Type systems for programming languages

Didier Rémy

Academic year 2020-2021
Version of October 18, 2022
# Contents

1 Introduction .................................................. 9
   1.1 Overview of the course .................................... 9
   1.2 Requirements ............................................. 11
   1.3 About Functional Programming ............................ 11
   1.4 About Types ................................................ 11
   1.5 Acknowledgment ............................................. 13

2 The untyped $\lambda$-calculus ................................... 15
   2.1 Syntax .................................................... 15
   2.2 Semantics ................................................ 17
      2.2.1 Strong v.s. weak reduction strategies ............... 17
      2.2.2 Call-by-value semantics ............................ 18
   2.3 Answers to exercises ..................................... 20

3 Simply-typed lambda-calculus .................................... 23
   3.1 Syntax .................................................... 23
   3.2 Dynamic semantics ....................................... 23
   3.3 Type system .............................................. 24
   3.4 Type soundness ........................................... 27
      3.4.1 Proof of subject reduction ......................... 28
      3.4.2 Proof of progress .................................. 30
   3.5 Simple extensions ...................................... 32
      3.5.1 Unit ............................................... 32
      3.5.2 Boolean ........................................... 32
      3.5.3 Pairs .............................................. 33
      3.5.4 Sums ............................................... 34
      3.5.5 Modularity of extensions ............................ 34
      3.5.6 Recursive functions ................................. 35
      3.5.7 A derived construct: let-bindings ................... 35
   3.6 Exceptions .............................................. 37
      3.6.1 Semantics .......................................... 37
CONTENTS

3.6.2 Typing rules ............................................ 38
3.6.3 Variations ............................................... 39

3.7 References .................................................. 41
3.7.1 Language definition .................................... 41
3.7.2 Type soundness .......................................... 43
3.7.3 Tracing effects with a monad ......................... 44
3.7.4 Memory deallocation .................................. 45

3.8 Ommitted proofs and answers to exercises ............... 46

4 Polymorphism and System $\mathbf{F}$ ............................. 51
4.1 Polymorphism ................................................. 51
4.2 Polymorphic $\lambda$-calculus ............................... 53
4.2.1 Types and typing rules ................................. 53
4.2.2 Semantics ................................................. 54
4.2.3 Extended System $\mathbf{F}$ with datatypes .......... 56
4.3 Type soundness .............................................. 60
4.4 Type erasing semantics ................................... 64
4.4.1 Implicitly-typed System $\mathbf{F}$ ...................... 64
4.4.2 Type instance ............................................. 67
4.4.3 Type containment in System $\mathbf{F}$, ............... 68
4.4.4 A definition of principal typings .................... 70
4.4.5 Type soundness for implicitly-typed System $\mathbf{F}$ . 71
4.5 References ................................................... 75
4.5.1 A counter example ...................................... 75
4.5.2 Internalizing configurations ......................... 77
4.6 Damas and Milner’s type system ......................... 79
4.6.1 Definition ................................................ 80
4.6.2 Syntax-directed presentation ......................... 82
4.6.3 Type soundness for ML ............................... 84
4.7 Ommitted proofs and answers to exercises ............... 86

5 Existential types .............................................. 93
5.1 Towards typed closure conversion ....................... 94
5.2 Existential types .......................................... 96
5.2.1 Existential types in Church style (explicitly typed) . 96
5.2.2 Implicitly-typed existential types .................... 99
5.2.3 Existential types in ML ............................. 101
5.2.4 Existential types in OCaml ......................... 102
5.3 Typed closure conversion ................................... 103
5.3.1 Environment-passing closure conversion ............ 103
5.3.2 Closure-passing closure conversion .................. 105
## 6 Fomega: higher-kinds and higher-order types

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1 Introduction</td>
<td>111</td>
</tr>
<tr>
<td>6.2 From System F to System Fω</td>
<td>112</td>
</tr>
<tr>
<td>6.2.1 Properties</td>
<td>115</td>
</tr>
<tr>
<td>6.3 Expressiveness</td>
<td>115</td>
</tr>
<tr>
<td>6.3.1 Map on pairs</td>
<td>115</td>
</tr>
<tr>
<td>6.3.2 Abstracting over type operators</td>
<td>116</td>
</tr>
<tr>
<td>6.3.3 Existential types</td>
<td>117</td>
</tr>
<tr>
<td>6.3.4 Church encoding of non-regular ADT</td>
<td>118</td>
</tr>
<tr>
<td>6.3.5 Encoding GADT—with explicit coercions</td>
<td>121</td>
</tr>
<tr>
<td>6.4 Beyond Fω</td>
<td>123</td>
</tr>
<tr>
<td>6.4.1 Stratification</td>
<td>123</td>
</tr>
<tr>
<td>6.4.2 Kinds</td>
<td>123</td>
</tr>
<tr>
<td>6.4.3 Recursion</td>
<td>123</td>
</tr>
<tr>
<td>6.4.4 Encoding of functors</td>
<td>124</td>
</tr>
<tr>
<td>6.4.5 System Fω in OCaml</td>
<td>126</td>
</tr>
</tbody>
</table>

## 7 Logical Relations

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1 Introduction</td>
<td>129</td>
</tr>
<tr>
<td>7.1.1 Parametricity</td>
<td>129</td>
</tr>
<tr>
<td>7.2 Normalization of simply-typed λ-calculus</td>
<td>131</td>
</tr>
<tr>
<td>7.3 Observational equivalence</td>
<td>134</td>
</tr>
<tr>
<td>7.4 Logical rel in simply-typed λ-calculus</td>
<td>135</td>
</tr>
<tr>
<td>7.4.1 Logical equivalence for closed terms</td>
<td>135</td>
</tr>
<tr>
<td>7.4.2 Logical equivalence for open terms</td>
<td>137</td>
</tr>
<tr>
<td>7.5 Logical rel. in F</td>
<td>140</td>
</tr>
<tr>
<td>7.5.1 Logical equivalence for closed terms</td>
<td>141</td>
</tr>
<tr>
<td>7.6 Applications</td>
<td>146</td>
</tr>
<tr>
<td>7.7 Extensions</td>
<td>148</td>
</tr>
<tr>
<td>7.7.1 Natural numbers</td>
<td>148</td>
</tr>
<tr>
<td>7.7.2 Products</td>
<td>148</td>
</tr>
<tr>
<td>7.7.3 Sums</td>
<td>148</td>
</tr>
<tr>
<td>7.7.4 Lists</td>
<td>148</td>
</tr>
<tr>
<td>7.7.5 Existential types</td>
<td>150</td>
</tr>
<tr>
<td>7.7.6 Step-indexed logical relations</td>
<td>151</td>
</tr>
</tbody>
</table>
8 Type reconstruction

8.1 Introduction .................................................. 151
8.2 Type inference for simply-typed λ-calculus ................. 152
  8.2.1 Constraints .............................................. 153
  8.2.2 A detailed example .................................. 154
  8.2.3 Soundness and completeness of type inference ....... 156
  8.2.4 Constraint solving .................................. 156
8.3 Type inference for ML ......................................... 158
  8.3.1 Milner’s Algorithm J .................................. 158
  8.3.2 Constraints .............................................. 159
  8.3.3 Constraint solving by example ....................... 163
  8.3.4 Type reconstruction .................................. 166
8.4 Type annotations ............................................... 169
  8.4.1 Explicit binding of type variables .................... 170
  8.4.2 Polymorphic recursion ................................ 173
  8.4.3 mixed-prefix ............................................ 174
8.5 Equi- and iso-recursive types ............................... 175
  8.5.1 Equi-recursive types .................................. 175
  8.5.2 Iso-recursive types .................................. 177
  8.5.3 Algebraic data types .................................. 178
8.6 HM(X) .......................................................... 179
8.7 Type reconstruction in System F ............................. 181
  8.7.1 Type inference based on Second-order unification .... 181
  8.7.2 Bidirectional type inference ......................... 182
  8.7.3 Partial type inference in MLF ....................... 184
8.8 Proofs and Solution to Exercises ............................ 184

9 Overloading ....................................................... 187

9.1 An overview .................................................. 187
  9.1.1 Why use overloading? ................................. 187
  9.1.2 Different forms of overloading ....................... 188
  9.1.3 Static overloading .................................... 189
  9.1.4 Dynamic resolution with a type passing semantics .... 189
  9.1.5 Dynamic overloading with a type erasing semantics .... 190
9.2 Mini Haskell ................................................... 191
  9.2.1 Examples in MH ........................................ 191
  9.2.2 The definition of Mini Haskell ....................... 192
  9.2.3 Semantics of Mini Haskell ............................ 194
  9.2.4 Elaboration of expressions ........................... 196
  9.2.5 Summary of the elaboration ......................... 197
Chapter 7

Logical Relations

7.1 Introduction

So far, most proofs involving terms have proceeded by induction on typing derivations, or equivalently, on the structure of terms.

Logical relations are relations between well-typed terms defined inductively on the structure of types. They allow proofs between terms by induction on the structure of types.

Logical relations may be n-ary. However, we mostly use unary and binary logical relations. Unary logical relations are typed-indexed predicates on terms or, equivalently, type-indexed sets of terms. They are typically used to give the semantics of types as sets of terms, and as a particular case, prove type soundness or termination of reduction. Binary logical relations are type-indexed relations, or type-indexed sets of pairs of terms. They are typically used to prove equivalence of programs and non-interference properties.

Logical relations are a common proof method for programming languages.

7.1.1 Parametricity

Parametricity is a consequence of polymorphism: polymorphic functions cannot examine the argument of polymorphic types, and therefore must treat them parametrically. This often implies that polymorphic functions have actually relatively few inhabitants—up to $\beta\eta$ convertibility. Thus, a polymorphic type can reveal a lot of information about the terms that inhabit it.

Finding inhabitants of polymorphic functions

For example, what can do a term of type $\forall \alpha. \alpha \rightarrow \text{int}$? The function cannot examine its argument. Therefore, it must always return the same integer, that is, it must be a constant function. For example, it could be $\lambda x. n$, $\lambda x. (\lambda y. y) n$, $\lambda x. (\lambda y. n) x$, etc. What do they all have in common? They are all $\beta\eta$-equivalent to a term of the form $\lambda x. n$
CHAPTER 7. LOGICAL RELATIONS

What can do a term of type \(\forall \alpha. \alpha \to \alpha\)? Well it receives an argument \(V\) of type \(\alpha\) and must return a value of type \(\alpha\)—but cannot examine \(\alpha\). Thus, it must eventually return \(v\), i.e. it behaves as \(\lambda x. x\)—again up to \(\beta\eta\) equivalence.

A term type of type \(\forall \alpha. \alpha \to \beta \to \alpha\) is not very different, it additionally receives a value of type \(w\) of type \(\beta\), but there is no way \(v\) and \(w\) can interact. So that function must also return \(v\), i.e. it behaves as \(\lambda x. \lambda y. x\).

Now, a term of type \(\forall \alpha. \alpha \to \alpha \to \alpha\) receives two arguments \(v\) and \(w\) of type \(\alpha\) and must return a value of type \(\alpha\). Again, the arguments cannot interact, as we do not have any operation available of type \(\alpha\). Hence it must return either \(v\) or \(w\). That is, it behaves either as \(\lambda x. \lambda y. x\) or as \(\lambda x. \lambda y. y\)—up to \(\beta\eta\) conversion.

Theorems for free

The type of a polymorphic function may also reveal a “free theorem” about its behavior!

For example, what properties may we learn from a function \(\text{whoami}\) of type \(\forall \alpha. \text{list } \alpha \to \text{list } \alpha\)?

- the length of the result depends only on the length of the argument;
- all elements of the results are elements of the argument.
- the choice \((i, j)\) of pairs such that \(i\)-th element of the result is the \(j\)-th element of the argument does not depend on the element itself;
- the function is preserved by a transformation of its argument that preserves the shape of the argument:
  \[
  \forall f, x, \quad \text{whoami}(\text{map } f x) = \text{map } f (\text{whoami } x)
  \]

What property may we learn for the list sorting function? From it type:

\[
\text{sort} : \forall \alpha. (\alpha \to \alpha \to \text{bool}) \to \text{list } \alpha \to \text{list } \alpha
\]

we can actually deduce that if \(f\) is order-preserving, then sorting commutes with \(\text{map}\). Formally:

\[
(\forall x, y, \quad \text{cmp}_2(f x)(f y) = \text{cmp}_1 x y) \implies \\
\forall \ell, \quad \text{sort } \text{cmp}_2(\text{map } \ell) = \text{map } f (\text{sort } \text{cmp}_1 \ell)
\]

Such properties can be used to significantly reduce testing: in particular, if \(\text{sort}\) is correct on lists of integers, then it is correct on any list. Note that there are many other inhabitants of the type of \(\text{sort}\), (e.g., a function that sorts in reverse order, or a function that removes or adds duplicates), but they all satisfy this free theorem.
7.2 Normalization of simply-typed $\lambda$-calculus

In general, types also ensure termination of programs—as long as no form of recursion in types or terms has been added. Even if one wishes to add recursion explicitly later on, it is an important property of the design that non-termination is originating from the constructs for recursion only and could not occur without them.

The simply-typed $\lambda$-calculus is also lifted at the level of types in richer type systems such as System $F^\omega$ where the language of types is itself a simply-typed lambda-calculus and the decidability of type-equality depends on the termination of the reduction at the type level.

Proving termination of reduction in fragments of the $\lambda$-calculus is often a difficult task because reduction may create new redexes or duplicate existing ones. However, the proof of termination for the simply-typed $\lambda$-calculus is simple enough and interesting to be presented here. Notice that our presentation of simply-typed $\lambda$-calculus is equipped with a call-by-value semantics, while proofs of termination are usually done with a strong evaluation strategy where reduction can occur in any context.

We follow the proof schema of Pierce (2002), which is a modern presentation in a call-by-value setting of an older proof by Hindley and Seldin (1986). The proof method, which is now a standard one, is due to Tait (1967).

The idea is to first build the set $\mathcal{E}[\tau]$ of terminating closed terms of type $\tau$, and then show that any term of type $\tau$ is actually in $\mathcal{E}[\tau]$, by induction on terms. Unfortunately, stated as such, this hypothesis is too weak. The difficulty in such cases is usually to find a strong enough induction hypothesis. The solution in this case is to require that terms in $\mathcal{E}[\tau_1 \rightarrow \tau_2]$ not only terminate but also terminate when applied to any term in $\mathcal{E}[\tau_1]$.

We take the call-by-value simply-typed $\lambda$-calculus with primitive booleans and conditional. Write $\mathcal{B}$ the type of booleans and $\tt$ and $\ff$ for true and false.

Definition 2 We recursively define $\mathcal{V}[\tau]$ and $\mathcal{E}[\tau]$, subsets of closed values and closed ex-
expressions of (ground) type $\tau$ by induction on types as follows:

$\mathcal{V}[B] \triangleq \{ \text{tt, ff} \}$

$\mathcal{V}[\tau_1 \rightarrow \tau_2] \triangleq \{ \lambda x : \tau_1. M \mid \forall V \in \mathcal{V}[\tau_1], (\lambda x : \tau_1. M) V \in \mathcal{E}[\tau_2] \}$

$\mathcal{E}[\tau] \triangleq \{ M \mid \exists V \in \mathcal{V}[\tau], M \Downarrow V \}$

We write $M \Downarrow N$ as a shorthand for $M \Downarrover N$. The goal is to show that any closed expression of type $\tau$ is in $\mathcal{E}[\tau]$.

**Remark** Although usual with logical relations, well-typedness is actually not required here and omitted: otherwise, we would have to carry unnecessary type-preservation proof obligations.

The set $\mathcal{E}[\tau]$ can be seen as a predicate, i.e. a unary relation. It is called a (unary) logical relation because it is defined inductively on the structure of types.

**Immediate properties**

- $\mathcal{V}[\tau] \subseteq \mathcal{E}[\tau]$ by definition.

- $\mathcal{E}[\tau]$ is closed by inverse reduction—by definition, i.e. If $M \Downarrow N$ and $N \in \mathcal{E}[\tau]$ then $M \in \mathcal{E}[\tau]$.

- $\mathcal{E}[\tau]$ is closed by reduction. By confluence (since the reduction is deterministic), if $M \Downarrow N$ and $M \Downarrow V$, then $N \Downarrow V$.

- For any term in $\mathcal{E}[\tau]$, the reduction of $M$ terminates—by definition of $\mathcal{E}[\tau]$.

**Normalization** Therefore, it just remains to show that any term of type $\tau$ is in $\mathcal{E}[\tau]$:

**Lemma 30** If $\emptyset \vdash M : \tau$, then $M \in \mathcal{E}[\tau]$.

The proof is by induction on (the typing derivation of) $M$. However, the case for abstraction requires some similar statement, but for open terms. We need to strengthen the lemma, i.e. also give a semantics to open terms, which can be given by abstracting over the semantics of their free variables, interpreting free term variables of type $\tau$ as closed values in $\mathcal{V}[\tau]$.

We define a semantic judgment for open terms $\Gamma \models M : \tau$ so that $\emptyset \vdash M : \tau$ implies $\Gamma \models M : \tau$ and $\emptyset \models M : \tau$ means $M \in \mathcal{E}[\tau]$.

We interpret environments $\Gamma$ as closing substitutions $\gamma$, i.e. mappings from term variables to closed values: We write $\gamma \in \mathcal{G}[\Gamma]$ to mean $\text{dom}(\gamma) = \text{dom}(\Gamma)$ and $\gamma(x) \in \mathcal{V}[\tau]$ for all $x : \tau \in \Gamma$. Then, we define

$$\Gamma \models M : \tau \iff \forall \gamma \in \mathcal{G}[\Gamma], \gamma(M) \in \mathcal{E}[\tau]$$
Theorem 15 (fundamental lemma) If \( \Gamma \vdash M : \tau \) then \( \Gamma \models M : \tau \).

Corollary 31 (termination of well-typed terms) If \( \emptyset \vdash M : \tau \) then \( M \in \mathcal{E}[\tau] \).

That is, closed well-typed terms of type \( \tau \) evaluates to values of type \( \tau \).

**Proof:** By induction on the typing derivation

**Routine cases**

*Case \( \Gamma \vdash tt : B \) or \( \Gamma \vdash ff : B \):* by definition, \( tt, ff \in \mathcal{V}[B] \) and \( \mathcal{V}[B] \subseteq \mathcal{E}[B] \).

*Case \( \Gamma \vdash x : \tau \):* \( \gamma \in \mathcal{G}[\Gamma] \), thus \( \gamma(x) \in \mathcal{V}[\tau] \subseteq \mathcal{E}[\tau] \)

*Case \( \Gamma \vdash M_1 M_2 : \tau \):*

By inversion, \( \Gamma \vdash M_1 : \tau_2 \rightarrow \tau \) and \( \Gamma \vdash M_2 : \tau_2 \).

Let \( \gamma \in \mathcal{G}[\Gamma] \). We have \( \gamma(M_1 M_2) = (\gamma(M_1)) (\gamma(M_2)) \). By IH, we have \( \Gamma \vdash M_1 : \tau_2 \rightarrow \tau \) and \( \Gamma \vdash M_2 : \tau_2 \). Thus \( \gamma M_1 \in \mathcal{E}[\tau_2 \rightarrow \tau] \) (1) and \( \gamma M_2 \in \mathcal{E}[\tau_2] \) (2). By (2), there exists \( V \in \mathcal{V}[\tau_2] \) such that \( \gamma M_2 \Downarrow V \). Thus \( (\gamma M_1) (\gamma M_2) \Downarrow (\gamma M_1) V \in \mathcal{E}[\tau] \) by (1). Then, \( (\gamma M_1) (\gamma M_2) \), i.e. \( \gamma(M_1 M_2) \) is in \( \mathcal{E}[\tau] \) by closure by inverse reduction.

*Case \( \Gamma \vdash if M then M_1 else M_2 : \tau \):* By cases on the evaluation of \( \gamma M \) for \( \gamma \in \mathcal{G}[\Gamma] \).

**The interesting case**

*Case \( \Gamma \vdash \lambda x : \tau_1 . M : \tau_1 \rightarrow \tau \):*

Assume \( \gamma \in \mathcal{G}[\Gamma] \). We must show that \( \gamma(\lambda x : \tau_1 . M) \in \mathcal{E}[\tau_1 \rightarrow \tau] \) (1) That is, \( \lambda x : \tau_1 . \gamma M \in \mathcal{V}[\tau_1 \rightarrow \tau] \) (we may assume \( x \notin \text{dom}(\gamma) \) w.l.o.g.) Let \( V \in \mathcal{V}[\tau_1] \), it suffices to show \( (\lambda x : \tau_1 . \gamma M) V \Downarrow (\gamma M)[x \mapsto V] = \gamma' M \) where \( \gamma' \) is \( \gamma[x \mapsto V] \in \mathcal{G}[\Gamma, x : \tau_1] \) (3). Since \( \Gamma, x : \tau_1 \vdash M : \tau \), we have \( \Gamma, x : \tau_1 \vdash M : \tau \) by IH. Therefore by (3), we have \( \gamma' M \in \mathcal{E}[\tau] \). Since \( \mathcal{E}[\tau] \) is closed by inverse reduction, this proves (2) which finishes the proof of (1).

**Variations** We have shown both termination and type soundness, simultaneously. If we had a fix point, termination would not hold, but type soundness would still hold. The proof could then be modified by choosing:

\[
\mathcal{E}[\tau] = \{ M : \tau \mid \forall N, N \Downarrow \Rightarrow (N \in \mathcal{V}[\tau] \lor \exists N', N \rightarrow N') \}
\]

**Exercise 41** Show type soundness with this semantics.
CHAPTER 7. LOGICAL RELATIONS

7.3 Observational equivalence in simply-typed $\lambda$-calculus

The rest of these course notes are largely inspired by course notes Practical foundations for programming languages by Harper (2012) and the Introduction to Logical Relations by Skorstengaard (2019). You may also read earlier reference papers:

- Types, Abstraction and Parametric Polymorphism Reynolds (1983)
- Parametric Polymorphism and Operational Equivalence Pitts (2000).

We assume a call-by-value operational semantics (instead of call-by-name in Harper (2012)).

Program equivalence  Observational equivalence is answering the question: when are two programs $M$ and $N$ are equivalent?

We should at least include the case where one program reduces to the other, or even, more generally, when both programs reduce to the same value. But is this sufficient? Unfortunately not: what if $M$ and $N$ are functions—hence values: Aren’t $\lambda x. (x + x)$ and $\lambda x. 2 \times x$ also equivalent? Yes, they are. Indeed, two functions are observationally equivalent if when applied to equivalent arguments, they lead to observationally equivalent results. Still, are we general enough? How can we tell?

We can only observe the behavior of full programs, i.e. closed terms of some computational type, such as Booleans $B$ (the only one in our setting). We thus define:

**Definition 3** (Behavioral equivalence) Two closed programs $M$ and $N$ of the same base type are behaviorally equivalent and we write $M \simeq N$ iff there exists $V$ such that $M \Downarrow V$ and $N \Downarrow V$.

To compare programs at other types, we place them in arbitrary closing contexts. Since we often manipulate pairs of well-typed programs, we write $\Gamma \vdash M, N : \tau$ as an abbreviation for $\Gamma \vdash M : \tau \land \Gamma \vdash N : \tau$.

**Definition 4** (observational equivalence) Assume $\Gamma \vdash M, N : \tau$. We say that $M$ and $N$ are observationally equivalent and we write $\Gamma \vdash M \cong N : \tau$ if there are behaviorally equivalent when placed in any closing context at some base type. That is,

\[
\Gamma \vdash M \cong N : \tau \triangleq \forall C : (\Gamma \rhd \tau) \to (\emptyset \rhd \tau), \ C[M] \simeq C[N]
\]

**Definition 5** (Typing of context)

\[
C : (\Gamma \rhd \tau) \to (\Delta \rhd \sigma) \iff (\forall M, \ \Gamma \vdash M : \tau \implies \Delta \vdash C[M] : \sigma)
\]
There is an equivalent definition given by a set of typing rules. This is needed to prove some properties by induction on the typing derivations.

We write $M \equiv N$ as an abbreviation for $\varnothing \vdash M \equiv N : \tau$

**Lemma 32** Observational equivalence is the coarsest consistent congruence, where:

- a relation $\equiv$ is consistent if $\varnothing \vdash M \equiv N : \mathcal{B}$ implies $M \simeq N$.
- a relation $\equiv$ is a congruence if it is an equivalence and is closed by context, i.e.
  \[
  \Gamma \vdash M \equiv N : \tau \land \mathcal{C} : (\Gamma \rhd \tau) \leadsto (\Delta \rhd \sigma) \implies \Delta \vdash \mathcal{C}[M] \equiv \mathcal{C}[N] : \sigma
  \]

**Proof:**

*Consistent:* by definition, using the empty context.

*Congruence:* by compositionality of contexts.

*Coarsest:* Assume $\equiv$ is a consistent congruence. Assume $\Gamma \vdash M \equiv N : \tau$ holds and show that $\Gamma \vdash M \simeq N : \tau$ holds (1).

Let $\mathcal{C} : (\Gamma \rhd \tau) \leadsto (\varnothing \rhd \mathcal{B})$ (2). We must show that $\mathcal{C}[M] \simeq \mathcal{C}[N]$.

This follows by consistency applied to $\Gamma \vdash \mathcal{C}[M] \equiv \mathcal{C}[N] : \mathcal{B}$ which follows by congruence from (1) and (2).

**Problem with Observational Equivalence**  Observational equivalence is too difficult to test: Because of quantification over all contexts (too many for testing). but many contexts will do the same experiment.

The solution is to take advantage of types to reduce the number of experiments by defining and testing the equivalence on base types and propagating the definition mechanically at other types.

Logical relations provide the infrastructure for conducting such proofs.

## 7.4 Logical relations in simply-typed $\lambda$-calculus

### 7.4.1 Logical equivalence for closed terms

Unary logical relations interpret types by predicates on (i.e. sets of) closed values of that type. Binary relations interpret types by binary relations on closed values of that type, i.e. sets of pairs of related values of that type.

That is, $\mathcal{V}[\tau]$ is a subset of $\text{Val}(\tau) \times \text{Val}(\tau)$ and $\mathcal{E}[\tau]$, the closure of $\mathcal{V}[\tau]$ by inverse reduction is a subset of $\text{Expressions}_\tau \times \text{Exp}(\tau)$. 
Definition 6  (Logical equivalence for closed terms) We recursively define two relations $\mathcal{V}[\tau]$ and $\mathcal{E}[\tau]$ between values of type $\tau$ and expressions of type $\tau$ by

$$
\mathcal{V}[\text{B}] \triangleq \{(tt,tt), (ff,ff)\}
$$

$$
\mathcal{V}[\tau \rightarrow \sigma] \triangleq \{(V_1, V_2) \mid V_1, V_2 \vdash \tau \rightarrow \sigma \land \forall (W_1, W_2) \in \mathcal{V}[\tau], (V_1, W_1, V_2, W_2) \in \mathcal{E}[\sigma]\}
$$

$$
\mathcal{E}[\tau] \triangleq \{(M_1, M_2) \mid M_1, M_2 : \tau \land \exists (V_1, V_2) \in \mathcal{V}[\tau], M_1 \Downarrow V_1 \land M_2 \Downarrow V_2\}
$$

Notice the (highlighted) mutual recursion between $\mathcal{V}[\cdot]$ and $\mathcal{E}[\cdot]$. In the following we will leave the typing constraint in gray implicit, i.e. we will treat them as global conditions for sets $\mathcal{V}[\cdot]$ and $\mathcal{E}[\cdot]$. We also write $M_1 \sim_\tau M_2$ for $(M_1, M_2) \in \mathcal{E}[\tau]$ and $V_1 \approx_\tau V_2$ for $(V_1, V_2) \in \mathcal{V}[\tau]$.

Non-termination  In a language with non-termination, we change the definition of $\mathcal{E}[\tau]$ to

$$
\mathcal{E}[\tau] \triangleq \left\{ (M_1, M_2) \mid M_1, M_2 : \tau \land \begin{aligned}
\forall V_1, M_1 \Downarrow V_1 & \implies \exists V_2, M_2 \Downarrow V_2 \land (V_1, V_2) \in \mathcal{V}[\tau] \\
\land \forall V_2, M_2 \Downarrow V_2 & \implies \exists V_1, M_1 \Downarrow V_1 \land (V_1, V_2) \in \mathcal{V}[\tau] \end{aligned} \right\}
$$

Remark  In $\mathcal{V}[\sigma \rightarrow \sigma]$, all values are functions. Hence, we could have equivalently defined:

$$
\mathcal{V}[\sigma \rightarrow \sigma] \triangleq \{(\lambda x : \tau. M_1), (\lambda x : \tau. M_2) \mid (\lambda x : \tau. M_1), (\lambda x : \tau. M_2) \vdash \sigma \land \forall (W_1, W_2) \in \mathcal{V}[\tau], ((\lambda x : \tau. M_1) W_1, (\lambda x : \tau. M_2) W_2) \in \mathcal{E}[\sigma]\}
$$

This formulation is more explicit, but less concise.

Properties of logical equivalence for closed terms

Closure by reduction  By definition, since reduction is deterministic: Assume $M_1 \Downarrow N_1$ and $M_2 \Downarrow N_2$ and $(M_1, M_2) \in \mathcal{E}[\tau]$, i.e. there exists $(V_1, V_2) \in \mathcal{V}[\tau]$ (1) such that $M_i \Downarrow V_i$. Since reduction is deterministic, we must have $M_i \Downarrow N_i \Downarrow V_i$. This, together with (1), implies $(N_1, N_2) \in \mathcal{E}[\tau]$.

Closure by inverse reduction  Immediate, by construction of $\mathcal{E}[\tau]$.

Corollaries

- If $(M_1, M_2) \in \mathcal{E}[\tau \rightarrow \sigma]$ and $(N_1, N_2) \in \mathcal{E}[\tau]$, then $(M_1 N_1, M_2 N_2) \in \mathcal{E}[\sigma]$. 
7.4. LOGICAL REL IN SIMPLY-TYPED $\lambda$-CALCULUS

- To prove $(M_1, M_2) \in E[\tau \rightarrow \sigma]$, it suffices to show $(M_1 V_1, M_2 V_2) \in E[\sigma]$ for all $(V_1, V_2) \in V[\tau]$.

Consistency $(\sim_B) \subseteq (\approx)$. Immediate, by definition of $E[B]$ and $V[B] \subseteq (\approx)$.

Lemma 33 (Symmetry and transitivity) Logical equivalence is symmetric and transitive (at any given type).

Notice that reflexivity is not at all obvious! This will be the fundamental lemma of logical relations.

Proof: We show it simultaneously for $\sim_\tau$ and $\approx_\tau$ by induction on type $\tau$. For $\sim_\tau$, the proof is immediate by transitivity and symmetry of $\approx_\tau$. For $\approx_\tau$, it goes as follows:

Case $\tau$ is $B$: the result is immediate by symmetry and transitivity of behavioral equivalence.

Case $\tau$ is $\tau \rightarrow \sigma$:

By IH, symmetry and transitivity hold at types $\tau$ and $\sigma$.

For symmetry, assume $V_1 \approx_{\tau \rightarrow \sigma} V_2$ (1), we must show $V_2 \approx_{\tau \rightarrow \sigma} V_1$. Assume $W_1 \approx_\tau W_2$. We must show $V_2 M_1 \approx_\tau V_1 W_2$ (2). We have $W_2 \approx_\tau W_1$ by symmetry at type $\tau$. By (1), we have $V_2 W_2 \approx_\sigma V_1 W_1$ and (2) follows by symmetry of $\sim$ at type $\sigma$.

For transitivity, assume $V_1 \approx_{\tau \rightarrow \sigma} V_2$ (3) and $V_2 \approx_{\tau \rightarrow \sigma} V_3$ (4). To show $V_1 \approx_{\tau \rightarrow \sigma} V_3$, we assume $W_1 \approx_\tau W_3$ and show $V_1 W_1 \approx_\tau V_3 W_3$ (5). By (3), we have $V_1 W_1 \approx_\tau V_2 W_3$ (6). By symmetry and transitivity of $\approx_\tau$, we get $W_3 \approx_\tau W_3$ (7). By (4), we have $V_2 W_3 \approx_\sigma V_3 W_3$ (8). Then (2) follows by transitivity of $\sim_\sigma$ applied to (6) and (8).

Remark: that (7) is not using reflexivity, which has not been proved yet: this equality follows from the fact that $W_3$ is already known to be in relation with $W_1$.

7.4.2 Logical equivalence for open terms

When $\Gamma \vdash M_1, M_2 : \tau$, we wish to define a judgment $\Gamma \vdash M_1 \sim M_2 : \tau$ to mean that the open terms $M_1$ and $M_2$ are equivalent at type $\tau$.

The solution is to interpret program variables of $\text{dom}(\Gamma)$ by pairs of related values, and typing contexts $\Gamma$ by sets of bisubstitutions $\gamma$ mapping variable type assignments to pairs of related values at the given type:

$$G[\emptyset] \triangleq \{\emptyset\}$$
$$G[\Gamma, x : \tau] \triangleq \{\gamma, x \mapsto (V_1, V_2) \mid \gamma \in G[\Gamma] \land (V_1, V_2) \in V[\tau]\}$$

Given a bisubstitution $\gamma$, we write $\gamma_i$ for the substitution that maps $x$ to $V_i$ whenever $\gamma$ maps $x$ to $(V_1, V_2)$. 
Definition 7 (Logical equivalence for open terms)

\[ \Gamma \vdash M_1 \sim M_2 : \tau \quad \overset{\text{def}}{=} \quad \left\{ \begin{array}{l} \Gamma \vdash M_1, M_2 : \tau \\ \forall \gamma \in \mathcal{G}[\Gamma], \ (\gamma_1 M_1, \gamma_2 M_2) \in \mathcal{E}[\tau] \end{array} \right. \]

We also write \( \vdash M_1 \sim M_2 : \tau \) or \( M_1 \sim \tau M_2 \) for \( \emptyset \vdash M_1 \sim M_2 : \tau \).

Lemma 34 Open logical equivalence is symmetric and transitive.

Proof: The Proof is immediate by the definition and the symmetry and transitivity of closed logical equivalence.

Theorem 16 (Reflexivity) If \( \Gamma \vdash M : \tau \), then \( \Gamma \vdash M \sim M : \tau \).

The is also called the fundamental lemma of logical relations. The proof is by induction on the typing derivation, using compatibility lemmas.

Compatibility lemmas

\[
\begin{array}{c@{\quad}c@{\quad}c}
\text{C-TRUE} & \quad & \text{C-ABS} \\
\Gamma \vdash \text{tt} \sim \text{tt} : \text{bool} & \quad & \Gamma \vdash \lambda x : \tau \vdash M_1 \sim M_2 : \sigma \\
\text{C-FALSE} & \quad & \text{C-APPL} \\
\Gamma \vdash \text{ff} \sim \text{ff} : \text{bool} & \quad & \Gamma \vdash \lambda x : \tau \vdash M_1 \sim M_2 : \tau \rightarrow \sigma \\
\text{C-IF} & \quad & \\
\Gamma \vdash M_1 \sim M_2 : \tau & \quad & \Gamma \vdash \lambda x : \tau \vdash M_1 \sim M_2 : \tau \\
\Gamma \vdash N_1 \sim N_2 : \tau & \quad & \Gamma \vdash N_1 \sim N_2 : \tau \\
\end{array}
\]

Proof: Each case can be shown independently.

Rule C-ABS Assume \( \Gamma, x : \tau \vdash M_1 \sim M_2 : \sigma \) (1). We show \( \Gamma \vdash \lambda x : \tau \vdash M_1 \sim M_2 : \tau \rightarrow \sigma \).

Let \( \gamma \) be in \( \mathcal{G}[\Gamma] \). We show \( (\gamma_1 (\lambda x : \tau. M_1), \gamma_2 (\lambda x : \tau. M_2)) \in \mathcal{V}[\tau \rightarrow \sigma] \). Let \( (V_1, V_2) \) be in \( \mathcal{V}[\tau] \). It suffices to show that \( (\gamma_1 (\lambda x : \tau. M_1) V_1, \gamma_2 (\lambda x : \tau. M_2) V_2) \in \mathcal{E}[\sigma] \) (2).

Let \( \gamma' \) be \( \gamma, x \mapsto (V_1, V_2) \). We have \( \gamma' \) in \( \mathcal{G}[\Gamma, x : \tau] \). Thus, from (1), we have \( (\gamma'_1 M_1, \gamma'_2 M_2) \) in \( \mathcal{E}[\sigma] \), which proves (2), since \( \mathcal{E}[\sigma] \) is closed by inverse reduction and \( \gamma_i (\lambda x : \tau. M_i) V_i = \lambda x : \tau. \gamma_i (M_i) V_i \downarrow \gamma_i M_i[x \mapsto V_i] = \gamma'_i M_i \).

Rule C-APPL and C-IF By induction hypothesis and the fact that substitution distributes over application.

We must show \( \Gamma \vdash M_1 N_1 \sim M_2 N_2 : \sigma \) (3). Let \( \gamma \) be in \( \mathcal{G}[\Gamma] \). From the premises \( \Gamma \vdash M_1 \sim M_2 : \tau \rightarrow \sigma \) and \( \Gamma \vdash N_1 \sim N_2 : \tau \), we have \( (\gamma_1 M_1, \gamma_2 M_2) \) in \( \mathcal{E}[\tau \rightarrow \sigma] \) and \( (\gamma_1 N_1, \gamma_2 N_2) \) in \( \mathcal{E}[\tau] \). Therefore \( (\gamma_1 M_1, \gamma_1 N_1, \gamma_2 M_2, \gamma_2 N_2) \), i.e. \( (\gamma_1 (M_1 N_1), \gamma_2 (M_2 N_2)) \in \mathcal{E}[\sigma] \) in \( \mathcal{E}[\sigma] \), which proves (3).
7.4. LOGICAL REL IN SIMPLY-TYPED $\lambda$-CALCULUS

Rule $\text{C-If}$: Similar to the case of application. We show $\Gamma \vdash \text{if } M_1 \text{ then } N_1 \text{ else } N_1' \sim \text{if } M_2 \text{ then } N_2 \text{ else } N_2'$ where $\tau$. Assume $\gamma$ in $G[\gamma]$. We show $(\gamma_1(\text{if } M_1 \text{ then } N_1 \text{ else } N_1'), \gamma_2(\text{if } M_2 \text{ then } N_2 \text{ else } N_2'))$ in $E[\tau]$ (1).

From the premise $\Gamma \vdash M_1 \sim M_2 : B$, we have $(\gamma_1 M_1, \gamma_2 M_2) \in E[\gamma]$ (1). Therefore $M_1 \Downarrow V$ and $M_2 \Downarrow V$ where $V$ is either $tt$ or $ff$.

Case $V$ is $tt$: Then, $(\gamma_1 M_i, \gamma_2 N_i, \gamma_i N_i') \Downarrow V$, i.e. $\gamma_i(\text{if } M_i \text{ then } N_i \text{ else } N_i') \Downarrow V$.

From the premise $\Gamma \vdash N_1 \sim N_2 : \tau$, we have $(\gamma_1 N_1, \gamma_2 N_2)$ in $E[\tau]$ and (1) follows by closure by inverse reduction.

Case $V$ is $ff$: similar.

Rule $\text{C-True}$, $\text{C-False}$, and $\text{C-Var}$ are immediate.

Proof: (of reflexivity)

By induction on the proof of $\Gamma \vdash M : \tau$. All cases are easy. We must show $\Gamma \vdash M \sim M : \tau$:

Case $M$ is $tt$ or $ff$: Immediate by Rule $\text{C-True}$ or Rule $\text{C-False}$

Case $M$ is $x$: Immediate by Rule $\text{C-Var}$

Case $M$ is $M' N$: By inversion of the typing rule $\text{App}$ induction hypothesis, and Rule $\text{C-App}$

Case $M$ is $\lambda x : \tau. N$: By inversion of the typing rule $\text{Var}$ induction hypothesis, and Rule $\text{C-Var}$

Properties of logical relations

Corollary 35 (equivalence) Open logical relation is an equivalence relation

Lemma 36 Logical equivalence is a congruence.
If $\Gamma \vdash M \sim M' : \tau$ and $C : (\Gamma \triangleright \tau) \Rightarrow (\Delta \triangleright \sigma)$, then $\Delta \vdash C[M] \sim C[M'] : \sigma$.

Proof: By induction on the proof of $C : (\Gamma \triangleright \tau) \Rightarrow (\Delta \triangleright \sigma)$.

The proof is similar to the proof of reflexivity—but we need a syntactic definition of context typing derivations (which we have omitted) to be able to reason by induction on the context typing derivations.

Theorem 17 (Soundness of logical equivalence) Logical equivalence implies observational equivalence. If $\Gamma \vdash M \sim M' : \tau$ then $\Gamma \vdash M \equiv M' : \tau$. 

Proof: Logical equivalence is a consistent congruence, hence included in observational equivalence which is the coarsest such relation.

\[ \text{Theorem 18 (Completeness of logical equivalence)} \]
Observational equivalence of closed terms implies logical equivalence. That is \((\simeq) \subseteq (\sim)\).

\[ \text{Proof: Proof by induction on } \tau. \]

\[ \text{Case } B: \text{ In the empty context, by consistency, } \simeq_B \text{ is a subrelation of } \simeq_B \text{ which coincides with } \nsim_B. \]

\[ \text{Case } \tau \rightarrow \sigma: \text{ By congruence of observational equivalence.} \]

By hypothesis, we have \(M_1 \simeq_{\tau \rightarrow \sigma} M_2\) (1). To show \(M_1 \nsim_\tau M_2\) (2) and then, it suffices to show \(M_1 \nsim_\nu M_2\) (3).

By soundness applied to (2), we have \(V_1 \simeq_\nu V_2\) from (4). By congruence with (1), we have \(M_1 V_1 \simeq_\sigma M_2 V_2\), which implies (3) by IH at type \(\nu\).

\[ \text{Exercise 42 (Application)} \]
Let not be \(\lambda x: B. \text{if } x \text{ then } \text{ff} \text{ else } \text{tt}\) and \(M\) and \(M'\) be the expressions \(\lambda x: B. \lambda y: \tau. \lambda z: \tau. \text{if not } x \text{ then } y \text{ else } z\) and \(\lambda x: B. \lambda y: \tau. \lambda z: \tau. \text{if } x \text{ then } z \text{ else } y\).

Show that \(M \simeq B \rightarrow \tau \rightarrow \tau \rightarrow \tau M'\).

\[ \text{Solution: It suffices to show } M V_1 V_2 \nsim \tau M' V_1' V_2' \text{ whenever } V_0 \simeq_B V_0' (1) \text{ and } V_1 \simeq_\nu V_1' (2) \text{ and } V_2 \simeq_\nu V_2' (3). \]

By inverse reduction, it suffices to show: if not \(V_0\) then \(V_1\) else \(V_2\) \(\nsim_\tau\) if \(V_0'\) then \(V_2'\) else \(V_1'\) (4). It follows from (1) that we have only two cases:

Case \(V_0 = V_0' = \nu\): Then not \(V_0 \Downarrow \text{ff}\) and thus \(M \Downarrow V_2\) while \(M' \Downarrow V_2\). Then (4) follows from (3) and closure by inverse reduction.

Case \(V_0 = V_0' = \text{ff}\): is symmetric.

\[ \text{7.5 Logical relations in } F \]

We now extend observational and logical equivalence to System F.

\[ \tau ::= \ldots \mid \alpha \mid \forall \alpha. \tau \quad M ::= \ldots \mid \Lambda \alpha. M \mid M \tau \]

We write typing contexts \(\Delta; \Gamma\) where \(\Delta\) binds type variables and \(\Gamma\) binds program variables.

Typing of contexts becomes \(C : (\Delta; \Gamma \triangleright \tau) \Rightarrow (\Delta'; \Gamma' \triangleright \tau')\).

\[ \text{Definition 8 (observational equivalence)} \]
We defined \(\Delta; \Gamma \vdash M \simeq N : \tau\) as

\[ \forall \forall C : (\Delta; \Gamma \triangleright \tau) \Rightarrow (\emptyset; \emptyset \triangleright B) \quad C[M] \simeq C[N] \]

We write \(M \simeq_\tau N\) for \(\emptyset; \emptyset \vdash M \simeq N : \tau\) (in particular, when \(\tau, M,\) and \(N\) are closed).
7.5. LOGICAL REL. IN F

7.5.1 Logical equivalence for closed terms

For closed terms (no free program variables), we now need to give the semantics of polymorphic types $\forall \alpha. \tau$. Unfortunately, it cannot be defined in terms of the semantics of instances $\tau[\alpha \mapsto \sigma]$, since the semantics is defined by induction on types.

The work around is to define the semantics of terms with open types in some suitable environment that interprets type variables by relations (sets of pairs of related values) of closed types.

This relation will also be used to give the semantics of type variables. A key point however, it to interpret type variables by heterogeneous values, relating values of different types on both sides.

We write $\rho$ for closed types. Let $\mathcal{R}(\rho_1, \rho_2)$ be the set of relations on values of closed types $\rho_1$ and $\rho_2$, that is, $\mathcal{P}(\text{Val}(\rho_1) \times \text{Val}(\rho_2))$. We optionally restrict all such relations to be admissible, and we write $\mathcal{R}^l(\rho_1, \rho_2)$ the subset of admissible relations, which in our setting means closed by observational equivalence, i.e.

$$R \in \mathcal{R}^l(\rho_1, \rho_2) \iff \forall (V_1, V_2) \in R, \forall W_1, W_2, W_1 \cong_{\rho_1} V_1 \land W_2 \cong_{\rho_2} V_2 \implies (W_1, W_2) \in R$$

Admissibility will be required for completeness of logical relations with respect to observational equivalence. However, it is not required for soundness of logical relations. Choosing relations that are not admissible is sometimes easier when one only soundness of logical relations is needed.

Example 2 Both $R_1 \triangleq \{(\text{tt}, 0), (\text{ff}, 1)\}$ and $R_2 \triangleq \{(\text{tt}, 0)\} \cup \{(\text{ff}, n) | n \in \mathbb{Z}^*\}$ are admissible relations in $\mathcal{R}(\text{B}, \text{int})$. By contrast $R_3 \triangleq \{(\text{tt}, \lambda x : \tau. 0), (\text{ff}, \lambda x : \tau. 1)\}$ is in $\mathcal{R}(\text{B}, \tau \rightarrow \text{int})$ but it is not admissible. Indeed, taking $M_0 \triangleq \lambda x : \tau. (\lambda z : \text{int}. z) 0$. we have $M_0 \cong_{\tau \rightarrow \text{int}} \lambda x : \tau. 0$ but $(\text{tt}, M_0)$ is not in $R_3$.

Interpretation of type environments We interpret type variables $\alpha$ by triples of the form $(\rho_1, \rho_2, R)$ where $R \in \mathcal{R}(\rho_1, \rho_2)$. We write $\eta$ for mappings of type variables to such triples. Given a list of type variables $\Delta$, we define the set $\mathcal{D}[\Delta]$ of interpretations of $\Delta$ as:

$$\mathcal{D}[\emptyset] \triangleq \{\emptyset\}$$
$$\mathcal{D}[\Delta, \alpha] \triangleq \{\eta, \alpha \mapsto (\rho_1, \rho_2, R) | \eta \in \mathcal{D}[\Delta] \land R \in \mathcal{R}(\rho_1, \rho_2)\}$$
Definition 9 (Logical equivalence for closed terms)

\[ \forall[\alpha]_\eta \triangleq \eta_R(\alpha) \]

\[ \forall[\forall \alpha. \tau]_\eta \triangleq \{ (V_1, V_2) \mid V_1 \vdash \eta_1(\forall \alpha. \tau) \land \forall \rho_1, \rho_2, R \in \mathcal{R}(\rho_1, \rho_2), (V_1 \rho_1, V_2 \rho_2) \in \mathcal{E}[\tau]_{\eta, \alpha \mapsto (\rho_1, \rho_2, R)} \} \]

\[ \forall[B]_\eta \triangleq \{ (tt, tt), (ff, ff) \} \]

\[ \forall[\tau \rightarrow \sigma]_\eta \triangleq \{ (V_1, V_2) \mid V_1 \vdash \eta_1(\tau \rightarrow \sigma) \land \forall (W_1, W_2) \in \forall[\tau]_\eta, (V_1 W_1, V_2 W_2) \in \mathcal{E}[\sigma]_\eta \} \]

\[ \mathcal{E}[\tau]_\eta \triangleq \{ (M_1, M_2) \mid M_1 : \eta_1 \tau M_2 : \eta_2 \tau \land \exists (V_1, V_2) \in \forall[\tau]_\eta, M_1 \Downarrow V_1 \land M_2 \Downarrow V_2 \} \]

\[ \mathcal{G}[\emptyset]_\eta \triangleq \{ \emptyset \} \]

\[ \mathcal{G}[\Gamma, x : \tau]_\eta \triangleq \{ \gamma, x \mapsto (V_1, V_2) \mid \gamma \in \mathcal{G}[\Gamma]_\eta \land (V_1, V_2) \in \forall[\tau]_\eta \} \]

Notice that there are really just two new cases \( \forall[\alpha]_\eta \) and \( \forall[\forall \alpha. \tau]_\eta \), as the other cases are just adjusting the previous definition to carry around the environment \( \eta \) (which we have here typeset in highlighted to emphasize the minor difference).

Notice again that \( \forall \alpha. \tau \) is interpreted by choosing two different types \( \rho_1 \) and \( \rho_2 \) and therefore heterogeneous pairs of types in \( \mathcal{R}(\rho_1, \rho_2) \) to interpret \( \alpha \).

Definition 10 (Logical equivalence for open terms) We say \( \Delta; \Gamma \vdash M \sim M' : \tau \) as

\[ \Delta; \Gamma \vdash M, M' : \tau \land \forall \eta \in \mathcal{D}[\Delta], \forall \gamma \in \mathcal{G}[\Gamma]_\eta, (\eta_1(\gamma_1 M_1), \eta_2(\gamma_2 M_2)) \in \mathcal{E}[\tau]_\eta \]

We also write \( M_1 \sim M_2 \) for \( \vdash M_1 \sim M_2 : \tau \) (i.e. \( \emptyset; \emptyset \vdash M_1 \sim M_2 : \tau \)). In this case, \( \tau \) is a closed type and \( M_1 \) and \( M_2 \) are closed terms of type \( \tau \); hence, this coincides with the previous definition \( (M_1, M_2) \) in \( \mathcal{E}[\tau]_\emptyset \), which may still be used as a shorthand for \( \mathcal{E}[\tau] \).

Lemma 37 (Compositionality)

Assume \( \Delta \vdash \sigma \) and \( \Delta, \alpha \vdash \tau \) and \( \eta \in \mathcal{D}[\Delta] \). Then, \( \forall[\tau[\alpha \mapsto \sigma]]_\eta = \forall[\tau]_{\eta, \alpha \mapsto (\eta_1 \sigma, \eta_2 \sigma, \mathcal{V}[\sigma]_\eta)} \).

Proof: Let us write \( \theta \) for \( [\alpha \mapsto \sigma] \) and \( \eta^\alpha \) for \( \eta, \alpha \mapsto (\eta_1 \sigma, \eta_2 \sigma, R) \). We show \( \forall[\tau \theta]_\eta = \forall[\tau]_{\eta^\alpha} \).

Case \( \tau \) is \( \alpha \): The right-hand side \( \forall[\alpha]_{\eta^\alpha} \) is by definition \( \eta_R^\alpha(\alpha) \), which is \( R(\alpha) \), i.e. \( \forall[\sigma]_\eta \) by hypothesis.

Case \( \tau \) is \( \sigma \rightarrow \sigma' \): Since \( (\sigma \rightarrow \sigma') \theta \) is \( \sigma \theta \rightarrow \sigma' \theta \), the left-hand side is \( \forall[\sigma \theta \rightarrow \sigma' \theta]_\eta \), i.e. by definition:

\[ \{ (V_1, V_2) \mid \forall (W_1, W_2) \in \forall[\sigma \theta]_\eta, (V_1 W_1, V_2 W_2) \in \mathcal{E}[\sigma' \theta]_\eta \} \]
By induction hypothesis, we may replaced $\mathcal{V}[\sigma\theta]_\eta$ by $\mathcal{V}[\sigma]_{\eta'^\alpha}$ and $\mathcal{E}[\sigma'\theta]_\eta$ by $\mathcal{E}[\sigma'^\beta]_{\eta'^\alpha}$ which gives exactly the definition of the right-hand side $\mathcal{V}[\sigma \to \sigma']_{\eta'^\beta}$.

Case $\tau$ is $B$: Both sides are equal to $\mathcal{V}[B]$.

Case $\tau$ is $\forall \beta. \sigma$: Assume $\alpha \neq \beta$. Since $\theta(\forall \alpha. \sigma)$ is then $\forall \alpha, \theta \alpha \sigma$, the left-hand side is $\mathcal{V}[\forall \alpha. \sigma \theta]_\eta$ which is, by definition:

$$\{ (V_1, V_2) \mid \forall \rho_1, \rho_2, \forall S \in R(\rho_1, \rho_2), (V_1 \rho_1, V_2 \rho_2) \in \mathcal{E}[\sigma \theta]_{\eta, \beta \mapsto (\rho_1, \rho_2, S)} \}$$

Since $R$ and $S$ are relations between closed types the substitutions $\alpha \mapsto (\gamma_1, \gamma_2, R)$ and $\beta \mapsto (\rho_1, \rho_2, S)$ commute. Thus, by induction hypothesis, we may replace $\mathcal{E}[\sigma \theta]_\eta$ by $\mathcal{E}[\sigma]_{\eta'^\alpha, \beta \mapsto (\rho_1, \rho_2, S)}$, which gives the definition of the right-hand side.

**Theorem 19 (Reflexivity, also called the fundamental lemma)**

If $\Delta; \Gamma \vdash M : \tau$ then $\Delta; \Gamma \vdash M \sim M : \tau$.

Admissibility is not required for the fundamental lemma.

**Proof:** By induction on the typing derivation of $\Delta; \Gamma \vdash M : \tau$, using compatibility lemmas.

**Lemma 38 (Compatibility lemmas)** We redefined previous the lemmas to work in a typing context of the form $\Delta, \Gamma$ instead of $\Gamma$. In addition, we have:

<table>
<thead>
<tr>
<th>C-TABS</th>
<th>C-TAPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Delta, \alpha; \Gamma \vdash M_1 \sim M_2 : \tau$</td>
<td>$\Delta; \Gamma \vdash M_1 \sim M_2 : \forall \alpha. \tau$</td>
</tr>
<tr>
<td>$\Delta; \Gamma \vdash \Lambda \alpha. M_1 \sim \Lambda \alpha. M_2 : \forall \alpha. \tau$</td>
<td>$\Delta; \Gamma \vdash M_1 \sigma \sim M_2 \sigma : \tau[\alpha \mapsto \sigma]$</td>
</tr>
</tbody>
</table>

**Proof:** We show each rule independently. In each case, the typing conditions follow immediately from the mimicking of the typing rules.

**Rule C-TABS** Assume $\Delta, \alpha; \Gamma \vdash M_1 \sim M_2 : \tau$ (1). We show $\Delta; \Gamma \vdash \Lambda \alpha. N \sim \Lambda \alpha. N : \forall \alpha. \tau$.

Let $\eta \in \mathcal{D}[\Delta]$ and $\gamma \in \mathcal{G}[\Gamma]_\eta$. We show $(\eta_1(\gamma_1(\Lambda \alpha. M_1)), \eta_2(\gamma_2(\Lambda \alpha. M_2))) \in \mathcal{E}[\forall \alpha. \tau]_\eta$, i.e. $(\eta_1(\gamma_1(\Lambda \alpha. M_1))) \rho_1, (\eta_2(\gamma_2(\Lambda \alpha. M_2))) \rho_2 \in \mathcal{E}[\tau]_{\eta, \alpha \mapsto (\rho_1, \rho_2, R)}$ (2), for any ground types $\rho_1$ and $\rho_2$ and $R \in R(\rho_1, \rho_2)$.

We may assume $\alpha \notin \text{dom}(\gamma)$ w.l.o.g.. Then $(\eta_1(\gamma_1(\Lambda \alpha. M_1))) \rho_i$ is equal to $\eta_1((\Lambda \alpha. \gamma_i.M_1) \rho_i)$ which reduces to $\eta_1(\gamma_i(M_i))$, i.e. $\eta_1(\gamma_i(M_i))$ where $\gamma_i$ is $\alpha \mapsto \rho_i$.

Since $\gamma_i \in \mathcal{D}[\Delta, \alpha]$, we have by $(\eta_1(\gamma_i'(M_1)), \eta_2(\gamma_2'(M_2))) \in \mathcal{E}[\tau]_{\eta, \alpha \mapsto (\rho_1, \rho_2, R)}$ by IH applied to (1), from which (2) follows by closure under inverse reduction.

**Rule C-TAPP** Assume $\Delta; \Gamma \vdash M_1 \sim M_2 : \forall \alpha. \tau$ (1) and $\Delta \vdash \sigma$. We show $\Delta; \Gamma \vdash M_1 \sigma \sim M_2 \sigma : \tau[\alpha \mapsto \sigma]$. Let $\eta \in \mathcal{D}[\Delta]$ and $\gamma \in \mathcal{G}[\Gamma]_\eta$. We just need to show $(\eta_1 \gamma_1(M_1 \sigma), \eta_2 \gamma_2(M_2 \sigma))$
in $\mathcal{E}[\tau[\alpha \mapsto \sigma]]_\eta$ (2). From (1), we have $(\eta_1 \gamma_1 M_1, \eta_2 \gamma_2 M_2) \in \mathcal{E}[\forall \alpha. \tau]_\eta$. By definition, this implies $((\eta_1 \gamma_1 M_1) (\eta_1 \sigma), (\eta_2 \gamma_2 M_2) (\eta_2 \sigma))$, i.e., $(\eta_1 \gamma_1 (M_1 \sigma), \eta_2 \gamma_2 (M \sigma))$ is in $\mathcal{E}[\tau]_{\eta'}$ where $\eta'$ is $\eta, \alpha \mapsto (\eta_1 \sigma, \eta_2 \sigma, \mathcal{V}[\sigma]_\eta)$, which exactly proves (2) by compositionality. (Notice, that by corollary 40 this relation is admissible if we are working under the admissibility assumption.)

Other rules: their proof is quite similar to the same corresponding rule for closed types.

**Theorem 20 (Soundness of logical equivalence)** Logical equivalence implies implies observational equivalence. That is, if $\Delta; \Gamma \vdash M_1 \sim M_2 : \tau$ then $\Delta; \Gamma \vdash M_1 \equiv M_2 : \tau$.

**Lemma 39 (Respect for observational equivalence)** Under the admissibility condition, If $(M_1, M_2) \in \mathcal{E}[\tau]_\eta$ and $M_1 \equiv_{\eta, \tau} N_1$ and $M_2 \equiv_{\eta, \tau} N_2$, then $(N_1, N_2) \in \mathcal{E}[\tau]_\eta$.

**Proof:** By symmetry, we may just show it when $N_2$ is $M_2$, the case when $N_1$ is $M_1$ is symmetric and the general case follows by two applications of the lemma that falls in the two previous cases.

We assume $(M_1, M_2) \in \mathcal{E}[\tau]_\eta$ (1) and $M_1 \equiv_{\eta, \tau} N_1$ (2). We show $(N_1, M_2) \in \mathcal{E}[\tau]_\eta$ (3) by induction on $\tau$.

**Case $\tau$ is $\forall \alpha. \sigma$:** Assume $R \in \mathcal{R}(\rho_1, \rho_2)$. Let $\eta^a$ be $\eta, \alpha \mapsto (\rho_1, \rho_2, R)$. It suffices to show $(M_1 \rho_1, M_2 \rho_2) \in \mathcal{E}[\sigma]_{\eta^a}$ (4). We have $(M_1 \rho_1, M_2 \rho_2) \in \mathcal{E}[\sigma]_{\eta_1}$, from (1). By congruence applied to (2), we have $N_1 \rho_1 \equiv_{\eta_1, \tau} M_1 \rho_1$. Then (4) follows by induction hypothesis at type $\sigma$.

**Case $\tau$ is $\alpha$:** We know that $(M_1, M_2)$ reduces to a pair $(V_1, V_2)$ in $\mathcal{V}[\alpha]_\eta$, i.e. $\eta_R(\alpha)$, which is by assumption is admissible, i.e. closed by observational equivalence (between values). Therefore, we just need to show that $V \equiv_{\eta, \alpha} V_1$ where $V$ is such that $N_1 \not\Downarrow V$. This follows from $N_1 \equiv_{\eta_1, \tau} M_1$ since observational equivalence of closed terms is closed by reduction.

**Case $\tau$ is $B$:** By definition $\mathcal{E}[B]_\eta$ does not depend on $\eta$ and is equal to $\equiv_B$, which is included in $\equiv_B$ and closed by transitivity.

**Case $\tau$ is $\sigma' \rightarrow \sigma$:** Assume $V_1, V_2$ is in $\mathcal{E}[\sigma']_\eta$ (5). It suffices to show that $(N_1 V_1, M_2 V_2)$ is in $\mathcal{E}[\sigma']_{\eta_1}$ (6). By (1), we have $(M_1 V_1, M_2 V_2)$ in $\mathcal{E}[\sigma']_{\eta_1}$. By congruence applied to (2), we have $N_1 V_1 \equiv_{\eta_1(\sigma)} M_1 V_1$. Then (6) follows by IH, since then $\mathcal{E}[\sigma']_\eta$ respects observational equivalence.

**Corollary 40** Under the admissibility condition, the relation $\mathcal{V}[\tau]_{\eta_1}$ is an admissible relation in $\mathcal{R}(\eta_1, \eta_2, \tau)$.

This may be useful to build admissibility relations, when admissibility is required.

**Lemma 41 (Closure by observational equivalence)** Under the admissibility condition, if $\Delta; \Gamma \vdash M_1 \sim_1 M_2 : \tau$ and $\Delta; \Gamma \vdash M_1 \equiv N_1 : \tau$ and $\Delta; \Gamma \vdash M_2 \equiv N_2 : \tau$, then $\Delta; \Gamma \vdash N_1 \sim_1 N_2 : \tau$. 


This lemma is used in the proof of correctness of logical equivalence.

Proof: By symmetry, we may just show it when $N_2$ is $M_2$, the case when $N_1$ is $M_1$ is symmetric and the general case follows by two applications of the lemma that falls in the two previous cases.

The proof is by induction on $\tau$.

Assume that $\Delta, \Gamma \vdash M_1 \sim M_2 : \tau$ (1) and $\Delta; \Gamma \vdash N_1 \equiv_{\eta_1} M_1$ (2). Assume $\eta$ in $D[\Delta]$ and $\gamma$ in $G[\Gamma]$. We are to show that $(\eta_1 \gamma_1 N_1, \eta_2 \gamma_2 M_2)$ is in $E[\tau]_{\eta}$. (3).

Let $C$ be the context $(\Lambda \Delta, \lambda \Gamma, [\]) \eta_1 (\Delta) \gamma_1 (\Gamma)$ where $\eta_1 \Delta$ and $\gamma_1 \Gamma$ are sequences of ground types and of closed values of ground types taken in the appropriate (i.e., reverse) order. We have $C(\Delta; \Gamma \triangleright \tau) \sim (\emptyset; \emptyset \triangleright \eta_1 \tau)$. It then follows from (2) that $C[N_1] \equiv_{\eta_1 \tau} C[M_1]$, which implies $\eta_1 \gamma_1 N_1 \equiv_{\tau} \eta_1 \gamma_1 M_1$, since observational equivalence of closed terms is closed by reduction. From (1), we have $(\eta_1 \gamma_1 M_1, \eta_2 \gamma_2 M_2)$ in $E[\tau]_{\eta}$. Then, the conclusion (3) follows by respect for observational equivalence.

Theorem 21 (Completeness of logical equivalence) Under the admissibility condition, observational equivalence implies logical equivalence.

If $\Delta; \Gamma \vdash M_1 \equiv M_2 : \tau$ then $\Delta; \Gamma \vdash M_1 \sim M_2 : \tau$.

In particular, $(\equiv_\tau) \subseteq (\sim_\tau)$ for closed types $\tau$.

Proof: Assume $\Delta; \Gamma \vdash M_1 \equiv M_2 : \tau$. The conclusion $\Delta, \Gamma \vdash M_1 \sim M_2 : \tau$. follows from the fundamental lemma, $\Delta, \Gamma \vdash M_1 \sim M_1 : \tau$ and respect for observation equivalence.

Remark Admissibility is required for completeness, but not for soundness. ($\sim_\tau$ means $\sim$ when admissibility is required—for all relations.)

As a particular case, for closed terms, we have $M_1 \sim_\tau M_2$ iff $M_1 \equiv_{\tau} M_2$.

Lemma 42 (Extensionality)

- $M_1 \equiv_{\tau \rightarrow \sigma} M_2 \iff \forall V \in \text{Val}(\tau), M_1 V \equiv_{\sigma} M_2 V \iff \forall N \in \text{Exp}(\tau), M_1 N \equiv_{\sigma} M_2 N$

- $M_1 \equiv_{\forall \alpha, \tau} M_2 \iff \forall \rho, M_1 \rho \equiv_{\tau[\alpha \mapsto \rho]} M_2 \rho$.

Extensionality does not require admissibility—since it does not refer to logical equivalence, but we need admissibility to conduct the proof, which relies on respect for observational equivalence.
CHAPTER 7. LOGICAL RELATIONS

Proof: We reason under admissibility (left implicit in notations). The right most equivalence for value abstractions results from the closure of $E[\tau]$ by reduction and anti-reduction.

The forward direction follows in both cases from the congruence of $\equiv$. The backward is as follows:

Value abstraction: It suffices to show $M_1 \sim_{\tau \rightarrow \sigma} M_2$. That is, assuming $V_1 \equiv \tau$ $V_2$ (1), we show $M_1 V_1 \sim_{\sigma} M_2 V_2$ (2). By assumption, we have $M_1 V_1 \equiv_{\sigma} M_2 V_1$ (3). By the fundamental lemma, we have $M_2 \sim_{\tau \rightarrow \sigma} M_2$. Hence, from (1), read as a logical equivalence, we deduce $M_2 V_1 \equiv_{\sigma} M_2 V_2$, We conclude (2) by respect for observational equivalence with (3).

Type abstraction: It suffices to show $M_1 \sim_{\gamma_{\alpha \rightarrow \tau}} M_2$. That is, given $R \in \mathcal{R}(\rho_1, \rho_2)$, we show $(M_1 \rho_1, M_2 \rho_2) \in E[\tau]_{\alpha \rightarrow (\rho_1, \rho_2, R)}$ (4). By assumption, we have $M_1 \rho_1 \equiv_{\tau} M_2 \rho_1$ (5). By the fundamental lemma, we have $M_2 \sim_{\gamma_{\alpha \rightarrow \tau}} M_2$. Hence, we have $(M_2 \rho_1, M_2 \rho_2) \in E[\tau]_{\alpha \rightarrow (\rho_1, \rho_2, R)}$ We conclude (4) by respect for observational equivalence with (5).

Identity extension Let $\theta$ be a substitution of type variables for ground types. Let $R$ be the restriction of $\equiv_{\alpha \theta}$ to $\text{Val}(\alpha \theta) \times \text{Val}(\alpha \theta))$ and $\eta : \alpha \mapsto (\alpha \theta, \alpha \theta, R)$. Then $E[\tau]_{\eta}$ is equal to $\equiv_{\tau \theta}$—assuming admissibility.

The proof uses respects for observational equivalence.

7.6 Applications

Exercise 43 (Inhabitants of $\forall \alpha. \alpha \rightarrow \alpha$) If $M : \forall \alpha. \alpha \rightarrow \alpha$, then $M \equiv_{\forall \alpha \rightarrow \alpha} id$ where $id \triangleq \lambda \alpha. \lambda x : \alpha. x$.

Solution: By extensionality, it suffices to show that for any $\rho$ and $V : \rho$ we have $M \rho V \equiv_{\rho} id \rho V$. In fact, by closure by inverse reduction, it suffices to show $M \rho V \equiv_{\rho} V$ (1).

By parametricity, we have $M \sim_{\forall \alpha \rightarrow \alpha} M$ (2). Consider $R$ in $\mathcal{R}(\rho, \rho)$ equal to $\{(V, V)\}$ and $\eta$ be $[\alpha \mapsto (\rho, \rho, R)]$. Since $R(V, V)$, we have $(V, V) \in \text{Val}[\alpha]_{\eta}$ by definition. Hence, from (2), we have $(M \rho V, M \rho V) \in E[\alpha]_{\eta}$, which means that the pair of expressions $(M \rho V, M \rho V)$ reduces to a pair of values in $R$ and, in particular, $M \rho V$ reduces to $V$, which implies (1).

Exercise 44 (Inhabitants of $\forall \alpha. \alpha \rightarrow \alpha \rightarrow \alpha$) If $M : \forall \alpha. \alpha \rightarrow \alpha \rightarrow \alpha$, then either $M \equiv_{\alpha}$

$W_1 \triangleq \Lambda \alpha. \lambda x_1 : \alpha. \lambda x_2 : \alpha. x_1$ or $M \equiv_{\alpha} W_2 \triangleq \Lambda \alpha. \lambda x_1 : \alpha. \lambda x_2 : \alpha. x_2$

Solution: By extensionality, it suffices to show that for either $i = 1$ or $i = 2$, for any closed type $\rho$ and $V_1, V_2 : \rho$, we have $M \rho V_1 V_2 \equiv_{\rho} W_i \rho V_1 V_2$ or just $M \rho V_1 V_2 \equiv_{\rho} W_2 \rho V_1 V_2$ (1) by closure by inverse reduction, since $W_i \rho V_1 V_2$ reduces to $V_i$.

Let $\rho$ and $V_1, V_2 : \rho$ be fixed. Consider $R$ equal to $\{(tt, V_i), (ff, V_2)\}$ in $\mathcal{R}(\text{B}, \rho)$ and $\eta$ be $\alpha \mapsto (\text{B}, \rho, R)$. We have $(tt, V_1) \in \text{Val}[\alpha]_{\eta}$ since $R(tt, V_1)$ and, similarly, $(ff, V_2) \in \text{Val}[\alpha]_{\eta}$. By parametricity, we have $(M, M) \in E[\alpha]_{\eta}$. Hence, $(M \text{ B} tt, M \rho V_1 V_2) \in E[\alpha]_{\eta}$, which means
that \((M \mathbf{B} \mathbf{t t} \mathbf{f f}, M \rho V_1 V_2)\) reduces to a pair of values in \(R\), i.e. either \((\mathbf{t t}, V_1)\) or \((\mathbf{f f}, V_2)\), which implies:

\[
\text{either } M \mathbf{B} \mathbf{t t} \mathbf{f f} \cong_M \mathbf{t t} \land M \rho V_1 V_2 \cong_M V_1 \\
\text{or } M \mathbf{B} \mathbf{t t} \mathbf{f f} \cong_M \mathbf{f f} \land M \rho V_1 V_2 \cong_M V_2
\]

In summary, we have shown

\[
\forall \rho, V_1, V_2, \quad \lor \begin{cases} M \mathbf{B} \mathbf{t t} \mathbf{f f} \cong_M \mathbf{t t} \land M \rho V_1 V_2 \cong_M V_1 \\
M \mathbf{B} \mathbf{t t} \mathbf{f f} \cong_M \mathbf{f f} \land M \rho V_1 V_2 \cong_M V_2 \end{cases}
\]

However, since \(M \mathbf{B} \mathbf{t t} \mathbf{f f}\) is independent of \(\rho, V_1, \text{and } V_2\) and the two branches are incompatible as \(\mathbf{t t} \neq \mathbf{f f}\), the choice is actually independent of \(\rho, V_1\) and \(V_2\). Therefore, we also have:

\[
\lor \begin{cases} \forall \rho, V_1, V_2, \quad M \mathbf{B} \mathbf{t t} \mathbf{f f} \cong_M \mathbf{t t} \land M \rho V_1 V_2 \cong_M V_1 \\
\forall \rho, V_1, V_2, \quad M \mathbf{B} \mathbf{t t} \mathbf{f f} \cong_M \mathbf{f f} \land M \rho V_1 V_2 \cong_M V_2 \end{cases}
\]

that is (1). \(\square\)

**Remark** Notice that the proof could have been conducted by choosing 0 and 1 of type \(\mathbf{nat}\), or even \(W_1\) and \(W_2\) of type \(\sigma\), instead of \(\mathbf{t t}\) and \(\mathbf{f f}\) of type \(\mathbf{B}\).

**Exercise 45 (Inhabitants of \(\forall \alpha. (\alpha \to \alpha) \to \alpha \to \alpha\))** Let \(\mathbf{nat}\) be \(\forall \alpha. (\alpha \to \alpha) \to \alpha \to \alpha\).

If \(M : \mathbf{nat}\), then \(M \cong_{\mathbf{nat}} N_n\) for some integer \(n\), where \(N_n \triangleq \Lambda \alpha. \lambda f : \alpha \to \alpha. \lambda x : \alpha. f^n x\).

(That is, the inhabitants of \(\mathbf{nat}\) are the Church naturals.)

**Solution:** By extensionality, it suffices to show that there exists \(n\) such for any closed type \(\rho\) and closed values \(V_1 : \rho \to \rho\) and \(V_2 : \rho\), we have \(M \rho V_1 V_2 \cong_M N_n \rho V_1 V_2\), or, by closure by inverse reduction, \(M \rho V_1 V_2 \cong_M V_1^n V_2\) (1).

Let \(\rho\) and \(V_1 : \rho \to \rho\) and \(V_2 : \rho\) be fixed. Let \(Z\) and \(S\) be \(M_0 \mathbf{nat}\) and \(M_2 \mathbf{nat}\). Let \(R\) be \(\{(S^k Z, V_1^k V_2) \mid k \in \mathbb{N}\}\) in \(R(\mathbf{nat}, \rho)\) and \(\eta\) be \(\alpha \mapsto (\mathbf{nat}, \rho, R)\).

We have \((Z, V_2) \in \mathbb{V}[\alpha]_\eta\) (2). We also have \((S, V_1) \in \mathbb{V}[\alpha \to \alpha]_\eta\) (3), (which is a key to the proof). Indeed, assume \((W_1, W_2)\) is in \(\mathbb{V}[\alpha]_\eta\), that is, of the form \((S^k Z, V_1^k V_2)\). for some \(k\). Then, \((S W_1, V_1 W_2)\) is equal to \((S^{k+1} Z, V_1^{k+1} V_2)\), which belongs to \(\mathbb{E}[\alpha]_\eta\).

By parametricity, we have \(M \cong_{\mathbf{nat}} M\). Hence, the pair \((M \mathbf{nat} S Z, M \rho V_1 V_2)\) is in \(\mathbb{E}[\alpha]_\eta\). Thus, it must reduce to a pair in \(\mathbb{V}[\alpha]_\eta\), i.e. \(R\). Therefore, there exists \(n\) such that \(M \mathbf{nat} S Z \cong_{\mathbf{nat}} S^n Z\) and \(M \rho V_1 V_2 \cong_M V_1^n V_2\) We have shown,

\[
\forall \rho, \forall V_1 \in \mathbb{V}[\rho \to \rho], \forall V_2 \in \mathbb{V}[\rho], \exists n \in \mathbb{N}, \quad M \mathbf{nat} S Z \cong_{\mathbf{nat}} S^n Z \land M \rho V_1 V_2 \cong_M V_1^n V_2
\]

Since, \(M \mathbf{nat} S Z\) is independent of \(n\), and all \(S^n Z\) are in different observational equivalence classes (which is easy to prove, e.g. by applying it to the successor function and primitive integer 0), \(n\) is actually independent of \(V_1\) and \(V_2\). Hence, we have:

\[
\exists n \in \mathbb{N}, \forall \rho, \forall V_1 \in \mathbb{V}[\rho \to \rho], \forall V_2 \in \mathbb{V}[\rho], \quad M \mathbf{nat} S Z \cong_{\mathbf{nat}} S^n Z \land M \rho V_1 V_2 \cong_M V_1^n V_2
\]

which implies (1). \(\square\)
7.7 Extensions

7.7.1 Natural numbers

We have shown that all expressions of type nat behave as natural numbers. Hence, natural numbers are definable in System F.

Still, we can also provide a type nat of primitive natural numbers. Then we would define behavioral equivalence on nat as the relation in Val(nat) × Val(nat) by

\[ M_1 \equiv_{\text{nat}} M_2 \overset{\text{def}}{\iff} \exists n : \text{nat}, M_1 \Downarrow n \land M_2 \Downarrow n \]

As for the logical equivalence, we defined

\[ \mathcal{V}[\text{nat}] = \{(n, n) \mid n \in \text{Val(nat)}\} \]

Notice that nat is another observable type. All properties are preserved.

7.7.2 Products

\textbf{Encodable} Given closed types \( \tau_1 \) and \( \tau_2 \), we defined

\[ \tau_1 \times \tau_2 \overset{\Delta}{=} \forall \alpha. (\tau_1 \to \tau_2 \to \alpha) \to \alpha \]

\[ (M_1, M_2) \overset{\Delta}{=} \Lambda \alpha. \lambda x : \tau_1 \to \tau_2 \to \alpha. x M_1 M_2 \]

\[ M.i \overset{\Delta}{=} M (\lambda x_1 : \tau_1. \lambda x_2 : \tau_2. x_i) \]

\textbf{Lemma 43}

If \( M : \tau_1 \times \tau_2 \), then \( M \equiv_{\tau_1 \times \tau_2} (M_1, M_2) \) for some \( M_1 : \tau_1 \) and \( M_2 : \tau_2 \).

If \( M : \tau_1 \times \tau_2 \) and \( M.1 \equiv_{\tau_1} M_1 \) and \( M.2 \equiv_{\tau_2} M_2 \), then \( M \equiv_{\tau_1 \times \tau_2} (M_1, M_2) \)

\textbf{Primitive} With primitive pairs, we define:

\[ \mathcal{V}[\tau \times \sigma]_\eta \overset{\Delta}{=} \{ ((V_1, W_1), (V_2, W_2)) \mid (V_1, V_2) \in \mathcal{V}[\tau]_\eta \land (W_1, W_2) \in \mathcal{V}[\sigma]_\eta \} \]

7.7.3 Sums

\[ \mathcal{V}[\tau + \sigma]_\eta \overset{\Delta}{=} \{ (\text{inj}_1 V_1, \text{inj}_1 V_2) \mid (V_1, V_2) \in \mathcal{V}[\tau]_\eta \} \cup \{ (\text{inj}_2 W_1, \text{inj}_2 W_2) \mid (W_1, W_2) \in \mathcal{V}[\sigma]_\eta \} \]

Notice that sums, as all datatypes, can also be encoded in System F.

7.7.4 Lists

We could extend the language with lists and define:

\[ \mathcal{V}[\text{list } \tau]_\eta \overset{\Delta}{=} \{ ([V_1^1; \ldots; V_1^n], [V_2^1; \ldots; V_2^n]) \mid n \in \mathbb{N} \land \forall k \in [1, n], (V_1^k, V_2^k) \in \mathcal{V}[\tau]_\eta \} \]
Assume that $\alpha \mapsto (\rho_1, \rho_2, R)$ is in $\eta$ such that $R$ in $\mathcal{R}(\rho_1, \rho_2)$ represents the graph $(g)$ of a function $g : \rho_1 \rightarrow \rho_2$, that is $R = \{(V_1, V_2) \mid g V_1 \downarrow V_2\}$.

Then $\mathcal{V}[\text{list } \alpha]_\eta$ is equal to $(\text{map } \rho_1 \rho_2, g)$, that is composed of all pairs $(V_1, V_2)$ such $\text{map } \rho_1 \rho_2 g W_1 \downarrow W_2$.

Indeed, a pair $(W_1, W_2)$ in $\mathcal{V}[\text{list } \alpha]_\eta$ is of the form $\{(V_1; \ldots V_n), [V'_1; \ldots V'_n]\}$ for some $n$ where all pairs $(V_1^k, V_2^k)$ are in $\mathcal{V}[\tau]_\eta$, that is, $\vartriangleleft g$, hence such that $g V_1 \downarrow V_2$. Therefore $[g V_1^1; \ldots g V_1^n] \downarrow [V'_1; \ldots V'_n]$. That is, $\text{map } \rho_1 \rho_2 W_1 \downarrow W_2$.

**Exercise 46 (sort)**

Assume $\text{sort} : \forall \alpha. (\alpha \rightarrow \alpha \rightarrow \mathbb{B}) \rightarrow \text{list } \alpha \rightarrow \text{list } \alpha (1)$. Show that for all $g$ of ground type $\rho_1 \rightarrow \rho_2$, and all (comparison) functions $\text{cmp}_1$ of type $\rho_1 \rightarrow \rho_1 \rightarrow \mathbb{B}$ and $\text{cmp}_2$ of type $\rho_2 \rightarrow \rho_2 \rightarrow \mathbb{B}$ satisfying

$$\forall V, W \in \text{Val}(\rho_1), \ \text{cmp}_2 (g V) (g W) \cong \text{cmp}_1 V W$$

we have, for all $U$ in $\text{Val(\text{list } \rho_1)}$,

$$\text{sort } \rho_2 \text{ cmp}_2 (\text{map } \rho_1 \rho_2 g U) \cong \text{map } \rho_1 \rho_2 g (\text{sort } \rho_1 \text{ cmp}_1 U)$$

**Solution:** Let $\rho_1$ and $\rho_2$ be fixed and $g$ be a function $g$ satisfying (2). We show (3). By the fundamental lemma applied to (1), we have $\text{sort } \vartriangleleft \text{sort}$ where $\vartriangleleft$ is $\forall \alpha. (\alpha \rightarrow \alpha \rightarrow \mathbb{B}) \rightarrow \text{list } \alpha \rightarrow \text{list } \alpha$. Thus, for all $\rho_1$, $\rho_2$, relations $R$ in $\mathcal{R}(\rho_1, \rho_2)$, we have

$$\forall (\text{cmp}_1, \text{cmp}_2) \in \mathcal{V}[\alpha]_\eta, \ \forall (V_1, V_2) \in \mathcal{V}[\text{list } \alpha]_\eta, (\text{sort } \rho_1 \text{ cmp}_1 V_1, \text{sort } \rho_2 \text{ cmp}_2 (V_2)) \in \mathcal{E}[\text{list } \alpha]_\eta$$

where $\eta$ is $\alpha \mapsto (\rho_1, \rho_2, R))$. We may choose $R$ to be the graph $(g)$ of the function $g$.

Let us show (4). Let $(V_1, V_2)$ and $(W_1, W_2)$ be in $\mathcal{V}[\alpha]_\eta$, i.e. $g V_1 \downarrow V_2$ and $g W_1 \downarrow W_2$. Hence $\text{cmp}_2 (g V_1) (g W_1) \cong \text{cmp}_2 V_2 W_2$. Which implies $\text{cmp}_2 (g V_1) (g W_1) \cong \text{cmp}_2 V_2 W_2$. Combining with (2), we have $\text{cmp}_1 V_1 W_1 \cong \text{cmp}_2 V_2 W_2$. Since we are at type $\mathbb{B}$, this coincide with logical equivalence, which proves $\text{cmp}_1, V_1 W_1, \text{cmp}_2, V_2 W_2) \in \mathcal{E}[\mathbb{B}]_\eta$, as expected.

Therefore, (5) holds, which given that $\mathcal{V}[\alpha]_\eta$ is equal to $(\text{map } \rho_1 \rho_2, g)$, reads

$$\forall V_1 : \text{list } \rho_1, V_2 : \text{list } \rho_2, \ \left\{ \begin{array}{l}
\text{map } \rho_1 \rho_2 g V_1 \downarrow V_2 \implies \exists W_1, W_2, \text{map } \rho_1 \rho_2 g W_1 \downarrow W_2 \\
\text{sort } \rho_1 \text{ cmp}_1 V_1 \downarrow W_1 \\
\text{sort } \rho_2 \text{ cmp}_2 V_2 \downarrow W_2
\end{array} \right.$$
Which implies
\[ \forall V : \text{list} \, \rho_1,
          \map \, \rho_1 \, \rho_2 \, g \, (\text{sort} \, \rho_1 \, \text{cmp}_1 \, V) \cong \text{sort} \, \rho_2 \, \text{cmp}_2 \, (\map \, \rho_1 \, \rho_2 \, g \, V) \]

7.7.5 Existential types

We define:
\[ \forall \exists \alpha. \tau \eta \triangleq \{ (\text{pack} \, V_1, \rho_1 \, \text{as} \, \exists \alpha. \tau, \text{pack} \, V_2, \rho_2 \, \text{as} \, \exists \alpha. \tau) \mid V_1 \vdash \eta_1 (\exists \alpha. \tau) \land V_2 \vdash \eta_2 (\exists \alpha. \tau) \land \exists \rho_1, \rho_2, R \in \mathcal{R}(\rho_1, \rho_2), (V_1, V_2) \in \mathcal{E}[\tau]_{\eta, \rho_1 \mapsto (\rho_1, \rho_2, R)} \} \]

Example 3 Consider \( V_1 \triangleq (\text{not}, \text{tt}) \) and \( V_2 \triangleq (\text{succ}, 0) \) and \( \sigma \triangleq (\alpha \to \alpha) \times \alpha \). Let \( R \) in \( \mathcal{R}(\text{B}, \text{nat}) \) be \( \{(\text{tt}, 2n), (\text{ff}, 2n + 1) \mid n \in \mathbb{N}\} \) and \( \eta \) be \( \alpha \mapsto (\text{B}, \text{nat}, R) \).

We have \( (\text{pack} \, V_1, \text{B} \, \text{as} \, \exists \alpha. \sigma, \text{pack} \, V_2, \text{nat} \, \text{as} \, \exists \alpha. \sigma) \in \forall \exists \alpha. \sigma \eta \). To see this it suffices to show \( (V_1, V_2) \in \forall \exists \sigma \eta \), that is \( ((\text{not}, \text{tt}), (\text{succ}, 0)) \in \forall [(\alpha \to \alpha) \times \alpha] \eta \). In turn, it suffices to show both \( \text{(not, succ)} \in \forall [\alpha \to \alpha] \eta \) and \( (\text{tt}, 0) \in \forall [\alpha] \eta \). The latter holds by construction since \( (\text{tt}, 0) \in R \). To show the former, we assume \( (W_1, W_2) \in \forall [\alpha] \eta \), i.e. in \( R \). Hence, it must be either of the form

- \( (\text{tt}, 2n) \); and \( \text{(not } W_1, \text{succ } W_2) \) reduces to \( (\text{ff}, 2n + 1) \), or of the form

- \( (\text{ff}, 2n + 1) \) and \( \text{(not } W_1, \text{succ } W_2) \) reduces to \( (\text{tt}, 2n + 2) \).

In both cases, \( \text{(not } W_1, \text{succ } W_2) \) reduces to a pair in \( R \), i.e. in \( \forall [\alpha] \eta \), hence it is in \( \forall [\alpha] \eta \).

Representation independence A client of an existential type \( \exists \alpha. \tau \) should not see the difference between two implementations \( N_1 \) and \( N_2 \) of \( \exists \alpha. \tau \) with witness types \( \rho_1 \) and \( \rho_2 \).

Assume that \( \rho_1 \) and \( \rho_2 \) are two closed representation types and \( R \) is in \( \mathcal{R}(\rho_1, \rho_2) \). Let \( \eta \) be \( \alpha \mapsto (\rho_1, \rho_2, R) \). Suppose that \( N_1 : \tau[\alpha \mapsto \rho_1] \) and \( N_2 : \tau[\alpha \mapsto \rho_2] \) are two equivalent implementations of the operations, i.e. \( (N_1, N_2) \in \mathcal{E}[\tau] \eta \).

A client \( M \) has type \( \forall \alpha. \tau \to \sigma \) with \( \alpha \notin \text{fv}(\sigma) \); it must use the argument parametrically, and the result is independent of the witness type. Indeed the client satisfies \( (M, M) \in \mathcal{E}[\forall \alpha. \tau \to \sigma] \eta \) and therefore \( (M \, \rho_1 \, N_1, M \, \rho_2 \, N_2) \) is in \( \mathcal{E}[\sigma] \) (as \( \alpha \) is not free in \( \sigma \)), which implies \( M \, \rho_1 \, N_1 \cong \sigma \, M \, \rho_2 \, N_2 \).

That is, the behavior with the implementation \( N_1 \) with representation type \( \rho_1 \) is indistinguishable from the behavior with implementation \( N_2 \) with representation type \( \rho_2 \).
7.7. EXTENSIONS

7.7.6 Step-indexed logical relations

How do we deal with recursive types? Assume that we allow equi-recursive types.

\[ \tau ::= \ldots | \mu \alpha. \tau \]

A naive definition would be

\[ V[\mu \alpha. \tau]_\eta = V[[\alpha \mapsto \mu \alpha. \tau]]_{\eta} \]

But this is ill-founded, because \([\alpha \mapsto \mu \alpha. \tau]_{\tau}\) is usually larger than \(\tau\).

The solution is to use indexed-logical relations.

We use a sequence of decreasing relations indexed by integers (fuel), which is consumed during unfolding of recursive types.

**Step-indexing (a taste)** We define a sequence \(V_k[\tau]_\eta\) indexed by natural numbers \(n \in \mathbb{N}\) that relates values of type \(\tau\) up to \(n\) reduction steps.

\[
\begin{align*}
V_k[B]_\eta &= \{(tt, tt), (ff, ff)\} \\
V_k[\tau \rightarrow \sigma]_\eta &= \{(V_1, V_2) | \forall j < k, \forall (W_1, W_2) \in V_j[\tau]_\eta, (V_1, W_1, V_2, W_2) \in E_j[\sigma]_\eta\} \\
V_k[\alpha]_\eta &= (\eta R\alpha).k \\
V_k[\forall \alpha. \tau]_\eta &= \{(V_1, V_2) | \forall \rho_1, \rho_2, R \in R^k(\rho_1, \rho_2), \forall j < k, (V_1, \rho_1, V_2, \rho_2) \in V_j[\tau]_{\eta, \alpha \mapsto (\rho_1, \rho_2, R)}\} \\
V_k[\mu \alpha. \tau]_\eta &= V_{k-1}[\alpha \mapsto \mu \alpha. \tau]_\eta \\
E_k[\tau]_\eta &= \{(M_1, M_2) | \forall j < k, M_1 \Downarrow_j V_1 \implies \exists V_2, M_2 \Downarrow_j V_2 \land (V_1, V_2) \in V_{k-j}[\tau]_\eta\}
\end{align*}
\]

By \(\Downarrow_j\), we mean *reduces in \(j\)-steps*. \(R^j(\rho_1, \rho_2)\) is a sequence of decreasing relations between closed values of closed types \(\rho_1\) and \(\rho_2\) of length (at least) \(j\).

Notice that the relation is asymmetric.

We define

\[
\Delta; \Gamma \vdash M_1 \preceq M_2 : \tau \overset{\text{def}}{=} \left\{ \begin{array}{l}
\forall \eta \in R^k_{\Delta}(\delta_1, \delta_2), \forall (\gamma_1, \gamma_2) \in \mathcal{G}_k[\Gamma], \\
(\gamma_1(\delta_1(M_1)), \gamma_2(\delta_2(M_2))) \in E_k[\tau]_\eta
\end{array} \right\}
\]

and

\[
\Delta; \Gamma \vdash M_1 \sim M_2 : \tau \overset{\text{def}}{=} \bigwedge \left\{ \Delta; \Gamma \vdash M_1 \preceq M_2 : \tau \bigwedge \Delta; \Gamma \vdash M_2 \preceq M_1 : \tau \right\}
\]

Notations and proofs get a bit involved.
Bibliography

▷ A tour of scala: Implicit parameters. Part of scala documentation.


BIBLIOGRAPHY


François Pottier. A typed store-passing translation for general references. In *Proceedings of the 38th ACM Symposium on Principles of Programming Languages (POPL’11)*, Austin, Texas, January 2011. [Supplementary material](#)


