e_0 \leadsto e'_0 \\
E\{e_0\} \rightarrow E\{e'_0\}.
\end{align*}$$

This formulation is simpler insofar as it leaves implicit the definition of the decomposition of the left- and right-hand sides. The deeper advantage, which we will exploit in Chapter 15, is that the transition judgement in contextual semantics applies only to closed expressions of a fixed type, whereas structural semantics transitions are necessarily defined over expressions of every type.

### 10.3 Equational Semantics

Another formulation of the dynamic semantics of a language is based on regarding computation as a form of equational deduction, much in the style of elementary algebra. For example, in algebra we may show that the polynomials $x^2 + 2x + 1$ and $(x + 1)^2$ are equivalent by a simple process of calculation and re-organization using the familiar laws of addition and multiplication. The same laws are sufficient to determine the value of any polynomial, given the values of its variables. So, for example, we may plug in 2 for $x$ in the polynomial $x^2 + 2x + 1$ and calculate that $2^2 + 2\times1 = 9$, which is indeed $(2 + 1)^2$. This gives rise to a model of computation in which we may determine the value of a polynomial for a given value of its variable by substituting the given value for the variable and proving that the resulting expression is equal to its value.

Very similar ideas give rise to the concept of definitional, or computational, equivalence of expressions in $\mathcal{L}\{\text{num str}\}$, which we write as $\mathcal{X} \mid \Gamma \vdash e \equiv e' : \tau$, where $\Gamma$ consists of one assumption of the form $x : \tau$ for each
x ∈ X. We only consider definitional equality of well-typed expressions, so that when considering the judgement Γ ⊢ e ≡ e’ : τ, we tacitly assume that Γ ⊢ e : τ and Γ ⊢ e’ : τ. Here, as usual, we omit explicit mention of the parameters, X, when they can be determined from the forms of the assumptions Γ.

Definitional equivalence of expressions in L{num str} is inductively defined by the following rules:

\[
\begin{align*}
\Gamma &\vdash e \equiv e : \tau \\
\Gamma &\vdash e' \equiv e : \tau \\
\Gamma &\vdash e \equiv e' : \tau
\end{align*}
\]

(10.9a)

(10.9b)

(10.9c)

\[
\begin{align*}
\Gamma &\vdash e_1 \equiv e'_1 : \text{num} \quad \Gamma &\vdash e_2 \equiv e'_2 : \text{num} \\
&\quad \text{Γ}\vdash \text{plus}(e_1; e_2) \equiv \text{plus}(e'_1; e'_2) : \text{num}
\end{align*}
\]

(10.9d)

\[
\begin{align*}
\Gamma &\vdash e_1 \equiv e'_1 : \text{str} \quad \Gamma &\vdash e_2 \equiv e'_2 : \text{str} \\
&\quad \text{Γ}\vdash \text{cat}(e_1; e_2) \equiv \text{cat}(e'_1; e'_2) : \text{str}
\end{align*}
\]

(10.9e)

\[
\begin{align*}
\Gamma &\vdash e_1 \equiv e'_1 : \tau_1 \quad \Gamma &\vdash x : \tau_1 \vdash e_2 \equiv e'_2 : \tau_2 \\
&\quad \text{Γ}\vdash \text{let}(e_1; x. e_2) \equiv \text{let}(e'_1; x. e'_2) : \tau_2
\end{align*}
\]

(10.9f)

\[
\begin{align*}
&\quad n_1 + n_2 = n \text{ nat} \\
\Gamma &\vdash \text{plus}(\text{num}[n_1]; \text{num}[n_2]) \equiv \text{num}[n] : \text{num}
\end{align*}
\]

(10.9g)

\[
\begin{align*}
&\quad s_1 \cdot s_2 = s \text{ str} \\
\Gamma &\vdash \text{cat}(\text{str}[s_1]; \text{str}[s_2]) \equiv \text{str}[s] : \text{str}
\end{align*}
\]

(10.9h)

\[
\begin{align*}
\Gamma &\vdash \text{let}(e_1; x. e_2) \equiv [e_1/x]e_2 : \tau
\end{align*}
\]

(10.9i)

Rules (10.9a) through (10.9c) state that definitional equivalence is an equivalence relation. Rules (10.9d) through (10.9f) state that it is a congruence relation, which means that it is compatible with all expression-forming constructs in the language. Rules (10.9g) through (10.9i) specify the meanings of the primitive constructs of L{num str}. For the sake of conciseness, Rules (10.9) may be characterized as defining the strongest congruence closed under Rules (10.9g), (10.9h), and (10.9i).
10.3 Equational Semantics

Rules (10.9) are sufficient to allow us to calculate the value of an expression by an equational deduction similar to that used in high school algebra. For example, we may derive the equation

\[
\text{let } x \equiv 1 + 2 \text{ in } x + 3 + 4 \equiv 10 : \text{num}
\]

by applying Rules (10.9). Here, as in general, there may be many different ways to derive the same equation, but we need find only one derivation in order to carry out an evaluation.

Definitional equivalence is rather weak in that many equivalences that one might intuitively think are true are not derivable from Rules (10.9). A prototypical example is the putative equivalence

\[
x : \text{num}, y : \text{num} \vdash x_1 + x_2 \equiv x_2 + x_1 : \text{num}, (10.10)
\]

which, intuitively, expresses the commutativity of addition. Although we shall not prove this here, this equivalence is not derivable from Rules (10.9). And yet we may derive all of its closed instances,

\[
n_1 + n_2 \equiv n_2 + n_1 : \text{num}, \quad (10.11)
\]

where \(n_1\) nat and \(n_2\) nat are particular numbers.

The “gap” between a general law, such as Equation (10.10), and all of its instances, given by Equation (10.11), may be filled by enriching the notion of equivalence to include a principle of proof by mathematical induction. Such a notion of equivalence is sometimes called \textit{semantic}, or \textit{observational}, equivalence, since it expresses relationships that hold by virtue of the semantics of the expressions involved.\(^2\) Semantic equivalence is a \textit{synthetic judgement}, one that requires proof. It is to be distinguished from definitional equivalence, which expresses an \textit{analytic judgement}, one that is self-evident based solely on the dynamic semantics of the operations involved. As such definitional equivalence may be thought of as \textit{symbolic evaluation}, which permits simplification according to the evaluation rules of a language, but which does not permit reasoning by induction.

Definitional equivalence is adequate for evaluation in that it permits the calculation of the value of any closed expression.

\textbf{Theorem 10.3.} \(e \equiv e' : \tau\) iff there exists \(e_0\) \textit{val} such that \(e \mapsto^* e_0\) and \(e' \mapsto^* e_0\).

\(^2\)This rather vague concept of equivalence is developed rigorously in Chapter 48.
Proof. The proof from right to left is direct, since every transition step is a valid equation. The converse follows from the following, more general, proposition. If \( x_1 : \tau_1, \ldots, x_n : \tau_n \vdash e \equiv e' : \tau \), then whenever \( e_1 : \tau_1, \ldots, e_n : \tau_n \), if

\[
[e_1, \ldots, e_n / x_1, \ldots, x_n]e \equiv [e_1, \ldots, e_n / x_1, \ldots, x_n]e' : \tau,
\]

then there exists \( e_0 \text{ val} \) such that

\[
[e_1, \ldots, e_n / x_1, \ldots, x_n]e \mapsto^* e_0
\]

and

\[
[e_1, \ldots, e_n / x_1, \ldots, x_n]e' \mapsto^* e_0.
\]

This is proved by rule induction on Rules (10.9).

The formulation of definitional equivalence for the by-value semantics of binding requires a bit of additional machinery. The key idea is motivated by the modifications required to Rule (10.9i) to express the requirement that \( e_1 \) be a value. As a first cut one might consider simply adding an additional premise to the rule:

\[
\frac{e_1 \text{ val}}{\Gamma \vdash \text{let}(e_1; x.e_2) \equiv [e_1/x]e_2 : \tau} \quad (10.12)
\]

This is almost correct, except that the judgement \( e \text{ val} \) is defined only for closed expressions, whereas \( e_1 \) might well involve free variables in \( \Gamma \). What is required is to extend the judgement \( e \text{ val} \) to the hypothetical judgement

\[
x_1 \text{ val}, \ldots, x_n \text{ val} \vdash e \text{ val}
\]

in which the hypotheses express the assumption that variables are only ever bound to values, and hence can be regarded as values. To maintain this invariant, we must maintain a set, \( \Xi \), of such hypotheses as part of definitional equivalence, writing \( \Xi \Gamma \vdash e \equiv e' : \tau \), and modifying Rule (10.9f) as follows:

\[
\frac{\Xi \Gamma \vdash e_1 \equiv e'_1 : \tau_1 \quad \Xi, x \text{ val} \Gamma, x : \tau_1 \vdash e_2 \equiv e'_2 : \tau_2}{\Xi \Gamma \vdash \text{let}(e_1; x.e_2) \equiv \text{let}(e'_1; x.e'_2) : \tau_2} \quad (10.13)
\]

The other rules are correspondingly modified to simply carry along \( \Xi \) is an additional set of hypotheses of the inference.
10.4 Exercises

1. For the structural operational semantics of $\mathcal{L}\{\text{num str}\}$, prove that if $e \mapsto e_1$ and $e \mapsto e_2$, then $e_1 =_a e_2$.

2. Formulate a variation of $\mathcal{L}\{\text{num str}\}$ with both a by-name and a by-value let construct.
Chapter 11

Type Safety

Most contemporary programming languages are safe (or, type safe, or strongly typed). Informally, this means that certain kinds of mismatches cannot arise during execution. For example, type safety for \( L\{\text{num str}\} \) states that it will never arise that a number is to be added to a string, or that two numbers are to be concatenated, neither of which is meaningful.

In general type safety expresses the coherence between the static and the dynamic semantics. The static semantics may be seen as predicting that the value of an expression will have a certain form so that the dynamic semantics of that expression is well-defined. Consequently, evaluation cannot “get stuck” in a state for which no transition is possible, corresponding in implementation terms to the absence of “illegal instruction” errors at execution time. This is proved by showing that each step of transition preserves typability and by showing that typable states are well-defined. Consequently, evaluation can never “go off into the weeds,” and hence can never encounter an illegal instruction.

More precisely, type safety for \( L\{\text{num str}\} \) may be stated as follows:

**Theorem 11.1** (Type Safety).

1. If \( e : \tau \) and \( e \rightarrow e' \), then \( e' : \tau \).

2. If \( e : \tau \), then either \( e \text{ val} \), or there exists \( e' \) such that \( e \rightarrow e' \).

The first part, called preservation, says that the steps of evaluation preserve typing; the second, called progress, ensures that well-typed expressions are either values or can be further evaluated. Safety is the conjunction of preservation and progress.

We say that an expression, \( e \), is stuck iff it is not a value, yet there is no \( e' \) such that \( e \rightarrow e' \). It follows from the safety theorem that a stuck state is
necessarily ill-typed. Or, putting it the other way around, that well-typed states do not get stuck.

11.1 Preservation

The preservation theorem for \( L\{\text{num \ str}\} \) defined in Chapters 9 and 10 is proved by rule induction on the transition system (rules (10.2)).

**Theorem 11.2** (Preservation). If \( e : \tau \) and \( e \rightarrow e' \), then \( e' : \tau \).

**Proof.** We will consider two cases, leaving the rest to the reader. Consider rule (10.2b),

\[
\frac{e_1 \rightarrow e'_1}{\text{plus}(e_1; e_2) \rightarrow \text{plus}(e'_1; e_2)}.
\]

Assume that \( \text{plus}(e_1; e_2) : \tau \). By inversion for typing, we have that \( \tau = \text{num} \), \( e_1 : \text{num} \), and \( e_2 : \text{num} \). By induction we have that \( e'_1 : \text{num} \), and hence \( \text{plus}(e'_1; e_2) : \text{num} \). The case for concatenation is handled similarly.

Now consider rule (10.2g),

\[
\frac{e_1 \text{ val}}{\text{let}(e_1; x . e_2) \rightarrow [e_1/x]e_2}.
\]

Assume that \( \text{let}(e_1; x . e_2) : \tau_2 \). By the inversion lemma 9.2 on page 72, \( e_1 : \tau_1 \) for some \( \tau_1 \) such that \( x : \tau_1 \vdash e_2 : \tau_2 \). By the substitution lemma 9.4 on page 72 \( [e_1/x]e_2 : \tau_2 \), as desired. \( \square \)

The proof of preservation is naturally structured as an induction on the transition judgement, since the argument hinges on examining all possible transitions from a given expression. In some cases one may manage to carry out a proof by structural induction on \( e \), or by an induction on typing, but experience shows that this often leads to awkward arguments, or, in some cases, cannot be made to work at all.

11.2 Progress

The progress theorem captures the idea that well-typed programs cannot “get stuck”. The proof depends crucially on the following lemma, which characterizes the values of each type.

**Lemma 11.3** (Canonical Forms). If \( e \text{ val} \) and \( e : \tau \), then
11.2 Progress

1. If $\tau = \text{num}$, then $e = \text{num}[n]$ for some number $n$.

2. If $\tau = \text{str}$, then $e = \text{str}[s]$ for some string $s$.

Proof. By induction on rules (9.1) and (10.1).

Progress is proved by rule induction on rules (9.1) defining the static semantics of the language.

**Theorem 11.4 (Progress).** *If $e : \tau$, then either $e \text{ val}$, or there exists $e'$ such that $e \rightarrow e'$.*

Proof. The proof proceeds by induction on the typing derivation. We will consider only one case, for rule (9.1d),

$$\begin{align*}
ed_1 : \text{num} & \quad ed_2 : \text{num} \\
\text{plus}(ed_1; ed_2) & : \text{num} 
\end{align*}$$

where the context is empty because we are considering only closed terms.

By induction we have that either $ed_1 \text{ val}$, or there exists $ed'_1$ such that $ed_1 \rightarrow ed'_1$. In the latter case it follows that $\text{plus}(ed_1; ed_2) \rightarrow \text{plus}(ed'_1; ed_2)$, as required. In the former we also have by induction that either $ed_2 \text{ val}$, or there exists $ed'_2$ such that $ed_2 \rightarrow ed'_2$. In the latter case we have that $\text{plus}(ed_1; ed_2) \rightarrow \text{plus}(ed_1; ed'_2)$, as required. In the former, we have, by the Canonical Forms Lemma 11.3 on the facing page, $ed_1 = \text{num}[n_1]$ and $ed_2 = \text{num}[n_2]$, and hence

$$\text{plus}(\text{num}[n_1]; \text{num}[n_2]) \rightarrow \text{num}[n_1 + n_2].$$

Since the typing rules for expressions are syntax-directed, the progress theorem could equally well be proved by induction on the structure of $e$, appealing to the inversion theorem at each step to characterize the types of the parts of $e$. But this approach breaks down when the typing rules are not syntax-directed, that is, when there may be more than one rule for a given expression form. No difficulty arises if the proof proceeds by induction on the typing rules.

Summing up, the combination of preservation and progress together constitute the proof of safety. The progress theorem ensures that well-typed expressions do not “get stuck” in an ill-defined state, and the preservation theorem ensures that if a step is taken, the result remains well-typed (with the same type). Thus the two parts work hand-in-hand to ensure that the static and dynamic semantics are coherent, and that no ill-defined states can ever be encountered while evaluating a well-typed expression.
11.3 Run-Time Errors

Suppose that we wish to extend \( \mathcal{L}\{\text{num,str}\} \) with, say, a quotient operation that is undefined for a zero divisor. The natural typing rule for quotients is given by the following rule:

\[
\frac{e_1 : \text{num} \quad e_2 : \text{num}}{\text{div}(e_1; e_2) : \text{num}}.
\]

But the expression \( \text{div}(\text{num}[3]; \text{num}[0]) \) is well-typed, yet stuck! We have two options to correct this situation:

1. Enhance the type system, so that no well-typed program may divide by zero.
2. Add dynamic checks, so that division by zero signals an error as the outcome of evaluation.

Either option is, in principle, viable, but the most common approach is the second. The first requires that the type checker prove that an expression be non-zero before permitting it to be used in the denominator of a quotient. It is difficult to do this without ruling out too many programs as ill-formed. This is because one cannot reliably predict statically whether an expression will turn out to be non-zero when executed (because this is an undecidable property). We therefore consider the second approach, which is typical of current practice.

The general idea is to distinguish checked from unchecked errors. An unchecked error is one that is ruled out by the type system. No run-time checking is performed to ensure that such an error does not occur, because the type system rules out the possibility of it arising. For example, the dynamic semantics need not check, when performing an addition, that its two arguments are, in fact, numbers, as opposed to strings, because the type system ensures that this is the case. On the other hand the dynamic semantics for quotient must check for a zero divisor, because the type system does not rule out the possibility.

One approach to modelling checked errors is to give an inductive definition of the judgment \( e \ err \) stating that the expression \( e \) incurs a checked run-time error, such as division by zero. Here are some representative rules that would appear in a full inductive definition of this judgement:

\[
\frac{e_1 \ \text{val}}{\text{div}(e_1; \text{num}[0]) \ err} \quad (11.1a)
\]
11.3 Run-Time Errors

\[
\frac{e_1 \text{ err}}{\text{plus}(e_1; e_2) \text{ err}} \quad (11.1b)
\]

\[
\frac{e_1 \text{ val} \quad e_2 \text{ err}}{\text{plus}(e_1; e_2) \text{ err}} \quad (11.1c)
\]

Rule (11.1a) signals an error condition for division by zero. The other rules propagate this error upwards: if an evaluated sub-expression is a checked error, then so is the overall expression.

The preservation theorem is not affected by the presence of checked errors. However, the statement (and proof) of progress is modified to account for checked errors.

**Theorem 11.5 (Progress With Error).** If \( e : \tau \), then either \( e \text{ err} \), or \( e \text{ val} \), or there exists \( e' \) such that \( e \mapsto e' \).

**Proof.** The proof is by induction on typing, and proceeds similarly to the proof given earlier, except that there are now three cases to consider at each point in the proof.

A disadvantage of this approach to the formalization of error checking is that it appears to require a special set of evaluation rules to check for errors. An alternative is to fold in error checking with evaluation by enriching the language with a special error expression, \( \text{error} \), which signals that an error has arisen. Since an error condition aborts the computation, the static semantics assigns an arbitrary type to \( \text{error} \):

\[
\text{error} : \tau \quad (11.2)
\]

This rule destroys the unicity of typing property (Lemma 9.1 on page 71). This can be restored by introducing a special error expression for each type, but we shall not do so here for the sake of simplicity.

The dynamic semantics is augmented with rules that provoke a checked error (such as division by zero), plus rules that propagate the error through other language constructs.

\[
\frac{e_1 \text{ val}}{\text{div}(e_1; \text{num}[0]) \mapsto \text{error}} \quad (11.3a)
\]

\[
\frac{\text{plus}(\text{error}; e_2) \mapsto \text{error}}{} \quad (11.3b)
\]
\( \frac{e_1 \text{ val}}{\text{plus}(e_1; \text{error}) \rightarrow \text{error}} \) \hspace{1cm} (11.3c)

There are similar error propagation rules for the other constructs of the language. By defining \( e \ err \) to hold exactly when \( e = \text{error} \), the revised progress theorem continues to hold for this variant semantics.

## 11.4 Exercises

1. Complete the proof of preservation.

2. Complete the proof of progress.
Chapter 12

Evaluation Semantics

In Chapter 10 we defined the dynamic semantics of \( L\{\text{num str}\} \) using the method of structural semantics. This approach is useful as a foundation for proving properties of a language, but other methods are often more appropriate for other purposes, such as writing user manuals. Another method, called evaluation semantics, or ES, presents the dynamic semantics as a relation between a phrase and its value, without detailing how it is to be determined in a step-by-step manner. Two variants of evaluation semantics are also considered, namely environment semantics, which delays substitution, and cost semantics, which records the number of steps that are required to evaluate an expression.

12.1 Evaluation Semantics

Another method for defining the dynamic semantics of \( L\{\text{num str}\} \), called evaluation semantics, consists of an inductive definition of the evaluation judgement, \( e \downarrow v \), stating that the closed expression, \( e \), evaluates to the value, \( v \).

\[
\begin{align*}
\text{num}[n] & \downarrow \text{num}[n] \quad (12.1a) \\
\text{str}[s] & \downarrow \text{str}[s] \quad (12.1b) \\
\end{align*}
\]

\[
\begin{align*}
\frac{e_1 \downarrow \text{num}[n_1] \quad e_2 \downarrow \text{num}[n_2] \quad n_1 + n_2 = n \text{ nat}}{\text{plus}(e_1; e_2) \downarrow \text{num}[n]} \quad (12.1c) \\
\frac{e_1 \downarrow \text{str}[s_1] \quad e_2 \downarrow \text{str}[s_2] \quad s_1 \hat{s}_2 = s \text{ str}}{\text{cat}(e_1; e_2) \downarrow \text{str}[s]} \quad (12.1d)
\end{align*}
\]
12.2 Relating Transition and Evaluation Semantics

The value of a let expression is determined by substitution of the binding into the body. The rules are therefore not syntax-directed, since the premise of Rule (12.1f) is not a sub-expression of the expression in the conclusion of that rule.

The evaluation judgement is inductively defined, we prove properties of it by rule induction. Specifically, to show that the property \( P(e \Downarrow v) \) holds, it is enough to show that \( P \) is closed under Rules (12.1):

1. Show that \( P(\text{num}[n] \Downarrow \text{num}[n]) \).
2. Show that \( P(\text{str}[s] \Downarrow \text{str}[s]) \).
3. Show that \( P(\text{plus}(e_1; e_2) \Downarrow \text{num}[n]), \) if \( P(e_1 \Downarrow \text{num}[n_1]), P(e_2 \Downarrow \text{num}[n_2]), \) and \( n_1 + n_2 = n \text{ nat} \).
4. Show that \( P(\text{cat}(e_1; e_2) \Downarrow \text{str}[s]), \) if \( P(e_1 \Downarrow \text{str}[s_1]), P(e_2 \Downarrow \text{str}[s_2]), \) and \( s_1 \cdot s_2 = s \text{ str} \).
5. Show that \( P(\text{let}(e_1; x.e_2) \Downarrow v_2), \) if \( P([e_1/x]e_2 \Downarrow v_2) \).

This induction principle is not the same as structural induction on \( e \text{ exp} \), because the evaluation rules are not syntax-directed!

**Lemma 12.1.** If \( e \Downarrow v \), then \( v \text{ val} \).

**Proof.** By induction on Rules (12.1). All cases except Rule (12.1f) are immediate. For the latter case, the result follows directly by an appeal to the inductive hypothesis for the second premise of the evaluation rule.

12.2 Relating Transition and Evaluation Semantics

We have given two different forms of dynamic semantics for \( L\{\text{num str}\} \). It is natural to ask whether they are equivalent, but to do so first requires that we consider carefully what we mean by equivalence. The transition
12.2 Relating Transition and Evaluation Semantics

Semantics describes a step-by-step process of execution, whereas the evaluation semantics suppresses the intermediate states, focusing attention on the initial and final states alone. This suggests that the appropriate correspondence is between complete execution sequences in the transition semantics and the evaluation judgement in the evaluation semantics. (We will consider only numeric expressions, but analogous results hold also for string-valued expressions.)

**Theorem 12.2.** For all closed expressions $e$ and values $v$, $e \mapsto^* v$ iff $e \downarrow v$.

How might we prove such a theorem? We will consider each direction separately. We consider the easier case first.

**Lemma 12.3.** If $e \downarrow v$, then $e \mapsto^* v$.

*Proof.* By induction on the definition of the evaluation judgement. For example, suppose that $\text{plus}(e_1; e_2) \downarrow \text{num}[n]$ by the rule for evaluating additions. By induction we know that $e_1 \mapsto^* \text{num}[n_1]$ and $e_2 \mapsto^* \text{num}[n_2]$. We reason as follows:

\[
\begin{align*}
\text{plus}(e_1; e_2) & \mapsto^* \text{plus}(\text{num}[n_1]; e_2) \\
& \mapsto^* \text{plus}(\text{num}[n_1]; \text{num}[n_2]) \\
& \mapsto \text{num}[n_1 + n_2]
\end{align*}
\]

Therefore $\text{plus}(e_1; e_2) \mapsto^* \text{num}[n_1 + n_2]$, as required. The other cases are handled similarly. \[\square\]

For the converse, recall from Chapter 4 the definitions of multi-step evaluation and complete evaluation. Since $v \downarrow v$ whenever $v$ val, it suffices to show that evaluation is closed under reverse execution.

**Lemma 12.4.** If $e \mapsto e'$ and $e' \downarrow v$, then $e \downarrow v$.

*Proof.* By induction on the definition of the transition judgement. For example, suppose that $\text{plus}(e_1; e_2) \mapsto \text{plus}(e'_1; e_2)$, where $e_1 \mapsto e'_1$. Suppose further that $\text{plus}(e'_1; e_2) \downarrow v$, so that $e'_1 \downarrow \text{num}[n_1]$, $e_2 \downarrow \text{num}[n_2]$, $n_1 + n_2 = n \text{ nat}$, and $v$ is $\text{num}[n]$. By induction $e_1 \downarrow \text{num}[n_1]$, and hence $\text{plus}(e_1; e_2) \downarrow \text{num}[n]$, as required. \[\square\]
12.3 Type Safety, Revisited

The type safety theorem for $L\{\text{num \ str}\}$ (Theorem 11.1 on page 85) states that a language is safe iff it satisfies both preservation and progress. This formulation depends critically on the use of a transition system to specify the dynamic semantics. But what if we had instead specified the dynamic semantics as an evaluation relation, instead of using a transition system? Can we state and prove safety in such a setting?

The answer, unfortunately, is that we cannot. While there is an analogue of the preservation property for an evaluation semantics, there is no clear analogue of the progress property. Preservation may be stated as saying that if $e \Downarrow v$ and $e : \tau$, then $v : \tau$. This can be readily proved by induction on the evaluation rules. But what is the analogue of progress? One might be tempted to phrase progress as saying that if $e : \tau$, then $e \Downarrow v$ for some $v$. While this property is true for $L\{\text{num \ str}\}$, it demands much more than just progress — it requires that every expression evaluate to a value! If $L\{\text{num \ str}\}$ were extended to admit operations that may result in an error (as discussed in Section 11.3 on page 88), or to admit non-terminating expressions, then this property would fail, even though progress would remain valid.

One possible attitude towards this situation is to simply conclude that type safety cannot be properly discussed in the context of an evaluation semantics, but only by reference to a transition semantics. Another point of view is to instrument the semantics with explicit checks for run-time type errors, and to show that any expression with a type fault must be ill-typed. Re-stated in the contrapositive, this means that a well-typed program cannot incur a type error. A difficulty with this point of view is that one must explicitly account for a class of errors solely to prove that they cannot arise! Nevertheless, we will press on to show how a semblance of type safety can be established using evaluation semantics.

The main idea is to define a judgement $e \Uparrow$ stating, in the jargon of the literature, that the expression $e$ goes wrong when executed. The exact definition of “going wrong” is given by a set of rules, but the intention is that it should cover all situations that correspond to type errors. The following rules are representative of the general case:

\begin{align*}
\frac{}{\text{plus}(\text{str}[s]; e_2) \Uparrow} & \quad (12.2a) \\
\frac{e_1 \text{ val}}{\text{plus}(e_1; \text{str}[s]) \Uparrow} & \quad (12.2b)
\end{align*}
These rules explicitly check for the misapplication of addition to a string; similar rules govern each of the primitive constructs of the language.

**Theorem 12.5.** If $e \upharpoonright$, then there is no $\tau$ such that $e : \tau$.

**Proof.** By rule induction on Rules (12.2). For example, for Rule (12.2a), we observe that $\text{str}[s] : \text{str}$, and hence $\text{plus}(\text{str}[s]; e_2)$ is ill-typed.

**Corollary 12.6.** If $e : \tau$, then $\neg(e \upharpoonright)$.

Apart from the inconvenience of having to define the judgement $e \upharpoonright$ only to show that it is irrelevant for well-typed programs, this approach suffers a very significant methodological weakness. If we should omit one or more rules defining the judgement $e \upharpoonright$, the proof of Theorem 12.5 remains valid; there is nothing to ensure that we have included sufficiently many checks for run-time type errors. We can prove that the ones we define cannot arise in a well-typed program, but we cannot prove that we have covered all possible cases. By contrast the transition semantics does not specify any behavior for ill-typed expressions. Consequently, any ill-typed expression will “get stuck” without our explicit intervention, and the progress theorem rules out all such cases. Moreover, the transition system corresponds more closely to implementation—a compiler need not make any provisions for checking for run-time type errors. Instead, it relies on the static semantics to ensure that these cannot arise, and assigns no meaning to any ill-typed program. Execution is therefore more efficient, and the language definition is simpler, an elegant win-win situation for both the semantics and the implementation.

### 12.4 Cost Semantics

A structural semantics provides a natural notion of *time complexity* for programs, namely the number of steps required to reach a final state. An evaluation semantics, on the other hand, does not provide such a direct notion of complexity. Since the individual steps required to complete an evaluation are suppressed, we cannot directly read off the number of steps required to evaluate to a value. Instead we must augment the evaluation relation with a cost measure, resulting in a *cost semantics*.

Evaluation judgements have the form $e \Downarrow^k v$, with the meaning that $e$ evaluates to $v$ in $k$ steps.

\[
\text{num}[n] \Downarrow^0 \text{num}[n]
\]
Theorem 12.7. For any closed expression $e$ and closed value $v$ of the same type, $e \Downarrow^k v$ iff $e \rightarrow^k v$.

Proof. From left to right proceed by rule induction on the definition of the cost semantics. From right to left proceed by induction on $k$, with an inner rule induction on the definition of the transition semantics.

12.5 Exercises

1. Prove that if $e \Downarrow v$, then $v \text{ val}$.

2. Prove that if $e \Downarrow v_1$ and $e \Downarrow v_2$, then $v_1 = v_2$.

3. Complete the proof of equivalence of evaluation and transition semantics.

4. Prove preservation for the instrumented evaluation semantics, and conclude that well-typed programs cannot go wrong.

5. Is it possible to use environments in a structural semantics? What difficulties do you encounter?
Part IV

Function Types
Chapter 13

Function Definitions and Values

In the language $\mathcal{L}\{\text{num str}\}$ we may perform calculations such as the doubling of a given expression, but we cannot express the concept of doubling itself. The general concept may be expressed by abstracting away from the expression being doubled, leaving behind just the pattern of doubling some fixed, but unspecified, number, represented by a variable. Specific instances of doubling are recovered by substituting an expression for the variable. A function is an expression with a designated free variable.

We consider two methods for permitting a function to be used more than once in an expression (for example, to double several different numbers). One method is through the introduction of function definitions, which give names to functions. An instance of the function is obtained by applying the function name to another expression, its argument. Each function has a domain and a range type, which in $\mathcal{L}\{\text{num str}\}$ must be either num or str. A function whose domain and range are base type is said to be a first-order function. A language in which functions are first-order and confined to function definitions is said to have second-class functions, since they are not values in the same sense as numbers or strings.

A more general method for supporting functions is as first-class values of function type whose domain and range are arbitrary types, including function types. A language with function types is said to be higher-order, in contrast to first-order, since it allows functions to be passed as arguments to and returned as results from other functions. Higher-order languages are surprisingly powerful, and they are, correspondingly, remarkably subtle, and have led to notorious design errors in programming languages.
13.1 First-Order Functions

The language $L\{\text{num str fun}\}$ is the extension of $L\{\text{num str}\}$ with function definitions and function applications as described by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expr</td>
<td>$e$</td>
<td>$\text{fun}[\tau_1; \tau_2] (x_1.e_2; f.e)$</td>
<td>$\text{fun} f(x_1: \tau_1): \tau_2 = e_2 \text{ in } e$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{call}<a href="e">f</a>$</td>
<td>$f(e)$</td>
</tr>
</tbody>
</table>

The variable $f$ ranges over a distinguished class of variables, called function names. The expression $\text{fun}[\tau_1; \tau_2] (x_1.e_2; f.e)$ binds the function name $f$ within $e$ to the pattern $x_1.e_2$, which has parameter $x_1$ and definition $e_2$. The domain and range of the function are, respectively, the types $\tau_1$ and $\tau_2$. The expression $\text{call}[f](e)$ instantiates the abstractor bound to $f$ with the argument $e$.

The static semantics of $L\{\text{num str fun}\}$ defines two forms of judgement:

1. Expression typing, $e : \tau$, stating that $e$ has type $\tau$;
2. Function typing, $f(\tau_1) : \tau_2$, stating that $f$ is a function with argument type $\tau_1$ and result type $\tau_2$.

The judgment $f(\tau_1) : \tau_2$ specifies the function header of $f$, since it resembles the syntax for a function definition given earlier.

The static semantics of $L\{\text{num str fun}\}$ is defined by the following rules:

$$
\frac{\Gamma, x_1 : \tau_1 \vdash e_2 : \tau_2 \quad \Gamma, f(\tau_1) : \tau_2 \vdash e : \tau}{\Gamma \vdash \text{fun}[\tau_1; \tau_2] (x_1.e_2; f.e) : \tau} 
\quad \text{(13.1a)}
$$

$$
\frac{\Gamma \vdash f(\tau_1) : \tau_2 \quad \Gamma \vdash e : \tau_1}{\Gamma \vdash \text{call}[f](e) : \tau_2} 
\quad \text{(13.1b)}
$$

The operation of function substitution, written $[x.e/f]e'$, is inductively defined similarly to ordinary substitution, but bearing in mind that the function name, $f$, may only occur within $e'$ as part of a function call. The rule governing such occurrences is given as follows:

$$
[x.e/f] \text{call}[f](e') = \text{let}(e'; x.e) 
\quad \text{(13.2)}
$$

That is, at call sites to $f$, we bind $x$ to $e'$ within $e$ to instantiate the pattern substituted for $f$. 

14:36 DRAFT DECEMBER 18, 2009
Lemma 13.1. If $\Gamma, f(\tau_1) : \tau_2 \vdash e : \tau$ and $\Gamma, x_1 : \tau_2 \vdash e_2 : \tau_2$, then $\Gamma \vdash [x_1.e_2/f]e : \tau$.

Proof. By induction on the structure of $e'$.

The dynamic semantics of $L\{\text{num str fun}\}$ is defined using function substitution:

$$\text{fun}[\tau_1; \tau_2](x_1.e_2; f.e) \mapsto [x_1.e_2/f]e \quad (13.3)$$

Observe that the use of function substitution eliminates all applications of $f$ within $e$, so that no rule is required for evaluating them. This rule imposes either a call-by-name or a call-by-value application discipline according to whether the let binding is given a by-name or a by-value interpretation.

The safety of $L\{\text{num str fun}\}$ may be proved separately, but it may also be obtained as a corollary of the safety of the more general language of higher-order functions, which we discuss next.

### 13.2 Higher-Order Functions

The syntactic and semantic similarity between variable definitions and function definitions in $L\{\text{num str fun}\}$ is striking. This suggests that it may be possible to consolidate the two concepts into a single definition mechanism. The gap that must be bridged is the segregation of functions from expressions. A function name $f$ is bound to an abstractor $x.e$ specifying a pattern that is instantiated when $f$ is applied. To consolidate function definitions with expression definitions it is sufficient to reify the abstractor into a form of expression, called a $\lambda$-abstraction, written $\text{lam}[\tau_1](x.e)$. Correspondingly, we must generalize application to have the form $\text{ap}(e_1; e_2)$, where $e_1$ is any expression, and not just a function name. These are, respectively, the introduction and elimination forms for the function type, $\text{arr}(\tau_1; \tau_2)$, whose elements are functions with domain $\tau_1$ and range $\tau_2$.

The language $L\{\text{num str } \rightarrow\}$ is the enrichment of $L\{\text{num str}\}$ with function types, as specified by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>$\tau$</td>
<td>$\text{arr}(\tau_1; \tau_2)$</td>
<td>$\tau_1 \rightarrow \tau_2$</td>
</tr>
<tr>
<td>Expr</td>
<td>$e$</td>
<td>$\text{lam}<a href="x.e">\tau</a>$</td>
<td>$\lambda (x: \tau.e)$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{ap}(e_1; e_2)$</td>
<td>$e_1(e_2)$</td>
</tr>
</tbody>
</table>

December 18, 2009
The static semantics of $\mathcal{L}\{\text{num str} \rightarrow\}$ is given by extending Rules (9.1) with the following rules:

\[
\begin{align*}
\Gamma, x : \tau_1 \vdash e : \tau_2 \\
\Rightarrow \Gamma \vdash \text{lam}[^{\tau_1}](x. e) : \text{arr}(\tau_1; \tau_2) \\
\Gamma \vdash e_1 : \text{arr}(\tau_2; \tau) \quad \Gamma \vdash e_2 : \tau_2 \\
\Rightarrow \Gamma \vdash \text{ap}(e_1; e_2) : \tau
\end{align*}
\]

(13.4a)

(13.4b)

Lemma 13.2 (Inversion). Suppose that $\Gamma \vdash e : \tau$.

1. If $e = \text{lam}[^{\tau_1}](x. e)$, then $\tau = \text{arr}(\tau_1; \tau_2)$ and $\Gamma, x : \tau_1 \vdash e : \tau_2$.

2. If $e = \text{ap}(e_1; e_2)$, then there exists $\tau_2$ such that $\Gamma \vdash e_1 : \text{arr}(\tau_2; \tau)$ and $\Gamma \vdash e_2 : \tau_2$.

Proof. The proof proceeds by rule induction on the typing rules. Observe that for each rule, exactly one case applies, and that the premises of the rule in question provide the required result.

Lemma 13.3 (Substitution). If $\Gamma, x : \tau \vdash e' : \tau'$, and $\Gamma \vdash e : \tau$, then $\Gamma \vdash [e/x]e' : \tau'$.

Proof. By rule induction on the derivation of the first judgement.

The dynamic semantics of $\mathcal{L}\{\text{num str} \rightarrow\}$ extends that of $\mathcal{L}\{\text{num str}\}$ with the following additional rules:

\[
\begin{align*}
\text{lam}[^{\tau}](x. e) \Rightarrow \text{val} \\
e_1 \mapsto e'_1 \\
\text{ap}(e_1; e_2) \mapsto \text{ap}(e'_1; e_2) \\
\text{ap}(\text{lam}[^{\tau_2}](x. e_1); e_2) \mapsto [e_2/x]e_1
\end{align*}
\]

(13.5a)

(13.5b)

(13.5c)

These rules specify a call-by-name discipline for function application. It is a good exercise to formulate a call-by-value discipline as well.

Theorem 13.4 (Preservation). If $e : \tau$ and $e \mapsto e'$, then $e' : \tau$. 
Proof. The proof is by induction on rules (13.5), which define the dynamic semantics of the language.

Consider rule (13.5c),

\[
\text{ap}(\lambda [\tau_2](x.e_1);e_2) \rightarrow [e_2/x]e_1.
\]

Suppose that \(\text{ap}(\lambda [\tau_2](x.e_1);e_2) : \tau_1\). By Lemma 13.2 on the preceding page \(e_2 : \tau_2\) and \(x : \tau_2 \vdash e_1 : \tau_1\), so by Lemma 13.3 on the facing page \([e_2/x]e_1 : \tau_1\).

The other rules governing application are handled similarly. \(\square\)

Lemma 13.5 (Canonical Forms). If \(e\) val and \(e : \text{arr}(\tau_1;\tau_2)\), then \(e = \lambda [\tau_1](x.e_2)\) for some \(x\) and \(e_2\) such that \(x : \tau_1 \vdash e_2 : \tau_2\).

Proof. By induction on the typing rules, using the assumption \(e\) val. \(\square\)

Theorem 13.6 (Progress). If \(e : \tau\), then either \(e\) is a value, or there exists \(e'\) such that \(e \mapsto e'\).

Proof. The proof is by induction on rules (13.4). Note that since we consider only closed terms, there are no hypotheses on typing derivations.

Consider rule (13.4b). By induction either \(e_1\) val or \(e_1 \mapsto e'_1\). In the latter case we have \(\text{ap}(e_1;e_2) \mapsto \text{ap}(e'_1;e_2)\). In the former case, we have by Lemma 13.5 that \(e_1 = \lambda [\tau_2](x.e)\) for some \(x\) and \(e\). But then \(\text{ap}(e_1;e_2) \mapsto [e_2/x]e\). \(\square\)

13.3 Evaluation Semantics and Definitional Equivalence

An inductive definition of the evaluation judgement \(e \Downarrow v\) for \(L\{\text{num str} \rightarrow\}\) is given by the following rules:

\[
\begin{align*}
\lambda [\tau](x.e) & \Downarrow \lambda [\tau](x.e) \\
 e_1 & \Downarrow \lambda [\tau](x.e) \\
 [e_2/x]e & \Downarrow v \\
\text{ap}(e_1;e_2) & \Downarrow v
\end{align*}
\]

It is easy to check that if \(e \Downarrow v\), then \(v\) val, and that if \(e\) val, then \(e \Downarrow e\).
Theorem 13.7. $e \downarrow v \text{ iff } e \rightarrow^* v \text{ and } v \text{ val.}$

Proof. In the forward direction we proceed by rule induction on Rules (13.6). The proof makes use of a pasting lemma stating that, for example, if $e_1 \rightarrow^* e'_1$, then $\text{ap}(e_1; e_2) \rightarrow^* \text{ap}(e'_1; e_2)$, and similarly for the other constructs of the language.

In the reverse direction we proceed by rule induction on Rules (4.1). The proof relies on a converse evaluation lemma, which states that if $e \rightarrow e'$ and $e' \downarrow v$, then $e \downarrow v$. This is proved by rule induction on Rules (13.5). \qed

Definitional equivalence for the call-by-name semantics of $L\{	ext{num str} \rightarrow\}$ is defined by a straightforward extension to Rules (10.9).

\begin{align*}
\Gamma \vdash \text{ap}(\text{lam}[	au](x.e_2); e_1) & \equiv [e_1/x]e_2 : \tau_2 \quad (13.7a) \\
\Gamma \vdash e_1 \equiv e'_1 : \tau_2 \rightarrow \tau \quad \Gamma \vdash e_2 \equiv e'_2 : \tau_2 \\
\Gamma \vdash \text{ap}(e_1; e_2) & \equiv \text{ap}(e'_1; e'_2) : \tau \quad (13.7b) \\
\Gamma, x : \tau_1 \vdash e_2 \equiv e'_2 : \tau_2 \quad \Gamma \vdash \text{lam}[	au_1](x.e_2) & \equiv \text{lam}[	au_1](x.e'_2) : \tau_1 \rightarrow \tau_2 \quad (13.7c)
\end{align*}

Definitional equivalence for call-by-value requires a small bit of additional machinery. The main idea is to restrict Rule (13.7a) to require that the argument be a value. However, to be fully expressive, we must also widen the concept of a value to include all variables that are in scope, so that Rule (13.7a) would apply even when the argument is a variable. The justification for this is that in call-by-value, the parameter of a function stands for the value of its argument, and not for the argument itself. The call-by-value definitional equivalence judgement has the form

$$\Xi \Gamma \vdash e_1 \equiv e_2 : \tau,$$

where $\Xi$ is the finite set of hypotheses $x_1 \text{ val, \ldots, } x_k \text{ val}$ governing the variables in scope at that point. We write $\Xi \vdash e \text{ val}$ to indicate that $e$ is a value under these hypotheses, so that, for example, $\Xi, x \text{ val} \vdash x \text{ val}$.

The rule of definitional equivalence for call-by-value are similar to those for call-by-name, modified to take account of the scopes of value variables. Two illustrative rules are as follows:

\begin{align*}
\Xi, x \text{ val} \Gamma, x : \tau_1 \vdash e_2 \equiv e'_2 : \tau_2 \\
\Xi \Gamma \vdash \text{lam}[	au_1](x.e_2) & \equiv \text{lam}[	au_1](x.e'_2) : \tau_1 \rightarrow \tau_2 \quad (13.8a)
\end{align*}
13.4 Dynamic Scope

The dynamic semantics of function application given by Rules (13.5) is defined for closed expressions (those without free variables). Variables are never encountered during evaluation, because a closed expression will have been substituted for it before it is needed during evaluation. This accurately reflects the meaning of a variable as an unknown whose value may be specified by substitution. This treatment of variables is called static scope, or static binding, because it respects the statically determined scoping rules defined in Chapter 7.

Another evaluation strategy for $\mathcal{L}\{\to\}$ is sometimes considered as an alternative to static binding, called dynamic scope, or dynamic binding. The semantics of a dynamically scoped version of $\mathcal{L}\{\to\}$ is given by the same rules as for static binding, but altered in two crucial respects. First, evaluation is defined for open terms (those with free variables), as well as for closed terms. It is, however, an error to evaluate a variable; as with static scope, we must arrange that its binding is determined before its value is needed. Second, the binding of a variable is specified by a special form of substitution that incurs, rather than avoids, capture of free variables.

To avoid confusion, we will use the term replacement to refer to the capture-incurring form of substitution, which we write as $[x ← e_1]e_2$. As an example of replacement, let $e$ be the expression $\lambda (x: \sigma. y)$ (with a free variable $y$), and let $e'$ be the expression $\lambda (y: \tau. f(y))$, where $f$ is a variable. The result of the substitution $[e / f]e'$ is the expression

$$\lambda (y': \tau. \lambda (x: \sigma. y) (y')),$$

in which the bound variable, $y$, has been renamed to $y'$ to avoid confusion with the free variable, $y$, in $e$. The variable $y$ remains free in the result. In contrast, the result of the replacement $[f ← e]e'$ is the expression

$$\lambda (y: \tau. \lambda (x: \sigma. y) (y)),$$

which has no free variables because the free $y$ in $e$ is captured by the binding for $y$ in $e'$.

The implications of these alterations to the semantics of $\mathcal{L}\{\to\}$ are far-reaching. An immediate question suggested by the foregoing example is
whether typing is preserved by replacement (as distinct from substitution). The answer is no! In the example if \( \sigma \neq \tau \), then the result of replacement is not well-typed, even though both \( e \) and \( e' \) are well-typed (assuming \( y : \tau \) and \( f : \tau \rightarrow \tau' \)). For this reason, dynamic scope is usually only considered feasible for languages with only one type, so that such considerations do not arise.\(^1\) An alternative is to consider a much richer type system that accounts for the types of the free variables in an expression; this possibility is explored in Chapter 35.

Setting aside these concerns, there is a further problem with dynamic scope that merits careful consideration, since it is closely tied to its purported advantages. The idea of dynamic scope is to make it convenient to parameterize a function by the values of one or more variables, without having to pass them as additional arguments. So, for example, a function \( \lambda (x : \sigma. e) \) with \( y \) free is to be regarded as a family of functions, one for each choice of the parameter \( y \). Using replacement, rather than substitution, allows the specification of a value for \( y \) to be determined by the context in which the function is used, rather than the context in which the function is introduced. (This is what gives rise to the terminology “dynamic scope.”) Thus, in the example above, the meaning of the expression \( e \) is not fixed until after the replacement of \( f \) by \( e \) in \( e' \), at which point \( y \) is tied to the argument of the function \( e' \). Whatever that turns out to be will determine the particular instance of \( e \) that will be used.

The chief difficulty with dynamic scope is that the names of bound variables matter. For example, consider the expression \( e'' \) given by \( \lambda (y' : \tau. \lambda (x : \sigma. y) (y')) \). The expression \( e' \) is \( \alpha \)-equivalent to \( e'' \); all we have done is to rename the bound variable from \( y \) to \( y' \). The principles of binding and scope described in Chapter 7 state that these two expressions should be interchangeable in all situations, and indeed they are under static scope. However, with dynamic scope they behave quite differently. In particular, the replacement \([x \leftarrow e]e'' \) results in the expression

\[
\lambda (y' : \tau. \lambda (x : \sigma. y) (y')),
\]

which differs from the replacement \([x \leftarrow e]e' \), even though \( e' \) and \( e'' \) are \( \alpha \)-equivalent.

From a programmer’s perspective, the author of the expression \( e \) must be aware of the parameter naming conventions used by the author of \( e' \) (or \( e'' \)). This does violence to any form of modularity or separation of concerns; the two pieces of code must be written in conjunction with each other, and

---

\(^1\)See Chapter 22 for a discussion of useful programming languages with but one type.
this intimate relationship must be maintained as the code evolves. Experience shows that this is an impossible demand. For this reason, together with the difficulties with typing, dynamic scoping of variables is often treated with skepticism. However, there are other means of supporting essentially the same functionality, but without doing violence to the fundamental principles of binding and scope explained in Chapter 7. This concept, called fluid binding, is the subject of Chapter 35.

13.5 Exercises
Chapter 14

Gödel’s System T

The language $L\{\text{nat} \to \}$, better known as Gödel’s System T, is the combination of function types with the type of natural numbers. In contrast to $L\{\text{num str} \}$, which equips the naturals with some arbitrarily chosen arithmetic primitives, the language $L\{\text{nat} \to \}$ provides a general mechanism, called primitive recursion, from which these primitives may be defined. Primitive recursion captures the essential inductive character of the natural numbers, and hence may be seen as an intrinsic termination proof for each program in the language. Consequently, we may only define total functions in the language, those that always return a value for each argument. In essence every program in $L\{\text{nat} \to \}$ “comes equipped” with a proof of its termination. While this may seem like a shield against infinite loops, it is also a weapon that can be used to show that some programs cannot be written in $L\{\text{nat} \to \}$! To do so would require a master termination proof for every possible program in the language, something that we shall prove does not exist.

14.1 Statics
110 14.1 Statics

The syntax of \( L\{\text{nat} \to \} \) is given by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>( \tau )</td>
<td>( \text{nat} )</td>
<td>( \tau \to \tau )</td>
</tr>
<tr>
<td>Expr</td>
<td>( e )</td>
<td>( x )</td>
<td>( s(e) )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( z )</td>
<td>( s(\ldots s(z)) )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( \text{natrec}(e; e_0; x . y . e_1) )</td>
<td>( \text{natrec}(e; e_0; s(x) \text{ with } y \Rightarrow e_1) )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( \text{lam}[\tau](x . e) )</td>
<td>( \lambda(x: \tau . e) )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( \text{ap}(e_1; e_2) )</td>
<td>( e_1(e_2) )</td>
</tr>
</tbody>
</table>

We write \( n \) for the expression \( s(\ldots s(z)) \), in which the successor is applied \( n \geq 0 \) times to zero. The expression

\[
\text{natrec}(e; e_0; x . y . e_1)
\]

is called primitive recursion. It represents the \( e \)-fold iteration of the transformation \( x . y . e_1 \) starting from \( e_0 \). The bound variable \( x \) represents the predecessor and the bound variable \( y \) represents the result of the \( x \)-fold iteration. The "with" clause in the concrete syntax for the recursor binds the variable \( y \) to the result of the recursive call, as will become apparent shortly.

Sometimes iteration, written \( \text{natiter}(e; e_0; y . e_1) \), is considered as an alternative to primitive recursion. It has essentially the same meaning as primitive recursion, except that only the result of the recursive call is bound to \( y \) in \( e_1 \), and no binding is made for the predecessor. Clearly iteration is a special case of primitive recursion, since we can always ignore the predecessor binding. Conversely, primitive recursion is definable from iteration, provided that we have product types (Chapter 16) at our disposal. To define primitive recursion from iteration we simultaneously compute the predecessor while iterating the specified computation.

The static semantics of \( L\{\text{nat} \to \} \) is given by the following typing rules:

\[
\frac{}{\Gamma, x : \text{nat} \vdash x : \text{nat}} \quad (14.1a)
\]
\[
\frac{}{\Gamma \vdash z : \text{nat}} \quad (14.1b)
\]
\[
\frac{\Gamma \vdash e : \text{nat}}{\Gamma \vdash s(e) : \text{nat}} \quad (14.1c)
\]
\[
\frac{\Gamma \vdash e : \text{nat} \quad \Gamma \vdash e_0 : \tau \quad \Gamma, x : \text{nat}, y : \tau \vdash e_1 : \tau}{\Gamma \vdash \text{natrec}(e; e_0; x . y . e_1) : \tau} \quad (14.1d)
\]
As usual, admissibility of the structural rule of substitution is crucially important.

**Lemma 14.1.** If $\Gamma \vdash e : \tau$ and $\Gamma, x : \tau \vdash e' : \tau'$, then $\Gamma \vdash [e/x]e' : \tau'$.

### 14.2 Dynamics

The dynamic semantics of $\mathcal{L}\{\text{nat} \to\}$ adopts a call-by-name interpretation of function application, and requires that the successor operation evaluate its argument (so that values of type $\text{nat}$ are numerals).

The closed values of $\mathcal{L}\{\text{nat} \to\}$ are determined by the following rules:

\[
\begin{align*}
\text{z val} & \\
\text{e val} & \quad \text{s(e) val} \\
\lambda \tau (x.e) & \text{ val}
\end{align*}
\]  

(14.2a)  

(14.2b)  

(14.2c)

The dynamic semantics of $\mathcal{L}\{\text{nat} \to\}$ is given by the following rules:

\[
\begin{align*}
\text{e } & \mapsto e' \\
\text{s(e) } & \mapsto s(e') \\
\text{e}_1 & \mapsto e'_1 \\
\text{ap(e}_1 e_2 & \mapsto \text{ap(e'}_1 e_2 \\
\text{ap(\lambda \tau (x.e);e}_2 & \mapsto [e_2/x]e \\
\text{e } & \mapsto e'
\end{align*}
\]  

(14.3a)  

(14.3b)  

(14.3c)  

(14.3d)  

(14.3e)

December 18, 2009
Rules (14.3e) and (14.3f) specify the behavior of the recursor on $z$ and $s(e)$. In the former case the recursor evaluates $e_0$, and in the latter case the variable $x$ is bound to the predecessor, $e$, and $y$ is bound to the (unevaluated) recursion on $e$. If the value of $y$ is not required in the rest of the computation, the recursive call will not be evaluated.

Lemma 14.2 (Canonical Forms). If $e : \tau$ and $e \text{ val}$, then

1. If $\tau = \text{nat}$, then $e = s(s(\ldots z))$ for some number $n \geq 0$ occurrences of the successor starting with zero.

2. If $\tau = \tau_1 \rightarrow \tau_2$, then $e = \lambda (x : \tau_1). e_2$ for some $e_2$.

Theorem 14.3 (Safety). 1. If $e : \tau$ and $e \mapsto e'$, then $e' : \tau$.

2. If $e : \tau$, then either $e \text{ val}$ or $e \mapsto e'$ for some $e'$.

14.3 Definability

A mathematical function $f : \mathbb{N} \rightarrow \mathbb{N}$ on the natural numbers is definable in $\mathcal{L}\{\text{nat} \rightarrow \}$ iff there exists an expression $e_f$ of type $\text{nat} \rightarrow \text{nat}$ such that for every $n \in \mathbb{N}$,

$$e_f(n) \equiv f(n) : \text{nat}. \quad (14.4)$$

That is, the numeric function $f : \mathbb{N} \rightarrow \mathbb{N}$ is definable iff there is an expression $e_f$ of type $\text{nat} \rightarrow \text{nat}$ such that, when applied to the numeral representing the argument $n \in \mathbb{N}$, is definitionally equivalent to the numeral corresponding to $f(n) \in \mathbb{N}$.

Definitional equivalence for $\mathcal{L}\{\text{nat} \rightarrow \}$, written $\Gamma \vdash e \equiv e' : \tau$, is the strongest congruence containing these axioms:

$$\Gamma \vdash \text{ap(lam} [\tau] (x.e_2); e_1) \equiv [e_1/x]e_2 : \tau \quad (14.5a)$$

$$\Gamma \vdash \text{natrec}(z; e_0; x.y.e_1) \equiv e_0 : \tau \quad (14.5b)$$

$$\Gamma \vdash \text{natrec}(s(e); e_0; x.y.e_1) \equiv [e, \text{natrec}(e; e_0; x.y.e_1) / x, y]e_1 : \tau \quad (14.5c)$$
14.3 Definability

For example, the doubling function, \( d(n) = 2 \times n \), is definable in \( L\{\text{nat} \rightarrow \} \) by the expression \( e_d : \text{nat} \rightarrow \text{nat} \) given by

\[
\lambda \ (x : \text{nat}. \text{natrec} \ x \ {\{z \Rightarrow z \mid s(u) \ with \ v \Rightarrow s(s(v))\}}).
\]

To check that this defines the doubling function, we proceed by induction on \( n \in \mathbb{N} \). For the basis, it is easy to check that

\[ e_d(\overline{0}) \equiv \overline{0} : \text{nat}. \]

For the induction, assume that

\[ e_d(\overline{n}) \equiv \overline{d(n)} : \text{nat}. \]

Then calculate using the rules of definitional equivalence:

\[
e_d(\overline{n + 1}) \equiv s(s(e_d(\overline{n})))
\]

\[= s(s(\overline{2 \times n}))
\]

\[= \overline{2 \times (n + 1)}
\]

\[= \overline{d(n + 1)}. \]

As another example, consider the following function, called Ackermann’s function, defined by the following equations:

\[
A(0, n) = n + 1
\]

\[
A(m + 1, 0) = A(m, 1)
\]

\[
A(m + 1, n + 1) = A(m, A(m + 1, n)).
\]

This function grows very quickly. For example, \( A(4, 2) \approx 2^{65,536} \), which is often cited as being much larger than the number of atoms in the universe! Yet we can show that the Ackermann function is total by a lexicographic induction on the pair of argument \((m, n)\). On each recursive call, either \( m \) decreases, or else \( m \) remains the same, and \( n \) decreases, so inductively the recursive calls are well-defined, and hence so is \( A(m, n) \).

A first-order primitive recursive function is a function of type \( \text{nat} \rightarrow \text{nat} \) that is defined using primitive recursion, but without using any higher order functions. Ackermann’s function is defined so that it is not first-order primitive recursive, but is higher-order primitive recursive. The key is to showing that it is definable in \( L\{\text{nat} \rightarrow \} \) is to observe that \( A(m + 1, n) \) iterates the function \( A(m, -) \) for \( n \) times, starting with \( A(m, 1) \). As an auxiliary, let us define the higher-order function

\[ \text{it} : (\text{nat} \rightarrow \text{nat}) \rightarrow \text{nat} \rightarrow \text{nat} \rightarrow \text{nat} \]
to be the $\lambda$-abstraction

$$
\lambda (f:\text{nat} \to \text{nat} \cdot \lambda (n:\text{nat}. \text{natrec} n \{ z \Rightarrow \text{id} | s(\_ \cdot) \text{ with } g \Rightarrow f \circ g\})),
$$

where $\text{id} = \lambda (x:\text{nat}. x)$ is the identity, and $f \circ g = \lambda (x:\text{nat}. f(g(x)))$ is the composition of $f$ and $g$. It is easy to check that

$$
\text{it}(f)(m)(m) \equiv f^{(n)}(m) : \text{nat},
$$

where the latter expression is the $n$-fold composition of $f$ starting with $m$. We may then define the Ackermann function

$$
e_a : \text{nat} \to \text{nat} \to \text{nat}
$$
to be the expression

$$
\lambda (m:\text{nat}. \text{natrec} m \{ z \Rightarrow \text{succ} | s(\_ \cdot) \text{ with } f \Rightarrow \lambda (n:\text{nat}. \text{it}(f)(n)(f(\overline{1})))\}).
$$

It is instructive to check that the following equivalences are valid:

$$
e_a(\overline{0})(m) \equiv s(m) \quad (14.6)
$$

$$
e_a(m + \overline{1})(\overline{0}) \equiv e_a(m)(\overline{1}) \quad (14.7)
$$

$$
e_a(m + \overline{1})(n + \overline{1}) \equiv e_a(m)(e_a(s(m))(\overline{n})). \quad (14.8)
$$

That is, the Ackermann function is definable in $L\{\text{nat} \to\}$.

### 14.4 Non-Definability

It is impossible to define an infinite loop in $L\{\text{nat} \to\}$.

**Theorem 14.4.** If $e : \tau$, then there exists $v \text{ val}$ such that $e \equiv v : \tau$.

**Proof.** See Corollary 48.9 on page 449.

Consequently, values of function type in $L\{\text{nat} \to\}$ behave like mathematical functions: if $f : \sigma \to \tau$ and $e : \sigma$, then $f(e)$ evaluates to a value of type $\tau$. Moreover, if $e : \text{nat}$, then there exists a natural number $n$ such that $e \equiv n : \text{nat}$.

Using this, we can show, using a technique called diagonalization, that there are functions on the natural numbers that are not definable in the $L\{\text{nat} \to\}$. We make use of a technique, called Gödel-numbering, that assigns a unique natural number to each closed expression of $L\{\text{nat} \to\}$. This
allows us to manipulate expressions as data values in \( L^{\text{nat} \rightarrow} \), and hence permits \( L^{\text{nat} \rightarrow} \) to compute with its own programs.\(^1\)

The essence of Gödel-numbering is captured by the following simple construction on abstract syntax trees. (The generalization to abstract binding trees is slightly more difficult, the main complication being to ensure that \( a \)-equivalent expressions are assigned the same Gödel number.) Recall that a general ast, \( a \), has the form \( o(a_1, \ldots, a_k) \), where \( o \) is an operator of arity \( k \). Fix an enumeration of the operators so that every operator has an index \( i \in \mathbb{N} \), and let \( m \) be the index of \( o \) in this enumeration. Define the Gödel number \( \llbracket a \rrbracket \) of \( a \) to be the number
\[
2^m 3^{n_1} 5^{n_2} \ldots p_k^{n_k},
\]
where \( p_k \) is the \( k \)th prime number (so that \( p_0 = 2, p_1 = 3, \) and so on), and \( n_1, \ldots, n_k \) are the Gödel numbers of \( a_1, \ldots, a_k \), respectively. This obviously assigns a natural number to each ast. Conversely, given a natural number, \( n \), we may apply the prime factorization theorem to “parse” \( n \) as a unique abstract syntax tree. (If the factorization is not of the appropriate form, which can only be because the arity of the operator does not match the number of factors, then \( n \) does not code any ast.)

Now, using this representation, we may define a (mathematical) function \( f_{\text{univ}} : \mathbb{N} \rightarrow \mathbb{N} \rightarrow \mathbb{N} \) such that, for any \( e : \text{nat} \rightarrow \text{nat} \), \( f_{\text{univ}}(\llbracket e \rrbracket)(m) = n \) iff \( e(m) \equiv n : \text{nat} \).\(^2\) The determinacy of the dynamic semantics, together with Theorem 14.4 on the preceding page, ensure that \( f_{\text{univ}} \) is a well-defined function. It is called the universal function for \( L^{\text{nat} \rightarrow} \) because it specifies the behavior of any expression \( e \) of type \( \text{nat} \rightarrow \text{nat} \). Using the universal function, let us define an auxiliary mathematical function, called the diagonal function, \( d : \mathbb{N} \rightarrow \mathbb{N} \), by the equation \( d(m) = f_{\text{univ}}(m)(m) \). This function is chosen so that \( d(\llbracket e \rrbracket) = n \) iff \( e(\llbracket e \rrbracket) \equiv n : \text{nat} \). (The motivation for this definition will be apparent in a moment.)

The function \( d \) is not definable in \( L^{\text{nat} \rightarrow} \). Suppose that \( d \) were defined by the expression \( e_d \), so that we have
\[
e_d(\llbracket e \rrbracket) \equiv e(\llbracket e \rrbracket) : \text{nat}.
\]
Let \( e_D \) be the expression
\[
\lambda (x : \text{nat.} \, s(e_d(x)))
\]
\(^1\)The same technique lies at the heart of the proof of Gödel’s celebrated incompleteness theorem. The non-definability of certain functions on the natural numbers within \( L^{\text{nat} \rightarrow} \) may be seen as a form of incompleteness similar to that considered by Gödel.

\(^2\)The value of \( f_{\text{univ}}(k)(m) \) may be chosen arbitrarily to be zero when \( k \) is not the code of any expression \( e \).
of type $\text{nat} \to \text{nat}$. We then have

$$e_D(\overline{e_D}) \equiv s(e_D(\overline{e_D}))$$
$$\equiv s(e_D(\overline{e_D})).$$

But the termination theorem implies that there exists $n$ such that $e_D(\overline{e_D}) \equiv n$, and hence we have $\overline{n} \equiv s(\overline{n})$, which is impossible.

The function $f_{\text{univ}}$ is computable (that is, one can write an interpreter for $L\{\text{nat} \to \}$), but it is not programmable in $L\{\text{nat} \to \}$ itself. In general a language $L$ is universal if we can write an interpreter for $L$ in the language $L$ itself. The foregoing argument shows that $L\{\text{nat} \to \}$ is not universal. Consequently, there are computable numeric functions, such as the diagonal function, that cannot be programmed in $L\{\text{nat} \to \}$. Consequently, the universal function for $L\{\text{nat} \to \}$ cannot be programmed in the language. In other words, one cannot write an interpreter for $L\{\text{nat} \to \}$ in the language itself!

14.5 Exercises

1. Explore variant dynamic semantics for $L\{\text{nat} \to \}$, both separately and in combination, in which the successor does not evaluate its argument, and in which functions are called by value.
Chapter 15

Plotkin’s PCF

The language $\mathcal{L}\{\text{nat} \rightarrow\}$, also known as Plotkin’s PCF, integrates functions and natural numbers using general recursion, a means of defining self-referential expressions. In contrast to $\mathcal{L}\{\text{nat} \rightarrow\}$ expressions in $\mathcal{L}\{\text{nat} \rightarrow\}$ may not terminate when evaluated; consequently, functions are partial (may be undefined for some arguments), rather than total (which explains the “partial arrow” notation for function types). Compared to $\mathcal{L}\{\text{nat} \rightarrow\}$, the language $\mathcal{L}\{\text{nat} \rightarrow\}$ moves the termination proof from the expression itself to the mind of the programmer. The type system no longer ensures termination, which permits a wider range of functions to be defined in the system, but at the cost of admitting infinite loops when the termination proof is either incorrect or absent.

The crucial concept embodied in $\mathcal{L}\{\text{nat} \rightarrow\}$ is the fixed point characterization of recursive definitions. In ordinary mathematical practice one may define a function $f$ by recursion equations such as these:

\[
\begin{align*}
f(0) &= 1 \\
f(n + 1) &= (n + 1) \times f(n)
\end{align*}
\]

These may be viewed as simultaneous equations in the variable, $f$, ranging over functions on the natural numbers. The function we seek is a solution to these equations—a function $f : \mathbb{N} \rightarrow \mathbb{N}$ such that the above conditions are satisfied. We must, of course, show that these equations have a unique solution, which is easily shown by mathematical induction on the argument to $f$.

The solution to such a system of equations may be characterized as the fixed point of an associated functional (operator mapping functions to
functions). To see this, let us re-write these equations in another form:

\[
  f(n) = \begin{cases} 
    1 & \text{if } n = 0 \\
    n \times f(n') & \text{if } n = n' + 1 
  \end{cases}
\]

Re-writing yet again, we seek \( f \) such that

\[
  f : n \mapsto \begin{cases} 
    1 & \text{if } n = 0 \\
    n \times f(n') & \text{if } n = n' + 1 
  \end{cases}
\]

Now define the functional \( F \) by the equation \( F(f) = f' \), where

\[
  f' : n \mapsto \begin{cases} 
    1 & \text{if } n = 0 \\
    n \times f(n') & \text{if } n = n' + 1 
  \end{cases}
\]

Note well that the condition on \( f' \) is expressed in terms of the argument, \( f \), to the functional \( F \), and not in terms of \( f' \) itself! The function \( f \) we seek is then a fixed point of \( F \), which is a function \( f : \mathbb{N} \to \mathbb{N} \) such that \( f = F(f) \). In other words \( f \) is defined to the fix(\( F \)), where fix is an operator on functionals yielding a fixed point of \( F \).

Why does an operator such as \( F \) have a fixed point? Informally, a fixed point may be obtained as the limit of series of approximations to the desired solution obtained by iterating the functional \( F \). This is where partial functions come into the picture. Let us say that a partial function, \( \phi \) on the natural numbers, is an approximation to a total function, \( f \), if \( \phi(m) = n \) implies that \( f(m) = n \). Let \( \bot : \mathbb{N} \to \mathbb{N} \) be the totally undefined partial function—\( \bot (n) \) is undefined for every \( n \in \mathbb{N} \). Intuitively, this is the “worst” approximation to the desired solution, \( f \), of the recursion equations given above. Given any approximation, \( \phi \), of \( f \), we may “improve” it by considering \( \phi' = F(\phi) \). Intuitively, \( \phi' \) is defined on 0 and on \( m + 1 \) for every \( m \geq 0 \) on which \( \phi \) is defined. Continuing in this manner, \( \phi'' = F(\phi') = F(F(\phi)) \) is an improvement on \( \phi' \), and hence a further improvement on \( \phi \). If we start with \( \bot \) as the initial approximation to \( f \), then pass to the limit

\[
  \lim_{i \geq 0} F^{(i)}(\bot),
\]

we will obtain the least approximation to \( f \) that is defined for every \( m \in \mathbb{N} \), and hence is the function \( f \) itself. Turning this around, if the limit exists, it must be the solution we seek.

This fixed point characterization of recursion equations is taken as a primitive concept in \( \mathcal{L} \{\text{nat} \to \} \)—we may obtain the least fixed point of any
functional definable in the language. Using this we may solve any set of
recursion equations we like, with the proviso that there is no guarantee
that the solution is a total function. Rather, it is guaranteed to be a partial
function that may be undefined on some, all, or no inputs. This is the price
we may for expressive power—we may solve all systems of equations, but
the solution may not be as well-behaved as we might like it to be. It is our
task as programmer’s to ensure that the functions defined by recursion are
total—all of our loops terminate.

15.1 Statics

The abstract binding syntax of \( L\{\text{nat} \rightarrow\} \) is given by the following gram-
mar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>( \tau )</td>
<td>( \text{nat} )</td>
<td>( \text{nat} )</td>
</tr>
<tr>
<td></td>
<td>( \text{parr}(\tau_1;\tau_2) )</td>
<td>( \tau_1 \rightarrow \tau_2 )</td>
<td>( \tau_1 \rightarrow \tau_2 )</td>
</tr>
<tr>
<td>Expr</td>
<td>( e )</td>
<td>( x )</td>
<td>( x )</td>
</tr>
<tr>
<td></td>
<td>( z )</td>
<td>( z )</td>
<td>( z )</td>
</tr>
<tr>
<td></td>
<td>( s(e) )</td>
<td>( s(e) )</td>
<td>( s(e) )</td>
</tr>
<tr>
<td></td>
<td>( \text{ifz}(e;e_0;x.e_1) )</td>
<td>( { z \Rightarrow e_0 \mid s(x) \Rightarrow e_1 } )</td>
<td>( { z \Rightarrow e_0 \mid s(x) \Rightarrow e_1 } )</td>
</tr>
<tr>
<td></td>
<td>( \text{lam}<a href="x.e">\tau</a> )</td>
<td>( \lambda(x:\tau.e) )</td>
<td>( \lambda(x:\tau.e) )</td>
</tr>
<tr>
<td></td>
<td>( \text{ap}(e_1;e_2) )</td>
<td>( e_1(e_2) )</td>
<td>( e_1(e_2) )</td>
</tr>
<tr>
<td></td>
<td>( \text{fix}<a href="x.e">\tau</a> )</td>
<td>( \text{fix } x : \tau \Rightarrow e )</td>
<td>( \text{fix } x : \tau \Rightarrow e )</td>
</tr>
</tbody>
</table>

The expression \( \text{fix}[\tau](x.e) \) is called general recursion; it is discussed in
more detail below. The expression \( \text{ifz}(e;e_0;x.e_1) \) branches according to
whether \( e \) evaluates to \( z \) or not, binding the predecessor to \( x \) in the case
that it is not.

The static semantics of \( L\{\text{nat} \rightarrow\} \) is inductively defined by the follow-
ing rules:

\[
\Gamma, x : \tau \vdash x : \tau \tag{15.1a}
\]

\[
\Gamma \vdash z : \text{nat} \tag{15.1b}
\]

\[
\Gamma \vdash e : \text{nat} \tag{15.1c}
\]

\[
\Gamma, x : \text{nat} \vdash e_1 : \tau \tag{15.1d}
\]

\[
\Gamma \vdash \text{ifz}(e;e_0;x.e_1) : \tau \tag{15.1d}
\]
\[ \Gamma, x : \tau_1 \vdash e : \tau_2 \]
\[ \Gamma \vdash \text{lam}[\tau_1](x.e) : \text{parr}(\tau_1;\tau_2) \] (15.1e)

\[ \Gamma \vdash e_1 : \text{parr}(\tau_2;\tau) \quad \Gamma \vdash e_2 : \tau_2 \]
\[ \Gamma \vdash \text{ap}(e_1; e_2) : \tau \] (15.1f)

\[ \Gamma, x : \tau \vdash e : \tau \]
\[ \Gamma \vdash \text{fix}[\tau](x.e) : \tau \] (15.1g)

Rule (15.1g) reflects the self-referential nature of general recursion. To show that \( \text{fix}[\tau](x.e) \) has type \( \tau \), we assume that it is the case by assigning that type to the variable, \( x \), which stands for the recursive expression itself, and checking that the body, \( e \), has type \( \tau \) under this very assumption.

The structural rules, including in particular substitution, are admissible for the static semantics.

**Lemma 15.1.** If \( \Gamma, x : \tau \vdash e' : \tau' \), \( \Gamma \vdash e : \tau \), then \( \Gamma \vdash [e/x]e' : \tau' \).

### 15.2 Dynamics

The dynamic semantics of \( \mathcal{L}\{\text{nat} \rightarrow \} \) is defined by the judgements \( e \text{ val} \), specifying the closed values, and \( e \mapsto e' \), specifying the steps of evaluation. We will consider a call-by-name dynamics for function application, and require that the successor evaluate its argument.

The judgement \( e \text{ val} \) is defined by the following rules:

\[ \text{z val} \] (15.2a)

\[ e \text{ val} \]
\[ s(e) \text{ val} \] (15.2b)

\[ \text{lam}[\tau](x.e) \text{ val} \] (15.2c)

The transition judgement \( e \mapsto e' \) is defined by the following rules:

\[ e \mapsto e' \]
\[ s(e) \mapsto s(e') \] (15.3a)

\[ e \mapsto e' \]
\[ \text{ifz}(e; e_0; x.e_1) \mapsto \text{ifz}(e'; e_0; x.e_1) \] (15.3b)
15.2 Dynamics

\[
\text{ifz}(z; e_0; x.e_1) \mapsto e_0
\] (15.3c)

\[
s(e) \text{ val} \\
\text{ifz}(s(e); e_0; x.e_1) \mapsto [e/x]e_1
\] (15.3d)

\[
e_1 \mapsto e'_1 \\
ap(e_1; e_2) \mapsto ap(e'_1; e_2)
\] (15.3e)

\[
ap(lam[\tau](x.e); e_2) \mapsto [e_2/x]e
\] (15.3f)

\[
\text{fix}[\tau](x.e) \mapsto [\text{fix}[\tau](x.e)/x]e
\] (15.3g)

Rule (15.3g) implements self-reference by substituting the recursive expression itself for the variable \( x \) in its body. This is called \textit{unwinding} the recursion.

**Theorem 15.2 (Safety).**

1. If \( e : \tau \) and \( e \mapsto e' \), then \( e' : \tau \).

2. If \( e : \tau \), then either \( e \text{ val} \) or there exists \( e' \) such that \( e \mapsto e' \).

**Proof.** The proof of preservation is by induction on the derivation of the transition judgement. Consider Rule (15.3g). Suppose that \( \text{fix}[\tau](x.e) : \tau \). By inversion of typing we have \( \text{fix}[\tau](x.e) : \tau \vdash [\text{fix}[\tau](x.e)/x]e : \tau \), from which the result follows directly by transitivity of the hypothetical judgement. The proof of progress proceeds by induction on the derivation of the typing judgement. For example, for Rule (15.1g) the result follows immediately since we may make progress by unwinding the recursion. \( \square \)

Definitional equivalence for \( L\{\text{nat} \to \} \), written \( \Gamma \vdash e_1 \equiv e_2 : \tau \), is defined to be the strongest congruence containing the following axioms:

\[
\Gamma \vdash \text{ifz}(\tau; z; e_0, x.e_1) \equiv e_0 : \tau
\] (15.4a)

\[
\Gamma \vdash \text{ifz}(\tau; s(e); e_0, x.e_1) \equiv [e/x]e_1 : \tau
\] (15.4b)

\[
\Gamma \vdash \text{fix}[\tau](x.e) \equiv [\text{fix}[\tau](x.e)/x]e : \tau
\] (15.4c)

\[
\Gamma \vdash \text{ap}(\text{lam}[\tau](x.e_2); e_1) \equiv [e_1/x]e_2 : \tau
\] (15.4d)

These rules are sufficient to calculate the value of any closed expression of type \( \text{nat} \): if \( e : \text{nat} \), then \( e \equiv \overline{n} : \text{nat} \) iff \( e \mapsto^* \overline{n} \).
15.3 Definability

General recursion is a very flexible programming technique that permits a wide variety of functions to be defined within $L_{nat \rightarrow}$. The drawback is that, in contrast to primitive recursion, the termination of a recursively defined function is not intrinsic to the program itself, but rather must be proved extrinsically by the programmer. The benefit is a much greater freedom in writing programs.

General recursive functions are definable from general recursion and non-recursive functions. Let us write $\text{fun } x : t_1 \rightarrow t_2 \text{ is } e$ for a recursive function within whose body, $e : t_2$, are bound two variables, $y : t_1$ standing for the argument and $x : t_1 \rightarrow t_2$ standing for the function itself. The dynamic semantics of this construct is given by the axiom

$$\text{fun } x : t_1 \rightarrow t_2 \text{ is } e \rightarrow [\text{fun } x : t_1 \rightarrow t_2 \text{ is } e, e_1/x, y]e.$$  

That is, to apply a recursive function, we substitute the recursive function itself for $x$ and the argument for $y$ in its body.

Recursive functions may be defined in $L_{nat \rightarrow}$ using a combination of recursion and functions, writing

$$\text{fix } x : t_1 \rightarrow t_2 \text{ is } \lambda (y : t_1. e)$$

for $\text{fun } x : t_1 \rightarrow t_2 \text{ is } e$. It is a good exercise to check that the static and dynamic semantics of recursive functions are derivable from this definition.

The primitive recursion construct of $L_{nat \rightarrow}$ is defined in $L_{nat \rightarrow}$ using recursive functions by taking the expression

$$\text{natrec e } \{ z \Rightarrow e_0 | s(x) \text{ with } y \Rightarrow e_1 \}$$

to stand for the application, $e'(e)$, where $e'$ is the general recursive function

$$\text{fun } f(u : nat) : t \text{ is ifz u } \{ z \Rightarrow e_0 | s(x) \Rightarrow [f(x)/y]e_1 \}.$$  

The static and dynamic semantics of primitive recursion are derivable in $L_{nat \rightarrow}$ using this expansion.

In general, functions definable in $L_{nat \rightarrow}$ are partial in that they may be undefined for some arguments. A partial (mathematical) function, $\phi : \mathbb{N} \rightarrow \mathbb{N}$, is definable in $L_{nat \rightarrow}$ iff there is an expression $e_\phi : nat \rightarrow nat$ such that $\phi(m) = n$ iff $e_\phi(m) \equiv n : nat$. So, for example, if $\phi$ is the totally undefined function, then $e_\phi$ is any function that loops without returning whenever it is called.
It is informative to classify those partial functions \( \phi \) that are definable in \( L\{ \text{nat} \to \} \). These are the so-called \textit{partial recursive functions}, which are defined to be the primitive recursive functions augmented by the \textit{minimization} operation: given \( \phi \), define \( \psi(m) \) to be the least \( n \geq 0 \) such that (1) for \( m < n \), \( \phi(m) \) is defined and non-zero, and (2) \( \phi(n) = 0 \). If no such \( n \) exists, then \( \psi(m) \) is undefined.

**Theorem 15.3.** A partial function \( \phi \) on the natural numbers is definable in \( L\{ \text{nat} \to \} \) iff it is partial recursive.

**Proof sketch.** Minimization is readily definable in \( L\{ \text{nat} \to \} \), so it is at least as powerful as the class of partial recursive functions. Conversely, we may, with considerable tedium, define an evaluator for expressions of \( L\{ \text{nat} \to \} \) as a partial recursive function, using Gödel-numbering to represent expressions as numbers. Consequently, \( L\{ \text{nat} \to \} \) does not exceed the power of the class of partial recursive functions.

Church’s Law states that the partial recursive functions coincide with the class of effectively computable functions on the natural numbers—those that can be carried out by a program written in any programming language currently available or that will ever be available.\(^1\) Therefore \( L\{ \text{nat} \to \} \) is as powerful as any other programming language with respect to the class of definable functions on the natural numbers.

The universal function, \( \phi_{\text{univ}} \), for \( L\{ \text{nat} \to \} \) is the partial function on the natural numbers defined by

\[
\phi_{\text{univ}}(\langle e \rangle)(m) = n \text{ iff } e(m) \equiv n : \text{nat}.
\]

In contrast to \( L\{ \text{nat} \to \} \), the universal function \( \phi_{\text{univ}} \) for \( L\{ \text{nat} \to \} \) is partial (may be undefined for some inputs). It is, in essence, an interpreter that, given the code \( \langle e \rangle \) of a closed expression of type \( \text{nat} \to \text{nat} \), simulates the dynamic semantics to calculate the result, if any, of applying it to the \( m \), obtaining \( n \). Since this process may not terminate, the universal function is not defined for all inputs.

By Church’s Law the universal function is definable in \( L\{ \text{nat} \to \} \). In contrast, we proved in Chapter 14 that the analogous function is not definable in \( L\{ \text{nat} \to \} \) using the technique of diagonalization. It is instructive to examine why that argument does not apply in the present setting. As in Section 14.4 on page 114, we may derive the equivalence

\[
e_D(\langle e_D \rangle) \equiv s(e_D(\langle e_D \rangle))
\]

\(^1\)See Chapter 21 for further discussion of Church’s Law.
The difference, however, is that this equation is not inconsistent! Rather than being contradictory, it is merely a proof that the expression \( e_D(⌜e_D⌝) \) does not terminate when evaluated, for if it did, the result would be a number equal to its own successor, which is impossible.

15.4 Co-Natural Numbers

The evaluation strategy for the successor operation specified by Rules (15.3) ensures that the type \( \text{nat} \) is interpreted standardly as the type of natural numbers. This means that if \( e : \text{nat} \) and \( e \text{ val} \), then \( e \) is definitionally equivalent to a numeral. In contrast the lazy interpretation of successor, obtained by omitting Rule (15.3a), and requiring that \( s(e) \text{ val} \) for any \( e \), ruins this correspondence. The expression

\[
\omega = \text{fix}_{\text{nat}} \ x \text{ is } s(x)
\]

evaluates to \( s(\omega) \), which is a value of type \( \text{nat} \). The “number” \( \omega \) may be thought of as an infinite stack of successors, which is therefore larger than any finite stack of successors starting with zero. In other words \( \omega \) is larger than any (finite) natural number, and hence can be regarded as an infinite “natural number.”

Of course it is stretching the terminology to refer to \( \omega \) as a number, much less as a natural number. Rather, we should say that the lazy interpretation of the successor operation gives rise to a distinct type, called the lazy natural numbers, or the co-natural numbers. The latter terminology arises from considering the co-natural numbers as “dual” to the ordinary natural numbers in the following sense. The standard natural numbers are inductively defined as the least type such that if \( e \equiv z : \text{nat} \) or \( e \equiv s(e') : \text{nat} \) for some \( e' : \text{nat} \), then \( e : \text{nat} \). Dually, the co-natural numbers may be regarded as the largest type such that if \( e : \text{conat} \), then either \( e \equiv z : \text{conat} \), or \( e \equiv s(e') : \text{nat} \) for some \( e' : \text{conat} \). The difference is that \( \omega : \text{conat} \), because \( \omega \) is definitionally equivalent to its own successor, whereas it is not the case that \( \omega : \text{nat} \), according to these definitions.

The duality between the natural numbers and the co-natural numbers is developed further in Chapter 19, wherein we consider the concepts of inductive and co-inductive types. Eagerness and laziness in general is discussed further in Chapter 39.

15.5 Exercises
Part V

Finite Data Types
Chapter 16

Product Types

The binary product of two types consists of ordered pairs of values, one from each type in the order specified. The associated elimiatory forms are projections, which select the first and second component of a pair. The nullary product, or unit, type consists solely of the unique “null tuple” of no values, and has no associated elimiatory form. The product type admits both a lazy and an eager dynamics. According to the lazy dynamics, a pair is a value without regard to whether its components are values; they are not evaluated until (if ever) they are accessed and used in another computation. According to the eager dynamics, a pair is a value only if its components are values; they are evaluated when the pair is created.

More generally, we may consider the finite product, $\prod_{i \in I} \tau_i$, indexed by a finite set of indices, $I$. The elements of the finite product type are $I$-indexed tuples whose $i$th component is an element of the type $\tau_i$, for each $i \in I$. The components are accessed by $I$-indexed projection operations, generalizing the binary case. Special cases of the finite product include $n$-tuples, indexed by sets of the form $I = \{0,\ldots,n-1\}$, and labelled tuples, or records, indexed by finite sets of symbols. Similarly to binary products, finite products admit both an eager and a lazy interpretation.

16.1 Nullary and Binary Products
The abstract syntax of products is given by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>τ</td>
<td>::= unit</td>
<td>unit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>prod(τ₁; τ₂)</td>
<td>τ₁ × τ₂</td>
<td></td>
</tr>
<tr>
<td>Expr</td>
<td>e</td>
<td>::= triv</td>
<td>(</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>pair(e₁; e₂)</td>
<td>⟨e₁, e₂⟩</td>
<td></td>
</tr>
<tr>
<td></td>
<td>proj<a href="e">l</a></td>
<td>e · l</td>
<td></td>
</tr>
<tr>
<td></td>
<td>proj<a href="e">r</a></td>
<td>e · r</td>
<td></td>
</tr>
</tbody>
</table>

The type \(\text{prod}(\tau₁; \tau₂)\) is sometimes called the \textit{binary product} of the types \(\tau₁\) and \(\tau₂\), and the type \text{unit} is correspondingly called the \textit{nullary product} (of no types). We sometimes speak loosely of \textit{product types} in such a way as to cover both the binary and nullary cases. The introductory form for the product type is called \textit{pairing}, and its eliminatory forms are called \textit{projections}. For the unit type the introductory form is called the \textit{unit element}, or \textit{null tuple}. There is no eliminatory form, there being nothing to extract from a null tuple.

The static semantics of product types is given by the following rules.

\[
\Gamma \vdash \text{triv} : \text{unit}\quad (16.1a)
\]

\[
\Gamma \vdash e₁ : \tau₁ \quad \Gamma \vdash e₂ : \tau₂ \\
\Gamma \vdash \text{pair}(e₁; e₂) : \text{prod}(\tau₁; \tau₂)\quad (16.1b)
\]

\[
\Gamma \vdash e : \text{prod}(\tau₁; \tau₂) \\
\Gamma \vdash \text{proj}[l](e) : \tau₁\quad (16.1c)
\]

\[
\Gamma \vdash e : \text{prod}(\tau₁; \tau₂) \\
\Gamma \vdash \text{proj}[r](e) : \tau₂\quad (16.1d)
\]

The dynamic semantics of product types is specified by the following rules:

\[
\text{triv val}\quad (16.2a)
\]

\[
\{e₁ \text{ val}\} \quad \{e₂ \text{ val}\} \\
\text{pair}(e₁; e₂) \text{ val}\quad (16.2b)
\]

\[
\left\{ \begin{array}{l}
e₁ \mapsto e'₁ \\
\text{pair}(e₁; e₂) \mapsto \text{pair}(e'₁; e₂)
\end{array} \right.\quad (16.2c)
\]
finite products 129

\[
\begin{align*}
\{ e_1 \text{ val } & \quad e_2 \mapsto e'_2 \} \\
\text{pair}(e_1;e_2) \mapsto \text{pair}(e_1;e'_2) \}
\end{align*}
\]

(16.2d)

\[
e \mapsto e'
\]

\[
\text{proj}[l](e) \mapsto \text{proj}[l](e')
\]

(16.2e)

\[
e \mapsto e'
\]

\[
\text{proj}[r](e) \mapsto \text{proj}[r](e')
\]

(16.2f)

\[
\{e_1 \text{ val}\} \quad \{e_2 \text{ val}\}
\]

\[
\text{proj}[l](\text{pair}(e_1;e_2)) \mapsto e_1
\]

(16.2g)

\[
\{e_1 \text{ val}\} \quad \{e_2 \text{ val}\}
\]

\[
\text{proj}[r](\text{pair}(e_1;e_2)) \mapsto e_2
\]

(16.2h)

The bracketed rules and premises are to be omitted for a lazy semantics, and included for an eager semantics of pairing.

The safety theorem applies to both the eager and the lazy dynamics, with the proof proceeding along similar lines in each case.

**Theorem 16.1 (Safety).**

1. If \( e : \tau \) and \( e \mapsto e' \), then \( e' : \tau \).

2. If \( e : \tau \) then either \( e \text{ val} \) or there exists \( e' \) such that \( e \mapsto e' \).

**Proof.** Preservation is proved by induction on transition defined by Rules (16.2). Progress is proved by induction on typing defined by Rules (16.1).

16.2 Finite Products

The syntax of finite product types is given by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>( \tau )</td>
<td>( \prod_{i \in I} \tau_i )</td>
<td>( \prod_{i \in I} \tau_i )</td>
</tr>
<tr>
<td>Expr</td>
<td>( e )</td>
<td>( \langle e_i \rangle_{i \in I} )</td>
<td>( \langle e_i \rangle_{i \in I} )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( \text{proj}[I]<a href="e">i</a> )</td>
<td>( \text{proj}[I]<a href="e">i</a> )</td>
</tr>
</tbody>
</table>

For \( I \) a finite index set of size \( n \geq 0 \), the syntactic form \( \text{prod}[I](i \mapsto \tau_i) \) specifies an \( n \)-argument operator of arity \((0,0,\ldots,0)\) whose \( i \)th argument is the type \( \tau_i \). When it is useful to emphasize the tree structure, such an abt is written in the form \( \prod \langle i_0 : \tau_0, \ldots, i_{n-1} : \tau_{n-1} \rangle \). Similarly, the syntactic form \( \text{tuple}[I](i \mapsto e_i) \) specifies an abt constructed from an \( n \)-argument
operator whose \( i \) operand is \( e_i \). This may alternatively be written in the form \( \langle i_0 : e_0, \ldots, i_{n-1} : e_{n-1} \rangle \).

The static semantics of finite products is given by the following rules:

\[
\begin{align*}
(\forall i \in I) & \quad \Gamma \vdash e_i : \tau_i \\
\Gamma & \vdash \text{tuple}[I](i \mapsto e_i) : \text{prod}[I](i \mapsto \tau_i) \\
\end{align*}
\] (16.3a)

\[
\Gamma \vdash e : \text{prod}[I](i \mapsto e_i) \quad j \in I
\]

\[
\Gamma \vdash \text{proj}[I][j](e) : \tau_j
\] (16.3b)

In Rule (16.3b) the index \( j \in I \) is a particular element of the index set \( I \), whereas in Rule (16.3a), the index \( i \) ranges over the index set \( I \).

The dynamic semantics of finite products is given by the following rules:

\[
\begin{align*}
\{(\forall i \in I) e_i \text{ val}\} & \quad \text{tuple}[I](i \mapsto e_i) \text{ val} \\
\end{align*}
\] (16.4a)

\[
\begin{align*}
\left\{e_j \mapsto e'_j \quad (\forall i \neq j) e'_i = e_i \right\} & \quad \text{tuple}[I](i \mapsto e_i) \mapsto \text{tuple}[I](i \mapsto e'_i) \\
\end{align*}
\] (16.4b)

\[
\begin{align*}
e \mapsto e' \quad \text{proj}[I][j](e) \mapsto \text{proj}[I][j](e') \\
\end{align*}
\] (16.4c)

\[
\begin{align*}
\text{tuple}[I](i \mapsto e_i) \text{ val} & \quad \text{proj}[I][j](\text{tuple}[I](i \mapsto e_i)) \mapsto e_j \\
\end{align*}
\] (16.4d)

Rule (16.4b) specifies that the components of a tuple are to be evaluated in some sequential order, without specifying the order in which they components are considered. It is straightforward, if a bit technically complicated, to impose a linear ordering on index sets that determines the evaluation order of the components of a tuple.

**Theorem 16.2** (Safety). If \( e : \tau \), then either \( e \text{ val} \) or there exists \( e' \) such that \( e' : \tau \) and \( e \mapsto e' \).

**Proof.** The safety theorem may be decomposed into progress and preservation lemmas, which are proved as in Section 16.1 on page 127. \( \square \)

We may define nullary and binary products as particular instances of finite products by choosing an appropriate index set. The type unit may be defined as the product \( \prod_{\varnothing} \varnothing \) of the empty family over the empty index set, taking the expression \( \langle \rangle \) to be the empty tuple, \( \langle \varnothing \rangle_{\varnothing} \). Binary products
16.3 Primitive and Mutual Recursion 131

$\tau_1 \times \tau_2$ may be defined as the product $\prod_{i \in \{1,2\}} \tau_i$ of the two-element family of types consisting of $\tau_1$ and $\tau_2$. The pair $\langle e_1, e_2 \rangle$ may then be defined as the tuple $\langle e_i \rangle_{i \in \{1,2\}}$, and the projections $e \cdot 1$ and $e \cdot 2$ are correspondingly defined, respectively, to be $e \cdot 1$ and $e \cdot 2$.

Finite products may also be used to define labelled tuples, or records, whose components are accessed by symbolic names. If $L = \{ l_1, \ldots, l_n \}$ is a finite set of symbols, called field names, or field labels, then the product type $\prod \langle l_0 : \tau_0, \ldots, l_{n-1} : \tau_{n-1} \rangle$ has as values tuples of the form $\langle l_0 : e_0, \ldots, l_{n-1} : e_{n-1} \rangle$ in which $e_i : \tau_i$ for each $0 \leq i < n$. If $e$ is such a tuple, then $e \cdot l$ projects the component of $e$ labeled by $l \in L$.

16.3 Primitive and Mutual Recursion

Using products we may simplify the primitive recursion construct described in Chapter 14 by avoiding to pass the predecessor itself to the inductive step separately from passing the result of the recursive call on the predecessor. Writing $\text{natiter } e \{ z \Rightarrow e_0 \mid s(x) \Rightarrow e_1 \}$ for this slightly simplified form of the recursor, we may define the original form, $\text{natrec } e \{ z \Rightarrow e_0 \mid s(x_1) \text{ with } x_2 \Rightarrow e_1 \}$, to be the expression $e' \cdot r$, where $e'$ is the expression

$$\text{natiter } e \{ z \Rightarrow \langle z, e_0 \rangle \mid s(x) \Rightarrow \langle s(x \cdot 1), [x \cdot 2, x \cdot 1, x / x_0, x_1] e_1 \rangle \}.$$ 

The idea is to compute inductively both the number, $n$, and the result of the recursive call on $n$, from which we can compute both $n + 1$ and the result of an additional recursion using $e_1$. The base case is computed directly as the pair of zero and $e_0$. It is easy to check that the static and dynamic semantics of the recursor are preserved by this definition.

We may also use product types to implement mutual recursion, which allows several mutually recursive computations to be defined simultaneously. For example, consider the following recursion equations defining two mathematical functions on the natural numbers:

\[
\begin{align*}
E(0) &= 1 \\
O(0) &= 0 \\
E(n + 1) &= O(n) \\
O(n + 1) &= E(n)
\end{align*}
\]

Intuitively, $E(n)$ is non-zero iff $n$ is even, and $O(n)$ is non-zero iff $n$ is odd. If we wish to define these functions in $L\{\text{nat} \rightarrow \}$, we immediately face the

DECEMBER 18, 2009  DRAFT 14:36
problem of how to define two functions simultaneously. There is a trick available in this special case that takes advantage of the fact that \( E \) and \( O \) have the same type: simply define \( \text{eo} \) of type \( \text{nat} \rightarrow \text{nat} \rightarrow \text{nat} \) so that \( \text{eo}(0) \) represents \( E \) and \( \text{eo}(1) \) represents \( O \). (We leave the details as an exercise for the reader.)

A more general solution is to recognize that the definition of two mutually recursive functions may be thought of as the recursive definition of a pair of functions. In the case of the even and odd functions we will define the labelled tuple, \( e_{EO} \), of type, \( \tau_{EO} \), given by

\[
\prod \langle \text{even}: \text{nat} \rightarrow \text{nat}, \text{odd}: \text{nat} \rightarrow \text{nat} \rangle.
\]

From this we will obtain the required mutually recursive functions as the projections \( e_{EO} \cdot \text{even} \) and \( e_{EO} \cdot \text{odd} \).

To effect the mutual recursion the expression \( e_{EO} \) is defined to be

\[
\text{fix this}: \tau_{EO} \text{ is } \langle \text{even}: e_E, \text{odd}: e_O \rangle,
\]

where \( e_E \) is the expression

\[
\lambda (x: \text{nat}. \text{ifz} x \{ z \Rightarrow s(z) \mid s(y) \Rightarrow \text{this} \cdot \text{odd}(y) \}),
\]

and \( e_O \) is the expression

\[
\lambda (x: \text{nat}. \text{ifz} x \{ z \Rightarrow z \mid s(y) \Rightarrow \text{this} \cdot \text{even}(y) \}).
\]

The functions \( e_E \) and \( e_O \) refer to each other by projecting the appropriate component from the variable \( \text{this} \) standing for the object itself. The choice of variable name with which to effect the self-reference is, of course, immaterial, but it is common to use \( \text{this} \) or \( \text{self} \) to emphasize its role.

In the context of so-called object-oriented languages, labelled tuples of mutually recursive functions defined in this manner are called objects, and their component functions are called methods. Component projection is called message passing, viewing the component name as a “message” sent to the object to invoke the method by that name in the object. Internally to the object the methods refer to one another by sending a “message” to \( \text{this} \), the canonical name for the object itself.

### 16.4 Exercises
Chapter 17

Sum Types

Most data structures involve alternatives such as the distinction between a leaf and an interior node in a tree, or a choice in the outermost form of a piece of abstract syntax. Importantly, the choice determines the structure of the value. For example, nodes have children, but leaves do not, and so forth. These concepts are expressed by sum types, specifically the binary sum, which offers a choice of two things, and the nullary sum, which offers a choice of no things. Finite sums generalize nullary and binary sums to permit an arbitrary number of cases indexed by a finite index set. As with products, sums come in both eager and lazy variants, differing in how values of sum type are defined.

17.1 Binary and Nullary Sums

The abstract syntax of sums is given by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>τ</td>
<td>::=</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>void</td>
<td>void</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sum(τ₁; τ₂)</td>
<td>τ₁ + τ₂</td>
</tr>
<tr>
<td>Expr</td>
<td>e</td>
<td>::=</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>abort<a href="e">τ</a></td>
<td>abortₜe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>in[l]<a href="e">τ</a></td>
<td>l·e</td>
</tr>
<tr>
<td></td>
<td></td>
<td>in[r]<a href="e">τ</a></td>
<td>r·e</td>
</tr>
<tr>
<td></td>
<td>case(e; x₁; e₁; x₂; e₂)</td>
<td>case e {l · x₁ ⇒ e₁</td>
<td>r · x₂ ⇒ e₂}</td>
</tr>
</tbody>
</table>

The type void is the nullary sum type, whose values are selected from a choice of zero alternatives — there are no values of this type, and so no introductory forms. The eliminatory form, abort[τ](e), aborts the computation in the event that e evaluates to a value, which it cannot do. The type
\( \tau = \text{sum}(\tau_1; \tau_2) \) is the binary sum. The elements of the sum type are labelled to indicate whether they are drawn from the left or the right summand, either \( \text{in}[1] [\tau] (e) \) or \( \text{in}[r] [\tau] (e) \). A value of the sum type is eliminated by case analysis on the label of the value.

The static semantics of sum types is given by the following rules.

\[
\begin{align*}
\Gamma \vdash e : \text{void} & \quad \Rightarrow \quad \Gamma \vdash \text{abort}[\tau](e) : \tau \\
\Gamma \vdash e : \tau_1 \quad \tau = \text{sum}(\tau_1; \tau_2) & \quad \Rightarrow \quad \Gamma \vdash \text{in}[1][\tau](e) : \tau \\
\Gamma \vdash e : \tau_2 \quad \tau = \text{sum}(\tau_1; \tau_2) & \quad \Rightarrow \quad \Gamma \vdash \text{in}[r][\tau](e) : \tau \\
\Gamma \vdash e : \text{sum}(\tau_1; \tau_2) & \quad \Gamma, x_1 : \tau_1 \vdash e_1 : \tau \quad \Gamma, x_2 : \tau_2 \vdash e_2 : \tau \quad \Rightarrow \quad \Gamma \vdash \text{case}(e; x_1, e_1; x_2, e_2) : \tau
\end{align*}
\]

Both branches of the case analysis must have the same type. Since a type expresses a static “prediction” on the form of the value of an expression, and since a value of sum type could evaluate to either form at run-time, we must insist that both branches yield the same type.

The dynamic semantics of sums is given by the following rules:

\[
\begin{align*}
\text{abort}[\tau](e) & \mapsto \text{abort}[\tau](e') & (17.2a) \\
\{e\} & \mapsto \text{val} & (17.2b) \\
\{e\} & \mapsto \text{val} & (17.2c) \\
\{e\} & \mapsto \text{val} \\
\{e\} & \mapsto \text{val} & (17.2d) \\
\{e\} & \mapsto \text{val} & (17.2e) \\
\text{case}(e; x_1, e_1; x_2, e_2) & \mapsto \text{case}(e'; x_1, e_1; x_2, e_2) & (17.2f) \\
\{e\} & \mapsto \text{val} \\
\text{case}(\text{in}[1][\tau](e); x_1, e_1; x_2, e_2) & \mapsto \text{val} & (17.2g)
\end{align*}
\]
The bracketed premises and rules are to be included for an eager semantics, and excluded for a lazy semantics.

The coherence of the static and dynamic semantics is stated and proved as usual.

**Theorem 17.1** (Safety). 1. If $e : \tau$ and $e \rightarrow e'$, then $e' : \tau$.

2. If $e : \tau$, then either $e \mathit{val}$ or $e \rightarrow e'$ for some $e'$.

**Proof.** The proof proceeds along standard lines, by induction on Rules (17.2) for preservation, and by induction on Rules (17.1) for progress. $\square$

### 17.2 Finite Sums

Just as we may generalize nullary and binary products to finite products, so may we also generalize nullary and binary sums to finite sums. The syntax for finite sums is given by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>$\tau$</td>
<td>$\mathit{sum}[I](i \mapsto \tau_i)$</td>
<td>$\sum_{i \in I} \tau_i$</td>
</tr>
<tr>
<td>Expr</td>
<td>$e$</td>
<td>$\mathit{in}[I]<a href="e">j</a>$</td>
<td>$j \cdot e$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\mathit{case}[I](e; i \mapsto x_i.e_i)$</td>
<td>$\mathit{case} e {i \cdot x_i \mapsto e_i}_{i \in I}$</td>
</tr>
</tbody>
</table>

The abstract binding tree representation of the finite case expression involves an $I$-indexed family of abstractors $x_i.e_i$, but is otherwise similar to the binary form. We write $\sum \{i_0 : \tau_0, \ldots, i_{n-1} : \tau_{n-1}\}$ for $\sum_{i \in I} \tau_i$, where $I = \{i_0, \ldots, i_{n-1}\}$.

The static semantics of finite sums is defined by the following rules:

\[
\begin{align*}
\Gamma \vdash e : \tau_j & \quad j \in I \\
\Gamma \vdash \mathit{in}[I][j](e) : \mathit{sum}[I](i \mapsto \tau_i)
\end{align*}
\] (17.3a)

\[
\begin{align*}
\Gamma \vdash e : \mathit{sum}[I](i \mapsto \tau_i) & \quad (\forall i \in I) \; \Gamma, x_i : \tau_i \vdash e_i : \tau \\
\Gamma \vdash \mathit{case}[I](e; i \mapsto x_i.e_i) : \tau
\end{align*}
\] (17.3b)

These rules generalize to the finite case the static semantics for nullary and binary sums given in Section 17.1 on page 133.
The dynamic semantics of finite sums is defined by the following rules:

\[
\begin{align*}
\text{in}_{[I]}[j](e) & \quad \text{val} \quad (17.4a) \\
\{ e \mapsto e' \} & \quad \text{in}_{[I]}[j](e) \mapsto \text{in}_{[I]}[j](e') \quad (17.4b) \\
\text{case}_{[I]}(e;i \mapsto x_i.e_i) & \quad \text{case}_{[I]}(e';i \mapsto x_i.e_i) \quad (17.4c) \\
\text{in}_{[I]}[j](e) & \quad \text{val} \quad \text{case}_{[I]}(\text{in}_{[I]}[j](e);i \mapsto x_i.e_i) \mapsto [e/x_j]e_j \quad (17.4d)
\end{align*}
\]

These again generalize the dynamic semantics of binary sums given in Section 17.1 on page 133.

**Theorem 17.2** (Safety). If \( e : \tau \), then either \( e \) \text{ val} or there exists \( e' : \tau \) such that \( e \mapsto e' \).

**Proof.** The proof is similar to that for the binary case, as described in Section 17.1 on page 133. \( \square \)

As with products, nullary and binary sums are special cases of the finite form. The type \texttt{void} may be defined to be the sum type \( \sum_{\varepsilon \in \emptyset} \emptyset \) of the empty family of types. The expression \texttt{abort}(e) may corresponding be defined as the empty case analysis, \texttt{case } e \{ \emptyset \}. Similarly, the binary sum type \( \tau_1 + \tau_2 \) may be defined as the sum \( \sum_{i \in I} \tau_i \), where \( I = \{ l, r \} \) is the two-element index set. The binary sum injections \( l \cdot e \) and \( r \cdot e \) are defined to be their counterparts, \( 1 \cdot e \) and \( x \cdot e \), respectively. Finally, the binary case analysis,

\[
\text{case } e \{ 1 \cdot x_1 \Rightarrow e_1 | r \cdot x_r \Rightarrow e_r \},
\]

is defined to be the case analysis, \texttt{case } e \{ i \cdot x_i \Rightarrow \tau_i \}_{i \in I}. It is easy to check that the static and dynamic semantics of sums given in Section 17.1 on page 133 is preserved by these definitions.

Two special cases of finite sums arise quite commonly. The \textit{n-ary sum} corresponds to the finite sum over an index set of the form \( \{ 0, \ldots, n - 1 \} \) for some \( n \geq 0 \). The \textit{labelled sum} corresponds to the case of the index set being a finite set of symbols serving as symbolic indices for the injections.
17.3 Uses for Sum Types

Sum types have numerous uses, several of which we outline here. More interesting examples arise once we also have recursive types, which are introduced in Part VI.

17.3.1 Void and Unit

It is instructive to compare the types unit and void, which are often confused with one another. The type unit has exactly one element, triv, whereas the type void has no elements at all. Consequently, if e : unit, then if e evaluates to a value, it must be unit — in other words, e has no interesting value (but it could diverge). On the other hand, if e : void, then e must not yield a value; if it were to have a value, it would have to be a value of type void, of which there are none. This shows that what is called the void type in many languages is really the type unit because it indicates that an expression has no interesting value, not that it has no value at all!

17.3.2 Booleans

Perhaps the simplest example of a sum type is the familiar type of Booleans, whose syntax is given by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>τ</td>
<td>bool</td>
<td>bool</td>
</tr>
<tr>
<td>Expr</td>
<td>e</td>
<td>tt</td>
<td>tt</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ff</td>
<td>ff</td>
</tr>
<tr>
<td></td>
<td></td>
<td>if(e; e₁; e₂)</td>
<td>if e then e₁ else e₂</td>
</tr>
</tbody>
</table>

The values of type bool are tt and ff. The expression if(e; e₁; e₂) branches on the value of e : bool. We leave a precise formulation of the static and dynamic semantics of this type as an exercise for the reader.

The type bool is definable in terms of binary sums and nullary products:

\[
\text{bool} = \text{sum(unit;unit)} \quad (17.5a) \\
\text{tt} = \text{in[l][bool]}(\text{triv}) \quad (17.5b) \\
\text{ff} = \text{in[r][bool]}(\text{triv}) \quad (17.5c) \\
\text{if}(e; e₁; e₂) = \text{case}(e; x₁.e₁;x₂.e₂) \quad (17.5d)
\]
In the last equation above the variables $x_1$ and $x_2$ are chosen arbitrarily such that $x_1 \notin e_1$ and $x_2 \notin e_2$. (We often write an underscore in place of a variable to stand for a variable that does not occur within its scope.) It is a simple matter to check that the evident static and dynamic semantics of the type `bool` is engendered by these definitions.

### 17.3.3 Enumerations

More generally, sum types may be used to define *finite enumeration* types, those whose values are one of an explicitly given finite set, and whose elimination form is a case analysis on the elements of that set. For example, the type `suit`, whose elements are ♠️, ♦️, ♥️, and ♣️, has as elimination form the case analysis

\[
\text{case } e \{ \text{♠️} \Rightarrow e_0 | \text{♦️} \Rightarrow e_1 | \text{♥️} \Rightarrow e_2 | \text{♣️} \Rightarrow e_3 \},
\]

which distinguishes among the four suits. Such finite enumerations are easily representable as sums. For example, we may define `suit = ∑_{e \in I} \text{unit}`, where $I = \{ ♠️, ♦️, ♥️, ♣️ \}$ and the type family is constant over this set. The case analysis form for a labelled sum is almost literally the desired case analysis for the given enumeration, the only difference being the binding for the uninteresting value associated with each summand, which we may ignore.

### 17.3.4 Options

Another use of sums is to define the *option* types, which have the following syntax:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>$\tau$</td>
<td><code>opt(\tau)</code></td>
<td>$\tau$ <code>opt</code></td>
</tr>
<tr>
<td>Expr</td>
<td>$e$</td>
<td><code>null</code></td>
<td><code>null</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><code>just(e)</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><code>ifnull[\tau](e;e_1;x.e_2)</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>`check e { null \Rightarrow e_1</td>
</tr>
</tbody>
</table>

The type `opt(\tau)` represents the type of “optional” values of type $\tau$. The introductory forms are `null`, corresponding to “no value”, and `just(e)`, corresponding to a specified value of type $\tau$. The elimination form discriminates between the two possibilities.
17.3 Uses for Sum Types

The option type is definable from sums and nullary products according to the following equations:

\[ \text{opt}(\tau) = \text{sum}(\text{unit}; \tau) \]  
\[ \text{null} = \text{in}[l][\text{opt}(\tau)](\text{triv}) \]  
\[ \text{just}(e) = \text{in}[r][\text{opt}(\tau)](e) \]  
\[ \text{ifnull}[\tau](e; e_1; x_2.e_2) = \text{case}(e; e_1; x_2.e_2) \]

(17.6a) (17.6b) (17.6c) (17.6d)

We leave it to the reader to examine the static and dynamic semantics implied by these definitions.

The option type is the key to understanding a common misconception, the null pointer fallacy. This fallacy, which is particularly common in object-oriented languages, is based on two related errors. The first error is to deem the values of certain types to be mysterious entities called pointers, based on suppositions about how these values might be represented at run-time, rather than on the semantics of the type itself. The second error compounds the first. A particular value of a pointer type is distinguished as the null pointer, which, unlike the other elements of that type, does not designate a value of that type at all, but rather rejects all attempts to use it as such.

To help avoid such failures, such languages usually include a function, say \( \text{null} : \tau \rightarrow \text{bool} \), that yields \( \text{tt} \) if its argument is null, and \( \text{ff} \) otherwise. This allows the programmer to take steps to avoid using null as a value of the type it purports to inhabit. Consequently, programs are riddled with conditionals of the form

\[ \text{if null}(e) \text{ then... error ... else... proceed ....} \]

(17.7)

Despite this, “null pointer” exceptions at run-time are rampant, in part because it is quite easy to overlook the need for such a test, and in part because detection of a null pointer leaves little recourse other than abortion of the program.

The underlying problem may be traced to the failure to distinguish the type \( \tau \) from the type \( \text{opt}(\tau) \). Rather than think of the elements of type \( \tau \) as pointers, and thereby have to worry about the null pointer, one instead distinguishes between a genuine value of type \( \tau \) and an optional value of type \( \tau \). An optional value of type \( \tau \) may or may not be present, but, if it is, the underlying value is truly a value of type \( \tau \) (and cannot be null). The elimination form for the option type,

\[ \text{ifnull}[\tau](e; e_{error}; x.e_{ok}) \]

(17.8)
propagates the information that $e$ is present into the non-null branch by binding a genuine value of type $\tau$ to the variable $x$. The case analysis effects a change of type from “optional value of type $\tau$” to “genuine value of type $\tau$”, so that within the non-null branch no further null checks, explicit or implicit, are required. Observe that such a change of type is not achieved by the simple Boolean-valued test exemplified by expression (17.7); the advantage of option types is precisely that it does so.

17.4 Exercises

1. Formulate general $n$-ary sums in terms of nullary and binary sums.

2. Explain why it makes little sense to consider self-referential sum types.
Chapter 18

Pattern Matching

Pattern matching is a natural and convenient generalization of the elimination forms for product and sum types. For example, rather than write

```plaintext
let x be e in x · 1 + x · r
```
to add the components of a pair, e, of natural numbers, we may instead write

```plaintext
match e { x, y, ⟨x, y⟩ ⇒ x + y },
```
using pattern matching to name the components of the pair and refer to them directly. The first argument to the `match` expression is called the `match value` and the second argument consist of a finite sequence of `rules`, separated by vertical bars. In this example there is only one rule, but as we shall see shortly there is, in general, more than one rule in a given `match` expression. Each rule consists of a `pattern`, possibly involving variables, and an `expression` that may involve those variables (as well as any others currently in scope). The value of the `match` is determined by considering each rule in the order given to determine the first rule whose pattern matches the `match value`. If such a rule is found, the value of the `match` is the value of the expression part of the matching rule, with the variables of the pattern replaced by the corresponding components of the `match value`.

Pattern matching becomes more interesting, and useful, when combined with sums. The patterns `l · x` and `r · x` match the corresponding values of sum type. These may be used in combination with other patterns to express complex decisions about the structure of a value. For example, the following `match` expresses the computation that, when given a pair of type `(unit + unit) × nat`, either doubles or squares its second component
depending on the form of its first component:

\[
\text{match } e \{x . (1 \cdot \langle \rangle), x \} \Rightarrow x + x \mid y . (r \cdot \langle \rangle), y \} \Rightarrow y \ast y. \quad (18.1)
\]

It is an instructive exercise to express the same computation using only the primitives for sums and products given in Chapters 16 and 17.

In this chapter we study a simple language, \( L\{\text{pat} \} \), of pattern matching over eager product and sum types.

### 18.1 A Pattern Language

The main challenge in formalizing \( L\{\text{pat} \} \) is to manage properly the binding and scope of variables. The key observation is that a rule, \( p \Rightarrow e \), binds variables in both the pattern, \( p \), and the expression, \( e \), simultaneously. Each rule in a sequence of rules may bind a different number of variables, independently of the preceding or succeeding rules. This gives rise to a somewhat unusual abstract syntax for sequences of rules that permits each rule to have a different valence. For example, the abstract syntax for expression (18.1) is given by

\[
\text{match } e \{r_1; r_2\},
\]

where \( r_1 \) is the rule

\[
x . (1 \cdot \langle \rangle), x \} \Rightarrow x + x
\]

and \( r_2 \) is the rule

\[
y . (r \cdot \langle \rangle), y \} \Rightarrow y \ast y.
\]

The salient point is that each rule binds its own variables, in both the pattern and the expression.

The abstract syntax of \( L\{\text{pat} \} \) is defined by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expr</td>
<td>( e )</td>
<td>( \text{match}(e; rs) )</td>
<td>( \text{match } e {rs} )</td>
</tr>
<tr>
<td>Rules</td>
<td>( rs )</td>
<td>( \text{rules}[!\mid r_1; \ldots; r_n !\mid] )</td>
<td>( r_1 \mid \ldots \mid r_n )</td>
</tr>
<tr>
<td>Rule</td>
<td>( r )</td>
<td>( x_1, \ldots, x_k . \text{rule}(p; e) )</td>
<td>( x_1, \ldots, x_n . p \Rightarrow e )</td>
</tr>
<tr>
<td>Pattern</td>
<td>( p )</td>
<td>( \text{wild} )</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( x )</td>
<td>( x )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( \text{triv} )</td>
<td>( \langle \rangle )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( \text{pair}(p_1; p_2) )</td>
<td>( \langle p_1, p_2 \rangle )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( \text{in}<a href="p">l</a> )</td>
<td>( 1 \cdot p )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( \text{in}<a href="p">r</a> )</td>
<td>( r \cdot p )</td>
</tr>
</tbody>
</table>
The operator rules \( [n] \) has arity \((k_1, \ldots, k_n)\), where \( n \geq 0 \) and, for each \( 1 \leq i \leq n \), the \( i \)th rule has valence \( k_i \geq 0 \). Correspondingly, the \( i \)th rule consists of an abstractor binding \( k_i \) variables in the pattern and expression. A pattern is either a variable, a wild card pattern, a unit pattern matching only the trivial element of the unit type, a pair pattern, or a choice pattern.

18.2 Statics

The static semantics of \( \mathcal{L}\{pat\} \) makes use of a linear hypothetical judgement of the form

\[
\begin{array}{c}
\mathcal{x}_1 : \tau_1, \ldots, \mathcal{x}_k : \tau_k \vdash p : \tau.
\end{array}
\]

The meaning of this judgement is almost the same as that of the ordinary judgement

\[
\begin{array}{c}
\mathcal{x}_1 : \tau_1, \ldots, \mathcal{x}_k : \tau_k \vdash p : \tau,
\end{array}
\]

except that the hypotheses are treated specially so as to ensure that each variable is used exactly once in the pattern. This is achieved by dropping the usual structural rules of weakening and contraction, and limiting the combination of assumptions \( \Lambda_1 \Lambda_2 \) to disjoint sets of assumptions, which is written \( \Lambda_1 \# \Lambda_2 \).

The pattern typing judgement \( \Lambda \vdash p : \tau \) is inductively defined by the following rules:

\[
\frac{}{x : \tau \vdash x : \tau} \quad \text{(18.2a)}
\]

\[
\frac{}{\emptyset \vdash \epsilon : \tau} \quad \text{(18.2b)}
\]

\[
\frac{}{\emptyset \vdash \langle \rangle : \text{unit}} \quad \text{(18.2c)}
\]

\[
\frac{\Lambda_1 \vdash p_1 : \tau_1 \quad \Lambda_2 \vdash p_2 : \tau_2 \quad \Lambda_1 \# \Lambda_2}{\Lambda_1 \Lambda_2 \vdash \langle p_1, p_2 \rangle : \tau_1 \times \tau_2} \quad \text{(18.2d)}
\]

\[
\frac{\Lambda_1 \vdash p : \tau_1}{\Lambda_1 \vdash 1 \cdot p : \tau_1 + \tau_2} \quad \text{(18.2e)}
\]

\[
\frac{\Lambda_2 \vdash p : \tau_2}{\Lambda_2 \vdash \tau \cdot p : \tau_1 + \tau_2} \quad \text{(18.2f)}
\]

Rule (18.2a) states that a variable is a pattern of type \( \tau \) provided that \( x : \tau \) is the only assumption of the judgement. Rule (18.2d) expresses the formation of a pair pattern from patterns for its components, and imposes the
requirement that the variables used in the two sub-patterns must be disjoint, ensuring thereby that no variable may be used more than once in a pattern.

The judgment $x_1, \ldots, x_k. p \Rightarrow e : \tau > \tau'$ states that the rule $x_1, \ldots, x_k. p \Rightarrow e$ matches a value of type $\tau$ against the pattern $p$, binding the variables $x_1, \ldots, x_k$, and yields a value of type $\tau'$.

$$\begin{align*}
\Lambda \vdash p : \tau & \quad \Gamma \vdash e : \tau' \quad \Lambda = x_1 : \tau_1, \ldots, x_k : \tau_k \quad \Gamma \# \Lambda \\
\Gamma \vdash x_1, \ldots, x_k. p \Rightarrow e : \tau > \tau' & (18.3a) \\
\Gamma \vdash r_1 : \tau > \tau' \quad \ldots \quad \Gamma \vdash r_n : \tau > \tau' & (18.3b)
\end{align*}$$

Rule (18.3a) makes use of the pattern typing judgement to determine both the type of the pattern, $p$, and also the types of its variables, $\Lambda$. These variables are available for use within $e$, along with any other variables that may be in scope, without restriction. In Rule (18.3b) if the parameter, $n$, is zero, then the rule states that the empty sequence has an arbitrary domain and range, since it matches no value and yields no result.

Finally, the typing rule for the match expression is given as follows:

$$\begin{align*}
\Gamma \vdash e : \tau & \quad \Gamma \vdash rs : \tau > \tau' \\
\Gamma \vdash \text{match } e \{ rs \} : \tau' & (18.4)
\end{align*}$$

The match expression has type $\tau'$ if the rules transform any value of type $\tau$, the type of the match expression, to a value of type $\tau'$.

### 18.3 Dynamics

The dynamics of pattern matching is defined using substitution to “guess” the bindings of the pattern variables. The dynamics is given by the judgements $e \rightarrow e'$, representing a step of computation, and $e \err$, representing the checked condition of pattern matching failure.

$$\begin{align*}
e \rightarrow e' & (18.5a) \\
\text{match } e \{ rs \} \rightarrow \text{match } e' \{ rs \}
\end{align*}$$

$$\text{match } e \{ \} \err (18.5b)$$

---

1It may help to read the hypotheses, $\Lambda$, as an “output,” rather than as an “input,” of the judgement, in contrast to the usual reading of a hypothetical judgement.
Rule (18.5b) specifies that evaluation results in a checked error once all rules are exhausted. Rules (18.5c) specifies that the rules are to be considered in order. If the match value, \( e \), matches the pattern, \( p_0 \), of the initial rule in the sequence, then the result is the corresponding instance of \( e_0 \); otherwise, matching continues by considering the remaining rules.

**Theorem 18.1 (Preservation).** If \( e \mapsto e' \) and \( e : \tau \), then \( e' : \tau \).

**Proof.** By a straightforward induction on the derivation of \( e \mapsto e' \), making use of the evident substitution lemma for the statics. \( \square \)

The formulation of pattern matching given in Rules (18.5) does not define how pattern matching is to be accomplished, rather it simply checks whether there is substitution for the variables in the pattern that results in the candidate value. This streamlines the presentation of the dynamics and the proof of preservation, but could be considered “too slick” in that it does not show how to find such a substitution or to determine that none exists. This gap may be filled by introducing two judgements. The first,

\[
e_1 \triangleleft x_1, \ldots, e_k \triangleleft x_k \vdash p \triangleleft e,
\]

where \( e \) val and \( e_i \) val for each \( 1 \leq i \leq k \), is a linear hypothetical judgement stating that \([e_1, \ldots, e_k / x_1, \ldots, x_k]p = e\). The second, \( e \perp p \), where \( e \) val, states that \( e \) fails to match the pattern \( p \).

The pattern matching judgement is defined by the following rules, writing \( \Theta \) for the assumptions governing variables:

\[
\frac{}{x \triangleleft e \vdash x \triangleleft e} \quad (18.6a)
\]

\[
\frac{}{\emptyset \vdash \_ \triangleleft e} \quad (18.6b)
\]

\[
\frac{}{\emptyset \vdash \langle \rangle \triangleleft \langle \rangle} \quad (18.6c)
\]
The rules for a pattern mismatch are as follows:

\[ e_1 \perp p_1 \]
\[ \langle e_1, e_2 \rangle \perp \langle p_1, p_2 \rangle \]
\[ e_2 \perp p_2 \]
\[ \langle e_1, e_2 \rangle \perp \langle p_1, p_2 \rangle \]
\[ 1 \cdot e \perp r \cdot p \]
\[ e \perp p \]
\[ 1 \cdot e \perp 1 \cdot p \]
\[ r \cdot e \perp 1 \cdot p \]
\[ e \perp p \]
\[ r \cdot e \perp r \cdot p \]

Neither a variable nor a wildcard nor a null-tuple can mismatch any value of appropriate type. A pair can only mismatch a pair pattern due to a mismatch in one of its components. An injection into a sum type can mismatch the opposite injection, or it can mismatch the same injection by having its argument mismatch the argument pattern.

The salient property of these judgements is that they are complementary.

**Theorem 18.2.** Suppose that \( e : \tau, x_1 : \tau_1, \ldots, x_k : \tau_k \parallel p : \tau, \) and \( e \ val. \) Then either there exists \( e_1, \ldots, e_k \) such that \( x_1 \triangleleft e_1, \ldots, x_k \triangleleft e_k \parallel p \triangleleft e, \) or \( e \perp p. \)

**Proof.** By rule induction on Rules (18.2), making use of the canonical forms lemma to characterize the shape of \( e \) based on its type. \[\square\]
18.4 Exhaustiveness and Redundancy

While it is possible to state and prove a progress theorem for $L\{pat\}$ as defined in Section 18.1 on page 142, it would not have much force, because the statics does not rule out pattern matching failure. What is missing is enforcement of the *exhaustiveness* of a sequence of rules, which ensures that every value of the domain type of a sequence of rules must match some rule in the sequence. In addition it would be useful to rule out *redundancy* of rules, which arises when a rule can only match values that are also matched by a preceding rule. Since pattern matching considers rules in the order in which they are written, such a rule can never be executed, and hence can be safely eliminated.

The statics of rules given in Section 18.1 on page 142 does not ensure exhaustiveness or irredundancy of rules. To do so we introduce a language of *match conditions* that identify a subset of the closed values of a type. With each rule we associate a match condition that classifies the values that are matched by that rule. A sequence of rules is *exhaustive* if every value of the domain type of the rule satisfies the match condition of some rule in the sequence. A rule in a sequence is *redundant* if every value that satisfies its match condition also satisfies the match condition of some preceding rule.

The language of match conditions is defined by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cond</td>
<td>$\xi$</td>
<td>$\text{any} \tau$</td>
<td>$\top \tau$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{in}[l][\text{sum}(\tau_1; \tau_2)][\xi_1]$</td>
<td>$\bot l \cdot \xi_1$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{in}[r][\text{sum}(\tau_1; \tau_2)][\xi_2]$</td>
<td>$\bot r \cdot \xi_2$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{triv}$</td>
<td>$\bot$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{pair}(\xi_1; \xi_2)$</td>
<td>$\langle \xi_1, \xi_2 \rangle$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{nil}[\tau]$</td>
<td>$\bot \tau$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{alt}(\xi_1; \xi_2)$</td>
<td>$\xi_1 \lor \xi_2$</td>
</tr>
</tbody>
</table>

The judgement $\xi : \tau$ is defined by the following rules:

\[
\begin{align*}
\top & : \tau \\
\xi_1 : \tau_1 & \quad \xi_1 : \tau_1 + \tau_2 \\
\bot l \cdot \xi_1 & : \tau_1 + \tau_2 \\
\bot r \cdot \xi_1 & : \tau_1 + \tau_2
\end{align*}
\]
18.4 Exhaustiveness and Redundancy

\[
\langle \rangle : \text{unit} 
\]  
(18.8d)

\[
\begin{align*}
\xi_1 : \tau_1 & \quad \xi_2 : \tau_2 \\
\langle \xi_1, \xi_2 \rangle & : \tau_1 \times \tau_2 
\end{align*} 
\]  
(18.8e)

\[
\bot_\tau : \tau 
\]  
(18.8f)

\[
\begin{align*}
\xi_1 : \tau & \quad \xi_2 : \tau \\
\xi_1 \lor \xi_2 & : \tau 
\end{align*} 
\]  
(18.8g)

Informally, \( \xi : \tau \) means that \( \xi \) constrains values of type \( \tau \).

For \( \xi : \tau \), \( e : \tau \), and \( e \text{ val} \), we define the satisfaction judgement \( e \models \xi \) as follows:

\[
\frac{}{e \models \top_\tau} 
\]  
(18.9a)

\[
\frac{e_1 \models \xi_1}{1 \cdot e_1 \models 1 \cdot \xi_1} 
\]  
(18.9b)

\[
\frac{e_2 \models \xi_2}{x \cdot e_2 \models x \cdot \xi_2} 
\]  
(18.9c)

\[
\frac{}{\langle \rangle \models \langle \rangle} 
\]  
(18.9d)

\[
\frac{e_1 \models \xi_1 \quad e_2 \models \xi_2}{\langle e_1, e_2 \rangle \models \langle \xi_1, \xi_2 \rangle} 
\]  
(18.9e)

\[
\frac{e \models \xi_1}{e \models \xi_1 \lor \xi_2} 
\]  
(18.9f)

\[
\frac{e \models \xi_2}{e \models \xi_1 \lor \xi_2} 
\]  
(18.9g)

The entailment judgement \( \xi_1 \models \xi_2 \), where \( \xi_1 : \tau \) and \( \xi_2 : \tau \), is defined to hold iff \( e \models \xi_1 \) implies \( e \models \xi_2 \).

Finally, we instrument the statics of patterns and rules to associate a match condition that specifies the values that may be matched by that pattern or rule. This allows us to ensure that rules are both exhaustive and irredundant.
The judgement $\Lambda \vdash p : \tau [\xi]$ augments the judgement $\Lambda \vdash p : \tau$ with a match constraint characterizing the set of values of type $\tau$ matched by the pattern $p$. It is inductively defined by the following rules:

$$
\frac{}{x : \tau \vdash x : \tau [\top]} \quad (18.10a)
$$

$$
\frac{}{\emptyset \vdash \_ : \tau [\top]} \quad (18.10b)
$$

$$
\frac{}{\emptyset \vdash \emptyset : \text{unit} [\emptyset]} \quad (18.10c)
$$

$$
\frac{\Lambda_1 \vdash p : \tau_1 [\hat{\xi}_1]}{\Lambda_1 \vdash 1 \cdot p : \tau_1 + \tau_2 [1 \cdot \hat{\xi}_1]} \quad (18.10d)
$$

$$
\frac{\Lambda_2 \vdash p : \tau_2 [\hat{\xi}_2]}{\Lambda_2 \vdash r \cdot p : \tau_1 + \tau_2 [r \cdot \hat{\xi}_2]} \quad (18.10e)
$$

$$
\frac{\Lambda_1 \vdash p_1 : \tau_1 [\hat{\xi}_1] \quad \Lambda_2 \vdash p_2 : \tau_2 [\hat{\xi}_2] \quad \Lambda_1 \# \Lambda_2}{\Lambda_1 \Lambda_2 \vdash \langle p_1, p_2 \rangle : \tau_1 \times \tau_2 [\langle \hat{\xi}_1, \hat{\xi}_2 \rangle]} \quad (18.10f)
$$

Rules (18.10a) to (18.10b) specify that all values of the pattern type are matched. Rule (18.10c) specifies that the only value of type unit is matched by the pattern. Rules (18.10d) to (18.10e) specify that the pattern matches only those values with the specified injection tag and whose argument is matched by the specified pattern. Rule (18.10f) specifies that the pattern matches only pairs whose components match the specified patterns.

The judgement $\Gamma \vdash r : \tau > \tau' [\xi]$ augments the formation judgement for a rule with a match constraint characterizing the pattern component of the rule. The judgement $\Gamma \vdash rs : \tau > \tau' [\xi]$ augments the formation judgement for a sequence of rules with a match constraint characterizing the values matched by some rule in the given rule sequence.

$$
\frac{\Lambda \vdash p : \tau [\xi] \quad \Gamma \vdash e : \tau'}{\Gamma \vdash x_1, \ldots, x_k \cdot p \Rightarrow e : \tau > \tau' [\xi]} \quad (18.11a)
$$

$$
\frac{\Gamma \vdash r_1 : \tau > \tau' [\xi_1] \quad \ldots \quad \Gamma \vdash r_n : \tau > \tau' [\xi_n]}{(\forall 1 \leq i \leq n) \; \xi_i \neq \xi_1 \lor \ldots \lor \xi_{i-1}} \quad (18.11b)
$$

Rule (18.11b) ensures that each successive rule is irredundant relative to the preceding rules in that it demands that it not be the case that every value
satisfying $\xi_i$ satisfies some preceding $\xi_j$. That is, it requires that there be some value satisfying $\xi_i$ that does not satisfy some preceding $\xi_j$.

Finally, the typing rule for match expressions requires exhaustiveness:

$$
\frac{
\Gamma \vdash e : \tau \quad \Gamma \vdash rs : \tau' [\xi] \quad \top_{\tau} \models \xi
}{
\Gamma \vdash \text{match } e \{ rs \} : \tau'
} \quad (18.12)
$$

The third premise ensures that every value of type $\tau$ satisfies the constraint $\xi$ representing the values matched by some rule in the given rule sequence.

The additional constraints on the statics are sufficient to ensure progress, because no well-formed match expression can fail to match a value of the specified type. If a given sequence of rules is inexhaustive, this can always be rectified by including a “default” rule of the form $x. x \Rightarrow e_x$, where $e_x$ handles the unmatched value $x$ gracefully, perhaps by raising an exception (see Chapter 28 for a discussion of exceptions).

**Theorem 18.3.** If $e : \tau$, then either $e \text{ val}$ or there exists $e'$ such that $e \rightarrow e'$.

### 18.5 Exercises
Part VI

Infinite Data Types
Chapter 19

Inductive and Co-Inductive Types

The inductive and the coinductive types are two important classes of recursive types. Inductive types correspond to least, or initial, solutions of certain type isomorphism equations, and coinductive types correspond to their greatest, or final, solutions. Intuitively, the elements of an inductive type are those that may be obtained by a finite composition of its introductory forms. Consequently, if we specify the behavior of a function on each of the introductory forms of an inductive type, then its behavior is determined for all values of that type. Such a function is called a recursor, or catamorphism. Dually, the elements of a coinductive type are those that behave properly in response to a finite composition of its elimination forms. Consequently, if we specify the behavior of an element on each elimination form, then we have fully specified that element as a value of that type. Such an element is called an generator, or anamorphism.

19.1 Motivating Examples

The most important example of an inductive type is the type of natural numbers as formalized in Chapter 14. The type nat is defined to be the least type containing z and closed under s(−). The minimality condition is witnessed by the existence of the recursor, natiter e \{z\to e_0 \mid s(x)\to e_1\}, which transforms a natural number into a value of type τ, given its value for zero, and a transformation from its value on a number to its value on the successor of that number. This operation is well-defined precisely because there are no other natural numbers. Put the other way around, the existence
of this operation expresses the inductive nature of the type \( \text{nat} \).

With a view towards deriving the type \( \text{nat} \) as a special case of an inductive type, it is useful to consolidate zero and successor into a single introductory form, and to correspondingly consolidate the basis and inductive step of the recursor. This following rules specify the static semantics of this reformulation:

\[
\Gamma \vdash e : \text{unit} + \text{nat} \\
\Gamma \vdash \text{foldnat} (e) : \text{nat} 
\]

\[
\Gamma, x : \text{unit} + \tau \vdash e_1 : \tau \\
\Gamma \vdash e_2 : \text{nat} \\
\Gamma \vdash \text{recnat} [x.e_1] (e_2) : \tau
\]

The expression \( \text{foldnat} (e) \) is the unique introductory form of the type \( \text{nat} \). Using this, the expression \( z \) is defined to be \( \text{foldnat} (1 \cdot \langle \rangle) \), and \( s(e) \) is defined to be \( \text{foldnat} (r \cdot e) \). The recursor, \( \text{recnat} [x.e_1] (e_2) \), takes a consolidated basis and inductive step as argument, as well as the natural number of which to recur.

The dynamic semantics of the consolidated primitives is defined by the following rules:

\[
\frac{\text{fold}(e) \text{ val}}{e_2 \mapsto e'_2} 
\]

\[
\frac{\text{recnat} [x.e_1] (e_2) \mapsto \text{recnat} [x.e_1] (e'_2)}{e_b = 1 \cdot \langle \rangle \quad e_s = r \cdot \text{recnat} [x.e_1] (y)} \\
\frac{\text{recnat} [x.e_1] (\text{foldnat} (e_2))}{\mapsto \text{case} e_2 \{1 \cdot \_ \Rightarrow [e_b / x]e_1 \mid r \cdot y \Rightarrow [e_s / x]e_1\}}
\]

Observe that in the successor branch of Rule (19.2c) the recursor is applied to the predecessor before substituting the result into \( e_1 \).

An illustrative example of a coinductive type is the type of \( \text{streams} \) of natural numbers. A stream is an infinite sequence of natural numbers such that nan element of the stream can be computed only after computing all preceding elements in that stream. That is, the computations of successive elements of the stream are sequentially dependent in that the computation of one element influences the computation of the next. This characteristic of the introductory form for streams is dual to the analogous property of the eliminatory form for natural numbers whereby the result for a number is determined by its result for all preceding numbers.
19.1 Motivating Examples

A stream is characterized by its behavior under the elimination forms for the stream type: \( \text{hd}(e) \) returns the next, or head, element of the stream, and \( \text{tl}(e) \) returns the tail of the stream, the stream resulting when the head element is removed. A stream is introduced by a generator, the dual of a recursor, that determines the head and the tail of the stream in terms of the current state of the stream, which is represented by a value of some type. The static semantics of streams is given by the following rules:

\[
\Gamma \vdash e : \text{stream} \\
\Gamma \vdash \text{hd}(e) : \text{nat} \\
\Gamma \vdash e : \text{stream} \\
\Gamma \vdash \text{tl}(e) : \text{stream} \\
\Gamma \vdash e : \tau \\
\Gamma, x : \tau \vdash e_1 : \text{nat} \\
\Gamma, x : \tau \vdash e_2 : \tau \\
\Gamma \vdash \text{strgen} \langle \text{hd}(x) \Rightarrow e_1 \& \text{tl}(x) \Rightarrow e_2 \rangle : \text{stream}
\] (19.3a)

In Rule (19.3c) the current state of the stream is given by the expression \( e \) of some type \( \tau \), and the head and tail of the stream are determined by the expressions \( e_1 \) and \( e_2 \), respectively, as a function of the current state.

The dynamic semantics of the foregoing stream primitives is given by the following rules:

\[
\text{strgen} \langle \text{hd}(x) \Rightarrow e_1 \& \text{tl}(x) \Rightarrow e_2 \rangle \Rightarrow \text{val} \\
\text{val} \Rightarrow e' \\
\text{hd}(e) \Rightarrow \text{hd}(e') \\
\text{tl}(\text{strgen} \langle \text{hd}(x) \Rightarrow e_1 \& \text{tl}(x) \Rightarrow e_2 \rangle) \\
\text{tl}(e) \Rightarrow \text{tl}(e') \\
\text{strgen} \langle e/x \rangle [e_2 \text{hd}(x) \Rightarrow e_1 \& \text{tl}(x) \Rightarrow e_2] \\
\]

(19.4a)

(19.4b)

(19.4c)

(19.4d)

(19.4e)

Rules (19.4c) and (19.4e) express the dependency of the head and tail of the stream on its current state. Observe that the tail is obtained by applying the generator to the new state determined by \( e_2 \) as a function of the current state.
To derive streams as a special case of a coinductive type, we consolidate
the head and the tail into a single eliminatory form, and reorganize the
generator correspondingly. This leads to the following static semantics:

\[
\Gamma \vdash e : \text{stream} \\
\Gamma \vdash \text{unfoldstream}(e) : \text{nat} \times \text{stream}
\]  

(19.5a)

\[
\Gamma, x : \tau \vdash e_1 : \text{nat} \times \tau \quad \Gamma \vdash e_2 : \tau \\
\Gamma \vdash \text{genstream}[(x . e_1)](e_2) : \text{stream}
\]  

(19.5b)

Rule (19.5a) states that a stream may be unfolded into a pair consisting of its
head, a natural number, and its tail, another stream. The head, \( \text{hd}(e) \), and
tail, \( \text{tl}(e) \), of a stream, \( e \), are defined to be the projections \( \text{unfoldstream}(e) \cdot l \) and \( \text{unfoldstream}(e) \cdot r \), respectively. Rule (19.5b) states that a stream
may be generated from the state element, \( e_2 \), by an expression \( e_1 \) that yields
the head element and the next state as a function of the current state.

The dynamic semantics of these primitives is given by the following
rules:

\[
\text{genstream}[(x . e_1)](e_2) \text{ val} \\
\]

(19.6a)

\[
e \mapsto e' \\
\]

(19.6b)

\[
\text{unfoldstream}(e) \mapsto \text{unfoldstream}(e')
\]

(19.6c)

\[
e_h = ([e_2/x]e_1) \cdot l \\
e_t = ([e_2/x]e_1) \cdot r
\]

The generator is applied to the new state component of \( [e_2/x]e_1 \) in Rule (19.6c)
to obtain the tail of the stream.

\section*{19.2 Generic Programming}

A fully general account of inductive and coinductive types requires the
concept of \textit{type-generic}, or just \textit{generic}, programming. A generic program is
one whose behavior is determined by a \textit{type operator}, which is a type
expression with a distinguished type variable. The generic program induced
by a type operator is one that performs a specified operation at each spot
in a data structure corresponding to an occurrence of the type variable in
the operator expression, and otherwise leaves all other parts of the data
structure fixed.
19.2.1 Positive Type Operators

A type operator is an abstractor of the form $t \cdot \tau$ such that $\{ t \} \vdash t \text{ type } \vdash \tau$ type. A type operator is therefore a type, $\tau$, containing zero or more occurrences of a type variable, $t$. The occurrences of $t$ in $\tau$ mark the spots at which we wish to perform some computation, leaving the other spots alone. We may substitute another type, $\sigma$, for occurrences of $t$ in $\tau$ to obtain $[\sigma / t] \tau$, and we may perform a computation transforming values of type $\sigma_1$ into values of type $\sigma_2$ at occurrence of $t$ in $\tau$, thereby transforming a value of type $[\sigma_1 / t] \tau$ into a value of type $[\sigma_2 / t] \tau$. Such a transformation is always possible, provided that $t \cdot \tau$ is a positive type operator, one for which $t$ never occurs within the domain of a function type.

For example, given a transformation, $f$, from values of type $\sigma_1$ to values of type $\sigma_2$, the (positive) type operator $t \cdot \text{unit} + t$ induces a transformation from type $\text{unit} + \sigma_1$ to type $\text{unit} + \sigma_2$ that sends $l \cdot \langle \rangle$ to itself, and $r \cdot e$ to $r \cdot f(e)$. Similarly, the type operator $t \cdot \text{unit} + (\text{nat} \times t)$ induces a transformation from type $\text{unit} + (\text{nat} \times \sigma_1)$ to type $\text{unit} + (\text{nat} \times \sigma_2)$ that sends $l \cdot \langle \rangle$ to itself, and sends $r \cdot \langle e_1, e_2 \rangle$ to $r \cdot \langle e_1, f(e_2) \rangle$. No such transformation is possible for the (non-positive) type operator $t \cdot t \rightarrow t$, because to transform $\sigma_1 \rightarrow \sigma_2$ to $\sigma_2 \rightarrow \sigma_2$ requires a transformation from $\sigma_2$ to $\sigma_1$ as well as one in the other direction.

To make these ideas precise, we define a class of positive type operators to which we associate an action on both types and terms. The positivity judgement, $\Delta \vdash t \cdot \tau \text{ pos}$ is inductively defined by the following rules:

\[
\frac{}{\Delta \vdash t \cdot t \text{ pos}} \quad (19.7a)
\]

\[
\frac{\Delta \vdash u \text{ type } u \neq t}{\Delta \vdash t \cdot u \text{ pos}} \quad (19.7b)
\]

\[
\frac{}{\Delta \vdash t \cdot \text{unit} \text{ pos}} \quad (19.7c)
\]

\[
\frac{\Delta \vdash t \cdot \tau_1 \text{ pos } \Delta \vdash t \cdot \tau_2 \text{ pos}}{\Delta \vdash t \cdot \tau_1 \times \tau_2 \text{ pos}} \quad (19.7d)
\]

\[
\frac{}{\Delta \vdash t \cdot \text{void} \text{ pos}} \quad (19.7e)
\]

\[
\frac{\Delta \vdash t \cdot \tau_1 \text{ pos } \Delta \vdash t \cdot \tau_2 \text{ pos}}{\Delta \vdash t \cdot \tau_1 + \tau_2 \text{ pos}} \quad (19.7f)
\]
In Rule (19.7g), the type variable \( t \) is excluded from the domain of the function type by demanding that it be well-formed without regard to \( t \).

The positivity judgement is preserved under substitution.

**Lemma 19.1.** If \( t \cdot \sigma \) pos and \( u \cdot \tau \) pos, then \( t \cdot [\sigma / u] \tau \) pos.

**Proof.** By rule induction on Rules (19.7). \qed

### 19.2.2 Action of a Positive Type Operator

Positive type operators admit a covariant action, or map operation, that transforms types and expressions in tandem. Specifically, if \( t \cdot \tau \) pos, then

1. If \( \sigma \) type, then \( \text{Map}[t \cdot \tau](\sigma) \) type.

2. If \( x : \sigma_1 \vdash e : \sigma_2 \) and \( \text{map}[t \cdot \tau](x \cdot e) = x' \cdot e' \), then \( x' : \text{Map}[t \cdot \tau](\sigma_1) \vdash e' : \text{Map}[t \cdot \tau](\sigma_2) \).

The action on types is given by substitution:

\[
\text{Map}[t \cdot \tau](\sigma) := [\sigma / t] \tau.
\]

The action of the type operator \( t \cdot \tau \) on an abstraction \( x \cdot e \) transforms an element \( e_1 \) of type \( \text{Map}[t \cdot \tau](\sigma_1) \) into an element of \( e_2 \) of type \( \text{Map}[t \cdot \tau](\sigma_2) \). This is achieved by replacing each sub-expression, \( d \), of \( e_1 \) corresponding to an occurrence of \( t \) in \( \tau \) by the expression \([d / x]e_2\).

For example, consider the type operator

\[
t \cdot \text{unit} + (\text{nat} \times t).
\]

The action of this operator on \( x \cdot e \) such that

\[
x : \sigma_1 \vdash e : \sigma_2
\]

is an abstractor \( x' \cdot e' \) of type

\[
x' : \text{unit} + (\text{nat} \times \sigma_1) \vdash e' : \text{unit} + (\text{nat} \times \sigma_2)
\]

that behaves as described above.
The action of a positive type operator on an abstraction is defined by the judgement
\[ \text{map}[t.\tau](x.e) = x'.e', \]
which is inductively defined by the following rules:

19.8a \[ \text{map}[t.t](x.e) = x.e \]

19.8b \[ u \neq t \quad \text{map}[t.u](x.e) = x.x \]

19.8c \[ \text{map}[t.\text{unit}](x.e) = x'.\langle \rangle \]

19.8d \[ \text{map}[t.\tau_1 \times \tau_2](x.e) = x'.[x' \cdot 1, x' \cdot r/x'_1, x'_2](e'_1, e'_2) \]

19.8e \[ \text{map}[t.\text{void}](x.e) = x'.\text{abort}(x') \]

19.8f \[ \text{map}[t.\tau_1](x_1.e) = x'_1.e'_1 \]
\[ \text{map}[t.\tau_2](x_2.e) = x'_2.e'_2 \]

19.8g \[ \text{map}[t.\tau_1 + \tau_2](x.e) = x'.\text{case } x'\{1 \cdot x'_1 \Rightarrow l \cdot e'_1 | r \cdot x'_2 \Rightarrow r \cdot e'_2\} \]

\[ \text{map}[t.\tau_1 \rightarrow \tau_2](x.e) = x'.\lambda (x'_1 : \tau_1).[x'(x'_1)/x'_2]e'_2 \]

**Lemma 19.2.** Suppose that \( t.\tau \text{ pos. If } x : \sigma \vdash e : \sigma', \text{and } \text{map}[t.\tau](x.e) = x'.e' \), then \( x' : \text{Map}[t.\tau](\sigma) \vdash e' : \text{Map}[t.\tau](\sigma') \).

**Proof.** By rule induction on Rules (19.8).

## 19.3 Static Semantics

We may now give a fully general account of inductive and coinductive types, which are defined in terms of positive type operators. We will consider the language \( \mathcal{L}\{\mu_i \mu_i\} \), which extends \( \mathcal{L}\{\rightarrow \times +\} \) with inductive and co-inductive types.
### 19.3.1 Types

The syntax of inductive and coinductive types involves *type variables*, which are, of course, variables ranging over the class of types. The abstract syntax of inductive and coinductive types is given by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>( \tau )</td>
<td>( t )</td>
<td>( t )</td>
</tr>
<tr>
<td></td>
<td>( \text{ind}(t.\tau) )</td>
<td>( \mu_i(t.\tau) )</td>
<td></td>
</tr>
<tr>
<td></td>
<td>( \text{coi}(t.\tau) )</td>
<td>( \mu_i(t.\tau) )</td>
<td></td>
</tr>
</tbody>
</table>

The subscripts on the inductive and coinductive types stand for "initial" and "final", respectively.

*Type formation* judgements have the form

\[
t_1 \text{ type}, \ldots, t_n \text{ type} \vdash \tau \text{ type},
\]

where \( t_1, \ldots, t_n \) are type names. We let \( \Delta \) range over finite sets of hypotheses of the form \( t \text{ type} \), where \( t \text{ name} \) is a type name. The type formation judgement is inductively defined by the following rules:

\[
\Delta, t \text{ type} \vdash t \text{ type} \quad (19.9a)
\]

\[
\Delta \vdash \text{unit type} \quad (19.9b)
\]

\[
\Delta \vdash \tau_1 \text{ type} \quad \Delta \vdash \tau_2 \text{ type} \quad (19.9c)
\]

\[
\Delta \vdash \text{prod}(\tau_1; \tau_2) \text{ type} \quad (19.9d)
\]

\[
\Delta \vdash \tau_1 \text{ type} \quad \Delta \vdash \tau_2 \text{ type} \quad (19.9e)
\]

\[
\Delta \vdash \text{sum}(\tau_1; \tau_2) \text{ type} \quad (19.9f)
\]

\[
\Delta, t \text{ type} \vdash \tau \text{ type} \quad \Delta \vdash t.\tau \text{ pos} \quad (19.9g)
\]

\[
\Delta, t \text{ type} \vdash \tau \text{ type} \quad \Delta \vdash t.\tau \text{ pos} \quad (19.10)
\]
### 19.3.2 Expressions

The abstract syntax of expressions for inductive and coinductive types is given by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expr</td>
<td>e</td>
<td>::=</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>fold[t.τ] (e)</td>
<td>fold(e)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rec[t.τ][x.τ] (e')</td>
<td>rec [x.e] (e')</td>
</tr>
<tr>
<td></td>
<td></td>
<td>unfold[t.τ] (e)</td>
<td>unfold(e)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>gen[t.τ][x.τ] (e')</td>
<td>gen [x.e] (e')</td>
</tr>
</tbody>
</table>

The expression \(\text{rec}[x.e] (e')\) is called an **recursor**, and the expression \(\text{gen}[x.e] (e')\) is called a **generator**. The expression \(\text{fold}(e)\) is called a **fold** operation, or **constructor**, and \(\text{unfold}(e)\) is called an **unfold** operation, or **destructor**.

The static semantics for inductive and coinductive types is given by the following typing rules:

\[
\Gamma \vdash e : \left[\text{ind}(t.\tau) / t\right] \tau
\]

\[
\Gamma \vdash \text{fold}[t.\tau] (e) : \text{ind}(t.\tau)
\]

\[
\begin{align*}
\Gamma & \vdash e' : \text{ind}(t.\tau) \\
\Gamma & \vdash x : \rho/t \tau \\
\Gamma & \vdash e : \rho
\end{align*}
\]

\[
\Gamma \vdash \text{rec}[t.\tau][x.e] (e') : \rho
\]

\[
\Gamma \vdash \text{unfold}[t.\tau] (e) : \left[\text{coi}(t.\tau) / t\right] \tau
\]

\[
\begin{align*}
\Gamma & \vdash e' : \rho \\
\Gamma & \vdash x : \rho \\
\Gamma & \vdash e : \left[\rho/t\right] \tau
\end{align*}
\]

\[
\Gamma \vdash \text{gen}[t.\tau][x.e] (e') : \text{coi}(t.\tau)
\]

The dynamic semantics of these constructs is given in terms of the action of a positive type operator, which we now define.

### 19.4 Dynamic Semantics

The dynamic semantics of inductive and coinductive types is given in terms of the covariant action of the associated type operator. The following rules specify a lazy dynamics for \(L\{\mu_i \nu_i\}\):

\[
\text{fold}(e) \quad \text{val}
\]

\[
e' \mapsto e'' \\
\text{rec}[x.e] (e') \mapsto \text{rec}[x.e] (e'')
\]
\[
\text{map}[t.\tau](x'.\text{rec}[x.e](x')) = x''.e'' \\
\text{rec}[x.e](\text{fold}(e')) \mapsto [(e'/x'')e''/x]e
\] (19.12c)

\[
\text{gen}[x.e](e') \mapsto \text{val}
\] (19.12d)

\[
e \mapsto e' \\
\text{unfold}(e) \mapsto \text{unfold}(e')
\] (19.12e)

\[
\text{map}[t.\tau](x'.\text{gen}[x.e](x')) = x''.e'' \\
\text{unfold}(\text{gen}[x.e](e')) \mapsto [(e'/x)\text{e'/x'']e'']
\] (19.12f)

Rule (19.12c) states that to evaluate the recursor on a value of recursive type, we inductively apply the recursor as guided by the type operator to the value, and then perform the inductive step on the result. Rule (19.12f) is simply the dual of this rule for coinductive types.

**Lemma 19.3.** If \(e : \tau\) and \(e \mapsto e'\), then \(e' : \tau\).

**Proof.** By rule induction on Rules (19.12). □

**Lemma 19.4.** If \(e : \tau\), then either \(e \text{ val}\) or there exists \(e'\) such that \(e \mapsto e'\).

**Proof.** By rule induction on Rules (19.11). □

Although we shall not give the proof here, the language \(L\{\mu_i\mu_f\}\) is terminating, and all functions defined within it are total.

**Theorem 19.5.** If \(e : \tau\) in \(L\{\mu_i\mu_f\}\), then there exists \(e'\) val such that \(e \mapsto^* e'\).

19.5 Exercises
Chapter 20

General Recursive Types

Inductive and coinductive types may be seen as initial and final solutions to certain forms of recursive type equations. Both the inductive type, \( \mu_i(t.\tau) \), and the coinductive type, \( \mu_f(t.\tau) \), are fixed points of the type operator \( t.\tau \). Thus both are solutions to the recursion equation \( t \cong \tau \) “up to isomorphism” in that both

\[ \mu_i(t.\tau) \cong [\mu_i(t.\tau) / t] \tau \]

and

\[ \mu_f(t.\tau) \cong [\mu_f(t.\tau) / t] \tau. \]

However, inductive and coinductive types provide solutions to type isomorphisms only for positive type operators. In many situations this restriction cannot be met. For example, to model self-reference we require a solution to the type isomorphism \( t \cong t \rightarrow \sigma \) for which the associated type operator \( t.\sigma \) is not positive.

In this chapter we study the language \( \mathcal{L}\{+\times \rightarrow \mu\} \), which provides solutions to general type isomorphism equations, without positivity restrictions. The (general) recursive type \( \mu t.\tau \) is defined to be a solution to the type isomorphism

\[ \mu t.\tau \cong [\mu t.\tau / t] \tau. \]

This is witnessed by the operations

\[ x : \mu t.\tau \vdash \text{unfold}(x) : [\mu t.\tau / t] \tau \]

and

\[ x : [\mu t.\tau / t] \tau \vdash \text{fold}(x) : \mu t.\tau, \]

which are mutually inverse to each other.
Postulating solutions to arbitrary type isomorphism equations may seem suspicious, since we know by Cantor’s Theorem that isomorphisms such as $X \cong \wp(X)$ do not exist, provided that we interpret types as sets and $\wp(X)$ as the set of all subsets of $X$. But rather than presenting a paradox, this observation simply means that types cannot be naively interpreted as sets of values. If we interpret types as classifying potentially undefined computations, rather than as fixed collections of well-defined values, then the proof of Cantor’s Theorem breaks down. Somewhat counterintuitively, the failure of Cantor’s Theorem is precisely what makes type theory so powerful. In particular, we may solve a rich variety of type isomorphisms that are impossible to solve in a set-theoretic setting.

### 20.1 Solving Type Isomorphisms

The recursive type $\mu t.\tau$, where $t.\tau$ is a type operator, represents a solution for $t$ to the isomorphism $t \cong \tau$. The solution is witnessed by two operations, $\text{fold}(e)$ and $\text{unfold}(e)$, that relate the recursive type $\mu t.\tau$ to its unfolding, $[\mu t.\tau/t]\tau$, and serve, respectively, as its introduction and elimination forms.

The language $\mathcal{L}\{+\times\rightarrow\mu\}$ extends $\mathcal{L}\{\rightarrow\}$ with recursive types and their associated operations.

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>$\tau$</td>
<td>$t$</td>
<td>$t$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$</td>
<td>\text{rec}(t.\tau)$</td>
</tr>
<tr>
<td>Expr</td>
<td>$e$</td>
<td>$\text{fold}<a href="e">t.\tau</a>$</td>
<td>$\text{fold}(e)$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{unfold}(e)$</td>
<td>$\text{unfold}(e)$</td>
</tr>
</tbody>
</table>

The expression $\text{fold}(e)$ is the introductory form for the recursive type, and $\text{unfold}(e)$ is its eliminatory form.

The static semantics of $\mathcal{L}\{+\times\rightarrow\mu\}$ consists of two forms of judgement. The first, called type formation, is a general hypothetical judgement of the form

$$T \mid \Delta \vdash \tau \text{ type},$$

where $T = \{t_1, \ldots, t_k\}$ and $\Delta$ is $t_1 \text{ type}, \ldots, t_k \text{ type}$. As usual we drop explicit mention of $T$, relying on typographical conventions to make clear which are the type variables of the judgement.

Type formation is inductively defined by the following rules:

$$\Delta, t \text{ type} \vdash t \text{ type} \quad (20.1a)$$
20.1 Solving Type Isomorphisms 165

\[ \Delta \vdash \tau_1 \text{ type } \quad \Delta \vdash \tau_2 \text{ type} \]
\[ \Delta \vdash \text{arr}(\tau_1; \tau_2) \text{ type} \quad (20.1b) \]

\[ \Delta, t \text{ type} \vdash \tau \text{ type} \]
\[ \Delta \vdash \text{rec}(t.\tau) \text{ type} \quad (20.1c) \]

The second form of judgement comprising the static semantics is the typing judgement, which is a general hypothetical judgement of the form

\[ \mathcal{X} \mid \Gamma \vdash e : \tau, \]

where we assume that \( \tau \) is type. The parameter set, \( \mathcal{X} \), is a finite set of variables, each of which is governed by a typing hypothesis in \( \Gamma \). We ordinarily suppress the parameter set, \( \mathcal{X} \), in favor of relying on the form of \( \Gamma \) to make clear what is intended.

Typing for \( \mathcal{L}\{+ \times \rightarrow \mu\} \) is inductively defined by the following rules:

\[ \Gamma \vdash e : [\text{rec}(t.\tau) / t] \tau \]
\[ \Gamma \vdash \text{fold}[t.\tau](e) : \text{rec}(t.\tau) \quad (20.2a) \]

\[ \Gamma \vdash e : \text{rec}(t.\tau) \]
\[ \Gamma \vdash \text{unfold}(e) : [\text{rec}(t.\tau) / t] \tau \quad (20.2b) \]

The dynamic semantics of \( \mathcal{L}\{+ \times \rightarrow \mu\} \) is specified by one axiom stating that the elimination form is inverse to the introduction form, together with rules specifying the order of evaluation (eager or lazy, according to whether the bracketed rules and premises are included or omitted):

\[ \begin{align*}
\{ e \text{ val} \} \\
\text{fold}[t.\tau](e) \text{ val}
\end{align*} \quad (20.3a) \]

\[ \begin{align*}
\{ e \mapsto e' \\
\text{fold}[t.\tau](e) \mapsto \text{fold}[t.\tau](e')
\end{align*} \quad (20.3b) \]

\[ e \mapsto e' \\
\text{unfold}(e) \mapsto \text{unfold}(e') \quad (20.3c) \]

\[ \text{fold}[t.\tau](e) \text{ val} \\
\text{unfold} \circ \text{fold}[t.\tau](e) \mapsto e \quad (20.3d) \]

Definitional equivalence for \( \mathcal{L}\{+ \times \rightarrow \mu\} \) is the least congruence containing the following rule:

\[ \Gamma \vdash \text{unfold} \circ \text{fold}[t.\tau](e) \equiv e : [\text{rec}(t.\tau) / t] \tau \quad (20.4) \]

It is a straightforward exercise to prove type safety for \( \mathcal{L}\{+ \times \rightarrow \mu\} \).
Theorem 20.1 (Safety).
1. If $e : \tau$ and $e \rightarrow e'$, then $e' : \tau$.
2. If $e : \tau$, then either $e \text{ val}$, or there exists $e'$ such that $e \rightarrow e'$.

20.2 Recursive Data Structures

One important application of recursive types is to the representation of data structures such as lists and trees whose size and content is determined during the course of execution of a program.

One example is the type of natural numbers, which we have taken as primitive in Chapter 15. We may instead treat $\text{nat}$ as a recursive type by thinking of it as a solution (up to isomorphism) of the type equation $t \cong 1 + t$, which is to say that every natural number is either zero or the successor of another natural number. More formally, we may define $\text{nat}$ to be the recursive type

$$
\mu t. [z : \text{unit}, s : t],
$$

which specifies that

$$
\text{nat} \cong [z : \text{unit}, s : \text{nat}].
$$

The zero and successor operations are correspondingly defined by the following equations:

$$
z \equiv \text{fold}(z \cdot \emptyset),
$$

$$
s(e) \equiv \text{fold}(s \cdot e).
$$

The conditional branch on zero is defined by the following equation:

$$
\text{ifz } e \{ z \Rightarrow e_0 \mid s(x) \Rightarrow e_1 \} = \text{case unfold}(e) \{ z \Rightarrow e_0 \mid s \cdot x \Rightarrow e_1 \},
$$

where the “underscore” indicates a variable that does not occur free in $e_0$. It is easy to check that these definitions exhibit the expected behavior in that they correctly simulate the dynamic semantics given in Chapter 15.

As another example, the type $\text{nat list}$ of lists of natural numbers may be represented by the recursive type

$$
\mu t. [n : \text{unit}, c : \text{nat} \times t]
$$

so that we have the isomorphism

$$
\text{nat list} \cong [n : \text{unit}, c : \text{nat} \times \text{nat list}].
$$
The list formation operations are represented by the following equations:

\[
\text{nil} = \text{fold}(n \cdot \langle \rangle) \\
\text{cons}(e_1; e_2) = \text{fold}(c \cdot \langle e_1, e_2 \rangle).
\]

A conditional branch on the form of the list may be defined by the following equation:

\[
\text{listcase } e \{ \text{nil } \Rightarrow e_0 | \text{cons}(x; y) \Rightarrow e_1 \} = \\
\text{case unfold}(e) \{ n \cdot _\_ \Rightarrow e_0, | c \cdot \langle x, y \rangle \Rightarrow e_1 \},
\]

where we have used an underscore for a “don’t care” variable, and used pattern-matching syntax to bind the components of a pair.

There is a natural correspondence between this representation of lists and the conventional “blackboard notation” for linked lists. We may think of \text{fold} as an abstract heap-allocated pointer to a tagged cell consisting of either (a) the tag \( n \) with no associated data, or (b) the tag \( c \) attached to a pair consisting of a natural number and another list, which must be an abstract pointer of the same sort.

### 20.3 Self-Reference

In the general recursive expression, \( \text{fix}[\tau](x.e) \), the variable, \( x \), stands for the expression itself. This is ensured by the unrolling transition

\[
\text{fix}[\tau](x.e) \rightarrow [\text{fix}[\tau](x.e)/x]e,
\]

which substitutes the expression itself for \( x \) in its body during execution. It is useful to think of \( x \) as an implicit argument to \( e \), which is to be thought of as a function of \( x \) that it implicitly implied to the recursive expression itself whenever it is used. In many well-known languages this implicit argument has a special name, such as \text{this} or \text{self}, that emphasizes its self-referential interpretation.

Using this intuition as a guide, we may derive general recursion from recursive types. This derivation shows that general recursion may, like other language features, be seen as a manifestation of type structure, rather than an \textit{ad hoc} language feature. The derivation is based on isolating a type of self-referential expressions of type \( \tau \), written \text{self}(\tau). The introduction form of this type is (a variant of) general recursion, written \text{self}[\tau](x.e), and the elimination form is an operation to unroll the recursion by one step,
written \texttt{unroll}(e). The static semantics of these constructs is given by the following rules:

\[
\begin{align*}
\Gamma, x : \text{self}(\tau) & \vdash e : \tau \\
\Gamma & \vdash \text{self}[\tau](x.e) : \text{self}(\tau) \\
\Gamma & \vdash e : \text{self}(\tau) \\
\Gamma & \vdash \text{unroll}(e) : \tau
\end{align*}
\]  

(20.6a) (20.6b)

The dynamic semantics is given by the following rule for unrolling the self-reference:

\[
\text{self}[\tau](x.e) \xrightarrow{\text{val}} e
\]  

(20.7a)

\[
\text{unroll}(e) \xrightarrow{\text{unroll}} e'
\]  

(20.7b)

\[
\text{unroll}(\text{self}[\tau](x.e)) \xrightarrow{\text{unroll}} \left[ \text{self}[\tau](x.e)/x \right] e
\]  

(20.7c)

The main difference, compared to general recursion, is that we distinguish a type of self-referential expressions, rather than impose self-reference at every type. However, as we shall see shortly, the self-referential type is sufficient to implement general recursion, so the difference is largely one of technique.

The type \text{self}(\tau) is definable from recursive types. As suggested earlier, the key is to consider a self-referential expression of type \tau to be a function of the expression itself. That is, we seek to define the type \text{self}(\tau) so that it satisfies the isomorphism

\[
\text{self}(\tau) \cong \text{self}(\tau) \rightarrow \tau.
\]

This means that we seek a fixed point of the type operator \(t.t \rightarrow \tau\), where \(t \notin \tau\) is a type variable standing for the type in question. The required fixed point is just the recursive type

\[
\text{rec}(t.t \rightarrow \tau),
\]

which we take as the definition of \text{self}(\tau).

The self-referential expression \text{self}[\tau](x.e) is then defined to be the expression

\[
\text{fold}(\lambda (x:\tau \text{self}.e)).
\]

We may easily check that Rule (20.6a) is derivable according to this definition. The expression \text{unroll}(e) is correspondingly defined to be the expression

\[
\text{unfold}(e)(e).
\]
It is easy to check that Rule (20.6b) is derivable from this definition. Moreover, we may check that the definitional equivalence

\[ \text{unroll}(\text{self } y \text{ is } e) \equiv [\text{self } y \text{ is } e/y]e \]

also holds by expanding the definitions and applying the rules of definitional equivalence for recursive types.

This completes the derivation of the type \( \text{self}(\tau) \) of self-referential expressions of type \( \tau \). Using this type we may define general recursion at any type \( \tau \) by simply inserting unrolling operations that are implicit in the semantics of general recursion. Specifically, we may define \( \text{fix } x : \tau \text{ is } e \) to be the expression

\[ \text{unroll}(\text{self } y \text{ is } \{\text{unroll}(y)/x\}e). \]

It is easy to check that this verifies the static semantics of general recursion given in Chapter 15. Moreover, it also validates the dynamic semantics, as evidenced by the following derivation:

\[
\begin{align*}
\text{fix } x : \tau \text{ is } e &= \text{unroll}(\text{self } y \text{ is } [\text{unroll}(y)/x]e) \\
&\equiv [\text{unroll}(\text{self } y \text{ is } [\text{unroll}(y)/x]e)/x]e \\
&= [\text{fix } x : \tau \text{ is } e/x]e.
\end{align*}
\]

By replacing \( x \) in \( e \) by \( \text{unroll}(e) \), and wrapping the entire self-referential expression similarly, we ensure that the self-reference is unrolled implicitly as in Chapter 15, rather than explicitly, as here.

One consequence of this derivation is that adding recursive types to a programming language is a non-conservative extension. For suppose that we add recursive types to a terminating language such as \( \mathcal{L}\{\text{nat} \rightarrow \} \) defined in Chapter 14. The foregoing argument shows that general recursion is definable in this extension, and hence that the termination property of the language has been destroyed. This is in contrast to extensions with, say, product and sum types, which do not disrupt the termination properties of the language. In short, adding new language features (new forms of type) can have subtle, and often surprising, consequences!

### 20.4 Exercises
Part VII

Dynamic Types
Chapter 21

The Untyped $\lambda$-Calculus

Types are the central organizing principle in the study of programming languages. Yet many languages of practical interest are said to be untyped. Have we missed something important? The answer is no! The supposed opposition between typed and untyped languages turns out to be illusory. In fact, untyped languages are special cases of typed languages with a single, pre-determined recursive type. Far from being untyped, such languages are instead uni-typed.\(^1\)

In this chapter we study the premier example of a uni-typed programming language, the (untyped) $\lambda$-calculus. This formalism was introduced by Church in the 1930’s as a universal language of computable functions. It is distinctive for its austere elegance. The $\lambda$-calculus has but one “feature”, the higher-order function, with which to compute. Everything is a function, hence every expression may be applied to an argument, which must itself be a function, with the result also being a function. To borrow a well-worn phrase, in the $\lambda$-calculus it’s functions all the way down!

21.1 The $\lambda$-Calculus

The abstract syntax of $\mathcal{L}\{\lambda\}$ is given by the following grammar:

\begin{center}
\begin{tabular}{llll}
Category & Item & Abstract & Concrete \\
Term & $u$ & $x$ & $x$ \\
& | & $\lambda(x. u)$ & $\lambda x. u$ \\
& | & \text{ap}(u_1; u_2) & $u_1(u_2)$ \\
\end{tabular}
\end{center}

\(^1\)An apt description suggested by Dana Scott.
The second form of expression is called a \( \lambda \)-abstraction, and the third is called application.

The static semantics of \( \mathcal{L}\{\lambda\} \) is defined by general hypothetical judgements of the form \( x_1, \ldots, x_n \vdash x \mathsf{ok} \), stating that \( u \) is a well-formed expression involving the variables \( x_1, \ldots, x_n \). (As usual, we omit explicit mention of the parameters when they can be determined from the form of the hypotheses.) This relation is inductively defined by the following rules:

\[
\begin{align*}
\Gamma, x \mathsf{ok} & \vdash x \mathsf{ok} \quad (21.1a) \\
\Gamma \vdash u_1 \mathsf{ok} & \quad \Gamma \vdash u_2 \mathsf{ok} \\
& \Rightarrow \quad \Gamma \vdash \text{ap}(u_1; u_2) \mathsf{ok} \quad (21.1b) \\
\Gamma, x \mathsf{ok} & \vdash u \mathsf{ok} \\
& \Rightarrow \quad \Gamma \vdash \lambda(x. u) \mathsf{ok} \quad (21.1c)
\end{align*}
\]

The dynamic semantics is given by the following rules:

\[
\begin{align*}
\lambda(x. u) \mathsf{val} & \quad (21.2a) \\
\text{ap}(\lambda(x. u_1); u_2) & \mapsto [u_2/x]u_1 \quad (21.2b) \\
\text{ap}(u_1; u_2) & \mapsto \text{ap}(u'_{1}; u_2) \quad (21.2c)
\end{align*}
\]

In the \( \lambda \)-calculus literature this judgement is called weak head reduction. The first rule is called \( \beta \)-reduction; it defines the meaning of function application as substitution of argument for parameter.

Despite the apparent lack of types, \( \mathcal{L}\{\lambda\} \) is nevertheless type safe!

**Theorem 21.1.** If \( u \mathsf{ok} \), then either \( u \mathsf{val} \), or there exists \( u' \) such that \( u \mapsto u' \) and \( u' \mathsf{ok} \).

**Proof.** Exactly as in preceding chapters. We may show by induction on transition that well-formation is preserved by the dynamic semantics. Since every closed value of \( \mathcal{L}\{\lambda\} \) is a \( \lambda \)-abstraction, every closed expression is either a value or can make progress. \( \square \)

Definitional equivalence for \( \mathcal{L}\{\lambda\} \) is a judgement of the form \( \Gamma \vdash u \equiv u' \), where \( \Gamma = x_1 \mathsf{ok}, \ldots, x_n \mathsf{ok} \) for some \( n \geq 0 \), and \( \varepsilon \) and \( \varepsilon' \) are terms...
having at most the variables \( x_1, \ldots, x_n \) free. It is inductively defined by the following rules:

\[
\frac{\Gamma, u \ ok \vdash u \equiv u}{\Gamma \vdash u \equiv u} \quad (21.3a)
\]

\[
\frac{\Gamma \vdash u \equiv u'}{\Gamma \vdash u' \equiv u} \quad (21.3b)
\]

\[
\frac{\Gamma \vdash u \equiv u', \Gamma \vdash u' \equiv u''}{\Gamma \vdash u \equiv u''} \quad (21.3c)
\]

\[
\frac{\Gamma \vdash e_1 \equiv e_1', \Gamma \vdash e_2 \equiv e_2'}{\Gamma \vdash \text{ap}(e_1; e_2) \equiv \text{ap}(e_1'; e_2')} \quad (21.3d)
\]

\[
\frac{\Gamma, x \ ok \vdash u \equiv u'}{\Gamma \vdash \lambda(x. u) \equiv \lambda(x. u')} \quad (21.3e)
\]

\[
\frac{\Gamma \vdash \text{ap}(\lambda(x. e_2); e_1) \equiv [e_1/x]e_2}{\Gamma \vdash \text{ap}(\lambda(x. e_2); e_1) \equiv [e_1/x]e_2} \quad (21.3f)
\]

We often write just \( u \equiv u' \) when the variables involved need not be emphasized or are clear from context.

### 21.2 Definability

Interest in the untyped \( \lambda \)-calculus stems from its surprising expressive power: it is a *Turing-complete* language in the sense that it has the same capability to expression computations on the natural numbers as does any other known programming language. Church’s Law states that any conceivable notion of computable function on the natural numbers is equivalent to the \( \lambda \)-calculus. This is certainly true for all *known* means of defining computable functions on the natural numbers. The force of Church’s Law is that it postulates that all future notions of computation will be equivalent in expressive power (measured by definability of functions on the natural numbers) to the \( \lambda \)-calculus. Church’s Law is therefore a *scientific law* in the same sense as, say, Newton’s Law of Universal Gravitation, which makes a prediction about all future measurements of the acceleration due to the gravitational field of a massive object.\(^2\)

\(^2\)Unfortunately, it is common in Computer Science to put forth as “laws” assertions that are not scientific laws at all. For example, Moore’s Law is merely an observation about a near-term trend in microprocessor fabrication that is certainly not valid over the long term, and Amdahl’s Law is but a simple truth of arithmetic. Worse, Church’s Law, which is a true scientific law, is usually called *Church’s Thesis*, which, to the author’s ear, suggests something less than the full force of a scientific law.
We will sketch a proof that the untyped $\lambda$-calculus is as powerful as the language PCF described in Chapter 15. The main idea is to show that the PCF primitives for manipulating the natural numbers are definable in the untyped $\lambda$-calculus. This means, in particular, that we must show that the natural numbers are definable as $\lambda$-terms in such a way that case analysis, which discriminates between zero and non-zero numbers, is definable. The principal difficulty is with computing the predecessor of a number, which requires a bit of cleverness. Finally, we show how to represent general recursion, completing the proof.

The first task is to represent the natural numbers as certain $\lambda$-terms, called the Church numerals.

$$
\bar{0} = \lambda b. \lambda s. b
$$

$$
\bar{n + 1} = \lambda b. \lambda s. s (\bar{n} (b) (s))
$$

It follows that

$$
\bar{n} (u_1) (u_2) \equiv u_2 (\ldots (u_2 (u_1)))
$$

the $n$-fold application of $u_2$ to $u_1$. That is, $\bar{n}$ iterates its second argument (the induction step) $n$ times, starting with its first argument (the basis).

Using this definition it is not difficult to define the basic functions of arithmetic. For example, successor, addition, and multiplication are defined by the following untyped $\lambda$-terms:

$$\text{succ} = \lambda x. \lambda b. \lambda s. s (x (b) (s))$$

$$\text{plus} = \lambda x. \lambda y. y (x) (\text{succ})$$

$$\text{times} = \lambda x. \lambda y. y (\bar{0}) ((\text{plus} (x)))$$

It is easy to check that $\text{succ} (\bar{n}) \equiv \bar{n + 1}$, and that similar correctness conditions hold for the representations of addition and multiplication.

We may readily define $\text{ifz} (u; u_0; u_1)$ to be the application $u (u_0) (\lambda u. u_1)$, where the underscore stands for a dummy variable chosen apart from $u_1$. We can use this to define $\text{ifz} (u; u_0; x. u_1)$, provided that we can compute the predecessor of a natural number. Doing so requires a bit of ingenuity. We wish to find a term $\text{pred}$ such that

$$\text{pred} (\bar{0}) \equiv \bar{0}$$

$$\text{pred} (\bar{n + 1}) \equiv \bar{n}.$$

To compute the predecessor using Church numerals, we must show how to compute the result for $\bar{n + 1}$ as a function of its value for $\bar{n}$. At first glance
this seems straightforward—just take the successor—until we consider the base case, in which we define the predecessor of \(0\) to be \(0\). This invalidates the obvious strategy of taking successors at inductive steps, and necessitates some other approach.

What to do? A useful intuition is to think of the computation in terms of a pair of “shift registers” satisfying the invariant that on the \(n\)th iteration the registers contain the predecessor of \(n\) and \(n\) itself, respectively. Given the result for \(n\), namely the pair \((n - 1, n)\), we pass to the result for \(n + 1\) by shifting left and incrementing to obtain \((n, n + 1)\). For the base case, we initialize the registers with \((0, 0)\), reflecting the stipulation that the predecessor of zero be zero. To compute the predecessor of \(n\) we compute the pair \((n - 1, n)\) by this method, and return the first component.

To make this precise, we must first define a Church-style representation of ordered pairs.

\[
\langle u_1, u_2 \rangle = \lambda f. f (u_1) (u_2) \tag{21.10}
\]

\[
u \cdot 1 = u (\lambda x. \lambda y. x) \tag{21.11}
\]

\[
u \cdot x = u (\lambda x. \lambda y. y) \tag{21.12}
\]

It is easy to check that under this encoding \(\langle u_1, u_2 \rangle \cdot 1 \equiv u_1\), and similarly for the second projection. We may now define the required term \(u\) representing the predecessor:

\[
u'_p = \lambda x. x (\langle 0, 0 \rangle) (\lambda y. \langle y \cdot r, s (y \cdot r) \rangle) \tag{21.13}
\]

\[
u_p = \lambda x. u (x) \cdot 1 \tag{21.14}
\]

It is then easy to check that this gives us the required behavior. Finally, we may define \(\text{ifz}(u; u_0; x)\) \(u_1\) to be the untyped term

\[
u (u_0) (\lambda \omega [u_p (u) / x] u_1).
\]

This gives us all the apparatus of PCF, apart from general recursion. But this is also definable using a fixed point combinator. There are many choices of fixed point combinator, of which the best known is the \(Y\) combinator:

\[
Y = \lambda F. (\lambda f. F (f (f))) (\lambda f. F (f (f))). \tag{21.15}
\]

Observe that

\[
Y (F) \equiv F (Y (F)).
\]

Using the \(Y\) combinator, we may define general recursion by writing \(Y (\lambda x. u)\), where \(x\) stands for the recursive expression itself.

DECEMBER 18, 2009 DRAFT 14:36
21.3 Scott’s Theorem

Definitional equivalence for the untyped λ-calculus is undecidable: there is no algorithm to determine whether or not two untyped terms are definitionally equivalent. The proof of this result is based on two key lemmas:

1. For any untyped λ-term u, we may find an untyped term v such that
   \[ u(\overline{\nu}) \equiv v, \]
   where \( \overline{\nu} \) is the Gödel number of \( v \), and \( \overline{\nu} \) is its representation as a Church numeral. (See Chapter 14 for a discussion of Gödel-numbering.)

2. Any two non-trivial\(^3\) properties \( A_0 \) and \( A_1 \) of untyped terms that respect definitional equivalence are inseparable. This means that there is no decidable property \( B \) of untyped terms such that \( A_0 \ u \) implies that \( B \ u \) and \( A_1 \ u \) implies that it is not the case that \( B \ u \). In particular, if \( A_0 \) and \( A_1 \) are inseparable, then neither is decidable.

For a property \( B \) of untyped terms to respect definitional equivalence means that if \( B \ u \) and \( u \equiv u' \), then \( B \ u' \).

**Lemma 21.2.** For any \( u \) there exists \( v \) such that \( u(\overline{\nu}) \equiv v \).

**Proof Sketch.** The proof relies on the definability of the following two operations in the untyped λ-calculus:

1. \( \text{ap}(\overline{\nu_1})(\overline{\nu_2}) \equiv \overline{\nu_1(\nu_2)} \).
2. \( \text{nm}(\overline{n}) \equiv \overline{n} \).

Intuitively, the first takes the representations of two untyped terms, and builds the representation of the application of one to the other. The second takes a numeral for \( n \), and yields the representation of \( \overline{n} \). Given these, we may find the required term \( v \) by defining \( v = w(\overline{\nu}) \), where \( w = \lambda x. u(\text{ap}(x)(\text{nm}(x))) \). We have

\[
v = w(\overline{\nu}) \\
\equiv u(\text{ap}(\overline{\nu})(\text{nm}(\overline{\nu}))) \\
\equiv u(\overline{w(\overline{\nu})}) \\
\equiv u(\overline{v}).
\]

---

\(^3\)A property of untyped terms is said to be trivial if it either holds for all untyped terms or never holds for any untyped term.
The definition is very similar to that of $Y(u)$, except that $u$ takes as input the representation of a term, and we find a $v$ such that, when applied to the representation of $v$, the term $u$ yields $v$ itself. □

**Lemma 21.3.** Suppose that $A_0$ and $A_1$ are two non-vacuous properties of untyped terms that respect definitional equivalence. Then there is no untyped term $w$ such that

1. For every $u$ either $w(\bar{\Gamma}u^\perp) \equiv \bar{0}$ or $w(\bar{\Gamma}u^\perp) \equiv \bar{1}$.
2. If $A_0 u$, then $w(\bar{\Gamma}u^\perp) \equiv \bar{0}$.
3. If $A_1 u$, then $w(\bar{\Gamma}u^\perp) \equiv \bar{1}$.

**Proof.** Suppose there is such an untyped term $w$. Let $v$ be the untyped term $\lambda x.\text{ifz}(w(x);u_1;u_0)$, where $A_0 u_0$ and $A_1 u_1$. By Lemma 21.2 on the facing page there is an untyped term $t$ such that $v(\bar{\Gamma}t^\perp) \equiv t$. If $w(\bar{\Gamma}t^\perp) \equiv \bar{0}$, then $t \equiv v(\bar{\Gamma}t^\perp) \equiv u_1$, and so $A_1 t$, since $A_1$ respects definitional equivalence and $A_1 u_1$. But then $w(\bar{\Gamma}t^\perp) \equiv \bar{1}$ by the defining properties of $w$, which is a contradiction. Similarly, if $w(\bar{\Gamma}t^\perp) \equiv \bar{1}$, then $A_0 t$, and hence $w(\bar{\Gamma}t^\perp) \equiv \bar{0}$, again a contradiction. □

**Corollary 21.4.** There is no algorithm to decide whether or not $u \equiv u'$.

**Proof.** For fixed $u$ consider the property $E_u u'$ defined by $u' \equiv u$. This is non-vacuous and respects definitional equivalence, and hence is undecidable. □

### 21.4 Untyped Means Uni-Typed

The untyped $\lambda$-calculus may be faithfully embedded in the typed language $L\{+\times\rightarrow\mu\}$, enriched with recursive types. This means that every untyped $\lambda$-term has a representation as an expression in $L\{+\times\rightarrow\mu\}$ in such a way that execution of the representation of a $\lambda$-term corresponds to execution of the term itself. If the execution model of the $\lambda$-calculus is call-by-name, this correspondence holds for the call-by-name variant of $L\{+\times\rightarrow\mu\}$, and similarly for call-by-value. It is important to understand that this form of embedding is not a matter of writing an interpreter for the $\lambda$-calculus in $L\{+\times\rightarrow\mu\}$ (which we could
surely do), but rather a direct representation of untyped λ-terms as certain typed expressions of \( L\{ + \times \rightarrow \mu \} \). It is for this reason that we say that untyped languages are just a special case of typed languages, provided that we have recursive types at our disposal.

The key observation is that the untyped λ-calculus is really the uni-typed λ-calculus! It is not the absence of types that gives it its power, but rather that it has only one type, namely the recursive type

\[
D = \mu t. t \rightarrow t.
\]

A value of type \( D \) is of the form \( \text{fold}(e) \) where \( e \) is a value of type \( D \rightarrow D \) — a function whose domain and range are both \( D \). Any such function can be regarded as a value of type \( D \) by “rolling”, and any value of type \( D \) can be turned into a function by “unrolling”. As usual, a recursive type may be seen as a solution to a type isomorphism equation, which in the present case is the equation

\[
D \cong D \rightarrow D.
\]

This specifies that \( D \) is a type that is isomorphic to the space of functions on \( D \) itself, something that is impossible in conventional set theory, but is feasible in the computationally-based setting of the λ-calculus.

This isomorphism leads to the following embedding, \( u^\dagger \), of \( u \) into \( L\{ + \times \rightarrow \mu \} \):

\[
\begin{align*}
x^\dagger &= x \tag{21.16a} \\
\lambda x. u^\dagger &= \text{fold}(\lambda (x: D. u^\dagger)) \tag{21.16b} \\
u_1(u_2)^\dagger &= \text{unfold}(u_1^\dagger)(u_2^\dagger) \tag{21.16c}
\end{align*}
\]

Observe that the embedding of a λ-abstraction is a value, and that the embedding of an application exposes the function being applied by unrolling the recursive type. Consequently,

\[
\begin{align*}
\lambda x. u_1(u_2)^\dagger &= \text{unfold}(\text{fold}(\lambda (x: D. u_1^\dagger))) (u_2^\dagger) \\
&\equiv \lambda (x: D. u_1^\dagger) (u_2^\dagger) \\
&\equiv [u_2^\dagger/x]u_1^\dagger \\
&= ([u_2/x]u_1)^\dagger.
\end{align*}
\]

The last step, stating that the embedding commutes with substitution, is easily proved by induction on the structure of \( u_1 \). Thus \( \beta \)-reduction is faithfully implemented by evaluation of the embedded terms.
Thus we see that the canonical untyped language, \( \mathcal{L}\{\lambda}\), which by dint of terminology stands in opposition to typed languages, turns out to be but a typed language after all! Rather than eliminating types, an untyped language consolidates an infinite collection of types into a single recursive type. Doing so renders static type checking trivial, at the expense of incurring substantial dynamic overhead to coerce values to and from the recursive type. In Chapter 22 we will take this a step further by admitting many different types of data values (not just functions), each of which is a component of a “master” recursive type. This shows that so-called dynamically typed languages are, in fact, statically typed. Thus a traditional distinction can hardly be considered an opposition, since dynamic languages are but particular forms of static language in which (undue) emphasis is placed on a single recursive type.

21.5 Exercises
Chapter 22

Dynamic Typing

We saw in Chapter 21 that an untyped language may be viewed as a untyped language in which the so-called untyped terms are terms of a distinguished recursive type. In the case of the untyped $\lambda$-calculus this recursive type has a particularly simple form, expressing that every term is isomorphic to a function. Consequently, no run-time errors can occur due to the misuse of a value—the only elimination form is application, and its first argument can only be a function. Obviously this property breaks down once more than one class of value is permitted into the language. For example, if we add natural numbers as a primitive concept to the untyped $\lambda$-calculus (rather than defining them via Church encodings), then it is possible to incur a run-time error arising from attempting to apply a number to an argument, or to add a function to a number.

One school of thought in language design is to turn this vice into a virtue by embracing a model of computation that has multiple classes of value of a single type. Such languages are said to be \emph{dynamically typed}, in supposed opposition to the \emph{statically typed} languages we have studied thus far. In this chapter we show that the supposed opposition between static and dynamic languages is fallacious: dynamic typing is but a mode of use of static typing, and, moreover, it is profitably seen as such. Dynamic typing can hardly be in opposition to that of which it is a special case!

22.1 Dynamically Typed PCF

To illustrate dynamic typing we formulate a dynamically typed version of $\mathcal{L}\{\text{nat} \to\}$, called $\mathcal{L}\{\text{dyn}\}$. The abstract syntax of $\mathcal{L}\{\text{dyn}\}$ is given by the
following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expr</td>
<td>$d := x$</td>
<td>$x$</td>
<td>$x$</td>
</tr>
<tr>
<td></td>
<td>$\text{num}(\bar{n})$</td>
<td>$\bar{n}$</td>
<td>$\bar{n}$</td>
</tr>
<tr>
<td></td>
<td>$\text{zero}$</td>
<td>$\text{zero}$</td>
<td>$\text{zero}$</td>
</tr>
<tr>
<td></td>
<td>$\text{succ}(d)$</td>
<td>$\text{succ}(d)$</td>
<td>$\text{succ}(d)$</td>
</tr>
<tr>
<td></td>
<td>$\text{ifz}(d; d_0; x \cdot d_1)$</td>
<td>$\text{ifz}(d { \text{zero} \Rightarrow d_0 \mid \text{succ}(x) \Rightarrow d_1 })$</td>
<td>$\text{ifz}(d { \text{zero} \Rightarrow d_0 \mid \text{succ}(x) \Rightarrow d_1 })$</td>
</tr>
<tr>
<td></td>
<td>$\text{fun}(\lambda(x \cdot d))$</td>
<td>$\lambda x . d$</td>
<td>$\lambda x . d$</td>
</tr>
<tr>
<td></td>
<td>$\text{dap}(d_1; d_2)$</td>
<td>$d_1(d_2)$</td>
<td>$d_1(d_2)$</td>
</tr>
<tr>
<td></td>
<td>$\text{fix}(x \cdot d)$</td>
<td>$\text{fix} x \text{is} d$</td>
<td>$\text{fix} x \text{is} d$</td>
</tr>
</tbody>
</table>

There are two classes of values in $L\{\text{dyn}\}$, the numbers, which have the form $\bar{n}$,\(^1\) and the functions, which have the form $\lambda x . d$. The elimination forms of $L\{\text{dyn}\}$ operate on classified values, and must check that their arguments are of the appropriate class at run-time. The expressions $\text{zero}$ and $\text{succ}(d)$ are not in themselves values, but rather are operations that evaluate to classified values, as we shall see shortly.

The concrete syntax of $L\{\text{dyn}\}$ is somewhat deceptive, in keeping with common practice in dynamic languages. For example, the concrete syntax for a number is a bare numeral, $\bar{n}$, but in fact it is just a convenient notation for the classified value, $\bar{n}$, of class $\text{num}$. Similarly, the concrete syntax for a function is a bare $\lambda$-abstraction, $\lambda x . d$, which must be regarded as standing for the classified value $\lambda x . d$ of class $\text{fun}$. It is the responsibility of the parser to translate the surface syntax into the abstract syntax, adding class information to values in the process.

The static semantics of $L\{\text{dyn}\}$ is essentially the same as that of $L\{\lambda\}$ given in Chapter 21: it merely checks that there are no free variables in the expression. The judgement

$$x_1 \text{ ok}, \ldots, x_n \text{ ok} \vdash d \text{ ok}$$

states that $d$ is a well-formed expression with free variables among those in the hypothesis list.

The dynamic semantics for $L\{\text{dyn}\}$ checks for errors that would never arise in a safe statically typed language. For example, function application must ensure that its first argument is a function, signaling an error in the case that it is not, and similarly the case analysis construct must ensure that its first argument is a number, signaling an error if not. The reason for

\(^1\)The numerals, $\bar{n}$, are $n$-fold compositions of the form $s(s(\ldots s(z) \ldots))$. 

14:36 DRAFT DECEMBER 18, 2009
having classes labelling values is precisely to make this run-time check possible. One could argue that the required check may be made by inspection of the unlabelled value itself, but this is unrealistic. At run-time both numbers and functions might be represented by machine words, the former a two’s complement number, the latter an address in memory. But given an arbitrary word, one cannot determine whether it is a number or an address!

The value judgement, \( d \text{ val} \), states that \( d \) is a fully evaluated (closed) expression:

\[
\frac{}{\text{num}(\overline{n}) \text{ val}} (22.1a)
\]

\[
\frac{}{\text{fun}(\lambda (x. d) \text{ val}} (22.1b)
\]

The dynamic semantics makes use of judgements that check the class of a value, and recover the underlying \( \lambda \)-abstraction in the case of a function.

\[
\frac{}{\text{num}(\overline{n}) \text{ is_num } \overline{n}} (22.2a)
\]

\[
\frac{}{\text{fun}(\lambda (x. d) \text{ is_fun } \lambda (x. d)} (22.2b)
\]

The second argument of each of these judgements has a special status—it is not an expression of \( \mathcal{L}\{\text{dyn}\} \), but rather just a special piece of syntax used internally to the transition rules given below.

We also will need the “negations” of the class-checking judgements in order to detect run-time type errors.

\[
\frac{}{\text{num}(\_.) \text{ isnt_fun}} (22.3a)
\]

\[
\frac{}{\text{fun}(\_.) \text{ isnt_num}} (22.3b)
\]

The transition judgement, \( d \rightarrow d' \), and the error judgement, \( d \text{ err} \), are defined simultaneously by the following rules.

\[
\frac{}{\text{zero} \rightarrow \text{num}(z)} (22.4a)
\]

\[
\frac{}{d \rightarrow d' \quad \text{succ}(d) \rightarrow \text{succ}(d')} (22.4b)
\]

\[
\frac{d \text{ is_num } \overline{n}}{\text{succ}(d) \rightarrow \text{num}(s(\overline{n}))} (22.4c)
\]

\[
\frac{d \text{ isnt_num}}{\text{succ}(d) \text{ err}} (22.4d)
\]
\[
\begin{align*}
\text{ifz}(d; d_0; x.d_1) &\rightarrow \text{ifz}(d'; d_0; x.d_1) \\
\text{if} &\text{z(d; d;0; } x.d_1) \rightarrow d_0 \\
\text{if} &\text{z(d; d;0; } x.d_1) \rightarrow [\text{num(n)}]/x.d_1 \\
\text{if} &\text{z(d; d;0; } x.d_1) \rightarrow \text{err} \\
\text{dap(d; d_2; d_1) } &\rightarrow \text{dap(d; d_2; d_1)} \\
\text{dap(d; d_2; d_1) } &\rightarrow [d_2/x]d_1 \\
\text{dap(d; d_2; d_1) } &\rightarrow \text{err} \\
\text{fix(x.d) } &\rightarrow [\text{fix(x.d)}]/x.d 
\end{align*}
\]
22.2 Critique of Dynamic Typing

The safety of $L\{\text{dyn}\}$ is often promoted as an advantage of dynamic over static typing. Unlike static languages, essentially every piece of abstract syntax has a well-defined dynamic semantics. But this can also be seen as a disadvantage, since errors that could be ruled out at compile time by type checking are not signalled until run time in $L\{\text{dyn}\}$. To make this possible, the dynamic semantics of $L\{\text{dyn}\}$ incurs significant overhead to enforce the classification of values.

Consider, for example, the addition function in $L\{\text{dyn}\}$, whose specification is that, when passed two values of class num, returns their sum, which is also of class num:

$$
\text{fun}(\lambda(x.\text{fix }p \text{ is } \lambda(y.\text{if } z(y;x;y'.\text{succ}(\text{dap}(p;y'))))))).
$$

The addition function may, deceptively, be written in concrete syntax as follows:

$$
\lambda x.\text{fix } p \text{ is } \lambda y.\text{if } z(y;x;\text{succ}(\text{dap}(p;y'))).
$$

It is deceptive, because the concrete syntax obscures the class tags on values, and obscures the use of primitives that check those tags. Let us now examine the costs of these operations in a bit more detail.

First, observe that the body of the fixed point expression is labelled with class fun. The semantics of the fixed point construct binds $p$ to this function. This means that the dynamic class check incurred by the application of $p$ in the recursive call is guaranteed to succeed. But $L\{\text{dyn}\}$ offers no means of suppressing this redundant check, because it cannot express the invariant that $p$ is always bound to a value of class fun.

Second, observe that the result of applying the inner $\lambda$-abstraction is either $x$, the argument of the outer $\lambda$-abstraction, or the successor of a recursive call to the function itself. The successor operation checks that its argument is of class num, even though this is guaranteed for all but the base case, which returns the given $x$, which can be of any class at all. In principle we can check that $x$ is of class num once, and observe that it is otherwise a loop invariant that the result of applying the inner function is of this class. However, $L\{\text{dyn}\}$ gives us no way to express this invariant; the

---

2This specification imposes no restrictions on the behavior of addition on arguments that are not classified as numbers, but one could make the further demand that the function abort when applied to arguments that are not classified by num.
repeated, redundant tag checks imposed by the successor operation cannot be avoided.

Third, the argument, \( y \), to the inner function is either the original argument to the addition function, or is the predecessor of some earlier recursive call. But as long as the original call is to a value of class \( \text{num} \), then the semantics of the conditional will ensure that all recursive calls have this class. And again there is no way to express this invariant in \( \mathcal{L}\{\text{dyn}\} \), and hence there is no way to avoid the class check imposed by the conditional branch.

Classification is not free—storage is required for the class label, and it takes time to detach the class from a value each time it is used and to attach a class to a value whenever it is created. Although the overhead of classification is not asymptotically significant (it slows down the program only by a constant factor), it is nevertheless non-negligible, and should be eliminated whenever possible. But this is impossible within \( \mathcal{L}\{\text{dyn}\} \), because it cannot enforce the restrictions required to express the required invariants. For that we need a static type system!

### 22.3 Hybrid Typing

Consider the language \( \mathcal{L}\{\text{nat dyn } \Rightarrow} \), which extends \( \mathcal{L}\{\text{nat } \Rightarrow} \) (defined in Chapter 15) with the following additional constructs:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>( \tau )</td>
<td>( \text{dyn} )</td>
<td>( \text{dyn} )</td>
</tr>
<tr>
<td>Expr</td>
<td>( e )</td>
<td>( \text{new}<a href="e">\text{l}</a> )</td>
<td>( \text{l} \ ! e )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( \text{cast}<a href="e">\text{l}</a> )</td>
<td>( e \ ? \text{l} )</td>
</tr>
<tr>
<td>Class</td>
<td>( l )</td>
<td>( \text{num} )</td>
<td>( \text{num} )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( \text{fun} )</td>
<td>( \text{fun} )</td>
</tr>
</tbody>
</table>

The type \( \text{dyn} \) represents the type of dynamically classified values. (Here we have only two classes of data, numbers and functions, but a richer language would have many more possibilities.) The \text{new} operation attaches a classifier to a value, and the \text{cast} operation checks the classifier and returns the associated value. It is important to note that the cast operation checks the \text{class}, not the \text{type}, of its argument.

The static semantics for \( \mathcal{L}\{\text{nat dyn } \Rightarrow} \) extends that of \( \mathcal{L}\{\text{nat } \Rightarrow} \) with the following additional rules:

\[
\Gamma \vdash e : \text{nat} \\
\Gamma \vdash \text{new}[\text{num}](e) : \text{dyn}
\]  

(22.5a)
22.3 Hybrid Typing

The static semantics ensures that class labels are applied to objects of the appropriate type, namely `num` for natural numbers, and `fun` for functions defined over labelled values.

The dynamic semantics of $L\{\text{nat dyn} \mapsto \}$ extends that of $L\{\text{nat} \mapsto \}$ with the following rules:

\[
\begin{align*}
\Gamma \vdash e : \text{parr(dyn; dyn)} \\
\Gamma \vdash \text{new[fun]}(e) : \text{dyn} \\
\Gamma \vdash e : \text{dyn} \\
\Gamma \vdash \text{cast[fun]}(e) : \text{parr(dyn; dyn)}
\end{align*}
\]

(Casting compares the class of the object to the required class, returning the underlying object if these coincide, and signalling an error otherwise.

**Lemma 22.2 (Canonical Forms).** If $e : \text{dyn}$ and $e \text{ val}$, then $e = \text{new[l]}(e')$ for some class $l$ and some $e'$ val. If $l = \text{num}$, then $e' : \text{nat}$, and if $l = \text{fun}$, then $e' : \text{parr(dyn; dyn)}$.

**Proof.** By a straightforward rule induction on static semantics of $L\{\text{nat dyn} \mapsto \}$.

**Theorem 22.3 (Safety).** The language $L\{\text{nat dyn} \mapsto \}$ is safe:

1. If $e : \tau$ and $e \mapsto e'$, then $e' : \tau$.
2. If $e : \tau$, then either $e \text{ val}$, or $e \text{ err}$, or $e \mapsto e'$ for some $e'$.
Proof. Preservation is proved by rule induction on the dynamic semantics, and progress is proved by rule induction on the static semantics, making use of the canonical forms lemma. The opportunities for run-time errors are the same as those for $\mathcal{L}^{\text{dyn}}$—a well-typed cast might fail at run-time if the class of the case does not match the class of the value. 

### 22.4 Optimization of Dynamic Typing

The language $\mathcal{L}\{\text{nat dyn} \rightarrow\}$ combines static and dynamic typing by enriching $\mathcal{L}\{\text{nat} \rightarrow\}$ with the type, dyn, of classified values. It is, for this reason, called a hybrid language. The advantage of the hybrid type system is that it allows us to express invariants that are crucial to the optimization of programs in $\mathcal{L}\{\text{dyn}\}$.

Let us examine how this plays out in the case of the addition function, which may be rendered in $\mathcal{L}\{\text{nat dyn} \rightarrow\}$ by the expression

$$\text{fun ! } \lambda (x : \text{dyn}. \text{fix } p : \text{dyn} \text{ is fun ! } \lambda (y : \text{dyn}. e_{x,p,y})), $$

where

$$x : \text{dyn}, p : \text{dyn}, y : \text{dyn} \vdash e_{x,p,y} : \text{dyn}$$

is defined to be the expression

$$\text{ifz } (y \text{ ? num}) \{ \text{zero } \Rightarrow x | \text{succ } (y') \Rightarrow \text{num ! } (s((p \text{ ? fun})(\text{num ! } y') \text{ ? num})) \}.$$

This is a re-formulation of the dynamic addition function given in Section 22.2 on page 187 in which we have made explicit the checking and imposition of classes on values. We will exploit the static type system of $\mathcal{L}\{\text{nat dyn} \rightarrow\}$ to optimize this dynamically typed implementation of addition in accordance with the specification given in Section 22.2 on page 187.

First, note that the body of the fix expression is an explicitly labelled function. This means that when the recursion is unwound, the variable $p$ is bound to this value of type dyn. Consequently, the check that $p$ is labelled with class fun is redundant, and can be eliminated. This is achieved by re-writing the function as follows:

$$\text{fun ! } \lambda (x : \text{dyn}. \text{fun ! fix } p : \text{dyn} \rightarrow \text{dyn} \text{ is fun ! } \lambda (y : \text{dyn}. e'_{x,p,y})), $$

---

3But as we shall see in Section 22.6 on page 193, it is simply a statically typed language with a distinguished recursive type.
where \( e'_{x,p,y} \) is the expression

\[
\text{ifz } (y \text{ ? num}) \begin{cases} \text{zero} \Rightarrow x \text{ | succ}(y') \Rightarrow \text{num} \text{ ! } (s(p(\text{num} ! y') \text{ ? num})) \end{cases}.
\]

We have “hoisted” the function class label out of the loop, and suppressed the cast inside the loop. Correspondingly, the type of \( p \) has changed to \( \text{dyn} \rightarrow \text{dyn} \), reflecting that the body is now a “bare function”, rather than a labelled function value of type \( \text{dyn} \).

Next, observe that the parameter \( y \) of type \( \text{dyn} \) is cast to a number on each iteration of the loop before it is tested for zero. Since this function is recursive, the bindings of \( y \) arise in one of two ways, at the initial call to the addition function, and on each recursive call. But the recursive call is made on the predecessor of \( y \), which is a true natural number that is labelled with \( \text{num} \) at the call site, only to be removed by the class check at the conditional on the next iteration. This suggests that we hoist the check on \( y \) outside of the loop, and avoid labelling the argument to the recursive call. Doing so changes the type of the function, however, from \( \text{dyn} \rightarrow \text{dyn} \) to \( \text{nat} \rightarrow \text{dyn} \). Consequently, further changes are required to ensure that the entire function remains well-typed.

Before doing so, let us make another observation. The result of the recursive call is checked to ensure that it has class \( \text{num} \), and, if so, the underlying value is incremented and labelled with class \( \text{num} \). If the result of the recursive call came from an earlier use of this branch of the conditional, then obviously the class check is redundant, because we know that it must have class \( \text{num} \). But what if the result came from the other branch of the conditional? In that case the function returns \( x \), which need not be of class \( \text{num} \! \). However, one might reasonably insist that this is only a theoretical possibility—after all, we are defining the addition function, and its arguments might reasonably be restricted to have class \( \text{num} \). This can be achieved by replacing \( x \) by \( x \text{ ? num} \), which checks that \( x \) is of class \( \text{num} \), and returns the underlying number.

Combining these optimizations we obtain the inner loop \( e''_x \) defined as follows:

\[
\text{fix } p : \text{nat} \rightarrow \text{nat} \text{ is } \lambda (y : \text{nat}. \text{ifz } y \begin{cases} \text{zero} \Rightarrow x \text{ | succ}(y') \Rightarrow \text{num} \text{ ! } (s(p(\text{num} ! y') \text{ ? num})) \end{cases}).
\]

This function has type \( \text{nat} \rightarrow \text{nat} \), and runs at full speed when applied to a natural number—all checks have been hoisted out of the inner loop.

Finally, recall that the overall goal is to define a version of addition that works on values of type \( \text{dyn} \). Thus we require a value of type \( \text{dyn} \rightarrow \text{dyn} \), but what we have at hand is a function of type \( \text{nat} \rightarrow \text{nat} \). This can be
converted to the required form by pre-composing with a cast to \texttt{num} and post-composing with a coercion to \texttt{num}:

\[
\text{fun } \lambda (x:\texttt{dyn} \to \texttt{fun} \to \texttt{nat}) \lambda (y:\texttt{dyn} \to \texttt{num}) (e''(y \to \texttt{num}))).
\]

The innermost \(\lambda\)-abstraction converts the function \(e''\) from type \(\texttt{nat} \to \texttt{nat}\) to type \(\texttt{dyn} \to \texttt{dyn}\) by composing it with a class check that ensures that \(y\) is a natural number at the initial call site, and applies a label to the result to restore it to type \(\texttt{dyn}\).

### 22.5 Static “Versus” Dynamic Typing

There have been many attempts to explain the distinction between dynamic and static typing, most of which are misleading or wrong. For example, it is often said that static type systems associate types with variables, but dynamic type systems associate types with values. This oft-repeated characterization appears to be justified by the absence of type annotations on \(\lambda\)-abstractions, and the presence of classes on values. But it is based on a confusion of classes with types—the \texttt{class} of a value (\texttt{num} or \texttt{fun}) is not its \texttt{type}. Moreover, a static type system assigns types to values just as surely as it does to variables, so the description fails on this account as well. Thus, this supposed distinction between dynamic and static typing makes no sense, and is best disregarded.

Another way to differentiate dynamic from static languages is to say that whereas static languages check types at compile time, dynamic languages check types at run time. While this description seems superficially accurate, it does not bear scrutiny. To say that static languages check types statically is to state a tautology, and to say that dynamic languages check types at run-time is to utter a falsehood. Dynamic languages perform \texttt{class checking}, not \texttt{type checking}, at run-time. For example, application checks that its first argument is labelled with \texttt{fun}; it does not type check the body of the function. Indeed, at no point does the dynamic semantics compute the \texttt{type} of a value, rather it checks its class against its expectations before proceeding. Here again, a supposed contrast between static and dynamic languages evaporates under careful analysis.

Another characterization is to assert that dynamic languages admit \textit{heterogeneous} lists, whereas static languages admit only \textit{homogeneous} lists. (The distinction applies to other collections as well.) To see why this description is wrong, let us consider briefly how one might add lists to \(L\{\texttt{dyn}\}\). One would add two constructs, \texttt{nil}, representing the empty list, and \texttt{cons}(\(d_1; d_2\),...
representing the non-empty list with head \( d_1 \) and tail \( d_2 \). The origin of the supposed distinction lies in the observation that each element of a list represented in this manner might have a different class. For example, one might form the list

\[
\text{cons}(s(z);\text{cons}(\lambda x.x;\text{nil})),
\]

whose first element is a number, and whose second element is a function. Such a list is said to be heterogeneous. In contrast static languages commit to a single type for each element of the list, and hence are said to be homogeneous. But here again the supposed distinction breaks down on close inspection, because it is based on the confusion of the type of a value with its class. Every labelled value has type \( \text{dyn} \), so that the lists are type homogeneous. But since values of type \( \text{dyn} \) may have different classes, lists are class heterogeneous—regardless of whether the language is statically or dynamically typed!

What, then, are we to make of the traditional distinction between dynamic and static languages? Rather than being in opposition to each other, we see that dynamic languages are a mode of use of static languages. If we have a type \( \text{dyn} \) in the language, then we have all of the apparatus of dynamic languages at our disposal, so there is no loss of expressive power. But there is a very significant gain from embedding dynamic typing within a static type discipline! We can avoid much of the overhead of dynamic typing by simply limiting our use of the type \( \text{dyn} \) in our programs, as was illustrated in Section 22.4 on page 190.

### 22.6 Dynamic Typing From Recursive Types

The type \( \text{dyn} \) codifies the use of dynamic typing within a static language. Its introduction form labels an object of the appropriate type, and its elimination form is a (possibly undefined) casting operation. Rather than treating \( \text{dyn} \) as primitive, we may derive it as a particular use of recursive types, according to the following definitions:\(^4\)

\[
\begin{align*}
\text{dyn} & = \mu t \cdot [\text{num}:\text{nat}, \text{fun}: t \rightarrow t] \\
\text{new}[\text{num}](e) & = \text{fold}(\text{num} \cdot e) \\
\text{new}[\text{fun}](e) & = \text{fold}(\text{fun} \cdot e)
\end{align*}
\]

\(^4\) Here we have made use of a special expression \( \text{error} \) to signal an error condition. In a richer language we would use exceptions, which are introduced in Chapter 28.
cast[num](e) = case unfold(e) {num · x ⇒ x | fun · x ⇒ error}  \hspace{1cm} (22.10)
cast[fun](e) = case unfold(e) {num · x ⇒ error | fun · x ⇒ x}  \hspace{1cm} (22.11)

One may readily check that the static and dynamic semantics for the type \texttt{dyn} are derivable according to these definitions.

This encoding shows that we need not include a special-purpose type \texttt{dyn} in a statically typed language in order to admit dynamic typing. Instead, one may use the general concepts of recursive types and sum types to define special-purpose dynamically typed sub-languages on a per-program basis. For example, if we wish to admit strings into our dynamic sub-language, then we may simply expand the type definition above to admit a third summand for strings, and so on for any type we may wish to consider. Classes emerge as labels of the summands of a sum type, and recursive types ensure that we can represent class-heterogeneous aggregates. Thus, not only is dynamic typing a special case of static typing, but we need make no special provision for it in a statically typed language, since we already have need of recursive types independently of this particular application.

### 22.7 Exercises
Part VIII

Variable Types
Chapter 23

Girard’s System F

The languages we have considered so far are all monomorphic in that every expression has a unique type, given the types of its free variables, if it has a type at all. Yet it is often the case that essentially the same behavior is required, albeit at several different types. For example, in \( \mathcal{L}\{\text{nat} \rightarrow \} \) there is a distinct identity function for each type \( \tau \), namely \( \lambda (x: \tau. x) \), even though the behavior is the same for each choice of \( \tau \). Similarly, there is a distinct composition operator for each triple of types, namely

\[
\circ_{\tau_1, \tau_2, \tau_3} = \lambda (f: \tau_2 \rightarrow \tau_3. \lambda (g: \tau_1 \rightarrow \tau_2. \lambda (x: \tau_1. f (g(x))))).
\]

Each choice of the three types requires a different program, even though they all exhibit the same behavior when executed.

Obviously it would be useful to capture the general pattern once and for all, and to instantiate this pattern each time we need it. The expression patterns codify generic (type-independent) behaviors that are shared by all instances of the pattern. Such generic expressions are said to be polymorphic. In this chapter we will study a language introduced by Girard under the name System F and by Reynolds under the name polymorphic typed \( \lambda \)-calculus. Although motivated by a simple practical problem (how to avoid writing redundant code), the concept of polymorphism is central to an impressive variety of seemingly disparate concepts, including the concept of data abstraction (the subject of Chapter 24), and the definability of product, sum, inductive, and coinductive types considered in the preceding chapters. (Only general recursive types extend the expressive power of the language.)
23.1 System F

System F, or the polymorphic \(\lambda\)-calculus, or \(\mathcal{L}\{\to \forall}\), is a minimal functional language that illustrates the core concepts of polymorphic typing, and permits us to examine its surprising expressive power in isolation from other language features. The syntax of System F is given by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>(\tau)</td>
<td>(\tau)</td>
<td>(\tau)</td>
</tr>
<tr>
<td></td>
<td>(\text{arr}(\tau_1; \tau_2))</td>
<td>(\tau_1 \to \tau_2)</td>
<td>(\tau_1 \to \tau_2)</td>
</tr>
<tr>
<td></td>
<td>(\text{all}(t.\tau))</td>
<td>(\forall(t.\tau))</td>
<td>(\forall(t.\tau))</td>
</tr>
<tr>
<td>Expr</td>
<td>(e)</td>
<td>(x)</td>
<td>(x)</td>
</tr>
<tr>
<td></td>
<td>(\text{lam}<a href="x.e">\tau</a>)</td>
<td>(\lambda(x:\tau.e))</td>
<td>(\lambda(x:\tau.e))</td>
</tr>
<tr>
<td></td>
<td>(\text{ap}(e_1; e_2))</td>
<td>(e_1(e_2))</td>
<td>(e_1(e_2))</td>
</tr>
<tr>
<td></td>
<td>(\text{Lam}(t.e))</td>
<td>(\Lambda(t.e))</td>
<td>(\Lambda(t.e))</td>
</tr>
<tr>
<td></td>
<td>(\text{App}<a href="e">\tau</a>)</td>
<td>(e[\tau])</td>
<td>(e[\tau])</td>
</tr>
</tbody>
</table>

The meta-variable \(t\) ranges over a class of type variables, and \(x\) ranges over a class of expression variables. The type abstraction, \(\text{Lam}(t.e)\), defines a generic, or polymorphic, function with type parameter \(t\) standing for an unspecified type within \(e\). The type application, or instantiation, \(\text{App}[\tau](e)\), applies a polymorphic function to a specified type, which is then plugged in for the type parameter to obtain the result. Polymorphic functions are classified by the universal type, \(\text{all}(t.\tau)\), that determines the type, \(\tau\), of the result as a function of the argument, \(t\).

The static semantics of \(\mathcal{L}\{\to \forall}\) consists of two judgement forms, the type formation judgement,

\[ T \mid \Delta \vdash \tau \text{ type}, \]

and the typing judgement,

\[ T, \chi \mid \Delta, \Gamma \vdash e : \tau. \]

These are generic judgements over the parameter set \(T\) of type variables and the parameter set \(\chi\) of expression variables. They are also hypothetical in a set \(\Delta\) of type assumptions of the form \(t \text{ type}\), where \(t \in T\), and typing assumptions of the form \(x : \tau\), where \(x \in T\) and \(\Delta \vdash \tau \text{ type}\). As usual we drop explicit mention of the parameter sets, relying on typographical conventions to determine them.

The rules defining the type formation judgement are as follows:

\[ \Delta, t \text{ type} \vdash t \text{ type} \quad (23.1a) \]
Lemma 23.1 (Regularity). If $\Delta, t \vdash \tau$ type and $\Delta \vdash \tau_i$ type for each assumption $x_i : \tau_i$ in $\Gamma$, then $\Delta \vdash \tau$ type.

Proof. By induction on Rules (23.2).

The static semantics admits the structural rules for a general hypothetical judgement. In particular, we have the following critical substitution property for type formation and expression typing.

Lemma 23.2 (Substitution). 1. If $\Delta, t \vdash \tau'$ type and $\Delta \vdash \tau$ type, then $\Delta \vdash [\tau / t] \tau'$ type.

2. If $\Delta, t \vdash e' : \tau'$ and $\Delta \vdash \tau$ type, then $\Delta \vdash [\tau / t] [\tau / t] e' : [\tau / t] \tau'$.

3. If $\Delta, x : \tau \vdash e' : \tau'$ and $\Delta \vdash e : \tau$, then $\Delta \vdash [e / x] e' : \tau'$.

The second part of the lemma requires substitution into the context, $\Gamma$, as well as into the term and its type, because the type variable $t$ may occur freely in any of these positions.
Returning to the motivating examples from the introduction, the polymorphic identity function, $I$, is written

$$\Lambda (t. \lambda (x : t). x);$$

it has the polymorphic type

$$\forall (t . t \rightarrow t).$$

Instances of the polymorphic identity are written $I[\tau]$, where $\tau$ is some type, and have the type $\tau \rightarrow \tau$.

Similarly, the polymorphic composition function, $C$, is written

$$\Lambda (t_1. \Lambda (t_2. \Lambda (t_3. \lambda (f : t_2 \rightarrow t_3. \lambda (g : t_1 \rightarrow t_2. \lambda (x : t_1. f (g (x))))))).)$$

The function $C$ has the polymorphic type

$$\forall (t_1 . \forall (t_2 . \forall (t_3 . (t_2 \rightarrow t_3) \rightarrow (t_1 \rightarrow t_2) \rightarrow (t_1 \rightarrow t_3))))).$$

Instances of $C$ are obtained by applying it to a triple of types, writing $C[\tau_1][\tau_2][\tau_3]$. Each such instance has the type

$$(\tau_2 \rightarrow \tau_3) \rightarrow (\tau_1 \rightarrow \tau_2) \rightarrow (\tau_1 \rightarrow \tau_3).$$

**Dynamic Semantics**

The dynamic semantics of $\mathcal{L}\{\rightarrow \forall\}$ is given as follows:

$$\begin{align*}
\lambda (\tau) (x . e) & \quad \text{val} \quad (23.3a) \\
\Lambda (t . e) & \quad \text{val} \quad (23.3b) \\
ap (\lambda (\tau_1) (x . e); e_2) & \rightarrow [e_2/x]e \quad (23.3c) \\
\begin{array}{c}
e_1 \mapsto e'_1 \\
ap (e_1; e_2) & \mapsto [e'_1; e_2] \\
ap (\tau) (\Lambda (t . e)) & \mapsto [\tau/t]e \quad (23.3e) \\
\end{array} \\
\begin{array}{c}
e \mapsto e' \\
ap (\tau) (e) & \mapsto [e'] \\
\end{array} \quad (23.3f)
\end{align*}$$

These rules endow $\mathcal{L}\{\rightarrow \forall\}$ with a call-by-name interpretation of application, but one could as well consider a call-by-value variant.

It is a simple matter to prove safety for $\mathcal{L}\{\rightarrow \forall\}$, using familiar methods.
23.2 Polymorphic Definability

Lemma 23.3 (Canonical Forms). Suppose that $e : \tau$ and $e \text{ val}$, then

1. If $\tau = \text{arr}(\tau_1; \tau_2)$, then $e = \text{lam}[\tau_1](x.e_2)$ with $x : \tau_1 \vdash e_2 : \tau_2$.

2. If $\tau = \text{all}(t. \tau')$, then $e = \text{Lam}(t. e')$ with $t \text{ type} \vdash e' : \tau'$.

**Proof.** By rule induction on the static semantics. \hfill \square

Theorem 23.4 (Preservation). If $e : \sigma$ and $e \hookrightarrow e'$, then $e' : \sigma$.

**Proof.** By rule induction on the dynamic semantics. \hfill \square

Theorem 23.5 (Progress). If $e : \sigma$, then either $e \text{ val}$ or there exists $e'$ such that $e \hookrightarrow e'$.

**Proof.** By rule induction on the static semantics. \hfill \square

23.2 Polymorphic Definability

The language $\mathcal{L}\{\rightarrow \forall\}$ is astonishingly expressive. Not only are all finite products and sums definable in the language, but so are all inductive and coinductive types, including both the eager and the lazy natural numbers! This is most naturally expressed using definitional equivalence, which is defined to be the least congruence containing the following two axioms:

$$
\frac{\Delta \Gamma, x : \tau_1 \vdash e : \tau_2 \quad \Delta \Gamma \vdash e_1 : \tau_1}{\Delta \Gamma \vdash \lambda(x : \tau. e_2)(e_1) \equiv [e_1/x]e_2 : \tau_2} \quad (23.4a)
$$

$$
\frac{\Delta, t \text{ type} \Gamma \vdash e : \tau \quad \Delta \vdash \sigma \text{ type}}{\Delta \Gamma \vdash \Lambda(t.e)[\sigma] \equiv [\sigma/t]e : [\sigma/t]\tau} \quad (23.4b)
$$

The remaining rules specify that definitional equivalence is reflexive, symmetric, and transitive, and that it is compatible with both forms of application and abstraction.
23.2 Polymorphic Definability

23.2.1 Products and Sums

The nullary product, or unit, type is definable in $L_{\rightarrow \forall}$ as follows:

\[ \text{unit} = \forall (r, r \rightarrow r) \]
\[ \langle \rangle = \Lambda (r, \lambda (x: r, x)) \]

It is easy to check that the static semantics given in Chapter 16 is derivable. There being no elimination rule, there is no requirement on the dynamic semantics.

Binary products are definable in $L_{\rightarrow \forall}$ by using encoding tricks similar to those described in Chapter 21 for the untyped $\lambda$-calculus:

\[ \tau_1 \times \tau_2 = \forall (r, (\tau_1 \rightarrow \tau_2 \rightarrow r) \rightarrow r) \]
\[ \langle e_1, e_2 \rangle = \Lambda (r, \lambda (x: \tau_1, \lambda (y: \tau_2, x) (e_1) (e_2))) \]
\[ e \cdot 1 = e [\tau_1] (\lambda (x: \tau_1, \lambda (y: \tau_2, x))) \]
\[ e \cdot r = e [\tau_2] (\lambda (x: \tau_1, \lambda (y: \tau_2, y))) \]

The static semantics given in Chapter 16 is derivable according to these definitions. Moreover, the following definitional equivalences are derivable in $L_{\rightarrow \forall}$ from these definitions:

\[ \langle e_1, e_2 \rangle \cdot 1 \equiv e_1 : \tau_1 \]

and

\[ \langle e_1, e_2 \rangle \cdot r \equiv e_2 : \tau_2. \]

The nullary sum, or void, type is definable in $L_{\rightarrow \forall}$:

\[ \text{void} = \forall (r, r) \]
\[ \text{abort} [\rho] (e) = e [\rho] \]

There is no definitional equivalence to be checked, there being no introductory rule for the void type.

Binary sums are also definable in $L_{\rightarrow \forall}$:

\[ \tau_1 + \tau_2 = \forall (r, (\tau_1 \rightarrow r) \rightarrow (\tau_2 \rightarrow r) \rightarrow r) \]
\[ 1 \cdot e = \Lambda (r, \lambda (x: \tau_1, \lambda (y: \tau_2, r, x (e)))) \]
\[ r \cdot e = \Lambda (r, \lambda (x: \tau_1, \lambda (y: \tau_2, r, y (e)))) \]
\[ \text{case } e \{ 1 \cdot x_1 \Rightarrow e_1 \mid r \cdot x_2 \Rightarrow e_2 \} = \]
\[ e [\rho] (\lambda (x_1: \tau_1, e_1) (\lambda (x_2: \tau_2, e_2))) \]
23.2 Polymorphic Definability

provided that the types make sense. It is easy to check that the following equivalences are derivable in \( L\{\to \forall\} \):

\[
\text{case } l \cdot d \{ l \cdot x_1 \Rightarrow e_1 \mid r \cdot x_2 \Rightarrow e_2 \} \equiv [e/x_1]e_1 : \rho
\]

and

\[
\text{case } r \cdot d \{ l \cdot x_1 \Rightarrow e_1 \mid r \cdot x_2 \Rightarrow e_2 \} \equiv [e/x_2]e_2 : \rho.
\]

Thus the dynamic behavior specified in Chapter 17 is correctly implemented by these definitions.

23.2.2 Natural Numbers

As we remarked above, the natural numbers (under a lazy interpretation) are also definable in \( L\{\to \forall\} \). The key is the representation of the iterator, whose typing rule we recall here for reference:

\[
e_0 : \texttt{nat} \quad e_1 : \tau \quad x : \tau \vdash e_2 : \tau
\]

\[
\text{natiter}(e_0; e_1; x; e_2) : \tau.
\]

Since the result type \( \tau \) is arbitrary, this means that if we have an iterator, then it can be used to define a function of type

\[
\texttt{nat} \to \forall(t : t \to (t \to t) \to t).
\]

This function, when applied to an argument \( n \), yields a polymorphic function that, for any result type, \( t \), if given the initial result for \( z \), and if given a function transforming the result for \( x \) into the result for \( s(x) \), then it returns the result of iterating the transformer \( n \) times starting with the initial result.

Since the only operation we can perform on a natural number is to iterate up to it in this manner, we may simply identify a natural number, \( n \), with the polymorphic iterate-up-to-\( n \) function just described. This means that we may define the type of natural numbers in \( L\{\to \forall\} \) by the following equations:

\[
\texttt{nat} = \forall(t : t \to (t \to t) \to t)
\]

\[
z = \Lambda(t : t \to (t : t \to t)) \quad s(e) = \Lambda(t : t \to (t : t \to t \to t))
\]

\[
\text{natiter}(e_0; e_1; x; e_2) = e_0(t)(e_1)(x : t \to e_2).
\]

It is a straightforward exercise to check that the static and dynamic semantics given in Chapter 14 is derivable in \( L\{\to \forall\} \) under these definitions.
This shows that $\mathcal{L}\{\rightarrow\forall\}$ is at least as expressive as $\mathcal{L}\{\text{nat} \rightarrow\}$. But is it more expressive? Yes! It is possible to show that the evaluation function for $\mathcal{L}\{\text{nat} \rightarrow\}$ is definable in $\mathcal{L}\{\rightarrow\forall\}$, even though it is not definable in $\mathcal{L}\{\text{nat} \rightarrow\}$ itself. However, the same diagonal argument given in Chapter 14 applies here, showing that the evaluation function for $\mathcal{L}\{\rightarrow\forall\}$ is not definable in $\mathcal{L}\{\rightarrow\forall\}$. We may enrich $\mathcal{L}\{\rightarrow\forall\}$ a bit more to define the evaluator for $\mathcal{L}\{\rightarrow\forall\}$, but as long as the enriched language is itself total, we will once again have an undefinable function, the evaluation function for that extension! The extension process will never close as long as the language remains total.

### 23.3 Parametricity

A remarkable property of polymorphic typing is that it strongly constrains the behavior of an expression of that type. For example, if $i$ is any expression of type $\forall (t. t \rightarrow t)$, then it must behave like the identity function in the following sense. For an arbitrary type $\tau$ and an arbitrary expression $e : \tau$, it must be that $i[\tau] (e) \equiv e$. The informal reason is that $i$, being polymorphic, must, when applied to an arbitrary argument of arbitrary type must return a result of that type. Since not even the type, much less the value, of the argument is known in advance, the function $i$ has no choice but to return the argument as result if it is to achieve the specified typing. Similarly, if $c$ is any expression of type $\forall (t. t \rightarrow t \rightarrow t)$, then for any type $\tau$ and any $e_1 : \tau$ and $e_2 : \tau$, it must be that either $c[\tau] (e_1) (e_2) \equiv e_1$ or $c[\tau] (e_1) (e_2) \equiv e_2$.

A rigorous justification of these claims is deferred to Chapter 50. Meanwhile we content ourselves with a brief summary of the argument developed there. The crucial idea is that types may be interpreted as relations, and we may prove that every well-typed expression of $\mathcal{L}\{\rightarrow\forall\}$ preserves any such relational interpretation. Theorem 50.8 on page 472, when specialized to $i : \forall (t. t \rightarrow t)$, implies that for any type $\tau$, any predicate $P$ on expressions of type $\tau$, and any $e : \tau$, if $P(e)$, then $P(i[\tau] (e))$. Fix $\tau$ and $e : \tau$, and define $P(x)$ to hold iff $x \equiv e$. By the theorem we have that for any $e' : \tau$, if $e' \equiv e$, then $i[\tau] (e') \equiv e$, and so in particular $i[\tau] (e) \equiv e$. Similarly, if $c : \forall (t. t \rightarrow t \rightarrow t)$, then, fixing $\tau$, $e_1 : \tau$, and $e_2 : \tau$, we may define $P(e)$ to hold iff either $e \equiv e_1$ or $e \equiv e_2$. It follows from the theorem that either $c[\tau] (e_1) (e_2) \equiv e_1$ or $c[\tau] (e_1) (e_2) \equiv e_2$.

What is remarkable is that these properties of $i$ and $c$ have been derived without knowing anything about the expressions themselves, but only their types! The theory of parametricity implies that we are able to derive the-
orems about the behavior of a program knowing only its type. Such theo-
rems are sometimes called free theorems because they come “for free” as
a consequence of typing, and require no program analysis or verification
to derive (beyond the once-and-for-all proof of Theorem 50.8 on page 472).
Free theorems such as those illustrated above underly the experience that in
a polymorphic language, well-typed programs tend to behave as expected
no further debugging or analysis required. Parametricity so constrains the
behavior of a program that it is relatively easy to ensure that the code works
just by checking its type. Free theorems also underly the principle of rep-
resentation independence for abstract types, which is discussed further in
Chapter 24.

23.4 Restricted Forms of Polymorphism

In this section we briefly examine some restricted forms of polymorphism
with less than the full expressive power of $L\{\to \forall\}$. These are obtained in
one of two ways:

1. Restricting type quantification to unquantified types.
2. Restricting the occurrence of quantifiers within types.

23.4.1 Predicative Fragment

The remarkable expressive power of the language $L\{\to \forall\}$ may be traced
to the ability to instantiate a polymorphic type with another polymorphic
type. For example, if we let $\tau$ be the type $\forall (t. t \to t)$, and, assuming that
$e : \tau$, we may apply $e$ to its own type, obtaining the expression $e[\tau]$ of type
$\tau \to \tau$. Written out in full, this is the type

$$\forall (t. t \to t) \to \forall (t. t \to t),$$

which is larger (both textually, and when measured by the number of oc-
currences of quantified types) than the type of $e$ itself. In fact, this type is
large enough that we can go ahead and apply $e[\tau]$ to $e$ again, obtaining the expression $e[\tau] (e)$, which is again of type $\tau$ — the very type of $e$!

This property of $L\{\to \forall\}$ is called impredicativity\footnote{pronounced im-PRED-i-ca-tiv-i-ty}; the language $L\{\to \forall\}$
is said to permit impredicative (type) quantification. The distinguishing char-
acteristic of impredicative polymorphism is that it involves a kind of cir-
cularity in that the meaning of a quantified type is given in terms of its
instances, including the quantified type itself. This quasi-circularity is responsible for the surprising expressive power of $\mathcal{L}\{\to \forall\}$, and is correspondingly the prime source of complexity when reasoning about it (for example, in the proof that all expressions of $\mathcal{L}\{\to \forall\}$ terminate).

Contrast this with $\mathcal{L}\{\to\}$, in which the type of an application of a function is evidently smaller than the type of the function itself. For if $e : \tau_1 \to \tau_2$, and $e_1 : \tau_1$, then we have $e(e_1) : \tau_2$, a smaller type than the type of $e$. This situation extends to polymorphism, provided that we impose the restriction that a quantified type can only be instantiated by an un-quantified type. For in that case passage from $\forall(t. \tau)$ to $[\sigma/t]\tau$ decreases the number of quantifiers (even if the size of the type expression viewed as a tree grows). For example, the type $\forall(t. t \to t)$ may be instantiated with the type $u \to u$ to obtain the type $(u \to u) \to (u \to u)$. This type has more symbols in it than $\tau$, but is smaller in that it has fewer quantifiers. The restriction to quantification only over unquantified types is called predicative polymorphism. The predicative fragment is significantly less expressive than the full impredicative language. In particular, the natural numbers are no longer definable in it.

The formalization of $\mathcal{L}\{\to \forall\}$ is left to Chapter 25, where the appropriate technical machinery is available.

23.4.2 Prenex Fragment

A rather more restricted form of polymorphism, called the prenex fragment, further restricts polymorphism to occur only at the outermost level — not only is quantification predicative, but quantifiers are not permitted to occur within the arguments to any other type constructors. This restriction, called prenex quantification, is often imposed for the sake of type inference, which permits type annotations to be omitted entirely in the knowledge that they can be recovered from the way the expression is used. We will not discuss type inference here, but we will give a formulation of the prenex fragment of $\mathcal{L}\{\to \forall\}$, because it plays an important role in the design of practical polymorphic languages.

The prenex fragment of $\mathcal{L}\{\to \forall\}$ is designated $\mathcal{L}\{\to \forall\}_p$, for reasons that will become clear in the next subsection. It is defined by stratifying types into two classes, the monotypes (or rank-0 types) and the polytypes (or rank-1 types). The monotypes are those that do not involve any quantification, and may be used to instantiate the polymorphic quantifier. The polytypes

\footnote{pronounced PRED-i-ca-tive}
include the monotypes, but also permit quantification over monotypes. These classifications are expressed by the judgements $\Delta \vdash \tau \text{ mono}$ and $\Delta \vdash \tau \text{ poly}$, where $\Delta$ is a finite set of hypotheses of the form $t \text{ mono}$, where $t$ is a type variable not otherwise declared in $\Delta$. The rules for deriving these judgements are as follows:

(23.5a) \[
\frac{}{\Delta, t \text{ mono} \vdash t \text{ mono}}
\]

(23.5b) \[
\frac{\Delta \vdash \tau_1 \text{ mono} \quad \Delta \vdash \tau_2 \text{ mono}}{\Delta \vdash \text{arr}(\tau_1; \tau_2) \text{ mono}}
\]

(23.5c) \[
\frac{\Delta \vdash \tau \text{ mono}}{\Delta \vdash \tau \text{ poly}}
\]

(23.5d) \[
\frac{\Delta, t \text{ mono} \vdash \tau \text{ poly}}{\Delta \vdash \text{all}(t. \tau) \text{ poly}}
\]

Base types, such as nat (as a primitive), or other type constructors, such as sums and products, would be added to the language as monotypes.

The static semantics of $L^1\{\rightarrow \forall\}$ is given by rules for deriving hypothetical judgements of the form $\Delta \Gamma \vdash e : \sigma$, where $\Delta$ consists of hypotheses of the form $t \text{ mono}$, and $\Gamma$ consists of hypotheses of the form $x : \sigma$, where $\Delta \vdash \sigma \text{ poly}$. The rules defining this judgement are as follows:

(23.6a) \[
\frac{}{\Delta \Gamma, x : \tau \vdash x : \tau}
\]

(23.6b) \[
\frac{\Delta \vdash \tau_1 \text{ mono} \quad \Delta, \Gamma, x : \tau_1 \vdash e_2 : \tau_2}{\Delta \Gamma \vdash \text{lam}[\tau_1](x.e_2) : \text{arr}(\tau_1; \tau_2)}
\]

(23.6c) \[
\frac{\Delta \Gamma \vdash e_1 : \text{arr}(\tau_2; \tau) \quad \Delta \Gamma \vdash e_2 : \tau_2}{\Delta \Gamma \vdash \text{ap}(e_1; e_2) : \tau}
\]

(23.6d) \[
\frac{\Delta, t \text{ mono} \vdash e : \tau}{\Delta \Gamma \vdash \text{Lam}(t.e) : \text{all}(t. \tau)}
\]

(23.6e) \[
\frac{\Delta \vdash \tau \text{ mono} \quad \Delta \Gamma \vdash e : \text{all}(t. \tau')}{\Delta \Gamma \vdash \text{App}[\tau](e) : [\tau/t] \tau'}
\]

We tacitly exploit the inclusion of monotypes as polytypes so that all typing judgements have the form $e : \sigma$ for some expression $e$ and polytype $\sigma$.

The restriction on the domain of a $\lambda$-abstraction to be a monotype means that a fully general $\text{let}$ construct is no longer definable—there is no means of binding an expression of polymorphic type to a variable. For this reason
it is usual to augment \( L \{ \rightarrow \forall_p \} \) with a primitive \texttt{let} construct whose static semantics is as follows:

\[
\Delta \vdash \tau_1 \text{poly} \quad \Delta \Gamma \vdash e_1 : \tau_1 \quad \Delta \Gamma, x : \tau_1 \vdash e_2 : \tau_2

\Rightarrow \quad \Delta \Gamma \vdash \text{let}[\tau_1](e_1; x. e_2) : \tau_2.
\]

(23.7)

For example, the expression

\[
\text{let } \nu(t. t \rightarrow t) \text{ be } \Lambda(t. \lambda(x : t. x)) \text{ in } I[\tau \rightarrow \tau](I[\tau])
\]

has type \( \tau \rightarrow \tau \) for any polytype \( \tau \).

### 23.4.3 Rank-Restricted Fragments

The binary distinction between monomorphic and polymorphic types in \( L^1 \{ \rightarrow \forall \} \) may be generalized to form a hierarchy of languages in which the occurrences of polymorphic types are restricted in relation to function types. The key feature of the prenex fragment is that quantified types are not permitted to occur in the domain of a function type. The prenex fragment also prohibits polymorphic types from the range of a function type, but it would be harmless to admit it, there being no significant difference between the type \( \sigma \rightarrow \forall(t. \tau) \) and the type \( \forall(t. \sigma \rightarrow \tau) \) (where \( t \notin \sigma \)).

This motivates the definition of a hierarchy of fragments of \( L \{ \rightarrow \forall \} \) that subsumes the prenex fragment as a special case.

We will define a judgement of the form \( \tau \text{ type } [k] \), where \( k \geq 0 \), to mean that \( \tau \) is a type of rank \( k \). Informally, types of rank 0 have no quantification, and types of rank \( k + 1 \) may involve quantification, but the domains of function types are restricted to be of rank \( k \). Thus, in the terminology of Section 23.4.2 on page 206, a monotype is a type of rank 0 and a polytype is a type of rank 1.

The definition of the types of rank \( k \) is defined simultaneously for all \( k \) by the following rules. These rules involve hypothetical judgements of the form \( \Delta \vdash \tau \text{ type } [k] \), where \( \Delta \) is a finite set of hypotheses of the form \( t_i \text{ type } [k_i] \) for some pairwise distinct set of type variables \( t_i \). The rules defining these judgements are as follows:

\[
\Delta, t \text{ type } [k] \vdash t \text{ type } [k]
\]

(23.8a)

\[
\Delta \vdash \tau_1 \text{ type } [0] \quad \Delta \vdash \tau_2 \text{ type } [0]

\Rightarrow \quad \Delta \vdash \text{arr}(\tau_1; \tau_2) \text{ type } [0]
\]

(23.8b)
With these restrictions in mind, it is a good exercise to define the static semantics of $L_k\{\rightarrow\forall\}$, the restriction of $L\{\rightarrow\forall\}$ to types of rank $k$ (or less). It is most convenient to consider judgements of the form $e : \tau[k]$ specifying simultaneously that $e : \tau$ and $\tau$ type $[k]$. For example, the rank-limited rules for $\lambda$-abstractions is phrased as follows:

$$
\frac{
\Delta \vdash \tau_1 \text{ type } [k] \quad \Delta \vdash \tau_2 \text{ type } [k+1]
}{
\Delta \vdash \text{arr}(\tau_1; \tau_2) \text{ type } [k+1]
}(23.8c)
$$

$$
\frac{
\Delta \vdash \tau \text{ type } [k]
}{
\Delta \vdash \tau \text{ type } [k+1]
}(23.8d)
$$

$$
\frac{
\Delta, t \text{ type } [k] \vdash \tau \text{ type } [k+1]
}{
\Delta \vdash \text{all}(t, \tau) \text{ type } [k+1]
}(23.8e)
$$

The remaining rules follow a similar pattern.

The rank-limited languages $L_k\{\rightarrow\forall\}$ clarifies the requirement for a primitive $\text{let}$ construct in $L^1\{\rightarrow\forall\}$. The prenex fragment of $L\{\rightarrow\forall\}$ corresponds to the rank-one fragment $L^1\{\rightarrow\forall\}$. The $\text{let}$ construct for rank-one types is definable in $L^2\{\rightarrow\forall\}$ from $\lambda$-abstraction and application. This definition only makes sense at rank two, since it abstracts over a rank-one polymorphic type.

### 23.5 Exercises

1. Show that primitive recursion is definable in $L\{\rightarrow\forall\}$ by exploiting the definability of iteration and binary products.

2. Investigate the representation of eager products and sums in eager and lazy variants of $L\{\rightarrow\forall\}$.

3. Show how to write an interpreter for $L\{\text{nat} \rightarrow\}$ in $L\{\rightarrow\forall\}$.
Chapter 24

Abstract Types

Data abstraction is perhaps the most important technique for structuring programs. The main idea is to introduce an interface that serves as a contract between the client and the implementor of an abstract type. The interface specifies what the client may rely on for its own work, and, simultaneously, what the implementor must provide to satisfy the contract. The interface serves to isolate the client from the implementor so that each may be developed in isolation from the other. In particular one implementation may be replaced by another without affecting the behavior of the client, provided that the two implementations meet the same interface and are, in a sense to be made precise below, suitably related to one another. (Roughly, each simulates the other with respect to the operations in the interface.) This property is called representation independence for an abstract type.

Data abstraction may be formalized by extending the language $\mathcal{L}\{	o\forall\}$ with existential types. Interfaces are modelled as existential types that provide a collection of operations acting on an unspecified, or abstract, type. Implementations are modelled as packages, the introductory form for existentials, and clients are modelled as uses of the corresponding elimination form. It is remarkable that the programming concept of data abstraction is modelled so naturally and directly by the logical concept of existential type quantification. Existential types are closely connected with universal types, and hence are often treated together. The superficial reason is that both are forms of type quantification, and hence both require the machinery of type variables. The deeper reason is that existentials are definable from universals — surprisingly, data abstraction is actually just a form of polymorphism! One consequence of this observation is that representation independence is just a use of the parametricity properties of polymorphic
functions discussed in Chapter 23.

24.1 Existential Types

The syntax of $\mathcal{L}\{\rightarrow\forall\exists\}$ is the extension of $\mathcal{L}\{\rightarrow\forall\}$ with the following constructs:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Types</td>
<td>$\tau$</td>
<td>$\text{some}(t.\tau)$</td>
<td>$\exists(t.\tau)$</td>
</tr>
<tr>
<td>Expr</td>
<td>$e$</td>
<td>$\text{pack}[t.\tau]<a href="e">\rho</a>$</td>
<td>$\text{pack }\rho\text{ with }e\text{ as }\exists(t.\tau)$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{open}[t.\tau][\rho](e_1; t, x. e_2)$</td>
<td>$\text{open }e_1\text{ as }t\text{ with }x:t\text{ in }e_2$</td>
</tr>
</tbody>
</table>

The introductory form for the existential type $\sigma = \exists(t.\tau)$ is a package of the form $\text{pack }\rho\text{ with }e\text{ as }\exists(t.\tau)$, where $\rho$ is a type and $e$ is an expression of type $[\rho/t]\tau$. The type $\rho$ is called the representation type of the package, and the expression $e$ is called the implementation of the package. The eliminator form for existentials is the expression $\text{open }e_1\text{ as }t\text{ with }x:t\text{ in }e_2$, which opens the package $e_1$ for use within the client $e_2$ by binding its representation type to $t$ and its implementation to $x$ for use within $e_2$. Crucially, the typing rules ensure that the client is type-correct independently of the actual representation type used by the implementor, so that it may be varied without affecting the type correctness of the client.

The abstract syntax of the open construct specifies that the type variable, $t$, and the expression variable, $x$, are bound within the client. They may be renamed at will by $\alpha$-equivalence without affecting the meaning of the construct, provided, of course, that the names are chosen so as not to conflict with any others that may be in scope. In other words the type, $t$, may be thought of as a “new” type, one that is distinct from all other types, when it is introduced. This is sometimes called generativity of abstract types: the use of an abstract type by a client “generates” a “new” type within that client. This behavior is simply a consequence of identifying terms up to $\alpha$-equivalence, and is not particularly tied to data abstraction.

24.1.1 Static Semantics

The static semantics of existential types is specified by rules defining when an existential is well-formed, and by giving typing rules for the associated introductory and eliminatory forms.

$$
\frac{}{\Delta, t \text{ type } \vdash \tau \text{ type}} \\
\frac{}{\Delta \vdash \text{some}(t.\tau) \text{ type}} \quad (24.1a)
$$
24.1 Existential Types

\[
\Delta \vdash \rho \text{ type} \quad \Delta, t \vdash \tau \text{ type} \quad \Delta \Gamma \vdash e : \left[\rho / t\right] \tau \\
\Delta \Gamma \vdash \text{pack}[t \cdot \tau \left[\rho\right]](e) : \text{some}(t \cdot \tau)
\]

(24.1b)

\[
\Delta \Gamma \vdash e_1 : \text{some}(t \cdot \tau) \quad \Delta, t \vdash \Gamma, x : \tau \vdash e_2 : \tau_2 \quad \Delta \vdash \tau_2 \text{ type} \\
\Delta \Gamma \vdash \text{open}[t \cdot \tau \left[\tau_2\right]](e_1 ; t, x, e_2) : \tau_2
\]

(24.1c)

Rule (24.1c) is complex, so study it carefully! There are two important things to notice:

1. The type of the client, \(\tau_2\), must not involve the abstract type \(t\). This restriction prevents the client from attempting to export a value of the abstract type outside of the scope of its definition.

2. The body of the client, \(e_2\), is type checked without knowledge of the representation type, \(t\). The client is, in effect, polymorphic in the type variable \(t\).

Lemma 24.1 (Regularity). Suppose that \(\Delta \Gamma \vdash e : \tau\). If \(\Delta \vdash \tau_i \text{ type}\) for each \(x_i : \tau_i\) in \(\Gamma\), then \(\Delta \vdash \tau\ \text{type}\).

**Proof.** By induction on Rules (24.1).

\[
\text{24.1.2 Dynamic Semantics}
\]

The dynamic semantics of existential types is specified as follows:

\[
\begin{array}{l}
\{e \text{ val}\} \\
\text{pack}[t \cdot \tau \left[\rho\right]](e) \text{ val} \\
\end{array}
\]

(24.2a)

\[
\begin{array}{l}
\{e \mapsto e'\} \\
\text{pack}[t \cdot \tau \left[\rho\right]](e) \mapsto \text{pack}[t \cdot \tau \left[\rho\right]](e') \\
\end{array}
\]

(24.2b)

\[
\begin{array}{l}
e_1 \mapsto e'_1 \\
\text{open}[t \cdot \tau \left[\tau_2\right]](e_1 ; t, x, e_2) \mapsto \text{open}[t \cdot \tau \left[\tau_2\right]](e'_1 ; t, x, e_2) \\
\end{array}
\]

(24.2c)

\[
\begin{array}{l}
\{e \text{ val}\} \\
\text{open}[t \cdot \tau \left[\tau_2\right]](\text{pack}[t \cdot \tau \left[\rho\right]](e) ; t, x, e_2) \mapsto [\rho, e/t, x]e_2 \\
\end{array}
\]

(24.2d)

These rules endow \(\mathcal{L}\{\rightarrow \forall \exists\}\) with a lazy semantics for packages. More importantly, these rules specify that there are no abstract types at run time! The representation type is exposed to the client by substitution when the package is opened. In other words, data abstraction is a compile-time discipline that leaves no traces of its presence at execution time.
24.1.3 Safety

The safety of the extension is stated and proved as usual. The argument is a simple extension of that used for $\mathcal{L}\{\rightarrow \forall\}$ to the new constructs.

**Theorem 24.2 (Preservation).** If $e : \tau$ and $e \mapsto e'$, then $e' : \tau$.

*Proof.* By rule induction on $e \mapsto e'$, making use of substitution for both expression- and type variables. \qed

**Lemma 24.3 (Canonical Forms).** If $e : \text{some}(t.\tau)$ and $e \text{ val}$, then $e = \text{pack}[t.\tau][\rho](e')$ for some type $\rho$ and some $e' \text{ val}$ such that $e' : [\rho/t]\tau$.

*Proof.* By rule induction on the static semantics, making use of the definition of closed values. \qed

**Theorem 24.4 (Progress).** If $e : \tau$ then either $e \text{ val}$ or there exists $e'$ such that $e \mapsto e'$.

*Proof.* By rule induction on $e : \tau$, making use of the canonical forms lemma. \qed

24.2 Data Abstraction Via Existentials

To illustrate the use of existentials for data abstraction, we consider an abstract type of queues of natural numbers supporting three operations:

1. Formation of the empty queue.
2. Inserting an element at the tail of the queue.
3. Remove the head of the queue.

This is clearly a bare-bones interface, but is sufficient to illustrate the main ideas of data abstraction. Queue elements may be taken to be of any type, $\tau$, of our choosing; we will not be specific about this choice, since nothing depends on it.

The crucial property of this description is that nowhere do we specify what queues actually *are*, only what we can *do* with them. This is captured
by the following existential type, \( \exists (t. \tau) \), which serves as the interface of the queue abstraction:

\[
\exists (t. (\text{emp}: t, \text{ins}: \text{nat} \times t \to t, \text{rem}: t \to \text{nat} \times t)).
\]

The representation type, \( t \), of queues is abstract — all that is specified about it is that it supports the operations \( \text{emp} \), \( \text{ins} \), and \( \text{rem} \), with the specified types.

An implementation of queues consists of a package specifying the representation type, together with the implementation of the associated operations in terms of that representation. Internally to the implementation, the representation of queues is known and relied upon by the operations. Here is a very simple implementation, \( e_i \), in which queues are represented as lists:

\[
\text{pack list with } (\text{emp} = \text{nil}, \text{ins} = e_i, \text{rem} = e_r) \text{ as } \exists (t. \tau),
\]

where

\[
e_i : \text{nat} \times \text{list} \to \text{list} = \lambda (x: \text{nat} \times \text{list}. e'_i),
\]

and

\[
e_r : \text{list} \to \text{nat} \times \text{list} = \lambda (x: \text{list}. e'_r).
\]

Here the expression \( e'_i \) conses the first component of \( x \), the element, onto the second component of \( x \), the queue. Correspondingly, the expression \( e'_r \) reverses its argument, and returns the head element paired with the reversal of the tail. These operations “know” that queues are represented as values of type \( \text{list} \), and are programmed accordingly.

It is also possible to give another implementation, \( e_p \), of the same interface, \( \exists (t. \tau) \), but in which queues are represented as pairs of lists, consisting of the “back half” of the queue paired with the reversal of the “front half”. This representation avoids the need for reversals on each call, and, as a result, achieves amortized constant-time behavior:

\[
\text{pack list } \times \text{list with } (\text{emp} = \langle \text{nil, nil} \rangle, \text{ins} = e_i, \text{rem} = e_r) \text{ as } \exists (t. \tau).
\]

In this case \( e_i \) has type

\[
\text{nat} \times (\text{list } \times \text{list}) \to (\text{list } \times \text{list}),
\]

and \( e_r \) has type

\[
(\text{list } \times \text{list}) \to \text{nat} \times (\text{list } \times \text{list}).
\]
24.3 Definability of Existentials

These operations “know” that queues are represented as values of type \(\text{list} \times \text{list}\), and are implemented accordingly.

The important point is that the same client type checks regardless of which implementation of queues we choose. This is because the representation type is hidden, or held abstract, from the client during type checking. Consequently, it cannot rely on whether it is \(\text{list}\) or \(\text{list} \times \text{list}\) or some other type. That is, the client is independent of the representation of the abstract type.

24.3 Definability of Existentials

It turns out that it is not necessary to extend \(L\{\rightarrow \forall\}\) with existential types to model data abstraction, because they are already definable using only universal types! Before giving the details, let us consider why this should be possible. The key is to observe that the client of an abstract type is polymorphic in the representation type. The typing rule for

\[
\text{open } e \text{ as } t \text{ with } x : \tau \text{ in } e' : \tau',
\]

where \(e : \exists(t.\tau)\), specifies that \(e' : \tau'\) under the assumptions \(t\) type and \(x : \tau\). In essence, the client is a polymorphic function of type

\[
\forall(t.\tau \rightarrow \tau'),
\]

where \(t\) may occur in \(\tau\) (the type of the operations), but not in \(\tau'\) (the type of the result).

This suggests the following encoding of existential types:

\[
\exists(t.\sigma) = \forall(t'.\forall(t.\sigma \rightarrow t') \rightarrow t')
\]

\[
\text{pack } \rho \text{ with } e \text{ as } \exists(t.\sigma) = \Lambda(t'.\lambda(x: \forall(t.\sigma \rightarrow t').x[\rho](e)))(e)
\]

\[
\text{open } e \text{ as } t \text{ with } x: \sigma \text{ in } e' = e[t'](\Lambda(t.\lambda(x: \sigma.e'))
\]

An existential is encoded as a polymorphic function taking the overall result type, \(t'\), as argument, followed by a polymorphic function representing the client with result type \(t'\), and yielding a value of type \(t'\) as overall result. Consequently, the open construct simply packages the client as such a polymorphic function, instantiates the existential at the result type, \(\tau\), and applies it to the polymorphic client. (The translation therefore depends on knowing the overall result type, \(\tau\), of the open construct.) Finally, a package consisting of a representation type \(\rho\) and an implementation \(e\) is a
polymorphic function that, when given the result type, \( t \), and the client, \( x \), instantiates \( x \) with \( \rho \) and passes to it the implementation \( e \).

It is then a straightforward exercise to show that this translation correctly reflects the static and dynamic semantics of existential types.

### 24.4 Representation Independence

An important consequence of parametricity is that it ensures that clients are insensitive to the representations of abstract types. More precisely, there is a criterion, called bisimilarity, for relating two implementations of an abstract type such that the behavior of a client is unaffected by swapping one implementation by another that is bisimilar to it. This leads to a simple methodology for proving the correctness of candidate implementation of an abstract type, which is to show that it is bisimilar to an obviously correct reference implementation of it. Since the candidate and the reference implementations are bisimilar, no client may distinguish them from one another, and hence if the client behaves properly with the reference implementation, then it must also behave properly with the candidate.

To derive the definition of bisimilarity of implementations, it is helpful to examine the definition of existentials in terms of universals given in Section 24.3 on the facing page. It is an immediate consequence of the definition that the client of an abstract type is polymorphic in the representation of the abstract type. A client, \( c \), of an abstract type \( \exists (t. \sigma) \) has type \( \forall (t (\sigma \rightarrow t \rightarrow t) \rightarrow t) \), where \( t \) does not occur free in \( \tau \) (but may, of course, occur in \( \sigma \)). Applying the parametricity property described informally in Chapter 23 (and developed rigorously in Chapter 50), this says that if \( R \) is a bisimulation relation between any two implementations of the abstract type, then the client behaves identically on both of them. The fact that \( t \) does not occur in the result type ensures that the behavior of the client is independent of the choice of relation between the implementations, provided that this relation is preserved by the operation that implement it.

To see what this means requires that we specify what is meant by a bisimulation. This is best done by example. So suppose that \( \sigma \) is the type

\[
\langle \text{emp} : t, \text{ins} : t \times t \rightarrow t, \text{rem} : t \rightarrow t \times t \rangle.
\]

Theorem 50.8 on page 472 ensures that if \( \rho \) and \( \rho' \) are any two closed types, \( R \) is a relation between expressions of these two types, then if any the implementations \( e : [\rho/x]\sigma \) and \( e' : [\rho'/x]\sigma \) respect \( R \), then \( c[\rho]e \) behaves the
same as \( c[\rho]_e' \). It remains to define when two implementations respect the relation \( R \). Let
\[
\begin{align*}
e &= (\text{emp} = e_m, \text{ins} = e_i, \text{rem} = e_r) \\
e' &= (\text{emp} = e'_m, \text{ins} = e'_i, \text{rem} = e'_r).
\end{align*}
\]

For these implementations to respect \( R \) means that the following three conditions hold:

1. The empty queues are related: \( R(e_m, e'_m) \).

2. Inserting the same element on each of two related queues yields related queues: if \( d : \tau \) and \( R(q, q') \), then \( R(e_i(d)(q), e_i(d)(q')) \).

3. If two queues are related, their front elements are the same and their back elements are related: if \( R(q, q') \), \( e_r(q) \equiv (d, r) \), \( e_r(q) \equiv (d', r') \), then \( d \) is \( d' \) and \( R(r, r') \).

If such a relation \( R \) exists, then the implementations \( e \) and \( e' \) are said to be bisimilar. The terminology stems from the requirement that the operations of the abstract type preserve the relation: if it holds before an operation is performed, then it must also hold afterwards, and the relation must hold for the initial state of the queue. Thus each implementation simulates the other up to the relationship specified by \( R \).

To see how this works in practice, let us consider informally two implementations of the abstract type of queues specified above. For the reference implementation we choose \( \rho \) to be the type \( \text{list} \), and define the empty queue to be the empty list, insert to add the specified element to the front of the list, and remove to remove the last element of the list. (A remove therefore takes time linear in the length of the list.) For the candidate implementation we choose \( \rho' \) to be the type \( \text{list} \times \text{list} \) consisting of two lists, \( (b, f) \), where \( b \) represents the "back" of the queue, and \( f \) represents the "front" of the queue represented in reverse order of insertion. The empty queue consists of two empty lists. To insert \( d \) onto \( (b, f) \), we simply return \( \langle \text{cons}(d; b), f \rangle \), placing it on the "back" of the queue as expected. To remove an element from \( (b, f) \) breaks into two cases. If the front, \( f \), of the queue is non-empty, say \( \text{cons}(d; f') \), then return \( \langle d, (b, f') \rangle \) consisting of the front element and the queue with that element removed. If, on the other hand, \( f \) is empty, then we must move elements from the "back" to the "front" by reversing \( b \) and re-performing the remove operation on \( (\text{nil}, \text{rev}(b)) \), where \( \text{rev} \) is the obvious list reversal function.
To show that the candidate implementation is correct, we show that it is bisimilar to the reference implementation. This reduces to specifying a relation, $R$, between the types `list` and `list × list` such that the three simulation conditions given above are satisfied by the two implementations just described. The relation in question states that $R(l, \langle b, f \rangle)$ iff the list $l$ is the list $\text{app}(b) (\text{rev}(f))$, where $\text{app}$ is the evident append function on lists. That is, thinking of $l$ as the reference representation of the queue, the candidate must maintain that the elements of $b$ followed by the elements of $f$ in reverse order form precisely the list $l$. It is easy to check that the implementations just described preserve this relation. Having done so, we are assured that the client, $c$, behaves the same regardless of whether we use the reference or the candidate. Since the reference implementation is obviously correct (albeit inefficient), the candidate must also be correct in that the behavior of any client is unaffected by using it instead of the reference.

### 24.5 Exercises
Chapter 25

Constructors and Kinds

Types such as \( \tau_1 \rightarrow \tau_2 \) or \( \text{list} \) may be thought of as being built from other types by the application of a type constructor, or type operator. These two examples differ from each other in that the function space type constructor takes two arguments, whereas the list type constructor takes only one. We may, for the sake of uniformity, think of types such as \( \text{nat} \) as being built by a type constructor of no arguments. More subtly, we may even think of the types \( \forall (t. \tau) \) and \( \exists (t. \tau) \) as being built up in the same way by regarding the quantifiers as higher-order type operator.

These seemingly disparate cases may be treated uniformly by enriching the syntactic structure of a language with a new layer of constructors. To ensure that constructors are used properly (for example, that the list constructor is given only one argument, and that the function constructor is given two), we classify constructors by kinds. Constructors of a distinguished kind, Type, are types, which may be used to classify expressions. To allow for multi-argument and higher-order constructors, we will also consider finite product and function kinds. (Later we shall consider even richer kinds.)

The distinction between constructors and kinds on one hand and types and expressions on the other reflects a fundamental separation between the static and dynamic phase of processing of a programming language, called the phase distinction. The static phase implements the static semantics, and the dynamic phase implements the dynamic semantics. Constructors may be seen as a form of static data that is manipulated during the static phase of processing. Expressions are a form of dynamic data that is manipulated at run-time. Since the dynamic phase follows the static phase (we only execute well-typed programs), we may also manipulate constructors at run-
time.

Adding constructors and kinds to a language introduces more technical complications than might at first be apparent. The main difficulty is that as soon as we enrich the kind structure beyond the distinguished kind of types, it becomes essential to simplify constructors to determine whether they are equivalent. For example, if we admit product kinds, then a pair of constructors is a constructor of product kind, and projections from a constructor of product kind are also constructors. But what if we form the first projection from the pair consisting of the constructors \texttt{nat} and \texttt{str}? This should be equivalent to \texttt{nat}, since the elimination form if post-inverse to the introduction form. Consequently, any expression (say, a variable) of the one type should also be an expression of the other. That is, typing should respect definitional equivalence of constructors.

There are two main ways to deal with this. One is to introduce a concept of definitional equivalence for constructors, and to demand that the typing judgement for expressions respect definitional equivalence of constructors of kind \texttt{Type}. This means, however, that we must show that definitional equivalence is decidable if we are to build a complete implementation of the language. The other is to prohibit formation of awkward constructors such as the projection from a pair so that there is never any issue of when two constructors are equivalent (only when they are identical). But this complicates the definition of substitution, since a projection from a constructor variable is well-formed, until you substitute a pair for the variable. Both approaches have their benefits, but the second is simplest, and is adopted here.

25.1 Statics

The syntax of kinds is given by the following grammar:

```
<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kind ( \kappa )</td>
<td>( \kappa )</td>
<td>Type</td>
<td>Type</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\texttt{Unit}</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\texttt{Prod}(\kappa_1;\kappa_2)</td>
<td>( \kappa_1 \times \kappa_2 )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\texttt{Arr}(\kappa_1;\kappa_2)</td>
<td>( \kappa_1 \rightarrow \kappa_2 )</td>
</tr>
</tbody>
</table>
```

The kinds consist of the kind of types, \texttt{Type}, the unit kind, \texttt{Unit}, and are closed under formation of product and function kinds.

The syntax of constructors is divided into two categories, the \textit{neutral}
and the canonical, according to the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neutral</td>
<td>$a$</td>
<td>$u$</td>
<td>$u$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{proj}<a href="a">1</a>$</td>
<td>$\text{pr}_1(a)$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{proj}<a href="a">r</a>$</td>
<td>$\text{pr}_r(a)$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{app}(a_1;c_2)$</td>
<td>$a_1[c_2]$</td>
</tr>
<tr>
<td>Canonical</td>
<td>$c$</td>
<td>$\text{atom}(a)$</td>
<td>$\hat{a}$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>unit</td>
<td>$*$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{pair}(c_1;c_2)$</td>
<td>$\langle c_1,c_2 \rangle$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{lam}(u.c)$</td>
<td>$\lambda u.c$</td>
</tr>
</tbody>
</table>

The meta-variable $u$ ranges over constructor variables.

The reason to distinguish neutral from canonical constructors is to ensure that it is impossible to apply an elimination form to an introduction form, which demands an equation to capture the inversion principle. For example, the putative constructor $\text{pr}_1(\langle c_1,c_2 \rangle)$, which would be definitionally equivalent to $c_1$, is ill-formed according to Grammar (25.1). This is because the argument to a projection must be neutral, but a pair is only canonical, not neutral.

The canonical constructor $\text{atom}(a)$ is the inclusion of neutral constructors into canonical constructors. However, the grammar does not capture a crucial property of the static semantics that ensures that only neutral constructors of kind Type may be treated as canonical. This requirement is imposed to limit the forms of canonical constructors of the other kinds. In particular, variables of function, product, or unit kind will turn out not to be canonical, but only neutral.

The static semantics of constructors and kinds is specified by the judgements

<table>
<thead>
<tr>
<th>Judgement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Delta \vdash a \uparrow \kappa$</td>
<td>neutral constructor formation</td>
</tr>
<tr>
<td>$\Delta \vdash c \downarrow \kappa$</td>
<td>canonical constructor formation</td>
</tr>
</tbody>
</table>

In each of these judgements $\Delta$ is a finite set of hypotheses of the form

$u_1 \uparrow \kappa_1, \ldots, u_n \uparrow \kappa_n$

for some $n \geq 0$. The form of the hypotheses expresses the principle that variables are neutral constructors. The formation judgements are to be understood as parametric hypothetical judgements with parameters $u_1, \ldots, u_n$ that are determined by the forms of the hypotheses.

The rules for constructor formation are as follows:

$$\Delta, u \uparrow \kappa \vdash u \uparrow \kappa$$ (25.1a)
Adding Constructors and Kinds

\[ \Delta \vdash a \uparrow \kappa_1 \times \kappa_2 \]

\[ \Delta \vdash \text{pr}_1(a) \uparrow \kappa_1 \]

(25.1b)

\[ \Delta \vdash a \uparrow \kappa_1 \times \kappa_2 \]

\[ \Delta \vdash \text{pr}_2(a) \uparrow \kappa_2 \]

(25.1c)

\[ \Delta \vdash a_1 \uparrow \kappa_2 \rightarrow \kappa \quad \Delta \vdash c_2 \downarrow \kappa_2 \]

\[ \Delta \vdash a_1[c_2] \uparrow \kappa \]

(25.1d)

\[ \Delta \vdash a \uparrow \text{Type} \]

\[ \Delta \vdash \text{hat} \downarrow \text{Type} \]

(25.1e)

\[ \Delta \vdash * \downarrow 1 \]

(25.1f)

\[ \Delta \vdash c_1 \downarrow \kappa_1 \quad \Delta \vdash c_2 \downarrow \kappa_2 \]

\[ \Delta \vdash \langle c_1, c_2 \rangle \downarrow \kappa_1 \times \kappa_2 \]

(25.1g)

\[ \Delta, u \uparrow \kappa_1 \vdash c_2 \downarrow \kappa_2 \]

\[ \Delta \vdash \lambda u . c_2 \downarrow \kappa_1 \rightarrow \kappa_2 \]

(25.1h)

Rule (25.1e) specifies that the only neutral constructors that are canonical are those with kind \text{Type}. This ensures that the language enjoys the following canonical forms property, which is easily proved by inspection of Rules (25.1).

**Lemma 25.1.** Suppose that \( \Delta \vdash c \downarrow \kappa \).

1. If \( \kappa = 1 \), then \( c = * \).

2. If \( \kappa = \kappa_1 \times \kappa_2 \), then \( c = \langle c_1, c_2 \rangle \) for some \( c_1 \) and \( c_2 \) such that \( \Delta \vdash c_i \downarrow \kappa_i \) for \( i = 1, 2 \).

3. If \( \kappa = \kappa_1 \rightarrow \kappa_2 \), then \( c = \lambda u . c_2 \) with \( \Delta, u \uparrow \kappa_1 \vdash c_2 \downarrow \kappa_2 \).

25.2 Adding Constructors and Kinds

To equip a language, \( L \), with constructors and kinds requires that we augment its static semantics with hypotheses governing constructor variables, and that we relate constructors of kind \text{Type} (types as static data) to the classifiers of dynamic expressions (types as classifiers). To achieve this the
static semantics of \( \mathcal{L} \) must be defined to have judgements of the following two forms:

\[
\Delta \vdash \tau \text{ type} \quad \text{type formation}
\]
\[
\Delta \Gamma \vdash e : \tau \quad \text{expression formation}
\]

where, as before, \( \Gamma \) is a finite set of hypotheses of the form

\[
x_1 : \tau_1, \ldots, x_k : \tau_k
\]

for some \( k \geq 0 \) such that \( \Delta \vdash \tau_i \text{ type} \) for each \( 1 \leq i \leq k \).

As a general principle, every constructor of kind \( \text{Type} \) is a classifier:

\[
\frac{\Delta \vdash \tau \uparrow \text{Type}}{\Delta \vdash \tau \text{ type}} . \quad (25.2)
\]

In many cases this is the sole rule of type formation, so that every classifier is a constructor of kind \( \text{Type} \). However, this need not be the case. In some situations we may wish to have strictly more classifiers than constructors of the distinguished kind.

To see how this might arise, let us consider two extensions of \( \mathcal{L}\{\to, \forall\} \) from Chapter 23. In both cases we extend the universal quantifier \( \forall (t . \tau) \) to admit quantification over an arbitrary kind, written \( \forall_k u . \tau \), but the two languages differ in what constitutes a constructor of kind \( \text{Type} \). In one case, the impredicative, we admit quantified types as constructors, and in the other, the predicative, we exclude quantified types from the domain of quantification.

The impredicative fragment includes the following two constructor constants:

\[
\frac{}{\Delta \vdash \rightarrow \uparrow \text{Type} \to \text{Type} \to \text{Type}} . \quad (25.3a)
\]
\[
\frac{}{\Delta \vdash \forall_k \uparrow (\kappa \to \text{Type}) \to \text{Type}} . \quad (25.3b)
\]

We regard the classifier \( \tau_1 \to \tau_2 \) to be the application \( \to [\tau_1] [\tau_2] \). Similarly, we regard the classifier \( \forall_k u \cdot \tau \) to be the application \( \forall_k [\lambda u . \tau] \).

The predicative fragment excludes the constant specified by Rule (25.3b) in favor of a separate rule for the formation of universally quantified types:

\[
\frac{\Delta, u \uparrow \kappa \vdash \tau \text{ type}}{\Delta \vdash \forall_k u . \tau \text{ type}} . \quad (25.4)
\]

The important point is that \( \forall_k u . \tau \) is a type (as classifier), but is \( \textit{not} \) a constructor of kind type.
The significance of this distinction becomes apparent when we consider the introduction and elimination forms for the generalized quantifier, which are the same for both fragments:

\[
\Delta, u \uparrow \kappa \Gamma \vdash e : \tau \\
\Delta \Gamma \vdash \Lambda (u : \kappa . e) : \forall \kappa u . \tau
\]  

(25.5a)

\[
\Delta \Gamma \vdash e : \forall \kappa u . \tau \quad \Delta \vdash c \downarrow \kappa \\
\Delta \Gamma \vdash e [c] : [c/u] \tau
\]

(25.5b)

(Rule (25.5b) makes use of substitution, whose definition requires some care. We will return to this point in Section 25.3.)

Rule (25.5b) makes clear that a polymorphic abstraction quantifies over the constructors of kind \(\kappa\). When \(\kappa\) is Type this kind may or may not include all of the classifiers of the language, according to whether we are working with the impredicative formulation of quantification (in which the quantifiers are distinguished constants for building constructors of kind Type) or the predicative formulation (in which quantifiers arise only as classifiers and not as constructors).

The important principle here is that constructors are static data, so that a constructor abstraction \(\Lambda (u : \kappa . e)\) of type \(\forall \kappa u . \tau\) is a mapping from static data \(c\) of kind \(\kappa\) to dynamic data \([c/u] e\) of type \([c/u] \tau\). Rule (25.1e) tells us that every constructor of kind Type determines a classifier, but it may or may not be the case that every classifier arises in this manner.

### 25.3 Substitution

Rule (25.5b) involves substitution of a canonical constructor, \(c\), of kind \(\kappa\) into a family of types \(u \uparrow \kappa \vdash \tau\) type. This operation is is written \([c/u] \tau\), as usual. Although the intended meaning is clear, it is in fact impossible to interpret \([c/u] \tau\) as the standard concept of substitution defined for arbitrary abt’s in Chapter 7. The reason is that to do so would risk violating the distinction between neutral and canonical constructors. Consider, for example, the case of the family of types

\[ u \uparrow \text{Type} \rightarrow \text{Type} \vdash u [d] \uparrow \text{Type}, \]

where \(d \uparrow \text{Type}\). (It is not important what we choose for \(d\), so we leave it abstract.) Now if \(c \downarrow \text{Type} \rightarrow \text{Type}\), then by Lemma 25.1 on page 224 we have that \(c\) is \(\lambda u' . c'\). Thus, if interpreted conventionally, substitution of \(c\)
for \( u \) in the given family yields the “constructor” \( (\lambda u'. c') [d] \), which is not well-formed.

The solution is to define a form of canonizing substitution that simplifies such “illegal” combinations as it performs the replacement of a variable by a constructor of the same kind. In the case just sketched this means that we must ensure that

\[
[\lambda u'. c'/u]u [d] = [d'/u']c'.
\]

If viewed as a definition this equation is problematic because it switches from substituting for \( u \) in the constructor \( u [d] \) to substituting for \( u' \) in the unrelated constructor \( c' \). Why should such a process terminate? The answer lies in the observation that the kind of \( u' \) is definitely smaller than the kind of \( u \), since the former’s kind is the domain kind of the latter’s function kind. In all other cases of substitution (as we shall see shortly) the size of the target of the substitution becomes smaller; in the case just cited the size may increase, but the type of the target variable decreases. Therefore by a lexicographic induction on the type of the target variable and the structure of the target constructor, we may prove that canonizing substitution is well-defined.

We now turn to the task of making this precise. We will define simultaneously two principal forms of substitution, one of which divides into two cases:

\[
\begin{align*}
[c/u : \kappa]a &= a' & \text{canonical into neutral yielding neutral} \\
[c/u : \kappa]a &= c' \Downarrow \kappa' & \text{canonical into neutral yielding canonical and kind} \\
[c/u : \kappa]c' &= c'' & \text{canonical into canonical yielding canonical}
\end{align*}
\]

Substitution into a neutral constructor divides into two cases according to whether the substituted variable \( u \) occurs in critical position in a sense to be made precise below.

These forms of substitution are simultaneously inductively defined by the following rules, which are broken into groups for clarity.

The first set of rules defines substitution of a canonical constructor into a canonical constructor; the result is always canonical.

\[
\begin{align*}
[c/u : \kappa]a &= a'' & \text{(25.6a)} \\
[c/u : \kappa]a' &= a''' \\
\end{align*}
\]

\[
\begin{align*}
[c/u : \kappa]a' &= c'' \Downarrow \kappa'' & \text{(25.6b)} \\
[c/u : \kappa]a'' &= c'''
\end{align*}
\]
\begin{align*}
[u/\star: \kappa] = \star 
\quad \tag{25.6c}
\end{align*}

\begin{align*}
[c/\kappa] & = c'' \\
[c/\kappa] & = c'' \\
\langle c_1', c_2' \rangle & = \langle c_1'', c_2'' \rangle 
\quad \tag{25.6d}
\end{align*}

\begin{align*}
[c/\kappa] & = c'' \quad (u \neq u') \quad (u' \notin c) \\
[c/\kappa] & = \lambda u'.c'' 
\quad \tag{25.6e}
\end{align*}

The conditions on variables in Rule (25.6e) may always be met by renaming the bound variable, \( u' \), of the abstraction.

The second set of rules defines substitution of a canonical constructor into a neutral constructor, yielding another neutral constructor.

\begin{align*}
\frac{(u \neq u')}{[c/\kappa] u' = u'} 
\quad \tag{25.7a}
\end{align*}

\begin{align*}
\frac{[c/\kappa] a' = a''}{[c/\kappa] \text{pr}_1(a') = \text{pr}_1(a'')} 
\quad \tag{25.7b}
\end{align*}

\begin{align*}
\frac{[c/\kappa] a' = a''}{[c/\kappa] \text{pr}_2(a') = \text{pr}_2(a'')} 
\quad \tag{25.7c}
\end{align*}

\begin{align*}
\frac{[c/\kappa] a_1 = a_1' \quad [c/\kappa] a_2 = a_2'}{[c/\kappa] a_1.a_2 = a_1'.a_2''} 
\quad \tag{25.7d}
\end{align*}

Rule (25.7a) pertains to a \textit{non-critical} variable, which is not the target of substitution. The remaining rules pertain to situations in which the recursive call on a neutral constructor yields a neutral constructor.

The third set of rules defines substitution of a canonical constructor into a neutral constructor, yielding a canonical constructor and its kind.

\begin{align*}
[c/\kappa] u = c \Downarrow \kappa 
\quad \tag{25.8a}
\end{align*}

\begin{align*}
\frac{[c/\kappa] a' = \langle c_1', c_2' \rangle \Downarrow \kappa_1' \times \kappa_2'}{[c/\kappa] \text{pr}_1(a') = c_1' \Downarrow \kappa_1'} 
\quad \tag{25.8b}
\end{align*}

\begin{align*}
\frac{[c/\kappa] a' = \langle c_1', c_2' \rangle \Downarrow \kappa_1' \times \kappa_2'}{[c/\kappa] \text{pr}_2(a') = c_2' \Downarrow \kappa_2'} 
\quad \tag{25.8c}
\end{align*}
Rule (25.8a) governs a critical variable, which is the target of substitution. The substitution transforms it from a neutral constructor to a canonical constructor. This has a knock-on effect in the remaining rules of the group, which analyze the canonical form of the result of the recursive call to determine how to proceed. Rule (25.8d) is the most interesting rule. In the third premise, all three arguments to substitution change as we substitute the (substituted) argument of the application for the parameter of the (substituted) function into the body of that function. Here we require the type of the function in order to determine the type of its parameter.

Theorem 25.2. Suppose that \( \Delta \vdash c \downarrow \kappa \), and \( \Delta, u \uparrow \kappa \vdash c' \downarrow \kappa' \), and \( \Delta, u \uparrow \kappa \vdash a' \uparrow \kappa' \). There exists a unique \( \Delta \vdash c'' \downarrow \kappa' \) such that \( [c/u : \kappa]c' = c'' \). Either there exists a unique \( \Delta \vdash a'' \uparrow \kappa' \) such that \( [c/u : \kappa]a' = a'' \), or there exists a unique \( \Delta \vdash c'' \downarrow \kappa' \) such that \( [c/u : \kappa]a' = c'' \), but not both.

Proof. Simultaneously by a lexicographic induction with major component the structure of the kind \( \kappa \), and with minor component determined by Rules (25.1) governing the formation of \( c' \) and \( a' \). For all rules except Rule (25.8d) the inductive hypothesis applies to the premise(s) of the relevant formation rules. For Rule (25.8d) we appeal to the major inductive hypothesis applied to \( \kappa'_2 \), which is a component of the kind \( \kappa'_2 \rightarrow \kappa' \). \( \square \)
Chapter 26

Indexed Families of Types

26.1 Type Families

26.2 Exercises
Part IX

Control Effects
Chapter 27

Control Stacks

The technique of specifying the dynamic semantics as a transition system is very useful for theoretical purposes, such as proving type safety, but is too high level to be directly usable in an implementation. One reason is that the use of “search rules” requires the traversal and reconstruction of an expression in order to simplify one small part of it. In an implementation we would prefer to use some mechanism to record “where we are” in the expression so that we may “resume” from that point after a simplification. This can be achieved by introducing an explicit mechanism, called a control stack, that keeps track of the context of an instruction step for just this purpose. By making the control stack explicit the transition rules avoid the need for any premises—every rule is an axiom. This is the formal expression of the informal idea that no traversals or reconstructions are required to implement it. In this chapter we introduce an abstract machine, \( \mathcal{K}\{\text{nat} \rightarrow \} \), for the language \( \mathcal{L}\{\text{nat} \rightarrow \} \). The purpose of this machine is to make control flow explicit by introducing a control stack that maintains a record of the pending sub-computations of a computation. We then prove the equivalence of \( \mathcal{K}\{\text{nat} \rightarrow \} \) with the structural operational semantics of \( \mathcal{L}\{\text{nat} \rightarrow \} \).

27.1 Machine Definition

A state, \( s \), of \( \mathcal{K}\{\text{nat} \rightarrow \} \) consists of a control stack, \( k \), and a closed expression, \( e \). States may take one of two forms:

1. An evaluation state of the form \( k \triangleright e \) corresponds to the evaluation of a closed expression, \( e \), relative to a control stack, \( k \).
2. A return state of the form \( k \triangleleft e \), where \( e \) val, corresponds to the evaluation of a stack, \( k \), relative to a closed value, \( e \).

As an aid to memory, note that the separator “points to” the focal entity of the state, the expression in an evaluation state and the stack in a return state.

The control stack represents the context of evaluation. It records the “current location” of evaluation, the context into which the value of the current expression is to be returned. Formally, a control stack is a list of frames:

\[
e \text{stack} \quad \text{(27.1a)}
\]

\[
f \text{frame} \quad k \text{ stack} \quad \text{(27.1b)}
\]

The definition of frame depends on the language we are evaluating. The frames of \( K \{ \text{nat} \rightarrow \} \) are inductively defined by the following rules:

\[
s(\neg) \text{ frame} \quad \text{(27.2a)}
\]

\[
\text{ifz}(\neg; e_1; x. e_2) \text{ frame} \quad \text{(27.2b)}
\]

\[
\text{ap}(\neg; e_2) \text{ frame} \quad \text{(27.2c)}
\]

The frames correspond to rules with transition premises in the dynamic semantics of \( L \{ \text{nat} \rightarrow \} \). Thus, instead of relying on the structure of the transition derivation to maintain a record of pending computations, we make an explicit record of them in the form of a frame on the control stack.

The transition judgement between states of the \( K \{ \text{nat} \rightarrow \} \) is inductively defined by a set of inference rules. We begin with the rules for natural numbers.

\[
k \triangleright z \mapsto k \triangleleft z \quad \text{(27.3a)}
\]

\[
k \triangleright s(e) \mapsto k; s(\neg) \triangleright e \quad \text{(27.3b)}
\]

\[
k; s(\neg) \triangleleft e \mapsto k \triangleleft s(e) \quad \text{(27.3c)}
\]

To evaluate \( z \) we simply return it. To evaluate \( s(e) \), we push a frame on the stack to record the pending successor, and evaluate \( e \); when that returns with \( e' \), we return \( s(e') \) to the stack.
Next, we consider the rules for case analysis.

\[
\overline{k; \text{ifz}(\neg; e_1; x.e_2) \triangleright z} \rightarrow k; \text{ifz}(\neg; e_1; x.e_2) \triangleright e
\]  
\text{(27.4a)}

\[
\overline{k; \text{ifz}(\neg; e_1; x.e_2) \triangleleft z} \rightarrow k \triangleright e_1
\]  
\text{(27.4b)}

\[
\overline{k; \text{ifz}(\neg; e_1; x.e_2) \triangleleft s(e)} \rightarrow k \triangleright [e/x]e_2
\]  
\text{(27.4c)}

First, the test expression is evaluated, recording the pending case analysis on the stack. Once the value of the test expression has been determined, we branch to the appropriate arm of the conditional, substituting the predecessor in the case of a positive number.

Finally, we consider the rules for functions and recursion.

\[
\overline{k \triangleright \text{lam}[\tau](x.e)} \rightarrow k \triangleleft \text{lam}[\tau](x.e)
\]  
\text{(27.5a)}

\[
\overline{k \triangleright \text{ap}(e_1; e_2) \rightarrow k; \text{ap}(\neg; e_2) \triangleright e_1}
\]  
\text{(27.5b)}

\[
\overline{k; \text{ap}(\neg; e_2) \triangleleft \text{lam}[\tau](x.e) \rightarrow k \triangleright [e_2/x]e}
\]  
\text{(27.5c)}

\[
\overline{k \triangleright \text{fix}[\tau](x.e) \rightarrow k \triangleright [\text{fix}[\tau](x.e)/x]e}
\]  
\text{(27.5d)}

These rules ensure that the function is evaluated before the argument, applying the function when both have been evaluated. Note that evaluation of general recursion requires no stack space! (But see Chapter 39 for more on evaluation of general recursion.)

The initial and final states of the $\mathcal{K}\{\text{nat}\rightarrow\}$ are defined by the following rules:

\[
\overline{e \triangleright e \ \text{initial}}
\]  
\text{(27.6a)}

\[
\overline{\begin{array}{l}
e \ \text{val} \\
\overline{e \triangleleft e \ \text{final}}
\end{array}}
\]  
\text{(27.6b)}
27.2 Safety

To define and prove safety for \( K\{\text{nat} \rightarrow \} \) requires that we introduce a new typing judgement, \( k : \tau \), stating that the stack \( k \) expects a value of type \( \tau \). This judgement is inductively defined by the following rules:

\[
\begin{align*}
\bar{e} & : \tau & \quad (27.7a) \\
\frac{k : \tau' \quad f : \tau \Rightarrow \tau'}{k ; f : \tau} & \quad (27.7b)
\end{align*}
\]

This definition makes use of an auxiliary judgement, \( f : \tau \Rightarrow \tau' \), stating that a frame \( f \) transforms a value of type \( \tau \) to a value of type \( \tau' \).

\[
\begin{align*}
s(-) & : \text{nat} \Rightarrow \text{nat} & \quad (27.8a) \\
\frac{e_1 : \tau \quad x : \text{nat} \vdash e_2 : \tau}{\text{ifz}(-;e_1;x.e_2) : \text{nat} \Rightarrow \tau} & \quad (27.8b) \\
\frac{e_2 : \tau_2}{\text{ap}(-;e_2) : \text{arr} (\tau_2; \tau) \Rightarrow \tau} & \quad (27.8c)
\end{align*}
\]

The two forms of \( K\{\text{nat} \rightarrow \} \) state are well-formed provided that their stack and expression components match.

\[
\begin{align*}
\frac{k : \tau \quad e : \tau}{k \triangleright e \ ok} & \quad (27.9a) \\
\frac{k : \tau \quad e : \tau \quad e \text{ val}}{k \triangleleft e \ ok} & \quad (27.9b)
\end{align*}
\]

We leave the proof of safety of \( K\{\text{nat} \rightarrow \} \) as an exercise.

**Theorem 27.1 (Safety).**

1. If \( s \ \text{ok and } s \mapsto s' \), then \( s' \ \text{ok} \).

2. If \( s \ \text{ok} \), then either \( s \ \text{final} \) or there exists \( s' \) such that \( s \mapsto s' \).
27.3 Correctness of the Control Machine

It is natural to ask whether \( K: \text{nat} \rightarrow \) correctly implements \( L: \text{nat} \rightarrow \). If we evaluate a given expression, \( e \), using \( K: \text{nat} \rightarrow \), do we get the same result as would be given by \( L: \text{nat} \rightarrow \), and vice versa?

Answering this question decomposes into two conditions relating \( K: \text{nat} \rightarrow \) to \( L: \text{nat} \rightarrow \):

**Completeness** If \( e \mapsto^* e' \), where \( e' \)val, then \( e \mapsto^* e \triangleleft e' \).

**Soundness** If \( e \mapsto^* e \triangleleft e' \), then \( e \mapsto^* e' \) with \( e' \)val.

Let us consider, in turn, what is involved in the proof of each part.

For completeness it is natural to consider a proof by induction on the definition of multistep transition, which reduces the theorem to the following two lemmas:

1. If \( e \)val, then \( e \mapsto^* e \triangleleft e \).

2. If \( e \mapsto e' \), then, for every \( v \)val, if \( e \mapsto^* e \triangleleft v \), then \( e \mapsto^* e \triangleleft v \).

The first can be proved easily by induction on the structure of \( e \). The second requires an inductive analysis of the derivation of \( e \mapsto e' \), giving rise to two complications that must be accounted for in the proof. The first complication is that we cannot restrict attention to the empty stack, for if \( e \) is, say, \( \text{ap}(e_1; e_2) \), then the first step of the machine is

\[
\begin{align*}
k &\mapsto \text{ap}(e_1; e_2) \mapsto \text{ap}(e_1; e_2) \mapsto e_1,
\end{align*}
\]

and so we must consider evaluation of \( e_1 \) on a non-empty stack.

A natural generalization is to prove that if \( e \mapsto e' \) and \( k \mapsto^* k \triangleleft v \), then \( k \mapsto^* k \triangleleft v \). Consider again the case \( e = \text{ap}(e_1; e_2), e' = \text{ap}(e_1'; e_2) \), with \( e_1 \mapsto e_1' \). We are given that \( k \mapsto \text{ap}(e_1'; e_2) \mapsto^* k \triangleleft v \), and we are to show that \( k \mapsto \text{ap}(e_1; e_2) \mapsto^* k \triangleleft v \). It is easy to show that the first step of the former derivation is

\[
\begin{align*}
k &\mapsto \text{ap}(e_1'; e_2) \mapsto k; \text{ap}(e_1; e_2) \mapsto e_1',
\end{align*}
\]

We would like to apply induction to the derivation of \( e_1 \mapsto e_1' \), but to do so we must have a \( v_1 \) such that \( e_1' \mapsto^* v_1 \), which is not immediately at hand.

This means that we must consider the ultimate value of each sub-expression of an expression in order to complete the proof. This information is provided by the evaluation semantics described in Chapter 12, which has the property that \( e \downarrow e' \) iff \( e \mapsto^* e' \) and \( e' \)val.
Lemma 27.2. If $e \Downarrow v$, then for every $k$ stack, $k \triangleright e \rightarrow^* k \triangleleft v$.

The desired result follows by the analogue of Theorem 12.2 on page 93 for $L\{\text{nat} \rightarrow\}$, which states that $e \Downarrow v$ if $e \rightarrow^* v$.

For the proof of soundness, it is awkward to reason inductively about the multistep transition from $e \triangleright e \rightarrow^* e \triangleleft v$, because the intervening steps may involve alternations of evaluation and return states. Instead we regard each $K\{\text{nat} \rightarrow\}$ machine state as encoding an expression, and show that $K\{\text{nat} \rightarrow\}$ transitions are simulated by $L\{\text{nat} \rightarrow\}$ transitions under this encoding.

Specifically, we define a judgement, $s \leftrightarrow e$, stating that state $s$ “unravels to” expression $e$. It will turn out that for initial states, $s = e \triangleright e$, and final states, $s = e \triangleleft e$, we have $s \leftrightarrow e$. Then we show that if $s \rightarrow^* s'$, where $s'$ final, $s \leftrightarrow e$, and $s' \leftrightarrow e'$, then $e'$ val and $e \rightarrow^* e'$. For this it is enough to show the following two facts:

1. If $s \leftrightarrow e$ and $s$ final, then $e$ val.

2. If $s \rightarrow s'$, $s \leftrightarrow e$, $s' \leftrightarrow e'$, and $e' \rightarrow^* v$, where $v$ val, then $e \rightarrow^* v$.

The first is quite simple, we need only observe that the unravelling of a final state is a value. For the second, it is enough to show the following lemma.

Lemma 27.3. If $s \rightarrow s'$, $s \leftrightarrow e$, and $s' \leftrightarrow e'$, then $e \rightarrow^* e'$.

Corollary 27.4. $e \rightarrow^* \overline{n}$ iff $e \triangleright e \rightarrow^* e \triangleleft \overline{n}$.

The remainder of this section is devoted to the proofs of the soundness and completeness lemmas.

27.3.1 Completeness

Proof of Lemma 27.2. The proof is by induction on an evaluation semantics for $L\{\text{nat} \rightarrow\}$.

Consider the evaluation rule

\[
\begin{align*}
e_1 \Downarrow 1\text{am}[\text{\tau}_2](x.e) [e_2/x]e \Downarrow v \\
\text{ap}(e_1; e_2) \Downarrow v
d\end{align*}
\]

(27.10)

For an arbitrary control stack, $k$, we are to show that $k \triangleright \text{ap}(e_1; e_2) \rightarrow^* k \triangleleft v$. Applying both of the inductive hypotheses in succession, interleaved with

14:36
steps of the abstract machine, we obtain
\[ k \triangleright \text{ap}(e_1;e_2) \mapsto k; \text{ap}(-';e_2) \triangleright e_1 \]
\[ \mapsto^* k; \text{ap}(-';e_2) \triangleleft \text{lam}(\tau_2)(x.e) \]
\[ \mapsto k \triangleright [e_2/x]e \]
\[ \mapsto^* k \triangleleft v. \]

The other cases of the proof are handled similarly.

27.3.2 Soundness

The judgement \( s \rightsquigarrow e' \), where \( s \) is either \( k \triangleright e \) or \( k \triangleleft e \), is defined in terms of the auxiliary judgement \( k \triangleleft \triangleleft e = e' \) by the following rules:

\[
\begin{align*}
k \triangleleft \triangleleft e &= e' \\
k \triangleright e &\rightsquigarrow e' \tag{27.11a}
\end{align*}
\]

\[
\begin{align*}
k \triangleleft \triangleleft e &= e' \\
k \triangleleft e &\rightsquigarrow e' \tag{27.11b}
\end{align*}
\]

In words, to unravel a state we wrap the stack around the expression. The latter relation is inductively defined by the following rules:

\[
\begin{align*}
\epsilon \triangleleft \triangleleft e &= e \tag{27.12a}
\end{align*}
\]

\[
\begin{align*}
k \triangleleft \triangleleft s(e) &= e' \\
k; s(-) \triangleleft \triangleleft e &= e' \tag{27.12b}
\end{align*}
\]

\[
\begin{align*}
k \triangleleft \triangleleft \text{ifz}(e_1;e_2;x.e_3) &= e' \\
k; \text{ifz}(-;e_2;x.e_3) \triangleleft \triangleleft e_1 &= e' \tag{27.12c}
\end{align*}
\]

\[
\begin{align*}
k \triangleright \triangleleft \text{ap}(e_1;e_2) &= e \\
k; \text{ap}(-;e_2) \triangleleft \triangleleft e_1 &= e \tag{27.12d}
\end{align*}
\]

These judgements both define total functions.

**Lemma 27.5.** The judgement \( s \rightsquigarrow e \) has mode \( (\forall, \exists!) \), and the judgement \( k \triangleleft \triangleleft e = e' \) has mode \( (\forall, \forall, \exists!) \).

That is, each state unravels to a unique expression, and the result of wrapping a stack around an expression is uniquely determined. We are therefore justified in writing \( k \triangleleft \triangleleft e \) for the unique \( e' \) such that \( k \triangleleft \triangleleft e = e' \).

The following lemma is crucial. It states that unravelling preserves the transition relation.
Lemma 27.6. If \( e \mapsto e' \), \( k \triangleright e = d \), \( k \triangleright e' = d' \), then \( d \mapsto d' \).

Proof. The proof is by rule induction on the transition \( e \mapsto e' \). The inductive cases, in which the transition rule has a premise, follow easily by induction. The base cases, in which the transition is an axiom, are proved by an inductive analysis of the stack, \( k \).

For an example of an inductive case, suppose that \( e = \text{ap}(e_1; e_2) \), \( e' = \text{ap}(e'_1; e_2) \), and \( e_1 \mapsto e'_1 \). We have \( k \triangleright e = d \) and \( k \triangleright e' = d' \). It follows from Rules (27.12) that \( k; \text{ap}(\neg; e_2) \triangleright e_1 = d \) and \( k; \text{ap}(\neg; e_2) \triangleright e'_1 = d' \). So by induction \( d \mapsto d' \), as desired.

For an example of a base case, suppose that \( e = \text{ap}(\text{lam}[	au_2](x . e); e_2) \) and \( e' = [e_2/x]e \) with \( e \mapsto e' \) directly. Assume that \( k \triangleright e = d \) and \( k \triangleright e' = d' \); we are to show that \( d \mapsto d' \). We proceed by an inner induction on the structure of \( k \). If \( k = \epsilon \), the result follows immediately. Consider, say, the stack \( k = k' \triangleright \text{ap}(\neg; c_2) \). It follows from Rules (27.12) that \( k' \triangleright \text{ap}(c_2) = d \) and \( k' \triangleright \text{ap}(e'; c_2) = d' \). But by the SOS rules \( \text{ap}(c_2) \mapsto \text{ap}(e'; c_2) \), so by the inner inductive hypothesis we have \( d \mapsto d' \), as desired.

We are now in a position to complete the proof of Lemma 27.3 on page 240.

Proof of Lemma 27.3 on page 240. The proof is by case analysis on the transitions of \( \mathcal{K}\{\text{nat} \rightarrow \} \). In each case after unravelling the transition will correspond to zero or one transitions of \( \mathcal{L}\{\text{nat} \rightarrow \} \).

Suppose that \( s = k \triangleright s(e) \) and \( s' = k \triangleright e \). Note that \( k \triangleright s(e) = e' \) iff \( k; s(\neg) \triangleright e = e' \), from which the result follows immediately.

Suppose that \( s = k \triangleright \text{ap}(\text{lam}[	au](x . e_1); \neg) < e_2 \) and \( s' = k \triangleright [e_2/x]e_1 \). Let \( e' \) be such that \( k; \text{ap}(\text{lam}[	au](x . e_1); \neg) \triangleright e_2 = e' \) and let \( e'' \) be such that \( k \triangleright [e_2/x]e_1 = e'' \). Observe that \( k \triangleright \text{ap}(\text{lam}[	au](x . e_1); e_2) = e' \). The result follows from Lemma 27.6.

\( \square \)

27.4 Exercises
Chapter 28

Exceptions

Exceptions effect a non-local transfer of control from the point at which the exception is raised to an enclosing handler for that exception. This transfer interrupts the normal flow of control in a program in response to unusual conditions. For example, exceptions can be used to signal an error condition, or to indicate the need for special handling in certain circumstances that arise only rarely. To be sure, one could use explicit conditionals to check for and process errors or unusual conditions, but using exceptions is often more convenient, particularly since the transfer to the handler is direct and immediate, rather than indirect via a series of explicit checks.

28.1 Failures

A failure is a control mechanism that permits a computation to refuse to return a value to the point of its evaluation. Failure can be detected by catching it, diverting evaluation to another expression, called a handler. Failure can be turned into success, provided that the handler does not itself fail.

The following grammar defines the syntax of failures:

\[
\begin{array}{c|c|c|c}
\text{Category} & \text{Item} & \text{Abstract} & \text{Concrete} \\
\hline
\text{Expr} & e & \text{fail} & \text{fail} \\
& & \text{catch}(e_1; e_2) & \text{catch } e_1 \text{ ow } e_2 \\
\end{array}
\]

The expression fail aborts the current evaluation, and the expression catch\((e_1; e_2)\) handles any failure in \(e_1\) by evaluating \(e_2\) instead.

The static semantics of failures is straightforward:

\[
\Gamma \vdash \text{fail} : \tau
\]  
(28.1a)
A failure can have any type, because it never returns. The two expressions in a catch expression must have the same type, since either might determine the value of that expression.

The dynamic semantics of failures may be given using *stack unwinding*. Evaluation of a catch installs a handler on the control stack. Evaluation of a fail unwinds the control stack by popping frames until it reaches the nearest enclosing handler, to which control is passed. The handler is evaluated in the context of the surrounding control stack, so that failures within it propagate further up the stack.

Stack unwinding can be defined directly using structural operational semantics, but we prefer to make use of the stack machine defined in Chapter 27. In addition to states of the form $k \triangleright e$, which evaluates the expression $e$ on the stack $k$, and $k \triangleleft e$, which passes the value $e$ to the stack $k$, we make use of an additional form of state, $k \blacktriangleleft$, which passes a failure up the stack to the nearest enclosing handler.

The set of frames defined in Chapter 27 is extended with the additional form $\text{catch}(\_;e_2)$. The transition rules given in Chapter 27 are extended with the following additional rules:

\begin{align*}
    k \triangleright \text{fail} & \mapsto k \blacktriangleleft \quad \text{(28.2a)} \\
    k \triangleright \text{catch}(e_1;e_2) & \mapsto k;\text{catch}(\_;e_2) \triangleright e_1 \quad \text{(28.2b)} \\
    k;\text{catch}(\_;e_2) \triangleleft v & \mapsto k \triangleleft v \quad \text{(28.2c)} \\
    k;\text{catch}(\_;e_2) \blacktriangleleft & \mapsto k \triangleright e_2 \quad \text{(28.2d)} \\
    (f \neq \text{catch}(\_;e_2)) & \quad \frac{}{k;f \blacktriangleleft \mapsto k \blacktriangleleft} \quad \text{(28.2e)}
\end{align*}

Evaluating fail propagates a failure up the stack. Evaluating catch$(e_1;e_2)$ consists of pushing the handler onto the control stack and evaluating $e_1$. If a value is propagated to the handler, the handler is removed and the value continues to propagate upwards. If a failure is propagated to the
28.2 Exceptions

Failures are simplistic in that they do not distinguish different causes, and hence do not permit handlers to react differently to different circumstances. An exception is a generalization of a failure that associates a value with the failure. This value is passed to the handler, allowing it to discriminate between various forms of failures, and to pass data appropriate to that form of failure. The type of values associated with exceptions is discussed in Section 28.3 on page 247. For now, we simply assume that there is some type, $\tau_{exn}$, of values associated with a failure.

The syntax of exceptions is given by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expr</td>
<td>$e$</td>
<td>$\text{raise}<a href="e">\tau</a>$</td>
<td>$\text{raise}(e)$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{handle}(e_1;x,e_2)$</td>
<td>$\text{handle}e_1\text{ow }x \Rightarrow e_2$</td>
</tr>
</tbody>
</table>

Theorem 28.1 (Safety). 1. If $s\text{ ok}$ and $s \mapsto s'$, then $s'\text{ ok}$.

2. If $s\text{ ok}$, then either $s\text{ final}$ or there exists $s'$ such that $s \mapsto s'$.
The argument to `raise` is evaluated to determine the value passed to the handler. The expression `handle(e_1; x . e_2)` binds a variable, `x`, in the handler, `e_2`, to which the associated value of the exception is bound, should an exception be raised during the execution of `e_1`.

The statics of exceptions generalizes that of failures:

\[
\frac{\Gamma \vdash e : \tau_{\text{exn}}}{\Gamma \vdash \text{raise}[^\tau](e) : \tau} \quad (28.4a)
\]

\[
\frac{\Gamma \vdash e_1 : \tau \quad \Gamma, x : \tau_{\text{exn}} \vdash e_2 : \tau}{\Gamma \vdash \text{handle}(e_1; x . e_2) : \tau} \quad (28.4b)
\]

The dynamics of exceptions is a mild generalization of the dynamics of failures in which we generalize the failure state, \(k \triangleleft\), to the exception state, \(k \triangleleft e\), which passes a value of type \(\tau_{\text{exn}}\) along with the failure. The syntax of stack frames is extended to include `raise[^\tau](−)` and `handle(−; x . e_2)`. The dynamics of exceptions is specified by the following rules:

\[
\frac{k \triangleright \text{raise}[^\tau](e) \mapsto k; \text{raise}[^\tau](−) \triangleright e}{(28.5a)}
\]

\[
\frac{k; \text{raise}[^\tau](−) \triangleleft e \mapsto k \triangleleft e}{(28.5b)}
\]

\[
\frac{k; \text{raise}[^\tau](−) \triangleleft e \mapsto k \triangleleft e}{(28.5c)}
\]

\[
\frac{k \triangleright \text{handle}(e_1; x . e_2) \mapsto k; \text{handle}(−; x . e_2) \triangleright e_1}{(28.5d)}
\]

\[
\frac{k; \text{handle}(−; x . e_2) \triangleleft e \mapsto k \triangleleft e}{(28.5e)}
\]

\[
\frac{k; \text{handle}(−; x . e_2) \triangleleft e \mapsto k \triangleright [e/x]e_2}{(28.5f)}
\]

\[
\frac{(f \neq \text{handle}(−; x . e_2))}{k; f \triangleleft e \mapsto k \triangleleft e} \quad (28.5g)
\]

It is a straightforward exercise to extend the safety theorem given in Section 28.1 on page 243 to exceptions.
28.3 Exception Type

The static semantics of exceptions is parameterized by the type of exception values, $\tau_{\text{exn}}$. This type may be chosen arbitrarily, but it must be shared by all exceptions in a program to ensure type safety. For otherwise a handler cannot tell what type of value to expect from an exception, compromising safety.

But how do we choose the type of exceptions? A very naïve choice would be to take $\tau_{\text{exn}}$ to be the type $\text{str}$, so that, for example, one may write

\[
\text{raise } "\text{Division by zero error.}" 
\]

to signal the obvious arithmetic fault. This is fine as far as it goes, but a handler for such an exception would have to interpret the string if it is to distinguish one exception from another!

Motivated by this, we might choose $\tau_{\text{exn}}$ to be $\text{nat}$, which amounts to saying that exceptional conditions are coded as natural numbers.\footnote{In Unix these are called \texttt{errno}'s, for \textit{error numbers.}} This does allow the handler to distinguish one source of failure from another, but makes no provision for associating data with the failure. Moreover, it forces the programmer to impose a single, global convention for indexing the causes of failure, compromising modular development and evolution.

The first concern—how to associate data specific to the type of failure—can be addressed by taking $\tau_{\text{exn}}$ to be a labelled sum type whose classes are the forms of failure, and whose associated types determine the form of the data attached to the exception. For example, the type $\tau_{\text{exn}}$ might have the form

\[
\tau_{\text{exn}} = \left[ \text{div:unit, fnf:string, ...} \right].
\]

The class $\text{div}$ might represent an arithmetic fault, with no associated data, and the class $\text{fnf}$ might represent a “file not found” error, with associated data being the name of the file.

Using a sum type for $\tau_{\text{exn}}$ makes it easy for the handler to discriminate on the source of the failure, and to recover the associated data without fear of a type safety violation. For example, we might write

\[
\text{try e}_1 \text{ ow x } \Rightarrow \\
\text{match x } \{ \\
\text{ div } \langle \rangle \Rightarrow e_{\text{div}} \\
| \text{ fnf } s \Rightarrow e_{\text{fnf}} \}
\]
Encapsulation

to handle the exceptions specified by the sum type given in the preceding paragraph.

The problem with choosing a sum type for $\tau_{exn}$ is that it imposes a static classification of the sources of failure in a program. There must be one, globally agreed-upon type that classifies all possible forms of failure, and specifies their associated data. Using sums in this manner impedes modular development and evolution, since all of the modules comprising a system must agree on the one, central type of exception values. A better approach is to use dynamic classification for exception values by choosing $\tau_{exn}$ to be an extensible sum, one to which new classes may be added at execution time. This allows separate program modules to introduce their own failure classification scheme without worrying about interference with one another; the initialization of the module generates new classes at run-time that are guaranteed to be distinct from all other classes previously or subsequently generated. (See Chapter 36 for more on dynamic classification.)

28.4 Encapsulation

It is sometimes useful to distinguish expressions that can fail or raise an exception from those that cannot. An expression is called fallible, or exceptional, if it can fail or raise an exception during its evaluation, and is infallible, or unexceptional, otherwise. The concept of fallibility is intentionally permissive in that an infallible expression may be considered to be (vacuously) fallible, whereas infallibility is intended to be strict in that an infallible expression cannot fail. Consequently, if $e_1$ and $e_2$ are two infallible expressions both of whose values are required in a computation, we may evaluate them in either order without affecting the outcome. If, on the other hand, one or both are fallible, then the outcome of the computation is sensitive to the evaluation order (whichever fails first determines the overall result).

To formalize this distinction we distinguish two modes of expression, the fallible and the infallible, linked by a modality classifying the fallible
28.4 Encapsulation

expressions of a type.

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>τ</td>
<td>::= fallible(τ)</td>
<td>τ fallible</td>
</tr>
<tr>
<td>Fallible</td>
<td>f</td>
<td>::= fail</td>
<td>fail</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>succ(e)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>try(e; x. f₁; f₂)</td>
</tr>
<tr>
<td>Infallible</td>
<td>e</td>
<td>::= x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>fall(f)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>try(e; x. e₁; e₂)</td>
</tr>
</tbody>
</table>

The type τ fallible is the type of encapsulated fallible expressions of type τ. Fallible expressions include failures, successes (infallible expressions thought of as vacuously fallible), and handlers that intercept failures, but which may itself fail. Infallible expressions include variables, encapsulated fallible expressions, and handlers that intercepts failures, always yielding an infallible result.

The static semantics of encapsulated failures consists of two judgement forms, \( \Gamma \vdash e : \tau \) for infallible expressions and \( \Gamma \vdash f : \sim \tau \) for fallible expressions. These judgements are defined by the following rules:

\[
\begin{align*}
\Gamma, x : \tau & \vdash x : \tau \quad (28.6a) \\
\Gamma \vdash f : \sim \tau & \quad \Gamma \vdash \text{fail}(f) : \text{fallible}(\tau) \quad (28.6b) \\
\Gamma \vdash e : \text{fallible}(\tau) & \quad \Gamma, x : \tau \vdash e_1 : \tau' \quad \Gamma \vdash e_2 : \tau' \quad \Gamma \vdash \text{try}(e; x. e_1; e_2) : \tau' \quad (28.6c) \\
\Gamma \vdash \text{fail} : \sim \tau & \quad (28.6d) \\
\Gamma \vdash e : \tau & \quad \Gamma \vdash \text{succ}(e) : \sim \tau \quad (28.6e) \\
\Gamma \vdash e : \text{fallible}(\tau) & \quad \Gamma, x : \tau \vdash f_1 : \sim \tau' \quad \Gamma \vdash f_2 : \sim \tau' \quad \Gamma \vdash \text{try}(e; x. f_1; f_2) : \tau' \quad (28.6f)
\end{align*}
\]

Rule (28.6c) specifies that a handler may be used to turn a fallible expression (encapsulated by \( e \)) into an infallible computation, provided that the result is infallible regardless of whether the encapsulated expression succeeds or fails.
The dynamics of encapsulated failures is readily derived, though some care must be taken with the elimination form for the modality.

\[
\text{fall}(f) \ni \text{val}
\]  

(28.7a)

\[
k \triangleright \text{try}(e; x. e_1; e_2) \mapsto k; \text{try}(\neg; x. e_1; e_2) \ni e
\]

(28.7b)

\[
k; \text{try}(\neg; x. e_1; e_2) \ni \text{fall}(f) \mapsto k; \text{try}(\neg; x. e_1; e_2); \text{fall}(\neg) \ni f
\]

(28.7c)

\[
k \triangleright \text{fall} \mapsto k
\]

(28.7d)

\[
k \triangleright \text{succ}(e) \mapsto k; \text{succ}(\neg) \ni e
\]

(28.7e)

\[
k \triangleright \text{succ}(e) \mapsto k \ni \text{succ}(e)
\]

(28.7f)

\[
k; \text{try}(\neg; x. e_1; e_2); \text{fall}(\neg) \ni e \mapsto k \triangleright [e/x]e_1
\]

(28.7g)

\[
k; \text{try}(\neg; x. e_1; e_2); \text{fall}(\neg) \ni \ni k \ni e_2
\]

(28.7h)

We have omitted the rules for the fallible form of handler; they are similar to Rules (28.7b) to (28.7b) and (28.7g) to (28.7h), albeit with infallible subexpressions \(e_1\) and \(e_2\) replaced by fallible subexpressions \(f_1\) and \(f_2\).

An initial state has the form \(k \triangleright e\), where \(e\) is an infallible expression, and \(k\) is a stack of suitable type. Consequently, a fallible expression, \(f\), can only be evaluated on a stack of the form

\[
k; \text{try}(\neg; x. e_1; e_2); \text{fall}(\neg)
\]

in which a handler for any failure that may arise from \(f\) is present. Therefore, a final state has the form \(\varepsilon \ni e\), where \(e\ \text{val}\); no uncaught failure can arise.

28.5 Exercises
Chapter 29

Continuations

The semantics of many control constructs (such as exceptions and co-routines) can be expressed in terms of reified control stacks, a representation of a control stack as an ordinary value. This is achieved by allowing a stack to be passed as a value within a program and to be restored at a later point, even if control has long since returned past the point of reification. Reified control stacks of this kind are called first-class continuations, where the qualification “first class” stresses that they are ordinary values with an indefinite lifetime that can be passed and returned at will in a computation. First-class continuations never “expire”, and it is always sensible to reinstate a continuation without compromising safety. Thus first-class continuations support unlimited “time travel” — we can go back to a previous point in the computation and then return to some point in its future, at will.

Why are first-class continuations useful? Fundamentally, they are representations of the control state of a computation at a given point in time. Using first-class continuations we can “checkpoint” the control state of a program, save it in a data structure, and return to it later. In fact this is precisely what is necessary to implement threads (concurrently executing programs) — the thread scheduler must be able to checkpoint a program and save it for later execution, perhaps after a pending event occurs or another thread yields the processor.

29.1 Informal Overview

We will extend $L\{\to\}$ with the type $\text{cont}(\tau)$ of continuations accepting values of type $\tau$. The introduction form for $\text{cont}(\tau)$ is $\text{letcc}[\tau](x.e)$, which binds the current continuation (that is, the current control stack) to the
variable \( x \), and evaluates the expression \( e \). The corresponding elimination form is \( \text{throw}[\tau](e_1;e_2) \), which restores the value of \( e_1 \) to the control stack that is the value of \( e_2 \).

To illustrate the use of these primitives, consider the problem of multiplying the first \( n \) elements of an infinite sequence \( q \) of natural numbers, where \( q \) is represented by a function of type \( \text{nat} \to \text{nat} \). If zero occurs among the first \( n \) elements, we would like to effect an "early return" with the value zero, rather than perform the remaining multiplications. This problem can be solved using exceptions (we leave this as an exercise), but we will give a solution that uses continuations in preparation for what follows.

Here is the solution in \( \mathcal{L}\{\text{nat} \to \} \), without short-cutting:

\[
\begin{align*}
\text{fix } ms & \text{ is} \\
& \lambda q : \text{nat} \to \text{nat}. \\
& \lambda n : \text{nat}. \\
& \text{case } n \{ \\
& \quad z \Rightarrow s(z) \\
& \quad \mid s(n') \Rightarrow (q\ z) \times (ms\ (q \circ \text{succ})\ n')
\}
\end{align*}
\]

The recursive call composes \( q \) with the successor function to shift the sequence by one step.

Here is the version with short-cutting:

\[
\begin{align*}
\text{letcc } ret : \text{nat cont in} \\
& \text{let } ms \text{ be } \\
& \text{fix } ms \text{ is} \\
& \lambda q : \text{nat} \to \text{nat}. \\
& \lambda n : \text{nat}. \\
& \text{let } cc \text{ be} \\
& \text{case } n \{ \\
& \quad z \Rightarrow s(z) \\
& \quad \mid s(n') \Rightarrow (q\ z) \times (ms\ (q \circ \text{succ})\ n')
\}
\end{align*}
\]

14:36 Draft December 18, 2009
29.2 Semantics of Continuations

The letcc binds the return point of the function to the variable ret for use within the main loop of the computation. If zero is encountered, control is thrown to ret, effecting an early return with the value zero.

Let’s look at another example: given a continuation k of type τ cont and a function f of type τ’ → τ, return a continuation k’ of type τ’ cont with the following behavior: throwing a value v’ of type τ’ to k’ throws the value f(v’) to k. This is called composition of a function with a continuation. We wish to fill in the following template:

\[
\text{fun compose}(f : \tau' \to \tau, k : \tau \text{cont}) : \tau' \text{cont} = \ldots
\]

The first problem is to obtain the continuation we wish to return. The second problem is how to return it. The continuation we seek is the one in effect at the point of the ellipsis in the expression \(\text{throw } f(...) \text{ to } k\). This is the continuation that, when given a value v’, applies f to it, and throws the result to k. We can seize this continuation using letcc, writing

\[
\text{throw } f(\text{letcc } x : \tau' \text{cont in } \ldots) \text{ to } k
\]

At the point of the ellipsis the variable x is bound to the continuation we wish to return. How can we return it? By using the same trick as we used for short-circuiting evaluation above! We don’t want to actually throw a value to this continuation (yet), instead we wish to abort it and return it as the result. Here’s the final code:

\[
\text{fun compose } (f : \tau' \to \tau, k : \tau \text{cont}) : \tau' \text{cont} =
\begin{align*}
\text{letcc } \text{ret} : \tau' \text{cont cont in} \\
\text{throw } (f (\text{letcc } r \text{ in throw } r \text{ to } ret)) \text{ to } k
\end{align*}
\]

The type of ret is that of a continuation-expecting continuation!

### 29.2 Semantics of Continuations

We extend the language of \(L\{\to\}\) expressions with these additional forms:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>(\tau)</td>
<td>(\text{cont}(\tau))</td>
<td>(\tau \text{cont})</td>
</tr>
<tr>
<td>Expr</td>
<td>(e)</td>
<td>(\text{letcc}[x]_e)</td>
<td>(\text{letcc } x \text{ in } e)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(\text{throw}[\tau]_{e_1;e_2})</td>
<td>(\text{throw } e_1 \text{ to } e_2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(\text{cont}(k))</td>
<td></td>
</tr>
</tbody>
</table>

The expression \(\text{cont}(k)\) is a reified control stack; they arise during evaluation, but are not available as expressions to the programmer.
29.2 Semantics of Continuations

The static semantics of this extension is defined by the following rules:

\[ \Gamma, x : \text{cont}(\tau) \vdash e : \tau \]
\[ \Gamma \vdash \text{letcc}[\tau](x . e) : \tau \] (29.1a)

\[ \Gamma \vdash e_1 : \tau_1 \quad \Gamma \vdash e_2 : \text{cont}(\tau_1) \]
\[ \Gamma \vdash \text{throw}[\tau'](e_1 ; e_2) : \tau' \] (29.1b)

The result type of a \text{throw} expression is arbitrary because it does not return to the point of the call.

The static semantics of continuation values is given by the following rule:

\[ k : \tau \]
\[ \Gamma \vdash \text{cont}(k) : \text{cont}(\tau) \] (29.2)

A continuation value \text{cont}(k) has type \text{cont}(\tau) exactly if it is a stack accepting values of type \tau.

To define the dynamic semantics, we extend \( \mathcal{K}\{\text{nat} \rightarrow\} \) stacks with two new forms of frame:

\[ e_2 \text{ exp} \]
\[ \frac{\text{throw}[\tau](--;e_2) \text{ frame}}{} \] (29.3a)

\[ e_1 \text{ val} \]
\[ \frac{\text{throw}[\tau](e_1 ; --) \text{ frame}}{} \] (29.3b)

Every reified control stack is a value:

\[ k \text{ stack} \]
\[ \frac{\text{cont}(k) \text{ val}}{} \] (29.4)

The transition rules for the continuation constructs are as follows:

\[ k \triangleright \text{letcc}[\tau](x . e) \mapsto k \triangleright [\text{cont}(k)/x]e \] (29.5a)

\[ k ; \text{throw}[\tau](v; --) \triangleleft \text{cont}(k') \mapsto k' \triangleleft v \] (29.5b)

\[ k \triangleright \text{throw}[\tau](e_1 ; e_2) \mapsto k ; \text{throw}[\tau](--;e_2) \triangleright e_1 \] (29.5c)

\[ e_1 \text{ val} \]
\[ \frac{k ; \text{throw}[\tau](--;e_2) \triangleleft e_1 \mapsto k ; \text{throw}[\tau](e_1 ; --) \triangleright e_2}{k ; \text{throw}[\tau](--;e_2) \triangleleft e_1 \mapsto k ; \text{throw}[\tau](e_1 ; --) \triangleright e_2} \] (29.5d)

Evaluation of a \text{letcc} expression duplicates the control stack; evaluation of a \text{throw} expression destroys the current control stack.
29.3 Coroutines

The safety of this extension of \( \mathcal{L} \{ \rightarrow \} \) may be established by a simple extension to the safety proof for \( \mathcal{K} \{ \text{nat} \rightarrow \} \) given in Chapter 27.

We need only add typing rules for the two new forms of frame, which are as follows:

\[
\frac{e_2 : \text{cont}(\tau)}{\text{throw}[\tau](\_; e_2) : \tau \Rightarrow \tau'} \quad (29.6a)
\]

\[
\frac{e_1 : \tau \quad e_1 \text{ val}}{\text{throw}[\tau](e_1; \_): \text{cont}(\tau) \Rightarrow \tau'} \quad (29.6b)
\]

The rest of the definitions remain as in Chapter 27.

**Lemma 29.1** (Canonical Forms). If \( e : \text{cont}(\tau) \) and \( e \text{ val} \), then \( e = \text{cont}(k) \) for some \( k \) such that \( k : \tau \).

**Theorem 29.2** (Safety). 1. If \( s \text{ ok} \) and \( s \rightarrow s' \), then \( s' \text{ ok} \).

2. If \( s \text{ ok} \), then either \( s \text{ final} \) or there exists \( s' \) such that \( s \rightarrow s' \).

29.3 Coroutines

A familiar pattern of control flow in a program distinguishes the main routine of a computation, which represents the principal control path of the program, from a sub-routine, which represents a subsidiary path that performs some auxiliary computation. The main routine invokes the subroutine by passing it a data value, its argument, and a control point to return to once it has completed its work. This arrangement is asymmetric in that the main routine plays the active role, whereas the subroutine is passive. In particular the subroutine passes control directly to the return point without itself providing a return point with which it can be called back. A coroutine is a symmetric pattern of control flow in which each routine passes to the other the return point of the call. The asymmetric call/return pattern is symmetrized to a call/call pattern in which each routine is effectively a subroutine of the other. (This raises an interesting question of how the interaction commences, which we will discuss in more detail below.)

To see how coroutines are implemented in terms of continuations, it is best to think of the “steady state” interaction between the two routines, leaving the initialization phase to be discussed separately. A routine is represented by a continuation that, when invoked, is passed a data item, whose type is shared between the two routines, and a return continuation,
which represents the partner routine. Crucially, the argument type of the other continuation is again of the very same form, consisting of a data item and another return continuation. If we think of the coroutine as a trajectory through a succession of such continuations, then the state of the continuation (which changes as the interaction progresses) satisfies the type isomorphism

$$\text{state} \cong (\tau \times \text{state}) \text{cont},$$

where $\tau$ is the type of data exchanged by the routines. The solution to such an isomorphism is, of course, the recursive type

$$\text{state} = \mu t. (\tau \times t) \text{cont}.$$

Thus a state, $s$, encapsulates a pair consisting of a value of type $\tau$ together with another state.

The routines pass control from one to the other by calling the function resume of type

$$\tau \times \text{state} \to \tau \times \text{state}.$$

That is, given a datum, $d$, and a state, $s$, the application $\text{resume}(\langle d, s \rangle)$ passes $d$ and its own return address to the routine represented by the state $s$. The function resume is defined by the following expression:

$$\lambda (\langle x, s \rangle : \tau \times \text{state}. \text{let} \text{cc} k \in \text{throw}(x, \text{fold}(k)) \to \text{unfold}(s))$$

When applied, this function seizes the current continuation, and passes the given datum and this continuation to the partner routine, using the isomorphism between state and $(\tau \times \text{state}) \text{cont}$.

The general form of a coroutine consists of a loop that, on each iteration, takes a datum, $d$, and a state, $s$, performs a transformation on $d$, resuming its partner routine with the result, $d'$, of the transformation. The function corout builds a coroutine from a data transformation routine; it has type

$$(\tau \to \tau) \to (\tau \times \text{state}) \to \tau'.$$

The result type, $\tau'$, is arbitrary, because the routine never returns to the call site. A coroutine is shut down by an explicit exit operation, which will be specified shortly. The function corout is defined by the following expression (with types omitted for concision):

$$\lambda \text{next. fix loop is } \lambda \langle d, s \rangle. \text{loop(} \text{resume}(\langle \text{next}(d), s \rangle)) \rangle.$$ 

Each time through the loop, the partner routine, $s$, is resumed with the updated datum given by applying next to the current datum, $d$.  

14:36  
DRAFT  
DECEMBER 18, 2009
Let $\rho$ be the ultimate type of a computation consisting of two interacting coroutines that exchanges values of type $\tau$ during their execution. The function $\text{run}$, which has type

$$\tau \rightarrow ((\rho \text{ cont} \rightarrow \tau \rightarrow \tau) \times (\rho \text{ cont} \rightarrow \tau \rightarrow \tau)) \rightarrow \rho,$$$$

takes an initial value of type $\tau$ and two routines, each of type

$$\rho \text{ cont} \rightarrow \tau \rightarrow \tau,$$$$

and builds a coroutine of type $\rho$ from them. The first argument to each routine is the exit point, and the result is a data transformation operation. The definition of $\text{run}$ begins as follows:

$$\lambda \text{ init}. \lambda (r_1, r_2). \text{letcc } \text{exit} \in \text{let } r'_1 \text{ be } r_1(\text{exit}) \text{ in let } r'_2 \text{ be } r_2(\text{exit}) \in \ldots$$

First, $\text{run}$ establishes an exit point that is passed to the two routines to obtain their data transformation components. This allows either or both of the routines to terminate the computation by throwing the ultimate result value to $\text{exit}$. The implementation of $\text{run}$ continues as follows:

$$\text{corout}(r'_2)(\text{letcc } k \text{ in corout}(r'_1)((\text{init}, \text{fold}(k))))$$

The routine $r'_1$ is called with the initial datum, $\text{init}$, and the state $\text{fold}(k)$, where $k$ is the continuation corresponding to the call to $r'_2$. The first $\text{resume}$ from the coroutine built from $r'_1$ will cause the coroutine built from $r'_2$ to be initiated. At this point the steady state behavior is in effect, with the two routines exchanging control using $\text{resume}$. Either may terminate the computation by throwing a result value, $v$, of type $\rho$ to the continuation $\text{exit}$.

A good example of coroutining arises whenever we wish to interleave input and output in a computation. We may achieve this using a coroutine between a $\textit{producer}$ routine and a $\textit{consumer}$ routine. The producer emits the next element of the input, if any, and passes control to the consumer with that element removed from the input. The consumer processes the next data item, and returns control to the producer, with the result of processing attached to the output. The input and output are modeled as lists of type $\tau_i \text{ list}$ and $\tau_o \text{ list}$, respectively, which are passed back and forth between the routines.\footnote{In practice the input and output state are implicit, but we prefer to make them explicit for the sake of clarity.} The routines exchange messages according to the following
protocol. The message \( \text{OK}(\langle i, o \rangle) \) is sent from the consumer to producer to acknowledge receipt of the previous message, and to pass back the current state of the input and output channels. The message \( \text{EMIT}(\langle v, \langle i, o \rangle \rangle) \), where \( v \) is a value of type \( \tau_i \text{opt} \), is sent from the producer to the consumer to emit the next value (if any) from the input, and to pass the current state of the input and output channels to the consumer.

This leads to the following implementation of the producer/consumer model. The type \( \tau \) of data exchanged by the routines is the labelled sum type

\[
[\text{OK}: \tau_i \text{list} \times \tau_o \text{list}, \text{EMIT}: \tau_i \text{opt} \times (\tau_i \text{list} \times \tau_o \text{list})].
\]

This type specifies the message protocol between the producer and the consumer described in the preceding paragraph.

The producer, \( \text{producer} \), is defined by the expression

\[
\lambda \text{exit}. \lambda \text{msg}. \text{case } \text{msg} \{ b_1 \mid b_2 \mid b_3 \},
\]

where the first branch, \( b_1 \), is

\[
\text{OK} \cdot \langle \text{nil}, \text{os} \rangle \Rightarrow \text{EMIT} \cdot \langle \text{null}, \langle \text{nil}, \text{os} \rangle \rangle
\]

and the second branch, \( b_2 \), is

\[
\text{OK} \cdot \langle \text{cons}(i; \text{is}), \text{os} \rangle \Rightarrow \text{EMIT} \cdot \langle \text{just}(i), \langle \text{is}, \text{os} \rangle \rangle,
\]

and the third branch, \( b_3 \), is

\[
\text{EMIT} \cdot _2 \Rightarrow \text{error}.
\]

In words, if the input is exhausted, the producer emits the value \text{null}, along with the current channel state. Otherwise, it emits \text{just}(i), where \( i \) is the first remaining input, and removes that element from the passed channel state. The producer cannot see an \text{EMIT} message, and signals an error if it should occur.

The consumer, \( \text{consumer} \), is defined by the expression

\[
\lambda \text{exit}. \lambda \text{msg}. \text{case } \text{msg} \{ b'_1 \mid b'_2 \mid b'_3 \},
\]

where the first branch, \( b'_1 \), is

\[
\text{EMIT} \cdot \langle \text{null}, \langle \_ , \text{os} \rangle \rangle \Rightarrow \text{throw } \text{os} \text{ to exit},
\]
the second branch, $b'_2$, is
\[
\begin{align*}
\text{EMIT} \cdot \langle \text{just}(i), \langle \text{is}, \text{os} \rangle \rangle & \Rightarrow \text{OK} \cdot \langle \text{is}, \text{cons}(f(i); \text{os}) \rangle, \\
\text{and the third branch, } b'_3, \text{ is } & \\
\text{OK} \cdot \_ & \Rightarrow \text{error}.
\end{align*}
\]

The consumer dispatches on the emitted datum. If it is absent, the output channel state is passed to exit as the ultimate value of the computation. If it is present, the function $f$ (unspecified here) of type $\tau_i \rightarrow \tau_o$ is applied to transform the input to the output, and the result is added to the output channel. If the message OK is received, the consumer signals an error, as the producer never produces such a message.

The initial datum, init, has the form $\text{OK} \cdot \langle \text{is}, \text{os} \rangle$, where is and os are the initial input and output channel state, respectively. The computation is created by the expression
\[
\text{run(init)}(\langle \text{producer}, \text{consumer} \rangle),
\]
which sets up the coroutines as described earlier.

While it is relatively easy to visualize and implement coroutines involving only two partners, it is more complex, and less useful, to consider a similar pattern of control among $n \geq 2$ participants. In such cases it is more common to structure the interaction as a collection of $n$ routines, each of which is a coroutine of a central scheduler. When a routine resumes its partner, it passes control to the scheduler, which determines which routine to execute next, again as a coroutine of itself. When structured as coroutines of a scheduler, the individual routines are called threads. A thread yields control by resuming its partner, the scheduler, which then determines which thread to execute next as a coroutine of itself. This pattern of control is called cooperative multi-threading, since it is based on explicit yields, rather than implicit yields imposed by asynchronous events such as timer interrupts.

29.4 Exercises

1. Study the short-circuit multiplication example carefully to be sure you understand why it works!

2. Attempt to solve the problem of composing a continuation with a function yourself, before reading the solution.
3. Simulate the evaluation of \( \text{compose} \ (f, \ k) \) on the empty stack. Observe that the control stack substituted for \( x \) is

\[
\epsilon; \text{throw}[\tau] (\_; k) ; \text{ap}(f; \_)\]

This stack is returned from \( \text{compose} \). Next, simulate the behavior of throwing a value \( v' \) to this continuation. Observe that the stack is reinstated and that \( v' \) is passed to it.
Part X

Types and Propositions
Chapter 30

Constructive Logic

The correspondence between propositions and types, and the associated correspondence between proofs and programs, is the central organizing principle of programming languages. A type specifies a behavior, and a program implements it. Similarly, a proposition poses a problem, and a proof solves it. Static semantics relates a program to the type it implements, and a dynamic semantics relates a program to its simplification by an execution step. Similarly, a formal logical system relates a proof to the proposition it proves, and proof reduction relates equivalent proofs. The structural rule of substitution underlies the decomposition of a program into separate modules. Similarly, the structural rule of transitivity underlies the decomposition of a theorem into lemmas.

These correspondences are neither accidental nor incidental. The propositions-as-types principle, identifies propositions with types and proofs with programs. According to this principle, a proposition is the type of its proofs, and a proof is a program of that type. Consequently, every theorem has computational content, the its proof viewed as a program, and every program has mathematical content, the proof that the program represents.

Can every conceivable form of proposition also be construed as a type? Does every type correspond to a proposition? Must every proof have computational content? Is every program a proof of a theorem? To answer these questions would require a book of its own (and still not settle the matter). From a constructive perspective we may say that type theory en-

---

1The propositions-as-types principle is sometimes called the Curry-Howard Isomorphism. Although it is arguably snappier, this name ignores the essential contributions of Arend Heyting, Nicolaas deBruijn, and Per Martin-Löf to the development of the propositions-as-types principle.
riches logic to incorporate not only types of proofs, but also types for the
objects of study. In this sense logic is a particular mode of use of type the-
ory. If we think of type theory as a comprehensive view of mathematics,
this implies that, contrary to conventional wisdom, logic is based on math-
ematics, rather than mathematics on logic!

In this chapter we introduce the propositions-as-types correspondence
for a particularly simple system of logic, called propositional constructive logic.
In Chapter 31 we will extend the correspondence to propositional classical
logic. This will give rise to a computational interpretation of classical proofs
that makes essential use of continuations.

30.1 Constructive Semantics

Constructive logic is concerned with two judgements, $\phi$ prop, stating that
$\phi$ expresses a proposition, and $\phi$ true, stating that $\phi$ is a true proposi-
tion. What distinguishes constructive from non-constructive logic is that
a proposition is not conceived of as merely a truth value, but instead as a
problem statement whose solution, if it has one, is given by a proof. A propo-
sition is said to be true exactly when it has a proof, in keeping with ordinary
mathematical practice. There is no other criterion of truth than the existence of
a proof.

This principle has important, possibly surprising, consequences, the
most important of which is that we cannot say, in general, that a proposition
is either true or false. If for a proposition to be true means to have
a proof of it, what does it mean for a proposition to be false? It means
that we have a refutation of it, showing that it cannot be proved. That is, a
proposition is false if we can show that the assumption that it is true (has a
proof) contradicts known facts. In this sense constructive logic is a logic of
positive, or affirmative, information — we must have explicit evidence in the
form of a proof in order to affirm the truth or falsity of a proposition.

In light of this it should be clear that not every proposition is either
ture or false. For if $\phi$ expresses an unsolved problem, such as the famous
P $\neq$ NP problem, then we have neither a proof nor a refutation of it (the
mere absence of a proof not being a refutation). Such a problem is unde-
cided, precisely because it is unsolved. Since there will always be unsolved
problems (there being infinitely many propositions, but only finitely many
proofs at a given point in the evolution of our knowledge), we cannot say
that every proposition is decidable, that is, either true or false.

Having said that, some propositions are decidable, and hence may be
considered to be either true or false. For example, if $\phi$ expresses an inequality between natural numbers, then $\phi$ is decidable, because we can always work out, for given natural numbers $m$ and $n$, whether $m \leq n$ or $m \nleq n$ — we can either prove or refute the given inequality. This argument does not extend to the real numbers. To get an idea of why not, consider the presentation of a real number by its decimal expansion. At any finite time we will have explored only a finite initial segment of the expansion, which is not enough to determine if it is, say, less than 1. For if we have determined the expansion to be 0.99...9, we cannot decide at any time, short of infinity, whether or not the number is 1. (This argument is not a proof, because one may wonder whether there is some other representation of real numbers that admits such a decision to be made finitely, but it turns out that this is not the case.)

The constructive attitude is simply to accept the situation as inevitable, and make our peace with that. When faced with a problem we have no choice but to roll up our sleeves and try to prove it or refute it. There is no guarantee of success! Life’s hard, but we muddle through somehow.

### 30.2 Constructive Logic

The judgements $\phi$ prop and $\phi$ true of constructive logic are rarely of interest by themselves, but rather in the context of a hypothetical judgement of the form

$$\phi_1 \text{ true, } \ldots, \phi_n \text{ true} \vdash \phi \text{ true}.$$

This judgement expresses that the proposition $\phi$ is true (has a proof), under the assumptions that each of $\phi_1, \ldots, \phi_n$ are also true (have proofs). Of course, when $n = 0$ this is just the same as the categorical judgement $\phi$ true.

The structural properties of the hypothetical judgement, when specialized to constructive logic, define what we mean by reasoning under hypotheses:

$$\Gamma, \phi \text{ true} \vdash \phi \text{ true} \quad (30.1a)$$

$$\frac{\Gamma \vdash \phi_1 \text{ true}}{\Gamma, \phi_1 \text{ true} \vdash \phi_2 \text{ true}} \Gamma, \phi_1 \text{ true} \vdash \phi_2 \text{ true} \quad (30.1b)$$

$$\frac{\Gamma \vdash \phi_2 \text{ true}}{\Gamma, \phi_1 \text{ true} \vdash \phi_2 \text{ true}} \Gamma, \phi_1 \text{ true} \vdash \phi_2 \text{ true} \quad (30.1c)$$

$$\frac{\Gamma, \phi_1 \text{ true}, \phi_1 \text{ true} \vdash \phi_2 \text{ true}}{\Gamma, \phi_1 \text{ true} \vdash \phi_2 \text{ true}} \Gamma, \phi_1 \text{ true} \vdash \phi_2 \text{ true} \quad (30.1d)$$
\[ \Gamma, \phi_2 \text{ true}, \phi_1 \text{ true}, \Gamma_2 \vdash \phi \text{ true} \]
\[ \Gamma, \phi_1 \text{ true}, \phi_2 \text{ true}, \Gamma_2 \vdash \phi \text{ true} \] (30.1e)

The last two rules are implicit in that we regard \( \Gamma \) as a set of hypotheses, so that two “copies” are as good as one, and the order of hypotheses does not matter.

### 30.2.1 Rules of Provability

The syntax of propositional logic is given by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prop</td>
<td>( \phi )</td>
<td>true</td>
<td>( \top )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>false</td>
<td>( \bot )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and(( \phi_1; \phi_2 ))</td>
<td>( \phi_1 \lor \phi_2 )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>or(( \phi_1; \phi_2 ))</td>
<td>( \phi_1 \lor \phi_2 )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>imp(( \phi_1; \phi_2 ))</td>
<td>( \phi_1 \lor \phi_2 )</td>
</tr>
</tbody>
</table>

The connectives of propositional logic (truth, falsehood, conjunction, disjunction, and implication) are given meaning by rules that determine (a) what constitutes a “direct” proof of a proposition formed from a given connective, and (b) how to exploit the existence of such a proof in an “indirect” proof of another proposition. These are called the introduction and elimination rules for the connective. The principle of conservation of proof states that these rules are inverse to one another — the elimination rule cannot extract more information (in the form of a proof) than was put into it by the introduction rule, and the introduction rules can be used to reconstruct a proof from the information extracted from it by the elimination rules.

**Truth** Our first proposition is trivially true. No information goes into proving it, and so no information can be obtained from it.

\[ \Gamma \vdash \top \text{ true} \] (30.2a)

(\textit{no elimination rule})

\[ (30.2b) \]
Conjunction  Conjunction expresses the truth of both of its conjuncts.

\[
\Gamma \vdash \phi_1 \text{ true} \quad \Gamma \vdash \phi_2 \text{ true} \\
\hline
\Gamma \vdash \phi_1 \land \phi_2 \text{ true} 
\]

(30.3a)

\[
\Gamma \vdash \phi_1 \land \phi_2 \text{ true} \\
\hline
\Gamma \vdash \phi_1 \text{ true} 
\]

(30.3b)

\[
\Gamma \vdash \phi_1 \land \phi_2 \text{ true} \\
\hline
\Gamma \vdash \phi_2 \text{ true} 
\]

(30.3c)

Implication  Implication states the truth of a proposition under an assumption.

\[
\Gamma, \phi_1 \text{ true} \vdash \phi_2 \text{ true} \\
\hline
\Gamma \vdash \phi_1 \supset \phi_2 \text{ true} 
\]

(30.4a)

\[
\Gamma \vdash \phi_1 \supset \phi_2 \text{ true} \\
\hline
\Gamma \vdash \phi_1 \text{ true} \quad \Gamma \vdash \phi_2 \text{ true} \\
\hline
\Gamma \vdash \phi_2 \text{ true} 
\]

(30.4b)

Falsehood  Falsehood expresses the trivially false (refutable) proposition.

(no introduction rule)

(30.5a)

\[
\Gamma \vdash \bot \text{ true} \\
\hline
\Gamma \vdash \phi \text{ true} 
\]

(30.5b)

Disjunction  Disjunction expresses the truth of either (or both) of two propositions.

\[
\Gamma \vdash \phi_1 \text{ true} \\
\hline
\Gamma \vdash \phi_1 \lor \phi_2 \text{ true} 
\]

(30.6a)

\[
\Gamma \vdash \phi_2 \text{ true} \\
\hline
\Gamma \vdash \phi_1 \lor \phi_2 \text{ true} 
\]

(30.6b)

\[
\Gamma \vdash \phi_1 \lor \phi_2 \text{ true} \quad \Gamma, \phi_1 \text{ true} \vdash \phi \text{ true} \quad \Gamma, \phi_2 \text{ true} \vdash \phi \text{ true} \\
\hline
\Gamma \vdash \phi \text{ true} 
\]

(30.6c)
Negation The negation, ¬φ, of a proposition, φ, may be defined as the implication φ ⊃ ⊥. This means that ¬φ true if φ true ⊢ ⊥ true, which is to say that the truth of φ is refutable in that we may derive a proof of falsehood from any purported proof of φ. Because constructive truth is identified with the existence of a proof, the implied semantics of negation is rather strong. In particular, a problem, φ, is open exactly when we can neither affirm nor refute it. This is in contrast to the classical conception of truth, which assigns a fixed truth value to each proposition, so that every proposition is either true or false.

30.2.2 Rules of Proof

The key to the propositions-as-types principle is to make explicit the forms of proof. The categorical judgement φ true, which states that φ has a proof, is replaced by the judgement p : φ, stating that p is a proof of φ. (Sometimes p is called a “proof term”, but we will simply call p a “proof.”) The hypothetical judgement is modified correspondingly, with variables standing for the presumed, but unknown, proofs:

\[ x_1 : \phi_1, \ldots, x_n : \phi_n \vdash p : \phi. \]

We again let Γ range over such hypothesis lists, subject to the restriction that no variable occurs more than once.

The rules of constructive propositional logic may be restated using proof terms as follows.

\[
\begin{align*}
\Gamma \vdash \text{trueI}: \top & \quad (30.7a) \\
\Gamma \vdash p_1 : \phi_1 \quad \Gamma \vdash p_2 : \phi_2 & \quad (30.7b) \\
\Gamma \vdash \text{andI}(p_1; p_2) : \phi_1 \land \phi_2 & \quad (30.7c) \\
\Gamma \vdash p_1 : \phi_1 \land \phi_2 & \quad (30.7d) \\
\Gamma \vdash \text{andE}[l](p_1) : \phi_1 & \\
\Gamma \vdash \text{andE}[r](p_1) : \phi_2 & \\
\Gamma, x : \phi_1 \vdash p_2 : \phi_2 & \quad (30.7e) \\
\Gamma \vdash \text{impI}[\phi_1](x.p_2) : \phi_1 \supset \phi_2 & \\
\Gamma \vdash p : \phi_1 \supset \phi_2 \quad \Gamma \vdash p_1 : \phi_1 & \quad (30.7f) \\
\Gamma \vdash \text{impE}(p; p_1) : \phi_2 \\
\end{align*}
\]
30.3 Propositions as Types

Reviewing the rules of proof for constructive logic, we observe a striking correspondence between them and the rules for forming expressions of various types. For example, the introduction rule for conjunction specifies that a proof of a conjunction consists of a pair of proofs, one for each conjunct, and the elimination rule inverts this, allowing us to extract a proof of each conjunct from any proof of a conjunction. There is an obvious analogy with the static semantics of product types, whose introductory form is a pair and whose eliminatory forms are projections.

This correspondence extends to other forms of proposition as well, as summarized by the following chart relating a proposition, \( \phi \), to a type \( \phi^* \):

<table>
<thead>
<tr>
<th>Proposition</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \top )</td>
<td>unit</td>
</tr>
<tr>
<td>( \bot )</td>
<td>void</td>
</tr>
<tr>
<td>( \phi_1 \land \phi_2 )</td>
<td>( \phi_1 \times \phi_2^* )</td>
</tr>
<tr>
<td>( \phi_1 \lor \phi_2 )</td>
<td>( \phi_1^* \rightarrow \phi_2^* )</td>
</tr>
<tr>
<td>( \phi_1 \lor \phi_2 )</td>
<td>( \phi_1^* + \phi_2^* )</td>
</tr>
</tbody>
</table>

It is obvious that this correspondence is invertible, so that we may associate a proposition with each product, sum, or function type.

Importantly, this correspondence extends to the introductory and elim-
inatory forms of proofs and programs as well:

<table>
<thead>
<tr>
<th>Proof</th>
<th>Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>trueI</td>
<td>()</td>
</tr>
<tr>
<td>falseE<a href="p">\phi</a></td>
<td>abort(p*)</td>
</tr>
<tr>
<td>andI(p_1;p_2)</td>
<td>\langle p_1^<em>, p_2^</em> \rangle</td>
</tr>
<tr>
<td>andE<a href="p">\mathbf{l}</a></td>
<td>p^* \cdot l</td>
</tr>
<tr>
<td>andE<a href="p">\mathbf{r}</a></td>
<td>p^* \cdot r</td>
</tr>
<tr>
<td>impI[\phi_1](x_1 \cdot p_2)</td>
<td>\lambda (x_1 : \phi_1^* \cdot p_2^*)</td>
</tr>
<tr>
<td>impE(p; p_1)</td>
<td>p^* (p_1^*)</td>
</tr>
<tr>
<td>orI[\mathbf{l}]<a href="p">\phi_2</a></td>
<td>l \cdot p^*</td>
</tr>
<tr>
<td>orI[\mathbf{r}]<a href="p">\phi_1</a></td>
<td>r \cdot p^*</td>
</tr>
<tr>
<td>orE[\phi_1; \phi_2](p; x_1 \cdot p_1; x_2 \cdot p_2)</td>
<td>case p^* { l \cdot x_1 \Rightarrow p_1^*</td>
</tr>
</tbody>
</table>

Here again the correspondence is easily seen to be invertible, so that we may regard a program of a product, sum, or function type as a proof of the corresponding proposition.

**Theorem 30.1.**

1. If \( \phi \) prop, then \( \phi^* \) type.

2. If \( \Gamma \vdash p : \phi \), then \( \Gamma^* \vdash p^* : \phi^* \).

The foregoing correspondence between the statics of propositions and proofs on one hand, and types and programs on the other extends also to the dynamics, by applying the inversion principle stating that eliminatory forms are post-inverse to introductory forms. The dynamic correspondence may be expressed by the validity of these definitional equivalences under the static correspondences given above:

\[
\begin{align*}
\text{andE}[\mathbf{l}](\text{andI}(p; q)) & \equiv p \\
\text{andE}[\mathbf{r}](\text{andI}(p; q)) & \equiv q \\
\text{impE}(\text{impI}[\phi](x \cdot p_2); p_1) & \equiv [p_1/x]p_2 \\
\text{orE}[\phi_1; \phi_2](\text{orI}[\mathbf{l}][\phi_2](p); x_1 \cdot p_2; x_2 \cdot p_2) & \equiv [p/x_1]p_1 \\
\text{orE}[\phi_1; \phi_2](\text{orI}[\mathbf{r}][\phi_1](p); x_1 \cdot p_1; x_2 \cdot p_2) & \equiv [p/x_2]p_2 \\
\end{align*}
\]

Observe that these equations are all valid under the static correspondence given above. For example, the first of these equations corresponds to the definitional equivalence \( \langle e_1, e_2 \rangle \cdot 1 \equiv e_1 \), which is valid for the lazy interpretation of ordered pairs.
The significance of the dynamic correspondence is that it assigns *computational content* to proofs: a proof in constructive propositional logic may be read as a program. Put the other way around, it assigns *logical content* to programs: every expression of product, sum, or function type may be read as a proof of a proposition.

30.4 Exercises
Chapter 31

Classical Logic

In constructive logic a proposition is true exactly when it has a proof, a derivation of it from axioms and assumptions, and is false exactly when it has a refutation, a derivation of a contradiction from the assumption that it is true. Constructive logic is a logic of positive evidence. To affirm or deny a proposition requires a proof, either of the proposition itself, or of a contradiction, under the assumption that it has a proof. We are not always in a position to affirm or deny a proposition. An open problem is one for which we have neither a proof nor a refutation—so that, constructively speaking, it is neither true nor false!

In contrast classical logic (the one we learned in school) is a logic of perfect information in which every proposition is either true or false. One may say that classical logic corresponds to “god’s view” of the world—there are no open problems, rather all propositions are either true or false. Put another way, to assert that every proposition is either true or false is to weaken the notion of truth to encompass all that is not false, dually to the constructively (and classically) valid interpretation of falsity as all that is not true. The symmetry between truth and falsity is appealing, but there is a price to pay for this: the meanings of the logical connectives are weaker in the classical case than in the constructive.

A prime example is provided by the law of the excluded middle, the assertion that $\phi \lor \neg\phi$ true is valid for all propositions $\phi$. Constructively, this principle is not universally valid, because it would mean that every proposition either has a proof or a refutation, which is manifestly not the case. Classically, however, the law of the excluded middle is valid, because every proposition is either true or false. The discrepancy between the constructive and classical interpretations can be attributed to the different meanings
given to disjunction and negation by the two logics. In particular the classical truth of a disjunction cannot guarantee the constructive truth of one or the other disjunct. Something other than a constructive proof must be admitted as evidence for a disjunction if the law of the excluded middle is to hold true. And it is precisely for this reason that a classical proof expresses less than does a constructive proof of the same proposition.

Despite this weakness, classical logic admits a computational interpretation similar to, but somewhat less expressive than, that of constructive logic. The dynamics of classical proofs is derived from the complementarity of truth and falsity. A computation is initiated by juxtaposing a proof and a refutation—or, in programming terms, an expression and a continuation, or control stack. Continuations are essential to the meaning of classical proofs. In particular, the proof of the law of the excluded middle will be seen to equivocate between proving and refuting a proposition, using continuations to avoid getting caught in a contradiction.

31.1 Classical Logic

In constructive logic a connective is defined by giving its introduction and elimination rules. In classical logic a connective is defined by giving its truth and falsity conditions. Its truth rules correspond to introduction, and its falsity rules to elimination. The symmetry between truth and falsity is expressed by the principle of indirect proof. To show that $\phi$ true it is enough to show that $\phi$ false entails a contradiction, and, conversely, to show that $\phi$ false it is enough to show that $\phi$ true leads to a contradiction. While the second of these is constructively valid, the first is fundamentally classical, expressing the principle of indirect proof.

31.1.1 Provability and Refutability

There are three judgement forms in classical logic:

1. $\phi$ true, stating that the proposition $\phi$ is provable;
2. $\phi$ false, stating that the proposition $\phi$ is refutable;
3. $\#$, stating that a contradiction has been derived.

We will consider hypothetical judgements of the form

$$\phi_1 \text{ false}, \ldots, \phi_m \text{ false } \psi_1 \text{ true}, \ldots, \psi_n \text{ true} \vdash J,$$
where $J$ is any of the three basic judgement forms. The hypotheses are divided into two “zones” for convenience. We let $\Gamma$ stand for a finite set of “true” hypotheses, and $\Delta$ stand for a finite set of “false” hypotheses.

The rules of classical logic are organized around the symmetry between truth and falsity, which is mediated by the contradiction judgement.

The hypothetical judgement is reflexive:

$$\Delta, \phi \text{ false } \Gamma \vdash \phi \text{ false}$$  \hspace{1cm} (31.1a)

$$\Delta \Gamma, \phi \text{ true } \vdash \phi \text{ true}$$  \hspace{1cm} (31.1b)

The remaining rules are stated so that the structural properties of weakening, contraction, and transitivity are admissible.

A contradiction arises when a proposition is judged to be both true and false. A proposition is true if its falsity is absurd, and is false if its truth is absurd.

$$\Delta \Gamma \vdash \phi \text{ false} \quad \Delta \Gamma \vdash \phi \text{ true}$$  \hspace{1cm} (31.1c)

$$\Delta \Gamma \vdash \#$$  \hspace{1cm} (31.1d)

$$\Delta, \phi \text{ false } \Gamma \vdash \#$$

$$\Delta \Gamma \vdash \phi \text{ true}$$

$$\Delta \Gamma \vdash \phi \text{ true}$$  \hspace{1cm} (31.1e)

$$\Delta \Gamma \vdash \phi \text{ false}$$

Truth is trivially true, and cannot be refuted.

$$\Delta \Gamma \vdash \top \text{ true}$$  \hspace{1cm} (31.1f)

A conjunction is true if both conjuncts are true, and is false if either conjunct is false.

$$\Delta \Gamma \vdash \phi_1 \text{ true} \quad \Delta \Gamma \vdash \phi_2 \text{ true}$$

$$\Delta \Gamma \vdash \phi_1 \land \phi_2 \text{ true}$$  \hspace{1cm} (31.1g)

$$\Delta \Gamma \vdash \phi_1 \text{ false}$$

$$\Delta \Gamma \vdash \phi_1 \land \phi_2 \text{ false}$$  \hspace{1cm} (31.1h)

$$\Delta \Gamma \vdash \phi_2 \text{ false}$$

$$\Delta \Gamma \vdash \phi_1 \land \phi_2 \text{ false}$$  \hspace{1cm} (31.1i)

Falsity is trivially false, and cannot be proved.

$$\Delta \Gamma \vdash \bot \text{ false}$$  \hspace{1cm} (31.1j)
A disjunction is true if either disjunct is true, and is false if both disjuncts are false.

\[
\Delta \Gamma \vdash \phi_1 \text{ true} \\
\Delta \Gamma \vdash \phi_1 \lor \phi_2 \text{ true}
\]

\[
\Delta \Gamma \vdash \phi_2 \text{ true} \\
\Delta \Gamma \vdash \phi_1 \lor \phi_2 \text{ true}
\]

\[
\Delta \Gamma \vdash \phi_1 \text{ false} \quad \Delta \Gamma \vdash \phi_2 \text{ false} \\
\Delta \Gamma \vdash \phi_1 \lor \phi_2 \text{ false}
\]

Negation inverts the sense of each judgement:

\[
\Delta \Gamma \vdash \phi \text{ false} \\
\Delta \Gamma \vdash \neg \phi \text{ true}
\]

\[
\Delta \Gamma \vdash \phi \text{ true} \\
\Delta \Gamma \vdash \neg \phi \text{ false}
\]

An implication is true if its conclusion is true whenever the assumption is true, and is false if its conclusion is false yet its assumption is true.

\[
\Delta \Gamma, \phi_1 \text{ true} \vdash \phi_2 \text{ true} \\
\Delta \Gamma \vdash \phi_1 \supset \phi_2 \text{ true}
\]

\[
\Delta \Gamma \vdash \phi_1 \text{ true} \quad \Delta \Gamma \vdash \phi_2 \text{ false} \\
\Delta \Gamma \vdash \phi_1 \supset \phi_2 \text{ false}
\]

31.1.2 Proofs and Refutations

The dynamics of classical proofs is most easily explained by introducing a notation for the derivations of each of the judgement forms of classical logic:

1. \( p : \phi \), stating that \( p \) is a proof of \( \phi \);

2. \( k \vdash \phi \), stating that \( k \) is a refutation of \( \phi \);

3. \( k \# p \), stating that \( k \) and \( p \) are contradictory.
31.1 Classical Logic

We will consider hypothetical judgements of the form

\[ \frac{u_1 \div \phi_1, \ldots, u_m \div \phi_m \quad x_1 : \psi_1, \ldots, x_n : \psi_n}{\Delta \Gamma \vdash J,} \]

in which we have labelled the truth and falsity assumptions with variables.

A contradiction arises whenever a proposition is both true and false:

\[ \frac{\Delta, u \div \phi \Gamma \vdash k \# p \quad \Delta, u \div \phi \Gamma \vdash p : \phi}{\Delta, u \div \phi \Gamma \vdash k \# p} \quad (31.2a) \]

Truth and falsity are defined symmetrically in terms of contradiction:

\[ \frac{\Delta, u \div \phi \Gamma \vdash k \# p}{\Delta, u \div \phi \Gamma \vdash \text{ccr}(u \div \phi, k \# p) : \phi} \quad (31.2b) \]

\[ \frac{\Delta, x : \phi \Gamma \vdash k \# p}{\Delta, x : \phi \Gamma \vdash \text{ccp}(x : \phi, k \# p) : \phi} \quad (31.2c) \]

Reflexivity corresponds to the use of a variable hypothesis:

\[ \frac{\Delta, u \div \phi \Gamma \vdash u \div \phi}{\Delta, u \div \phi \Gamma \vdash u \div \phi} \quad (31.2d) \]

\[ \frac{\Delta, x : \phi \Gamma \vdash x : \phi}{\Delta, x : \phi \Gamma \vdash x : \phi} \quad (31.2e) \]

The other structure properties are admissible.

Truth is trivially true, and cannot be refuted.

\[ \frac{\Delta, u \div \phi \Gamma \vdash \langle \rangle : \top}{\Delta, u \div \phi \Gamma \vdash \langle \rangle : \top} \quad (31.2f) \]

A conjunction is true if both conjuncts are true, and is false if either conjunct is false.

\[ \frac{\Delta \Gamma \vdash p_1 : \phi_1 \quad \Delta \Gamma \vdash p_2 : \phi_2}{\Delta \Gamma \vdash \langle p_1, p_2 \rangle : \phi_1 \land \phi_2} \quad (31.2g) \]

\[ \frac{\Delta \Gamma \vdash k_1 \div \phi_1}{\Delta \Gamma \vdash \text{fst}; k_1 \div \phi_1 \land \phi_2} \quad (31.2h) \]

\[ \frac{\Delta \Gamma \vdash k_2 \div \phi_2}{\Delta \Gamma \vdash \text{snd}; k_2 \div \phi_1 \land \phi_2} \quad (31.2i) \]

Falsity is trivially false, and cannot be proved.

\[ \frac{\Delta \Gamma \vdash \text{abort} \div \bot}{\Delta \Gamma \vdash \text{abort} \div \bot} \quad (31.2j) \]
A disjunction is true if either disjunct is true, and is false if both disjuncts are false.

\[
\begin{align*}
\Delta \vdash p_1 : \phi_1 & \\
\Delta \vdash \text{inl}(p_1) : \phi_1 \lor \phi_2 & \quad (31.2k) \\
\Delta \vdash p_2 : \phi_2 & \\
\Delta \vdash \text{inr}(p_2) : \phi_1 \lor \phi_2 & \quad (31.2l) \\
\Delta \vdash k_1 \div \phi_1 & \Delta \vdash k_2 \div \phi_2 & \\
\Delta \vdash \text{case}(k_1; k_2) \div \phi_1 \lor \phi_2 & \quad (31.2m)
\end{align*}
\]

Negation inverts the sense of each judgement:

\[
\begin{align*}
\Delta \vdash k \div \phi & \\
\Delta \vdash \text{not}(k) \div \neg \phi & \quad (31.2n) \\
\Delta \vdash p \div \phi & \\
\Delta \vdash \text{not}(p) \div \neg \phi & \quad (31.2o)
\end{align*}
\]

An implication is true if its conclusion is true whenever the assumption is true, and is false if its conclusion false yet its assumption is true.

\[
\begin{align*}
\Delta, x : \phi_1, p_2 : \phi_2 & \\
\Delta \vdash \lambda (x : \phi_1, p_2) : \phi_1 \supset \phi_2 & \quad (31.2p) \\
\Delta \vdash p_1 : \phi_1 & \Delta \vdash k_2 \div \phi_2 & \\
\Delta \vdash \text{app}(p_1); k_2 \div \phi_1 \supset \phi_2 & \quad (31.2q)
\end{align*}
\]

### 31.2 Deriving Elimination Forms

The price of achieving a symmetry between truth and falsity in classical logic is that we must very often rely on the principle of indirect proof: to show that a proposition is true, we often must derive a contradiction from the assumption of its falsity. For example, a proof of

\[(\phi \land (\psi \land \theta)) \supset (\theta \land \phi)\]

in classical logic has the form

\[\lambda (w : \phi \land (\psi \land \theta). \text{ccr}(u \div \theta \land \phi. k \# w)),\]

where \(k\) is the refutation

\[\text{fst}; \text{ccp}(x : \phi. \text{snd}; \text{ccp}(y : \psi \land \theta. \text{snd}; \text{ccp}(z : \theta. u \# (z, x) \# y) \# w)).\]
And yet in constructive logic this proposition has a direct proof that avoids the circumlocations of proof by contradiction:

$$\lambda (w: \phi \land (\psi \land \theta). \text{andI}(\text{andE}[r](\text{andE}[r](w)); \text{andE}[1](w))).$$

But this proof cannot be expressed (as is) in classical logic, because classical logic lacks the elimination forms of constructive logic.

However, we may package the use of indirect proof into a slightly more palatable form by deriving the elimination rules of constructive logic. For example, the rule

$$\Delta \Gamma \vdash \phi \land \psi \text{ true}$$

is derivable in classical logic:

$$\frac{\Delta, \phi \text{ false} \Gamma \vdash \phi \text{ false} \quad \Delta, \phi \text{ false} \Gamma \vdash \phi \land \psi \text{ false} \quad \Delta, \phi \text{ false} \Gamma \vdash \phi \land \psi \text{ true}}{\Delta, \phi \text{ false} \Gamma \vdash \#}$$

$$\Delta \Gamma \vdash \phi \text{ true}$$

The other elimination forms are derivable in a similar manner, in each case relying on indirect proof to construct a proof of the truth of a proposition from a derivation of a contradiction from the assumption of its falsity.

The derivations of the elimination forms of constructive logic are most easily exhibited using proof and refutation expressions, as follows:

$$\text{falseE}[\phi](p) = \text{ccr}(u \div \phi . \text{abort} \# p)$$
$$\text{andE}[1](p) = \text{ccr}(u \div \phi . \text{fst}; u \# p)$$
$$\text{andE}[r](p) = \text{ccr}(u \div \psi . \text{snd}; u \# p)$$
$$\text{impE}(p_1; p_2) = \text{ccr}(u \div \psi . \text{app}(p_2); u \# p_1)$$
$$\text{orE}[\phi; \psi](p_1; x . p_2; y . p) = \text{ccr}(u \div \gamma . \text{case}(\text{ccp}(x: \phi . u \# p_2); \text{ccp}(y: \psi . u \# p)) \# p_1)$$

It is straightforward to check that the expected elimination rules hold. For example, the rule

$$\frac{\Delta \Gamma \vdash p_1: \phi \supset \psi \quad \Delta \Gamma \vdash p_2: \phi}{\Delta \Gamma \vdash \text{impE}(p_1; p_2): \psi}$$

is derivable using the definition of $\text{impE}(p_1; p_2)$ given above. By suppressing proof terms, we may derive the corresponding provability rule

$$\frac{\Delta \Gamma \vdash \phi \supset \psi \text{ true} \quad \Delta \Gamma \vdash \psi \text{ true}}{\Delta \Gamma \vdash \psi \text{ true}}.$$
31.3 Proof Dynamics

The dynamic semantics of classical logic arises from the simplification of the contradiction between a proof and a refutation of a proposition. To make this explicit we will define a transition system whose states are contradictions \( k \not\equiv p \) consisting of a proof, \( p \), and a refutation, \( k \), of the same proposition. The steps of the computation consist of simplifications of the contradictory state based on the form of \( p \) and \( k \).

The truth and falsity rules for the connectives play off one another in a pleasing manner:

\[
\begin{align*}
\text{fst}; k \not\equiv \langle p_1, p_2 \rangle & \mapsto k \not\equiv p_1 \\
\text{snd}; k \not\equiv \langle p_1, p_2 \rangle & \mapsto k \not\equiv p_2 \\
\text{case}(k_1; k_2) \not\equiv \text{inl}(p_1) & \mapsto k_1 \not\equiv p_1 \\
\text{case}(k_1; k_2) \not\equiv \text{inr}(p_2) & \mapsto k_2 \not\equiv p_2 \\
\text{not}(p) \not\equiv \text{not}(k) & \mapsto k \not\equiv p \\
\text{app}(p_1); k \not\equiv \lambda \langle x : \phi \rangle. p_2 & \mapsto k \not\equiv [p_1/x]p_2
\end{align*}
\]

The rules of indirect proof give rise to the following transitions:

\[
\begin{align*}
\text{ccp}(x : \phi. k_1 \not\equiv p_1) \not\equiv p_2 & \mapsto [p_2/x]k_1 \not\equiv [p_2/x]p_1 \\
k_1 \not\equiv \text{ccr}(u \div \phi. k_2 \not\equiv p_2) & \mapsto [k_1/u]k_2 \not\equiv [k_1/u]p_2
\end{align*}
\]

The first of these defines the behavior of the refutation of \( \phi \) that proceeds by contradicting the assumption that \( \phi \) is true. This refutation is activated by presenting it with a proof of \( \phi \), which is then substituted for the assumption in the new state. Thus, “ccp” stands for “call with current proof.” The second transition defines the behavior of the proof of \( \phi \) that proceeds by contradicting the assumption that \( \phi \) is false. This proof is activated by presenting it with a refutation of \( \phi \), which is then substituted for the assumption in the new state. Thus, “ccr” stands for “call with current refutation.”

A canonical proof is any proof other than an indirect proof, and a canonical refutation is any refutation other than an indirect refutation. We write \( p \) canonical to mean that \( p \) is a canonical proof, and \( k \) canonical to mean that \( k \) is a canonical refutation. To initiate computation we postulate that \( \text{halt} \) is a canonical refutation of any proposition. The initial and final states of computational are defined as follows:

\[
\text{halt} \not\equiv p \; \text{initial} \quad (31.6a)
\]
Theorem 31.1 (Preservation). If \( k \div \phi, \ p : \phi, \text{ and } k \# p \rightarrow k' \# p' \), then \( k' \div \phi \) and \( p' : \phi \).

Proof. By rule induction on the dynamics of classical logic.

Theorem 31.2 (Progress). If \( k \div \phi \) and \( p : \phi \), then either \( k \# p \text{ final} \), or \( k \# p \rightarrow k' \# p' \).

Proof. By rule induction on the statics of classical logic.

Rules (31.5g) to (31.5h) overlap in that there are two possible transitions for a state of the form

\[
\text{ccp}(x : \phi. k_1 \# p_1) \# \text{ccr}(u \div \phi. k_2 \# p_2),
\]

one to the state \( [p/x]k_1 \# [p/x]p_1 \), where \( p \) is \( \text{ccr}(u \div \phi. k_2 \# p_2) \), and one to the state \( [k/u]k_2 \# [k/u]p_2 \), where \( k \) is \( \text{ccp}(x : \phi. k_1 \# p_1) \).

This shows that the dynamics of classical logic is non-deterministic. But this means that it is difficult to predict the outcome of a computation, since it could be radically different in the case of the overlapping state just described. To avoid this one may impose a priority ordering among the two cases, preferring one transition over the other when there is a choice. Preferring the first corresponds to a “lazy” semantics for proofs, because we pass the unevaluated proof, \( p \), to the refutation on the left, which is thereby activated. Preferring the second corresponds to an “eager” semantics for proofs, in which we pass the unevaluated refutation, \( k \), to the proof, which is thereby activated.

31.4 Law of the Excluded Middle
The law of the excluded middle is derivable in classical logic:

\[
\begin{align*}
\phi \lor \neg \phi & \text{ false}, \phi \text{ true } \vdash \phi \text{ true} \\
\phi \lor \neg \phi & \text{ true}, \phi \text{ true } \vdash \phi \lor \neg \phi \text{ true} \\
\phi \lor \neg \phi & \text{ false}, \phi \text{ true } \vdash \phi \lor \neg \phi \text{ true} \\
\phi \lor \neg \phi & \text{ false}, \phi \text{ true } \vdash \phi \lor \neg \phi \text{ true} \\
\phi \lor \neg \phi & \text{ true}, \phi \text{ true } \vdash \phi \lor \neg \phi \text{ true} \\
\phi \lor \neg \phi & \text{ false}, \phi \text{ true } \vdash \phi \lor \neg \phi \text{ true} \\
\phi \lor \neg \phi & \text{ false}, \phi \text{ true } \vdash \phi \lor \neg \phi \text{ true}
\end{align*}
\]

When written out using explicit proofs and refutations, we obtain the proof term \( p_0 : \phi \lor \neg \phi \):

\[
ccr(u \div \phi \lor \neg \phi. u \# \text{inr}(\text{not}(\text{ccp}(x : \phi. u \# \text{inl}(x))))).
\]

To understand the computational meaning of this proof, let us juxtapose it with a refutation, \( k \div \phi \lor \neg \phi \), and simplify it using the dynamics given in Section 31.3 on page 280. The first step is the transition

\[
k \# ccr(u \div \phi \lor \neg \phi. u \# \text{inr}(\text{not}(\text{ccp}(x : \phi. u \# \text{inl}(x)))))) \quad \implies \quad k \# \text{inr}(\text{not}(\text{ccp}(x : \phi. k \# \text{inl}(x))))),
\]

wherein we have replicated \( k \) so that it occurs in two places in the result state. By virtue of its type the refutation \( k \) must have the form \( \text{case}(k_1; k_2) \), where \( k_1 \div \phi \) and \( k_2 \div \neg \phi \). Continuing the reduction, we obtain:

\[
\text{case}(k_1; k_2) \# \text{inr}(\text{not}(\text{ccp}(x : \phi. \text{case}(k_1; k_2) \# \text{inl}(x)))))) \quad \implies \quad k_2 \# \text{not}(\text{ccp}(x : \phi. \text{case}(k_1; k_2) \# \text{inl}(x))).
\]

By virtue of its type \( k_2 \) must have the form \( \text{not}(p_2) \), where \( p_2 : \phi \), and hence the transition proceeds as follows:

\[
\text{not}(p_2) \# \text{not}(\text{ccp}(x : \phi. \text{case}(k_1; k_2) \# \text{inl}(x)))) \quad \implies \quad \text{ccp}(x : \phi. \text{case}(k_1; k_2) \# \text{inl}(x)) \# p_2.
\]
Observe that $p_2$ is a valid proof of $\phi$! Proceeding, we obtain

\[
\text{ccp}(x : \phi.\text{case}(k_1;k_2) \# \text{inl}(x)) \# p_2
\]

\[
\mapsto
\text{case}(k_1;k_2) \# \text{inl}(p_2)
\]

\[
\mapsto
k_2 \# p_2
\]

The first of these two steps is the crux of the matter: the refutation, $k = \text{case}(k_1;k_2)$, which was replicated at the outset of the derivation, is reused, but with a different argument. At the first use, the refutation, $k$, which is provided by the context of use of the law of the excluded middle, is presented with a proof $\text{inr}(p_1)$ of $\phi \lor \neg \phi$. That is, the proof behaves as though the right disjunct of the law is true, which is to say that $\phi$ is false. If the context is such that it inspects this proof, it can only be by providing the proof, $p_2$, of $\phi$ that refutes the claim that $\phi$ is false. Should this occur, the proof of the law of the excluded middle backtracks the context, providing instead the proof $\text{inl}(p_2)$ to $k$, which then passes $p_2$ to $k_2$ without further incident. The proof of the law of the excluded middle baldly asserts $\neg \phi$ true, regardless of the form of $\phi$. Then, if caught in its lie by the context providing a proof of $\phi$, changes its mind and asserts to the original context, $k$, after all! No further reversion is possible, because the context has itself provided a proof, $p_2$, of $\phi$.

The law of the excluded middle illustrates that classical proofs are to be thought of as interactions between proofs and refutations, which is to say interactions between a proof and the context in which it is used. In programming terms this corresponds to an abstract machine with an explicit control stack, or continuation, representing the context of evaluation of an expression. That expression may access the context (stack, continuation) to effect backtracking as necessary to maintain the perfect symmetry between truth and falsity. The penalty is that a closed proof of a disjunction no longer need reveal which disjunct it proves, for as we have just seen, it may, on further inspection, change its mind!

### 31.5 Exercises
Part XI

Subtyping
Chapter 32

Subtyping

A subtype relation is a pre-order (reflexive and transitive relation) on types that validates the subsumption principle:

if \( \sigma \) is a subtype of \( \tau \), then a value of type \( \sigma \) may be provided whenever a value of type \( \tau \) is required.

The subsumption principle relaxes the strictures of a type system to permit values of one type to be treated as values of another.

Experience shows that the subsumption principle, while useful as a general guide, can be tricky to apply correctly in practice. The key to getting it right is the principle of introduction and elimination. To determine whether a candidate subtyping relationship is sensible, it suffices to consider whether every introductory form of the subtype can be safely manipulated by every eliminatory form of the supertype. A subtyping principle makes sense only if it passes this test; the proof of the type safety theorem for a given subtyping relation ensures that this is the case.

A good way to get a subtyping principle wrong is to think of a type merely as a set of values (generated by introductory forms), and to consider whether every value of the subtype can also be considered to be a value of the supertype. The intuition behind this approach is to think of subtyping as akin to the subset relation in ordinary mathematics. But this can lead to serious errors, because it fails to take account of the operations (eliminatory forms) that one can perform on values of the supertype. It is not enough to think only of the introductory forms; one must also think of the eliminatory forms. Subtyping is a matter of behavior, rather than containment.
32.1 Subsumption

A subtyping judgement has the form $\sigma <: \tau$, and states that $\sigma$ is a subtype of $\tau$. At a minimum we demand that the following structural rules of subtyping be admissible:

$$\tau <: \tau$$  \hspace{1cm} (32.1a)

$$\rho <: \sigma \quad \sigma <: \tau \quad \frac{}{\rho <: \tau}$$  \hspace{1cm} (32.1b)

In practice we either tacitly include these rules as primitive, or prove that they are admissible for a given set of subtyping rules.

The point of a subtyping relation is to enlarge the set of well-typed programs, which is achieved by the subsumption rule:

$$\Gamma \vdash e : \sigma \quad \sigma <: \tau \quad \frac{}{\Gamma \vdash e : \tau}$$  \hspace{1cm} (32.2)

In contrast to most other typing rules, the rule of subsumption is not syntax-directed, because it does not constrain the form of $e$. That is, the subsumption rule may be applied to any form of expression. In particular, to show that $e : \tau$, we have two choices: either apply the rule appropriate to the particular form of $e$, or apply the subsumption rule, checking that $e : \sigma$ and $\sigma <: \tau$.

32.2 Varieties of Subtyping

In this section we will informally explore several different forms of subtyping for various extensions of $L\{\rightarrow\}$. In Section 32.4 on page 296 we will examine some of these in more detail from the point of view of type safety.

32.2.1 Numeric Types

For languages with numeric types, our mathematical experience suggests subtyping relationships among them. For example, in a language with types int, rat, and real, representing, respectively, the integers, the rationals, and the reals, it is tempting to postulate the subtyping relationships

$$\text{int} <: \text{rat} <: \text{real}$$

by analogy with the set containments

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$
familiar from mathematical experience.

But are these subtyping relationships sensible? The answer depends on the representations and interpretations of these types! Even in mathematics, the containments just mentioned are usually not quite true—or are true only in a somewhat generalized sense. For example, the set of rational numbers may be considered to consist of ordered pairs \((m, n)\), with \(n \neq 0\) and \(\gcd(m, n) = 1\), representing the ratio \(m/n\). The set \(\mathbb{Z}\) of integers may be isomorphically embedded within \(\mathbb{Q}\) by identifying \(n \in \mathbb{Z}\) with the ratio \(n/1\). Similarly, the real numbers are often represented as convergent sequences of rationals, so that strictly speaking the rationals are not a subset of the reals, but rather may be embedded in them by choosing a canonical representative (a particular convergent sequence) of each rational.

For mathematical purposes it is entirely reasonable to overlook fine distinctions such as that between \(\mathbb{Z}\) and its embedding within \(\mathbb{Q}\). This is justified because the operations on rationals restrict to the embedding in the expected manner: if we add two integers thought of as rationals in the canonical way, then the result is the rational associated with their sum. And similarly for the other operations, provided that we take some care in defining them to ensure that it all works out properly. For the purposes of computing, however, one cannot be quite so cavalier, because we must also take account of algorithmic efficiency and the finiteness of machine representations. Often what are called “real numbers” in a programming language are, in fact, finite precision floating point numbers, a small subset of the rational numbers. Not every rational can be exactly represented as a floating point number, nor does floating point arithmetic restrict to rational arithmetic, even when its arguments are exactly represented as floating point numbers.

32.2.2 Product Types

Product types give rise to a form of subtyping based on the subsumption principle. The only elimination form applicable to a value of product type is a projection. Under mild assumptions about the dynamic semantics of projections, we may consider one product type to be a subtype of another by considering whether the projections applicable to the supertype may be validly applied to values of the subtype.

Consider a context in which a value of type \(\tau = \prod_{j \in J} \tau_j\) is required. The static semantics of finite products (Rules (16.3)) ensures that the only operation we may perform on a value of type \(\tau\), other than to bind it to a variable, is to take the \(j\)th projection from it for some \(j \in J\) to obtain a
value of type \( \tau_j \). Now suppose that \( e \) is of type \( \sigma \). If the projection \( e \cdot j \) is to be well-formed, then \( \sigma \) must be a finite product type \( \prod_{i \in I} \sigma_i \) such that \( j \in I \). Moreover, for this to be of type \( \tau_j \), it is enough to require that \( \sigma_j = \tau_j \). Since \( j \in J \) is arbitrary, we arrive at the following subtyping rule for finite product types:

\[
J \subseteq I \\
\prod_{i \in I} \tau_i <: \prod_{j \in J} \tau_j.
\] (32.3)

It is sufficient, but not necessary, to require that \( \sigma_j = \tau_j \) for each \( j \in J \); we will consider a more liberal form of this rule in Section 32.3 on page 292.

The argument for Rule (32.3) is based on a dynamic semantics in which we may evaluate \( e \cdot j \) regardless of the actual form of \( e \), provided only that it has a field indexed by \( j \in J \). Is this a reasonable assumption?

One common case is that \( I \) and \( J \) are initial segments of the natural numbers, say \( I = [0..m - 1] \) and \( J = [0..n - 1] \), so that the product types may be thought of as \( m \)- and \( n \)-tuples, respectively. The containment \( I \subseteq J \) amounts to requiring that \( m \geq n \), which is to say that a tuple type is regarded as a subtype of all of its prefixes. When specialized to this case, Rule (32.3) may be stated in the form

\[
m \geq n \\
\langle \tau_1, \ldots, \tau_m \rangle <: \langle \tau_1, \ldots, \tau_n \rangle.
\] (32.4)

One way to justify this rule is to consider elements of the subtype to be consecutive sequences of values of type \( \tau_0, \ldots, \tau_{n-1} \) from which we may calculate the \( j \)th projection for any \( 0 \leq j < n \leq m \), regardless of whether or not \( m \) is strictly bigger than \( n \).

Another common case is when \( I \) and \( J \) are finite sets of symbols, so that projections are based on the field name, rather than its position. When specialized to this case, Rule (32.3) takes the following form:

\[
m \geq n \\
\langle l_1 : \tau_{l_1}, \ldots, l_m : \tau_{l_m} \rangle <: \langle l_1 : \tau_{l_1}, \ldots, l_n : \tau_{l_n} \rangle.
\] (32.5)

Here we are taking advantage of the implicit identification of labeled tuple types up to reordering of fields, so that the rule states that any field of the supertype must be present in the subtype with the same type.

When using symbolic labels for the components of a tuple, it is perhaps slightly less clear that Rule (32.5) is well-justified. After all, how are we to find field \( l_i \), where \( 0 \leq i < n_i \), in a labeled tuple that may have additional fields anywhere within it? The trouble is that the label does not reveal the position of the field within the tuple, precisely because of subtyping. One
32.2 Varieties of Subtyping

A way to achieve this is to associate with a labeled tuple a dictionary mapping labels to positions within the tuple, which the projection operation uses to find the appropriate component of the record. Since the labels are fixed statically, this may be done in constant time using a perfect hashing function mapping labels to natural numbers, so that the cost of a projection remains constant. Another method is to use coercions that a value of the subtype to a value of the supertype whenever subsumption is used. In the case of labeled tuples this means creating a new labeled tuple containing only the fields of the supertype, copied from those of the subtype, so that the type specifies exactly the fields present in the value. This allows for more efficient implementation (for example, by a simple offset calculation), but is not compatible with languages that permit mutation (in-place modification) of fields because it destroys sharing.

32.2.3 Sum Types

By an argument dual to the one given for finite product types we may derive a related subtyping rule for finite sum types. If a value of type $\sum_{j \in J} \tau_j$ is required, the static semantics of sums (Rules (17.3)) ensures that the only non-trivial operation that we may perform on that value is a $J$-indexed case analysis. If we provide a value of type $\sum_{i \in I} \sigma_i$ instead, no difficulty will arise so long as $I \subseteq J$ and each $\sigma_i$ is equal to $\tau_i$. If the containment is strict, some cases cannot arise, but this does not disrupt safety. This leads to the following subtyping rule for finite sums:

$$I \subseteq J \quad \sum_{i \in I} \tau_i \prec : \sum_{j \in J} \tau_j.$$  \hspace{1cm} (32.6)

Note well the reversal of the containment as compared to Rule (32.3).

When $I$ and $J$ are initial segments of the natural numbers, we obtain the following special case of Rule (32.6):

$$m \leq n \quad [l_1 : \tau_1, \ldots, l_m : \tau_m] \prec : [l_1 : \tau_1, \ldots, l_n : \tau_n]$$  \hspace{1cm} (32.7)

One may also consider a form of width subtyping for unlabeled $n$-ary sums, by considering any prefix of an $n$-ary sum to be a subtype of that sum. Here again the elimination form for the supertype, namely an $n$-ary case analysis, is prepared to handle any value of the subtype, which is enough to ensure type safety.
32.3 Variance

In addition to basic subtyping principles such as those considered in Section 32.2 on page 288, it is also important to consider the effect of subtyping on type constructors. A type constructor is said to be covariant in an argument if subtyping in that argument is preserved by the constructor. It is said to be contravariant if subtyping in that argument is reversed by the constructor. It is said to be invariant in an argument if subtyping for the constructed type is not affected by subtyping in that argument.

32.3.1 Product Types

Finite product types are covariant in each field. For if \( e \) is of type \( \prod_{i \in I} \sigma_i \), and the projection \( e \cdot j \) is expected to be of type \( \tau_j \), then it is sufficient to require that \( j \in I \) and \( \sigma_j <: \tau_j \). This is summarized by the following rule:

\[
(\forall i \in I) \sigma_i <: \tau_i \\
\prod_{i \in I} \sigma_i <: \prod_{i \in I} \tau_i
\]  

(32.8)

It is implicit in this rule that the dynamic semantics of projection must not be sensitive to the precise type of any of the fields of a value of finite product type.

When specialized to \( n \)-tuples, Rule (32.8) reads as follows:

\[
\sigma_1 <: \tau_1, \ldots, \sigma_n <: \tau_n \\
\langle \sigma_1, \ldots, \sigma_n \rangle <: \langle \tau_1, \ldots, \tau_n \rangle
\]  

(32.9)

When specialized to symbolic labels, the covariance principle for finite products may be re-stated as follows:

\[
\sigma_1 <: \tau_1, \ldots, \sigma_n <: \tau_n \\
\langle l_1 : \sigma_1, \ldots, l_n : \sigma_n \rangle <: \langle l_1 : \tau_1, \ldots, l_n : \tau_n \rangle
\]  

(32.10)

32.3.2 Sum Types

Finite sum types are also covariant, because each branch of a case analysis on a value of the supertype expects a value of the corresponding summand, for which it is sufficient to provide a value of the corresponding subtype summand:

\[
(\forall i \in I) \sigma_i <: \tau_i \\
\sum_{i \in I} \sigma_i <: \sum_{i \in I} \tau_i
\]  

(32.11)
32.3 Variance

When specialized to symbolic labels as index sets, we obtain the following formulation of the covariance principle for sum types:

\[
\frac{\sigma_1 <: \tau_1 \quad \ldots \quad \sigma_n <: \tau_n}{[l_1 : \sigma_1, \ldots, l_n : \sigma_n] <: [l_1 : \tau_1, \ldots, l_n : \tau_n]}.
\] (32.12)

A case analysis on a value of the supertype is prepared, in the \(i\)th branch, to accept a value of type \(\tau_i\). By the premises of the rule, it is sufficient to provide a value of type \(\sigma_i\) instead.

32.3.3 Function Types

The variance of the function type constructor is a bit more subtle. Let us consider first the variance of the function type in its range. Suppose that \(e : \sigma \to \tau\). This means that if \(e_1 : \sigma\), then \(e(e_1) : \tau\). If \(\tau <: \tau'\), then \(e(e_1) : \tau'\) as well. This suggests the following covariance principle for function types:

\[
\frac{\tau <: \tau'}{\sigma \to \tau <: \sigma \to \tau'}
\] (32.13)

Every function that delivers a value of type \(\tau\) must also deliver a value of type \(\tau'\), provided that \(\tau <: \tau'\). Thus the function type constructor is covariant in its range.

Now let us consider the variance of the function type in its domain. Suppose again that \(e : \sigma \to \tau\). This means that \(e\) may be applied to any value of type \(\sigma\), and hence, by the subsumption principle, it may be applied to any value of any subtype, \(\sigma'\), of \(\sigma\). In either case it will deliver a value of type \(\tau\). Consequently, we may just as well think of \(e\) as having type \(\sigma' \to \tau\).

\[
\frac{\sigma' <: \sigma}{\sigma \to \tau <: \sigma' \to \tau}
\] (32.14)

The function type is contravariant in its domain position. Note well the reversal of the subtyping relation in the premise as compared to the conclusion of the rule!

Combining these rules we obtain the following general principle of contra- and co-variance for function types:

\[
\frac{\sigma' <: \sigma \quad \tau <: \tau'}{\sigma \to \tau <: \sigma' \to \tau'}
\] (32.15)

Beware of the reversal of the ordering in the domain!
32.3.4 Recursive Types

The variance principle for recursive types is rather subtle, and has been the source of errors in language design. To gain some intuition, consider the type of labeled binary trees with natural numbers at each node,

\[ \mu t. [\text{empty}: \text{unit}, \text{binode}: \langle \text{data}: \text{nat}, \text{lft}: t, \text{rht}: t \rangle] \]

and the type of “bare” binary trees, without labels on the nodes,

\[ \mu t. [\text{empty}: \text{unit}, \text{binode}: \langle \text{lft}: t, \text{rht}: t \rangle] \]

Is either a subtype of the other? Intuitively, one might expect the type of labeled binary trees to be a subtype of the type of bare binary trees, since any use of a bare binary tree can simply ignore the presence of the label.

Now consider the type of bare “two-three” trees with two sorts of nodes, those with two children, and those with three:

\[ \mu t. [\text{empty}: \text{unit}, \text{binode}: \langle \text{lft}: t, \text{rht}: t \rangle, \text{trinode}: \langle \text{lft}: t, \text{mid}: t, \text{rht}: t \rangle] \]

What subtype relationships should hold between this type and the preceding two tree types? Intuitively the type of bare two-three trees should be a supertype of the type of bare binary trees, since any use of a two-three tree must proceed by three-way case analysis, which covers both forms of binary tree.

To capture the pattern illustrated by these examples, we must formulate a subtyping rule for recursive types. It is tempting to consider the following rule:

\[
\frac{\text{rule} (32.16)}{\mu t. \sigma <: \mu t. \tau}
\]

That is, to determine whether one recursive type is a subtype of the other, we simply compare their bodies, with the bound variable treated as a parameter. Notice that by reflexivity of subtyping, we have \( t <: t \), and hence we may use this fact in the derivation of \( \sigma <: \tau \).

Rule (32.16) validates the intuitively plausible subtyping between labeled binary tree and bare binary trees just described. To derive this reduces to checking the subtyping relationship

\[ \langle \text{data}: \text{nat}, \text{lft}: t, \text{rht}: t \rangle <: \langle \text{lft}: t, \text{rht}: t \rangle, \]

generically in \( t \), which is evidently the case.
Unfortunately, Rule (32.16) also underwrites incorrect subtyping relationships, as well as some correct ones. As an example of what goes wrong, consider the recursive types
\[ \sigma = \mu \ell. (a : t \to \text{nat}, b : t \to \text{int}) \]
and
\[ \tau = \mu \ell. (a : t \to \text{int}, b : t \to \text{int}). \]
We assume for the sake of the example that \( \text{nat} < : \text{int} \), so that by using Rule (32.16) we may derive \( \sigma < : \tau \), which we will show to be incorrect. Let \( e : \sigma \) be the expression
\[
\text{fold}(\langle a = \lambda (x : \sigma) 4), b = \lambda (x : \sigma). q((\text{unfold}(x) \cdot a)(x))\rangle),
\]
where \( q : \text{nat} \to \text{nat} \) is the discrete square root function. Since \( \sigma < : \tau \), it follows that \( e : \tau \) as well, and hence
\[
\text{unfold}(e) : (a : \tau \to \text{int}, b : \tau \to \text{int}).
\]
Now let \( e' : \tau \) be the expression
\[
\text{fold}(\langle a = \lambda (x : \tau) -4), b = \lambda (x : \tau). 0\rangle).
\]
(The important point about \( e' \) is that the \( a \) method returns a negative number; the \( b \) method is of no significance.) To finish the proof, observe that
\[
(\text{unfold}(e) \cdot b)(e') \mapsto q(-4),
\]
which is a stuck state. We have derived a well-typed program that “gets stuck”, refuting type safety!

Rule (32.16) is therefore incorrect. But what has gone wrong? The error lies in the choice of a single parameter to stand for both recursive types, which does not correctly model self-reference. In effect we are regarding two distinct recursive types as equal while checking their bodies for a subtyping relationship. But this is clearly wrong! It fails to take account of the self-referential nature of recursive types. On the left side the bound variable stands for the subtype, whereas on the right the bound variable stands for the super-type. Confusing them leads to the unsoundness just illustrated.

As is often the case with self-reference, the solution is to assume what we are trying to prove, and check that this assumption can be maintained.
by examining the bodies of the recursive types. To do so we maintain a finite set, $\Psi$, of hypotheses of the form

$$s_1 <: t_1, \ldots, s_n <: t_n,$$

which is used to state the rule of subsumption for recursive types:

$$\frac{\Psi, s <: t \vdash \sigma <: \tau}{\Psi \vdash \mu s. \sigma <: \mu t. \tau} \quad (32.17)$$

That is, to check whether $\mu s. \sigma <: \mu t. \tau$, we assume that $s <: t$, since $s$ and $t$ stand for the respective recursive types, and check that $\sigma <: \tau$ under this assumption.

We tacitly include the rule of reflexivity for subtyping assumptions,

$$\frac{\Psi, s <: t \vdash s <: t}{\Psi} \quad (32.18)$$

Using reflexivity in conjunction with Rule (32.17), we may verify the subtypings among the tree types sketched above. Moreover, it is instructive to check that the unsound subtyping is not derivable using this rule. The reason is that the assumption of the subtyping relation is at odds with the contravariance of the function type in its domain.

### 32.4 Safety for Subtyping

Proving safety for a language with subtyping is considerably more delicate than for languages without. The rule of subsumption means that the static type of an expression reveals only partial information about the underlying value. This changes the proof of the preservation and progress theorems, and requires some care in stating and proving the auxiliary lemmas required for the proof.

As a representative case we will sketch the proof of safety for a language with subtyping for product types. The subtyping relation is defined by Rules (32.3) and (32.8). We assume that the static semantics includes subsumption, Rule (32.2).

**Lemma 32.1** (Structurality).

1. The tuple subtyping relation is reflexive and transitive.
2. The typing judgement $\Gamma \vdash e : \tau$ is closed under weakening and substitution.
32.4 Safety for Subtyping

Proof.

1. Reflexivity is proved by induction on the structure of types. Transitivity is proved by induction on the derivations of the judgements \( \rho <: \sigma \) and \( \sigma <: \tau \) to obtain a derivation of \( \rho <: \tau \).

2. By induction on Rules (16.3), augmented by Rule (32.2).

Lemma 32.2 (Inversion).

1. If \( e \cdot j : \tau \), then \( e : \prod_{i \in I} \tau_j, j \in I \), and \( \tau_j <: \tau \).

2. If \( \langle e_i \rangle_{i \in I} : \tau \), then \( \prod_{i \in I} \sigma_i <: \tau \) where \( e_i : \sigma_i \) for each \( i \in I \).

3. If \( \sigma <: \prod_{j \in J} \tau_j \), then \( \sigma = \prod_{i \in I} \sigma_i \) for some \( I \) and some types \( \sigma_i \) for \( i \in I \).

4. If \( \prod_{i \in I} \sigma_i <: \prod_{j \in J} \tau_j \), then \( I \subseteq J \) and \( \sigma_j <: \tau_j \) for each \( j \in J \).

Proof. By induction on the subtyping and typing rules, paying special attention to Rule (32.2).

Theorem 32.3 (Preservation). If \( e : \tau \) and \( e \mapsto e' \), then \( e' : \tau \).

Proof. By induction on Rules (16.4). For example, consider Rule (16.4d), so that \( e = \langle e_i \rangle_{i \in I} \cdot k \), \( e' = e_k \). By Lemma 32.2 we have that \( \langle e_i \rangle_{i \in I} : \prod_{j \in J} \tau_j \), \( k \in J \), and \( \tau_k <: \tau \). By another application of Lemma 32.2 for each \( i \in I \) there exists \( \sigma_i \) such that \( e_i : \sigma_i \) and \( \prod_{i \in I} \sigma_i <: \prod_{j \in J} \tau_j \). By Lemma 32.2 again, we have \( J \subseteq I \) and \( \sigma_j <: \tau_j \) for each \( j \in J \). But then \( e_k : \tau_k \), as desired. The remaining cases are similar.

Lemma 32.4 (Canonical Forms). If \( e \) val and \( e : \prod_{j \in J} \tau_j \), then \( e \) is of the form \( \langle e_i \rangle_{i \in I} \), where \( J \subseteq I \), and \( e_j : \tau_j \) for each \( j \in J \).

Proof. By induction on Rules (16.3) augmented by Rule (32.2).

Theorem 32.5 (Progress). If \( e : \tau \), then either \( e \) val or there exists \( e' \) such that \( e \mapsto e' \).
Proof. By induction on Rules (16.3) augmented by Rule (32.2). The rule of subsumption is handled by appeal to the inductive hypothesis on the premise of the rule. Rule (16.4d) follows from Lemma 32.4 on the preceding page.

To account for recursive subtyping in addition to finite product subtyping, the following inversion lemma is required.

Lemma 32.6.

1. If \( \Psi, s <: t \vdash \sigma' <: \tau' \) and \( \Psi, \sigma <: \tau \), then \( \Psi, [\sigma/s]\sigma' <: [\tau/t]\tau' \).

2. If \( \Psi \vdash \sigma <: \mu t . \tau' \), then \( \sigma = \mu s . \sigma' \) and \( \Psi, s <: t \vdash \sigma' <: \tau' \).

3. If \( \Psi \vdash \mu s . \sigma <: \mu t . \tau \), then \( \Psi \vdash [\mu s . \sigma/s] \sigma <: [\mu t . \tau/t] \tau \).

4. The subtyping relation is reflexive and transitive, and closed under weakening.

Proof.

1. By induction on the derivation of the first premise. Wherever the assumption is used, replace it by \( \sigma <: \tau \), and propagate forward.

2. By induction on the derivation of \( \sigma <: \mu t . \tau \).

3. Follows immediately from the preceding two properties of subtyping.

4. Reflexivity is proved by construction. Weakening is proved by an easy induction on subtyping derivations. Transitivity is proved by induction on the sizes of the types involved. For example, suppose we have \( \Psi \vdash \mu r . \rho <: \mu s . \sigma \) because \( \Psi, r <: s \vdash \rho <: \sigma \) and \( \Psi \vdash \mu s . \sigma <: \mu t . \tau \) because and \( \Psi, s <: t \vdash \sigma <: \tau \). We may assume without loss of generality that \( s \) does not occur free in either \( \rho \) or \( \tau \).

By weakening we have \( \Psi, r <: s, s <: t \vdash \rho <: \sigma \) and \( \Psi, r <: s, s <: t \vdash \sigma <: \tau \). Therefore by induction we have \( \Psi, r <: s, s <: t \vdash \rho <: \tau \). But since \( \Psi, r <: t \vdash r <: t \) and \( \Psi, r <: t \vdash t <: t \), we have by the first property above that \( \Psi, r <: t \vdash \rho <: \tau \), from which the result follows immediately.

The remainder of the proof of type safety in the presence of recursive subtyping proceeds along lines similar to that for product subtyping.
32.5 Exercises

32.5 Exercises
Chapter 33

Singleton and Dependent Kinds

The expression \( \text{let } e_1 : \tau \text{ be } x \text{ in } e_2 \) is a form of abbreviation mechanism by which we may bind \( e_1 \) to the variable \( x \) for use within \( e_2 \). In the presence of function types this expression is definable as the application \( \lambda (x: \tau. e_2) (e_1) \), which accomplishes the same thing. It is natural to consider an analogous form of \( \text{let} \) expression which permits a \textit{type expression} to be bound to a type variable within a specified scope. The expression \( \text{let } t \text{ be } \tau \text{ in } e \) binds \( t \) to \( \tau \) within \( e \), so that one may write expressions such as

\[
\text{let } t \text{ be } \text{nat} \times \text{nat} \text{ in } \lambda (x : t. s(x \cdot l)).
\]

For this expression to be type-correct the type variable \( t \) must be \textit{synonymous} with the type \( \text{nat} \times \text{nat} \), for otherwise the body of the \( \lambda \)-abstraction is not type correct.

Following the pattern of the expression-level \( \text{let} \), we might guess that \( \text{lettype} \) is an abbreviation for the polymorphic instantiation \( \Lambda (t. e) [\tau] \), which binds \( t \) to \( \tau \) within \( e \). This does, indeed, capture the dynamic semantics of type abbreviation, but it fails to validate the intended static semantics. The difficulty is that, according to this interpretation of \( \text{lettype} \), the expression \( e \) is type-checked in the absence of any knowledge of the binding of \( t \), rather than in the knowledge that \( t \) is synonymous with \( \tau \). Thus, in the above example, the expression \( s(x \cdot l) \) fails to type check, unless the binding of \( t \) were exposed.

The proposed definition of \( \text{lettype} \) in terms of type abstraction and type application fails. Lacking any other idea, one might argue that type abbreviation ought to be considered as a primitive concept, rather than a
derived notion. The expression \( \text{let } t \text{ be } \tau \text{ in } e \) would be taken as a primitive form of expression whose static semantics is given by the following rule:

\[
\Gamma \vdash [\tau/t]e : \tau' \\
\Gamma \vdash \text{let } t \text{ be } \tau \text{ in } e : \tau'
\]  

(33.1)

This would address the problem of supporting type abbreviations, but it does so in a rather \textit{ad hoc} manner. One might hope for a more principled solution that arises naturally from the type structure of the language.

Our methodology of identifying language constructs with type structure suggests that we ask not how to support type abbreviations, but rather what form of type structure gives rise to type abbreviations? And what else does this type structure suggest? By following this methodology we are led to the concept of \textit{singleton kinds}, which not only account for type abbreviations but also play a crucial role in the design of module systems.

### 33.1 Informal Overview

The central organizing principle of type theory is \textit{compositionality}. To ensure that a program may be decomposed into separable parts, we ensure that the composition of a program from constituent parts is mediated by the types of those parts. Put in other terms, the only thing that one portion of a program “knows” about another is its type. For example, the formation rule for addition of natural numbers depends only on the type of its arguments (both must have type \texttt{nat}), and not on their specific form or value. But in the case of a type abbreviation of the form \texttt{let t be \tau in e}, the principle of compositionality dictates that the only thing that \texttt{e} “knows” about the type variable \texttt{t} is its kind, namely \texttt{Type}, and not its binding, namely \texttt{\tau}. This is accurately captured by the proposed representation of type abbreviation as the combination of type abstraction and type application, but, as we have just seen, this is not the intended meaning of the construct!

We could, as suggested in the introduction, abandon the core principles of type theory, and introduce type abbreviations as a primitive notion. But there is no need to do so. Instead we can simply note that what is needed is for the kind of \texttt{t} to capture its identity. This may be achieved through the notion of a \textit{singleton kind}. Informally, the kind \texttt{Eqv(\tau)} is the kind of types that are definitionally equivalent to \texttt{\tau}. That is, up to definitional equality, this kind has only one inhabitant, namely \texttt{\tau}. Consequently, if \texttt{u :: Eqv(\tau)} is a variable of singleton kind, then within its scope, the variable \texttt{u} is synonymous with \texttt{\tau}. Thus we may represent \texttt{let t be \tau in e} by
Informal Overview

\( \Lambda (t : \text{Eqv}(\tau).e) [\tau] \), which correctly propagates the identity of \( t \), namely \( \tau \), to \( e \) during type checking.

A proper treatment of singleton kinds requires some additional machinery at the constructor and kind level. First, we must capture the idea that a constructor of singleton kind is \textit{a fortiori} a constructor of kind \text{Type}, and hence is a type. Otherwise, a variable, \( u \), singleton kind cannot be used as a type, even though it is explicitly defined to be one! This may be captured by introducing a \textit{subkinding} relation, \( \kappa_1 :<: \kappa_2 \), which is analogous to subtyping, exception at the kind level. The fundamental axiom of subkinding is \text{Eqv}(\tau) :<: \text{Type}, stating that every constructor of singleton kind is a type.

Second, we must account for the occurrence of a constructor of kind \text{Type} within the singleton kind \text{Eqv}(\tau). This intermixing of the constructor and kind level means that singletons are a form of \textit{dependent kind} in that a kind may depend on a constructor. Another way to say the same thing is that \text{Eqv}(\tau) represents a \textit{family of kinds} indexed by constructors of kind \text{Type}. This, in turn, implies that we must generalize the function and product kinds to \textit{dependent functions} and \textit{dependent products}. The dependent function kind, \( \Pi u : \kappa_1. \kappa_2 \) classifies functions that, when applied to a constructor \( c_1 :: \kappa_1 \), results in a constructor of kind \( [c_1/u]\kappa_2 \). The important point is that the kind of the result is sensitive to the argument, and not just to its kind.\(^1\) The dependent product kind, \( \Sigma u : \kappa_1. \kappa_2 \), classifies pairs \( \langle c_1, c_2 \rangle \) such that \( c_1 :: \kappa_1 \), as might be expected, and \( c_2 :: [c_1/u]\kappa_2 \), in which the kind of the second component is sensitive to the first component itself, and not just its kind.

Third, it is useful to consider singletons not just of kind \text{Type}, but also of higher kinds. To support this we introduce \textit{higher-kind singletons}, written \text{Eqv}(c :: \kappa), where \( \kappa \) is a kind and \( c \) is a constructor of kind \( k \). These are definable in terms of the primitive form of singleton kind by making use of dependent function and product kinds.

\[^1\]As we shall see in the development, the propagation of information as sketched here is managed through the use of singleton kinds.
Part XII

Symbols
Chapter 34

Symbols

A symbol is an atomic datum with no internal structure. The only way to compute with an unknown symbol is to compare it for identity with one or more known symbols, and branching according to the outcome. We shall make use of symbols for several purposes, including fluid binding, assignable variables, tags for classification of data, and names of communication channels. The common characteristic is that symbols are the indices of some family of operations, and that the types of the operations are conditioned by the type associated to the symbol. In this chapter we study symbols in isolation from their various applications.

34.1 Statics

We study a small language, called $\mathcal{L}\{\text{sym}\}$, for computing with symbols. The syntax of $\mathcal{L}\{\text{sym}\}$ is given by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>$\tau$</td>
<td>$\text{sym}(\tau)$</td>
<td>$\tau$ sym</td>
</tr>
<tr>
<td>Expr</td>
<td>$e$</td>
<td>$\text{newsym}<a href="a.e">\tau</a>$</td>
<td>$\text{newsym}\ a: \tau\ in\ e$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{sym}[a]$</td>
<td>$\text{sym}[a]$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{symcase}<a href="e;a.e;r_1,%5Cldots,r_n">t.\tau</a>$</td>
<td>$\text{symcase} e\ {{r_1 \mid \ldots \mid r_n}}\ ow\ a.e$</td>
</tr>
<tr>
<td>Rule</td>
<td>$r$</td>
<td>$\text{sym?}<a href="e">a</a>$</td>
<td>$\text{sym?}[a] \Rightarrow e$</td>
</tr>
</tbody>
</table>

In the match expression $\text{symcase}[t.\tau](e;a_0.e_0;r_1,\ldots,r_n)$ the symbol $a$ is bound within $e$, but the symbols $a_1,\ldots,a_n$ occurring within $r_1,\ldots,r_n$, respectively, are not bound.
The static semantics of $\mathcal{L}\{\text{sym}\}$ is given by a judgement of the form $\Gamma \vdash_{\Sigma} e : \tau$, where $\Sigma$ is a symbol context consisting of a finite set of declarations of the form

$$a_1 : \tau_1, \ldots, a_n : \tau_n$$

associating a type to each of a finite set of distinct symbols. This judgement is defined by the following rules:

$$(34.1a) \quad \Gamma \vdash_{\Sigma, \sigma} e : \tau \quad \tau \text{ mobile} \quad \Gamma \vdash_{\Sigma} \text{newsym}[\sigma](a,e) : \tau$$

$$(34.1b) \quad \Gamma \vdash_{\Sigma, \sigma} \text{sym}[a] : \text{sym}(\sigma)$$

$$(34.1c) \quad \Gamma \vdash_{\Sigma, \sigma} e : \tau \quad \Gamma \vdash_{\Sigma, \sigma} \text{sym?}[a](e) : \sigma > \tau$$

$$(34.1d) \quad \Gamma \vdash_{\Sigma} e : \text{sym}(\sigma) \quad \Gamma \vdash_{\Sigma, \sigma} e_0 : [\sigma/t]\tau \quad \Gamma \vdash_{\Sigma} \sigma_1 > [\sigma_1/t]\tau \quad \ldots \quad \Gamma \vdash_{\Sigma} \sigma_n > [\sigma_n/t]\tau \quad \Gamma \vdash_{\Sigma} \text{symcase}[t.\tau](e; a_0. e_0; r_1, \ldots, r_n) : [\sigma/t]\tau$$

Each of these rules merits careful analysis, as several quite subtle concepts are involved.

Rule (34.1a) gives the static semantics for the expression $\text{newsym}[\tau](a,e)$, which allocates a fresh symbol, $a$, of type $\tau$ for use within the expression, $e$. It is implicit that $a$ is chosen to not already be declared in $\Sigma$, ensuring that it is not otherwise in use. This assumption may always be met by suitably renaming the bound name, $a$, of the new expression prior to applying the rule. The requirement that the type $\tau$ be mobile constrains the type of the body of the declaration to ensure that its value does not depend on the locally declared symbol, $a$. This may be achieved either by limiting the class of mobile types so that the symbol does not escape its scope, or by treating all types as mobile and ensuring that the result is meaningful even if the symbol escapes (by implicitly widening its scope). These two options are considered in Sections 34.2 on the next page and 34.3 on page 310, respectively.

Rule (34.1b) is the introduction rule for the type $\text{sym}(\sigma)$. It states that if $a$ is a symbol with associated type $\sigma$, then $\text{sym}[a]$ is an expression of type $\text{sym}(\sigma)$. Rule (34.1c) to (34.1d) is the elimination rules for the type $\text{sym}(\sigma)$. The expression $\text{symcase}[t.\tau](e; a_0. e_0; r_1, \ldots, r_n)$ discriminates the value of $e$ according to the rules $r_1, \ldots, r_n$. If $e$ evaluates to $\text{sym}[a_i]$ for some $1 \leq$
\[ i \leq n, \text{ then the case expression evaluates to } e_i. \] Otherwise, if \( e \) evaluates to \( \text{sym}[a] \) such that \( a \) is not among the \( a_1, \ldots, a_n \), then the case expression evaluates to \( [a/a_0]e_0 \). (The non-matching symbol is passed to \( e_0 \) so that it can be used as the subject of further case analysis.)

The static semantics of this construct is given in terms of a specified type operator, \( t \cdot \tau \), which serves to propagate the type of a matched symbol to the corresponding branch of the case analysis. At the outset we know that the value, \( \text{sym}[a] \), of \( e \) is a symbol with associated type \( \sigma \), and that each symbol \( a_1, \ldots, a_n \) has associated type \( \sigma_1, \ldots, \sigma_n \), respectively. The type of the case analysis is \( [\sigma/t]\tau \), which propagates the type of the matched symbol into the result of the case analysis. The type of the \( i \)th branch is, however, \( [\sigma_i/t]\tau \). In the case that the symbol \( a \) is the symbol \( a_i \), we acquire the information that \( \sigma \) is \( \sigma_i \), and hence we satisfy the requirement that the overall type be \( [\sigma/t]\tau \). If, however, the symbol \( a \) does not match any branch, then the result of the case analysis is \( e_0 \), which has type \( [\sigma/t]\tau \), as required.

### 34.2 Scoped Dynamics

The \textit{scoped}, or \textit{stack-like}, dynamics of \( \mathcal{L}\{\text{sym}\} \) consists of a transition judgement of the form \( e \xrightarrow{\Sigma} e' \), where \( \Sigma \) specifies the symbols that may occur in \( e \) and \( e' \). The \texttt{new} construct introduces a \texttt{new}, or \texttt{fresh}, symbol for use within the body of the declaration. The new symbol is added to \( \Sigma \) during evaluation of the body of the \texttt{new}, and de-allocated afterwards. For this to make sense, though, we must ensure that the returned value of the declaration does not depend on the symbol that is about to be de-allocated.

This may be achieved by defining the judgement \( \tau \texttt{mobile} \) to hold only for types whose values cannot contain a symbol. For example, the type \( \texttt{nat} \) would be mobile, provided that it is given an eager interpretation. The type \( \texttt{unit} \) is clearly mobile, since its only value is the null tuple, and a product type \( \tau_1 \times \tau_2 \) would be mobile only if it is given an eager semantics and both \( \tau_1 \) and \( \tau_2 \) are mobile. On the other hand, symbol types are not mobile, nor would be function types, nor any other type whose constructors are evaluated lazily.

The scoped dynamics of \( \mathcal{L}\{\text{sym}\} \) consists of two judgement forms. The judgement \( e \texttt{val}_\Sigma \) states that \( e \) is a value relative to symbols \( \Sigma \), and the judgement \( e \xrightarrow{\Sigma} e' \) states that \( e \) transitions to \( e' \) in the presence of the symbols \( \Sigma \).

\[ \text{sym}[a] \texttt{val}_{\Sigma,a: \sigma} \]  
(34.2a)
\[ e \xrightarrow{a \sigma \epsilon} e' \]
\[ \text{newsym}[\sigma](a.e) \xrightarrow{\Sigma} \text{newsym}[\sigma](a.e') \] (34.2b)

\[ e \text{ val}_\Sigma \quad a \notin e \]
\[ \text{newsym}[\sigma](a.e) \xrightarrow{\Sigma} e \] (34.2c)

\[ e \xrightarrow{\Sigma} e' \]
\[ \text{symcase}[t.\tau](e; a_0.e_0; r_1, \ldots, r_n) \xrightarrow{\Sigma} \]
\[ \text{symcase}[t.\tau](e'; a_0.e_0; r_1, \ldots, r_n) \] (34.2d)

\[ \text{symcase}[t.\tau](\text{sym}[a]; a_0.e_0; e) \xrightarrow{\Sigma} [a/a_0]e_0 \]
\[ a = a_1 \]
\[ \text{symcase}[t.\tau](\text{sym}[a]; a_0.e_0; \text{sym?}[a_1](e_1), \ldots) \xrightarrow{\Sigma} e_1 \] (34.2e)

\[ a \neq a_1 \]
\[ \text{symcase}[t.\tau](\text{sym}[a]; a_0.e_0; \text{sym?}[a_1](e_1), \text{sym?}[a_2](e_2), \ldots) \xrightarrow{\Sigma} \]
\[ \text{symcase}[t.\tau](\text{sym}[a]; a_0.e_0; \text{sym?}[a_2](e_2), \ldots) \] (34.2f)

The second premise of Rule (34.2c) imposes the requirement that the returned value from the new is independent of the symbol \( a \). The definition of the judgment, \( \tau \) mobile, must be chosen so that the type guarantees that this condition is met.

### 34.3 Unscoped Dynamics

The unscoped, or heap-like, interpretation specifies that \( \text{newsym}[\sigma](a.e) \) generates a new symbol that may be used within \( e \), without imposing the requirement that the scope of \( a \) be limited to \( e \). This means that the symbol must continue to be available even after \( e \) returns a value. Consequently, all types may be regarded as mobile under a heap-like dynamics for symbol allocation.

To capture this we consider states of the form \( \nu \Sigma \{ e \} \), where \( \Sigma \) declares a finite set of symbols and their types, and \( e \) is an expression possibly involving the symbols declared in \( \Sigma \). The transition judgement \( \nu \Sigma \{ e \} \mapsto \ldots \)
\( \nu \Sigma' \{ e' \} \) states that evaluation of \( e \) relative to symbols \( \Sigma \) results in the expression \( e' \) in the extension \( \Sigma' \) of \( \Sigma \). New symbols come into existence during execution, but old symbols are never thrown away, nor are their associated types ever altered.

The unscoped dynamics of \( \mathcal{L}\{\text{sym}\} \) records the active set of symbols using a transition judgement of the form \( \nu \Sigma \{ e \} \rightarrow \nu \Sigma' \{ e' \} \) to ensure that symbols persist beyond their scope of declaration.

\[
\begin{align*}
\text{sym}[a] & \text{ val}_{\Sigma,a:\sigma} \\
\quad a \notin \text{ dom}(\Sigma) & \quad \nu \Sigma \{ \text{newsym}[\sigma](a.e) \} \rightarrow \nu \Sigma, a : \sigma \{ e \} \\
\quad v \Sigma \{ e \} & \rightarrow v \Sigma' \{ e' \} \\
\quad v \Sigma \{ \text{symcase}[t. \tau](e; a_0.e_0; r_1, \ldots, r_n) \} & \rightarrow v \Sigma' \{ \text{symcase}[t. \tau](e'; a_0.e_0; r_1, \ldots, r_n) \} \\
\quad v \Sigma \{ \text{symcase}[t. \tau](\text{sym}[a]; a_0.e_0; e) \} & \rightarrow v \Sigma \{ [a/a_0]e_0 \}
\end{align*}
\]

\[
\begin{align*}
\quad a = a_1 & \quad \nu \Sigma \{ \text{symcase}[t. \tau](\text{sym}[a]; a_0.e_0; \text{sym}[a_1](e_1), \ldots) \} \rightarrow \nu \Sigma \{ e_1 \} \\
\quad a \neq a_1 & \quad \nu \Sigma \{ \text{symcase}[t. \tau](\text{sym}[a]; a_0.e_0; \text{sym}[a_1](e_1), \text{sym}[a_2](e_2), \ldots) \} \\
\quad v \Sigma \{ \text{symcase}[t. \tau](\text{sym}[a]; a_0.e_0; \text{sym}[a_2](e_2), \ldots) \}
\end{align*}
\]

The chief difference compared to Rules (34.2) is in Rule (34.3b), which specifies that the set of active symbols is extended, and the body is executed in this extension without restriction.

### 34.4 Safety

We will focus on the safety of the unscoped dynamics. The proof for the scoped dynamics is similar, provided that we ensure that if \( \tau \) mobile, then \( a \notin e \) for every symbol \( a \), and every expression \( e : \tau \) such that \( e \text{ val} \).
Theorem 34.1 (Preservation). Suppose that $\nu \Sigma \{ e \} \mapsto \nu \Sigma' \{ e' \}$. Then $\Sigma' \supseteq \Sigma$ and $\vdash \Sigma' e' : \tau$.

Proof. By rule induction on Rules (34.3). The most interesting case arises when $e = \text{sym}[a]$ and $a = a_i$ for some rule $\text{sym}[a_i] (e_i)$. By inversion of typing we know that $\vdash \Sigma e_i : [\sigma_i/t] \tau$. We are to show that $\vdash \Sigma e_i : [\sigma_i/t] \tau$. Noting that if $a = a_i$, then by unicity of typing, $\sigma_i = \sigma$, the result follows immediately. \hfill $\square$

Lemma 34.2 (Canonical Forms). Suppose that $\vdash \Sigma e : \sigma \text{sym}$ and $e \text{val}_\Sigma$. Then $e = \text{sym}[a]$ for some $a$ such that $\Sigma = \Sigma', a : \sigma$.

Proof. By rule induction on Rules (34.1), taking account of the definition of values. \hfill $\square$

Theorem 34.3 (Progress). Suppose that $\vdash \Sigma e : \tau$. Then either $e \text{val}_\Sigma$, or $\nu \Sigma \{ e \} \mapsto \nu \Sigma' \{ e' \}$ for some $\Sigma'$ and $e'$.

Proof. By rule induction on Rules (34.1). For a case analysis of the form $\text{symcase} [t. \tau] (e; a_0.e_0.r_1, \ldots, r_n)$, where $e \text{val}_\Sigma$, we have by Lemma 34.2 that $e = \text{sym}[a]$ for some symbol $a$ of type $\sigma$. Then either $a = a_i$ for some rule $\text{sym}[a_i] (e_i)$, in which case we progress to $e_i$, or, if no rule matches, we progress to $[a/a_0]e_0$. \hfill $\square$

34.5 Exercises
Chapter 35

Fluid Binding

Recall from Chapter 13 that under the dynamic scope discipline evaluation is defined for expressions with free variables whose bindings are determined by capture-incurring substitution. Evaluation aborts if the binding of a variable is required in a context in which no binding for it exists. Otherwise, it uses whatever bindings for its free variables happen to be active at the point at which it is evaluated. In essence the bindings of variables are determined as late as possible during execution—just in time for evaluation to proceed. However, we found that as a language design dynamic scoping is deficient in (at least) two respects:

- Bound variables may not always be renamed in an expression without changing its meaning.
- Since the scopes of variables are resolved dynamically, it is difficult to ensure type safety.

These difficulties can be overcome by distinguishing two different concepts, namely static binding of variables, which is defined by substitution, and dynamic, or fluid, binding of symbols, which is defined by storing and retrieving bindings from a table during execution.

35.1 Statics
The language $L\{\text{fluid}\}$ extends the language $L\{\text{sym}\}$ defined in Chapter 34 with the following additional constructs:

\[
\begin{array}{|c|c|c|c|}
\hline
\text{Category} & \text{Item} & \text{Abstract} & \text{Concrete} \\
\hline
\text{Expr} & e & : = & \text{put}[a](e_1; e_2) \quad \text{put } e_1 \text{ for } a \text{ in } e_2 \\
 & & \text{ | } & \text{get}[a] \quad a \\
\hline
\end{array}
\]

As in Chapter 34, the variable $a$ ranges over some fixed set of symbols. The expression $e$ evaluates to the value of the current binding of $a$, if it has one, and is stuck otherwise. The expression $\text{put} e_1 \text{ for } a \text{ in } e_2$ binds the symbol $a$ to the value $e_1$ for the duration of the evaluation of $e_2$, at which point the binding of $a$ reverts to what it was prior to the execution. The symbol $a$ is not bound by the $\text{put}$ expression, but is instead a parameter of it.

The static semantics of $L\{\text{fluid}\}$ is defined by judgements of the form

\[
\Gamma \vdash_{\Sigma} e : \tau,
\]

where $\Sigma$ is a finite set $a_1 : \tau_1, \ldots, a_k : \tau_k$ of declarations of the pairwise distinct symbols $a_1, \ldots, a_k$, and $\Gamma$ is, as usual, a finite set $x_1 : \tau_1, \ldots, x_n : \tau_n$ of declarations of the pairwise distinct variables $x_1, \ldots, x_n$.

The static semantics of $L\{\text{fluid}\}$ extends that of $L\{\text{sym}\}$ (see Chapter 34) with the following rules:

\[
\begin{align*}
\Gamma \vdash_{\Sigma,a:\tau} \text{get}[a] : \tau & \quad & (35.1a) \\
\Gamma \vdash_{\Sigma,a:\tau_1} e_1 : \tau_1 & \quad \Gamma \vdash_{\Sigma,a:\tau_2} e_2 : \tau_2 & \rightarrow \\
\Gamma \vdash_{\Sigma,a:\tau_1} \text{put}[a](e_1; e_2) : \tau_2 & \quad & (35.1b)
\end{align*}
\]

Rule (35.1b) specifies that the symbol $a$ is a parameter of the expression that must be declared in $\Sigma$.

### 35.2 Dynamics

The dynamics of $L\{\text{fluid}\}$ is defined by maintaining an association of values to symbols that changes in a stack-like manner during execution. We define a family of transition judgements of the form $e : \Sigma \vdash_{\mu} e'$, where $\Sigma$ is as in the static semantics, and $\mu$ is a finite function mapping some subset of the symbols declared in $\Sigma$ to values of appropriate type. If $\mu$ is defined for some symbol $a$, then it has the form $\mu' \otimes (a : e)$ for some $\mu'$ and value $e$. If, on the other hand, $\mu$ is undefined for some symbol $a$, we may regard it as
having the form \( \mu' \otimes (a : \bullet) \). We will write \( (a : \_) \) to stand ambiguously for either \( (a : \bullet) \) or \( (a : e) \) for some expression \( e \).

The dynamic semantics of \( L\{\text{fluid}\} \) is given by the following rules:

\[
\begin{align*}
\frac{e \text{ val}_{\Sigma, \tau}}{\text{get}[a] \xrightarrow{\Sigma, \tau} e} \quad & \quad (35.2a) \\
\frac{e_1 \xrightarrow{\mu} e_1'}{\text{put}[a](e_1; e_2) \xrightarrow{\mu} \text{put}[a](e_1'; e_2)} \quad & \quad (35.2b) \\
\frac{e_1 \text{ val}_{\Sigma, \tau} e_2 \xrightarrow{\Sigma, \tau} e_2'}{\text{put}[a](e_1; e_2) \xrightarrow{\mu \otimes (a : e)} \text{put}[a](e_1'; e_2')} \quad & \quad (35.2c) \\
\frac{e_1 \text{ val}_{\Sigma, \tau} e_2 \text{ val}_{\Sigma, \tau}}{\text{put}[a](e_1; e_2) \xrightarrow{\mu} e_2} \quad & \quad (35.2d)
\end{align*}
\]

Rule (35.2a) specifies that \( \text{get}[a] \) evaluates to the current binding of \( a \), if any. Rule (35.2b) specifies that the binding for the symbol \( a \) is to be evaluated before the binding is created. Rule (35.2c) evaluates \( e_2 \) in an environment in which the symbol \( a \) is bound to the value \( e_1 \), regardless of whether or not \( a \) is already bound in the environment. Rule (35.2d) eliminates the fluid binding for \( a \) once evaluation of the extent of the binding has completed.

According to the dynamic semantics defined by Rules (35.2), there is no transition of the form \( \text{get}[a] \xrightarrow{\Sigma, \tau} e \) if \( \mu(a) = \bullet \). The judgement \( e \text{ unbound}_\mu \) states that execution of \( e \) leads to such a state. It is inductively defined by the following rules:

\[
\begin{align*}
\mu(a) = \bullet & \xrightarrow{} \text{get}[a] \text{ unbound}_\mu \quad & \quad (35.3a) \\
e_1 \text{ unbound}_\mu & \xrightarrow{} \text{put}[a](e_1; e_2) \text{ unbound}_\mu \quad & \quad (35.3b) \\
e_1 \text{ val}_{\Sigma} e_2 \text{ unbound}_\mu & \xrightarrow{} \text{put}[a](e_1; e_2) \text{ unbound}_\mu \quad & \quad (35.3c)
\end{align*}
\]
In addition to these rules we would also have, in a richer language, rules to propagate the unbound symbol error through other language constructs, as described in Chapter 11.

35.3 Type Safety

Define the auxiliary judgement $\mu : \Sigma$ by the following rules:

$$
\frac{}{\emptyset : \emptyset} ~ \quad ~ (35.4a)
$$

$$
\frac{\vdash \Sigma e : \tau \quad \mu : \Sigma}{\mu \otimes \langle a : e \rangle : \Sigma, a : \tau} \quad ~ (35.4b)
$$

$$
\frac{\mu : \Sigma}{\mu \otimes \langle a : \bullet \rangle : \Sigma, a : \tau} \quad ~ (35.4c)
$$

These rules specify that if a symbol is bound to a value, then that value must be of the type associated to the symbol in $\Sigma$. No demand is made in the case that the symbol is unbound (equivalently, bound to a "black hole").

Theorem 35.1 (Preservation). If $e \stackrel{\Sigma}{\rightarrow} e'$, where $\mu : \Sigma$ and $\vdash \Sigma e : \tau$, then $\vdash \Sigma e' : \tau$.

Proof. By rule induction on Rules (35.2). Rule (35.2a) is handled by the definition of $\mu : \Sigma$. Rule (35.2b) follows immediately by induction. Rule (35.2d) is handled by inversion of Rules (35.1). Finally, Rule (35.2c) is handled by inversion of Rules (35.1) and induction. \qed

Theorem 35.2 (Progress). If $\vdash \Sigma e : \tau$ and $\mu : \Sigma$, then either $e \text{ val}_\Sigma$, or $e$ unbound$\mu$, or there exists $e'$ such that $e \stackrel{\Sigma}{\rightarrow} e'$.

Proof. By induction on Rules (35.1). For Rule (35.1a), we have $\Sigma \vdash a : \tau$ from the premise of the rule, and hence, since $\mu : \Sigma$, we have either $\mu(a) = \bullet$ or $\mu(a) = e$ for some $e$ such that $\vdash \Sigma e : \tau$. In the former case we have $e$ unbound$\mu$, and in the latter we have get$[a] \stackrel{\Sigma}{\rightarrow} e$. For Rule (35.1b), we have by induction that either $e_1 \text{ val}_\Sigma$ or $e_1$ unbound$\mu$, or $e_1 \stackrel{\Sigma}{\rightarrow} e'_1$. In the
latter two cases we may apply Rule (35.2b) or Rule (35.3b), respectively. If $e_1 \text{ val}_\Sigma$, we apply induction to obtain that either $e_2 \text{ val}_\Sigma$, in which case Rule (35.2d) applies; $e_2 \text{ unbound}_\mu$, in which case Rule (35.3b) applies; or $e_2 \sum_{\mu} e'_2$, in which case Rule (35.2c) applies.

35.4 Subtleties of Fluid Binding

Fluid binding in the context of a first-order language is easy to understand. If the expression $\text{put } e_1 \text{ for } a \text{ in } e_2$ has a type such as $\text{nat}$, then its execution consists of the evaluation of $e_2$ to a number in the presence of a binding of $a$ to the value of expression $e_1$. When execution is completed, the binding of $a$ is dropped (reverted to its state in the surrounding context), and the value is returned. Since this value is a number, it cannot contain any reference to $a$, and so no issue of its binding arises.

But what if the type of $\text{put } e_1 \text{ for } a \text{ in } e_2$ is a function type, so that the returned value is a $\lambda$-abstraction? In that case the body of the $\lambda$ may contain references to the symbol $a$ whose binding is dropped upon return. This raises an important question about the interaction between fluid binding and higher-order functions. For example, consider the expression

$$\text{put } 17 \text{ for } a \text{ in } \lambda(x: \text{nat}. x + a), \quad (35.5)$$

which has type $\text{nat}$, given that $a$ is a symbol of the same type. Let us assume, for the sake of discussion, that $a$ is unbound at the point at which this expression is evaluated. Doing so binds $a$ to the number $17$, and returns the function $\lambda(x: \text{nat}. x + a)$. This function contains the symbol $a$, but is returned to a context in which the symbol $a$ is not bound. This means that, for example, application of the expression (35.5) to an argument will incur an error because the symbol $a$ is not bound.

Contrast this with the similar expression

$$\text{let } y \text{ be } 17 \text{ in } \lambda(x: \text{nat}. x + y), \quad (35.6)$$

in which we have replaced the fluid-bound symbol, $a$, by a statically bound variable, $y$. This expression evaluates to $\lambda(x: \text{nat}. x + 17)$, which adds 17 to its argument when applied. There is never any possibility of an unbound symbol arising at execution time, precisely because the identification of scope and extent ensures that the association between a variable and its binding is never violated.
It is hard to say whether either of these two behaviors is "right" or "wrong." Static binding is an important mechanism for encapsulation of behavior in a program; without static binding, one cannot ensure that the meaning of a variable is unchanged by the context in which it is used. Dynamic binding is used to avoid passing arguments to a function in order to specialize its behavior. Instead we rely on fluid binding to establish the binding of a symbol for the duration of execution of the function, avoiding the need to re-bind the fluids at each call site.

For example, let \( e \) stand for the value of expression (35.5), a \( \lambda \)-abstraction whose body is dependent on the binding of the symbol \( a \). This imposes the requirement that the programmer provide a binding for \( a \) whenever \( e \) is applied to an argument. For example, the expression

\[
\text{put } 7 \text{ for } a \text{ in } (e(9))
\]

evaluates to 15, and the expression

\[
\text{put } 8 \text{ for } a \text{ in } (e(9))
\]

evaluates to 17. Writing just \( e(9) \), without a surrounding binding for \( a \), results in a run-time error attempting to retrieve the binding of the unbound symbol \( a \).

The alternative to fluid binding is to add an additional parameter to \( e \) for the binding of the symbol \( a \), so that one would write

\[
e'(7)(9)
\]

and

\[
e'(8)(9),
\]

respectively, where \( e' \) is the \( \lambda \)-abstraction

\[
\lambda (a: \text{nat}. \lambda (x: \text{nat}. x + a)).
\]

Using additional arguments can be slightly inconvenient, though, when several call sites have the same binding for \( a \). Using fluid binding we may write

\[
\text{put } 7 \text{ for } a \text{ in } (e(8), e(9)),
\]

whereas using an additional argument we must write

\[
\langle e'(7)(8), e'(7)(9) \rangle.
\]
However, this sort of redundancy can be mitigated by simply factoring out the common part, writing

\[
\text{let } f \text{ be } e' (7) \text{ in } (f(\mathcal{S}), f(\mathcal{G})).
\]

One might argue, then, that it is all a matter of taste. However, a significant drawback of using fluid binding is that the requirement to provide a binding for \(a\) is not apparent in the type of \(e\), whereas the type of \(e'\) reflects the demand for an additional argument. One may argue that the type system should record the dependency of a computation on a specified set of fluid-bound symbols. For example, the expression \(e\) might be given a type of the form \(\text{nat} \rightarrow_a \text{nat}\), reflecting the demand that a binding for \(a\) be provided at the call site.

### 35.5 Fluid References

The foregoing treatment of fluid binding makes explicit the target of a get or put operation in the syntax of the language. It is sometimes useful to defer to execution time the choice of which fluid a get or a put acts on. This may be achieved by introducing references to fluids, which allow the name of a fluid to be represented as a value. References come equipped with analogues of the get and put primitives that act on references to fluids, rather than on fluids themselves.

References to fluid-bound symbols may be formalized by enriching \(L\{\text{fluid}\}\) as described in the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>(\tau)</td>
<td>(\text{fluid}(\tau))</td>
<td>(\tau\text{fluid})</td>
</tr>
<tr>
<td>Expr</td>
<td>(e)</td>
<td>(\text{fl}[a])</td>
<td>(\text{fl}[a])</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(\text{getfl}(e))</td>
<td>(\text{getfl})</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(\text{putfl}(e; e_1; e_2))</td>
<td>(\text{putfl})</td>
</tr>
</tbody>
</table>

The expression \(\text{fl}[a]\) is the symbol \(a\) thought of as a value of type \(\text{fluid}(\tau)\). The expressions \(\text{getfl}(e)\) and \(\text{putfl}(e; e_1; e_2)\) are analogues of the get and put operations for fluid-bound symbols.

The static semantics of these constructs is given by the following rules:

\[
\Gamma \vdash_{\Sigma; a: \tau} \text{fl}[a] : \text{fluid}(\tau) \tag{35.7a}
\]

\[
\Gamma \vdash_{\Sigma} e : \text{fluid}(\tau) \\quad \Gamma \vdash_{\Sigma} \text{getfl}(e) : \tau \tag{35.7b}
\]
\[ \Gamma \vdash \Sigma \ e : \text{fluid}(\tau) \quad \Gamma \vdash \Sigma \ e_1 : \tau \quad \Gamma \vdash \Sigma \ e_2 : \tau_2 \]

\[ \Gamma \vdash \Sigma \ \text{putfl}(e; e_1; e_2) : \tau_2 \quad (35.7c) \]

The dynamic semantics is given by these rules:

\[ \text{fl}[a] \text{ val}_{\Sigma, a : \tau} \]

\[ e \overset{\Sigma}{\mu} e' \quad (35.8a) \]

\[ \text{getfl}(e) \overset{\Sigma}{\mu} \text{getfl}(e') \]

\[ \text{getfl}(\text{fl}[e]) \overset{\Sigma}{\mu} \text{get}[a] \quad (35.8b) \]

\[ e \overset{\Sigma}{\mu} e' \]

\[ \text{putfl}(e; e_1; e_2) \overset{\Sigma}{\mu} \text{putfl}(e'; e_1; e_2) \quad (35.8c) \]

\[ \text{putfl}(\text{fl}[a]; e_1; e_2) \overset{\Sigma}{\mu} \text{put}[a](e_1; e_2) \quad (35.8d) \]

\[ \text{putfl}(\text{fl}[a]; e_1; e_2) \overset{\Sigma}{\mu} \text{put}[a](e_1; e_2) \quad (35.8e) \]

These operations determine the symbol to which the reference refers, and defers execution to the corresponding primitive acting on that symbol.

Fluid references are easily definable from symbols:

\[ \tau_{\text{fluid}} = \tau_{\text{sym}} \]

\[ \text{getfl} e = \text{symcase } e \{ \varepsilon \} \text{ ou } a . (a) \]

\[ \text{putfl } e \text{ is } e_1 \text{ in } e_2 = \text{symcase } e \{ \varepsilon \} \text{ ou } a . (\text{put } e_1 \text{ for } a \text{ in } e_2). \]

The symcase operation serves to introduce the symbol specified by \( e \) so that we may refer to the corresponding fluid binding primitives.

New dynamic fluids may be allocated by writing

\[ \text{newfl } x : \tau_{\text{fluid}} = e_1 \text{ in } e_2, \]

which stands for the expression

\[ \text{newsym } a : \tau \text{ in } (\text{put } e_1 \text{ for } a \text{ in } (\text{let } x \text{ be sym}[a] \text{ in } e_2)). \]

This expression allocates a new symbol, initializes its binding to \( e_1 \), and makes the new symbol available within \( e_2 \) by binding it to the variable \( x \) of type \( \tau_{\text{fluid}} \).
35.6 Exercises

1. Formalize deep binding and shallow binding using the stack machine of Chapter 27.
Chapter 36

Dynamic Classification

Sum types may be used to classify data values by labelling them with a class identifier that determines the type of the associated data item. For example, a sum type of the form $\sum \langle i_0 : \tau_0, \ldots, i_{n-1} : \tau_{n-1} \rangle$ consists of $n$ distinct classes of data, with the $i$th class labelling a value of type $\tau_i$. A value of this type is introduced by the expression $i \cdot e_i$, where $0 \leq i < n$ and $e_i : \tau_i$, and is eliminated by an $n$-ary case analysis binding the variable $x_i$ to the value of type $\tau_i$ labelled with class $i$.

Sum types are useful in situations where the type of a data item can only be determined at execution time, for example when processing input from an external data source. For example, a data stream from a sensor might consist of several different types of data according to the form of a stimulus. To ensure safe processing the items in the stream are labeled with a class that determines the type of the underlying datum. The items are processed by performing a case analysis on the class, and passing the underlying datum to a handler for items of that class.

A difficulty with using sums for this purpose, however, is that the developer must specify in advance the classes of data that are to be considered. That is, sums support static classification of data based on a fixed collection of classes. While this works well in the vast majority of cases, there are situations where static classification is inadequate, and dynamic classification is required. For example, we may wish to classify data in order to keep it secret from an intermediary in a computation. By creating a fresh class at execution time, two parties engaging in a communication can arrange that they, and only they, are able to compute with a given datum; all others must merely handle it passively without examining its structure or value.
One example of this sort of interaction arises when programming with
exceptions, as described in Chapter 28. One may consider the value asso-
ciated with an exception to be a secret that is shared between the program
component that raises the exception and the program component that han-
dles it. To ensure this, exception values are dynamically classified, with the
class being known to the raiser and to the handler, but to no others. No
intervening handler may intercept the exception value, because it cannot
decode the exception value without knowing its class.

Dynamic, as opposed to static, classification of exception values is re-
quired to support modularity. For if two different program components
happened to use the same, statically determined, class for an exception,
then a handler intended for one could inadvertently intercept an exception
raised by the other. To ensure that such collisions cannot occur while main-
taining modularity, dynamic classification is required. A class declared in
a module is generated when that module is initialized, ensuring that each
module generates its own classes, regardless of the names that happen to
be chosen by the programmer. This ensures that no conflicts—or accident-
al misinterpretations—can arise across independent components of a pro-
gram.

36.1 Statics

A classified value consists of a value of some type, τ, labelled by a symbol
of type τ. To compute with a classified value, we check whether its class is
among a specified finite set of known classes (of known types). If so, the
underlying value of that type is passed to an expression corresponding to
that class. If not, a default expression is evaluated.

The type of classified values, and its associated operations, are codified
by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>τ</td>
<td>:= clsfδ</td>
<td>clsfδ</td>
</tr>
<tr>
<td>Expr</td>
<td>e</td>
<td>:= in[a] (e)</td>
<td>in[a] (e)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>clscase(e; e₀; r₁, ..., rₙ)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>clscase e {r₁</td>
</tr>
<tr>
<td>Rule</td>
<td>r</td>
<td>:= in?[a] (x.e)</td>
<td>in?[a] (x) ⇒ e</td>
</tr>
</tbody>
</table>

The expression \( \text{in}[a](e) \) is a classified value with class \( a \) and underlying
value \( e \). The expression \( \text{clscase} e \{r₁ | ... | rₙ} \text{ow} e₀ \) branches on the class
of \( e \) according to rules \( r₁, ..., rₙ \). Each rule \( rᵢ \) has the form \( \text{in}?[aᵢ] (xᵢ) ⇒ eᵢ \),
36.2 Dynamics

consisting of a symbol, \( a_i \), representing a candidate class, a variable, \( x_i \), representing the associated data value for that class, and an expression, \( e_i \), to be evaluated for a classified value with class \( a_i \). If the class of the analyzed value does not match any of the rules, the default expression, \( e_0 \), is evaluated instead.

The static semantics of the type of classified values is given by the following rules:

\[
\Gamma \vdash \Sigma \quad a \colon \tau \\
\Gamma \vdash \Sigma \quad e \colon \tau \\
\Gamma \vdash \Sigma \quad r_1 : \sigma_1 \triangleright \tau \quad \ldots \\
\Gamma \vdash \Sigma \quad r_n : \sigma_n \triangleright \tau \\
\Gamma \vdash \Sigma \quad \text{clscase}(e; e_0; r_1, \ldots, r_n) : \tau 
\]

(36.1a)

\[
\Gamma \vdash \Sigma \quad e \colon \text{clsfd} \\
\Gamma, x : \sigma \vdash \Sigma \quad e : \tau \\
\Gamma \vdash \Sigma \quad \text{in}[a](x.e) : \sigma \triangleright \tau 
\]

(36.1b)

(36.1c)

36.2 Dynamics

Since a classified value is labelled with a symbol representing its class, it is essential that we employ an unscoped dynamics for symbols (as described in Chapter 34). This affords maximal flexibility in using classified values, since it places no restrictions on the scope of a class, each having global significance.

\[
\frac{e \ \text{val}_{\Sigma, a : \tau}}{\text{in}[a](e) \ \text{val}_{\Sigma, a : \tau}} 
\]

(36.2a)

\[
\nu \{ e \} \mapsto \nu \{ e' \} \\
\nu \{ \text{in}[a](e) \} \mapsto \nu \{ \text{in}[a](e') \} 
\]

(36.2b)

\[
\nu \{ \text{clscase}(e; e_0; r_1, \ldots, r_n) \} \mapsto \nu \{ \text{clscase}(e'; e_0; r_1, \ldots, r_n) \} 
\]

(36.2c)

\[
\frac{\text{in}[a](e) \ \text{val}_{\Sigma}}{\nu \{ \text{clscase}(\text{in}[a](e); e_0) \} \mapsto \nu \{ e_0 \}} 
\]

(36.2d)

\[
\frac{\text{in}[a](e) \ \text{val}_{\Sigma}}{\nu \{ \text{clscase}(\text{in}[a](e); e_0; \text{in}[a](x_1.e_1), \ldots) \} \mapsto \nu \{ [e/x_1]e_1 \}} 
\]

(36.2e)
36.3 Definability of Classification

Dynamic classification is definable from symbol, product, and existential types. The type \( \text{clsfd} \) stands for the existential type \( \exists (t.t \text{sym} \times t) \).

The classified value \( \text{in}[a](e) \) is defined to be the package

\[
\text{pack } \tau \text{ with } (\text{sym}[a],e) \text{ as } \exists (t.t \text{sym} \times t),
\]

where \( a \) is a symbol of type \( \tau \). Now suppose that the class case expression \( \text{clscase } e \{ r_1 | \ldots | r_n \} \) \( \omega e' \) has type \( \rho \), where \( r_i \) is the rule \( \text{in?} \{a_i\} (x_i) \Rightarrow e_i : \tau_i > \rho \). This expression is defined to be

\[
\text{open } \epsilon \text{ as } t \text{ with } (x,y) : t \text{sym} \times t \text{ in } (e_{\text{body}}(y)),
\]

where \( e_{\text{body}} \) is an expression to be defined shortly. Case analysis proceeds by opening the package, \( \epsilon \), representing the classified value, and decomposing it into a type, \( t \), a symbol, \( x \), of type \( t \text{sym} \), and an underlying value, \( y \), of type \( t \). The body of the open analyzes the class \( x \), yielding a function of
type $t \rightarrow \rho$, which is then applied to $y$ to pass the underlying value to the appropriate branch.

The core of the case analysis, namely the expression $e_{body}$, analyzes the encapsulated class, $x$, of the package. The case analysis is parameterized by the type abstractor $u.u \rightarrow \rho$, where $u$ is not free in $\rho$. The overall type of the case is $\lfloor t/u \rfloor u \rightarrow \rho = t \rightarrow \rho$, which ensures that the application to $y$ to the classified value is well-typed. Each branch of the case analysis has type $\tau_i \rightarrow \rho$. Putting it all together, the expression $e_{body}$ is defined to be the expression

$$\text{symcase } x \{ r'_1 | \ldots | r'_n \} \text{ ow } \lambda (\vdash t.e_0),$$

where for each $1 \leq i \leq n$, the rule $r'_i : \tau_i > (\tau_i \rightarrow \rho)$ is defined to be

$$\text{cls}[a_i] \Rightarrow \lambda (x_i : \tau_i.e_i).$$

One may check that the static and dynamic semantics of $\text{clsfd}$ are derivable according to these definitions.

### 36.4 Classifying Secrets

Dynamic classification may be used to enforce confidentiality and integrity of data values in a program. A value of type $\text{clsfd}$ may only be constructed by sealing it with some class, $a$, and may only be deconstructed by a case analysis that includes a branch for $a$. By controlling which parties in a multi-party interaction have access to the classifier, $a$, we may control how classified values are created (ensuring their integrity) and how they are inspected (ensuring their confidentiality). Any party that lacks access to $a$ cannot decipher a value classified by $a$, nor may it create a classified value with this class. Because classes are dynamically generated symbols, they provide an absolute privacy guarantee among parties in a computation.\(^1\)

To make this more precise, let us consider a simple protocol for controlling the integrity and privacy of data in a program. First, we allocate a fresh symbol, $a$, with which we will classify values of a specified type, $\tau$. Then we return two functions, of types $\tau \rightarrow \text{clsfd}$ and $\text{clsfd} \rightarrow \tau\text{opt}$, that, respectively, create a classified value of class $a$ and extract the underlying value classified with class $a$, if it is indeed classified by $a$.

\(^1\)Of course, this guarantee is for programs written in conformance with the static semantics given here. If the abstraction imposed by the type system is violated, no guarantees of privacy can be made.
newsym \( a : \tau \) in
\[
\{ \lambda (x:\tau.\text{in}[\!\! a \!\!] (x)),
\quad \lambda (x:\text{clsfd}.\text{clscase} \ x \ \{ \text{in?}[\!\! a \!\!] (y) \Rightarrow \text{just}(y) \ \text{ow null} \} ) \}.
\]

When executed, the symbol \( a \) is ensured (by \( \alpha \)-equivalence) to be fresh, and a pair consisting of a constructor and destructor function associated with class \( a \) are returned. Thereafter, the symbol \( a \) is out of scope, and therefore can never again be allocated by any subsequent \texttt{new} operation. Moreover, no value of type \( \tau \) can be classified with class \( a \), nor can any value classified with class \( a \) be deconstructed, other than by calling the constructor and destructor functions associated with the class \( a \).

To enforce the integrity of a value of type \( \tau \), only those parties who are entrusted with the constructor for \( a \) can create a value classified of class \( a \). Therefore, if a classified value of class \( a \) arises in a program, we can be sure that it could only have been introduced by a program component entrusted with the ability to create such a value. We may rely on the integrity of that value insofar as the trusted parties are honest in that they do not violate the integrity constraint which they have been entrusted to ensure.

Correspondingly, to enforce the privacy of a classified value of class \( a \), only those parties entrusted to recover the underlying data value of type \( \tau \) are to be given the deconstructor for \( a \). Since only those parties with access to the destructor for \( a \) can recover the underlying datum of a classified value of class \( a \), we can be sure that privacy of that datum is respected insofar as the entrusted parties are honest in that they do not disclose the value with which they have been entrusted.

What makes this protocol work is the combination of \( \alpha \)-equivalence to ensure the freshness of dynamically allocated classes, and the unscoped dynamics for symbol generation given in Chapter 34. This ensures that generated classes are unguessable secrets with global significance.

### 36.5 Exercises

1. Show how to use dynamic classification to implement a type of returned values for exceptions with the property that the raiser and handler agree on the class of value to be exchanged, and no other parties may raise or handle the agreed-upon exception value.
Part XIII

Storage Effects
Reynolds’s IA

Reynolds’s *Idealized Algol*, or IA, augments the expression types with a command type and higher-order function types to form an elegant block-structured programming language reminiscent of the classic language Algol. Like its progenitor, IA features a rich higher-order recursive function mechanism on top of a simple imperative language of commands. Commands are executed for their effect on the contents of the assignable variables, or just assignables, that are active within that command. Assignables are introduced by declaring them, and their contents are retrieved and altered by operations to get and set their contents, respectively. Commands may be sequenced one after the other, and there is a null command to end such a sequence. Repetition is achieved by a combination of sequencing and recursion.

The language IA imposes a modal distinction between pure expressions and impure commands. The meaning of a pure expression is independent of the assignables that may be in scope at that point. This ensures that there are no constraints on the order of evaluation of the components of a compound expression. The meaning of a command, however, depends on and affects the contents of the assignables, requiring a strictly specified evaluation order to ensure that the behavior of a command is predictable (that is, execution is deterministic).

The language IA is carefully designed to adhere to the stack discipline for allocating assignables. This means that an assignable may be deallocated on exit from the scope of its declaration, and hence that assignables may be allocated on a stack. This avoids the need for any form of automatic storage management beyond the conventional run-time stack.\(^1\) Surprisingly, this

---

\(^1\)A run-time stack is, of course, a simple form of automatic storage management, but it is
property is maintained even in the presence of a type of references (abstract pointers) to assignable variables.

### 37.1 Commands

The syntax of $\mathcal{L}\{\text{nat cmd} \rightarrow\}$ distinguishes pure expressions from impure commands. The expressions include those of $\mathcal{L}\{\text{nat} \rightarrow\}$ (as described in Chapter 15), augmented with one additional construct, and the commands are those of a simple imperative programming language based on assignment. The language maintains a sharp distinction between mathematical variables, or just variables, and assignable variables, or just assignables. Variables are introduced by $\lambda$-abstraction, and are given meaning by substitution. Assignables are introduced by a scoped declaration, and are given meaning by assignment and retrieval of their contents, which is, for the time being, restricted to natural numbers. Expressions evaluate to values, and have no effect on assignables. Commands are executed for their effect on assignables, and also return a value. Composition of commands not only sequences their execution order, but also passes the value returned by the first to the second before it is executed. The returned value of a command is, for the time being, restricted to the natural numbers. (But see Section 37.3 on page 338 for the general case.)

The syntax of $\mathcal{L}\{\text{nat cmd} \rightarrow\}$ is given by the following grammar, from which we have omitted repetition of the expression syntax of $\mathcal{L}\{\text{nat} \rightarrow\}$ for the sake of brevity.

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>$\tau$</td>
<td>$\text{cmd} \rightarrow\text{cmd}$</td>
<td>$\text{cmd}$</td>
</tr>
<tr>
<td>Expr</td>
<td>$e$</td>
<td>$\text{cmd}(m) \rightarrow\text{cmd} m$</td>
<td>$\text{ret}(e) \rightarrow\text{ret e}$</td>
</tr>
<tr>
<td>Cmd</td>
<td>$m$</td>
<td></td>
<td>$\text{seq}(e;x.m) \rightarrow\text{let cmd x be e in m}$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$\text{dcl}(e;a.m) \rightarrow\text{dcl a := e in m}$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$\text{get}[a] \rightarrow a$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$\text{set}<a href="e">a</a> \rightarrow a := e$</td>
</tr>
</tbody>
</table>

The expression $\text{cmd}(m)$ consists of the unevaluated command, $m$, thought of as a value of type $\text{cmd}$. The command, $\text{ret}(e)$, returns the value of the expression $e$ without having any effect on the assignables. The command

popular to draw a distinction between it and a more general form, called garbage collection. The difference lies largely in the eyes of the beholder.
seq(e; x. m) evaluates e to an encapsulated command, which is then executed and its returned value is substituted for x prior to executing m. The command dcl(e; a. m) introduces a new assignable, a, for use within the command, m, whose initial contents is given by the expression, e. The command get[a] returns the current contents of the assignable, a, and the command set[a](e) changes the contents of the assignable a to the value of e, and returns that value.

37.1.1 Statics

The static semantics of \( \mathcal{L}\{\text{nat cmd} \rightarrow \} \) consists of two forms of judgement:

1. Expression typing: \( \Gamma \vdash_\Sigma e : \tau \).
2. Command formation: \( \Gamma \vdash_\Sigma m \ ok \).

The context, \( \Gamma \), specifies the types of variables, as usual, and the state, \( \Sigma \), consists of a finite set of assignables. These judgements are inductively defined by the following rules:

\[
\frac{\Gamma \vdash_\Sigma m \ ok} {\Gamma \vdash_\Sigma \text{cmd}(m) : \text{cmd}} \tag{37.1a}
\]

\[
\frac {\Gamma \vdash_\Sigma e : \text{nat}} {\Gamma \vdash_\Sigma \text{ret}(e) \ ok} \tag{37.1b}
\]

\[
\frac {\Gamma \vdash_\Sigma e : \text{cmd} \quad \Gamma, x : \text{nat} \vdash_\Sigma m \ ok} {\Gamma \vdash_\Sigma \text{seq}(e; x. m) \ ok} \tag{37.1c}
\]

\[
\frac {\Gamma \vdash_\Sigma e : \text{nat} \quad \Gamma \vdash_{\Sigma, a} m \ ok} {\Gamma \vdash_{\Sigma, a} \text{dcl}(e; a. m) \ ok} \tag{37.1d}
\]

\[
\frac {\Gamma \vdash_{\Sigma, a} \text{get}[a] \ ok} {\Gamma \vdash_{\Sigma, a} e : \text{nat}} \tag{37.1e}
\]

\[
\frac {\Gamma \vdash_{\Sigma, a} \text{set}[\text{[a]}(e) \ ok} {\Gamma \vdash_{\Sigma, a} e : \text{nat}} \tag{37.1f}
\]

Rule (37.1a) is the introductory rule for the type cmd, and Rule (37.1c) is the corresponding eliminatory form. Rule (37.1d) introduces a new assignable for use within a specified command. The name, a, of the assignable is bound by the declaration, and hence may be renamed to satisfy the implicit constraint that it not already be present in \( \Sigma \). Rule (37.1e) states that
the command to retrieve the contents of an assignable, \( a \), returns a natural number. Rule (37.1f) that we may assign a natural number to an assignable, and that the returned value, which will be the assigned value, is of the same type.

### 37.1.2 Dynamics

The dynamic semantics of \( \mathcal{L}\{\text{nat cmd} \rightarrow \} \) is defined in terms of a memory, \( \mu \), a finite function assigning a numeral to each of a finite set of assignables.

The dynamics of expressions consists of these two judgement forms:

1. \( e \mbox{ val}_\Sigma \), stating that \( e \) is a value relative to \( \Sigma \).

2. \( e \overset{\Sigma}{\Rightarrow} e' \), stating that the expression \( e \) steps to the expression \( e' \).

These judgements are inductively defined by the following rules, together with the rules defining the dynamic semantics of \( \mathcal{L}\{\text{nat} \rightarrow \} \) (see Chapter 15). It is important, however, that the successor operation be given an eager, rather than lazy, semantics so that a closed value of type \( \text{nat} \) is a numeral (finite composition of successors starting with zero).

\[
\frac{}{\text{cmd}(m) \mbox{ val}_\Sigma} \quad (37.2a)
\]

Rule (37.2a) states that an encapsulated command is a value.

The dynamics of commands consists of these two judgement forms:

1. \( m \parallel \mu \mbox{ final}_\Sigma \) stating that the state \( m \parallel \mu \) is fully executed.

2. \( m \parallel \mu \overset{\Sigma}{\Rightarrow} m' \parallel \mu' \) stating that the state \( m \parallel \mu \) steps to the state \( m' \parallel \mu' \), relative to the set of assignables, \( \Sigma \).

These judgements are inductively defined by the following rules:

\[
\frac{e \mbox{ val}_\Sigma}{\text{ret}(e) \parallel \mu \mbox{ final}_\Sigma} \quad (37.3a)
\]

\[
\frac{e \overset{\Sigma}{\Rightarrow} e'}{\text{ret}(e) \overset{\Sigma}{\Rightarrow} \text{ret}(e')} \quad (37.3b)
\]

\[
\frac{e \overset{\Sigma}{\Rightarrow} e'}{\text{seq}(e; x.m) \parallel \mu \overset{\Sigma}{\Rightarrow} \text{seq}(e'; x.m) \parallel \mu} \quad (37.3c)
\]
37.1 Commands

\[
\begin{align*}
    m_1 & \parallel \mu \xrightarrow{\Sigma} m'_1 \parallel \mu' \\
    \text{seq}(\text{cmd}(m_1); x.m_2) & \parallel \mu \xrightarrow{\Sigma} \text{seq}(\text{cmd}(m'_1); x.m_2) \parallel \mu'
\end{align*}
\]

(37.3d)

\[
\begin{align*}
    e \xrightarrow{\Sigma} \text{val}_\Sigma \\
    \text{seq}(\text{cmd}(\text{ret}(e)); x.m) & \parallel \mu \xrightarrow{\Sigma} [e/x]m \parallel \mu
\end{align*}
\]

(37.3e)

\[
\begin{align*}
    \text{get}[a] & \parallel \mu \otimes \langle a : e \rangle \xrightarrow{\Sigma_{\mu_a}} \text{ret}(e) \parallel \mu \otimes \langle a : e \rangle \\
    e & \xrightarrow{\Sigma} e' \\
    \text{set}[a](e) & \parallel \mu \xrightarrow{\Sigma} \text{set}[a](e') \parallel \mu
\end{align*}
\]

(37.3f)

\[
\begin{align*}
    \text{set}[a](e) & \parallel \mu \otimes \langle a : x \rangle \xrightarrow{\Sigma_{\mu_a}} \text{ret}(e) \parallel \mu \otimes \langle a : x \rangle \\
    e & \xrightarrow{\Sigma} e' \\
    \text{dcl}(e; a.m) & \parallel \mu \xrightarrow{\Sigma} \text{dcl}(e'; a.m) \parallel \mu
\end{align*}
\]

(37.3g)

\[
\begin{align*}
    e & \xrightarrow{\Sigma} e' \\
    \text{dcl}(e; a.m) & \parallel \mu \xrightarrow{\Sigma} \text{dcl}(e'; a.m') \parallel \mu' \\
    e & \xrightarrow{\Sigma} e' \text{ val}_{\Sigma_a} \\
    \text{dcl}(e; a.\text{ret}(e')) & \parallel \mu \xrightarrow{\Sigma} \text{ret}(e') \parallel \mu
\end{align*}
\]

(37.3h)

Rule (37.3a) specifies that a \text{ret} command returns the value of its argument. Rules (37.3c) to (37.3e) specify the semantics of sequential composition. The expression, \( e \), must, by virtue of the type system, evaluate to an encapsulated command, which is to be executed to determine its return value, which is then substituted into \( m \) before executing it.

Rules (37.3i) to (37.3k) define the concept of block structure in a programming language. Declarations adhere to the stack discipline in that an assignable is allocated for the duration of evaluation of the body of the declaration, and deallocated after evaluation of the body is complete. Therefore the lifetime of an assignable can be identified with its scope, and hence we may visualize the dynamic lifetimes of assignables as being nested inside one another, in the same manner as their static scopes are nested inside one another. This stack-like behavior of assignables is a characteristic feature of what are known as Algol-like languages.
37.1.3 Safety

The auxiliary judgement \( \mu : \Sigma \) is defined by these two conditions:

1. \( \text{dom}(\mu) = \Sigma \);
2. for each \( a \in \Sigma \), there is an \( e \) such that \( \mu(a) = e \), \( e \text{ val}_\Sigma \) and \( \vdash \Sigma e : \text{nat} \).

This judgement states that the memory provides bindings for each of the assignables in \( \Sigma \), and that each binding is a closed value of type \( \text{nat} \) (since assignables can only contain natural numbers).

A state is well-formed, written \( m \parallel \mu \text{ ok}_\Sigma \), iff \( \mu : \Sigma \) and \( \vdash \Sigma m \text{ ok} \).

Theorem 37.1 (Preservation).

1. If \( e \overset{\Sigma}{\rightarrow} e' \) and \( \vdash \Sigma e : \tau \), then \( \vdash \Sigma e' : \tau \).
2. If \( m \parallel \mu \text{ ok}_\Sigma \) and \( m \parallel \mu \overset{\Sigma}{\rightarrow} m' \parallel \mu' \), then \( m' \parallel \mu' \text{ ok}_\Sigma \).

Proof. By induction on Rules (37.2) and (37.3). Consider Rule (37.3j). Assume that \( \text{dcl}(e; a. m) \parallel \mu \text{ ok}_\Sigma \). By inversion of typing we have \( \vdash \Sigma e : \text{nat} \), \( \vdash \Sigma a \text{ ok}_\Sigma \), and \( \mu : \Sigma \). Since \( e \text{ val}_\Sigma \), it follows that \( \mu \otimes \langle a : e \rangle : \Sigma, a \), and hence \( m \parallel \mu \otimes \langle a : e \rangle \text{ ok}_{\Sigma, a} \). By induction we have \( m' \parallel \mu' \otimes \langle a : e' \rangle \text{ ok}_{\Sigma, a} \), from which it follows that \( \text{dcl}(e'; a. m') \parallel \mu' \text{ ok}_\Sigma \), as required.

Consider Rule (37.3j). Assume that \( \text{dcl}(e; a. \text{ret}(e')) \parallel \mu \text{ ok}_\Sigma \). We are to show that \( \text{ret}(e) \parallel \mu \text{ ok}_\Sigma \). By inversion we know that \( \vdash \Sigma e : \text{nat} \), \( \vdash \Sigma a \text{ ret}(a) \text{ ok}_\Sigma \), and hence that \( \vdash \Sigma a e' : \text{nat} \). It suffices to show that \( \vdash \Sigma e' : \text{nat} \). But since \( e' \text{ val}_\Sigma \), the eager semantics of the successor operation ensures that \( e' \) must be a numeral, and hence \( \vdash \Sigma e' : \text{nat} \), as required.

Theorem 37.2 (Progress).

1. If \( \vdash \Sigma e : \tau \), then either \( e \text{ val}_\Sigma \), or there exists \( e' \) such that \( e \overset{\Sigma}{\rightarrow} e' \).
2. If \( m \parallel \mu \text{ ok}_\Sigma \), then either \( m \text{ final}_\Sigma \), or \( m \parallel \mu \overset{\Sigma}{\rightarrow} m' \parallel \mu' \) for some \( \mu' \) and \( m' \).

Proof. By induction on Rules (37.1). Consider Rule (37.1d). By the first inductive hypothesis we have either \( e \overset{\Sigma}{\rightarrow} e' \) or \( e \text{ val}_\Sigma \). In the former case Rule (37.3i) applies. In the latter, we have by the second inductive hypothesis either \( m \text{ final}_\Sigma \), or \( m \parallel \mu \otimes \langle a : e \rangle \overset{\Sigma, a}{\rightarrow} m' \parallel \mu' \otimes \langle a : e' \rangle \). In the former case we apply Rule (37.3j), and in the latter, Rule (37.3k).
37.2 Some Programming Idioms

The language $L\{\text{nat cmd} \rightarrow\}$ is designed to expose the elegant interplay between the execution of an expression for its value and the execution of a command for its effect on assignables. In this section we show how to derive several standard idioms of imperative programming in $L\{\text{nat cmd} \rightarrow\}$.

We begin by defining the binary sequential composition of commands, written $\{x \leftarrow m_1 ; m_2\}$, to be the command

$$\text{let cmd } x \text{ be cmd}(m_1) \text{ in } m_2.$$  

This generalizes to the $n$-ary sequential composition by defining

$$\{x_1 \leftarrow m_1 ; \ldots ; x_{n-1} \leftarrow m_{n-1} ; m_n\},$$

to stand for the iterated form

$$\{x_1 \leftarrow m_1 ; \ldots ; \{x_{n-1} \leftarrow m_{n-1} ; \{x_n \leftarrow m_n ; \text{ret } x_n\}\}\}.$$  

A related idiom, run $e$, executes an encapsulated command and returns its result, is defined to be the command \text{let cmd } x \text{ be } e \text{ in ret } x.$$

The conditional command, ifz $(m) m_1 \text{ else } m_2$, executes either $m_1$ or $m_2$ according to whether the result of executing $m$ is zero or not:

$$\text{seq(cmd(m)}; x. \text{seq(ifz(x; cmd(m_1); cmd(m_2)); y. ret(y))).}$$

The returned value of the conditional is the value returned by the selected command.

The while loop command, whilenz $(m_1) m_2$, repeatedly executes the command $m_2$ while the command $m_1$ yields a non-zero number. It is defined as follows:

$$\text{run fix loop: cmd is cmd(ifz(m_1) \text{ ret(z)} \text{ else } \{\_ \leftarrow m_2 ; \text{run loop}\}).}$$

This commands runs the self-referential encapsulated command that, when executed, first executes $m_1$, branching on the result. If the result is zero, the loop returns zero (arbitrarily). If the result is non-zero, the command $m_2$ is executed and the loop is repeated.

A procedure is a function of type $\tau \rightarrow \text{cmd}$ that takes an argument of some type, $\tau$, and yields an unexecuted command as result. A procedure call is the composition of a function application with the activation of the resulting command. If $e_1$ is a procedure and $e_2$ is its argument, then the procedure
37.3 Typed Commands and Assignables

338

37.3 Typed Commands and Assignables

So far we have restricted the type of the returned value of a command, and the contents of an assignable, to be \texttt{nat}. Can this restriction be relaxed, while adhering to the stack discipline?

The key to admitting other types of returned value and assignable variables is to consider the proof of Theorem 37.1 on page 336. There we relied on the fact that a value of type \texttt{nat} is a composition of successors, starting from zero, to ensure that the value is well-typed even in the absence of the locally declared assignable, \texttt{a}. The proof breaks down, and indeed the preservation theorem is false, when the return type of a command or the contents type of an assignable is unrestricted.

For example, if we may return values of procedure type, then we may violate safety as follows:

\begin{verbatim}
dcl \texttt{a} := \texttt{z} \in \texttt{ret} (\lambda (\texttt{x:nat}) \texttt{cmd} \texttt{a} := \texttt{x}).
\end{verbatim}
This command, when executed, allocates a new assignable, \( a \), and returns a procedure that, when called, assigns its argument to \( a \). But this makes no sense, because the assignable, \( a \), is deallocated when the body of the declaration returns, but the returned value still refers to it! If the returned procedure is called, execution will get stuck in the attempt to assign to \( a \).

A similar example shows that admitting assignables of arbitrary type is also unsound:

\[
dcl a := z \text{ in } b := \lambda (x : \text{nat}. \text{cmd} a := x).
\]

Here we assume that \( b \) is an assignable of procedure type. We assign to it a procedure that assigns to a locally declared assignable, \( a \), and then leaves the scope of the declaration. If we then call the procedure stored in \( b \), execution will get stuck attempting to assign to the non-existent assignable, \( a \), or, even worse, assign to a different assignable that happens to be named \( a \)!

The critical step in the proof of safety given in Section 37.1.3 on page 336 is to ensure the following safety condition:

\[
\text{if } \vdash_{\Sigma,a} e : \tau \text{ and } e \text{ val}_{\Sigma,a}, \text{ then } \vdash_{\Sigma} e : \tau. \tag{37.4}
\]

When \( \tau = \text{nat} \), this step is ensured, because \( e \) must be a numeral. If, on the other hand, \( \tau \) is a procedure type, then \( e \) may contain uses of the locally declared assignable, \( a \), and, indeed, the above counterexamples violate this safety condition.

We say that a type, \( \tau \), is mobile, written \( \tau \) mobile, if the safety condition (37.4) is valid for all values of that type. The proof of safety given above shows that \( \text{nat} \) is mobile. Obviously, reference types are not mobile, since they involve an assignable. The counterexamples show that procedure types are not mobile. Moreover, simple variations of these examples may be given to show that command types may not be considered mobile either. What about function types other than procedure types? One may think they are mobile, because a pure expression cannot depend on an assignable. While this is indeed the case, the safety condition (37.4) need not be satisfied for such a type. For example, consider the following value of type \( \text{nat} \rightarrow \text{nat} \):

\[
\lambda (x : \text{nat}. \lambda (\_ : \text{cmd} z)(\text{cmd}(\text{get}[a]))).
\]

Although the assignable \( a \) is not actually needed to compute the result, it nevertheless occurs in the value, in violation of the safety condition.
To account for this generalization, we must re-work the static semantics of $L\{\text{nat cmd} \rightarrow\}$ to record the returned type of a command and to record the type of the contents of each assignable. First, we generalize the finite set, $\Sigma$, of active assignables to assign a type to each active assignable so that $\Sigma$ has the form of a finite set of assumptions of the form $a : \tau$, where $a$ is an assignable. Second, we replace the judgement $\Gamma \vdash_\Sigma m \ ok$ by the more general form $\Gamma \vdash_\Sigma m : \sim \tau$, stating that $m$ is a well-formed command returning a value of type $\tau$. Third, the type $\text{cmd}$ must be generalized to $\text{cmd}(\tau)$ to reflect the return type of the encapsulated command.

The static semantics given in Section 37.1.1 on page 333 carries over in the evident manner, as follows:

\[
\begin{align*}
\Gamma \vdash_\Sigma m : \sim \tau \\
\Gamma \vdash_\Sigma \text{cmd}(m) : \text{cmd}(\tau)
\end{align*}
\]  

\[\text{(37.5a)}\]

\[
\begin{align*}
\Gamma \vdash_\Sigma e : \tau & \quad \tau \text{ mobile} \\
\Gamma \vdash_\Sigma \text{ret}(e) : \sim \tau
\end{align*}
\]  

\[\text{(37.5b)}\]

\[
\begin{align*}
\Gamma \vdash_\Sigma e : \text{cmd}(\tau) & \quad \Gamma, x : \tau \vdash_\Sigma m : \sim \tau' \\
\Gamma \vdash_\Sigma \text{seq}(e; x . m) : \sim \tau'
\end{align*}
\]  

\[\text{(37.5c)}\]

\[
\begin{align*}
\Gamma \vdash_\Sigma e : \tau & \quad \tau \text{ mobile} \quad \Gamma \vdash_\Sigma a : \tau \vdash_\Sigma m : \sim \tau' \\
\Gamma \vdash_\Sigma \text{dcl}(e; a . m) : \sim \tau'
\end{align*}
\]  

\[\text{(37.5d)}\]

\[
\begin{align*}
\Gamma \vdash_\Sigma a : \tau \vdash_\Sigma \text{get}[a] : \sim \tau
\end{align*}
\]  

\[\text{(37.5e)}\]

\[
\begin{align*}
\Gamma \vdash_\Sigma a : \tau & \quad e : \tau \\
\Gamma \vdash_\Sigma a : \tau \vdash_\Sigma \text{set}[a](e) : \sim \tau
\end{align*}
\]  

\[\text{(37.5f)}\]

Apart from the evident generalization to record returned types and content types, the most important change is to require that $\tau$ be mobile in Rules (37.5b) and (37.5d).

### 37.4 References to Assignables

The commands $\text{get}[a]$ and $\text{set}[a](e)$ make the assignable on which they operate explicit in the program text. Since different assignables have different contents, if $a \neq b$, then an assignment to $a$ cannot affect the contents of $b$, nor the other way around. This greatly simplifies reasoning, since we need never worry about interference between different assignables, the
References to Assignables

possibility that assigning to one interferes with the contents of the other. However, in some situations it can be useful to defer the choice of target of an assignable to execution time. For example, one may wish to pass to a procedure the assignable into which it should place its result. The question becomes, how does one pass an assignable as argument to a procedure? And how does that procedure assign to an assignable given as argument?

One method is to use a capability, an encapsulated command that, when executed, acts on one or more assignables. For example, we may associate with each assignable, \( a \), of type \( \tau \) a pair of type \( \tau \ cmd \times (\tau \rightarrow \tau \ cmd) \), namely

\[
\langle \text{cmd} (a), (\lambda (x: \tau . \text{cmd} (a := x))) \rangle.
\]

The first component of this pair is a command that returns the current contents of \( a \), and the second is a procedure that, when applied to \( x \), sets the contents of \( a \) to \( x \). These two capabilities, sometimes called a getter and a setter for \( a \), may be passed separately or together to another procedure that does not itself lie within the scope of \( a \).

The pair of capabilities serve as a reference to the assignable \( a \), since together they provide full access to \( a \). Rather than require references to be implemented in terms of encapsulated commands, we can instead treat them as a primitive notion. The type \( \text{ref}(\tau) \) is the type of references to assignables of type \( \tau \). A value of reference type is just the name of the assignable thought of as a value. There are two operations on reference types, one to get the contents, the other to set the contents, of the assignable to which it refers. These syntax of references is defined by the following grammar:

\[
\begin{array}{|c|c|c|c|}
\hline
\text{Category} & \text{Item} & \text{Abstract} & \text{Concrete} \\
\hline
\text{Type} & \tau & \text{ref}(\tau) & \tau \text{ref} \\
\text{Expr} & e & \text{ref}[a] & \text{ref}[a] \\
\text{Cmd} & m & \text{getref}(e) & \text{getref}(e) \\
&& \bowtie e & \text{setref}(e_1; e_2) \\
& & e_1 := e_2 & \\
\hline
\end{array}
\]

The primitives \( \text{getref} \) and \( \text{setref} \) take as argument a run-time value that will be a reference to an assignable.

The static semantics of references is given by the following rules:

\[
\Gamma, \Sigma \vdash a: \tau \\
\frac{}{\Gamma, \Sigma \vdash \text{ref}[a]: \text{ref}(\tau)} \quad (37.6a)
\]

\[
\Gamma, \Sigma \vdash e: \text{ref}(\tau)
\]

\[
\frac{}{\Gamma, \Sigma \vdash \text{getref}(e): \sim \tau} \quad (37.6b)
\]
37.4 References to Assignables

\[
\Gamma \vdash \Sigma e_1 : \tau \text{ ref } \quad \Gamma \vdash \Sigma e_2 : \tau \\
\Gamma \vdash \Sigma \text{ setref}(e_1; e_2) : \sim \tau
\]  
(37.6c)

Rule (37.6a) specifies that the name of any active assignable is an expression of type \( \text{ ref}(\tau) \).

The dynamic semantics defers to the corresponding operations on assignables, once the target assignable has been determined.

\[
\text{ref}[a] \mid \text{val}_{\Sigma; a}
\]  
(37.7a)

\[
\frac{e \xrightarrow{\Sigma} e'}{\text{getref}(e) \mid \mu \xrightarrow{\Sigma} \text{getref}(e') \mid \mu}
\]  
(37.7b)

\[
\frac{\text{getref}(\text{ref}[a]) \mid \mu \xrightarrow{\Sigma} \text{get}[a] \mid \mu}{e_1 \xrightarrow{\Sigma} e'_1}
\]  
(37.7c)

\[
\frac{\text{setref}(e_1; e_2) \mid \mu \xrightarrow{\Sigma} \text{setref}(e'_1; e_2) \mid \mu}{\text{setref}(\text{ref}[a]; e) \mid \mu \xrightarrow{\Sigma} \text{set}[a](e) \mid \mu}
\]  
(37.7d)

A reference to an assignable is a value. The \text{getref} and \text{setref} operations on references defer to the corresponding operations on assignables once the reference has been determined.

It may come as a surprise to realize that references do not disrupt the stack discipline. So long as reference types are not mobile, no assignable can escape its scope. We may pass references to procedures, and return them as results, but it is ensured by the type system that the reference will always be valid wherever it is used. (It is a good exercise to check the safety of the extension of \( L\{\text{nat cmd} \rightarrow \} \) with reference types.) References can even occur in data structures, but the type of such a data structure will not be mobile, and hence a value of that type cannot be stored in an assignable or returned from the scope of a declaration of an assignable. This severely limits their utility; relaxing this restriction is the subject of Chapter 38.

The main problem with reference types is that they introduce a serious source of program errors. Whereas distinct symbols name distinct assignables, distinct variables of reference type may well refer to the same
assignable. This is called *aliasing.* It arises because the meaning of a variable is given by substitution, and nothing prevents us from substituting the same reference for two distinct variables of reference type. Thus, even if $x$ and $y$ are distinct variables, it may be that a `setref` to $x$ will affect a `getref` of $y$, or *vice versa,* whereas if $a$ and $b$ are distinct symbols, a `get` of one cannot influence a `set` of the other. When using references, we must consider a quadratic number of aliasing possibilities, for each variable of reference type can influence the meaning of every other variable of reference type, and we must consider all possibilities when arguing for the correctness of a program. This quickly gets out of hand; numerous errors in programs can be attributed to unanticipated aliasing.

### 37.5 Exercises
Chapter 38
Mutable Cells

In Chapter 37 we considered an imperative programming language that adheres to the stack discipline in that assignables are allocated and deallocated on a last-in, first-out basis. To ensure this we restricted the types of return values from a command, the types of contents of assignables, to be mobile types, ones whose values cannot depend on the stack of assignables. Function and command types are not mobile, nor are reference types, because these all can classify values that make reference to a local assignable. A recursive type, such as a list, cannot be regarded as mobile unless all of its components are mobile.

To allow for mutable data structures (ones for which the structure can be altered during execution) it is necessary to broaden the definition of mobility to allow reference types to be considered mobile. This allows us to store values containing references in assignables, a critical building block for assembling a mutable data structure. Mobile references demand that assignables be given indefinite extent—they remain active and in scope as long as they are used in a data structure. We say that such assignables are scope-free, or simply free, in contrast to the scoped, or local, assignables considered in Chapter 37. With references being mobile, there is no further obstacle to decreeing that all types are mobile, with the result that there is no restriction on values that can appear as the content of an assignable or be returned as the result of a command.

We consider two formulations of a language with references to free assignables. The modal, or monadic, formulation, is a variant of Idealized Algol in which all types are defined to be mobile. To accommodate this the dynamic semantics must be changed so that assignables are allocated globally, rather than locally. The non-modal, or integral formulation, is ob-
tained from the modal one by eliminating the distinction between expressions and commands.\(^1\) This means, in particular, that expression evaluation may have an effect, and hence the dynamics of expressions must be altered to allow for this possibility. With this distinction eliminated, the type of suspended commands becomes the type of suspended expressions, a concept that will be developed further in Chapter 39.

The difference between the modal and integral formulations is whether the type of a phrase reflects its reliance on effects. The modal formulation distinguishes the type \(\tau\), whose inhabitants are pure expressions that are evaluated solely for their value, from the type \(\text{cmd}(\tau)\), whose inhabitants are commands that, when executed, may perform assignments and allocate new assignables. In many respects it is better to distinguish these types, but in at least one important class of situations the distinction is a nuisance. A benign effect is a use of mutation that is not externally visible; the overall behavior is pure, but effects are used internally for the sake of convenience or efficiency. The modal formulation exposes all uses of effects, including benign effects, whereas the integral formulation never reveals the reliance on effects, making it easier to support benign effects at the cost of hiding “malignant” ones.

### 38.1 Free Assignables

By stipulating that all types be mobile, we are demanding that assignables be globally, rather than locally allocated. For if any value may be exported from the scope of an assignable, then it is possible for a use of that assignable to escape its scope, leading to unsoundness. The solution is to simply ensure that assignables are always in scope by allocating them globally, rather than locally, so that they can never become “stale.” Such assignables are said to be scope-free, or just free, because they have no scope from which a usage of them might escape.

The dynamics of free assignables is defined in terms of states of the form \(\nu \Sigma \{ m \parallel \mu \}\) representing a command \(m\) executing in the presence of symbols \(\Sigma\) and memory \(\mu\). The scope of the symbols declared in \(\Sigma\) includes both \(m\) and \(\mu\). The dynamics consists of two forms of judgement:

\[
\begin{align*}
\nu \Sigma \{ m \parallel \mu \}\ & \text{final} \\
\nu \Sigma \{ m \parallel \mu \} \rightarrow \nu \Sigma' \{ m' \parallel \mu' \} & \text{\(m\) in \(\Sigma\) and \(\mu\) steps to \(m'\) in \(\Sigma'\) and \(\mu'\).}
\end{align*}
\]

\(^1\)Such a language is sometimes called an expression language, because all commands are forms of expression.
A command may not only access existing assignables, but may also allocate new ones.

These judgements are defined by the following rules:

\[
\begin{align*}
\frac{e \Sigma \rightarrow e'}{\nu \Sigma \{ \text{dcl}(e; a. m) \parallel \mu \} \rightarrow \nu \Sigma \{ \text{dcl}(e'; a. m) \parallel \mu \}} \\
\frac{e \text{ val}_\Sigma}{\nu \Sigma \{ \text{dcl}(e; a. m) \parallel \mu \} \rightarrow \nu \Sigma, a : \tau \{ m \parallel \mu \otimes a : e \}} \\
\frac{\nu \Sigma, a : \tau \{ \text{get}[a] \parallel \mu \otimes a : e \} \rightarrow \nu \Sigma, a : \tau \{ e \parallel \mu \otimes a : e \}} \\
\frac{e \Sigma \rightarrow e'}{\nu \Sigma \{ \text{set}[a](e) \parallel \mu \} \rightarrow \nu \Sigma \{ \text{set}[a](e') \parallel \mu \}} \\
\frac{e \text{ val}_\Sigma}{\nu \Sigma, a : \tau \{ \text{set}[a](e) \parallel \mu \otimes a : e \} \rightarrow \nu \Sigma, a : \tau \{ e \parallel \mu \otimes a : e \}}
\end{align*}
\]

(38.1a) (38.1b) (38.1c) (38.1d) (38.1e)

The most important difference is expressed by Rule (38.1b), which allows assignables to escape their scope of declaration by allocating them globally, rather than according to a stack discipline. The remaining rules are very similar to those given in Chapter 37, modified to account for heap allocation.

Execution of commands can only increase the set of active assignables.

**Lemma 38.1 (Monotonicity).** Suppose that \( \text{dom}(\mu) = \text{dom}(\Sigma) \). If \( \nu \Sigma \{ m \parallel \mu \} \rightarrow \nu \Sigma' \{ m' \parallel \mu' \} \), then \( \Sigma' \supseteq \Sigma \) and \( \text{dom}(\mu') = \text{dom}(\Sigma') \).

### 38.2 References

The only way to use a free assignable outside of its scope of declaration is via a reference type (or its representation using capabilities). For outside the scope of an assignable there is no way to refer to it other than by holding a reference to it that was exported from its scope. In particular the only way to create a mutable data structure is to incorporate within it references to free assignables. This means that reference types take on special significance in the presence of free assignables, so much so that it is common to eliminate explicit declaration of assignables altogether in favor of a
composite operation that both allocates a new free assignable (with global scope) and returns a reference to it.

The command \( \text{newref}[\tau](e) \) allocates a new free assignable, initializes it contents to the value of \( e \), and returns a reference to that assignable. It is as if this command were defined to be the composite command

\[
\text{dcl}(e; \text{a.ret}(\text{ref}[a])),
\]

except that we treat it as a primitive notion, rather than defined in terms of the declaration of a free assignable. Its static semantics is given by the rule

\[
\frac{\Gamma \vdash e : \tau}{\Gamma \vdash \text{newref}[\tau](e) : \sim \text{ref}(\tau)}.{38.2}
\]

The \( \text{getref} \) and \( \text{setref} \) primitives remain as defined in Chapter 37.

The dynamics of this formulation of references is defined by the following rules:

\[
\frac{\text{ref}[a] \text{ val}_{\Sigma,a: \tau}}{e \Sigma \mapsto e'} \quad (38.3a)
\]

\[
\frac{e \Sigma \mapsto e'}{\nu \Sigma \{ \text{newref}[\tau](e) \parallel \mu \} \mapsto \nu \Sigma \{ \text{newref}[\tau](e') \parallel \mu \}} \quad (38.3b)
\]

\[
\frac{e \Sigma \mapsto e'}{\nu \Sigma \{ \text{getref}(e) \parallel \mu \} \mapsto \nu \Sigma \{ \text{getref}(e') \parallel \mu \}} \quad (38.3c)
\]

\[
\frac{e \Sigma \mapsto e'}{\nu \Sigma \{ \text{setref}(e_1; e_2) \parallel \mu \} \mapsto \nu \Sigma \{ \text{setref}(e_1'; e_2) \parallel \mu \}} \quad (38.3d)
\]

\[
\frac{e_1 \Sigma \mapsto e_1'}{\nu \Sigma \{ \text{setref}(e_1; e_2) \parallel \mu \} \mapsto \nu \Sigma \{ \text{setref}(e_1'; e_2) \parallel \mu \}} \quad (38.3e)
\]

\[
\frac{e_1 \Sigma \text{ val}_{\Sigma \parallel \mu}}{e_2 \Sigma \mapsto e_2'} \quad (38.3f)
\]

\[
\frac{e_1 \Sigma \text{ val}_{\Sigma \parallel \mu}}{\nu \Sigma \{ \text{setref}(e_1; e_2) \parallel \mu \} \mapsto \nu \Sigma \{ \text{setref}(e_1'; e_2') \parallel \mu \}} \quad (38.3g)
\]
The integral formulation of references may be obtained from the modal formulation by collapsing the distinction between expressions and commands. Every expression is thereby a command (may mutate storage) and every command is thereby a form of expression (has a value).

The static semantics of integral references is given by the following rules:

\[ \Gamma \vdash \Sigma, a : \tau \vdash \text{ref}[a] : \text{ref}(\tau) \] (38.4a)

\[ \Gamma \vdash \Sigma, e : \tau \vdash \text{newref}[\tau](e) : \text{ref}(\tau) \] (38.4b)

\[ \Gamma \vdash \Sigma, e : \text{ref}(\tau) \vdash \text{getref}(e) : \tau \] (38.4c)

\[ \Gamma \vdash \Sigma, e_1 : \text{ref}(\tau), e_2 : \tau \vdash \text{setref}(e_1; e_2) : \tau \] (38.4d)

There is no analogue of Rule (37.1b), since there is no distinction between expressions and commands.

The dynamic semantics of the integral formulation consists of transition judgements of the form

\[ \nu \Sigma \{ e \parallel \mu \} \text{final} \]

\[ \nu \Sigma \{ e \parallel \mu \} \mapsto \nu \Sigma' \{ e' \parallel \mu' \} \]

\[ e \text{ in } \Sigma \text{ and } \mu \text{ steps to } e' \text{ in } \Sigma' \text{ and } \mu'. \]

In contrast to the modal formulation evaluation of an expression can allocate new assignables or alter the contents of any assignable.

The dynamics of the integral formulation is defined by the following rules:

\[ \nu \Sigma, a : \tau \{ \text{ref}[a] \parallel \mu \otimes \langle a : \_ \rangle \} \text{final} \] (38.5a)

\[ \nu \Sigma \{ e \parallel \mu \} \mapsto \nu \Sigma' \{ e' \parallel \mu' \} \]

\[ \nu \Sigma \{ \text{newref}[\tau](e) \parallel \mu \} \mapsto \nu \Sigma' \{ \text{newref}[\tau](e') \parallel \mu' \} \] (38.5b)

\[ \nu \Sigma \{ e \parallel \mu \} \text{final} \]

\[ \nu \Sigma \{ \text{newref}[\tau](e) \parallel \mu \} \mapsto \nu \Sigma, a : \tau \{ \text{ref}[a] \parallel \mu \otimes \langle a : e \rangle \} \] (38.5c)

\[ \nu \Sigma \{ e \parallel \mu \} \mapsto \nu \Sigma' \{ e' \parallel \mu' \} \]

\[ \nu \Sigma \{ \text{getref}(e) \parallel \mu \} \mapsto \nu \Sigma' \{ \text{getref}(e') \parallel \mu' \} \] (38.5d)
\[ \nu \Sigma, a : \tau \{ \text{getref}(\text{ref}[a]) \parallel \mu \otimes \langle a : e \rangle \} \mapsto \nu \Sigma, a : \tau \{ e \parallel \mu \otimes \langle a : e \rangle \} \]

(38.5e)

\[ \nu \Sigma \{ e_1 \parallel \mu \} \mapsto \nu \Sigma' \{ e'_1 \parallel \mu' \} \]

(38.5f)

\[ \nu \Sigma \{ \text{setref}(e_1; e_2) \parallel \mu \} \mapsto \nu \Sigma' \{ \text{setref}(e'_1; e'_2) \parallel \mu' \} \]

(38.5g)

\[ \nu \Sigma, a : \tau \{ e \parallel \mu \otimes \langle a : \_ \rangle \} \text{ final} \]

\[ \nu \Sigma, a : \tau \{ \text{setref}(\text{ref}[a]; e) \parallel \mu \otimes \langle a : \_ \rangle \} \mapsto \nu \Sigma, a : \tau \{ e \parallel \mu \otimes \langle a : e \rangle \} \]

(38.5h)

### 38.3 Safety

We will consider the safety of the integral formulation of references; the proof of safety of the modal formulation is similar. The key to the proof is the definition of the judgement \( \nu \Sigma \{ e \parallel \mu \} \text{ ok} \), which is defined as follows:

\[
\frac{
\Sigma \vdash e : \tau \quad \Sigma \vdash \mu : \Sigma
}{
\nu \Sigma \{ e \parallel \mu \} \text{ ok}
}
\]

(38.6)

The first premise of the rule states that \( e \) is well-formed relative to the typing assumptions \( \Sigma \); the particular choice of type \( \tau \) depends only on \( \Sigma \) and \( e \). The second premise states that the memory, \( \mu \), conforms to the typing assumptions \( \Sigma \). The definition of this judgement requires some care. Informally, we expect that every assignable declared in \( \Sigma \) be mapped by \( \mu \) to a value of the type specified in \( \Sigma \). So, for example, if \( \Sigma = \Sigma', a : \text{nat ref} \), then \( \mu \) must be of the form \( \mu' \otimes \langle a : \mathbb{N} \rangle \), where \( a' \) is declared in \( \Sigma' \) and is mapped to a numeral by \( \mu' \).

This example (wrongly) suggests that there may be a total ordering of assignables such that the contents of one assignable may depend only on preceding ones. But consider a memory, \( \mu \), of the form \( \mu' \otimes \langle a : e \rangle \), where \( e \) is the \( \lambda \)-abstraction

\[
\lambda (x : \text{nat}. \text{if } x \{ z \Rightarrow 1 \mid s(x') \Rightarrow x * (@a)(x') \}).
\]
This function effects a self-reference by indirection through the assignable \( a \), which is mapped by \( \mu \) to the function itself. (We shall see below that such a state can arise in the course of executing a well-typed program.)

This example shows that the definition of the judgement \( \mu : \Sigma \) must allow for the possibility of cyclic dependencies among the contents of each of the assignables in \( \mu \).

\[
\forall a : \tau \in \Sigma \mu(a) = e \text{ and } \Sigma' \vdash e : \tau \quad \frac{}{\Sigma' \vdash \mu : \sigma} \quad (38.7)
\]

That is, every assignable, \( a \), declared in \( \Sigma \) must be in the domain of \( \mu \), and the contents of \( a \) in \( \mu \) must have the type assigned to it by \( \Sigma \), relative to the assumptions \( \Sigma' \). Usually \( \Sigma' \) is just \( \Sigma \), but occasionally it is useful to allow for the extra generality.

**Theorem 38.2** (Preservation). If \( \nu \Sigma \{ e \parallel \mu \} \) ok and \( \nu \Sigma \{ e \parallel \mu \} \mapsto \nu \Sigma' \{ e' \parallel \mu' \} \), then \( \nu \Sigma' \{ e' \parallel \mu' \} \) ok.

**Proof.** Consider the transition

\[
\nu \Sigma \{ \text{newref}[\tau](e) \parallel \mu \} \mapsto \nu \Sigma, a : \tau \{ \text{ref}[a] \parallel \mu \otimes \langle a : e \rangle \}
\]

where, by tacit convention, \( a \notin \text{dom}(\Sigma) \). Since \( \nu \Sigma \{ \text{newref}[\tau](e) \parallel \mu \} \) ok, we have by inversion of typing \( \mu : \Sigma \) and \( \vdash e : \tau \). By weakening we have that \( \vdash_{\Sigma,a:\tau} e : \tau \), and hence \( \vdash_{\Sigma,a:\tau} \text{ref}[a] : \text{ref}(\tau) \) and \( \mu \otimes \langle a : e \rangle : \Sigma, a : \tau \), which suffices for the result. \( \Box \)

**Theorem 38.3** (Progress). If \( \nu \Sigma \{ e \parallel \mu \} \) ok then either \( \nu \Sigma \{ e \parallel \mu \} \) final or \( \nu \Sigma \{ e \parallel \mu \} \mapsto \nu \Sigma' \{ e' \parallel \mu' \} \) for some \( \Sigma', \mu', \) and \( e' \).

**Proof.** For example, suppose that \( \vdash_{\Sigma} \text{getref}_e : \tau \), where \( \vdash_{\Sigma} e : \tau \). By induction and the definition of final states, either \( e \) val or there exists \( \mu' \) and \( e' \) such that \( \nu \Sigma \{ e \parallel \mu \} \mapsto \nu \Sigma' \{ e' \parallel \mu' \} \). In the latter case we have

\[
\nu \Sigma \{ \text{getref}(e) \parallel \mu \} \mapsto \nu \Sigma' \{ \text{getref}(e') \parallel \mu' \}.
\]

In the former it follows that \( e = \text{ref}[a] \) for some \( a \) such that \( \Sigma = \Sigma', a : \tau \). Since \( \mu : \Sigma \), it follows that \( \mu = \mu' \otimes \langle a : e' \rangle \) for some \( \mu' \) and \( e' \) such that \( \vdash_{\Sigma} e' : \tau \). But then we have \( \nu \Sigma \{ \text{getref}(e) \parallel \mu \} \mapsto \nu \Sigma \{ e' \parallel \mu \} \). \( \Box \)
38.4 Benign Effects

The modal and integral formulations of references have complementary strengths and weaknesses. The chief virtue of the modal formulation is that the use of assignment is confined to commands, leaving expressions as pure computations. One consequence is that typing judgements for expressions retain their force even in the presence of references to free assignables, so that the type unit → unit contains only the identity and the divergent functions, and the type nat → nat consists solely of partial functions on the natural numbers. By contrast the integral formulation enjoys none of these properties. Any expression may alter or allocate new assignables, and the semantics of typing assertions is therefore significantly weakened compared to the modal formulation. In particular, the type unit → unit contains infinitely many distinct functions, and the type nat → nat contains procedures that in no way represent partial functions (for example, those whose returned value depends on previous returned values).

While the modal separation of pure expressions from impure commands may seem like an unalloyed good, it is important to recognize that the situation is not nearly so simple. The modal approach impedes the use of mutable storage to implement purely functional behavior. For example, a self-adjusting tree, such as a splay tree, uses in-place mutation to provide an efficient implementation of what is otherwise a purely functional dictionary structure mapping keys to values. The use of mutation is an example of a benign effect, a use of mutation that is not semantically visible to the client of an abstraction, but allows for more efficient execution time. In the modal formulation any use of assignment confines the programmer to the command sub-language, with no possibility of escape: there is no way to restore the purity of an impure computation!

Many other examples arise in practice. For example, suppose that we wish to instrument an otherwise pure functional program with code to collect execution statistics for profiling. In the integral setting it is a simple matter to allocate mutable cells that contain profiling information collected by assignments that update their contents at critical points in the program. In the modal setting, however, we must globally restructure the program to transform it from a pure expression to an impure command. Another example is provided by the technique of backpatching for implementing recursion using a mutable cell, which we now describe in more detail.

In the integral formulation we may implement the factorial function using backpatching as follows:
38.4 Benign Effects

\[
\begin{align*}
\text{do } & \{ \\
& \quad r \leftarrow \text{new}(\lambda n : \text{nat}. n) \\
& \quad f \leftarrow \lambda n : \text{nat}. \text{ifz}(n, 1, n'. n * (@ r)(n')) \\
& \quad _{-} \leftarrow r := f \\
& \quad f \\
\} \\
\end{align*}
\]

wherein we have used the do syntax derived from the suspension type to effect sequencing.

This expression returns a function of type \( \text{nat} \rightarrow \text{nat} \) that is obtained by (a) allocating a mutable cell initialized arbitrarily with a function of this type, (b) defining a \( \lambda \)-abstraction in which each “recursive call” consists of retrieving and applying the function stored in that cell, (c) assigning this function to the cell, and (d) returning that function. The result is a value of function type that uses a mutable cell “under the hood” in a manner not visible to its clients.

In contrast the modal formulation forces us to make explicit the reliance on private state.

\[
\begin{align*}
\text{do } & \{ \\
& \quad r \leftarrow \text{return} (\text{new} (\lambda n : \text{nat}. \text{comp}(\text{return} (n)))) \\
& \quad f \leftarrow \text{return} (\lambda n : \text{nat}. ...) \\
& \quad _{-} \leftarrow r := f \\
& \quad \text{return} f \\
\} \\
\end{align*}
\]

where the elided \( \lambda \)-abstraction is given as follows:

\[
\lambda (n : \text{nat}.
\begin{align*}
& \quad \text{ifz}(n, \\
& \quad \quad \text{comp}(\text{return}(\bar{1})), \\
& \quad \quad n'. \{\text{comp}}( \\
& \quad \quad \quad \text{do } \{ \\
& \quad \quad \quad f' \leftarrow \text{get} r \\
& \quad \quad \quad ; \text{return} (n*f'(n')) \\
& \quad \quad \} ) ) )\nonumber
\end{align*}
\]

Each branch of the conditional test returns a suspended command. In the case that the argument is zero, the command simply returns the value \( \bar{1} \). Otherwise, it fetches the contents of the associated assignable, applies this to the predecessor, and returns the result of the appropriate calculation.
The modal implementation of factorial is a command (not an expression) of type \( \text{nat} \to (\text{nat cmd}) \), which exposes two properties of the backpatching implementation:

1. The command that builds the recursive factorial function is impure, because it allocates and assigns to the assignable used to implement backpatching.

2. The body of the factorial function is impure, because it accesses the assignable to effect the recursive call.

As a result the factorial function (so implemented) may no longer be used as a function, but must instead be called as a procedure. For example, to compute the factorial of \( n \), we must write

\[
\text{do } \{ \\
\quad f \leftarrow \text{fact} \\
\quad x \leftarrow \text{let comp } (x: \text{nat}) \text{ be } f(n) \text{ in return } x \\
\quad \text{return } x \\
\}. \\
\]

Here \( \text{fact} \) stands for the command implementing factorial given above. This is bound to a variable, \( f \), which is then applied to yield an encapsulated command that, when activated, computes the desired result. This result is returned to the caller, which must itself be a command, and not an expression, propagating the reliance on effects from the callee to the caller.

### 38.5 Exercises
Part XIV

Laziness
Chapter 39

Lazy Evaluation

Lazy evaluation refers to a variety of concepts that seek to avoid evaluation of an expression unless its value is needed, and to share the results of evaluation of an expression among all uses of its, so that no expression need be evaluated more than once. Within this broad mandate, various forms of laziness are considered.

One is the call-by-need evaluation strategy for functions. This is a refinement of the call-by-name evaluation order in which arguments are passed unevaluated to functions so that it is only evaluated if needed, and, if so, the value is shared among all occurrences of the argument in the body of the function.

Another is the lazy evaluation strategy for data structures, including formation of pairs, injections into summands, and recursive folding. The decisions of whether to evaluate the components of a pair, or the argument to an injection or fold, are independent of one another, and of the decision whether to pass arguments to functions in unevaluated form.

Another aspect of laziness is the use of general recursion to define self-referential computations, including recursive functions. The role of laziness in this setting is to defer evaluation of any self-reference until it is actually required for a computation.

Traditionally, languages are classified into one of two categories. Lazy languages use a call-by-need interpretation of function application, impose a lazy evaluation strategy for data structures, and allow unrestricted use of general recursion. Strict languages take the opposite positions: call-by-value for function application, eager evaluation of data structures, and limitations on general recursion (typically, to functions). More recently, however, language designers have come to realize that it is not whole languages that
should be lazy or strict, but rather that the type system should distinguish lazy and strict evaluation order. In its most basic form this only requires the introduction of a type whose values are suspended computations that are evaluated by-need. (A more sophisticated approach is the subject of Chapter 40.)

39.1 Need Dynamics

The distinguishing feature of call-by-need is the use of memoization to record the value of an expression whenever it is computed so that, should the value of that expression ever be required again, the stored value can be returned without recomputing it. This is achieved by augmenting the computation state with a memo table that associates an expression (not necessarily a value) to each of a finite set of symbols. The symbols serve as names of the expressions to which they are associated by the memo table. Whenever the value of a name is required, the associated expression is evaluated and its value is both stored in the memo table under the same name and returned as the value of that name. This ensures that any subsequent evaluation of the same name returns the new value without recomputing it.

Another perspective on call-by-need is that it uses names to mediate sharing among multiple occurrences of a sub-expression within a larger expression. Ordinary substitution often replicates an expression, generating one copy for each occurrence of the target of the substitution. Under call-by-need each expression is given a name which serves as a proxy for it. In particular, expression names are substituted for variables so that all occurrences have the same name and hence refer to the same copy of the expression to which it is associated. In this way we economize on both the time required to evaluate the expression, which would be needlessly repeated under call-by-name, and the space required to store it during computation, which would be replicated under call-by-name.

The need dynamics for $\mathcal{L}\{\mathsf{nat} \to\}$ is based on a transition system with states of the form $\nu \Sigma \{e \parallel \mu\}$, where $\Sigma$ is a finite set of hypotheses $\alpha_1 : \tau_1, \ldots, \alpha_n : \tau_n$ associating types to names, $\mu$ is a finite mapping associating an expression to each name declared in $\Sigma$, and $e$ is an expression possibly involving those names.

By a slight abuse of notation, we write $\Sigma; \Gamma \vdash e : \tau$ to mean that the expression $e$ has type $\tau$ under the assumptions $\Sigma$ governing names and the assumptions $\Gamma$ governing variables. The judgement $\nu \Sigma \{e \parallel \mu\}$ ok is
39.1 Need Dynamics

defined by the following rules:

\[
\Sigma \vdash e : \tau \quad \Sigma \vdash \mu : \Sigma \\
\forall a : \tau \in \Sigma \quad \mu(a) = e \neq \bullet \implies \Sigma' \vdash e : \tau
\]

Rule (39.1b) permits self-reference through the memo table by allowing the expression associated to a name, \(a\), to contain \(a\), or, more generally, to contain a name whose associated expression contains \(a\), and so on through any finite chain of such dependencies. Moreover, a name that is bound to the “black hole” is considered to be of any type.

The call-by-need dynamics consists of the following two forms of judgement:

1. \(e \text{ val}_\Sigma\), stating that \(e\) is a value that may involve the names in \(a\).

2. \(\nu \Sigma \{ e \parallel \mu \} \mapsto \nu \Sigma' \{ e' \parallel \mu' \}\), stating that one step of evaluation of the expression \(e\) relative to memo table \(\mu\) with the names declared in \(\Sigma\) results in the expression \(e'\) relative to the memo table \(\mu'\) with names declared in \(\Sigma'\).

The dynamics is defined so that the collection of active names grows monotonically, and so that the type of a name never changes. The memo table may be altered destructively during execution to reflect progress in the evaluation of the expression associated with a given name.

The judgement \(e \text{ val}_\Sigma\) is defined by the following rules:

\[
\begin{align*}
\text{z val}_\Sigma \quad & (39.2a) \\
\overline{s(a)} \text{ val}_{\Sigma,a:\text{nat}} \quad & (39.2b) \\
\overline{\lambda \text{m}[\tau.(x.e)] \text{ val}_\Sigma} \quad & (39.2c)
\end{align*}
\]

Rules (39.2a) through (39.2c) specify that \(z\) is a value, any expression of the form \(s(a)\), where \(a\) is a name, is a value, and that any \(\lambda\)-abstraction, possibly containing names, is a value. It is important that names themselves are not values, rather they stand for (possibly unevaluated) expressions as specified by the memo table.
The initial and final states of evaluation are defined as follows:

\[
\nu \varnothing \{ e \parallel \varnothing \} \text{ initial}
\]

(39.3a)

\[
\nu \Sigma \{ e \parallel \mu \} \text{ final}
\]

(39.3b)

Rule (39.3a) specifies that an initial state consists of an expression evaluated relative to an empty memo table. Rule (39.3b) specifies that a final state has the form \( \nu \Sigma \{ e \parallel \mu \} \), where \( e \) is a value relative to \( \Sigma \).

The transition judgement for the call-by-need semantics of \( L\{\text{nat} \rightarrow \} \) is defined by the following rules:

\[
e \text{val}_{\Sigma, \tau} \quad \frac{v \Sigma, a : \tau \{ a \parallel \mu \otimes \langle a : e \rangle \} \rightarrow v \Sigma, a : \tau \{ e \parallel \mu \otimes \langle a : e \rangle \}}{v \Sigma, a : \tau \{ e \parallel \mu \otimes \langle a : \bullet \rangle \} \rightarrow v \Sigma', a : \tau \{ e' \parallel \mu' \otimes \langle a : \bullet \rangle \}}
\]

(39.4a)

\[
\frac{v \Sigma, a : \tau \{ e \parallel \mu \otimes \langle a : e \rangle \} \rightarrow v \Sigma', a : \tau \{ a \parallel \mu' \otimes \langle a : e' \rangle \}}{v \Sigma \{ s(e) \parallel \mu \} \rightarrow v \Sigma, a : \text{nat} \{ s(a) \parallel \mu \otimes \langle a : e \rangle \}}
\]

(39.4b)

\[
\frac{v \Sigma \{ e \parallel \mu \} \rightarrow v \Sigma' \{ e' \parallel \mu' \}}{v \Sigma \{ \text{ifz}(e; e_0; x.e_1) \parallel \mu \} \rightarrow v \Sigma' \{ \text{ifz}(e'; e_0; x.e_1) \parallel \mu' \}}
\]

(39.4c)

\[
\frac{v \Sigma \{ e \parallel \mu \} \rightarrow v \Sigma' \{ e' \parallel \mu' \}}{v \Sigma \{ \text{ifz}(z; e_0; x.e_1) \parallel \mu \} \rightarrow v \Sigma \{ e_0 \parallel \mu \}}
\]

(39.4d)

\[
\frac{v \Sigma, a : \text{nat} \{ \text{ifz}(s(a); e_0; x.e_1) \parallel \mu \otimes \langle a : e \rangle \} \rightarrow v \Sigma, a : \text{nat} \{ [a/x]e_1 \parallel \mu \otimes \langle a : e \rangle \}}{v \Sigma \{ e_1 \parallel \mu \} \rightarrow v \Sigma' \{ e'_1 \parallel \mu' \}}
\]

(39.4e)

\[
\frac{v \Sigma \{ e \parallel \mu \} \rightarrow v \Sigma' \{ e' \parallel \mu' \}}{v \Sigma \{ \text{ap}(e_1; e_2) \parallel \mu \} \rightarrow v \Sigma' \{ \text{ap}(e'_1; e_2) \parallel \mu' \}}
\]

(39.4f)
Rule (39.4a) governs a name whose associated expression is a value; the value of the name is the value associated to that name in the memo table. Rule (39.4b) specifies that if the expression associated to a name is not a value, then it is evaluated “in place” until such time as Rule (39.4a) applies. This is achieved by switching the focus of evaluation to the associated expression, while at the same time associating the black hole to that name. The black hole represents the absence of a value for that name, so that any attempt to access it during evaluation of its associated expression cannot make progress. This signals a circular dependency that, if not caught using a black hole, would initiate an infinite regress. We may therefore think of the black hole as catching a particular form of non-termination that arises when the value of an expression associated to a name depends on the name itself.

Rule (39.4c) specifies that evaluation of $s(e)$ allocates a fresh name, $a$, for the expression $e$, and yields the value $s(a)$. The value of $e$ is not determined until such time as the predecessor is required in a subsequent computation. This implements a lazy dynamics for the successor. Rule (39.4f), which governs a conditional branch on a successor, substitutes the name, $a$, for the variable, $x$, when computing the predecessor of a non-zero number, ensuring that all occurrences of $x$ share the same predecessor computation.

Rule (39.4g) specifies that the value of the function position of an application must be determined before the application can be executed. Rule (39.4h) specifies that to evaluate an application of a $\lambda$-abstraction we allocate a fresh name for the argument, and substitute this name for the parameter of the function. The argument is evaluated only if it is needed in the subsequent computation, and then that value is shared among all occurrences of the parameter in the body of the function.

General recursion is implemented by Rule (39.4i). Recall from Chapter 15 that the expression $\text{fix}[\tau](x.e)$ stands for the solution of the recursion equation $x = e$, where $x$ may occur within $e$. Rule (39.4i) computes this solution by associating a fresh name, $a$, with the body, $e$, substituting
a for x within e to effect the self-reference. It is this substitution that permits a named expression to depend on its own name. For example, the expression \( \text{fix } x : \tau \rightarrow x \) associates the expression a to a in the memo table, and returns a. The next step of evaluation is stuck, because it seeks to evaluate a with a bound to the black hole. In contrast an expression such as \( \text{fix } f : \sigma ightarrow \tau \rightarrow \lambda (x : \sigma . e) \) does not get stuck, because the self-reference is “hidden” within the \( \lambda \)-abstraction, and hence need not be evaluated to determine the value of the binding.

### 39.2 Safety

**Theorem 39.1** (Preservation). Suppose that \( v \Sigma \{ e \parallel \mu \} \rightarrow v \Sigma' \{ e' \parallel \mu' \} \). If \( v \Sigma \{ e \parallel \mu \} \) ok, then \( v \Sigma' \{ e' \parallel \mu' \} \) ok.

**Proof.** We prove by induction on Rules (39.4) that if \( v \Sigma \{ e \parallel \mu \} \rightarrow v \Sigma' \{ e' \parallel \mu' \} \) and \( \Sigma \vdash \mu : \Sigma \) and \( \Sigma \vdash e : \tau \), then \( \Sigma' \supseteq \Sigma \) and \( \Sigma' \vdash \mu' : \Sigma' \) and \( \Sigma' \vdash e' : \tau \).

Consider Rule (39.4b), for which we have

\[
\text{Assume that } \Sigma, a : \tau \vdash \mu : \Sigma, a : \tau. \text{ It follows that } \Sigma, a : \tau \vdash e_0 : \tau \text{ and } \Sigma, a : \tau \vdash \mu_0 \otimes \langle a : e_0 \rangle, \mu' = \mu'_0 \otimes \langle a : e'_0 \rangle, \text{ and }
\]

\[
v \Sigma, a : \tau \{ e_0 \parallel \mu_0 \otimes \langle a : \bullet \rangle \} \rightarrow v \Sigma', a : \tau \{ e'_0 \parallel \mu'_0 \otimes \langle a : \bullet \rangle \}. \]

But then

\[
\Sigma', a : \tau \vdash \mu' : \Sigma', a : \tau,
\]

which suffices for the result.

Consider Rule (39.4g), so that e is the application \( \text{ap}(e_1; e_2) \) and

\[
v \Sigma \{ e_1 \parallel \mu \} \rightarrow v \Sigma' \{ e'_1 \parallel \mu' \}. \]

Suppose that \( \Sigma \vdash \mu : \Sigma \) and \( \Sigma \vdash e : \tau \). By inversion of typing \( \Sigma \vdash e_1 : \tau_2 \rightarrow \tau \) for some type \( \tau_2 \) such that \( \Sigma \vdash e_2 : \tau_2 \). By induction \( \Sigma' \supseteq \Sigma \) and \( \Sigma' \vdash e'_1 : \Sigma' \) and \( \Sigma' \vdash e'_2 : \tau_2 \rightarrow \tau \). By weakening we have \( \Sigma' \vdash e_2 : \tau_2 \), so that \( \Sigma' \vdash \text{ap}(e'_1; e_2) : \tau \), which is enough for the result.

\( \square \)
The progress theorem must be stated so as to allow for stuck states arising from evaluating a name associated with a black hole. We define the judgement $\nu \Sigma \{ e \parallel \mu \}$ loops by the following rules:

$$
\begin{align*}
\nu \Sigma, a : \tau \{ a \parallel \mu \otimes \langle a : \bullet \rangle \} & \text{ loops } \quad (39.5a) \\
\nu \Sigma, a : \tau \{ e \parallel \mu \otimes \langle a : \bullet \rangle \} & \text{ loops } \quad (39.5b) \\
\nu \Sigma, a : \tau \{ a \parallel \mu \otimes \langle a : e \rangle \} & \text{ loops } \\
\nu \Sigma \{ e \parallel \mu \} & \text{ loops } \quad (39.5c) \\
\nu \Sigma \{ \text{ifz}(e; e_0; x.e_1) \parallel \mu \} & \text{ loops } \\
\nu \Sigma \{ e_1 \parallel \mu \} & \text{ loops } \quad (39.5d) \\
\nu \Sigma \{ \text{ap}(e_1; e_2) \parallel \mu \} & \text{ loops }
\end{align*}
$$

**Theorem 39.2 (Progress).** If $\nu \Sigma \{ e \parallel \mu \}$ ok, then either $\nu \Sigma \{ e \parallel \mu \}$ final, or $\nu \Sigma \{ e \parallel \mu \}$ loops, or there exists $\mu'$ and $e'$ such that $\nu \Sigma \{ e \parallel \mu \} \mapsto \nu \Sigma' \{ e' \parallel \mu' \}$.

**Proof.** By inversion of Rules (39.1) we have $\Sigma \vdash e : \tau$ and $\Sigma \vdash \mu : \Sigma$, which decomposes into $\Sigma \vdash e_1 : \tau_1, \ldots, \Sigma \vdash e_n : \tau_n$, where $\Sigma = a_1 : \tau_1, \ldots, a_n : \tau_n$. We proceed by induction on the static semantics of $\mathcal{L}\{\text{nat} \rightarrow \}$ given by Rules (15.1).

Consider Rule (15.1a), so that $\Sigma = \Sigma_0, a : \tau$ and $\Sigma \vdash \mu : \Sigma$. It follows that $\mu = \mu_0 \otimes \langle a : e_0 \rangle$ with $\Sigma \vdash \mu_0 : \Sigma_0$ and $\Sigma \vdash e_0 : \tau$. Note that $\Sigma \vdash \mu_0 \otimes \langle a : \bullet \rangle : \Sigma$. Applying induction to the derivation of $\Sigma \vdash e_0 : \tau$, we consider three cases:

1. $\nu \Sigma \{ e_0 \parallel \mu \otimes \langle a : \bullet \rangle \}$ final. By inversion of Rule (39.3b) we have $e_0 \ \text{val}_\Sigma$, and hence by Rule (39.4a) we obtain $\nu \Sigma \{ e_0 \parallel \mu \} \mapsto \nu \Sigma \{ e_0 \parallel \mu \}$.

2. $\nu \Sigma \{ e_0 \parallel \mu_0 \otimes \langle a : \bullet \rangle \}$ loops. By applying Rule (39.5b) we obtain $\nu \Sigma \{ e_0 \parallel \mu \}$ loops.

3. $\nu \Sigma \{ e_0 \parallel \mu_0 \otimes \langle a : \bullet \rangle \} \mapsto \nu \Sigma' \{ e'_0 \parallel \mu'_0 \otimes \langle a : \bullet \rangle \}$. By applying Rule (39.4b) we obtain

$$
\nu \Sigma \{ a \parallel \mu \otimes \langle a : e_0 \rangle \} \mapsto \nu \Sigma' \{ a \parallel \mu' \otimes \langle a : e'_0 \rangle \}.
$$
39.3 Lazy Data Structures

The call-by-need dynamics extends to product, sum, and recursive types in a straightforward manner. For example, the need dynamics of lazy product types is given by the following rules:

\[
\frac{\text{pair}(a_1; a_2)}{\text{val}_{\Sigma, a_1 : \mathcal{T}_1, a_2 : \mathcal{T}_2} (\text{pair}(a_1; a_2))} \tag{39.6a}
\]

\[
\left\{ \begin{array}{l}
\nu \Sigma \{ \text{pair}(e_1; e_2) \parallel \mu \} \\
\nu \Sigma, a_1 : \mathcal{T}_1, a_2 : \mathcal{T}_2 \{ \text{pair}(a_1; a_2) \parallel \mu \otimes (a_1 : e_1) \otimes (a_2 : e_2) \}
\end{array} \right. \rightarrow \\
\left\{ \begin{array}{l}
\nu \Sigma \{ e \parallel \mu \} \\
\nu \Sigma \{ \text{proj}[1](e) \parallel \mu \}
\end{array} \right. \rightarrow \\
\left\{ \begin{array}{l}
\nu \Sigma \{ e' \parallel \mu' \} \\
\nu \Sigma \{ \text{proj}[1](e') \parallel \mu' \}
\end{array} \right. \tag{39.6b}
\]

\[
\nu \Sigma \{ e \parallel \mu \} \rightarrow \nu \Sigma' \{ e' \parallel \mu' \} \\
\nu \Sigma \{ \text{proj}[1](e) \parallel \mu \} \\
\nu \Sigma \{ \text{proj}[1](e') \parallel \mu' \} \tag{39.6c}
\]

\[
\nu \Sigma \{ e \parallel \mu \} \rightarrow \nu \Sigma' \{ e' \parallel \mu' \} \\
\nu \Sigma \{ \text{proj}[1](e) \parallel \mu \} \\
\nu \Sigma \{ \text{proj}[1](e') \parallel \mu' \} \tag{39.6d}
\]

\[
\nu \Sigma \{ e \parallel \mu \} \rightarrow \nu \Sigma' \{ e' \parallel \mu' \} \\
\nu \Sigma \{ \text{proj}[1](e) \parallel \mu \} \\
\nu \Sigma \{ \text{proj}[1](e') \parallel \mu' \} \tag{39.6e}
\]

\[
\nu \Sigma \{ e \parallel \mu \} \rightarrow \nu \Sigma' \{ e' \parallel \mu' \} \\
\nu \Sigma \{ \text{proj}[1](e) \parallel \mu \} \\
\nu \Sigma \{ \text{proj}[1](e') \parallel \mu' \} \tag{39.6f}
\]

\[
\nu \Sigma \{ e \parallel \mu \} \rightarrow \nu \Sigma' \{ e' \parallel \mu' \} \\
\nu \Sigma \{ \text{proj}[1](e) \parallel \mu \} \\
\nu \Sigma \{ \text{proj}[1](e') \parallel \mu' \} \tag{39.6g}
\]

\[
\nu \Sigma \{ e \parallel \mu \} \rightarrow \nu \Sigma' \{ e' \parallel \mu' \} \\
\nu \Sigma \{ \text{proj}[1](e) \parallel \mu \} \\
\nu \Sigma \{ \text{proj}[1](e') \parallel \mu' \} \tag{39.6h}
\]

A pair is considered a value only if its arguments are names (Rule (39.6a)), which are introduced when the pair is created (Rule (39.6b)). The first and
second projections evaluate to one or the other name in the pair, inducing
a demand for the value of that component (Rules (39.6e) and (39.6h)).

Using similar techniques we may give a need dynamics to sums and
recursive types. We leave the formalization of these as an exercise for the
reader.

39.4 Suspensions

Another way to introduce laziness is to consolidate the machinery of the
by-need dynamics into a single type whose values are possibly uneval-
uated, memoized computations. The type of suspensions of type \( \tau \), writ-
ten \( \tau \text{susp} \), has as introductory form \( \text{susp} \ x : \tau \text{susp} \) representing the sus-
pended, possibly self-referential, computation, \( e \), of type \( \tau \), and as elimi-
natory form the operation \( \text{force}(e) \) that evaluates the suspended compu-
tation presented by \( e \), records the value in a memo table, and returns that
value as result.

Using suspension types we may construct other lazy types according to
our needs in a particular program. For example, the type of lazy pairs with
components of type \( \tau_1 \) and \( \tau_2 \) is expressible as the type

\[
\tau_1 \text{susp} \times \tau_2 \text{susp}
\]

and the type of call-by-need functions with domain \( \tau_1 \) and range \( \tau_2 \) is ex-
pressible as the type

\[
\tau_1 \text{susp} \to \tau_2.
\]

We may also express more complex combinations of eagerness and lazi-
ness, such as the type of “lazy lists” consisting of computations that, when
forced, evaluate either to the empty list, or a non-empty list consisting of a
natural number and another lazy list:

\[
\mu t. (\text{unit} + (\text{nat} \times t)) \text{susp}.
\]

This type should be contrasted with the type

\[
\mu t. (\text{unit} + (\text{nat} \times t \text{susp}))
\]

whose values are the empty list and a pair consisting of a natural number
and a computation of another such value.
The syntax of suspensions is given by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>τ</td>
<td>::= susp(τ)</td>
<td>τ susp</td>
</tr>
<tr>
<td>Expr</td>
<td>e</td>
<td>::= susp<a href="x.e">τ</a></td>
<td>susp x : τ is e</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>force(e)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>susp[a]</td>
</tr>
</tbody>
</table>

Suspensions are self-referential; the bound variable, \( x \), refers to the suspension itself. The expression \( \text{susp}[a] \) is a reference to the suspension named \( a \).

The statics of the suspension type is given using a judgement of the form \( \sum \Gamma \vdash e : \tau \), where \( \sum \) assigns types to the names of suspensions. It is defined by the following rules:

\[
\begin{align*}
\sum, x : \text{susp}(\tau) \vdash e : \tau & \quad (39.7a) \\
\sum \Gamma \vdash \text{susp}[\tau](x.e) : \text{susp}(\tau) & \\
\sum \Gamma \vdash e : \text{susp}(\tau) & \quad (39.7b) \\
\sum \Gamma \vdash \text{force}(e) : \tau & \\
\sum, a : \tau \Gamma \vdash \text{susp}[a] : \text{susp}(\tau) & \quad (39.7c)
\end{align*}
\]

Rule (39.7a) checks that the expression, \( e \), has type \( \tau \) under the assumption that \( x \), which stands for the suspension itself, has type \( \text{susp}(\tau) \).

The by-need dynamics of suspensions is defined by the following rules:

\[
\begin{align*}
\text{susp}[a] \text{ val}_{\sum, a : \tau} & \quad (39.8a) \\
\nu \sum \{ \text{susp}[\tau](x.e) \parallel \mu \} & \quad (39.8b) \\
\nu \sum, a : \tau \{ \text{susp}[a] \parallel \mu \otimes (a : e) \} & \\
\nu \sum, a : \tau \{ e \parallel \mu \} & \quad (39.8c) \\
\nu \sum \{ \text{force}(e) \parallel \mu \} & \quad (39.8d) \\
\nu \sum, a : \tau \{ \text{force}(\text{susp}[a]) \parallel \mu \otimes (a : e) \} & \\
\nu \sum, a : \tau \{ e \parallel \mu \otimes (a : e) \}
\end{align*}
\]
39.5 Exercises

\[ \nu \Sigma, a : \tau \{ e \parallel \mu \otimes \langle a : \bullet \rangle \} \]
\[ \mapsto \]
\[ \nu \Sigma', a : \tau \{ e' \parallel \mu' \otimes \langle a : \bullet \rangle \} \]
\[ \begin{cases} 
\nu \Sigma, a : \tau \{ \text{force(susp}[a]) \parallel \mu \otimes \langle a : e \rangle \} \\
\nu \Sigma', a : \tau \{ \text{force(susp}[a]) \parallel \mu' \otimes \langle a : e' \rangle \}
\end{cases} \] (39.8e)

Rule (39.8a) specifies that a reference to a suspension is a value. Rule (39.8b) specifies that evaluation of a delayed computation consists of allocating a fresh name for it in the memo table, and returning a reference to that suspension. Rules (39.8c) to (39.8e) specify that demanding the value of a suspension forces evaluation of the suspended computation, which is then stored in the memo table and returned as result.

39.5 Exercises
Chapter 40

Polarization

Up to this point we have frequently encountered arbitrary choices in the dynamic semantics of various language constructs. For example, when specifying the dynamics of pairs, we must choose, rather arbitrarily, between the lazy semantics, in which all pairs are values regardless of the value status of their components, and the eager semantics, in which a pair is a value only if its components are both values. We could even consider a half-eager (or, if you are a pessimist, half-lazy) semantics, in which a pair is a value only if, say, the first component is a value, but without regard to the second. Although the latter choice seems rather arbitrary, it is no less so than the choice between a fully lazy or a fully eager dynamics.

Similar questions arise with sums (all injections are values, or only injections of values are values), recursive types (all folds are values, or only folds whose arguments are values), and function types (functions should be called by-name or by-value). Whole languages are built around adherence to one policy or another. For example, Haskell decrees that products, sums, and recursive types are to be lazy, and functions are to be called by name, whereas ML decrees the exact opposite policy. Not only are these choices arbitrary, but it is also unclear why they should be linked. For example, one could very sensibly decree that products, sums, and recursive types are lazy, yet impose a call-by-value discipline on functions. Or one could have eager products, sums, and recursive types, yet insist on call-by-name. It is not at all clear which of these points in the space of choices is right; each language has its adherents, each has its drawbacks, and each has its advantages.

Are we therefore stuck in a tarpit of subjectivity? No! The way out is to recognize that these distinctions should not be imposed by the language
designer, but rather are choices that are to be made by the programmer. This is achieved by recognizing that differences in dynamics reflect fundamental type distinctions that are being obscured by languages that impose one policy or another. We can have both eager and lazy pairs in the same language by simply distinguishing them as two distinct types, and similarly we can have both eager and lazy sums in the same language, and both by-name and by-value function spaces, by providing sufficient type distinctions as to make the choice available to the programmer.

In this chapter we will introduce polarization to distinguish types based on whether their elements are defined by their values (the positive types) or by their behavior (the negative types). Put in other terms, positive types are “eager” (determined by their values), whereas negative types are “lazy” (determined by their behavior). Since positive types are defined by their values, they are eliminated by pattern matching against these values. Similarly, since negative types are defined by their behavior under a range of experiments, they are eliminated by performing an experiment on them.

To make these symmetries explicit we formalize polarization using a technique called focusing, or focalization. A focused presentation of a programming language distinguishes three general forms of expression, (positive and negative) values, (positive and negative) continuations, and (neutral) computations. Besides exposing the symmetries in a polarized type system, focusing also clarifies the design of the control machine introduced in Chapter 27. In a focused framework stacks are just continuations, and states are just computations; there is no need for any ad hoc apparatus to explain the flow of control in a program.

### 40.1 Polarization

Polarization consists of distinguishing positive from negative types according to the following two principles:

1. A positive type is defined by its introduction rules, which specify the values of that type in terms of other values. The elimination rules are inversions that specify a computation by pattern matching on values of that type.

2. A negative type is defined by its elimination rules, which specify the observations that may be performed on elements of that type. The

---

More precisely, we employ a weak form of focusing, rather than the stricter forms considered elsewhere in the literature.
introduction rules specify the values of that type by specifying how they respond to observations.

Based on this characterization we can anticipate that the type of natural numbers would be positive, since it is defined by zero and successor, whereas function types would be negative, since they are characterized by their behavior when applied, and not by their internal structure.

The language $L^\pm\{\text{nat} \to\}$ is a polarized formulation of $L\{\text{nat} \to\}$ in which the syntax of types is given by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pos. Type</td>
<td>$\tau^+$</td>
<td>$\text{dn}(\tau^-)$</td>
<td>$\downarrow \tau^-$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{nat}$</td>
<td>$\text{nat}$</td>
</tr>
<tr>
<td>Neg. Type</td>
<td>$\tau^-$</td>
<td>$\text{up}(\tau^+)$</td>
<td>$\uparrow \tau^+$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{parr}(\tau^+_1;\tau^+_2)$</td>
<td>$\tau^+_1 \to \tau^+_2$</td>
</tr>
</tbody>
</table>

The types $\downarrow \tau^-$ and $\uparrow \tau^+$ effect a polarity shift from negative to positive and positive to negative, respectively. Intuitively, the shifted type $\uparrow \tau^+$ is just the inclusion of positive into negative values, whereas the shifted type $\downarrow \tau^-$ represents the type of suspended computations of negative type.

The domain of the negative function type is required to be positive, but its range is negative. This allows us to form right-iterated function types

$$\tau^+_1 \to (\tau^+_2 \to (\ldots (\tau^+_n \to \tau^+)))))$$

directly, but to form a left-iterated function type requires shifting,

$$\downarrow (\tau^+_1 \to \tau^+_2) \to \tau^-,$$

to turn the negative function type into a positive type. Conversely, shifting is needed to define a function whose range is positive, $\tau^+_1 \to \uparrow \tau^+_2$.

\section*{40.2 Focusing}

The syntax of $L^\pm\{\text{nat} \to\}$ is motivated by the polarization of its types. For each polarity we have a class of values and a class of continuations with
which we may create (neutral) computations.

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pos. Value</td>
<td>$v^+$</td>
<td>$z$</td>
<td>$z$</td>
</tr>
<tr>
<td></td>
<td>$s(v^+)$</td>
<td>$s(v^+)$</td>
<td>$s(v^+)$</td>
</tr>
<tr>
<td></td>
<td>$\text{del}^-(e)$</td>
<td>$\text{del}^-(e)$</td>
<td>$\text{del}^-(e)$</td>
</tr>
<tr>
<td>Pos. Cont.</td>
<td>$k^+$</td>
<td>$\text{ifz}(e_0; x.e_1)$</td>
<td>$\text{ifz}(e_0; x.e_1)$</td>
</tr>
<tr>
<td></td>
<td>$\text{force}^-(k^-)$</td>
<td>$\text{force}^-(k^-)$</td>
<td>$\text{force}^-(k^-)$</td>
</tr>
<tr>
<td>Neg. Value</td>
<td>$v^-$</td>
<td>$\text{lam}<a href="x.e">\tau^+</a>$</td>
<td>$\lambda(x:\tau^+, e)$</td>
</tr>
<tr>
<td></td>
<td>$\text{del}^+(v^+)$</td>
<td>$\text{del}^+(v^+)$</td>
<td>$\text{del}^+(v^+)$</td>
</tr>
<tr>
<td></td>
<td>$\text{fix}(x.v^-)$</td>
<td>$\text{fix}(x.v^-)$</td>
<td>$\text{fix}(x.v^-)$</td>
</tr>
<tr>
<td>Neg. Cont.</td>
<td>$k^-$</td>
<td>$\text{ap}(v^+; k^-)$</td>
<td>$\text{ap}(v^+; k^-)$</td>
</tr>
<tr>
<td></td>
<td>$\text{force}^+(x.e)$</td>
<td>$\text{force}^+(x.e)$</td>
<td>$\text{force}^+(x.e)$</td>
</tr>
<tr>
<td>Computation</td>
<td>$e$</td>
<td>$\text{ret}(v^-)$</td>
<td>$\text{ret}(v^-)$</td>
</tr>
<tr>
<td></td>
<td>$\text{cut}^+(v^+; k^+)$</td>
<td>$v^+ \triangleright k^+$</td>
<td>$v^+ \triangleright k^+$</td>
</tr>
<tr>
<td></td>
<td>$\text{cut}^-(v^-; k^-)$</td>
<td>$v^- \triangleright k^-$</td>
<td>$v^- \triangleright k^-$</td>
</tr>
</tbody>
</table>

The positive values include the numerals, and the negative values include functions. In addition we may delay a computation of a negative value to form a positive value using $\text{del}^-(e)$, and we may consider a positive value to be a negative value using $\text{del}^+(v^+)$. The positive continuations include the conditional branch, *sans* argument, and the negative continuations include application sites for functions consisting of a positive argument value and a continuation for the negative result. In addition we include positive continuations to force the computation of a suspended negative value, and to extract an included positive value. Computations, which correspond to machine states, consist of returned negative values (these are final states), states passing a positive value to a positive continuation, and states passing a negative value to a negative continuation. General recursion appears as a form of negative value; the recursion is unrolled when it is made the subject of an observation.

### 40.3 Statics

The static semantics of $L^{\pm\{\text{nat} \rightarrow \}}$ consists of a collection of rules for deriving judgements of the following forms:

- Positive values: $\Gamma \vdash v^+ : \tau^+$.
- Positive continuations: $\Gamma \vdash k^+ : \tau^+ > \gamma^-$.
• Negative values: $\Gamma \vdash v^{-} : \tau^{-}$.
• Negative continuations: $\Gamma \vdash k^{-} : \tau^{-} > \gamma^{-}$.
• Computations: $\Gamma \vdash e : \gamma^{-}$.

Throughout $\Gamma$ is a finite set of hypotheses of the form

$$x_1 : \tau_1^+, \ldots, x_n : \tau_n^+,$$

for some $n \geq 0$, and $\gamma^{-}$ is any negative type.

The typing rules for continuations specify both an argument type (on which values they act) and a result type (of the computation resulting from the action on a value). The typing rules for computations specify that the outcome of a computation is a negative type. All typing judgements specify that variables range over positive types. (These restrictions may always be met by appropriate use of shifting.)

The static semantics of positive values consists of the following rules:

$$\Gamma, x : \tau^+ \vdash x : \tau^+ \tag{40.1a}$$

$$\Gamma \vdash z : \text{nat} \tag{40.1b}$$

$$\Gamma \vdash v^+ : \text{nat}, \quad \Gamma \vdash s(v^+) : \text{nat} \tag{40.1c}$$

$$\Gamma \vdash e : \tau^{-}, \quad \Gamma \vdash \text{del}^{-}(e) : \downarrow \tau^{-} \tag{40.1d}$$

Rule (40.1a) specifies that variables range over positive values. Rules (40.1b) and (40.1c) specify that the values of type $\text{nat}$ are just the numerals. Rule (40.1d) specifies that a suspended computation (necessarily of negative type) is a positive value.

The static semantics of positive continuations consists of the following rules:

$$\Gamma \vdash e_0 : \gamma^{-}, \quad \Gamma, x : \text{nat} \vdash e_1 : \gamma^{-} \quad \Gamma \vdash \text{ifz}(e_0; x.e_1) : \text{nat} > \gamma^{-} \tag{40.2a}$$

$$\Gamma \vdash k^{-} : \tau^{-} > \gamma^{-}, \quad \Gamma \vdash \text{force}^{-}(k^{-}) : \downarrow \tau^{-} > \gamma^{-} \tag{40.2b}$$

Rule (40.2a) governs the continuation that chooses between two computations according to whether a natural number is zero or non-zero. Rule (40.2b)
specifies the continuation that forces a delayed computation with the specified negative continuation.

The static semantics of negative values is defined by these rules:

\[
\frac{\Gamma, x : \tau_1 \vdash e : \tau_2}{\Gamma \vdash \lambda (x: \tau_1). e : \tau_1 \to \tau_2}
\] (40.3a)

\[
\frac{\Gamma \vdash v^+ : \tau^+}{\Gamma \vdash \text{del}^+(v^+) : \uparrow \tau^+}
\] (40.3b)

\[
\frac{\Gamma, x : \downarrow \tau^- \vdash v^- : \tau^-}{\Gamma \vdash \text{fix} x = v^- : \tau^-}
\] (40.3c)

Rule (40.3a) specifies the static semantics of a \(\lambda\)-abstraction whose argument is a positive value, and whose result is a computation of negative type. Rule (40.3b) specifies the inclusion of positive values as negative values. Rule (40.3c) specifies that negative types admit general recursion.

The static semantics of negative continuations is defined by these rules:

\[
\frac{\Gamma \vdash v_1^+ : \tau_1^+ \quad \Gamma \vdash k_2^- : \tau_2^- \to \gamma^-}{\Gamma \vdash \text{ap}(v_1^+; k_2^-) : \tau_1^+ \to \tau_2^- > \gamma^-}
\] (40.4a)

\[
\frac{\Gamma, x : \tau^+ \vdash e : \gamma^-}{\Gamma \vdash \text{force}^+(x.e) : \uparrow \tau^+ > \gamma^-}
\] (40.4b)

Rule (40.4a) is the continuation representing the application of a function to the positive argument, \(v_1^+\), and executing the body with negative continuation, \(k_2^-\). Rule (40.4b) specifies the continuation that passes a positive value, viewed as a negative value, to a computation.

The static semantics of computations is given by these rules:

\[
\frac{\Gamma \vdash v^- : \tau^-}{\Gamma \vdash \text{ret}(v^-) : \tau^-}
\] (40.5a)

\[
\frac{\Gamma \vdash v^+ : \tau^+ \quad \Gamma \vdash k^-_1 : \tau^+ \to \gamma^- \quad \Gamma \vdash k_2^- : \gamma^-}{\Gamma \vdash v^+ \triangleright k^- : \gamma^-}
\] (40.5b)

\[
\frac{\Gamma \vdash v^- : \tau^- \quad \Gamma \vdash k^- : \tau^- \to \gamma^-}{\Gamma \vdash v^- \triangleright k^- : \gamma^-}
\] (40.5c)

Rule (40.5a) specifies the basic form of computation that simply returns the negative value \(v^-\). Rules (40.5b) and (40.5c) specify computations that pass a value to a continuation of appropriate polarity.
40.4 Dynamics

The dynamics of $L^{\pm}\{\text{nat} \rightarrow\}$ is given by a transition system $e \mapsto e'$ specifying the steps of computation. The rules are all axioms; no premises are required because the continuation is used to manage pending computations.

The dynamic semantics consists of the following rules:

\begin{align*}
\text{z} & \triangleright \text{if}z(e_0;x.e_1) \rightarrow e_0 \quad (40.6a) \\
\text{s}(v^+) & \triangleright \text{if}z(e_0;x.e_1) \rightarrow [v^+/x]e_1 \quad (40.6b) \\
\text{del}^{-}(e) & \triangleright \text{force}^{-}(k^-) \rightarrow e;k^- \quad (40.6c) \\
\lambda(x:\tau^+.e) & \triangleright \text{ap}(v^+;k^-) \rightarrow [v^+/x]e;k^- \quad (40.6d) \\
\text{del}^{+}(v^+) & \triangleright \text{force}^{+}(x.e) \rightarrow [v^+/x]e \quad (40.6e) \\
\text{fix}(v^-) & \triangleright \text{if}(\text{fix}(v^-)) \rightarrow [\text{del}^{-}(\text{fix}(v^-))/x]v^- \triangleright k^- \quad (40.6f)
\end{align*}

These rules specify the interaction between values and continuations.

Rules (40.6) make use of two forms of substitution, $[v^+/x]e$ and $[v^+/x]v^-$, which are defined as in Chapter 7. They also employ a new form of composition, written $e;k_0$, which composes a computation with a continuation by attaching $k_0$ to the end of the computation specified by $e$. This composition is defined mutually recursive with the compositions $k^+;k_0$ and $k^-;k_0$, which essentially concatenate continuations (stacks).

\begin{align*}
\text{ret}(v^-);k^- & = v^- \triangleright k^- \quad (40.7a) \\
(k^-;k_0) & = k_1^- \\
(v^- \triangleright k^-);k_0 & = v^- \triangleright k_1^- \quad (40.7b) \\
(k^+;k_0) & = k_1^+ \\
(v^+ \triangleright k^+);k_0 & = v^+ \triangleright k_1^+ \quad (40.7c) \\
(e_0;k^- = e_0' \mid e_1;k^- = e_1') & \triangleright \text{if}z(e_0;x.e_1);k^- = \text{if}z(e_0'x.e_1') \quad (40.7d)
\end{align*}
376 40.5 Safety

\[
\begin{align*}
  k^-; k_0^- &= k_1^- \\
  \text{force}^- (k^-); k_0^- &= \text{force}^- (k_1^-) \\
  k^-; k_0^- &= k_1 \\
  \text{ap}(v^+; k^-); k_0^- &= \text{ap}(v^+; k_1^-) \\
  x | e; k_0^- &= e' \\
  \text{force}^+ (x.e); k_0^- &= \text{force}^+ (x.e')
\end{align*}
\] (40.7e)

(40.7f)

x | e; k_0^- = e'

(40.7g)

Rules (40.7d) and (40.7g) make use of the parametric general judgement defined in Chapter 3 to express that the composition is defined uniformly in the bound variable.

40.5 Safety

The proof of preservation for \( L^\pi \{\text{nat} \rightarrow \} \) reduces to the proof of the typing properties of substitution and composition.

**Lemma 40.1 (Substitution).** Suppose that \( \Gamma \vdash v^+ : \sigma^+ \).

1. If \( \Gamma, x : \sigma^+ \vdash e : \gamma^- \), then \( \Gamma \vdash [v^+/x]e : \gamma^- \).
2. If \( \Gamma, x : \sigma^+ \vdash v^- : \tau^- \), then \( \Gamma \vdash [v^+/x]v^- : \tau^- \).
3. If \( \Gamma, x : \sigma^+ \vdash k^+ : \tau^+ > \gamma^- \), then \( \Gamma \vdash [v^+/x]k^+ : \tau^+ > \gamma^- \).
4. If \( \Gamma, x : \sigma^+ \vdash v_1^+ : \tau^+ \), then \( \Gamma \vdash [v^+/x]v_1^+ : \tau^+ \).
5. If \( \Gamma, x : \sigma^+ \vdash k^- : \tau^- > \gamma^- \), then \( \Gamma \vdash [v^+/x]k^- : \tau^- > \gamma^- \).

**Proof.** Simultaneously, by induction on the derivation of the typing of the target of the substitution. \(\square\)

**Lemma 40.2 (Composition).**

1. If \( \Gamma \vdash e : \tau^- \) and \( \Gamma \vdash k^- : \tau^- > \gamma^- \), then \( \Gamma \vdash e ; k^- : \tau^- > \gamma^- \).
2. If \( \Gamma \vdash k_0^+ : \tau^+ > \gamma_0^+ \), and \( \Gamma \vdash k_1^+ : \gamma_0^+ > \gamma_1^+ \), then \( \Gamma \vdash k_0^+ ; k_1^+ : \tau^+ > \gamma_1^+ \).
3. If \( \Gamma \vdash k^-_0 : \tau^- > \gamma_0^- \), and \( \Gamma \vdash k^-_1 : \gamma_0^- > \gamma_1^- \), then \( \Gamma \vdash k^-_0 ; k^-_1 : \tau^- > \gamma_1^- \).
40.6 Definability

Proof. Simultaneously, by induction on the derivations of the first premises of each clause of the lemma.

\[
\text{Theorem 40.3 (Preservation). If } \Gamma \vdash e : \gamma^- \text{ and } e \mapsto e', \text{ then } \Gamma \vdash e' : \gamma^-.
\]

Proof. By induction on transition, appealing to inversion for typing and Lemmas 40.1 on the preceding page and 40.2 on the facing page.

The progress theorem reduces to the characterization of the values of each type. Focusing makes the required properties evident, since it defines directly the values of each type.

\[
\text{Theorem 40.4 (Progress). If } \Gamma \vdash e : \gamma^-, \text{ then either } e = \text{ret}(v^-) \text{ for some } v^-, \text{ or there exists } e' \text{ such that } e \mapsto e'.
\]

40.6 Definability

The syntax of \( L^\pm \{\text{nat}\rightarrow} \) exposes the symmetries between positive and negative types, and hence between eager and lazy computation. It is not, however, especially convenient for writing programs because it requires that each computation in a program be expressed in the stilted form of a value juxtaposed with a continuation. It would be useful to have a more natural syntax that is translatable into the present language.

But the question of what is a natural syntax begs the very question that motivated the language in the first place!

This chapter under construction . . . .

40.7 Exercises
Part XV

Parallelism
Chapter 41

Nested Parallelism

Parallel computation seeks to reduce the running times of programs by allowing many computations to be carried out simultaneously. For example, if one wishes to add two numbers, each given by a complex computation, we may consider evaluating the addends simultaneously, then computing their sum. The ability to exploit parallelism is limited by the dependencies among parts of a program. Obviously, if one computation depends on the result of another, then we have no choice but to execute them sequentially so that we may propagate the result of the first to the second. Consequently, the fewer dependencies among sub-computations, the greater the opportunities for parallelism. This argues for functional models of computation, because the possibility of mutation of shared assignables imposes sequentialization constraints on imperative code.

In this chapter we discuss nested parallelism in which we nest parallel computations within one another in a hierarchical manner. Nested parallelism is sometimes called fork-join parallelism to emphasize the hierarchical structure arising from forking two (or more) parallel computations, then joining these computations to combine their results before proceeding. We will consider two forms of semantics for nested parallelism. The first is a generalization of the familiar structural operational semantics in which a single transition on a compound expression may involve multiple transitions on its constituent expressions. The second is a cost semantics (introduced in Chapter 12) that focuses attention on the sequential and parallel complexity (also known as the work and depth) of a parallel program by associating a series-parallel graph with each computation.
41.1 BinaryFork-Join

We begin with a parallel language whose sole source of parallelism is the simultaneous evaluation of two variable bindings. This is modelled by a construct of the form letpar \( x_1 = e_1 \) and \( x_2 = e_2 \) in \( e \), in which we bind two variables, \( x_1 \) and \( x_2 \), to two expressions, \( e_1 \) and \( e_2 \), respectively, for use within a single expression, \( e \). This represents a simple fork-join primitive in which \( e_1 \) and \( e_2 \) may be evaluated independently of one another, with their results combined by the expression \( e \). Some other forms of parallelism may be defined in terms of this primitive. For example, a parallel pair construct might be defined as the expression

\[
\text{letpar}(e_1; e_2; x_1 . x_2)\
\]

which evaluates the components of the pair in parallel, then constructs the pair itself from these values.

The abstract syntax of the parallel binding construct is given by the abstract binding tree

\[
\text{letpar}(e_1; e_2; x_1 . x_2)\
\]

which makes clear that the variables \( x_1 \) and \( x_2 \) are bound only within \( e \), and not within their bindings. This ensures that evaluation of \( e_1 \) is independent of evaluation of \( e_2 \), and vice versa. The typing rule for an expression of this form is given as follows:

\[
\Gamma \vdash e_1 : \tau_1 \quad \Gamma \vdash e_2 : \tau_2 \quad \Gamma, x_1 : \tau_1, x_2 : \tau_2 \vdash e : \tau \\
\Gamma \vdash \text{letpar}(e_1; e_2; x_1 . x_2 . e) : \tau
\]

Although we emphasize the case of binary parallelism, it should be clear that this construct easily generalizes to \( n \)-way parallelism for any static value of \( n \). One may also define an \( n \)-way parallel let construct from the binary parallel let by cascading binary splits. (For a treatment of \( n \)-way parallelism for a dynamic value of \( n \), see Section 41.3 on page 388.)

We will give both a sequential and a parallel dynamic semantics of the parallel let construct. The definition of the sequential dynamics as a transition judgement of the form \( e \mapsto_{\text{seq}} e' \) is entirely straightforward:

\[
\begin{align*}
\text{letpar}(e_1; e_2; x_1 . x_2 . e) & \mapsto_{\text{seq}} \text{letpar}(e'_1; e_2; x_1 . x_2 . e) \\
\text{letpar}(e_1; e_2; x_1 . x_2 . e) & \mapsto_{\text{seq}} \text{letpar}(e_1; e'_2; x_1 . x_2 . e)
\end{align*}
\]
The parallel dynamics is given by a transition judgement of the form $e \mapsto \text{par} e'$, defined as follows:

\[
\frac{e_1 \mapsto \text{par} e'_1 \quad e_2 \mapsto \text{par} e'_2}{\text{letpar}(e_1; e_2; x_1.x_2.e) \mapsto \text{par} \text{letpar}(e'_1; e'_2; x_1.x_2.e)} \tag{41.3a}
\]

\[
\frac{e_1 \mapsto \text{par} e'_1 \quad e_2 \mapsto \text{par} e'_2}{\text{letpar}(e_1; e_2; x_1.x_2.e) \mapsto \text{par} \text{letpar}(e'_1; e'_2; x_1.x_2.e)} \tag{41.3b}
\]

\[
\frac{e_1 \mapsto \text{par} e'_1 \quad e_2 \mapsto \text{par} e'_2}{\text{letpar}(e_1; e_2; x_1.x_2.e) \mapsto \text{par} \text{letpar}(e'_1; e'_2; x_1.x_2.e)} \tag{41.3c}
\]

\[
\frac{e_1 \mapsto \text{par} e'_1 \quad e_2 \mapsto \text{par} e'_2}{\text{letpar}(e_1; e_2; x_1.x_2.e) \mapsto \text{par} \text{letpar}(e'_1; e'_2; x_1.x_2.e)} \tag{41.3d}
\]

The parallel semantics is idealized in that it abstracts away from any limitations on parallelism that would necessarily be imposed in practice by the availability of computing resources. (We will return to this point in Section 41.4 on page 390.)

An important advantage of the present approach is captured by the implicit parallelism theorem, which states that the sequential and the parallel semantics coincide. This means that one need never be concerned with the semantics of a parallel program (its meaning is determined by the sequential dynamics), but only with its performance. Since the sequential dynamics is deterministic (every expression has at most one value), the implicit parallelism theorem implies that the parallel dynamics is also deterministic. This clearly distinguishes parallelism, which is deterministic, from concurrency, which is non-deterministic (see Chapters 43 and 44 for more on concurrency).

**Lemma 41.1.** If \(\text{letpar}(e_1; e_2; x_1.x_2.e) \mapsto \text{par} v\) with \(v\) val, then there exists \(v_1\) val and \(v_2\) val such that \(e_1 \mapsto \text{par} v_1, e_2 \mapsto \text{par} v_2,\) and \([v_1, v_2 / x_1, x_2]e \mapsto \text{par} v\).

**Proof.** Since \(v\) val, the given derivation must consist of one or more steps. We proceed by induction on the derivation of the first step, \(\text{letpar}(e_1; e_2; x_1.x_2.e) \mapsto \text{par} e'\). For Rule (41.3d), we have \(e_1\) val and \(e_2\) val, and \(e' = [e_1, e_2 / x_1, x_2]e\), so we may take \(v_1 = e_1\) and \(v_2 = e_2\) to complete the proof. The other cases follow easily by induction. \(\square\)
Lemma 41.2. If $\text{letpar}(e_1; e_2; x_1 . x_2 . e) \rightarrow^*_{\text{seq}} v$ with $v$ val, then there exists $v_1$ val and $v_2$ val such that $e_1 \rightarrow^*_{\text{seq}} v_1$, $e_2 \rightarrow^*_{\text{seq}} v_2$, and $[v_1, v_2/ x_1, x_2] e \rightarrow^*_{\text{seq}} v$.

Proof. Similar to the proof of Lemma 41.2.

Theorem 41.3 (Implicit Parallelism). The sequential and parallel dynamics coincide: for all $v$ val, $e \rightarrow^*_{\text{seq}} v$ iff $e \rightarrow^*_{\text{par}} v$.

Proof. From left to right it is enough to prove that if $e \rightarrow^*_{\text{seq}} e' \rightarrow^*_{\text{par}} v$ with $v$ val, then $e \rightarrow^*_{\text{par}} v$. This may be shown by induction on the derivation of $e \rightarrow^*_{\text{seq}} e'$. If $e \rightarrow^*_{\text{seq}} e'$ by Rule (41.2c), then by Rule (41.3d) we have $e \rightarrow^*_{\text{par}} e'$, and hence $e \rightarrow^*_{\text{par}} v$. If $e \rightarrow^*_{\text{seq}} e'$ by Rule (41.2a), then we have $e = \text{letpar}(e_1; e_2; x_1 . x_2 . e)$, $e' = \text{letpar}(e'_1; e'_2; x_1 . x_2 . e)$, and $e_1 \rightarrow_{\text{par}} e'_1$. By Lemma 41.1 on the preceding page there exists $v_1$ val and $v_2$ val such that $e'_1 \rightarrow^*_{\text{par}} v_1$, $e'_2 \rightarrow^*_{\text{par}} v_2$, and $[v_1, v_2/ x_1, x_2] e \rightarrow^*_{\text{par}} v$. By induction we have $e_1 \rightarrow^*_{\text{par}} v_1$, and hence $e \rightarrow_{\text{par}} v$. The other cases are handled similarly.

From right to left, it is enough to prove that if $e \rightarrow_{\text{par}} e' \rightarrow^*_{\text{seq}} v$ with $v$ val, then $e \rightarrow^*_{\text{seq}} v$. We proceed by induction on the derivation of $e \rightarrow_{\text{par}} e'$. Rule (41.3d) carries over directly to the sequential case by Rule (41.2c). Consider Rule (41.3a). We have $\text{letpar}(e_1; e_2; x_1 . x_2 . e) \rightarrow_{\text{par}} \text{letpar}(e'_1; e'_2; x_1 . x_2 . e)$, $e_1 \rightarrow_{\text{par}} e'_1$, and $e_2 \rightarrow_{\text{par}} e'_2$. By Lemma 41.2 we have that there exists $v_1$ val and $v_2$ val such that $e'_1 \rightarrow^*_{\text{seq}} v_1$, $e'_2 \rightarrow^*_{\text{seq}} v_2$, and $[v_1, v_2/ x_1, x_2] e \rightarrow^*_{\text{seq}} v$. By induction we have $e_1 \rightarrow^*_{\text{seq}} v_1$ and $e_2 \rightarrow^*_{\text{seq}} v_2$, and hence $e \rightarrow^*_{\text{seq}} v$, as required. The other cases are handled similarly.

Theorem 41.3 states that parallelism is implicit in that the use of a parallel evaluation strategy does not affect the semantics of a program, but only its efficiency. The program means the same thing under a parallel execution strategy as it does under a sequential one. Correctness concerns are factored out, focusing attention on time (and space) complexity of a parallel execution strategy.

41.2 Cost Semantics

In this section we define a parallel cost semantics that assigns a cost graph to the evaluation of an expression. Cost graphs are defined by the following
41.2 Cost Semantics

grammar:
\[
\text{Cost } c ::= \begin{align*}
0 & \quad \text{zero cost} \\
1 & \quad \text{unit cost} \\
c_1 \otimes c_2 & \quad \text{parallel combination} \\
c_1 \oplus c_2 & \quad \text{sequential combination}
\end{align*}
\]

A cost graph is a form of *series-parallel* directed acyclic graph, with a designated *source* node and *sink* node. For 0 the graph consists of one node and no edges, with the source and sink both being the node itself. For 1 the graph consists of two nodes and one edge directed from the source to the sink. For \( c_1 \otimes c_2 \), if \( g_1 \) and \( g_2 \) are the graphs of \( c_1 \) and \( c_2 \), respectively, then the graph has two additional nodes, a source node with two edges to the source nodes of \( g_1 \) and \( g_2 \), and a sink node, with edges from the sink nodes of \( g_1 \) and \( g_2 \) to it. Finally, for \( c_1 \oplus c_2 \), where \( g_1 \) and \( g_2 \) are the graphs of \( c_1 \) and \( c_2 \), the graph has as source node the source of \( g_1 \), as sink node the sink of \( g_2 \), and an edge from the sink of \( g_1 \) to the source of \( g_2 \).

The intuition behind a cost graph is that nodes represent subcomputations of an overall computation, and edges represent *sequentiality constraints* stating that one computation depends on the result of another, and hence cannot be started before the one on which it depends completes. The product of two graphs represents *parallelism opportunities* in which there are no sequentiality constraints between the two computations. The assignment of source and sink nodes reflects the overhead of *forking* two parallel computations and *joining* them after they have both completed.

We associate with each cost graph two numeric measures, the *work*, \( \text{wk}(c) \), and the *depth*, \( \text{dp}(c) \). The work is defined by the following equations:

\[
\text{wk}(c) = \begin{cases} 
0 & \text{if } c = 0 \\
1 & \text{if } c = 1 \\
\text{wk}(c_1) + \text{wk}(c_2) & \text{if } c = c_1 \otimes c_2 \\
\text{wk}(c_1) + \text{wk}(c_2) & \text{if } c = c_1 \oplus c_2
\end{cases}
\] (41.4)

The depth is defined by the following equations:

\[
\text{dp}(c) = \begin{cases} 
0 & \text{if } c = 0 \\
1 & \text{if } c = 1 \\
\max(\text{dp}(c_1), \text{dp}(c_2)) & \text{if } c = c_1 \otimes c_2 \\
\text{dp}(c_1) + \text{dp}(c_2) & \text{if } c = c_1 \oplus c_2
\end{cases}
\] (41.5)
Informally, the work of a cost graph determines the total number of computation steps represented by the cost graph, and thus corresponds to the sequential complexity of the computation. The depth of the cost graph determines the critical path length, the length of the longest dependency chain within the computation, which imposes a lower bound on the parallel complexity of a computation. The critical path length is the least number of sequential steps that can be taken, even if we have unlimited parallelism available to us, because of steps that can be taken only after the completion of another.

In Chapter 12 we introduced cost semantics as a means of assigning time complexity to evaluation. The proof of Theorem 12.7 on page 96 shows that $e \Downarrow^k v$ iff $e \rightarrow^k v$. That is, the step complexity of an evaluation of $e$ to a value $v$ is just the number of transitions required to derive $e \rightarrow^* v$. Here we use cost graphs as the measure of complexity, then relate these cost graphs to the transition semantics given in Section 41.1 on page 382.

The judgement $e \Downarrow^c v$, where $e$ is a closed expression, $v$ is a closed value, and $c$ is a cost graph specifies the cost semantics. By definition we arrange that $e \Downarrow^0 v$ when $v$ val. The cost assignment for let is given by the following rule:

\[
\frac{e_1 \Downarrow^c_1 v_1 \quad e_2 \Downarrow^c_2 v_2 \quad [v_1, v_2/x_1, x_2]e \Downarrow^c v}{\text{letpar}(e_1; e_2; x_1.x_2.e) \Downarrow^{(c_1 \otimes c_2) \oplus 1 \oplus c} v}
\]  

(41.6)

The cost assignment specifies that, under ideal conditions, $e_1$ and $e_2$ are to be evaluated in parallel, and that their results are to be propagated to $e$. The cost of fork and join is implicit in the parallel combination of costs, and assign unit cost to the substitution because we expect it to be implemented in practice by a constant-time mechanism for updating an environment. The cost semantics of other language constructs is specified in a similar manner, using only sequential combination so as to isolate the source of parallelism to the let construct.

The link between the cost semantics and the transition semantics given in the preceding section is established by the following theorem, which states that the work cost is the sequential complexity, and the depth cost is the parallel complexity, of the computation.

**Theorem 41.4 (Work Efficiency).** If $e \Downarrow^c v$, then $e \rightarrow^w_{\text{seq}} v$ and $e \rightarrow^d_{\text{par}} v$, where $w = \text{wk}(c)$ and $d = \text{dp}(c)$. Conversely, if $e \rightarrow^w_{\text{seq}} v$ and $e \rightarrow^d_{\text{par}} v$, where $v$ val, then $e \Downarrow^c v$ for some cost graph $c$ such that $\text{wk}(c) = w$ and $\text{dp}(c) = d$.

**Proof.** The first part is proved by induction on the derivation of $e \Downarrow^c v$, the interesting case being Rule (41.6). By induction we have $e_1 \rightarrow^w_{\text{seq}} v_1$, 

generality, that d 
It follows from the form of e 
de 
Calculating e 
Calculating dp((c_1 \otimes c_2) \oplus 1 \oplus c) = max(d_1, d_2) + 1 + d completes the proof. 

Dec 18, 2009
then $e \downarrow^c v$, where $c = (c_1 \otimes c_2) \oplus 1 \oplus c_0$. Calculating, we obtain

$$dp(c) = \max(dp(c'_1) + 1, dp(c'_2) + 1) + 1 + dp(c_0) \quad (41.15)$$
$$= \max(dp(c'_1), dp(c'_2)) + 1 + 1 + dp(c_0) \quad (41.16)$$
$$= dp((c'_1 \otimes c'_2) \oplus 1 \oplus c_0) + 1 \quad (41.17)$$
$$= dp(c') + 1 \quad (41.18)$$
$$= d' + 1 \quad (41.19)$$
$$= d, \quad (41.20)$$

which completes the proof. \qed

Theorem 41.4 on page 386 implies that fork-join parallelism is work-efficient—the computations performed in any execution, sequential or parallel, are precisely those that must be performed according to the sequential semantics. This is in contrast to speculative parallelism, as discussed in Chapter 42, in which we may schedule a task for execution whose outcome is not needed to determine the overall result of the computation.

### 41.3 Multiple Fork-Join

So far we have confined attention to binary fork/join parallelism induced by the parallel let construct. While technically sufficient for many purposes, a more natural programming model admit an unbounded number of parallel tasks to be spawned simultaneously, rather than forcing them to be created by a cascade of binary forks and corresponding joins. Such a model, often called data parallelism, ties the source of parallelism to a data structure of unbounded size. The principal example of such a data structure is a vector of values of a specified type. The primitive operations on vectors provide a natural source of unbounded parallelism. For example, one may consider a parallel map construct that applies a given function to every element of a vector simultaneously, forming a vector of the results.

We will consider here a very simple language of vector operations to
41.3 Multiple Fork-Join

illustrate the main ideas.

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>( \tau )</td>
<td>( \tau \text{ vec} )</td>
<td>( \tau \text{ vec} )</td>
</tr>
<tr>
<td>Expr</td>
<td>( e )</td>
<td>( [e_0, \ldots, e_{n-1}] )</td>
<td>( [e_0, \ldots, e_{n-1}] )</td>
</tr>
<tr>
<td></td>
<td>( \text{sub}(e_1; e_2) )</td>
<td>( e_1[e_2] )</td>
<td>( e_1[e_2] )</td>
</tr>
<tr>
<td></td>
<td>( \text{rpl}(e_1; e_2) )</td>
<td>( \text{rpl}(e_1; e_2) )</td>
<td>( \text{rpl}(e_1; e_2) )</td>
</tr>
<tr>
<td></td>
<td>( \text{len}(e) )</td>
<td>( \text{len}(e) )</td>
<td>( \text{len}(e) )</td>
</tr>
<tr>
<td></td>
<td>( \text{idx}(e) )</td>
<td>( \text{idx}(e) )</td>
<td>( \text{idx}(e) )</td>
</tr>
<tr>
<td></td>
<td>( \text{map}(e_1; x. e_2) )</td>
<td>( &lt;e_2</td>
<td>x \in e_1&gt; )</td>
</tr>
<tr>
<td></td>
<td>( \text{cat}(e_1; e_2) )</td>
<td>( \text{cat}(e_1; e_2) )</td>
<td>( \text{cat}(e_1; e_2) )</td>
</tr>
</tbody>
</table>

The expression \( \text{vec}(e_0, \ldots, e_{n-1}) \) evaluates to an \( n \)-vector whose elements are given by the expressions \( e_0, \ldots, e_{n-1} \). The operation \( \text{sub}(e_1; e_2) \) retrieves the element of the vector given by \( e_1 \) at the index given by \( e_2 \). The operation \( \text{rpl}(e_1; e_2) \) creates a vector whose length is given by \( e_1 \) consisting solely of the element given by \( e_2 \). The operation \( \text{len}(e) \) returns the number of elements in the vector given by \( e \). The operation \( \text{idx}(e) \) creates a vector of length \( n \) (given by \( e \)) whose elements are 0, \ldots, \( n-1 \). The operation \( \text{map}(e_1; x. e_2) \) computes the vector whose \( i \)th element is the result of evaluating \( e_2 \) with \( x \) bound to the \( i \)th element of the vector given by \( e_1 \). The operation \( \text{cat}(e_1; e_2) \) concatenates two vectors of the same type.

The static semantics of these operations is given by the following typing rules:

\[
\begin{align*}
\Gamma \vdash e_0: \tau & \quad \ldots \quad \Gamma \vdash e_{n-1}: \tau \\
\Gamma \vdash \text{vec}(e_0, \ldots, e_{n-1}): \text{vec}(\tau) & \\
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash e_1: \text{vec}(\tau) & \quad \Gamma \vdash e_2: \text{nat} \\
\Gamma \vdash \text{sub}(e_1; e_2): \tau & \\
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash e_1: \text{nat} & \quad \Gamma \vdash e_2: \tau \\
\Gamma \vdash \text{rpl}(e_1; e_2): \text{vec}(\tau) & \\
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash e: \text{vec}(\tau) \\
\Gamma \vdash \text{len}(e): \text{nat} & \\
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash e: \text{nat} \\
\Gamma \vdash \text{idx}(e): \text{vec}(\text{nat}) & \\
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash e_1: \text{vec}(\tau) & \quad \Gamma, x: \tau \vdash e_2: \tau' \\
\Gamma \vdash \text{map}(e_1; x. e_2): \text{vec}(\tau') & \\
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash e_1: \text{vec}(\tau) & \quad \Gamma \vdash e_2: \text{vec}(\tau) \\
\Gamma \vdash \text{cat}(e_1; e_2): \text{vec}(\tau) & \\
\end{align*}
\]

December 18, 2009  DRAFT  14:36
The cost semantics of these primitives is given by the following rules:

\[
\begin{align*}
\text{vec}(e_0, \ldots, e_{n-1}) & \Downarrow \bigotimes_{i=0}^{n-1} c_i \text{ vec}(v_0, \ldots, v_{n-1}) \\
\text{vec}(v_0, \ldots, v_{n-1}) & \Downarrow c_0 v_0 & \ldots & e_{n-1} \Downarrow c_{n-1} v_{n-1} \\
\text{vec}(v_0, \ldots, v_{n-1}) & \Downarrow c_0 v_0 & \ldots & \text{vec}(v_0, \ldots, v_{n-1}) & \Downarrow & c_0 v_0 & \ldots & \text{vec}(v_0, \ldots, v_{n-1})
\end{align*}
\]

(41.22a)

\[
\begin{align*}
e_1 \Downarrow c_1 \text{ vec}(v_0, \ldots, v_{n-1}) & \quad e_2 \Downarrow c_2 \text{ num}[i] & \quad (0 \leq i < n) \\
\text{sub}(e_1; e_2) & \Downarrow c_1 \oplus c_2 v_i \\
\text{rpl}(e_1; e_2) & \Downarrow c_1 \oplus c_2 \text{ vec}(v_0, \ldots, v_{n-1})
\end{align*}
\]

(41.22b)

\[
\begin{align*}
e \Downarrow c_1 \text{ vec}(v_0, \ldots, v_{n-1}) & \quad \text{len}(e) \Downarrow c_1 \text{ num}[n] \\
\text{idx}(e) & \Downarrow c_1 \text{ num}[n] \\
\text{map}(e_1; x. e_2) & \Downarrow c_1 \bigotimes_{i=0}^{m+n-1} c_i \text{ vec}(v_0, \ldots, v_{m-1})
\end{align*}
\]

(41.22c)

(41.22d)

(41.22e)

(41.22f)

(41.22g)

The cost semantics for vector operations may be validated by introducing a sequential and parallel cost semantics and extending the proof of Theorem 41.4 on page 386 to cover this extension.

## 41.4 Provable Implementation

Theorem 41.4 on page 386 states that the cost semantics accurately models the dynamics of the parallel let construct, whether executed sequentially or in parallel. This validates the cost semantics from the point of view of the dynamics of the language, and permits us to draw conclusions about the asymptotic complexity of a parallel program that abstracts away from the limitations imposed by a concrete implementation. Chief among these is the restriction to a fixed number, \( p > 0 \), of processors on which to schedule the workload. In addition to limiting the available parallelism this also imposes some synchronization overhead that must be accounted for in order
41.4 Provable Implementation

to make accurate predictions of run-time behavior on a concrete parallel platform. A provable implementation is one for which we may establish an asymptotic bound on the actual execution time once these overheads are taken into account.

For the purposes of this chapter, we define a symmetric multiprocessor, or SMP, to be a shared-memory multiprocessor with an interconnection network that implements a synchronization construct equivalent to a parallel-fetch-and-add instruction in which any number of processors may simultaneously add a value to a shared memory location, retrieving the previous contents, while ensuring that each processor obtains the result it would obtain in some sequential ordering of their execution. Most multiprocessors implement an instruction of expressive power equivalent to the fetch-and-add to provide a foundation for parallel programming. In the following analysis we assume that the fetch-and-add instruction takes constant time, but the result can be adjusted (as noted below) to account for the overhead of implementing it under more relaxed assumptions about the processor network.

The main result relating the abstract cost to its concrete realization on a p-processor SMP is an application of Brent’s Principle, which describes how to implement arithmetic expressions on a parallel processor.

**Theorem 41.5.** If \( e \downarrow^c v \) with \( wk(c) = w \) and \( dp(c) = d \), then \( e \) may be evaluated on a p-processor SMP in time \( O(\max(w/p, d)) \).

Since the work always dominates the depth, if \( p = 1 \), then the theorem reduces to the statement that \( e \) may be evaluated in time \( O(w) \), the sequential complexity of the expression. That is, the work cost is asymptotically realizable on a single processor machine. For the general case the theorem tells us that we can never evaluate \( e \) in fewer steps than its depth cost, since this is the critical path length, and, for computations with shallow depth, we can achieve the best-possible result of dividing up the work evenly among the \( p \) processors.

Theorem 41.5 suggests a characterization of those problems for which having a great degree of parallelism (more processing elements) improves the running time. For a computation of depth \( d \) and work \( w \), we can make good use of parallelism whenever \( w/p > d \), which occurs when the parallelizability ratio, \( w/d \), is at least \( p \). In a highly sequential program the work is directly proportional to the depth, and so the parallelizability is constant. This implies that increasing \( p \) does not speed up the computation. On the other hand, a highly parallelizable computation is one with constant depth,
or depth $d$ proportional to $\log w$. Such programs have a high parallelizability ratio, and hence are amenable to speedup by increasing the number of available processors. It is worth stressing that it is not known whether all problems admit a parallelizable solution or not. The best we can say, on present knowledge, is that there are algorithms for some problems that have a high degree of parallelizability, and there are problems for which no such algorithm is known. It is an important open problem in complexity theory to characterize which problems are parallelizable, and which are not.

The proof of Theorem 41.5 on the previous page amounts to a design for the implementation of binary nested parallelism. A critical ingredient is scheduling the workload onto the $p$ processors so as to maximize their utilization. This is achieved by maintaining a shared worklist of tasks that have been created by evaluation of a parallel $\text{let}$ construct, all of which must be completed to determine the final outcome of the computation. (Here we make use of shared memory so that all processors have access to the central worklist.) Execution is divided into rounds. At the end of each round a processor may complete execution, in which case further work can be scheduled onto it; it may continue execution into the next round; or it may fork two additional tasks to be scheduled for execution, blocking until they complete.

To start the next round the processors must collectively assign work to themselves so that if sufficient work is available, then all $p$ processors will be assigned work. Assume that we have at least $p$ units of work remaining to be done at any given time (otherwise just consider all remaining work in what follows). Each step of execution on each processor consists of executing an instruction of the language. After this step a task may either be complete, or may continue with further execution, or may fork two new tasks as a result of executing a parallel $\text{let}$ instruction, or it may join two completed tasks into one. The synchronization required for a join may be implemented on an SMP by allocating a data structure to each (dynamic) join point, and arranging that the parallel threads signal their completion by atomically posting their result to this data structure. The first thread to complete stores its result in this data structure (atomically, to avoid race conditions). When the second thread completes, it continues from the join point, passing along its own result and that of the first thread to complete.

Theorem 41.5 on the preceding page may also be extended to the vector operations discussed in Section 41.3 on page 388. The proof requires that we specify an algorithm to implement each of the operations in the time
bounds specified by the cost semantics in accordance with the theorem.

To get an idea of what is involved, let us consider how to implement the operation $\text{id}(e)$ on a $p$-processor SMP. We wish to show, consistently with Theorem 41.5 on page 391, that this operation may be implemented in time $O(\max(n/p, 1))$, where $e$ evaluates to $n$. This may be achieved as follows. First, reserve, in constant time, an uninitialized region of $n$ words of memory for the vector to be created by this operation. To initialize this memory, we assign responsibility for a segment of size $n/p$ to each of the $p$ processors, which then execute in parallel to fill in the required values. To do this we must assign to processor $i$ the starting point, $n_i$, of the $i$th segment. The starting points are calculated by constructing, in constant time, the vector of numbers $0, \ldots, p-1$, each of which is then multiplied by $n/p$ to obtain the required vector $n_0, \ldots, n_{p-1}$. Processor $i$ will then initialize the segment starting at $n_i$ to the numbers $n_i, n_i + 1, \ldots, n_i + (n/p) - 1$. Each processor required $O(n/p)$ to perform this, and all processors may execute in parallel without further coordination, achieving the required bound. Note that had we specified, say, a unit cost for the index operation, we would have been unable to extend the proof of Theorem 41.5 on page 391, because it is not possible to write the required $O(n)$ data items in $O(1)$ time.

### 41.5 Exercises
Chapter 42

Futures and Speculation

A future is a computation whose evaluation is initiated in advance of any demand for its value. Like a suspension, a future represents a value that is to be determined later. Unlike a suspension, a future is always evaluated, regardless of whether its value is actually required. In a sequential setting futures are of no interest; a future of type $\tau$ is just an expression of type $\tau$. Lacking parallelism, the future must be fully evaluated immediately, regardless of whether its value is ultimately required in the subsequent computation. In the presence of parallelism, however, futures provide the ability to schedule a computation to be executed simultaneously with its continuation until such time as the continuation actually requires the value of the future, at which point further progress is stopped until the computation of the future has been completed.

Futures are useful for expressing pipelined computations—multistage computations in which subsequent stages start executing before previous stages have completed so as to minimize latency. Of course once one stage requires the result of a previous stage, it must synchronize with the earlier stage before proceeding. Ideally, the work of the previous stage is completed by the time that the later stage requires it. If not, there is a stall while the later stage waits for the outcome of the earlier.

Speculation is a parallel semantics for suspensions in which suspended computations are executed in parallel with the main thread of computation without regard to whether the suspension is forced. If the value of the suspension is eventually required, then speculation pays off, but if not, the effort to evaluate it wasted. Speculation is therefore not work-efficient: if the value of the suspension is never needed, more work has been undertaken than is necessary to determine the outcome of the computation. Specu-
Futures can be useful in situations where there is an excess of computing resources available, more than can be used in a guaranteed work-efficient manner. In such situations it cannot hurt to perform extra work as long as resources are used that would otherwise be idle.\(^1\)

### 42.1 Futures

The syntax of futures is given by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>(\tau)</td>
<td>fut((\tau))</td>
<td>(\tau) fut</td>
</tr>
<tr>
<td>Expr</td>
<td>(e)</td>
<td>fut((e))</td>
<td>fut((e))</td>
</tr>
<tr>
<td></td>
<td></td>
<td>syn((e))</td>
<td>syn((e))</td>
</tr>
<tr>
<td></td>
<td></td>
<td>fut[(a)]</td>
<td>fut[(a)]</td>
</tr>
</tbody>
</table>

The type \(\tau\) fut is the type of futures of type \(\tau\). Futures are introduced by the expression \(\text{fut}(e)\), which schedules \(e\) for evaluation and returns a reference to it. References to futures have the form \(\text{fut}[a]\), where \(a\) is a symbol serving as the name of the future. Futures are eliminated by the expression \(\text{syn}(e)\), which synchronizes with the future referred to by \(e\), returning its value. Evaluation of the synchronizing expression cannot proceed until evaluation of the future has completed.

### 42.1.1 Statics

The static semantics of futures comprises the following rules:

\[
\frac{\Gamma \vdash e : \tau}{\Gamma \vdash \text{fut}(e) : \text{fut}(\tau)} \quad (42.1a)
\]
\[
\frac{\Gamma \vdash e : \text{fut}(\tau)}{\Gamma \vdash \text{syn}(e) : \tau} \quad (42.1b)
\]
\[
\frac{\Gamma \vdash \Sigma, a : \tau \ \text{fut}[a] : \text{fut}(\tau)}{} \quad (42.1c)
\]

\(^1\)Actually, the situation is more subtle than that, because speculative executions introduce contention for shared resources, such as memory, that can impede the progress of non-speculative computations.
42.1 Futures

42.1.2 Dynamics

The sequential dynamics of futures is trivial. Futures are evaluated eagerly, and their value is returned when synchronized; references are not needed.

\[
\begin{align*}
\text{\( e \)} & \text{ val} \\
\text{fut}(e) & \text{ val} \\
\hline
\end{align*}
\]

\[\frac{e \mapsto e'}{\text{fut}(e) \mapsto \text{fut}(e')}\quad (42.2a)\]

\[\frac{e \mapsto e'}{\text{syn}(e) \mapsto \text{syn}(e')}\quad (42.2c)\]

\[\frac{e \text{ val}}{\text{syn}(\text{fut}(e)) \mapsto e}\quad (42.2d)\]

The parallel dynamics of futures relies on an explicit allocation of tasks to be executed simultaneously. A state of the parallel dynamics has the form \( v \Sigma \{ e \parallel \mu \} \) in which \( \Sigma \) declares the names and types of the active futures, \( \mu \) assigns an expression to each future declared in \( \Sigma \), and \( e \) is an expression possibly involving the names declared in \( \Sigma \). We sometimes describe the expression \( e \) as being the focus of evaluation. It represents the flow of control specified by the sequential semantics of execution that must, from time to time, synchronize with the futures executing in parallel with it.

The initial and final states are defined by the following rules:

\[\frac{\text{\( \mu \)} \text{ val}_\Sigma}{\frac{\forall a \in \text{dom}(\mu)}{\mu(a) \text{ val}_\Sigma}}\quad (42.3b)\]

\[\frac{\text{\( \nu \)} \otimes \{ e \parallel \otimes \} \text{ initial}}{\text{\( e \)} \text{ val}_\Sigma \quad \mu \text{ val}_\Sigma}{\frac{\nu \Sigma \{ e \parallel \mu \} \text{ final}}}{\frac{\nu \Sigma \{ e \parallel \mu \} \text{ final}}}{\frac{\nu \Sigma \{ e \parallel \mu \} \text{ final}}}{(42.3d)}\]

In the initial state no futures are active, and the focus, \( e \), is any closed expression. In a final state the focus, \( e \), is a value, and all of the active futures have been fully evaluated.
The dynamic semantics of futures is divided into two phases, the *local* phase, which defines the basic steps of evaluation of an expression, and the *global* phase, which executes all possible local steps in parallel.

The local transition judgement

\[
\nu \Sigma \{ e \parallel \mu \} \xrightarrow{\text{local}} \nu \Sigma' \{ e' \parallel \mu' \}
\]

is defined by the following rules:

\begin{align*}
\frac{e \text{ val}_\Sigma}{\nu \Sigma \{ e \parallel \mu \} \xrightarrow{\text{local}} \nu \Sigma \{ e \parallel \mu \}} & \quad (42.4a) \\
\frac{\nu \Sigma \{ \text{fut}(e) \parallel \mu \} \xrightarrow{\text{local}} \nu \Sigma, a : \tau \{ \text{fut}[a] \parallel \mu \otimes \langle a : e' \rangle \}}{\nu \Sigma \{ e \parallel \mu \} \xrightarrow{\text{local}} \nu \Sigma' \{ e' \parallel \mu' \}} & \quad (42.4b) \\
\frac{\nu \Sigma \{ \text{syn}(e) \parallel \mu \} \xrightarrow{\text{local}} \nu \Sigma' \{ \text{syn}(e') \parallel \mu' \}}{\nu \Sigma \{ e \parallel \mu \} \xrightarrow{\text{local}} \nu \Sigma' \{ e' \parallel \mu' \}} & \quad (42.4c) \\
\frac{\nu \Sigma, a : \tau \{ \text{syn} \langle \text{fut}[a] \rangle \parallel \mu \otimes \langle a : e' \rangle \}}{\nu \Sigma, a : \tau \{ e' \parallel \mu \otimes \langle a : e' \rangle \}} & \quad (42.4d)
\end{align*}

Rule (42.4a) states that a value transitions to itself.\(^2\) Rule (42.4b) activates a future named \(a\) executing the expression \(e\) and returns a reference to it. Rule (42.4d) synchronizes with a future whose value has been determined.

It is easy to check that each local transition has the form

\[
\nu \Sigma \{ e \parallel \mu \} \xrightarrow{\text{local}} \nu \Sigma \Sigma' \{ e' \parallel \mu \otimes \mu' \}
\]

where \(\Sigma'\) is either empty or declares the type of a single symbol, and \(\mu'\) is either empty or of the form \(\langle a : e' \rangle\) for some expression \(e'\). That is, each local step of evaluation can have one of three outcomes:

1. The result state is a value. Evaluation of that expression is complete.

2. The result state is another expression. Evaluation will continue on that expression in the next round.

\(^2\)This unusual rule is a technical device used to facilitate the definition of the global transition judgement.
3. The transition allocates a new future, and yields a reference to it. Another expression is available for execution on the next round.

The third possibility is the one that complicates matters, because it requires coordination with the other steps of execution to combine the individual result states into a single next state of execution.

We may now specify the global transition judgement. Intuitively, each global step consists of one local step of evaluation of the focal expression and one local step of evaluation on each of the futures, provided that in each case the expression in question is not yet a value. Thus each global step corresponds to one step of an idealized parallel computer that admits as many simultaneous steps of execution as we may desire. This idealized form of parallelism provides the basis for an abstract cost semantics that is independent of the limitations of the computing fabric on which the program is to be run. These limitations may be factored in to obtain a concrete cost semantics for an expression as a function of its abstract cost and certain parameters, such as the number of processors, that characterize the computing platform.

\[ \mu = \langle a_1 : e_1 \rangle \otimes \cdots \otimes \langle a_n : e_n \rangle \]

\[ v \Sigma \{ e \parallel \mu \} \xrightarrow{\text{local}} v \Sigma \Sigma^\prime \{ e' \parallel \mu \otimes \mu' \} \]

\[ (\forall 1 \leq i \leq n) \quad v \Sigma \{ e_i \parallel \mu \} \xrightarrow{\text{local}} v \Sigma \Sigma_i^\prime \{ e_i' \parallel \mu \otimes \mu_i' \} \]

\[ \left\{ \begin{array}{c} v \Sigma \{ e \parallel \mu \} \\ v \Sigma \Sigma_i^\prime \ldots \Sigma_n^\prime \{ e' \parallel \mu \otimes \mu_i' \otimes \cdots \otimes \mu_n' \} \end{array} \right\} \]

(42.5a)

The futures allocated by the local steps of execution are consolidated in the result of the global step. We assume without loss of generality that the names of the new futures in each local step are pairwise disjoint so that the combination makes sense.

Satisfying this disjointness assumption represents a significant complication for an implementation of futures. It implies that the local steps must be synchronized when allocating new futures to ensure that the same name is not used for two different futures. This requirement, together with the synchronization implied by Rule (42.4d), are the only forms of synchronization involved in the implementation of futures.
42.2 Speculation

We will consider speculation as an evaluation strategy for suspensions, which were introduced in Chapter 39. The syntax and static semantics of suspensions is as described therein, but the dynamics differs in that we may evaluate a suspended computation at will, without regard to whether its value is needed to make progress on the focus of evaluation.

As with futures, we divide the dynamics into two phases, the local and the global phase. The initial and final states are defined by the following rules:

\[ \text{susp}[a] \text{ val}_{\Sigma,a: \tau} \] (42.6a)

\[ \nu \emptyset \{ e \parallel \emptyset \} \text{ initial} \] (42.6b)

\[ e \text{ val}_{\Sigma} \]

\[ \nu \Sigma \{ e \parallel \mu \} \text{ final} \] (42.6c)

The difference compared to futures is that a state is final when the focus is a value, regardless of whether all active suspensions have been evaluated or not.

The local phase consists of Rules (39.8), minus Rule (39.8e). We repeat these rules here for the sake of convenient reference, restricting attention to non-recursive suspensions for the sake of simplicity:

\[ \nu \Sigma \{ \text{susp}(e) \parallel \mu \} \xrightarrow{\text{local}} \nu \Sigma, a : \tau \{ \text{susp}[a] \parallel \mu \otimes \langle a : e \rangle \} \] (42.7a)

\[ \nu \Sigma \{ e \parallel \mu \} \xrightarrow{\text{local}} \nu \Sigma' \{ e' \parallel \mu' \} \]

\[ \nu \Sigma \{ \text{force}(e) \parallel \mu \} \xrightarrow{\text{local}} \nu \Sigma' \{ \text{force}(e') \parallel \mu' \} \]

\[ e' \text{ val}_{\Sigma,a: \tau} \]

\[ \left\{ \nu \Sigma, a : \tau \{ \text{force(susp}[a]) \parallel \mu \otimes \langle a : e' \rangle \} \right\} \xrightarrow{\text{local}} \nu \Sigma, a : \tau \{ e' \parallel \mu \otimes \langle a : e' \rangle \} \] (42.7c)

Rules (42.7a) to (42.7c) are essentially identical to Rules (42.4b) to (42.4d). The difference between futures and speculation lies in the global transition judgement, which determines the parallel execution strategy.
The global phase consists of choosing some number of suspensions to evaluate speculatively, as described by the following rule:

\[
\mu = \mu_0 \otimes \langle a_1 : e_1 \rangle \otimes \cdots \otimes \langle a_n : e_n \rangle
\]

\[
\nu \Sigma \{ e \parallel \mu \} \xrightarrow{local} \nu \Sigma \Sigma' \{ e' \parallel \mu \otimes \mu' \}
\]

\[
(\forall 1 \leq i \leq n) \quad \nu \Sigma \{ e_i \parallel \mu \} \xrightarrow{local} \nu \Sigma \Sigma'_i \{ e'_i \parallel \mu \otimes \mu'_i \}
\]

\[
\left\{ \begin{array}{l} 
\nu \Sigma \{ e \parallel \mu \} \\
\nu \Sigma \Sigma'_1 \Sigma'_2 \cdots \Sigma'_n \{ e' \parallel \mu \otimes \mu'_0 \otimes \mu'_1 \otimes \cdots \otimes \mu'_n \} 
\end{array} \right. \tag{42.8a}
\]

Rule (42.8a) is similar to Rule (42.5a), with these differences:

1. We may choose at each step to take a step of execution on any suspension for which a (non-idle) local transition is possible. In contrast to futures there is no requirement that we do so for all suspensions on which progress is possible.

2. We demand that progress be made on the focus of evaluation at each step, because the computation is complete when it achieves a value, regardless of whether all suspensions have been fully evaluated or not.

As with futures, we assume that the suspension names generated by each local step (\(\Sigma'_1\) and \(\Sigma'_2, \ldots, \Sigma'_n\)) are pairwise disjoint to ensure that the overall result step, which combines these names, is well-defined. In implementation terms this amounts to the synchronization of the parallel computations on the allocation of suspension names.

### 42.3 Exercises
Part XVI

Concurrency
Chapter 43

Process Calculus

So far we have mainly studied the static and dynamic semantics of programs in isolation, without regard to their interaction with the world. But to extend this analysis to even the most rudimentary forms of input and output requires that we consider external agents that interact with the program. After all, the whole purpose of a computer is to interact with a person!

To extend our investigations to interactive systems, we begin with the study of process calculi, which are abstract formalisms that capture the essence of interaction among independent agents. There are many forms of process calculi, differing in technical details and in emphasis. We will consider the best-known formalism, which is called the π-calculus. The development will proceed in stages, starting with simple action models, then extending to interacting concurrent processes, and finally to the synchronous and asynchronous variants of the π-calculus itself.

Our presentation of the π-calculus differs from that in the literature in several respects. Most significantly, we maintain a distinction between processes and events. The basic form of process is one that awaits a choice of events. Other forms of process include parallel composition, the introduction of a communication channel, and, in the asynchronous case, a send on a channel. The basic form of event is the ability to read (and, in the synchronous case, write) on a channel. Events are combined by a non-deterministic choice operator. Even the choice operator can be eliminated in favor of a protocol for treating a parallel composition of events as a non-deterministic choice among them.
43.1 Actions and Events

Our treatment of concurrent interaction is based on the notion of an event, which specifies the set of actions that a process is prepared to undertake in concert with another process. Two processes interact by undertaking two complementary actions, which may be thought of as a read and a write on a common channel. The processes synchronize on these complementary actions, after which they may proceed independently to interact with other processes.

To begin with we will focus on sequential processes, which simply await the arrival of one of several possible actions, known as an event.

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>$P$</td>
<td>$\text{await}(E)$</td>
<td>$E$</td>
</tr>
<tr>
<td>Event</td>
<td>$E$</td>
<td>$\text{null}$</td>
<td>$0$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{choice}(E_1;E_2)$</td>
<td>$E_1 + E_2$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{rcv}<a href="P">a</a>$</td>
<td>$?a . P$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{snd}<a href="P">a</a>$</td>
<td>!$a . P$</td>
</tr>
</tbody>
</table>

The variables $a$, $b$, and $c$ range over channels, which serve as synchronization sites between processes.

We will handle events modulo structural congruence, written $P_1 \equiv P_2$ and $E_1 \equiv E_2$, respectively, which is the strongest equivalence relation closed under the following rules:

\[
\frac{E \equiv E'}{\$E \equiv \$E'} \quad (43.1a)
\]
\[
\frac{E_1 \equiv E_1' \quad E_2 \equiv E_2'}{E_1 + E_2 \equiv E_1' + E_2'} \quad (43.1b)
\]
\[
\frac{P \equiv P'}{?a . P \equiv ?a . P'} \quad (43.1c)
\]
\[
\frac{P \equiv P'}{!a . P \equiv !a . P'} \quad (43.1d)
\]
\[
\frac{}{E + 0 \equiv E} \quad (43.1e)
\]
\[
\frac{}{E_1 + E_2 \equiv E_2 + E_1} \quad (43.1f)
\]
\[
\frac{}{E_1 + (E_2 + E_3) \equiv (E_1 + E_2) + E_3} \quad (43.1g)
\]
The importance of imposing structural congruence on sequential processes is that it enables us to think of an event as having the form of a finite sum of send or receive events, with the sum of zero events being the null event, 0.

An illustrative example of Robin Milner’s is a simple vending machine that may take in a 2p coin, then optionally either permit selection of a cup of tea, or take another 2p coin, then permit selection of a cup of coffee.

\[ V = \$ (?2p.\!(\text{tea}.V + ?2p.\!(\text{cof}.V))) \]

As the example indicates, we tacitly permit recursive definitions of processes, with the understanding that a defined identifier may always be replaced with its definition wherever it occurs.

Because the computation occurring within a process is suppressed, sequential processes have no dynamics on their own, but only through their interaction with other processes. For the vending machine to operate there must be another process (you!) who initiates the events expected by the machine, causing both your state (the coins in your pocket) and its state (as just described) to change as a result.

### 43.2 Concurrent Interaction

We enrich the language of processes with concurrent composition.

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>(P)</td>
<td>\text{await}(E) \quad $ E \quad \text{stop} \quad \text{1} \quad \text{par}(P_1; P_2) \quad P_1 \parallel P_2</td>
<td></td>
</tr>
</tbody>
</table>

The process \text{1} represents the inert process, and the process \(P_1 \parallel P_2\) represents the concurrent composition of \(P_1\) and \(P_2\). One may identify \text{1} with \$0, the process that awaits the event that will never occur, but we prefer to treat the inert process as a primitive concept.

Structural congruence for processes is enriched by the following rules governing the inert process and concurrent composition of processes:

\[
P \parallel \text{1} \equiv P \quad \text{(43.2a)}
\]

\[
P_1 \parallel P_2 \equiv P_2 \parallel P_1 \quad \text{(43.2b)}
\]
43.2 Concurrent Interaction

\[ P_1 \parallel (P_2 \parallel P_3) \equiv (P_1 \parallel P_2) \parallel P_3 \]  
(43.2c)

\[ P_1 \equiv P'_1 \quad P_2 \equiv P'_2 \]
\[ P_1 \parallel P_2 \equiv P'_1 \parallel P'_2 \]  
(43.2d)

Up to structural equivalence every process has the form

\[ \$ E_1 \parallel \ldots \parallel \$ E_n \]

for some \( n \geq 0 \), it being understood that when \( n = 0 \) this is the process \( 1 \).

The dynamic semantics of concurrent interaction is defined by an action-indexed family of transition judgements, \( P \xmapsto{\alpha} P' \), where \( \alpha \) is an action as specified by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>( \alpha )</td>
<td>( \box{rcv}[a] )</td>
<td>( ?a )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( \box{snd}[a] )</td>
<td>( !a )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sil</td>
<td>( \epsilon )</td>
</tr>
</tbody>
</table>

The action label on a transition specifies the effect of an execution step on the environment in which it occurs. The receive action, \( ?a \), and the send action, \( !a \), are complementary. Two concurrent processes may interact whenever they announce complementary actions, resulting in a silent transition, which is labelled by the silent action, \( \text{sil} \).

\[ P_1 \equiv P'_1 \quad P'_1 \xmapsto{\alpha} P'_2 \quad P'_2 \equiv P_2 \]
\[ P_1 \xmapsto{\alpha} P_2 \]  
(43.3a)

\[ \$ (\!a \cdot P + E) \xmapsto{\!a} P \]  
(43.3b)

\[ \$ (\?a \cdot P + E) \xmapsto{\?a} P \]  
(43.3c)

\[ P_1 \parallel P_2 \xmapsto{\alpha} P'_1 \parallel P'_2 \]
\[ P_1 \xmapsto{\alpha} P'_1 \]  
(43.3d)

\[ P_1 \xmapsto{!a} P'_1 \quad P_2 \xmapsto{?a} P'_2 \]
\[ P_1 \parallel P_2 \xmapsto{\alpha} P'_1 \parallel P'_2 \]  
(43.3e)
43.3 Replication

Rules (43.3b) and (43.3c) specify that any of the events on which a process is synchronizing may occur. Rule (43.3e) synchronizes two processes that take complementary actions.

As an example, let us consider the interaction of the vending machine, \( V \), with the user process, \( U \), defined as follows:

\[
\]

Here is a trace of the interaction between \( V \) and \( U \):

\[
V \parallel U \rightarrow \rightarrow !tea. V + ?2p. !cof. V \parallel !2p. !cof. 1
\]

\[
\rightarrow !cof. V \parallel !cof. 1
\]

\[
\rightarrow V
\]

These steps are justified, respectively, by the following pairs of labelled transitions:

\[
U \stackrel{!2p}{\rightarrow} U' = !2p. ?cof. 1
\]

\[
V \stackrel{?2p}{\rightarrow} V' = (!tea. V + ?2p. !cof. V)
\]

\[
U' \stackrel{!2p}{\rightarrow} U'' = ?cof. 1
\]

\[
V' \stackrel{?2p}{\rightarrow} V'' = !cof. V
\]

\[
U'' \stackrel{?cof}{\rightarrow} 1
\]

\[
V'' \stackrel{!cof}{\rightarrow} V
\]

We have suppressed uses of structural congruence in the above derivations to avoid clutter, but it is important to see its role in managing the non-deterministic choice of events by a process.

43.3 Replication

Some presentations of process calculus forego reliance on defining equations for processes in favor of a replication construct, which we write \( *P \). This process stands for as many concurrently executing copies of \( P \) as one may require, which may be modeled by the structural congruence

\[
*P \equiv P \parallel *P.
\]
Taking this as a principle of structural congruence hides the overhead of process creation, and gives no hint as to how often it can or should be applied. One could alternatively build replication into the dynamic semantics to model the details of replication more closely:

\[ \star P \rightarrow P \parallel \star P. \]

Since the application of this rule is unconstrained, it may be applied at any time to effect a new copy of the replicated process \( P \).

So far we have been using recursive process definitions to define processes that interact repeatedly according to some protocol. Rather than take recursive definition as a primitive notion, we may instead use replication to model repetition. This may be achieved by introducing an “activator” process that is contacted to effect the replication. Consider the recursive definition \( X = P(X) \), where \( P \) is a process expression involving occurrences of the process variable, \( X \), to refer to itself. This may be simulated by defining the activator process

\[ A = \star \$(\ ?a.\ 1) \], \]

in which we have replaced occurrences of \( X \) within \( P \) by an initiator process that signals the event \( a \) to the activator. Observe that the activator, \( A \), is structurally congruent to the process \( A' \parallel A \), where \( A' \) is the process

\[ \$(\ ?a.\ 1) \]. \]

To start process \( P \) we concurrently compose the activator, \( A \), with an initiator process, \( \$(\ !a.\ 1) \). Observe that

\[ A \parallel \$(\ !a.\ 1) \rightarrow A \parallel P(\ !a.\ 1), \]

which starts the process \( P \) while maintaining a running copy of the activator, \( A \).

As an example, let us consider Milner’s vending machine written using replication, rather than using recursive process definition:

\[ V_1 = \star \$(\ ?v.\ V_2) \]
\[ V_2 = \$(\ ?2p.\ $(\ !tea.\ V_0 + ?2p.\ $(\ !cof.\ V_0))) \]
\[ V_0 = \$(\ !v.\ 1) \]

The process \( V_1 \) is a replicated server that awaits a signal on channel \( v \) to create another instance of the vending machine. The recursive calls are replaced by signals along \( v \) to re-start the machine. The original machine, \( V \), is simulated by the concurrent composition \( V_0 \parallel V_1 \).
43.4 Private Channels

It is often desirable to isolate interactions among a group of concurrent processes from those among another group of processes. This can be achieved by creating a private channel that is shared among those in the group, and which is inaccessible from all other processes. This may be modeled by enriching the language of processes with a construct for creating a new channel:

\[
\begin{array}{llll}
\text{Category} & \text{Item} & \text{Abstract} & \text{Concrete} \\
\hline
\text{Process} & P & ::= & \text{new}(a.P) \\
\hline
\end{array}
\]

As the syntax suggests, this is a binding operator in which the channel \(a\) is bound within \(P\).

Structural congruence is extended with the following rules:

\[
\frac{P =_a P'}{P \equiv P'} \quad (43.7a)
\]

\[
\frac{P \equiv P'}{\nu(a.P) \equiv \nu(a.P')} \quad (43.7b)
\]

\[
\frac{a \notin P_2}{\nu(a.P_1) \parallel P_2 \equiv v(a.P_1 \parallel P_2)} \quad (43.7c)
\]

The last rule, called \textit{scope extrusion}, is not strictly necessary at this stage, but will be important in the treatment of communication in the next section.

The dynamic semantics is extended with one additional rule permitting steps to take place within the scope of a binder.

\[
\frac{P \xrightarrow{a} P'}{\nu(a.P) \xrightarrow{a} v(a.P')} \quad (43.8)
\]

No process may interact with \(\nu(a.P)\) along the newly-allocated channel, for to do so would require knowledge of the private channel, \(a\), which is chosen, by the magic of \(a\)-equivalence, to be distinct from all other channels in the system.

As an example, let us consider again the non-recursive definition of the vending machine. The channel, \(v\), used to initialize the machine should be considered private to the machine itself, and not be made available to a user process. This is naturally expressed by the process expression \(\nu(v.V_0 \parallel V_1)\), where \(V_0\) and \(V_1\) are as defined above using the designated channel, \(v\). This process correctly simulates the original machine, \(V\), because it precludes
interaction with a user process on channel \( v \). If \( U \) is a user process, the interaction begins as follows:

\[
v(v.V_0 \parallel V_1) \parallel U \mapsto v(v.V_2) \parallel U \equiv v(v.V_2 \parallel U)
\]

The interaction continues as before, albeit within the scope of the binder, provided that \( v \) has been chosen (by structural congruence) to be apart from \( U \), ensuring that it is private to the internal workings of the machine.

### 43.5 Synchronous Communication

The concurrent process calculus presented in the preceding section models synchronization based on the willingness of two processes to undertake complementary actions. A natural extension of this model is to permit data to be passed from one process to another as part of synchronization. Since we are abstracting away from the computation occurring within a process, it would not make much sense to consider, say, passing an integer during synchronization. A more interesting possibility is to permit passing channels, so that new patterns of connectivity can be established as a consequence of inter-process synchronization. This is the core idea of the \( \pi \)-calculus.

The syntax of events is changed to account for communication by generalizing send and receive events as specified in the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event</td>
<td>( E )</td>
<td>( \mathit{rcv}<a href="x.P">a</a> )</td>
<td>( ?a(x).P )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( \mathit{snd}<a href="P">a;b</a> )</td>
<td>( !a(b).P )</td>
</tr>
</tbody>
</table>

The event \( ?a(x).P \) binds the variable \( x \) within the process expression \( P \). The rest of the syntax remains as described earlier in this chapter.

The syntax of actions is generalized along similar lines, with both the send and receive actions specifying the data communicated by the action.

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>( a )</td>
<td>( \mathit{rcv}<a href="b">a</a> )</td>
<td>( ?a(b) )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( \mathit{snd}<a href="b">a</a> )</td>
<td>( !a(b) )</td>
</tr>
</tbody>
</table>

The action \( !a(b) \) represents a write, or send, of a channel, \( b \), along a channel, \( a \). The action \( ?a(b) \) represents a read, or receive, along channel, \( a \), of another channel, \( b \).
Interaction in the $\pi$-calculus consists of synchronization on the concurrent availability of complementary actions on a channel, passing a channel from the sender to the receiver.

\[
\$ (!a(b) . P + E) \xrightarrow{!a(b)} P \quad (43.9a)
\]

\[
\$ (?a(x) . P + E) \xrightarrow{?a(b)} [b/x]P \quad (43.9b)
\]

\[
\frac{P_1 \xrightarrow{!a(b)} P_1' \quad P_2 \xrightarrow{?a(b)} P_2'}{P_1 \parallel P_2 \xrightarrow{} P_1' \parallel P_2'} \quad (43.9c)
\]

In contrast to pure synchronization the message-passing form of interaction is fundamentally asymmetric — the receiver continues with the channel passed by the sender substituted for the bound variable of the action. Rule (43.9b) may be seen as “guessing” that the received data will be $b$, which is substituted into the resulting process.

### 43.6 Polyadic Communication

So far communication is limited to sending and receiving a single channel along another channel. It is often useful to consider more flexible forms of communication in which zero or more channels are communicated by a single interaction. Transmitting no data corresponds to a pure signal on a channel in which the mere fact of the communication is all that is transmitted between the sender and the receiver. Transmitting more than one channel corresponds to a packet in which a single interaction communicates a finite number of channels from sender to receiver.

The polyadic $\pi$-calculus is the generalization of the $\pi$-calculus to admit communication of multiple channels between sender and receiver in a single interaction. The syntax of the polyadic $\pi$-calculus is a simple extension of the monadic $\pi$-calculus in which send and receive events, and their corresponding actions, are generalized as follows:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event $E$</td>
<td>$rcv[a] (x_1, \ldots, x_k . P)$</td>
<td>$?a(x_1, \ldots, x_k) . P$</td>
<td>$a(b_1, \ldots, b_k) . P$</td>
</tr>
<tr>
<td></td>
<td>$snd[a; b_1, \ldots, b_k] (P)$</td>
<td>$!a(b_1, \ldots, b_k)$</td>
<td>$?a(b_1, \ldots, b_k)$</td>
</tr>
<tr>
<td>Action $a$</td>
<td>$rcv[a] (b_1, \ldots, b_k)$</td>
<td>$?a(b_1, \ldots, b_k)$</td>
<td>$a(b_1, \ldots, b_k)$</td>
</tr>
<tr>
<td></td>
<td>$snd[a] (b_1, \ldots, b_k)$</td>
<td>$!a(b_1, \ldots, b_k)$</td>
<td>$?a(b_1, \ldots, b_k)$</td>
</tr>
</tbody>
</table>
43.7 Mutable Cells as Processes

Let us consider a reference cell server that, when contacted on a pre-determined channel with an initial value and a response channel, creates a fresh cell that may be contacted on a dedicated channel that is returned on the response channel. The client may either receive from or send a value along the dedicated channel dedicated in order to retrieve or modify the current contents of the associated cell.

The reference server, when contacted on channel \( r \) providing an initial contents and a response channel, creates a new cell server process and a new channel on which to contact it.

\[
R(r) = \ast \$ (?r(x,k) . v(l . \$( !c(x,l) . 1) \parallel \$( !k(l) . 1)))
\]

The reference server, when provided an initial value, \( x \), and a response channel, \( k \), allocates a new channel that serves as the name of the newly allocated cell, then contacts the cell service, providing \( x \) and \( l \), to create a new cell, and sends \( l \) back along the response channel.

The cell server, when contacted on channel \( c \) providing an initial contents, \( x \), and a channel, \( l \), creates a server that may be contacted on channel \( l \) to set and retrieve the contents of that cell.

\[
\begin{align*}
C(c) &= \ast \$ (?c(x,l) . \$( S(l) + G(x,l))) \\
S(l) &= ?l(x') . \$( !c(x',l) . 1) \\
G(x,l) &= !l(x) . \$( !c(x,l) . 1)
\end{align*}
\]

The cell server listens on channel \( c \) for an initial contents and a channel, \( l \), and establishes a server that listens on channel \( l \) for either a send or a receive. If a new value is received it creates a new cell server with that value.
as contents, but that may be contacted on the same channel. Otherwise it sends the current value on the same channel, and restarts the server loop.

The use the reference service in a process $P$, we concurrently compose $P$ with $R(r)$ and $C(c)$, where $r$ and $c$ are distinct channels dedicated to these services.

$$\nu(r.\nu(c.P \parallel R(r) \parallel C(c))).$$

The process $P$ allocates a response channel, and communicates with the reference server:

$$P = \nu(k.\$!r(x_0,k).1 \parallel \$?k(l) \ldots)$$

The process allocates a response channel, and sends it to the reference server, along with the initial contents of the cell. It then listens on the response channel for the channel on which to contact the cell, then proceeds (in the elided portion of the code) to interact with the cell along that channel.

### 43.8 Asynchronous Communication

This form of interaction is called synchronous, because both the sender and the receiver are blocked from further interaction until synchronization has occurred. On the receiving side this is inevitable, because the receiver cannot continue execution until the channel which it receives has been determined, much as the body of a function cannot be executed until its argument has been provided. On the sending side, however, there is no fundamental reason why notification is required; the sender could simply send the message along a channel without specifying how to continue once that message has been received. This “fire and forget” semantics is called asynchronous communication, in constrast to the synchronous form just described.

The asynchronous $\pi$-calculus is obtained by removing the synchronous send event, $!a(b).P$, and adding a new form of process, the asynchronous send process, written $!a(b)$, which has no continuation after the send.
syntax of the asynchronous π-calculus is given by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>$P ::= $</td>
<td>$\text{snd}<a href="b">a</a>$</td>
<td>$!a(b)$</td>
</tr>
<tr>
<td></td>
<td>$\mid$</td>
<td>$\text{await}(E)$</td>
<td>$$E$</td>
</tr>
<tr>
<td></td>
<td>$\mid$</td>
<td>$\text{par}(P_1;P_2)$</td>
<td>$P_1 \parallel P_2$</td>
</tr>
<tr>
<td></td>
<td>$\mid$</td>
<td>$\text{new}(a.P)$</td>
<td>$\nu(a.P)$</td>
</tr>
<tr>
<td>Event</td>
<td>$E ::= $</td>
<td>$\text{null}$</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>$\mid$</td>
<td>$\text{rcv}<a href="x.P">a</a>$</td>
<td>$?a(x).P$</td>
</tr>
<tr>
<td></td>
<td>$\mid$</td>
<td>$\text{choice}(E_1;E_2)$</td>
<td>$E_1 + E_2$</td>
</tr>
</tbody>
</table>

Up to structural congruence, an event is just a choice of zero or more reads along any number of channels.

The dynamic semantics for the asynchronous π-calculus is defined by omitting Rule (43.9a), and adding the following rule for the asynchronous send process:

$$
\text{!}a(b) \xrightarrow{\text{!}a(b)} 1 \quad (43.10)
$$

One may regard the pending asynchronous write as a kind of buffer in which the message is held until a receiver is chosen.

In a sense the synchronous π-calculus is more fundamental than the asynchronous variant, because we may always mimic the asynchronous send by a process of the form $\$!a(b).1$, which performs the send, and then becomes the inert process 1. In another sense, however, the asynchronous π-calculus is more fundamental, because we may encode a synchronous send by introducing a notification channel on which the receiver sends a message to notify the sender of the successful receipt of its message. This exposes the implicit communication required to implement synchronous send, and avoids it in cases where it is not needed (in particular, when the resumed process is just the inert process, as just illustrated).

To get an idea of what is involved in the encoding of the synchronous π-calculus in the asynchronous π-calculus, we sketch the implementation of an acknowledgement protocol that only requires (polyadic) asynchronous communication. A synchronous process of the form

$$
v(a.\$((!a(b).P) + E) \parallel \$((?a(x).Q) + F))
$$

is represented by the asynchronous process

$$
v(a.\nu(a_0.P' \parallel Q')),
$$
where $a_0 \notin P$, $a_0 \notin Q$, and we define

$$P' = !a(b,a_0) \parallel $( ?a_0(). P + E$)$$

and

$$Q' = $( ?a(x,x_0). ( !x_0(). Q) + F$).$$

The process that is awaiting the outcome of a send event along channel $a$ instead sends the argument, $b$, along with a newly allocated acknowledgement channel, $a_0$, along the channel $a$, then awaits receipt of a signal in the form of a null message along $a_0$, then acts as the process $P$. Correspondingly, the process that is awaiting a receive event along channel $a$ must be prepared to receive, in addition, the acknowledgement channel, $x_0$, on which it sends an asynchronous signal back to the sender, and proceeds to act as the process $Q$. It is easy to check that the synchronous interaction of the original process is simulated by several steps of execution of the translation into asynchronous form.

43.9 Exercises
Chapter 44

Concurrency

In this chapter we utilize the process calculus presented in Chapter 43 to derive a uniform treatment of several seemingly disparate concepts: mutable storage, speculative parallelism, input/output, process creation, and inter-process communication. The unifying theme is to use a process calculus to give an account of context-sensitive execution. For example, inter-process communication necessarily involves the execution of two processes, each in a context that includes the other. The two processes synchronize, and continue execution separately after their rendezvous.

44.1 Framework

The syntax of $\mathcal{L}$ is given by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>$\tau$</td>
<td>$\text{cmd}(\tau)$</td>
<td>$\tau$ cmd</td>
</tr>
<tr>
<td>Expr</td>
<td>$e$</td>
<td>$\text{cmd}(m)$</td>
<td>$\text{cmd } m$</td>
</tr>
<tr>
<td>Comm</td>
<td>$m$</td>
<td>$\text{ret}(e)$</td>
<td>$\text{ret } e$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{seq}(e;x.m)$</td>
<td>$\text{let } \text{cmd } x \text{ be } e \text{ in } m$</td>
</tr>
<tr>
<td>Proc</td>
<td>$p$</td>
<td>$\text{proc}<a href="m">a</a>$</td>
<td>${ a : m }$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{par}(p_1; p_2)$</td>
<td>$p_1 \parallel p_2$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{new}<a href="x.p">\tau</a>$</td>
<td>$v(x:\tau.p)$</td>
</tr>
</tbody>
</table>

The basic form of process is $\text{proc}[a](m)$, consisting of a single command, $m$, labelled with a symbol, $a$, that serves to identify it. We may also form the parallel composition of processes, and generate a new symbol for use within a process.
As always, we identify syntactic objects up to \( \alpha \)-equivalence, so that bound names may always be chosen so as to satisfy any finitary constraint on their occurrence. As in Chapter 43, we also identify processes up to structural congruence, which specifies that parallel composition is commutative and associative, and that new symbol generation may have its scope expanded to encompass any parallel process, subject only to avoidance of capture.

In the succeeding sections of this chapter, the language \( \mathcal{L}\{\text{conc}\} \) will be extended to model various forms of computational phenomena. In each case we will enrich the language with new forms of command, representing primitive capabilities of the language, and new forms of process, used to model the context in which commands are executed. In this respect it is misleading to think of processes as necessarily having to do with concurrent execution and synchronization! Rather, what processes provide is a simple, uniform means of describing the context in which a command is executed. This can include concurrent interaction (synchronization) in the familiar sense, but is not limited to this case.

Let \( \Sigma \) range over finite sets of judgements of the form \( a : \tau \), where \( a \) is a symbol and \( \tau \) is a type, such that no symbol is the subject of more than one such judgement in \( \Sigma \). We define the judgement \( p \) ok by the following rules:

\[
\begin{align*}
\Sigma; \Gamma \vdash m : \sim \tau & \quad \text{(44.1a)} \\
\Sigma, a : \text{proc}(\tau); \Gamma \vdash \text{proc}[a](m) \text{ ok} \\
\Sigma; \Gamma \vdash p_1 \text{ ok} & \quad \Sigma \vdash p_2 \text{ ok} \\
\Sigma; \Gamma \vdash \text{par}(p_1; p_2) \text{ ok} & \quad \text{(44.1b)} \\
\Sigma, a : \tau; \Gamma \vdash p \text{ ok} & \quad \text{(44.1c)} \\
\Sigma; \Gamma \vdash \text{new}[\tau](a.p) \text{ ok} \\
\Sigma; \Gamma \vdash p' \text{ ok} & \quad p \equiv p' \\
\Sigma; \Gamma \vdash p \text{ ok} & \quad \text{(44.1d)}
\end{align*}
\]

Rule (44.1a) specifies that a process of the form \( \text{proc}[a](m) \) is well-formed if \( m \) is a command yielding a value of type \( \tau \), where \( a \) is a process identifier of type \( \tau \). The type \( \text{proc}(\tau) \) is the type of process identifiers returning a value of type \( \tau \). Rule (44.1b) states that a parallel composition of processes is well-formed if both processes are well-formed. Rule (44.1c) enriches \( \Sigma \) with a new symbol with a type \( \tau \) chosen so that \( p \) is well-formed under this assumption. Finally, Rule (44.1d) states that typing respects structural congruence. Ordinarily such a rule is left implicit, but we state it explicitly for emphasis.
Each extension of $L\{\text{conc}\}$ considered below may introduce new forms of process governed by new formation and execution rules.

The dynamic semantics of $L\{\text{conc}\}$ is defined by judgements of the form $p \leadsto p'$, where $p$ and $p'$ are processes. Execution of processes includes structural normalization, may apply to any active process, may occur within the scope of a newly introduced symbol, and respects structural congruence:

$$m \leadsto m' \quad \frac{}{\text{proc}[a](m) \leadsto \text{proc}[a](m')} \quad (44.2a)$$

$$\frac{}{\text{proc}[a](\text{ret}(e)) \overset{\text{!a}(e)}{\leadsto} \text{proc}[a](\text{ret}(e))} \quad (44.2b)$$

$$\frac{}{\text{par}(p_1; p_2) \leadsto \text{par}(p'_1; p_2)} \quad (44.2c)$$

$$\frac{}{p \leadsto p'} \quad (44.2d)$$

$$\frac{}{\text{new}[\tau](a.p) \leadsto \text{new}[\tau](a.p')} \quad (44.2e)$$

Rule (44.2b) specifies that a process whose execution has completed normally announces this fact to the ambient context by offering the returned value labelled with the process’s identifier. This allows for other processes to notice that the process labelled $a$ has terminated, and to recover its returned value.

In the rest of this chapter we consider various forms of computation, each of which gives rise to new rules for process execution. These rules generally have the form of transitions of the form

$$\{a : m\} \overset{\alpha}{\leadsto} v(a_1 : \tau_1 \ldots v(a_j : \tau_j . (p_1 \parallel \ldots \parallel p_k))$$

where $j, k \geq 0$ and $\alpha$ is an action appropriate to that form of computation.

### 44.2 Input/Output

Character input and output are readily modeled in $L\{\text{conc}\}$ by considering input and output ports to be channels on which we may transmit characters.

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comm</td>
<td>$m$</td>
<td>:= getc()</td>
<td>getc()</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>putc($e$)</td>
</tr>
</tbody>
</table>
The static semantics assumes that we have a type `char` of characters:

\[
\Sigma \Gamma \models \text{getc()} : \sim \text{char}
\] (44.3a)

\[
\Sigma \Gamma \models \text{e} : \text{char}
\]

\[
\Sigma \Gamma \models \text{putc(e)} : \sim \text{char}
\] (44.3b)

Given two distinguished ports, `in` and `out`, the dynamic semantics of character input/output may be given by the following rules:

\[
\{a : \text{getc()}\} \xrightarrow{?\text{in}(c)} \{a : \text{ret c}\}
\] (44.4a)

\[
\{a : \text{putc(c)}\} \xrightarrow{!\text{out}(c)} \{a : \text{ret c}\}
\] (44.4b)

As a technical convenience, Rule (44.3b) specifies that `putc` returns the character that it sent to the output.

### 44.3 Mutable Cells

Here we develop a representation of mutable storage in \(\mathcal{L}\{\text{conc}\}\) in which each reference cell is a process that enacts a protocol for retrieving and altering its contents. The process \(\langle l : e \rangle\), where \(e\) is a value of some type \(\tau\), represents a mutable cell at location \(l\) with contents \(e\) of type \(\tau\). This process is prepared to send the value \(e\) along the channel named \(l\), once again becoming the same process. It is also prepared to receive a value along channel \(l\), which becomes the new contents of the reference cell with location \(l\). Thus we may think of a reference cell as a “server” that emits the current contents of the cell, and that may respond to requests to change its contents.

To model reference cells as processes we extend the grammar of \(\mathcal{L}\{\text{conc}\}\) to incorporate reference types as described in Chapter 38 and to introduce a new form of process representing a reference cell:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>(\tau)</td>
<td>\text{ref}(\tau)</td>
<td>(\tau) ref</td>
</tr>
<tr>
<td>Expr</td>
<td>(e)</td>
<td>\text{ref}[l]</td>
<td>\text{ref}[l]</td>
</tr>
<tr>
<td>Comm</td>
<td>(m)</td>
<td>\text{newref}<a href="e">l</a></td>
<td>\text{newref} e</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\text{getref}(e)</td>
<td>\text{getref} e</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\text{setref}(e_1; e_2)</td>
<td>(e_1 := e_2)</td>
</tr>
<tr>
<td>Proc</td>
<td>(p)</td>
<td>\text{ref}<a href="e">l</a></td>
<td>\langle l : e \rangle</td>
</tr>
</tbody>
</table>
The process \( \langle l : e \rangle \) represents a mutable cell at location \( l \) with contents \( e \), where \( e \) is a value.

The typing rule for references is given as follows:

\[
\frac{
\Sigma, l : \tau_{\text{ref}} \vdash e : \tau \\
\Sigma, l : \tau_{\text{ref}} \vdash e \text{ val}
}{
\Sigma, l : \tau_{\text{ref}} \vdash \langle l : e \rangle \text{ ok}
}
\] (44.5)

The process \( \langle l : e \rangle \) is well-formed if the assumed type of \( l \) is \( \tau_{\text{ref}} \), where \( e \) is of type \( \tau \) under the full set of typing assumptions for locations.

The dynamic semantics of mutable storage is specified in \( \mathcal{L}\{\text{conc}\} \) by the following rules:

\[
\frac{e \text{ val}}{
\{ a : \text{newref } e \} \rightarrow \nu (l : \tau_{\text{ref}}, \{ a : \text{ret } l \} \parallel \langle l : e \rangle)
}
\] (44.6a)

\[
\frac{e \text{ val}}{
\{ a : @ l \} \rightarrow \{ a : \text{ret } e \}
}
\] (44.6b)

\[
\frac{e \text{ val}}{
\{ a : l := e \} \rightarrow \{ a : \text{ret } e \}
}
\] (44.6c)

\[
\frac{e \text{ val}}{
\langle l : e \rangle \rightarrow \langle l : e \rangle
}
\] (44.6d)

\[
\frac{e \text{ val} \quad e' \text{ val}}{
\langle l : e \rangle \rightarrow \langle l : e' \rangle
}
\] (44.6e)

Rule (44.6a) gives the semantics of \text{new}, which allocates a new location, \( l \), which is returned to the calling process, and spawns a new process consisting of a reference cell at location \( l \) with contents \( e \). Rule (44.6b) specifies that the execution of the process \( \{ a : @ l \} \) consists of synchronizing with the reference cell at location \( l \) to obtain its contents, continuing with the value so obtained. Rule (44.6c) specifies that execution of \( \{ a : l := e \} \) synchronizes with the reference cell at location \( l \) to specify its new contents, \( e' \).

Rules (44.6d) and (44.6e) specify that a reference cell process, \( \langle l : e \rangle \), may interact with other processes via the location \( l \), by either sending the contents, \( e \), of \( l \) to a receiver without changing its state, or receiving its new contents, \( e' \), from a sender, and changing its contents accordingly.

\footnote{For the sake of concision we have omitted the evident rules for evaluation of the constituent expressions of the various forms of command.}
It is instructive to reconsider the proof of type safety for reference cells given in Chapter 38. Whereas in Chapter 38 the execution state for a command, $m$, has the form $m \parallel \mu$, where $\mu$ is a memory mapping locations to values, here the execution state for $m$ is a process that, up to structural congruence, has the form

$$v(l_1: \tau_1 \, \text{ref.} \ldots v(l_k: \tau_k \, \text{ref.}) \parallel l_1: e_1 \ldots \parallel l_k: e_k \parallel \{a : m\}). \tag{44.7}$$

The memory has been decomposed into a set of active locations, $l_1, \ldots, l_k$, and a set of processes $\langle l_1: e_1 \rangle, \ldots, \langle l_k: e_k \rangle$ governing the active locations.

It will turn out to be an invariant of the dynamic semantics that each active location is governed by exactly one process, but the static semantics of processes given by Rules (44.1) are not sufficient to ensure it. (This is as it should be, because the stated property is special to the semantics of reference cells, and not a general property of all possible uses of the process calculus.) The static semantics is sufficient to ensure that if a process of the form (44.7) is well-formed, then for each $1 \leq i \leq j$,

$$l_1: \tau_1 \, \text{ref.} \ldots l_k: \tau_k \, \text{ref} \vdash e_i: \tau_i.$$

As discussed in Chapter 38 this condition is necessary for type preservation, because memories may contain cyclic references.

The static semantics of processes is enough to ensure preservation; all that is required is that the contents of each location be type-consistent with its declared type. The static semantics is not, however, sufficient to ensure progress, for we may have fewer reference cell processes than declared locations, and hence the program may “get stuck” referring to the contents of a location, $l$, for which there is no process of the form $\langle l : e \rangle$ with which to interact. One prove that the following property is an invariant of the dynamic semantics in the sense that if $p$ satisfies this condition and is well-formed according to Rules (44.1), and $p \rightarrow q$, then $q$ also satisfies the same condition:

**Lemma 44.1.** If $p \equiv v(l: \tau \, \text{ref.}) \; p'$ and $p \rightarrow q$, then $q \equiv \langle l: e \rangle \parallel q'$ for some process $q'$ and value $e$.

For the proof of progress, observe that by inversion of Rules (44.1) and (44.5), if $p \; \text{ok}$, where

$$p \equiv v(l_1: \tau_1 \, \text{ref.} \ldots v(l_k: \tau_k \, \text{ref.}) \parallel \{a : m\}),$$

where $l$ occurs in $m$, then

$$p \equiv v(l: \tau \, \text{ref.}) \; p'.$$
44.4 Futures

The semantics of reference cells given in the preceding section makes use of concurrency to model mutable storage. By relaxing the restriction that the content of a cell be a value, we open up further possibilities for exploiting concurrency. In this section we model the concept of a future, a memoized, speculatively executed suspension, in the context of the language $\mathcal{L}\{\text{conc}\}$.

The syntax of futures is given by the following grammar:

<table>
<thead>
<tr>
<th>Category</th>
<th>Item</th>
<th>Abstract</th>
<th>Concrete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>$\tau$</td>
<td>$\text{fut}(\tau)$</td>
<td>$\tau\text{fut}$</td>
</tr>
<tr>
<td>Expr</td>
<td>$e$</td>
<td>$\text{fut}[l]$</td>
<td>$\text{fut}[l]$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{pid}[a]$</td>
<td>$a$</td>
</tr>
<tr>
<td>Comm</td>
<td>$m$</td>
<td>$\text{fut}(e)$</td>
<td>$\text{fut}(e)$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{syn}(e)$</td>
<td>$\text{syn}(e)$</td>
</tr>
<tr>
<td>Proc</td>
<td>$p$</td>
<td>$\text{fut}[\text{wait}]<a href="a">l</a>$</td>
<td>$[l:\text{wait}(a)]$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\text{fut}[\text{done}]<a href="e">l</a>$</td>
<td>$[l:\text{done}(e)]$</td>
</tr>
</tbody>
</table>

Expressions are enriched to include locations of futures, and process identifiers, or pid’s, for synchronization. The command $\text{fut}(e)$ creates a cell whose value is determined by evaluating $e$ simultaneously with the calling process. The command $\text{syn}(e)$ synchronizes with the future determined by $e$, returning its value once it is available. A future is represented by a process that may be in one of two states, corresponding to whether the computation of its value is pending or finished. A future in the wait state has the form $\text{fut}[\text{wait}][l](a)$, indicating that the value of the future at location $l$ will be determined by the result of executing the process with pid $a$. A future in the done state has the form $\text{fut}[\text{done}][l](e)$, indicating that the value of the future at location $l$ is $e$.

The static semantics of futures consists of the evident typing rules for the commands $\text{fut}(e)$ and $\text{syn}(e)$, together with rules for the new forms of process:

$$
\sum \Gamma \vdash e : \tau \\
\sum \Gamma \vdash \text{fut}(e) : \sim \tau\text{fut}
$$

(44.8a)

$$
\sum \Gamma \vdash e : \tau\text{fut} \\
\sum \Gamma \vdash \text{syn}(e) : \sim \tau
$$

(44.8b)
The dynamic semantics of futures is specified by the following rules:

\[
\begin{align*}
\Sigma \vdash l : \tau_{\text{proc}} \\
\Sigma \vdash \text{ref}[l] : \tau_{\text{fut}}
\end{align*}
\]
\[
\Sigma \vdash a : \tau_{\text{proc}} \\
\Sigma \vdash a : \tau_{\text{proc}}
\]

\[
\Sigma \vdash l : \tau_{\text{fut}} \quad \Sigma \vdash a : \tau_{\text{proc}} \\
\Sigma \vdash [l : \text{wait}(a)] \text{ok}
\]

\[
\Sigma \vdash l : \tau_{\text{fut}} \quad \Sigma \vdash e : \tau \\
\Sigma \vdash [l : \text{done}(e)] \text{ok}
\]

The dynamic semantics of futures is specified by the following rules:

\[
\begin{align*}
\{a : \text{fut}(e)\} \\
\longrightarrow \\
v(l : \tau_{\text{fut}}.v(b : \tau_{\text{proc}}.\{a : \text{ret}\} \parallel [l : \text{wait}(b)] \parallel \{b : \text{ret}\}))
\end{align*}
\]

\[
\begin{align*}
\{a : \text{syn}(l)\} \xrightarrow{?l(c)} \{a : \text{ret}\}
\end{align*}
\]

\[
[l : \text{wait}(a)] \xrightarrow{?a(c)} [l : \text{done}(e)]
\]

\[
[l : \text{done}(e)] \xrightarrow{!l(c)} [l : \text{done}(e)]
\]

Rule (44.9a) specifies that a future is created in the wait state pending termination of the process that evaluates its argument. Rule (44.9b) specifies that we may only retrieve the value of a future once it has reached the done state. Rules (44.9c) and (44.9d) specify the behavior of futures. A future changes from the wait to the done state when the process that determines its contents has completed execution. Observe that Rule (44.9c) synchronizes with the process labelled \( b \) by waiting for that process to announce its termination with its returned value, as described by Rule (44.2b). A future in the done state repeatedly offers its contents to any process that may wish to synchronize with it.
44.5 Fork and Join

The semantics of futures given in Section 44.4 on page 425 may be seen as a combination of the more primitive concepts of forking a new process, synchronizing with, or joining, another process, creating a reference cell to hold the state of the future, and sum types to represent the state of the future (either waiting or done). In this section we will focus on the fork and join primitives that underly the semantics of futures.

The syntax of \( L\{\text{conc}\} \) is extended with the following constructs:

\[
\begin{array}{|c|c|c|c|}
\hline
\text{Category} & \text{Item} & \text{Abstract} & \text{Concrete} \\
\hline
\text{Type} & \tau & \text{proc}(\tau) & \tau\text{proc} \\
\text{Expr} & e & \text{pid}[a] & a \\
\text{Comm} & m & \text{fork}(m) & \text{fork}(m) \\
 & & \text{join}(e) & \text{join}(e) \\
\hline
\end{array}
\]

The static semantics is given by the following rules:

\[
\frac{\Sigma \Gamma \vdash m : \sim \tau}{\Sigma \Gamma \vdash \text{fork}(m) : \sim \tau\text{proc}} \quad (44.10a)
\]

\[
\frac{\Sigma \Gamma \vdash e : \tau\text{proc}}{\Sigma \Gamma \vdash \text{join}(e) : \sim \tau} \quad (44.10b)
\]

The dynamic semantics is given by the following rules:

\[
\{a : \text{fork}(m)\} \rightarrow v(b.\{a : \text{ret } b\} \parallel \{b : m\}) \quad (44.11a)
\]

\[
\frac{}{\{a : \text{join}(b)\} \overset{?b(c)}{\rightarrow} \{a : \text{ret } e\}} \quad (44.11b)
\]

Rule (44.11a) creates a new process executing the given command, and returns the pid of the new process to the calling process. Rule (44.11b) synchronizes with the specified process, passing its return value to the caller when it has completed.

44.6 Synchronization

When programming with multiple processes it is necessary to take steps to ensure that they interact in a meaningful manner. For example, if two
processes have access to a reference cell representing the current balance in a bank account, it is important to ensure that updates by either process are atomic in that they are not compromised by any action of the other process. Suppose that one process is recording accrued interest by increasing the balance by \( r \% \), and the other is recording a debit of \( n \) dollars. Each proceeds by reading the current balance, performing a simple arithmetic computation, and storing the result back to record the result. However, we must ensure that each operation is performed in its entirety without interference from the other in order to preserve the semantics of the transactions.

To see what can go wrong, suppose that both processes read the balance, \( b \), then each calculate their own version of the new balance, \( b_1 = b + r \times b \) and \( b_2 = b - n \), and then both store their results in some order, say \( b_1 \) followed by \( b_2 \). The resulting balance, \( b_2 \), reflects the debit of \( n \) dollars, but not the interest accrual! If the stores occur in the opposite order, the new balance reflects the interest accrued, but not the debit. In either case the answer is wrong!

The solution is to ensure that a read-and-update operation is completed in its entirety without affecting or being affected by the actions of any other process. One way to achieve this is to use an \textit{mvar}, which is a reference cell that may, at any time, either hold a value or be empty.\(^2\) Thus an \textit{mvar} may be in one of two states: full or empty, according to whether or not it holds a value. A process may take the value from a full \textit{mvar}, thereby rendering it empty, or put a value into an empty \textit{mvar}, thereby rendering it full with that value. No process may take a value from an empty \textit{mvar}, nor may a process put a value to a full \textit{mvar}. Any attempt to do so blocks progress until the state of the \textit{mvar} has been changed by some other process so that it is once again possible to make progress. This simple primitive is sufficient to implement many higher-level constructs such as communication channels, as we shall see shortly.

The syntax of \textit{mvar’s} is given by the following grammar:

\[
\begin{align*}
\text{Category} & \quad \text{Item} \quad \text{Abstract} \quad \text{Concrete} \\
\text{Type} & \quad \tau \quad ::= \quad \text{mvar}(\tau) \quad \tau \text{mvar} \\
\text{Comm} & \quad m \quad ::= \quad \text{mvar}(e) \quad \text{mvar}(e) \\
& \quad \text{\quad |} \quad \text{take}(e) \quad \text{take}(e) \\
& \quad \text{\quad |} \quad \text{put}(e_1; e_2) \quad \text{put}(e_1; e_2) \\
\text{Proc} & \quad p \quad ::= \quad \text{mvar[full]}[l](e) \quad [l : \text{full}(e)] \\
& \quad \text{\quad |} \quad \text{mvar[empty]}[l] \quad [l : \text{empty}] \\
\end{align*}
\]

\(^2\)The name “\textit{mvar}” is admittedly cryptic, but is relatively standard. \textit{Mvar’s} are also known as \textit{mailboxes}, since their behavior is similar to that of a postal delivery box.
The static semantics for commands is analogous to that for reference cells, and is omitted. The rules governing the two new forms of process are as follows:

\[
\Sigma \vdash l : \tau \text{mvar} \quad \Sigma ; \Gamma \vdash e : \tau \\
\Sigma ; \Gamma \vdash [l : \text{full}(e)] \text{ ok}
\]

\[
\Sigma \vdash l : \tau \text{mvar} \\
\Sigma ; \Gamma \vdash [l : \text{empty}] \text{ ok}
\]

The dynamic semantics of mvars is given by the following transition rules:

\[
e \text{val} \\
\{a : \text{mvar}(e)\} \mapsto v(l : \tau \text{mvar} . \{a : \text{ret } l\} \parallel [l : \text{full}(e)])
\]

\[
\{a : \text{take}(l)\} \xrightarrow{?l(e)} \{a : \text{ret } e\}
\]

\[
e \text{val} \\
\{a : \text{put}(l ; e)\} \xrightarrow{!l(e)} \{a : \text{ret } e\}
\]

\[
[l : \text{full}(e)] \xrightarrow{!l(e)} \text{[l : empty]}
\]

\[
[l : \text{empty}] \xrightarrow{?l(e)} \text{[l : full}(e)]
\]

Rules (44.13d) and (44.13e) enforce the protocol ensuring that only one process at a time may access the contents of an mvar. If a full mvar synchronizes with a \text{take} (Rule (44.13b)), then its state changes to empty, precluding further reads of its value. Conversely, if an empty mvar synchronizes with a \text{put} (Rule (44.13e)), then its state changes to full with the value specified by the \text{put}.

Using mvar’s it is straightforward to implement communication channels over which processes may send and receive values of some specified type, \(\tau\). To be specific, a \textit{channel} is just an mvar containing a queue of messages maintained in the order in which they were received. Sending a message on a channel adds (atomically!) a message to the back of the queue associated with that channel, and receiving a message from a channel removes (again, atomically) a message from the front of the queue. We leave a full development of channels as an instructive exercise for the reader.
44.7 Exercises
Part XVII

Modularity
Chapter 45

Separate Compilation and Linking

45.1 Linking and Substitution

45.2 Exercises
Chapter 46

Basic Modules
Chapter 47

Parameterized Modules
Part XVIII

Equivalence
Chapter 48

Equational Reasoning for T

The beauty of functional programming is that equality of expressions in a functional language corresponds very closely to familiar patterns of mathematical reasoning. For example, in the language $L\{	ext{nat} \rightarrow\}$ of Chapter 14 in which we can express addition as the function `plus`, the expressions

$$\lambda (x:\text{nat}.\lambda (y:\text{nat}.\text{plus}(x)(y)))$$

and

$$\lambda (x:\text{nat}.\lambda (y:\text{nat}.\text{plus}(y)(x)))$$

are equal. In other words, the addition function as programmed in $L\{	ext{nat} \rightarrow\}$ is commutative.

This may seem to be obviously true, but why, precisely, is it so? More importantly, what do we even mean when we say that two expressions of a programming language are equal in this sense? It is intuitively obvious that these two expressions are not definitionally equivalent, because they cannot be shown equivalent by symbolic execution. One may say that these two expressions are definitionally inequivalent because they describe different algorithms: one proceeds by recursion on $x$, the other by recursion on $y$. On the other hand, the two expressions are interchangeable in any complete computation of a natural number, because the only use we can make of them is to apply them to arguments and compute the result. We say that two functions are extensionally equivalent if they give equal results for equal arguments—in particular, they agree on all possible arguments. Since their behavior on arguments is all that matters for calculating observable results, we may expect that extensionally equivalent functions are equal in the sense of being interchangeable in all complete programs. Thinking of
the programs in which these functions occur as observations of their behavior, we say that the these functions are observationally equivalent. The main result of this chapter is that observational and extensional equivalence coincide for a variant of $\mathcal{L}\{\text{nat} \to\}$ in which the successor is evaluated eagerly, so that a value of type $\text{nat}$ is a numeral.

### 48.1 Observational Equivalence

When are two expressions equal? Whenever we cannot tell them apart! This may seem tautological, but it is not, because it depends on what we consider to be a means of telling expressions apart. What “experiment” are we permitted to perform on expressions in order to distinguish them? What counts as an observation that, if different for two expressions, is a sure sign that they are different?

If we permit ourselves to consider the syntactic details of the expressions, then very few expressions could be considered equal. For example, if it is deemed significant that an expression contains, say, more than one function application, or that it has an occurrence of $\lambda$-abstraction, then very few expressions would come out as equivalent. But such considerations seem silly, because they conflict with the intuition that the significance of an expression lies in its contribution to the outcome of a computation, and not to the process of obtaining that outcome. In short, if two expressions make the same contribution to the outcome of a complete program, then they ought to be regarded as equal.

We must fix what we mean by a complete program. Two considerations inform the definition. First, the dynamic semantics of $\mathcal{L}\{\text{nat} \to\}$ is given only for expressions without free variables, so a complete program should clearly be a closed expression. Second, the outcome of a computation should be observable, so that it is evident whether the outcome of two computations differs or not. We define a complete program to be a closed expression of type $\text{nat}$, and define the observable behavior of the program to be the numeral to which it evaluates.

An experiment on, or observation about, an expression is any means of using that expression within a complete program. We define an expression context to be an expression with a “hole” in it serving as a placeholder for another expression. The hole is permitted to occur anywhere, including within the scope of a binder. The bound variables within whose scope the hole lies are said to be exposed (to capture) by the expression context. These variables may be assumed, without loss of generality, to be distinct from...
one another. A program context is a closed expression context of type nat—that is, it is a complete program with a hole in it. The meta-variable $C$ stands for any expression context.

Replacement is the process of filling a hole in an expression context, $C$, with an expression, $e$, which is written $C\{e\}$. Importantly, the free variables of $e$ that are exposed by $C$ are captured by replacement (which is why replacement is not a form of substitution, which is defined so as to avoid capture). If $C$ is a program context, then $C\{e\}$ is a complete program iff all free variables of $e$ are captured by the replacement. For example, if $C = \lambda (x: \text{nat} \cdot \circ)$, and $e = x + x$, then

$$C\{e\} = \lambda (x: \text{nat} \cdot x + x).$$

The free occurrences of $x$ in $e$ are captured by the $\lambda$-abstraction as a result of the replacement of the hole in $C$ by $e$.

We sometimes write $C\{\circ\}$ to emphasize the occurrence of the hole in $C$. Expression contexts are closed under composition in that if $C_1$ and $C_2$ are expression contexts, then so is

$$C\{\circ\} := C_1\{C_2\{\circ\}\},$$

and we have $C\{e\} = C_1\{C_2\{e\}\}$. The trivial, or identity, expression context is the “bare hole”, written $\circ$, for which $\circ\{e\} = e$.

The static semantics of expressions of $L\{\text{nat} \to\}$ is extended to expression contexts by defining the typing judgement

$$C : (\Gamma \triangleright \tau) \rightsquigarrow (\Gamma' \triangleright \tau')$$

so that if $\Gamma \vdash e : \tau$, then $\Gamma' \vdash C\{e\} : \tau'$. This judgement may be inductively defined by a collection of rules derived from the static semantics of $L\{\text{nat} \to\}$ (for which see Rules (14.1)). Some representative rules are as follows:

$$\circ : (\Gamma \triangleright \tau) \rightsquigarrow (\Gamma \triangleright \tau) \tag{48.1a}$$

$$C : (\Gamma \triangleright \tau) \rightsquigarrow (\Gamma' \triangleright \text{nat})$$
$$s(C) : (\Gamma \triangleright \tau) \rightsquigarrow (\Gamma' \triangleright \text{nat}) \tag{48.1b}$$

$$C : (\Gamma \triangleright \tau) \rightsquigarrow (\Gamma' \triangleright \text{nat})$$
$$\Gamma' \vdash e_0 : \tau'$$
$$\Gamma', x : \text{nat}, y : \tau' \vdash e_1 : \tau'$$
$$\text{natrec} C \{z \Rightarrow e_0 \mid s(x) \text{ with } y \Rightarrow e_1\} : (\Gamma \triangleright \tau) \rightsquigarrow (\Gamma' \triangleright \tau') \tag{48.1c}$$
48.1 Observational Equivalence

\[ \Gamma' \vdash e : \text{nat} \quad C_0 : (\Gamma \triangleright \tau) \rightsquigarrow (\Gamma' \triangleright \tau') \quad \Gamma', x : \text{nat}, y : \tau' \vdash e_1 : \tau' \]
\[ \text{natrec } \{ z \Rightarrow C_0 \mid s(x) \text{ with } y \Rightarrow e_1 \} : (\Gamma \triangleright \tau) \rightsquigarrow (\Gamma' \triangleright \tau') \]  
(48.1d)

\[ \Gamma' \vdash e : \text{nat} \quad \Gamma' \vdash e_0 : \tau' \quad C_1 : (\Gamma \triangleright \tau) \rightsquigarrow (\Gamma', x : \text{nat}, y : \tau' \triangleright \tau') \]
\[ \text{natrec } \{ z \Rightarrow e_0 \mid s(x) \text{ with } y \Rightarrow C_1 \} : (\Gamma \triangleright \tau) \rightsquigarrow (\Gamma' \triangleright \tau') \]  
(48.1e)

\[ C_2 : (\Gamma \triangleright \tau_1 \triangleright \tau_2) \]
\[ \lambda (x : \tau_1). C_2 : (\Gamma \triangleright \tau) \rightsquigarrow (\Gamma' \triangleright \tau_1 \triangleright \tau_2) \]  
(48.1f)

\[ C_1 : (\Gamma \triangleright \tau) \rightsquigarrow (\Gamma' \triangleright \tau_2 \rightarrow \tau') \quad \Gamma' \vdash e_2 : \tau_2 \]
\[ C_1(e_2) : (\Gamma \triangleright \tau) \rightsquigarrow (\Gamma' \triangleright \tau') \]  
(48.1g)

\[ \Gamma' \vdash e_1 : \tau_2 \rightarrow \tau' \quad C_2 : (\Gamma \triangleright \tau) \rightsquigarrow (\Gamma' \triangleright \tau_2) \]
\[ e_1(C_2) : (\Gamma \triangleright \tau) \rightsquigarrow (\Gamma' \triangleright \tau') \]  
(48.1h)

**Lemma 48.1.** If \( C : (\Gamma \triangleright \tau) \rightsquigarrow (\Gamma' \triangleright \tau') \), then \( \Gamma' \subseteq \Gamma \), and if \( \Gamma \vdash e : \tau \), then \( \Gamma' \vdash C \{ e \} : \tau' \).

Observe that the trivial context consisting only of a “hole” acts as the identity under replacement. Moreover, contexts are closed under composition in the following sense.

**Lemma 48.2.** If \( C : (\Gamma \triangleright \tau) \rightsquigarrow (\Gamma' \triangleright \tau') \), and \( C' : (\Gamma' \triangleright \tau') \rightsquigarrow (\Gamma'' \triangleright \tau'') \), then \( C' \{ C \circ \} : (\Gamma \triangleright \tau) \rightsquigarrow (\Gamma'' \triangleright \tau''). \)

**Lemma 48.3.** If \( C : (\Gamma \triangleright \tau) \rightsquigarrow (\Gamma' \triangleright \tau') \) and \( x \notin \text{dom}(\Gamma) \), then \( C : (\Gamma, x : \sigma \triangleright \tau) \rightsquigarrow (\Gamma', x : \sigma \triangleright \tau') \).

**Proof.** By induction on Rules (48.1). \( \square \)

A complete program is a closed expression of type nat.

**Definition 48.1.** We say that two complete programs, \( e \) and \( e' \), are Kleene equivalent, written \( e \simeq e' \), iff there exists \( n \geq 0 \) such that \( e \rightarrow^* \pi \) and \( e' \rightarrow^* \pi \).

Kleene equivalence is evidently reflexive and symmetric; transitivity follows from determinacy of evaluation. Closure under converse evaluation also follows directly from determinacy. It is obviously consistent in that \( \bar{0} \neq \bar{1} \).
**Definition 48.2.** Suppose that \( \Gamma \vdash e : \tau \) and \( \Gamma \vdash e' : \tau \) are two expressions of the same type. We say that \( e \) and \( e' \) are observationally equivalent, written \( e \cong e' : \tau \ [\Gamma] \), iff \( C\{e\} \simeq C\{e'\} \) for every program context \( C : (\Gamma \triangleright \tau) \leadsto (\emptyset \triangleright \text{nat}) \).

In other words, for all possible experiments, the outcome of an experiment on \( e \) is the same as the outcome on \( e' \). This is obviously an equivalence relation.

A family of equivalence relations \( e_1 \mathcal{E} e_2 : \tau \ [\Gamma] \) is a congruence iff it is preserved by all contexts. That is,

\[
\text{if } e \mathcal{E} e' : \tau \ [\Gamma], \text{ then } C\{e\} \mathcal{E} C\{e'\} : \tau' \ [\Gamma']
\]

for every expression context \( C : (\Gamma \triangleright \tau) \leadsto (\Gamma' \triangleright \tau') \). Such a family of relations is consistent iff \( e \mathcal{E} e' : \text{nat} \ [\emptyset] \) implies \( e \simeq e' \).

**Theorem 48.4.** Observational equivalence is the coarsest consistent congruence on expressions.

**Proof.** Consistency follows directly from the definition by noting that the trivial context is a program context. Observational equivalence is obviously an equivalence relation. To show that it is a congruence, we need only observe that type-correct composition of a program context with an arbitrary expression context is again a program context. Finally, it is the coarsest such equivalence relation, for if \( e \mathcal{E} e' : \tau \ [\Gamma] \) for some consistent congruence \( \mathcal{E} \), and if \( C : (\Gamma \triangleright \tau) \leadsto (\emptyset \triangleright \text{nat}) \), then by congruence \( C\{e\} \mathcal{E} C\{e'\} : \text{nat} \ [\emptyset] \), and hence by consistency \( C\{e\} \simeq C\{e'\} \).

A closing substitution, \( \gamma \), for the typing context \( \Gamma = x_1 : \tau_1, \ldots, x_n : \tau_n \) is a finite function assigning closed expressions \( e_1 : \tau_1, \ldots, e_n : \tau_n \) to \( x_1, \ldots, x_n \), respectively. We write \( \hat{\gamma}(e) \) for the substitution \([e_1, \ldots, e_n/x_1, \ldots, x_n]\) of \( e \), and write \( \gamma : \Gamma \) to mean that if \( x : \tau \) occurs in \( \Gamma \), then there exists a closed expression, \( e \), such that \( \gamma(x) = e \) and \( e : \tau \). We write \( \gamma \models \gamma' : \Gamma \), where \( \gamma : \Gamma \) and \( \gamma' : \Gamma \), to express that \( \gamma(x) \cong \gamma'(x) : \Gamma(x) \) for each \( x \) declared in \( \Gamma \).

**Lemma 48.5.** If \( e \cong e' : \tau \ [\Gamma] \) and \( \gamma : \Gamma \), then \( \hat{\gamma}(e) \cong \hat{\gamma}(e') : \tau \). Moreover, if \( \gamma \models \gamma' : \Gamma \), then \( \hat{\gamma}(e) \cong \hat{\gamma}(e') : \tau \) and \( \hat{\gamma}(e') \cong \hat{\gamma'(e')} : \tau \).

**Proof.** Let \( C : (\emptyset \triangleright \tau) \leadsto (\emptyset \triangleright \text{nat}) \) be a program context; we are to show that \( C\{\hat{\gamma}(e)\} \simeq C\{\hat{\gamma}(e')\} \). Since \( C \) has no free variables, this is equivalent to showing that \( \hat{\gamma}(C\{e\}) \simeq \hat{\gamma}(C\{e'\}) \). Let \( D \) be the context

\[
\lambda (x_1 : \tau_1, \ldots, x_n : \tau_n, C(\circ)) (e_1) \ldots (e_n),
\]

December 18, 2009 DRAFT 14:36
where $\Gamma = x_1 : \tau_1, \ldots, x_n : \tau_n$ and $\gamma(x_1) = e_1, \ldots, \gamma(x_n) = e_n$. By Lemma 48.3 on page 444 we have $C : (\Gamma \triangleright \tau) \sim (\emptyset \triangleright \text{nat})$, from which it follows directly that $D : (\Gamma \triangleright \tau) \sim (\emptyset \triangleright \text{nat})$. Since $e \equiv e' : [\Gamma]$, we have $D\{ e \} \simeq D\{ e' \}$. But by construction $D\{ e \} \simeq \hat{\gamma}(C\{ e \})$, and $D\{ e' \} \simeq \hat{\gamma}(C\{ e' \})$, so $\hat{\gamma}(C\{ e \}) \simeq \hat{\gamma}(C\{ e' \})$. Since $C$ is arbitrary, it follows that $\hat{\gamma}(e) \sim \hat{\gamma}(e') : \tau$.

Defining $D'$ similarly to $D$, but based on $\gamma'$, rather than $\gamma$, we may also show that $D'\{ e \} \simeq D'\{ e' \}$, and hence $\hat{\gamma}'(e) \equiv \hat{\gamma}'(e') : \tau$. Now if $\gamma \equiv \gamma' : \Gamma$, then by congruence we have $D\{ e \} \simeq D'\{ e \} : \text{nat}$, and $D\{ e' \} \simeq D'\{ e' \} : \text{nat}$. It follows that $D\{ e \} \simeq D'\{ e \} : \text{nat}$, and so, by consistency of observational equivalence, we have $D\{ e' \} \simeq D'\{ e' \}$, which is to say that $\hat{\gamma}(e) \sim \hat{\gamma}'(e') : \tau$. □

Theorem 48.4 on the previous page licenses the principle of proof by coinduction: to show that $e \equiv e' : [\Gamma]$, it is enough to exhibit a consistent congruence, $\mathcal{E}$, such that $e \in \mathcal{E} e' : [\Gamma]$. It can be difficult to construct such a relation. In the next section we will provide a general method for doing so that exploits types.

### 48.2 Extensional Equivalence

The key to simplifying reasoning about observational equivalence is to exploit types. Informally, we may classify the uses of expressions of a type into two broad categories, the passive and the active uses. The passive uses are those that merely manipulate expressions without actually inspecting them. For example, we may pass an expression of type $\tau$ to a function that merely returns it. The active uses are those that operate on the expression itself; these are the elimination forms associated with the type of that expression. For the purposes of distinguishing two expressions, it is only the active uses that matter; the passive uses merely manipulate expressions at arm’s length, affording no opportunities to distinguish one from another.

This leads to the definition of extensional equivalence alluded to in the introduction.

**Definition 48.3.** Extensional equivalence is a family of relations $e \sim e' : \tau$ between closed expressions of type $\tau$. It is defined by induction on $\tau$ as follows:

- $e \sim e' : \text{nat}$ iff $e \simeq e'$
- $e \sim e' : \tau_1 \rightarrow \tau_2$ iff if $e_1 \sim e'_1 : \tau_1$, then $e(e_1) \sim e'(e'_1) : \tau_2$
The definition of extensional equivalence at type $\text{nat}$ licenses the following principle of proof by $\text{nat}$-induction. To show that $\mathcal{E}(e, e')$ whenever $e \sim e' : \text{nat}$, it is enough to show that

1. $\mathcal{E}(\overline{0}, \overline{0})$, and
2. if $\mathcal{E}(\overline{n}, \overline{n})$, then $\mathcal{E}(\overline{n+1}, \overline{n+1})$.

This is, of course, justified by mathematical induction on $n \geq 0$, where $e \mapsto^n n$ and $e' \mapsto^n n$ by the definition of Kleene equivalence.

Extensional equivalence is extended to open terms by substitution of related closed terms to obtain related results. If $\gamma$ and $\gamma'$ are two substitutions for $\Gamma$, we define $\gamma \sim \gamma' : \Gamma$ to hold iff $\gamma(x) \sim \gamma'(x) : \Gamma(x)$ for every variable, $x$, such that $\Gamma \vdash x : \tau$. Finally, we define $e \sim e' : \tau[\Gamma]$ to mean that $\hat{\gamma}(e) \sim \hat{\gamma'}(e') : \tau$ whenever $\gamma \sim \gamma' : \Gamma$.

### 48.3 Extensional and Observational Equivalence Coincide

In this section we prove the coincidence of observational and extensional equivalence.

**Lemma 48.6 (Converse Evaluation).** Suppose that $e \sim e' : \tau$. If $d \mapsto e$, then $d \sim e' : \tau$, and if $d' \mapsto e'$, then $e \sim d' : \tau$.

**Proof.** By induction on the structure of $\tau$. If $\tau = \text{nat}$, then the result follows from the closure of Kleene equivalence under converse evaluation. If $\tau = \tau_1 \rightarrow \tau_2$, then suppose that $e \sim e' : \tau$, and $d \mapsto e$. To show that $d \sim e' : \tau$, we assume $e_1 \sim e'_1 : \tau_1$ and show $d(e_1) \sim e'(e'_1) : \tau_2$. It follows from the assumption that $e(e_1) \sim e'(e'_1) : \tau_2$. Noting that $d(e_1) \mapsto e(e_1)$, the result follows by induction.

**Lemma 48.7 (Consistency).** If $e \sim e' : \text{nat}$, then $e \simeq e'$.

**Proof.** Immediate, from Definition 48.3 on the facing page.

**Theorem 48.8 (Reflexivity).** If $\Gamma \vdash e : \tau$, then $e \sim e : \tau[\Gamma]$.
Proof. We are to show that if $\Gamma \vdash e : \tau$ and $\gamma \sim \gamma' : \Gamma$, then $\hat{\gamma}(e) \sim \hat{\gamma'}(e) : \tau$. The proof proceeds by induction on typing derivations; we consider a few representative cases.

Consider the case of Rule (13.4a), in which $\tau = \tau_1 \rightarrow \tau_2$ and $e = \lambda (x : \tau_1.e_2)$. Since $e$ is a value, we are to show that

$$\lambda (x : \tau_1.\hat{\gamma}(e_2)) \sim \lambda (x : \tau_1.\hat{\gamma'}(e_2)) : \tau_2.$$ Assume that $e_1 \sim e'_1 : \tau_1$; we are to show that $[e_1/x]\hat{\gamma}(e_2) \sim [e'_1/x]\hat{\gamma'}(e_2) : \tau_2$. Let $\gamma_2 = \gamma[x \mapsto e_1]$ and $\gamma'_2 = \gamma'[x \mapsto e'_1]$, and observe that $\gamma_2 \sim \gamma'_2 : \Gamma, x : \tau_1$. Therefore, by induction we have $\hat{\gamma}_2(e_2) \sim \hat{\gamma}'_2(e_2) : \tau_2$, from which the result follows directly.

Now consider the case of Rule (14.1d), for which we are to show that

$$\text{natrec}(\hat{\gamma}(e);\hat{\gamma}(e_0);x.y.\hat{\gamma}(e_1)) \sim \text{natrec}(\hat{\gamma'}(e);\hat{\gamma'}(e_0);x.y.\hat{\gamma'}(e_1)) : \tau.$$ By the induction hypothesis applied to the first premise of Rule (14.1d), we have

$$\hat{\gamma}(e) \sim \hat{\gamma'}(e) : \text{nat}.$$ We proceed by nat-induction. It suffices to show that

$$\text{natrec}(z;\hat{\gamma}(e_0);x.y.\hat{\gamma}(e_1)) \sim \text{natrec}(z;\hat{\gamma'}(e_0);x.y.\hat{\gamma'}(e_1)) : \tau, \quad (48.2)$$

and that

$$\text{natrec}(s(\pi);\hat{\gamma}(e_0);x.y.\hat{\gamma}(e_1)) \sim \text{natrec}(s(\pi);\hat{\gamma'}(e_0);x.y.\hat{\gamma'}(e_1)) : \tau, \quad (48.3)$$

assuming

$$\text{natrec}(\pi;\hat{\gamma}(e_0);x.y.\hat{\gamma}(e_1)) \sim \text{natrec}(\pi;\hat{\gamma'}(e_0);x.y.\hat{\gamma'}(e_1)) : \tau. \quad (48.4)$$

To show (48.2), by Lemma 48.6 on the previous page it is enough to show that $\hat{\gamma}(e_0) \sim \hat{\gamma'}(e_0) : \tau$. This is assured by the outer inductive hypothesis applied to the second premise of Rule (14.1d).

To show (48.3), define

$$\delta = \gamma[x \mapsto \pi][y \mapsto \text{natrec}(\pi;\hat{\gamma}(e_0);x.y.\hat{\gamma}(e_1))]$$

and

$$\delta' = \gamma'[x \mapsto \pi][y \mapsto \text{natrec}(\pi;\hat{\gamma'}(e_0);x.y.\hat{\gamma'}(e_1))].$$

By (48.4) we have $\delta \sim \delta' : \Gamma, x : \text{nat}, y : \tau$. Consequently, by the outer inductive hypothesis applied to the third premise of Rule (14.1d), and Lemma 48.6 on the preceding page, the required follows. $\square$
Corollary 48.9 (Termination). If \( e : \tau \), then there exists \( e' \) val such that \( e \rightarrow^* e' \).

Symmetry and transitivity of extensional equivalence are easily established by induction on types; extensional equivalence is therefore an equivalence relation.

Lemma 48.10 (Congruence). If \( C_0 : (\Gamma \triangleright \tau) \leadsto (\Gamma_0 \triangleright \tau_0) \), and \( e \sim e' : \tau[\Gamma] \), then \( C_0\{e\} \sim C_0\{e'\} : \tau_0[\Gamma_0] \).

Proof. By induction on the derivation of the typing of \( C_0 \). We consider a representative case in which \( C_0 = \lambda (x: \tau_1.C_2) \) so that \( C_0 : (\Gamma \triangleright \tau) \leadsto (\Gamma_0 \triangleright \tau_1 \rightarrow \tau_2) \) and \( C_2 : (\Gamma \triangleright \tau) \leadsto (\Gamma_0, x : \tau_1 \triangleright \tau_2) \). Assuming \( e \sim e' : \tau[\Gamma] \), we are to show that

\[
C_0\{e\} \sim C_0\{e'\} : \tau_1 \rightarrow \tau_2[\Gamma_0],
\]

which is to say

\[
\lambda (x : \tau_1.C_2\{e\}) \sim \lambda (x : \tau_1.C_2\{e'\}) : \tau_1 \rightarrow \tau_2[\Gamma_0].
\]

We know, by induction, that

\[
C_2\{e\} \sim C_2\{e'\} : \tau_2[\Gamma_0, x : \tau_1].
\]

Suppose that \( \gamma_0 \sim \gamma_0' : \Gamma_0 \), and that \( e_1 \sim e_1' : \tau_1 \). Let \( \gamma_1 = \gamma_0[x \mapsto e_1] \), \( \gamma_1' = \gamma_0'[x \mapsto e_1'] \), and observe that \( \gamma_1 \sim \gamma_1' : \Gamma_0, x : \tau_1 \). By Definition 48.3 on page 446 it is enough to show that

\[
\hat{\gamma}_1(C_2\{e\}) \sim \hat{\gamma}_1'(C_2\{e'\}) : \tau_2,
\]

which follows immediately from the inductive hypothesis.

\[\Box\]

Theorem 48.11. If \( e \sim e' : \tau[\Gamma] \), then \( e \equiv e' : \tau[\Gamma] \).


\[\Box\]

Corollary 48.12. If \( e : \text{nat} \), then \( e \equiv n : \text{nat} \), for some \( n \geq 0 \).

Proof. By Theorem 48.8 on page 447 we have \( e \sim e : \tau \). Hence for some \( n \geq 0 \), we have \( e \sim n : \text{nat} \), and so by Theorem 48.11, \( e \equiv n : \text{nat} \).

\[\Box\]
Lemma 48.13. For closed expressions $e : \tau$ and $e' : \tau$, if $e \equiv e' : \tau$, then $e \sim e' : \tau$.

Proof. We proceed by induction on the structure of $\tau$. If $\tau = \text{nat}$, consider the empty context to obtain $e \simeq e'$, and hence $e \sim e' : \text{nat}$. If $\tau = \tau_1 \rightarrow \tau_2$, then we are to show that whenever $e_1 \sim e'_1 : \tau_1$, we have $e(e_1) \sim e'(e'_1) : \tau_2$. By Theorem 48.11 on the previous page we have $e_1 \equiv e'_1 : \tau_1$, and hence by congruence of observational equivalence it follows that $e(e_1) \equiv e'(e'_1) : \tau_2$, from which the result follows by induction.


Proof. Assume that $e \equiv e' : [\Gamma]$, and that $\gamma \sim \gamma' : \Gamma$. By Theorem 48.11 on the preceding page we have $\gamma \equiv \gamma' : \Gamma$, so by Lemma 48.5 on page 445 $\hat{\gamma}(e) \equiv \hat{\gamma}'(e') : \tau$. Therefore, by Lemma 48.13, $\hat{\gamma}(e) \sim \hat{\gamma}'(e') : \tau$.

Corollary 48.15. $e \equiv e' : [\Gamma]$ iff $e \sim e' : [\Gamma]$.

Theorem 48.16. If $\Gamma \vdash e \equiv e' : \tau$, then $e \sim e' : [\Gamma]$, and hence $e \equiv e' : [\Gamma]$.

Proof. By an argument similar to that used in the proof of Theorem 48.8 on page 447 and Lemma 48.10 on the preceding page, then appealing to Theorem 48.11 on the previous page.

Corollary 48.17. If $e \equiv e' : \text{nat}$, then there exists $n \geq 0$ such that $e \mapsto^n n$ and $e' \mapsto^n n$.

Proof. By Theorem 48.16 we have $e \sim e' : \text{nat}$ and hence $e \simeq e'$.

48.4 Some Laws of Equivalence

In this section we summarize some useful principles of observational equivalence for $L\{\text{nat} \rightarrow \}$. For the most part these may be proved as laws of extensional equivalence, and then transferred to observational equivalence by appeal to Corollary 48.15. The laws are presented as inference rules with the meaning that if all of the premises are true judgements about observational equivalence, then so are the conclusions. In other words each rule is admissible as a principle of observational equivalence.
48.4 Some Laws of Equivalence

48.4.1 General Laws

Extensional equivalence is indeed an equivalence relation: it is reflexive, symmetric, and transitive.

\[
\begin{align*}
\text{Reflexivity: } & e \simeq e : \tau [\Gamma] \\
\text{Symmetry: } & e' \simeq e : \tau [\Gamma] \\
\text{Transitivity: } & e \simeq e' : \tau [\Gamma] \\
\end{align*}
\]

(48.5a)

(48.5b)

(48.5c)

Reflexivity is an instance of a more general principle, that all definitional equivalences are observational equivalences.

\[
\Gamma \vdash e \equiv e' : \tau \\
\]

(48.6a)

This is called the principle of symbolic evaluation.

Observational equivalence is a congruence: we may replace equals by equals anywhere in an expression.

\[
\begin{align*}
\text{Congruence: } & C : (\Gamma \triangleright \tau) \rightsquigarrow (\Gamma' \triangleright \tau') \\
\text{Substitution: } & C \{e\} \simeq C \{e'\} : \tau' [\Gamma'] \\
\end{align*}
\]

(48.7a)

Equivalence is stable under substitution for free variables, and substituting equivalent expressions in an expression gives equivalent results.

\[
\begin{align*}
\Gamma \vdash e : \tau & \quad e_2 \simeq e'_2 : \tau' [\Gamma, x : \tau] \\
\text{Substitution: } & \ [e/x] e_2 \equiv [e/x] e'_2 : \tau' [\Gamma] \\
\end{align*}
\]

(48.8a)

(48.8b)

48.4.2 Extensionality Laws

Two functions are equivalent if they are equivalent on all arguments.

\[
\begin{align*}
\text{Extensionality: } & e(x) \equiv e'(x) : \tau_2 [\Gamma, x : \tau_1] \\
\text{Substitution: } & e \equiv e' : \tau_1 \rightarrow \tau_2 [\Gamma] \\
\end{align*}
\]

(48.9)

Consequently, every expression of function type is equivalent to a \(\lambda\)-abstraction:

\[
\begin{align*}
\text{\(\lambda\)-abstraction: } & e \simeq \lambda (x : \tau_1, e(x)) : \tau_1 \rightarrow \tau_2 [\Gamma] \\
\end{align*}
\]

(48.10)
48.4.3 Induction Law

An equation involving a free variable, \( x \), of type \( \text{nat} \) can be proved by induction on \( x \).

\[
\frac{[\pi/x]e \equiv [\pi/x]e' : \tau [\Gamma] \ (\text{for every } n \in \mathbb{N})}{e \equiv e' : \tau [\Gamma, x : \text{nat}]} \tag{48.11a}
\]

To apply the induction rule, we proceed by mathematical induction on \( n \in \mathbb{N} \), which reduces to showing:

1. \([z/x]e \equiv [z/x]e' : \tau [\Gamma] \), and

2. \([s(\pi)/x]e \equiv [s(\pi)/x]e' : \tau [\Gamma] \), if \([\pi/x]e \equiv [\pi/x]e' : \tau [\Gamma] \).

48.5 Exercises
Chapter 49

Equational Reasoning for PCF

In this Chapter we develop the theory of observational equivalence for \( \mathcal{L}\{\text{nat} \rightarrow\} \), with an eager interpretation of the type of natural numbers. The development proceeds long lines similar to those in Chapter 48, but is complicated by the presence of general recursion. The proof depends on the concept of an admissible relation, one that admits the principle of proof by fixed point induction.

49.1 Observational Equivalence

The definition of observational equivalence, along with the auxiliary notion of Kleene equivalence, are defined similarly to Chapter 48, but modified to account for the possibility of non-termination.

The collection of well-formed \( \mathcal{L}\{\text{nat} \rightarrow\} \) contexts is inductively defined in a manner directly analogous to that in Chapter 48. Specifically, we define the judgement \( C : (\Gamma \triangleright \tau) \rightsquigarrow (\Gamma' \triangleright \tau') \) by rules similar to Rules (48.1), modified for \( \mathcal{L}\{\text{nat} \rightarrow\} \). (We leave the precise definition as an exercise for the reader.) When \( \Gamma \) and \( \Gamma' \) are empty, we write just \( C : \tau \rightsquigarrow \tau' \).

A complete program is a closed expression of type nat.

**Definition 49.1.** We say that two complete programs, \( e \) and \( e' \), are Kleene equivalent, written \( e \simeq e' \), iff for every \( n \geq 0 \), \( e \rightsquigarrow^* \pi \) iff \( e' \rightsquigarrow^* \pi \).

Kleene equivalence is easily seen to be an equivalence relation and to be closed under converse evaluation. Moreover, \( \emptyset \not\simeq \top \), and, if \( e \) and \( e' \) are both divergent, then \( e \simeq e' \).

Observational equivalence is defined as in Chapter 48.
Definition 49.2. We say that $\Gamma \vdash e : \tau$ and $\Gamma \vdash e' : \tau$ are observationally, or contextually, equivalent iff for every program context $C : (\Gamma \triangleright \tau) \rightsquigarrow (\emptyset \triangleright \text{nat})$, $C \{e\} \simeq C \{e'\}$.

Theorem 49.1. Observational equivalence is the coarsest consistent congruence.

Proof. See the proof of Theorem 48.4 on page 445.

Lemma 49.2 (Substitution and Functionality). If $e \equiv e' : \tau$ [Γ] and $\gamma : \Gamma$, then $\hat{\gamma}(e) \equiv \hat{\gamma}(e') : \tau$. Moreover, if $\gamma \equiv \gamma' : \Gamma$, then $\hat{\gamma}(e) \equiv \hat{\gamma'}(e) : \tau$ and $\hat{\gamma}(e') \equiv \hat{\gamma'}(e') : \tau$.

Proof. See Lemma 48.5 on page 445.

49.2 Extensional Equivalence

Definition 49.3. Extensional equivalence, $e \sim e' : \tau$, between closed expressions of type $\tau$ is defined by induction on $\tau$ as follows:

\[
e \sim e' : \text{nat} \quad \text{iff} \quad e \simeq e'
\]

\[
e \sim e' : \tau_1 \rightarrow \tau_2 \quad \text{iff} \quad e_1 \sim e'_1 : \tau_1 \text{ implies } e(e_1) \sim e'(e'_1) : \tau_2
\]

Formally, extensional equivalence is defined as in Chapter 48, except that the definition of Kleene equivalence is altered to account for non-termination. Extensional equivalence is extended to open terms by substitution. Specifically, we define $e \sim e' : \tau$ [Γ] to mean that $\hat{\gamma}(e) \sim \hat{\gamma}(e') : \tau$ whenever $\gamma \sim \gamma' : \Gamma$.

Lemma 49.3 (Strictness). If $e : \tau$ and $e' : \tau$ are both divergent, then $e \sim e' : \tau$.

Proof. By induction on the structure of $\tau$. If $\tau = \text{nat}$, then the result follows immediately from the definition of Kleene equivalence. If $\tau = \tau_1 \rightarrow \tau_2$, then $e(e_1)$ and $e'(e'_1)$ diverge, so by induction $e(e_1) \sim e'(e'_1) : \tau_2$, as required.

Lemma 49.4 (Converse Evaluation). Suppose that $e \sim e' : \tau$. If $d \mapsto e$, then $d \sim e' : \tau$, and if $d' \mapsto e'$, then $e \sim d' : \tau$. 

14:36 DRAFT DECEMBER 18, 2009
49.3 Extensional and Observational Equivalence Coincide

As a technical convenience, we enrich \( L(\text{nat} \rightarrow) \) with bounded recursion, with abstract syntax \( \text{fix}^m[\tau](x.e) \) and concrete syntax \( \text{fix}^m x : \tau \text{ is } e \), where \( m \geq 0 \). The static semantics of bounded recursion is the same as for general recursion:

\[
\Gamma, x : \tau \vdash e : \tau \\
\Gamma \vdash \text{fix}^m[\tau](x.e) : \tau.
\]  

(49.1a)

The dynamic semantics of bounded recursion is defined as follows:

\[
\text{fix}^0[\tau](x.e) \leftrightarrow \text{fix}^0[\tau](x.e) \\
\text{fix}^{m+1}[\tau](x.e) \leftrightarrow \text{fix}^m[\tau](x.e)/xe
\]  

(49.2b)

If \( m \) is positive, the recursive bound is decremented so that subsequent uses of it will be limited to one fewer unrolling. If \( m \) reaches zero, the expression steps to itself so that the computation diverges with no result.

The key property of bounded recursion is the principle of fixed point induction, which permits reasoning about a recursive computation by induction on the number of unrollings required to reach a value. The proof relies on compactness, which will be stated and proved in Section 49.4 on page 459 below.

**Theorem 49.5 (Fixed Point Induction).** Suppose that \( x : \tau \vdash e : \tau \). If

\[
(\forall m \geq 0) \text{fix}^m x : \tau \text{ is } e \sim \text{fix}^m x : \tau \text{ is } e', \tau,
\]

then \( \text{fix} x : \tau \text{ is } e \sim \text{fix} x : \tau \text{ is } e', \tau. \)

**Proof.** Define an applicative context, \( A \), to be either a hole, \( \circ \), or an application of the form \( A(e) \), where \( A \) is an applicative context. (The typing judgement \( A : \rho \sim \tau \) is a special case of the general typing judgment for contexts.) Define extensional equivalence of applicative contexts, written \( A \approx A' : \rho \sim \tau \), by induction on the structure of \( A \) as follows:

1. \( \circ \approx \circ : \rho \sim \rho; \)

2. if \( A \approx A' : \rho \sim \tau_2 \rightarrow \tau \) and \( e_2 \sim e'_2 : \tau_2 \), then \( A(e_2) \approx A'(e'_2) : \rho \sim \tau. \)
We prove by induction on the structure of $\tau$, if $A \approx A' : \rho \rightsquigarrow \tau$ and

for every $m \geq 0$, $A\{\text{fix}^m x : \rho \text{ is } e\} \sim A'\{\text{fix}^m x : \rho \text{ is } e'\} : \tau$, \hspace{1cm} (49.3)

then

\[ A\{\text{fix } x : \rho \text{ is } e\} \sim A'\{\text{fix } x : \rho \text{ is } e'\} : \tau. \hspace{1cm} (49.4) \]

Choosing $A = A' = \circ$ (so that $\rho = \tau$) completes the proof.

If $\tau = \text{nat}$, then assume that $A \approx A' : \rho \rightsquigarrow \text{nat}$ and (49.3). By Definition 49.3 on page 454, we are to show

\[ A\{\text{fix } x : \rho \text{ is } e\} \simeq A'\{\text{fix } x : \rho \text{ is } e'\}. \]

By Corollary 49.14 on page 461 there exists $m \geq 0$ such that

\[ A\{\text{fix}^m x : \rho \text{ is } e\} \simeq A\{\text{fix}^m x : \rho \text{ is } e\}. \]

By (49.3) we have

\[ A\{\text{fix}^m x : \rho \text{ is } e\} \simeq A'\{\text{fix}^m x : \rho \text{ is } e'\}. \]

By Corollary 49.14 on page 461

\[ A'\{\text{fix}^m x : \rho \text{ is } e'\} \simeq A'\{\text{fix}^m x : \rho \text{ is } e'\}. \]

The result follows by transitivity of Kleene equivalence.

If $\tau = \tau_1 \to \tau_2$, then by Definition 49.3 on page 454, it is enough to show

\[ A\{\text{fix } x : \rho \text{ is } e\}(e_1) \sim A'\{\text{fix } x : \rho \text{ is } e'\}(e_1') : \tau_2 \]

whenever $e_1 \sim e_1' : \tau_1$. Let $A_2 = A(e_1)$ and $A_2' = A'(e_1')$. It follows from (49.3) that for every $m \geq 0$

\[ A_2\{\text{fix}^m x : \rho \text{ is } e\} \sim A_2'\{\text{fix}^m x : \rho \text{ is } e'\} : \tau_2. \]

Noting that $A_2 \approx A_2' : \rho \rightsquigarrow \tau_2$, we have by induction

\[ A_2\{\text{fix } x : \rho \text{ is } e\} \sim A_2'\{\text{fix } x : \rho \text{ is } e'\} : \tau_2, \]

as required. \hspace{1cm} \square

**Lemma 49.6** (Reflexivity). If $\Gamma \vdash e : \tau$, then $e \sim e : \tau$, $\Gamma$. 

14:36 \hspace{1cm} DRAFT \hspace{1cm} DECEMBER 18, 2009
Proof. The proof proceeds along the same lines as the proof of Theorem 48.8 on page 447. The main difference is the treatment of general recursion, which is proved by fixed point induction. Consider Rule (15.1g). Assuming \( \gamma \sim \gamma' : \Gamma \), we are to show that
\[
\text{fix} x : \tau \text{ is } \hat{\gamma}(e) \sim \text{fix} x : \tau \text{ is } \hat{\gamma}'(e) : \tau.
\]
By Theorem 49.5 on page 455 it is enough to show that, for every \( m \geq 0 \),
\[
\text{fix}^m x : \tau \text{ is } \hat{\gamma}(e) \sim \text{fix}^m x : \tau \text{ is } \hat{\gamma}'(e) : \tau.
\]
We proceed by an inner induction on \( m \). When \( m = 0 \) the result is immediate, since both sides of the desired equivalence diverge. Assuming the result for \( m \), and applying Lemma 49.4 on page 454, it is enough to show that \( \hat{\gamma}(e_1) \sim \hat{\gamma}'(e_1) : \tau \), where
\[
e_1 = [\text{fix}^m x : \tau \text{ is } \hat{\gamma}(e)/x\hat{\gamma}(e)], \text{ and} \tag{49.5}
\]
\[
e'_1 = [\text{fix}^m x : \tau \text{ is } \hat{\gamma}'(e)/x\hat{\gamma}'(e)]. \tag{49.6}
\]
But this follows directly from the inner and outer inductive hypotheses. For by the outer inductive hypothesis, if
\[
\text{fix}^m x : \tau \text{ is } \hat{\gamma}(e) \sim \text{fix}^m x : \tau \text{ is } \hat{\gamma}'(e) : \tau,
\]
then
\[
[\text{fix}^m x : \tau \text{ is } \hat{\gamma}(e)/x\hat{\gamma}(e)] \sim [\text{fix}^m x : \tau \text{ is } \hat{\gamma}'(e)/x\hat{\gamma}'(e) : \tau.
\]
But the hypothesis holds by the inner inductive hypothesis, from which the result follows. \( \square \)

Symmetry and transitivity of eager extensional equivalence are easily established by induction on types, noting that Kleene equivalence is symmetric and transitive. Eager extensional equivalence is therefore an equivalence relation.

Lemma 49.7 (Congruence). If \( C_0 : (\Gamma \triangleright \tau) \leadsto (\Gamma_0 \triangleright \tau_0) \), and \( e \sim e' : \tau [\Gamma] \), then \( C_0\{e\} \sim C_0\{e'\} : \tau_0 [\Gamma_0] \).

Proof. By induction on the derivation of the typing of \( C_0 \), following along similar lines to the proof of Lemma 49.6 on the facing page. \( \square \)
Logical equivalence is consistent, by definition. Consequently, it is contained in observational equivalence.

**Theorem 49.8.** If \( e \sim e' : \tau [\Gamma] \), then \( e \cong e' : \tau [\Gamma] \).

*Proof.* By consistency and congruence of extensional equivalence. \( \square \)

**Lemma 49.9.** If \( e \cong e' : \tau \), then \( e \sim e' : \tau \).

*Proof.* By induction on the structure of \( \tau \). If \( \tau = \text{nat} \), then the result is immediate, since the empty expression context is a program context. If \( \tau = \tau_1 \rightarrow \tau_2 \), then suppose that \( e_1 \sim e'_1 : \tau_1 \). We are to show that \( e(e_1) \sim e'(e'_1) : \tau_2 \). By Theorem 49.8 \( e_1 \cong e'_1 : \tau_1 \), and hence by Lemma 49.2 on page 454 \( e(e_1) \cong e'(e'_1) : \tau_2 \), from which the result follows by induction. \( \square \)

**Theorem 49.10.** If \( e \cong e' : \tau [\Gamma] \), then \( e \sim e' : \tau [\Gamma] \).

*Proof.* Assume that \( e \cong e' : \tau [\Gamma] \). Suppose that \( \gamma \sim \gamma' : \Gamma \). By Theorem 49.8 we have \( \gamma \cong \gamma' : \Gamma \), and so by Lemma 49.2 on page 454 we have

\[ \hat{\gamma}(e) \cong \hat{\gamma}'(e') : \tau. \]

Therefore by Lemma 49.9 we have

\[ \hat{\gamma}(e) \sim \hat{\gamma}'(e') : \tau. \]

\( \square \)

**Corollary 49.11.** \( e \cong e' : \tau [\Gamma] \) iff \( e \sim e' : \tau [\Gamma] \).
49.4 Compactness

The principle of fixed point induction is derived from a critical property of \( \mathcal{L}\{\text{nat} \to \} \), called \textit{compactness}. This property states that only finitely many unwindings of a fixed point expression are needed in a complete evaluation of a program. While intuitively obvious (one cannot complete infinitely many recursive calls in a finite computation), it is rather tricky to state and prove rigorously.

The proof of compactness (Theorem 49.13 on the following page) makes use of the stack machine for \( \mathcal{L}\{\text{nat} \to \} \) defined in Chapter 27, augmented with the following transitions for bounded recursive expressions:

\[
\begin{align*}
\Gamma & \vdash \text{fix}^0 x : \tau \text{ is } e \Rightarrow \Gamma \vdash \text{fix}^0 x : \tau \text{ is } e \\
\Gamma & \vdash \text{fix}^{m+1} x : \tau \text{ is } e \Rightarrow \Gamma \vdash \text{fix}^m x : \tau \text{ is } e \text{/ } x \text{ is } e
\end{align*}
\]

(49.7a)

(49.7b)

It is straightforward to extend the proof of correctness of the stack machine (Corollary 27.4 on page 240) to account for bounded recursion.

To get a feel for what is involved in the compactness proof, consider first the factorial function, \( f \), in \( \mathcal{L}\{\text{nat} \to \} \):

\[
\text{fix} : \text{nat} \to \text{nat} \text{ is } \lambda (x : \text{nat}. \text{if} z \{ z \Rightarrow s(z) \mid s(x') \Rightarrow x * f(x') \}).
\]

Obviously evaluation of \( f(n) \) requires \( n \) recursive calls to the function itself. This means that, for a given input, \( n \), we may place a \textit{bound}, \( m \), on the recursion that is sufficient to ensure termination of the computation. This can be expressed formally using the \( m \)-bounded form of general recursion,

\[
\text{fix}^m : \text{nat} \to \text{nat} \text{ is } \lambda (x : \text{nat}. \text{if} z \{ z \Rightarrow s(z) \mid s(x') \Rightarrow x * f(x') \}).
\]

Call this expression \( f^{(m)} \). It follows from the definition of \( f \) that if \( f(\pi) \leadsto^* \bar{p} \), then \( f^{(m)}(\pi) \leadsto^* \bar{p} \) for some \( m \geq 0 \) (in fact, \( m = n \) suffices).

When considering expressions of higher type, we cannot expect to get the \textit{same} result from the bounded recursion as from the unbounded. For example, consider the addition function, \( a \), of type \( \tau = \text{nat} \to (\text{nat} \to \text{nat}) \), given by the expression

\[
\text{fix} p : \tau \text{ is } \lambda (x : \text{nat}. \text{if} z \{ z \Rightarrow \text{id} \mid s(x') \Rightarrow s \circ (p(x')) \}),
\]

where \( \text{id} = \lambda (y : \text{nat}. y) \) is the identity, \( e' \circ e = \lambda (x : \tau. e'(e(x))) \) is composition, and \( s = \lambda (x : \text{nat}. s(x)) \) is the successor function. The application
Compactness

$a(\pi)$ terminates after three transitions, regardless of the value of $n$, resulting in a $\lambda$-abstraction. When $n$ is positive, the result contains a residual copy of $a$ itself, which is applied to $n - 1$ as a recursive call. The $m$-bounded version of $a$, written $a^{(m)}$, is also such that $a^{(m)}()$ terminates in three steps, provided that $m > 0$. But the result is not the same, because the residuals of $a$ appear as $a^{(m-1)}$, rather than as $a$ itself.

Turning now to the proof, it is helpful to introduce some notation. Suppose that $x : \tau \vdash e_x : \tau$ for some arbitrary abstractor $x$. Define $f^{(\omega)} = \text{fix } x : \tau \vdash e_x$, and $f^{(m)} = \text{fix }^m x : \tau \vdash e_x$, and observe that $f^{(\omega)} : \tau$ and $f^{(m)} : \tau$ for any $m \geq 0$.

The following technical lemma governing the stack machine permits the bound on “passive” occurrences of a recursive expression to be raised without affecting the outcome of evaluation.

**Lemma 49.12.** If $[f^{(m)}/y]k \triangleright [f^{(m)}/y]e \mapsto^* e \triangleleft \pi$, where $e \neq y$, then $[f^{(m+1)}/y]k \triangleright [f^{(m+1)}/y]e \mapsto^* e \triangleleft \pi$.

**Proof.** By induction on the definition of the transition judgement for $K\{\text{nat} \mapsto \}$. \hfill $\square$

**Theorem 49.13** (Compactness). Suppose that $y : \tau \vdash e : \text{nat}$ where $y \notin f^{(\omega)}$. If $[f^{(\omega)}/y]e \mapsto^* \pi$, then there exists $m \geq 0$ such that $[f^{(m)}/y]e \mapsto^* \pi$.

**Proof.** We prove simultaneously the stronger statements that if

$[f^{(\omega)}/y]k \triangleright [f^{(\omega)}/y]e \mapsto^* e \triangleleft \pi$,

then for some $m \geq 0$,

$[f^{(m)}/y]k \triangleright [f^{(m)}/y]e \mapsto^* e \triangleleft \pi$,

and

$[f^{(\omega)}/y]k \triangleright [f^{(\omega)}/y]e \mapsto^* e \triangleleft \pi$

then for some $m \geq 0$,

$[f^{(m)}/y]k \triangleright [f^{(m)}/y]e \mapsto^* e \triangleleft \pi$.

(Note that if $[f^{(\omega)}/y]e \text{ val}$, then $[f^{(m)}/y]e \text{ val}$ for all $m \geq 0$.) The result then follows by the correctness of the stack machine (Corollary 27.4 on page 240).
49.4 Compactness

We proceed by induction on transition. Suppose that the initial state is

\[
[f^{(ω)} / y]k \triangleright f^{(ω)},
\]

which arises when \(e = y\), and the transition sequence is as follows:

\[
[f^{(ω)} / y]k \triangleright f^{(ω)} \mapsto [f^{(ω)} / y]k \triangleright [f^{(ω)} / x]e_x \mapsto^* e \triangleleft \bar{nil}.
\]

Noting that \([f^{(ω)} / x]e_x = [f^{(ω)} / y / x]e_x\), we have by induction that there exists \(m \geq 0\) such that

\[
[f^{(m)} / y]k \triangleright [f^{(m)} / x]e_x \mapsto^* e \triangleleft \bar{nil}.
\]

By Lemma 49.12 on the preceding page

\[
[f^{(m+1)} / y]k \triangleright [f^{(m)} / x]e_x \mapsto^* e \triangleleft \bar{nil}
\]

and we need only observe that

\[
[f^{(m+1)} / y]k \triangleright f^{(m+1)} \mapsto [f^{(m+1)} / y]k \triangleright [f^{(m)} / x]e_x
\]

to complete the proof. If, on the other hand, the initial step is an unrolling, but \(e \neq y\), then we have for some \(z \notin f^{(ω)}\) and \(z \neq y\)

\[
[f^{(ω)} / y]k \triangleright \text{fix } z : \tau is d_ω \mapsto [f^{(ω)} / y]k \triangleright [\text{fix } z : \tau is d_ω / z]d_ω \mapsto^* e \triangleleft \bar{nil}.
\]

where \(d_ω = [f^{(ω)} / y]d\). By induction there exists \(m \geq 0\) such that

\[
[f^{(m)} / y]k \triangleright [\text{fix } z : \tau is d_m / z]d_m \mapsto^* e \triangleleft \bar{nil},
\]

where \(d_m = [f^{(m)} / y]d\). But then by Lemma 49.12 on the facing page we have

\[
[f^{(m+1)} / y]k \triangleright [\text{fix } z : \tau is d_m+1 / z]d_{m+1} \mapsto^* e \triangleleft \bar{nil},
\]

where \(d_{m+1} = [f^{(m+1)} / y]d\), from which the result follows directly. \(\square\)

**Corollary 49.14.** There exists \(m \geq 0\) such that \([f^{(ω)} / y]e \simeq [f^{(m)} / y]e\).

**Proof.** If \([f^{(ω)} / y]e\) diverges, then taking \(m\) to be zero suffices. Otherwise, apply Theorem 49.13 on the preceding page to obtain \(m\), and note that the required Kleene equivalence follows. \(\square\)
49.5 Co-Natural Numbers

In Chapter 15 we considered a variation of $\mathcal{L}\{\text{nat} \to\}$ with the co-natural numbers, $\conat$, as base type. This is achieved by specifying that $s(e)$ eval regardless of the form of $e$, so that the successor does not evaluate its argument. Using general recursion we may define the infinite number, $\omega$, by $\fix x : \conat \is s(x)$, which consists of an infinite stack of successors. Since the successor is interpreted lazily, $\omega$ evaluates to a value, namely $s(\omega)$, its own successor. It follows that the principle of mathematical induction is not valid for the co-natural numbers. For example, the property of being equivalent to a finite numeral is satisfied by zero and is closed under successor, but fails for $\omega$.

In this section we sketch the modifications to the preceding development for the co-natural numbers. The main difference is that the definition of extensional equivalence at type $\conat$ must be formulated to account for laziness. Rather than being defined inductively as the strongest relation closed under specified conditions, we define it coinductively as the weakest relation consistent two analogous conditions. We may then show that two expressions are related using the principle of proof by coinduction.

If $\conat$ is to continue to serve as the observable outcome of a computation, then we must alter the meaning of Kleene equivalence to account for laziness. We adopt the principle that we may observe of a computation only its outermost form: it is either zero or the successor of some other computation. More precisely, we define $e \simeq e'$ iff (a) if $e \leadsto^* z$, then $e' \leadsto^* z$, and vice versa; and (b) if $e \leadsto^* s(e_1)$, then $e' \leadsto^* s(e'_1)$, and vice versa. Note well that we do not require anything of $e_1$ and $e'_1$ in the second clause. This means that $\tilde{0} \simeq \tilde{1}$, yet we retain consistency in that $\tilde{0} \not\simeq \tilde{1}$.

Corollary 49.14 on the preceding page can be proved for the co-natural numbers by essentially the same argument.

The definition of extensional equivalence at type $\conat$ is defined to be the weakest equivalence relation, $\mathcal{E}$, between closed terms of type $\conat$ satisfying the following $\conat$-consistency conditions: if $e \mathcal{E} e' : \conat$, then

1. If $e \leadsto^* z$, then $e' \leadsto^* z$, and vice versa.
2. If $e \leadsto^* s(e_1)$, then $e' \leadsto^* s(e'_1)$ with $e_1 \mathcal{E} e'_1 : \conat$, and vice versa.

It is immediate that if $e \sim e' : \conat$, then $e \simeq e'$, and so extensional equivalence is consistent. It is also strict in that if $e$ and $e'$ are both divergent expressions of type $\conat$, then $e \sim e' : \conat$—simply because the preceding two conditions are vacuously true in this case.
This is an example of the more general principle of proof by \textit{conat-coinduction}. To show that $e \sim e' : \text{conat}$, it suffices to exhibit a relation, $E$, such that

1. $e \ E \ e' : \text{conat}$, and

2. $E$ satisfies the \text{conat}-consistency conditions.

If these requirements hold, then $E$ is contained in extensional equivalence at type \text{conat}, and hence $e \sim e' : \text{conat}$, as required.

As an application of \text{conat-coinduction}, let us consider the proof of Theorem 49.5 on page 455. The overall argument remains as before, but the proof for the type \text{conat} must be altered as follows. Suppose that $A \approx A' : \rho \rightsquivalence \text{conat}$, and let $a = A\{\text{fix} \ x : \check{\rho} \ is \ e\}$ and $a' = A'\{\text{fix} \ x : \check{\rho} \ is \ e'\}$. Writing $a^{(m)} = A\{\text{fix}^m \ x : \check{\rho} \ is \ e\}$ and $a'^{(m)} = A'\{\text{fix}^m \ x : \check{\rho} \ is \ e'\}$, assume that

$$for \ every \ m \geq 0, \ a^{(m)} \sim a'^{(m)} : \text{conat}.$$ 

We are to show that

$$a \sim a' : \text{conat}.$$ 

Define the functions $p_n$ for $n \geq 0$ on closed terms of type \text{conat} by the following equations:

$$p_0(d) = d$$

$$p_{n+1}(d) = \begin{cases} d' & \text{if } p_n(d) \rightsquivalence^* s(d') \\ \text{undefined} & \text{otherwise} \end{cases}$$

For $n \geq 0$, let $a_n = p_n(a)$ and $a'_n = p_n(a')$. Correspondingly, let $a^{(m)}_n = p_n(a^{(m)})$ and $a'^{(m)}_n = p_n(a'^{(m)})$. Define $E$ to be the strongest relation such that $a_n \ E \ a'_n : \text{conat}$ for all $n \geq 0$. We will show that the relation $E$ satisfies the \text{conat}-consistency conditions, and so it is contained in extensional equivalence. Since $a \ E a' : \text{conat}$ (by construction), the result follows immediately.

To show that $E$ is \text{conat}-consistent, suppose that $a_n \ E a'_n : \text{conat}$ for some $n \geq 0$. We have by Corollary 49.14 on page 461 $a_n \simeq a^{(m)}_n$, for some $m \geq 0$, and hence, by the assumption, $a_n \simeq a'^{(m)}_n$, and so by Corollary 49.14 on page 461 again, $a^{(m)}_n \simeq a'^{(m)}_n$. Now if $a_n \rightsquivalence s(b_n)$, then $a^{(m)}_n \rightsquivalence s(b^{(m)}_n)$ for some $b^{(m)}_n$, and hence there exists $b^{(m)}_n$ such that $a^{(m)}_n \rightsquivalence b^{(m)}_n$, and so there exists $b'_n$ such that $a'_n \rightsquivalence s(b'_n)$. But $b_n = p_{n+1}(a)$ and $b'_n = p_{n+1}(a')$, and we have $b_n \ E b'_n : \text{conat}$ by construction, as required.
49.6 Exercises

1. Call-by-value variant, with recursive functions.
Chapter 50

Parametricity

The motivation for introducing polymorphism was to enable more programs to be written — those that are “generic” in one or more types, such as the composition function given in Chapter 23. Then if a program does not depend on the choice of types, we can code it using polymorphism. Moreover, if we wish to insist that a program can not depend on a choice of types, we demand that it be polymorphic. Thus polymorphism can be used both to expand the class of programs we may write, and also to limit the class of programs that are permissible in a given context.

The restrictions imposed by polymorphic typing give rise to the experience that in a polymorphic functional language, if the types are correct, then the program is correct. Roughly speaking, if a function has a polymorphic type, then the strictures of type genericity vastly cut down the set of programs with that type. Thus if you have written a program with this type, it is quite likely to be the one you intended!

The technical foundation for these remarks is called parametricity. The goal of this chapter is to give an account of parametricity for $\mathcal{L}\{\rightarrow\forall\}$ under a call-by-name interpretation.

50.1 Overview

We will begin with an informal discussion of parametricity based on a “seat of the pants” understanding of the set of well-formed programs of a type.

Suppose that a function value $f$ has the type $\forall(t.t \rightarrow t)$. What function could it be? When instantiated at a type $\tau$ it should evaluate to a function $g$ of type $\tau \rightarrow \tau$ that, when further applied to a value $v$ of type $\tau$ returns a value $v'$ of type $\tau$. Since $f$ is polymorphic, $g$ cannot depend on $v$, so $v'$
must be \( v \). In other words, \( g \) must be the identity function at type \( \tau \), and \( f \) must therefore be the \textit{polymorphic identity}.

Suppose that \( f \) is a function of type \( \forall (t.t) \). What function could it be? A moment’s thought reveals that it cannot exist at all! For it must, when instantiated at a type \( \tau \), return a value of that type. But not every type has a value (including this one), so this is an impossible assignment. The only conclusion is that \( \forall (t.t) \) is an \textit{empty} type.

Let \( N \) be the type of polymorphic Church numerals introduced in Chapter 23, namely \( \forall (t.t \to (t \to t) \to t) \). What are the values of this type? Given any type \( \tau \), and values \( z : \tau \) and \( s : \tau \to \tau \), the expression

\[
f[\tau](z)(s)
\]

must yield a value of type \( \tau \). Moreover, it must behave uniformly with respect to the choice of \( \tau \). What values could it yield? The only way to build a value of type \( \tau \) is by using the element \( z \) and the function \( s \) passed to it. A moment’s thought reveals that the application must amount to the \( n \)-fold composition

\[
s(s(\ldots s(z)\ldots)).
\]

That is, the elements of \( N \) are in one-to-one correspondence with the natural numbers.

### 50.2 Observational Equivalence

The definition of observational equivalence given in Chapters 48 and 49 is based on identifying a type of \textit{answers} that are observable outcomes of complete programs. Values of function type are not regarded as answers, but are treated as “black boxes” with no internal structure, only input-output behavior. In \( L\{\to\forall\} \), however, there are no (closed) base types! Every type is either a function type or a polymorphic type, and hence no types suitable to serve as observable answers.

One way to manage this difficulty is to augment \( L\{\to\forall\} \) with a base type of answers to serve as the observable outcomes of a computation. The only requirement is that this type have two elements that can be immediately distinguished from each other by evaluation. We may achieve this by enriching \( L\{\to\forall\} \) with a base type, \( 2 \), containing two constants, \( \text{tt} \) and \( \text{ff} \), that serve as possible answers for a complete computation. A complete program is a closed expression of type \( 2 \).

Kleene equivalence is defined for complete programs by requiring that \( e \simeq e' \) iff either (a) \( e \xrightarrow{\ast} \text{tt} \) and \( e' \xrightarrow{\ast} \text{tt} \); or (b) \( e \xrightarrow{\ast} \text{ff} \) and \( e' \xrightarrow{\ast} \text{ff} \).
This is obviously an equivalence relation, and it is immediate that \( \text{tt} \not\sim \text{ff} \), since these are two distinct constants. As before, we say that a type-indexed family of equivalence relations between closed expressions of the same type is consistent if it implies Kleene equivalence at the answer type, 2.

To define observational equivalence, we must first define the concept of an expression context for \( L \to \forall \) as an expression with a “hole” in it. More precisely, we may give an inductive definition of the judgement

\[
C : (\Delta; \Gamma \triangleright \tau) \rightharpoonup (\Delta'; \Gamma' \triangleright \tau'),
\]

which states that \( C \) is an expression context that, when filled with an expression \( \Delta; \Gamma \vdash e : \tau \) yields an expression \( \Delta'; \Gamma' \vdash C\{e\} : \tau \). (We leave the precise definition of this judgement, and the verification of its properties, as an exercise for the reader.)

**Definition 50.1.** Two expressions of the same type are observationally equivalent, written \( e \equiv e' : \tau [\Delta; \Gamma] \), iff \( C\{e\} \simeq C\{e'\} \) whenever \( C : (\Delta; \Gamma \triangleright \tau) \rightharpoonup (\emptyset \triangleright 2) \).

**Lemma 50.1.** Observational equivalence is the coarsest consistent congruence.

**Proof.** The composition of a program context with another context is itself a program context. It is consistent by virtue of the empty context being a program context.

**Lemma 50.2.**

1. If \( e \equiv e' : \tau [\Delta, t; \Gamma] \) and \( \rho \) type, then \( [\rho/t]e \equiv [\rho/t]e' : [\rho/t]\tau [\Delta; [\rho/t]\Gamma] \).

2. If \( e \equiv e' : \tau [\emptyset; \Gamma, x : \sigma] \) and \( d : \sigma \), then \( [d/x]e \equiv [d/x]e' : \tau [\emptyset; \Gamma] \). Moreover, if \( d \equiv d' : \sigma \), then \( [d/x]e \equiv [d'/x]e : \tau [\emptyset; \Gamma] \), and similarly for \( e' \).

**Proof.**

1. Let \( C : (\Delta; [\rho/t]\Gamma \triangleright [\rho/t]\tau) \rightharpoonup (\emptyset \triangleright 2) \) be a program context. We are to show that

\[
C\{[\rho/t]e\} \simeq C\{[\rho/t]e'\}.
\]

Since \( C \) is closed, this is equivalent to

\[
[\rho/t]C\{e\} \simeq [\rho/t]C\{e'\}.
\]
Let $C'$ be the context $\Lambda (t. C\{\circ\}) [\rho]$, and observe that

$$C' : (\Delta, t; \Gamma \triangleright \tau) \leadsto (\emptyset \triangleright 2).$$

Therefore, from the assumption,

$$C'\{e\} \simeq C'\{e'\}.$$

But $C'\{e\} \simeq [\rho/t]C\{e\}$, and $C'\{e'\} \simeq [\rho/t]C\{e'\}$, from which the result follows.

2. By an argument essentially similar to that for Lemma 48.5 on page 445.

\[\square\]

## 50.3 Logical Equivalence

In this section we introduce a form of logical equivalence that captures the informal concept of parametricity, and also provides a characterization of observational equivalence. This will permit us to derive properties of observational equivalence of polymorphic programs of the kind suggested earlier.

The definition of logical equivalence for $L\{\rightarrow \forall\}$ is somewhat more complex than for $L\{\text{nat} \rightarrow\}$. The main idea is to define logical equivalence for a polymorphic type, $\forall (t. \tau)$ to satisfy a very strong condition that captures the essence of parametricity. As a first approximation, we might say that two expressions, $e$ and $e'$, of this type should be logically equivalent if they are logically equivalent for “all possible” interpretations of the type $t$. More precisely, we might require that $e[\rho]$ be related to $e'[\rho]$ at type $[\rho/t]\tau$, for any choice of type $\rho$. But this runs into two problems, one technical, the other conceptual. The same device will be used to solve both problems.

The technical problem stems from impredicativity. In Chapter 48 logical equivalence is defined by induction on the structure of types. But when polymorphism is impredicative, the type $[\rho/t]\tau$ might well be larger than $\forall (t. \tau)!$ At the very least we would have to justify the definition of logical equivalence on some other grounds, but no criterion appears to be available. The conceptual problem is that, even if we could make sense of the definition of logical equivalence, it would be too restrictive. For such a definition amounts to saying that the unknown type $t$ is to be interpreted as logical equivalence at whatever type it turns out to be when instantiated.
To obtain useful parametricity results, we shall ask for much more than this. What we shall do is to consider separately instances of $e$ and $e'$ by types $\rho$ and $\rho'$, and treat the type variable $t$ as standing for any relation (of a suitable class) between $\rho$ and $\rho'$. One may suspect that this is asking too much: perhaps logical equivalence is the empty relation! Surprisingly, this is not the case, and indeed it is this very feature of the definition that we shall exploit to derive parametricity results about the language.

To manage both of these problems we will consider a generalization of logical equivalence that is parameterized by a relational interpretation of the free type variables of its classifier. The parameters determine a separate binding for each free type variable in the classifier for each side of the equation, with the discrepancy being mediated by a specified relation between them. This permits us to consider a notion of “equivalence” between two expressions of different type—they are equivalent, modulo a relation between the interpretations of their free type variables.

We will restrict attention to a certain class of “admissible” binary relations between closed expressions. The conditions are imposed to ensure that logical equivalence and observational equivalence coincide.

**Definition 50.2 (Admissibility).** A relation $R$ between expressions of types $\rho$ and $\rho'$ is admissible, written $R : \rho \leftrightarrow \rho'$, iff it satisfies two requirements:

1. Respect for observational equivalence: if $R(e, e')$ and $d \equiv e : \rho$ and $d' \equiv e' : \rho'$, then $R(d, d')$.

2. Closure under converse evaluation: if $R(e, e')$, then if $d \mapsto e$, then $R(d, e')$ and if $d' \mapsto e'$, then $R(e, d')$.

The second of these conditions will turn out to be a consequence of the first, but we are not yet in a position to establish this fact.

The judgement $\delta : \Delta$ states that $\delta$ is a type substitution that assigns a closed type to each type variable $t \in \Delta$. A type substitution, $\delta$, induces a substitution function, $\hat{\delta}$, on types given by the equation

$$\hat{\delta}(\tau) = [\delta(t_1), \ldots, \delta(t_n)/t_1, \ldots, t_n] \tau,$$

and similarly for expressions. Substitution is extended to contexts pointwise by defining $\hat{\delta}(\Gamma)(x) = \hat{\delta}(\Gamma(x))$ for each $x \in \text{dom}(\Gamma)$.

Let $\delta$ and $\delta'$ be two type substitutions of closed types to the type variables in $\Delta$. A relation assignment, $\eta$, between $\delta$ and $\delta'$ is an assignment of an admissible relation $\eta(t) : \delta(t) \leftrightarrow \delta'(t)$ to each $t \in \Delta$. The judgement $\eta : \delta \leftrightarrow \delta'$ states that $\eta$ is a relation assignment between $\delta$ and $\delta'$. 

**DECEMBER 18, 2009**
Logical equivalence is defined in terms of its generalization, called \textit{parametric logical equivalence}, written $e \sim e' : \tau [\eta : \delta \rightarrow \delta']$, defined as follows.

\textbf{Definition 50.3} (Parametric Logical Equivalence). The relation $e \sim e' : \tau [\eta : \delta \rightarrow \delta']$ is defined by induction on the structure of $\tau$ by the following conditions:

\begin{align*}
e \sim e' : t [\eta : \delta \rightarrow \delta'] & \iff \eta(t)(e,e') \\
e \sim e' : 2 [\eta : \delta \rightarrow \delta'] & \iff e \simeq e' \\
e \sim e' : \tau_1 \rightarrow \tau_2 [\eta : \delta \rightarrow \delta'] & \iff e_1 \sim e_1' : \tau_1 [\eta : \delta \rightarrow \delta'] \text{ implies } e(e_1) \sim e'(e_1') : \tau_2 [\eta : \delta \rightarrow \delta'] \\
e \sim e' : \forall (t.\tau) [\eta : \delta \rightarrow \delta'] & \iff \text{ for every } \rho, \rho', \text{ and every } R : \rho \rightarrow \rho', \\
 & \quad e[\rho] \sim e'[\rho'][t : \tau] : \tau [\eta[t \rightarrow R] : \delta[t \rightarrow \rho] \rightarrow \delta'[t \rightarrow \rho']] \end{align*}

Logical equivalence is defined in terms of parametric logical equivalence by considering all possible interpretations of its free type- and expression variables. An \textit{expression substitution}, $\gamma$, for a context $\Gamma$, written $\gamma : \Gamma$, is an substitution of a closed expression $\gamma(x) : \Gamma(x)$ to each variable $x \in \text{dom}(\Gamma)$. An expression substitution, $\gamma : \Gamma$, induces a substitution function, $\hat{\gamma}$, defined by the equation

$$\hat{\gamma}(e) = [\gamma(x_1), \ldots, \gamma(x_n)]e,$$

where the domain of $\Gamma$ consists of the variables $x_1, \ldots, x_n$.

The relation $\gamma \sim \gamma' : \Gamma [\eta : \delta \rightarrow \delta']$ is defined to hold iff $\text{dom}(\gamma) = \text{dom}(\gamma') = \text{dom}(\Gamma)$, and $\gamma(x) \sim \gamma'(x) : \Gamma(x) [\eta : \delta \rightarrow \delta']$ for every variable, $x$, in their common domain.

\textbf{Definition 50.4} (Logical Equivalence). The expressions $\Delta;\Gamma \vdash e : \tau$ and $\Delta;\Gamma \vdash e' : \tau$ are \textit{logically equivalent}, written $e \sim e' : \tau [\Delta;\Gamma]$ iff for every assignment $\delta$ and $\delta'$ of closed types to type variables in $\Delta$, and every relation assignment $\eta : \delta \rightarrow \delta'$, if $\gamma \sim \gamma' : \Gamma [\eta : \delta \rightarrow \delta']$, then $\hat{\gamma}(\delta)(e)) \sim \hat{\gamma'}(\delta')(e') : \tau [\eta : \delta \rightarrow \delta']$.

When $e$, $e'$, and $\tau$ are closed, then this definition states that $e \sim e' : \tau$ iff $e \sim e' : \tau [\emptyset : \emptyset \leftarrow \emptyset]$, so that logical equivalence is indeed a special case of its generalization.

\textbf{Lemma 50.3} (Closure under Converse Evaluation). Suppose that $e \sim e' : \tau [\eta : \delta \rightarrow \delta']$. If $d \rightarrow e$, then $d \sim e' : \tau$, and if $d' \rightarrow e'$, then $e \sim d' : \tau$.

\textit{Proof.} By induction on the structure of $\tau$. When $\tau = t$, the result holds by the definition of admissibility. Otherwise the result follows by induction, making use of the definition of the transition relation for applications and type applications. $\square$
Lemma 50.4 (Respect for Observational Equivalence). Suppose that \( e \sim e' : \tau [\eta : \delta \leftrightarrow \delta'] \). If \( d \equiv e : \delta(\tau) \) and \( d' \equiv e' : \delta'(\tau) \), then \( d \sim d' : \tau [\eta : \delta \leftrightarrow \delta'] \).

Proof. By induction on the structure of \( \tau \), relying on the definition of admissibility, and the congruence property of observational equivalence. For example, if \( \tau = \forall (t . \sigma) \), then we are to show that for every \( R : \rho \leftrightarrow \rho' \),

\[
d[\rho] \sim d'[\rho'] : \sigma [\eta[t \mapsto R] : \delta[t \mapsto \rho] \leftrightarrow \delta'[t \mapsto \rho']].
\]

Since observational equivalence is a congruence, \( d[\rho] \equiv e[\rho] : [\rho/t]\delta(\sigma) \), \( d'[\rho] \equiv e'[\rho] : [\rho'/t]\delta'(\sigma) \). From the assumption it follows that

\[
e[\rho] \sim e'[\rho'] : \sigma [\eta[t \mapsto R] : \delta[t \mapsto \rho] \leftrightarrow \delta'[t \mapsto \rho']],
\]

from which the result follows by induction. \( \Box \)

Corollary 50.5. The relation \( e \sim e' : \tau [\eta : \delta \leftrightarrow \delta'] \) is an admissible relation between closed types \( \delta(\tau) \) and \( \delta'(\tau) \).

Proof. By Lemmas 50.3 on the preceding page and 50.4. \( \Box \)

Logical Equivalence respects observational equivalence.

Corollary 50.6. If \( e \sim e' : \tau [\Delta; \Gamma] \), and \( d \equiv e : \tau [\Delta; \Gamma] \) and \( d' \equiv e' : \tau [\Delta; \Gamma] \), then \( d \sim d' : \tau [\Delta; \Gamma] \).

Proof. By Lemma 50.2 on page 467 and Corollary 50.5. \( \Box \)

Lemma 50.7 (Compositionality). Suppose that

\[
e \sim e' : \tau [\eta[t \mapsto R] : \delta[t \mapsto \delta(\rho)] \leftrightarrow \delta'[t \mapsto \delta'(\rho)]],
\]

where \( R : \delta(\rho) \leftrightarrow \delta'(\rho) \) is such that \( R(d, d') \) holds iff \( d \sim d' : \rho [\eta : \delta \leftrightarrow \delta'] \). Then \( e \sim e' : [\rho/t]\tau [\eta : \delta \leftrightarrow \delta'] \).

Proof. By induction on the structure of \( \tau \). When \( \tau = t \), the result is immediate from the definition of the relation \( R \). When \( \tau = t' \neq t \), the result holds vacuously. When \( \tau = \tau_1 \rightarrow \tau_2 \) or \( \tau = \forall (u . \tau) \), where without loss of generality \( u \neq t \) and \( u \notin \rho \), the result follows by induction. \( \Box \)
Despite the strong conditions on polymorphic types, logical equivalence is not overly restrictive—every expression satisfies its constraints. This result is sometimes called the \textit{parametricity theorem}.

\textbf{Theorem 50.8 (Parametricity).} If $\Delta; \Gamma \vdash e : \tau$, then $e \sim e : \tau$ [\(\Delta; \Gamma\)].

\textit{Proof.} By rule induction on the static semantics of $L\{\rightarrow \forall\}$ given by Rules (23.2).

We consider two representative cases here.

\textbf{Rule (23.2d)} Suppose $\delta : \Delta, \delta' : \Delta, \eta : \delta \leftrightarrow \delta'$, and $\gamma \sim \gamma' : \Gamma [\eta : \delta \leftrightarrow \delta']$.

By induction we have that for all $\rho, \rho'$, and $R : \rho \leftrightarrow \rho'$,

\[ [\rho/t] \hat{\gamma}(\delta(e)) \sim [\rho'/t] \hat{\gamma}'(\delta'(e)) : \tau [\eta_* : \delta_* \leftrightarrow \delta'_*], \]

where $\eta_* = \eta [t \mapsto R], \delta_* = \delta [t \mapsto \rho]$, and $\delta'_* = \delta'[t \mapsto \rho']$. Since

\[ \Lambda(t. \hat{\gamma}(\delta(e))) [\rho] \rightsquigarrow [\rho/t] \hat{\gamma}(\delta(e)) \]

and

\[ \Lambda(t. \hat{\gamma}'(\delta'(e))) [\rho'] \rightsquigarrow [\rho'/t] \hat{\gamma}'(\delta'(e)), \]

the result follows by Lemma 50.3 on page 470.

\textbf{Rule (23.2e)} Suppose $\delta : \Delta, \delta' : \Delta, \eta : \delta \leftrightarrow \delta'$, and $\gamma \sim \gamma' : \Gamma [\eta : \delta \leftrightarrow \delta']$.

By induction we have

\[ \hat{\gamma}(\delta(e)) \sim \hat{\gamma}'(\delta'(e)) : \forall (t. \tau) [\eta : \delta \leftrightarrow \delta'] \]

Let $\hat{\delta} = \hat{\delta}(\rho)$ and $\hat{\delta}' = \hat{\delta}'(\rho)$. Define the relation $R : \hat{\delta} \leftrightarrow \hat{\delta}'$ by $R(\hat{d}, \hat{d}')$ iff $d \sim d' : \rho [\eta : \delta \leftrightarrow \delta']$. By Corollary 50.5 on the preceding page, this relation is admissible.

By the definition of logical equivalence at polymorphic types, we obtain

\[ \hat{\gamma}(\delta(e)) [\rho] \sim \hat{\gamma}'(\delta'(e)) [\hat{\rho}'] : \tau [\eta[t \mapsto R] : \delta [t \mapsto \hat{\rho}] \leftrightarrow \delta'[t \mapsto \hat{\rho}']]. \]

By Lemma 50.7 on the previous page

\[ \hat{\gamma}(\delta(e)) [\rho] \sim \hat{\gamma}'(\delta'(e)) [\hat{\rho}'] : [\rho/t] \tau [\eta : \delta \leftrightarrow \delta'] \]

But

\begin{align*}
\hat{\gamma}(\delta(e)) [\rho] & = \hat{\gamma}(\delta(e)) [\delta(\rho)] \quad (50.1) \\
& = \hat{\gamma}(\delta(\rho)) , \quad (50.2)
\end{align*}
and similarly
\[
\hat{\gamma'}(\hat{\delta'}(\hat{\rho'})) = \hat{\gamma'}(\hat{\delta'}(e)) \tau
\]
\[
= \hat{\gamma'}(\hat{\delta'}(e)) \tau,
\]
(50.3)
(50.4)

from which the result follows.

Corollary 50.9. If \( e \equiv e' : \tau [\Delta; \Gamma] \), then \( e \sim e' : \tau [\Delta; \Gamma] \).

Proof. By Theorem 50.8 on the facing page, \( e \sim e : \tau [\Delta; \Gamma] \), and hence by Corollary 50.6 on page 471, \( e \sim e' : \tau [\Delta; \Gamma] \).

Lemma 50.10 (Congruence). If \( e \sim e' : \tau [\Delta; \Gamma] \) and \( C : (\Delta; \Gamma \triangleright \tau) \sim (\Delta'; \Gamma' \triangleright \tau') \), then \( C \{ e \} \sim C \{ e' \} : \tau [\Delta'; \Gamma'] \).

Proof. By induction on the structure of \( C \), following along very similar lines to the proof of Theorem 50.8 on the facing page.

Lemma 50.11 (Consistency). Logical equivalence is consistent.

Proof. Follows immediately from the definition of logical equivalence.

Corollary 50.12. If \( e \sim e' : \tau [\Delta; \Gamma] \), then \( e \equiv e' : \tau [\Delta; \Gamma] \).

Proof. By Lemma 50.11 Logical equivalence is consistent, and by Lemma 50.10, it is a congruence, and hence is contained in observational equivalence.

Corollary 50.13. Logical and observational equivalence coincide.

Proof. By Corollaries 50.9 and 50.12.

Therefore if a relation respects observational equivalence, it must also be closed under converse evaluation. This shows that the second condition on admissibility is redundant, though it cannot be omitted at such an early stage.
50.4 Parametricity Properties

The parametricity theorem enables us to deduce properties of expressions of $\mathcal{L}\{-\forall\}$ that hold solely because of their type. The stringencies of parametricity ensure that a polymorphic type has very few inhabitants. For example, we may prove that every expression of type $\forall(t. t \to t)$ behaves like the identity function.

**Theorem 50.14.** Let $e : \forall(t. t \to t)$ be arbitrary, and let $id$ be $\Lambda(t. \lambda(x : t). x)$. Then $e \equiv id : \forall(t. t \to t)$.

**Proof.** By Corollary 50.13 on the preceding page it is sufficient to show that $e \sim id : \forall(t. t \to t)$. Let $\rho$ and $\rho'$ be arbitrary closed types, let $R : \rho \leftrightarrow \rho'$ be an admissible relation, and suppose that $e_0 R e'_0$. We are to show

$$e[\rho](e_0) R id[\rho](e'_0),$$

which, given the definition of $id$, is to say

$$e[\rho](e_0) R e'_0.$$

It suffices to show that $e[\rho](e_0) \equiv e_0 : \rho$, for then the result follows by the admissibility of $R$ and the assumption $e_0 R e'_0$.

By Theorem 50.8 on page 472 we have $e \sim e : \forall(t. t \to t)$. Let the relation $S : \rho \leftrightarrow \rho$ be defined by $d S d'$ iff $d \equiv e_0 : \rho$ and $d' \equiv e_0 : \rho$. This is clearly admissible, and we have $e_0 S e_0$. It follows that

$$e[\rho](e_0) S e[\rho](e_0),$$

and so, by the definition of the relation $S$, $e[\rho](e_0) \equiv e_0 : \rho$.

In Chapter 23 we showed that product, sum, and natural numbers types are all definable in $\mathcal{L}\{-\forall\}$. The proof of definability in each case consisted of showing that the type and its associated introduction and elimination forms are encodable in $\mathcal{L}\{-\forall\}$. The encodings are correct in the (weak) sense that the dynamic semantics of these constructs as given in the earlier chapters is derivable from the dynamic semantics of $\mathcal{L}\{-\forall\}$ via these definitions. By taking advantage of parametricity we may extend these results to obtain a strong correspondence between these types and their encodings.
As a first example, let us consider the representation of the unit type, \( \text{unit} \), in \( \mathcal{L}\{\rightarrow\forall\} \), as defined in Chapter 23 by the following equations:

\[
\begin{align*}
\text{unit} &= \forall (r. r \rightarrow r) \\
\langle \rangle &= \Lambda (r. \lambda (x: r. r) (x))
\end{align*}
\]

It is easy to see that \( \langle \rangle : \text{unit} \) according to these definitions. But this merely says that the type \( \text{unit} \) is inhabited (has an element). What we would like to know is that, up to observational equivalence, the expression \( \langle \rangle \) is the only element of that type. But this is precisely the content of Theorem 50.14 on the facing page! We say that the type \( \text{unit} \) is strongly definable within \( \mathcal{L}\{\rightarrow\forall\} \).

Continuing in this vein, let us examine the definition of the binary product type in \( \mathcal{L}\{\rightarrow\forall\} \), also given in Chapter 23:

\[
\begin{align*}
\tau_1 \times \tau_2 &= \forall (r. (\tau_1 \rightarrow \tau_2 \rightarrow r) \rightarrow r) \\
\langle e_1, e_2 \rangle &= \Lambda (r. \lambda (x: \tau_1 \rightarrow \tau_2 \rightarrow r. x (e_1) (e_2))) \\
e \cdot 1 &= e [\tau_1] (\lambda (x: \tau_1. \lambda (y: \tau_2. x))) \\
e \cdot r &= e [\tau_2] (\lambda (x: \tau_1. \lambda (y: \tau_2. y)))
\end{align*}
\]

It is easy to check that \( \langle e_1, e_2 \rangle \cdot 1 \cong e_1 : \tau_1 \) and \( \langle e_1, e_2 \rangle \cdot r \cong e_2 : \tau_2 \) by a direct calculation.

We wish to show that the ordered pair, as defined above, is the unique such expression, and hence that Cartesian products are strongly definable in \( \mathcal{L}\{\rightarrow\forall\} \). We will make use of a lemma governing the behavior of the elements of the product type whose proof relies on Theorem 50.8 on page 472.

**Lemma 50.15.** If \( e : \tau_1 \times \tau_2 \), then \( e \cong \langle e_1, e_2 \rangle \) for some \( e_1 : \tau_1 \) and \( e_2 : \tau_2 \).

**Proof.** Expanding the definitions of pairing and the product type, and applying Corollary 50.13 on page 473, we let \( \rho \) and \( \rho' \) be arbitrary closed types, and let \( R : \rho \leftrightarrow \rho' \) be an admissible relation between them. Suppose further that

\[
h \sim h' : \tau_1 \rightarrow \tau_2 \rightarrow t [\eta : \delta \leftrightarrow \delta'],
\]

where \( \eta(t) = R, \delta(t) = \rho, \) and \( \delta'(t) = \rho' \) (and are each undefined on \( t' \neq t \)). We are to show that for some \( e_1 : \tau_1 \) and \( e_2 : \tau_2 \),

\[
e[\rho] (h) \sim h' (e_1) (e_2) : t [\eta : \delta \leftrightarrow \delta'],
\]
which is to say
\[ e[\rho](h) \ R h'(e_1)(e_2). \]

Now by Theorem 50.8 on page 472 we have \( e \sim e : \tau_1 \times \tau_2 \). Define the relation \( S : \rho \leftrightarrow \rho' \) by \( d S d' \) if the following conditions are satisfied:

1. \( d \sim h(d_1)(d_2) : \rho \) for some \( d_1 : \tau_1 \) and \( d_2 : \tau_2 \);
2. \( d' \sim h'(d'_1)(d'_2) : \rho' \) for some \( d'_1 : \tau_1 \) and \( d'_2 : \tau_2 \);
3. \( d R d' \).

This is clearly an admissible relation. Noting that \( h \sim h' : \tau_1 \rightarrow \tau_2 \rightarrow t[\eta' : \delta' \leftrightarrow \delta] \), where \( \eta'(t) = S \) and is undefined for \( t' \neq t \), we conclude that \( e[\rho](h) \ S e[\rho'](h') \), and hence
\[ e[\rho](h) \ R h'(d'_1)(d'_2), \]
as required.

Now suppose that \( e : \tau_1 \times \tau_2 \) is such that \( e \cdot 1 \cong e_1 : \tau_1 \) and \( e \cdot x \cong e_2 : \tau_2 \). We wish to show that \( e \cong \langle e_1, e_2 \rangle : \tau_1 \times \tau_2 \). From Lemma 50.15 on the preceding page it is easy to deduce that \( e \cong \langle e \cdot 1, e \cdot x \rangle : \tau_1 \times \tau_2 \) by congruence and direct calculation. Hence, by congruence we have \( e \cong \langle e_1, e_2 \rangle : \tau_1 \times \tau_2 \).

By a similar line of reasoning we may show that the Church encoding of the natural numbers given in Chapter 23 strongly defines the natural numbers in that the following properties hold:

1. natiter \( z \{ z \Rightarrow e_0 \mid s(x) \Rightarrow e_1 \} \cong e_0 : \rho. \)
2. natiter \( s(e) \{ z \Rightarrow e_0 \mid s(x) \Rightarrow e_1 \} \cong \text{natiter } e \{ z \Rightarrow e_0 \mid s(x) \Rightarrow e_1 \} / x | e_1 : \rho. \)
3. Suppose that \( x : \text{nat} \vdash r(x) : \rho \). If
   (a) \( r(z) \cong e_0 : \rho \), and
   (b) \( r(s(e)) \cong [r(e) / x]e_1 : \rho, \)
   then for every \( e : \text{nat}, r(e) \cong \text{natiter } e \{ z \Rightarrow e_0 \mid s(x) \Rightarrow e_1 \} : \rho. \)
The first two equations, which constitute weak definability, are easily established by calculation, using the definitions given in Chapter 23. The third property, the unicity of the iterator, is proved using parametricity by showing that every closed expression of type \( \text{nat} \) is observationally equivalent to a numeral \( n \). We then argue for unicity of the iterator by mathematical induction on \( n \geq 0 \).

**Lemma 50.16.** If \( e : \text{nat} \), then either \( e \equiv z : \text{nat} \), or there exists \( e' : \text{nat} \) such that \( e \equiv s(e') : \text{nat} \). Consequently, there exists \( n \geq 0 \) such that \( e \equiv \bar{n} : \text{nat} \).

**Proof.** By Theorem 50.8 on page 472 we have \( e \sim e : \text{nat} \). Define the relation \( R : \text{nat} \leftrightarrow \text{nat} \) to be the strongest relation such that \( d \sim z : \text{nat} \) and \( d' \sim z : \text{nat} \), or \( d \equiv s(d_1) : \text{nat} \) and \( d' \equiv s(d'_1) : \text{nat} \) and \( d_1 \sim d'_1 \). It is easy to see that \( z \sim z \), and if \( e \sim e' \), then \( s(e) \sim s(e') \). Letting \( \text{zero} = z \) and \( \text{succ} = \lambda (x : \text{nat}). s(x) \), we have

\[
e_{\text{nat}}(\text{zero})(\text{succ}) \sim e_{\text{nat}}(\text{zero})(\text{succ}).
\]

The result follows by the induction principle arising from the definition of \( R \) as the strongest relation satisfying its defining conditions.

A straightforward extension of this argument shows that, up to observational equivalence, inductive and coinductive types are strongly definable in \( \mathcal{L}\{\rightarrow \forall\} \).

## 50.5 Exercises
Part XIX

Working Drafts of Chapters