Report

The HOL–OCL book
Version 0.9.0

Author(s):
Brucker, Achim D.; Wolff, Burkhart

Publication Date:
2006

Permanent Link:
https://doi.org/10.3929/ethz-a-006781813

Rights / License:
In Copyright - Non-Commercial Use Permitted
The HOL-OCL Book

Version 0.9.0

http://www.brucker.ch/research/hol-ocl/

Achim D. Brucker       Burkhart Wolff

August 15, 2006

Information Security
Swiss Federal Institute of Technology (ETH)
8092 Zurich
Switzerland
Important note:
This manual describes HOL-OCL 0.9.0 with referential universes and smashed collection types.
The manual of version 0.9.0 is also available as technical report number 525 from the department of computer science, ETH Zurich.
# Contents

## I. Motivation and Introduction

1. Introduction
   1.1. Motivation ................................................................. 11
   1.2. How to Read This Document ........................................... 13
   1.3. Typographic Conventions ............................................. 14
   1.4. Acknowledgements ..................................................... 15

## II. Theory

3. Foundations
   3.1. An Overview of Embedding Techniques ................................ 27
   3.2. Embeddings of Specification Languages ............................... 28
   3.3. Challenges of a Shallow Embedding of UML/OCL .................... 29
   3.4. An Overview over Embedding Techniques ............................... 31

4. Faithfully Representing UML/OCL
   4.1. A Note About Standard Compliance ................................... 33
   4.2. Building-Blocks of the HOL-OCL Architecture ....................... 35
   4.3. Formal Preliminaries for Representing Semantics in HOL .......... 37
   4.4. Encoding Standard OCL Operations .................................... 39
   4.5. Textbook vs. Combinator Style Semantics of Operations .......... 40
   4.6. Compliance to the Standards OCL Requirements ..................... 42
   4.7. Organizing the Embedding into Layer ................................ 43
      4.7.1. Datatype Adaption .................................................. 45
      4.7.2. Functional Adaption .............................................. 46
      4.7.3. Embedding Adaption for Shallow Embedding .................... 48
   4.8. Extensible Universes in Typed Meta-Language ....................... 49
   4.9. Encoding Object Structures .......................................... 50
Contents

4.9.1. The Basics ............................................................ 50
4.9.2. The Formal Details of Encoding Object Structures .......... 53
4.9.3. Type Constructions ............................................... 54
4.9.4. Treatment of Instances .......................................... 57
4.9.5. Adaptation to Higher Layers .................................. 59

4.10. Faithful Representing UML Object Structures ............... 60

4.11. A Constrained Object Store ...................................... 61
4.11.1. A Co-Recursive Type and Kind Set Construction ............ 61
4.11.2. Functional Adoption: Invariant Awareness .................... 63
4.11.3. Defining Invariants ........................................... 63

4.12. An Object-Oriented Type-System ................................ 64

4.13. Operation Invocations ............................................. 64
4.13.1. The Invocation Encoding Scheme ............................... 65
4.13.2. Considering Conservativity .................................... 67
4.13.3. Limits to Recursive Invocations ............................... 68

4.14. Comparing the Referential and Non-Referential Universe .... 70

4.15. Specifying Frame Properties ..................................... 75

5. Calculi ....................................................................... 77
5.1. A Theory of Basic Judgement ....................................... 78
5.2. Basic Equivalences and Congruences .............................. 79
5.3. Reasoning on Context-Passing Predicate $cp$ ................... 80
5.4. Reasoning on Undefinedness and Definedness .................. 81
5.5. Logical Bridges Between $UC$, $LE$, $LJE$, and $LTC$ .......... 84
5.6. The Logics .................................................................. 84
5.6.1. Reasoning over Strong and Strict Equality .................. 84
5.6.2. Core-Logic (Boolean) ............................................ 85
5.6.3. Set Theory and Logics ........................................... 85
5.7. Arithmetic Computational Rules .................................. 89
5.8. Converting OCL to HOL ............................................. 90
5.9. The Judgement Tableaux Calculus LTC .......................... 90
5.10. Towards Automated Deduction in HOL-OCL ................... 91

6. The HOL-OCL System Architecture .................................. 97
6.1. An Architectural Overview ......................................... 97
6.2. The Model Repository: su4sml ................................. 97
6.3. The Encoder: An Object-oriented Datatype Package ......... 101
6.4. The HOL-OCL-Library .............................................. 103
6.5. The Theory-Morpher ................................................ 103

III. System Description ................................................. 105
## Contents

### 7. Installing HOL-OCL

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1. Prerequisites</td>
<td>107</td>
</tr>
<tr>
<td>7.2. Installation</td>
<td>107</td>
</tr>
<tr>
<td>7.2.1. Installation from Source</td>
<td>107</td>
</tr>
<tr>
<td>7.2.2. Using Debian Packages</td>
<td>108</td>
</tr>
<tr>
<td>7.3. Starting</td>
<td>109</td>
</tr>
</tbody>
</table>

### 8. Limitations of HOL-OCL

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1. The Supported UML Subset</td>
<td>113</td>
</tr>
<tr>
<td>8.2. The Supported OCL Subset</td>
<td>114</td>
</tr>
<tr>
<td>8.2.1. OCL Syntactical Variants</td>
<td>114</td>
</tr>
<tr>
<td>8.2.2. OCL context declarations</td>
<td>114</td>
</tr>
<tr>
<td>8.2.3. OCL Types</td>
<td>115</td>
</tr>
<tr>
<td>8.2.4. Predefined Properties</td>
<td>116</td>
</tr>
<tr>
<td>8.3. Reporting Bugs</td>
<td>116</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1. The Basic Workflow</td>
<td>117</td>
</tr>
<tr>
<td>9.2. The Modelling Phase</td>
<td>117</td>
</tr>
<tr>
<td>9.3. Using HOL-OCL: The Verification Phase</td>
<td>120</td>
</tr>
<tr>
<td>9.3.1. Getting Started</td>
<td>121</td>
</tr>
<tr>
<td>9.3.2. Loading XMI files</td>
<td>121</td>
</tr>
<tr>
<td>9.3.3. Canonizing Hypotheses</td>
<td>121</td>
</tr>
<tr>
<td>9.3.4. One-Step-Rewriting</td>
<td>122</td>
</tr>
<tr>
<td>9.3.5. Automated Proof-Procedures</td>
<td>122</td>
</tr>
<tr>
<td>9.4. Extending HOL-OCL</td>
<td>123</td>
</tr>
</tbody>
</table>

### 10. Case Studies

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1. Encoding a Stack in UML/OCL</td>
<td>125</td>
</tr>
</tbody>
</table>

### IV. Appendix

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. The Syntax of OCL</td>
<td>129</td>
</tr>
<tr>
<td>B. Isabelle Theories</td>
<td>135</td>
</tr>
<tr>
<td>B.1. Introduction</td>
<td>135</td>
</tr>
<tr>
<td>B.1.1. HOL-OCL Configurations</td>
<td>135</td>
</tr>
<tr>
<td>B.1.2. Notational Remarks</td>
<td>137</td>
</tr>
<tr>
<td>B.2. Overview</td>
<td>137</td>
</tr>
<tr>
<td>B.3. Foundations</td>
<td>138</td>
</tr>
<tr>
<td>B.3.1. The Theory of Lifting and its Combinators</td>
<td>138</td>
</tr>
<tr>
<td>B.3.2. The OCL Kernel</td>
<td>161</td>
</tr>
<tr>
<td>B.3.3. Type Definition for OclUndefined</td>
<td>162</td>
</tr>
<tr>
<td>B.3.4. Type Definition for Boolean</td>
<td>163</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>B.3.5. Type Definition for Integer</td>
<td>164</td>
</tr>
<tr>
<td>B.3.6. Type Definition for Real</td>
<td>164</td>
</tr>
<tr>
<td>B.3.7. Type Definition for String</td>
<td>164</td>
</tr>
<tr>
<td>B.3.8. Type Definition for OclAny</td>
<td>165</td>
</tr>
<tr>
<td>B.3.9. Type Definition for Collections</td>
<td>166</td>
</tr>
<tr>
<td>B.3.10. Type Definition for Set</td>
<td>166</td>
</tr>
<tr>
<td>B.3.11. Type Definition for Sequence</td>
<td>166</td>
</tr>
<tr>
<td>B.3.12. Type Definition for Bag</td>
<td>167</td>
</tr>
<tr>
<td>B.3.13. Type Definition for OrderedSet</td>
<td>167</td>
</tr>
<tr>
<td>B.3.14. The OCL Universe</td>
<td>168</td>
</tr>
<tr>
<td>B.4. Library</td>
<td>171</td>
</tr>
<tr>
<td>B.4.1. The OCL let expression</td>
<td>171</td>
</tr>
<tr>
<td>B.4.2. OCL Boolean</td>
<td>171</td>
</tr>
<tr>
<td>B.4.3. OCL Logic Core</td>
<td>200</td>
</tr>
<tr>
<td>B.4.4. OCL Logic</td>
<td>225</td>
</tr>
<tr>
<td>B.4.5. Numerals</td>
<td>229</td>
</tr>
<tr>
<td>B.4.6. OCL Integer</td>
<td>231</td>
</tr>
<tr>
<td>B.4.7. OCL Real</td>
<td>236</td>
</tr>
<tr>
<td>B.4.8. OCL String</td>
<td>238</td>
</tr>
<tr>
<td>B.4.9. OCL Collection</td>
<td>240</td>
</tr>
<tr>
<td>B.4.10. OCL Sequence</td>
<td>250</td>
</tr>
<tr>
<td>B.4.11. OCL Bag</td>
<td>316</td>
</tr>
<tr>
<td>B.4.12. OCL OrderedSet</td>
<td>346</td>
</tr>
<tr>
<td>B.4.13. OCL Set</td>
<td>355</td>
</tr>
<tr>
<td>B.4.14. OclAny</td>
<td>379</td>
</tr>
<tr>
<td>B.4.15. CharacteristicSets</td>
<td>383</td>
</tr>
<tr>
<td>B.4.16. The OCL Library</td>
<td>386</td>
</tr>
<tr>
<td>B.5. State</td>
<td>387</td>
</tr>
<tr>
<td>B.5.1. OCL State</td>
<td>387</td>
</tr>
<tr>
<td>B.5.2. The OCL Calculi</td>
<td>389</td>
</tr>
<tr>
<td>B.5.3. Encoding of OCL Operations</td>
<td>400</td>
</tr>
<tr>
<td>B.5.4. The Object Constraint Language: OCL</td>
<td>404</td>
</tr>
<tr>
<td>B.6. Requirements</td>
<td>404</td>
</tr>
<tr>
<td>B.6.1. Requirements for OCL Primitive Types</td>
<td>404</td>
</tr>
<tr>
<td>B.6.2. OCL Collection requirements</td>
<td>409</td>
</tr>
<tr>
<td>B.6.3. OCL Iterator requirements</td>
<td>431</td>
</tr>
<tr>
<td>B.7. OCL</td>
<td>437</td>
</tr>
<tr>
<td>B.7.1. The Object Constraint Language: OCL</td>
<td>437</td>
</tr>
</tbody>
</table>

## C. Encoding UML/OCL by Example

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>C.1. Encoding UML/OCL into HOL by Example</td>
<td>439</td>
</tr>
<tr>
<td>C.2. A Simple Example</td>
<td>439</td>
</tr>
<tr>
<td>C.3. Importing UML/OCL models</td>
<td>439</td>
</tr>
<tr>
<td>C.3.1. Encoding Level 0</td>
<td>440</td>
</tr>
<tr>
<td>C.3.2. Encoding Level 1</td>
<td>447</td>
</tr>
</tbody>
</table>
Contents

C.3.3. Encoding Level 2: ......................... 456

D. The GNU General Public Licence 473
  D.1. Preamble .................................. 473  
  D.2. Terms and conditions for copying, distribution and modification 474
  D.3. Appendix: How to Apply These Terms to Your New Programs . . . . 478

V. Bibliography and Index 481

  Bibliography 483
  List of Glitches 491
  List of Extensions 493
  List of Figures 495
  List of Tables 497
  List of Definitions 499
  Listings 501
Part I.

Motivation and Introduction
Chapter 1.

Introduction

1.1. Motivation

Building safe and secure software systems requires engineering techniques. Just as using “blueprints” in common engineering practice, the development of complex software systems requires a detailed specification describing its data structures and its desired behavior. Specification documents can vary in its precision from textual descriptions over structured text up to formal specification using a language based on mathematical logic such as Z [26] or VDM [27]. Depending on the precision (or formality), different computer-supported techniques can be applied that assure the consistency of specification documents. For example, type-checking or wellformedness-checking can be used to find contradictions in requirement and design documents of a system and thus provide an a-priori analysis. Moreover, more involved techniques can assure the correct transition from a specification document to its implementation in “real code”; such an a-posteriori analysis techniques is called validation. These techniques and their computer-support are summarized under the term formal methods. Obviously, the power of these techniques crucially depends on the degree of formality.

Producing formal specifications and maintaining their consistency during system development is a task that requires substantial efforts and training. This holds to an even larger extent for the validation phase, where techniques such as model-based testing, model-checking or even interactive theorem proving were applied. For this reason, the acceptance of formal methods has been very reluctant in industrial practice so far, although it is meanwhile widely accepted that specification and testing activities outweigh by far the costs of the implementation phase of a large system and that formal methods have a positive effect here. Rather, the overwhelming need for specification led to the development of semi-formal specification documents, that have their roots in light-weighed graphical notations. These semi-formal kinds of documents became eventually a more and more defined semantics and were annotated by programs or abstract test code. Thus, instead of using mathematical notation such as Z or the Hoare Calculus, there is a trend to introduce formal specification techniques such as pre and post conditions through the backdoor, leading to a more gradual transition of the industrial practice by bridging the gap to software developers by languages and notations they are familiar with.

The need for computer-support of these “light-weighed” specification methods led to a standardization effort and the Unified Modelling Language (UML), which achieved
Chapter 1. Introduction

remarkable acceptance in the industry. The UML offers an integrated object-oriented development methodology ranging from “object-oriented modeling” to code-generation in “model-based architecture” development. The UML is continuously defined by the Object Management Group (OMG) [41], an open standardization committee. The UML provides standards for graphical notations, their representation in abstract syntax (called meta-models) and partly also their semantics. These notations comprise among others activity charts, sequence charts, class diagrams and state charts. The latter two notations are of particular interest from the perspective of formal methods, since they represent forms of data-oriented and behavioral modeling, thus well-known concepts in a new shape. Moreover, since UML 1.3, a logical annotation formalism, called the Object Constraint Language (OCL) is a part of the UML and is heavily used in the specification documents of the meta-models of the UML itself.

To sum up, from the perspective of formal methods, the success of CASE tools supporting the UML [40] opens a door for bringing formal methods a step closer to industry. However, to turn this vision into reality, several challenges need to be faced: first, the semantics of UML/OCL is conceptually much closer to an object-oriented programming language than to a traditional logic, although OCL comprises a version of predicate logic and arithmetic. Second, considerable effort has to be invested to cope with the object-oriented features of OCL in a logically clean way, allowing for adequate symbolic computations. Third, a considerable research effort has to be invested to develop an adequate proof methodology for object-oriented modeling as it is meanwhile established in the user community of UML/OCL.

As a technical basis for a long-term effort to meet these challenges, we developed HOL-OCL, an interactive proof environment for acsocl. The main design goals of HOL-OCL are summarized as follows:

- HOL-OCL follows semantically the OCL 2.0 standard [41],
- HOL-OCL provides technical support for importing UML/OCL models (i.e., class-diagrams at the moment, start charts are under preparation) in form of XMI-formats generated by conventional UML/OCL modeling tools, and
- HOL-OCL is intended to analyze UML/OCL models with all the means provided by an up-to-date interactive, tactic-controlled theorem proving environment such as Isabelle [3].

In itself, HOL-OCL also provides achievements for the definition and development of the language UML/OCL itself:

- It defines and supports several syntactic formats for OCL (one more text-oriented for programmers and software developers, another more mathematical one for proof engineers).
- It defines a machine-checked formalization of the semantics as described in the standard 2.0. This is implemented as a conservative, shallow embedding consisting of OCL into the higher-order logic (HOL) instance of the interactive theorem
prover Isabelle. This includes a typed, extensible UML data models supporting inheritance and subtyping inside the typed lambda-calculus with parametric polymorphism. As consequence of conservativity with respect to HOL, we can guarantee the consistency of the semantic model (see 3 and in particular 2.1 for an in depth discussion). In fact, we consider it as an important contribution to provide a candidate for a “beau ideal” of the OCL semantics.

- The standard 2.0 postulates requirements to the semantics of OCL operators. The OCL semantics—which is contained in an appendix of the standards documents—is not formally related to these requirements. We provide formal proofs that our formalization of the OCL semantics indeed meets the requirements.

- In some (minor) parts, our work detected formal contradictions or inconveniences with respect to derived calculi. We strive for compliance with the standard 2.0. With respect to the faithfulness of our representation, see Sec. 4.5).

- It provides several derived calculi for UML/OCL that allows for formal derivations establishing the validity of UML/OCL formulae. Automated support for such proofs is also provided, however since HOL-OCL comprises predicate logic with equality and a typed set-theory, the validity of a formula is undecidable and the logic is inherently incomplete with respect to the class of standard models of HOL [8].

- It represents a technical framework (including a graphical front-end in form of ProofGeneral [5] and a programming interface for SML) enabling to implement particular formal methods based on UML/OCL.

These future method supports can be, for example,

- consistency checking of UML models (e.g., is a class-diagram implementable, i.e., do states exist that satisfy the invariants? Contradict pre-conditions and post-conditions to system invariants?),

- proving refinements between UML models,

- code verification of concrete programs with respect to a UML model by means of a Hoare-Calculus,

- proving temporal properties of UML models (e.g., do all reachable states satisfy a security-property?),

- automated test-case generation out of UML models for concrete code.

1.2. How to Read This Document

This book has three different aspects and describes them at various levels of detail. Therefore, we divided the material into three parts which can be read largely independently from each other:
Chapter 1. Introduction

- Part I gives an overall introduction and motivation. In particular, it introduces into the foundational notations and the target language.
- Part II presents the concepts of the underlying ideas and formalization techniques behind HOL-OCL.
- Part III explains the HOL-OCL system from a users perspective and can be seen as a kind of “users manual.”

Further, in the appendix a complete companion of the Isabelle theory files is provided, including the technical details of HOL-OCL and reference material such as, e.g., tables that compare different OCL syntax.

Depending on your background knowledge and interests, we recommend kind of cherry-picking strategy for reading this book. For example,

- If you are a HOL-OCL user and want to get a quick “hands-on” experience you may start with the installation instructions (chapter 7) and start reading with chapter 1 and chapter 2. You can then continue directly with chapters 9 and 10.
- If you are interested in the ideas and techniques of HOL-OCL we recommend (after reading the introductory chapters 1 and 2) an in depth study of chapters 3 to 5.
- If you are an Isabelle hacker and are interested in the details necessary for theorem proving work you can directly start with the theory-files in the appendix, i.e., chapter B. However, we advise to start with the more conceptual descriptions in 5.

1.3. Typographic Conventions

The following typographic conventions appear in this book:

- Pure OCL specifications are either written inline like `self.s->includes(5)` or together with their context specification:

<table>
<thead>
<tr>
<th>context A:</th>
</tr>
</thead>
<tbody>
<tr>
<td>inv: self.s-&gt;includes(5)</td>
</tr>
</tbody>
</table>

Keywords are printed in a blue typeface.

- OCL formulae that are interpreted within HOL-OCL, i.e., are written inline as `self.s->includes(5)`, or alternatively in mathematical syntax as: `5 \in (\text{self.s})`. As you can see, we use a (shorter) mathematical notation for OCL expressions. This notation is introduced as an alternative concrete syntax (see Table A.2 for a syntax comparison). Overall, HOL-OCL supports both notations, but we prefer the mathematical one for semantic definitions and proof work.
1.4. Acknowledgements

- We use a color coding to distinguish [OCL] and [HOL] sub-expressions in formulae containing both, e.g.:

\[ \bigcup \equiv \text{lift}_2 \left( \text{strictify}(\lambda X. \text{strictify}(\lambda Y. \text{AbsSet}\left[ \text{RepSet } X \cup \text{RepSet } Y \right])) \right) , \]

or

\[ _+ \equiv \text{lift}_2(\text{strictify}(\lambda x. \text{strictify}(\lambda y. [x] + [y]))) . \]

Overall, [HOL] expressions are printed using the default color. We resolve ambiguities between the underlying mathematical syntax (i.e., [HOL]) and the [OCL] level by using colors: Expressions that are internally used within HOL-OCL, like the lifting operator \( \dashv \) are printed in a green typeface. Using our mathematical OCL syntax, expressions on the OCL level, like \( _\land _ \), are written in a magenta typeface. For the concrete syntax presented in the standard, e.g., \( _\land _ \), we use a magenta typeface. In rare cases, notable for the arithmetic operators like \( _+ _ \), we deviate from this scheme out of technical reasons.

- [HOL] formulae are written using the usual mathematical notion, i.e., \( s \in S \).

Theory files for HOL-OCL and Isabelle/HOL are printed as follows:

```plaintext
theory royals_and_loyals imports OCL begin load_xmi "royals_and_loyals_ocl.xmi" end
```

Keywords are printed in a green typeface.

- SML code fragments are written inline like `fn x => 2 * x` or in display style:

```
data
type OclType = Integer | Real | String | Boolean
            | OclAny | Set of OclType (* ... *)
```

Keywords are printed in a blue typeface.

Further, we mark problems and extensions to the OCL standard as follows:

- Errors in the standard are marked by with a danger sign on the margin throughout this document, and our definitions can be seen as our proposal for repair.

- In some cases we see our proposals as an extension of the standard, these cases are marked with an exclamation sign on the margin.

1.4. Acknowledgements

- HOL-OCL uses the component su4smil which is developed by Achim D. Brucker, Jürgen Doser, and Burkhart Wolff as the underlying UML repository.
Chapter 1. Introduction

- Internally, su4sml uses the XML parser Functional Extensible Markup Language (XML) Parser (FXP) [2].
- During his semester thesis, Simon Meier checked the library for completeness and substantially extended the theory.
Chapter 2.

Background

2.1. Higher-order Logic

Higher-order Logic ($\text{HOL}$) \cite{14} \cite{8} is a classical logic with equality enriched by total polymorphic\footnote{to be more specific: parametric polymorphism} higher-order functions. It is more expressive than first-order logic, e.g., induction schemes can be expressed inside the logic. Pragmatically, $\text{HOL}$ can be viewed as a combination of a typed functional programming language like SML or Haskell extended by logical quantifiers.

$\text{HOL}$ is based on the typed $\lambda$-calculus—i.e., the terms of $\text{HOL}$ are $\lambda$-expressions. The application is written by juxtaposition $E E'$, and the abstraction is written $\lambda x. E$. Types may be built from type variables (like $\alpha$, $\beta$, ..., optionally annotated by type classes as in $\alpha :: \text{order}$ or $\alpha :: \text{bot}$) or type constructors (like bool or nat). Type constructors may have arguments (as in $\alpha$ list or $\alpha$ set). The type constructor for the function space $\Rightarrow$ is written infix: $\alpha \Rightarrow \beta$; multiple applications like $\tau_1 \Rightarrow (\ldots \Rightarrow \tau_{n+1} \ldots)$ have the alternative syntax $[\tau_1, \ldots, \tau_n] \Rightarrow \tau_{n+1}$. $\text{HOL}$ is centered around the extensional logical equality $\_ = \_ \in [\alpha, \alpha] \Rightarrow \text{bool}$, where bool is the fundamental logical type. We use infix notation: instead of $(\_ = \_) E_1 E_2$ we write $E_1 = E_2$. The logical connectives $\_ \land \_$, $\_ \lor \_$, $\_ \to \_$ of $\text{HOL}$ have type $[\text{bool, bool}] \Rightarrow \text{bool}$, $\neg \_$ has type bool $\Rightarrow$ bool. The quantifiers $\forall \_ \in \_$ and $\exists \_ \in \_$ have type $[\alpha \text{ set}, \alpha \Rightarrow \text{bool}] \Rightarrow \text{bool}$. The quantifiers may range over types of higher order, i.e., functions.

The type discipline rules out paradoxes such as Russel’s paradox in untyped set theory. Sets of type $\alpha$ set can be defined isomorphic to functions of type $\alpha \Rightarrow \text{bool}$; the elementhood $\_ \in \_$ has then type $[\alpha, \alpha \text{ set}] \Rightarrow \text{bool}$ and corresponds basically to the application; in contrast, the set comprehension $\\{ \_ \in \_ \}$ has type $[\alpha \text{ set}, \alpha \Rightarrow \text{bool}] \Rightarrow \alpha$ set and corresponds to the $\lambda$-abstraction. The definition of $\_ \cup \_$, $\_ \cap \_$ and set complement is standard, as well as bounded versions of the quantifiers $\forall \_ \in \_$ and $\exists \_ \in \_ \_ \_$ of type $[\alpha \Rightarrow \text{bool}] \Rightarrow \text{bool}$.

Thus, $\text{HOL}$ allows for specifications in a very natural (mathematical) way, similar to naive set theory. In contrast to the latter, however, $\text{HOL}$ is a consistent logical system (relative to ZFC) provided that all formulae can be type-checked, which we always assume throughout this text and which is technically done behind the scenes.

The modules of larger logical systems built on top of $\text{HOL}$ are Isabelle theory files (or just: theories, if no confusion arises). Among many other constructs, they con-
Chapter 2. Background

tain type and constant declarations as well as axioms. Since stating arbitrary axioms
in a theory is extremely error-prone and should be avoided, only very limited forms
of axioms should be admitted and the constraints (both syntactical and semantical)
checked by machine. These fixed blocks of declarations and axioms described by a
syntactic scheme were called conservative theory extensions since and extended theory
is consistent (‘has models’) provided the original theory was. Four different conser-
vative extensions were discussed in the literature: constant definition, type definition,
constant specification, type specification (see [17] for an in depth discussion, which also
includes the correctness proofs). For example, the mostly used constant definition
consists of a constant declaration
\[ c :: \tau \]
and an axiom of the form:
\[ c = E \]
where \( c \) has not been previously declared, the axiom is well-typed, \( E \) is a closed ex-
pression (i.e., does not contain free variables) and \( E \) does not contain \( c \) (no recursion).
A further restriction forbids type variables in the types of constants in \( E \) that do not
occur in the type \( \tau \). As a whole, a constant definition can be seen as an “abbreviation”
which makes the conservativity of the construction plausible (but see [17] for the hairy
details), and the syntactic side-conditions are checked by Isabelle automatically.

The idea of an “abbreviation” is also applied for the conservative type definition of
a type \((\alpha_1, \ldots, \alpha_n)T\) from a set \( \{x \mid P(x)\} \).

In this case, the set of type constructors is extended by the constructor \( T \) of arity \( n \).
The predicate \( P \) of type \( \tau \Rightarrow \text{bool} \) for a base type \( \tau \) constructs a set of elements \( \tau \) set;
the new type is defined to be isomorphic to this set. Technically, this isomorphism
is stated by the declaration of two constants representing the abstraction and the
representation function and by two axioms over them. More precisely, the constant
Abs\( _T \) of type \( \tau \Rightarrow (\alpha_1, \ldots, \alpha_n)T \) and the constant Rep\( _T \) of type \((\alpha_1, \ldots, \alpha_n)T \Rightarrow \tau \)
were declared. The two isomorphism axioms have the form:
\[ \text{Abs}_T(\text{Rep}_T(x)) = x \]
and
\[ P(x) \Rightarrow \text{Rep}_T(\text{Abs}_T(x)) = x \]
where the precise meaning of the \( _\Rightarrow _\) arrow will become apparent in the next
section; for the moment, we can consider it equivalent to the logical implication \( _\rightarrow _\).
The type definition is conservative if the proof obligation \( \exists x. P(x) \) holds; this assures
that the type is non-empty as required by the semantics of \text{HOL}.

The Isabelle/\text{HOL} library (and the libraries of similar \text{HOL} systems) prove, that the
typed set theory including least fixedpoint theory, order theory including well-founded
recursion, number theory including real number theory and theories for data-structures
like pairs, type sums and lists can be build on top of the \text{HOL} core-language entirely
by these conservative definitions. A large part of these theories consists in deriving
2.2. Concepts and Use of Isabelle/HOL

Isabelle [37] is a generic theorem prover of the Logic for Computable Functions (LCF) prover family implemented in Standard Meta Language (SML). We heavily use the possibility to build SML programs performing symbolic computations over formulae in a logically safe way on top of the logical core engine: this is how the proof procedures of HOL-OCL are built technically. Isabelle/HOL offers support for checks for conservativity of definitions, data types, primitive and well-founded recursion, and powerful generic proof engines based on rewriting and tableaux provers.

Isabelle’s proof engine can directly process natural deduction rules: \( A_1 \implies \ldots \implies A_n \implies A_{n+1} \), also written \([A_1; \ldots; A_n] \implies A_{n+1}\), is viewed as a rule of the form “from assumptions \( A_1 \) to \( A_n \), infer conclusion \( A_{n+1} \).” Here, \( \_ \implies \_ \) denotes the built-in meta-implication of Isabelle. With meta-implications, also more complex rules like: if assumption \( B \) can be inferred from assumption \( A \), infer \( A \rightarrow B \) (also called: implication introduction) can exactly be expressed in Isabelle by: \((A \implies B) \implies A \rightarrow B\). In the mathematical literature, such natural deduction rules were also written as:

\[
\frac{A_1 \ldots A_n}{A_{n+1}} \quad \text{and} \quad \frac{[A]}{B} \quad \frac{A \rightarrow B}{\_}.
\]

A proof state in Isabelle contains an implicitly conjoint sequence of Horn-clause-like rules called subgoals \( \phi_1, \ldots, \phi_n \) and a goal \( \phi \). Logically, subgoals and the goal are connected to a theorem of the form \([\phi_1; \ldots; \phi_n] \implies \phi\). In order to cope with quantifiers naturally occurring in logic, subgoals have a slightly more general format than just Horn-clauses: variables may be bound by a built-in meta-quantifier:

\[
\lambda x_1, \ldots, x_m. [A_1; \ldots; A_n] \implies A_{n+1}.
\]

The meta-quantifier \( \lambda \) helps to capture the usual side-constraints “\( x \) must not occur free in the assumptions” for quantifier rules; meta-quantified variables can be logically considered as free variables. Further, Isabelle supports meta-variables (written \(?x, ?y, \ldots\)), which can be seen as “holes in a term” that can still be substituted. Meta-variables are instantiated by Isabelle’s built-in higher-order unification and occur only inside proofs.

The initial proof state is built from the trivially true theorem \( \phi \implies \phi \) for any (typed) formula \( \phi \). A theorem is proven if a final proof state of the form \( \phi \) could be reached by tactics i.e., SML functions allowing for the transformation of proof states. It is a key feature of Isabelle’s design that all tactics are based on a few operations provided by the logical core engine of Isabelle. Moreover, these core operations log all logical operations in a derivation tree called proof-object; thus, if someone has serious doubts on the correct implementation of Isabelle’s proof procedures (i.e., tactics),
he/she may generate the proof objects and check the derivations by an independent program following the rules of the logic.

Besides the SML-based programming interface, there is also an own input language to Isabelle theories, called Intelligible semi-automated reasoning (Isar). Isar allows for writing specifications consisting of definitions, proofs, and technical setups for the prover in a fairly readable way. In particular, Isabelle can generate \LaTeX\-documentation while checking the entire hierarchy of theories (this is, what this document is ...).

Isabelle theories written in Isar are supported by a fairly powerful Emacs-based front-end called ProofGeneral. HOL-OCL is in fact integrated and customized for this front-end, such that HOL-OCL specific Isar commands and HOL-OCL specific fonts can be used.

2.3. A Short Introduction into \textbf{UML/OCL}

Now we introduce the concepts of the target of our work, namely Unified Modelling Language (UML) and Object Constraint Language (OCL). As mentioned, Unified Modelling Language (UML) provides a variety of diagram types for describing dynamic (e.g., state charts, activity diagrams) and static (e.g., class diagrams, object diagrams) system properties.

One of the more prominent diagram types of the UML is the \textit{class diagram} for modeling the underlying \textit{object-oriented} data model of a system. The class diagram in Figure 2.1 illustrates a simple accounting scenario where customers can own different kinds of accounts and transfer money between them. In more detail: customers are modelled as a \textit{class}. There are further \textit{classes} modelling the different account types, a checkbook with checks and also transactions. A class does not only describe a set of \textit{object instances}, i.e., record-like data consisting of \textit{attributes} such as balance, but also \textit{operations} defined over them. The class Customer in our example has only attributes, namely name, address, gender, and title. The different account types are organized in a hierarchy of subtypes denoted by an arrow, i.e., between Account and BankAccount. Such an subtype relation is called \textit{inheritance} in the object-oriented paradigm. Sometimes this is also called \textit{specialization}, i.e., a CurrencyTrading specializes a BankAccount. Further, it is characteristic for the object-oriented paradigm that the functional behavior of a class and all its methods are also accessible for all subtypes. A class is allowed to redefine an inherited method, as long as the method interface does not change; this is called \textit{overriding}, as it is done in the example for the operation makeWithdrawal().

Of course, there is a relation between customers and accounts. This is modelled in UML by an \textit{association belongsTo}. An association can be constrained by \textit{multiplicities}. In Figure 2.1 the multiplicities of the association belongsTo requires that every object instance of Account is associated with exactly one object instance of Bank. This captures the requirement that every account belongs to a unique bank. In the other direction, the association models that an instance of class Bank is related to a (non-empty) set of instances of class Account or its subtypes.
2.3. A Short Introduction into UML/OCL

Figure 2.1.: Modeling a simple banking scenario with UML
Chapter 2. Background

Understanding OCL as a data-oriented specification formalism, it seems natural to refine class diagrams using OCL for specifying invariants, pre-conditions and post-conditions of operations. By specifying the following OCL constraints one can make the specification of the class Account much more precise, e.g., we can describe that accountNumbers are unique:

```plaintext
context BankAccount
inv: BankAccount.allInstances
    -> forAll(a1,a2 | a1 <> a2 implies a1.accountNumber <> a2.accountNumber)
```

Or constrain the effects of operations:

```plaintext
context BankAccount::getBalance(): Integer
post: result = balance

context BankAccount::getCurrency(): String
post: result = currency

context BankAccount::makeDeposit(amount: Integer): Boolean
post: balance = balance@pre + amount

context BankAccount::makeWithdrawal(amount: Integer): Boolean
post: balance = balance@pre - amount
    and currency = currency@pre
```

where in post-conditions @pre allows one to access the previous state.

In UML class members can contain attributes of the type of the defining class. Thus, UML can represent (mutually) recursive data types. Moreover, OCL introduces also recursively specified methods [41]; however, at present, a dynamic semantics of a method call is missing ([12] gives a short discussion of the resulting problems).

Note, that many diagrammatic UML-features can be translated to OCL-expression without losing any information, e.g., associations can be represented by introducing implicit set-valued attributes into the objects with a suitable data invariant describing the multiplicity. These transformations are already described in the UML-standard [40]. Some of these transformation were done during the process of loading an UML/OCL specification into HOL-OCL, e.g., we have not to provide a special treating for associations in our proof environment.

2.4. A Note About Standards

OMG standards are developed in an open process leading to a variety of “standardization” documents. Especially for UML and OCL which have a long history and our particular choice needs some explanation.

---

2Direct support for associations is planned for the future.
2.4. A Note About Standards

OCL was introduced as an OMG specification language as additional document [38] completing the UML 1.1 standard [39]. In later releases of the UML standards of the version 1.x series the OCL standard was a chapter of the UML specification, e.g., [40, Chapt. 6]. As several shortcomings of the OCL 1.x specifications were discussed [50, 32, 21] the development of OCL 2.0 led to many documents describing the different intermediate states.

For our work we have chosen the following two documents as our main references:

1. **OMG Unified Modeling Language Specification** (excluding Chapt. 6 which describes OCL 1.5)[40] which is publicly available at [http://www.omg.org/cgi-bin/apps/doc?formal/03-03-01.pdf](http://www.omg.org/cgi-bin/apps/doc?formal/03-03-01.pdf)


This combination is also used by a many recent tools, especially the OCL type-checker [1] from the Dresden University which is integrated into our tool chain.

---

3 also known as OMG document “formal/03-03-01”
4 also known as OMG document “ptc/03-10-14”
Chapter 2. Background
Part II.

Theory
Chapter 3.
Foundations

3.1. An Overview of Embedding Techniques

A theory representing syntax and semantics of a programming or specification language in another specification language is called an embedding. While the underlying techniques are known since the invention of typed $\lambda$-calculus, it was not before the late seventies that the overall importance of higher-order abstract syntax (HOAS) \[43\] for the representation of binding in logical rules and program transformations \[24\] and for implementations \[43\] was recognized.

As an example, we revise the universal quantifier of $\text{HOL}$ already introduced in Section 2.1: it is represented in higher-order abstract syntax (HOAS) by a constant $\text{All} : (\alpha \Rightarrow \text{bool}) \Rightarrow \text{bool}$, where the term $\text{All}(\lambda x. P(x))$ is paraphrased by the usual notation $\forall x. P(x)$. This is in contrast to the usual textbook definition for predicate logic, where a free datatype for terms and predicates, explicit substitution and well-typedness functions over them is provided. This conventional representation requires explicit side-conditions in logical rules over quantifiers preventing variable-clashes and variable capture. The representation using higher-order abstract syntax (HOAS) has two advantages:

1. the substitution required by logical rules like $\forall x. P(x) \Rightarrow P(t)$ can be directly implemented by the $\beta$-reduction underlying the $\lambda$-calculus, and

2. the typing discipline of the typed $\lambda$-calculus can be used to represent the typing of the represented language. For example, a multi-sorted first-order logic (having syntactic categories for arithmetic terms, list terms, etc.) is immediately possible by admitting expressions of type nat and $\alpha$ list.

In short, HOAS has the advantage of “internalization” of substitution and typing into the meta-language, which can therefore be handled significantly more general and substantially more efficient, which is a prerequisite for using Isabelle as an implementation platform.

When using HOAS-style semantic definitions, the technique is extended into a “shallow embedding” \[9\] of an object-language, a technique which is opposed to a “deep embedding” which treats syntax by free datatypes and semantics via semantic interpretation functions as common in logical textbooks.

A shallow embedding definition of the universal quantifier is, for example, $\text{All} P \equiv (P = \lambda x. \text{true})$ (the propositional function of the “body” of the quantifier must be
Chapter 3. Foundations

equal to the function that yields true for any argument), a deep representation follows usual textbooks:

$$\text{Sem}\left[\forall x. P(x)\right]_\gamma \equiv \begin{cases} \text{true} & \text{if } \text{Sem}\left[P(x)\right]_\gamma[x := d] \text{ for all } d \\ \text{false} & \text{otherwise} \end{cases}$$

where we assume a meta-language with well-defined concepts such as if, otherwise, and for all, e.g., Zermelo-Fränkel-set theory.

As can be seen, shallow embeddings can have a remarkably different flavor in their semantic presentation, in particular when striving for conservativity as in the example above. However, since the usual inference rules were derived from these definitions (like the rule $\forall x. P(x) \implies P(t)$ from above), they are finally proven as semantically equivalent.

If a shallow embedding is built entirely by conservative theory extensions (which implies that the language definition is consistent if the meta-language is; cf. Section 2.1), we also speak of a **conservative embedding**.

### 3.2. Embeddings of Specification Languages

Since shallow embeddings in itself are fairly well-known in principle, the question arises, what the fundamental problems and technical challenges exist for representing “real world” specification languages. The main difficulty stems from the fact, that the most successful shallow-embeddings (as, for example, HOL encoded in typed $\lambda$-calculus) are designed to fit to the underlying meta-language. In contrast, “Real world” languages are typically conceived solely on a kind of mathematical notation based on naïve set theory and no specific experience in theorem proving in mind; in some cases, the definition process of a “real” specification language takes place in a “development by committee” process prone to all sorts of arcane compromises. While a deep embedding is always possible whenever a formal semantics exists, a shallow embedding may conflict with certain constraints the shallow technique imposes, be it on the representability of the binding structure, the type discipline and the semantics of the language.

As an example for a different outcome of language design decisions, one might consider the following pathological case: In standard logic textbooks (like [31]), the notion of a model also admits empty carrier sets for sorts or types. Therefore, in many textbook-driven research papers, a lot of consideration of these pathological cases is made. In a tool-oriented research approach, it suffices to see that $\beta$-reduction is simply not sound\(^1\). Given the fact that $\beta$-reduction is vital for higher-order logic provers and for the issue of internalization of substitution, this led to a modification of the model notion, i.e., to ruling out non-empty carrier sets and living with the methodological consequences such as side conditions in type definitions.

\(^1\)Consider the two types $a$ and $b$ with some empty carrier set $A$ and a non-empty carrier $B$. Since $B^A$ is the empty set, $(\lambda x :: a \Rightarrow b. C)$ is an uninterpretable term and $(\lambda x :: a \Rightarrow b. C) = C$ does not hold for some constant $C$ interpretable in $B$ and some variable $X$.
Thus, even fairly worked out semi-formal semantic descriptions of a specification language may be quite distant to a formal (i.e., machine-checkable) representation, and even a formal semantic representation may be quite distant to a set of derived rules that allow for the formal support of a particular method of this language. Providing paradigmatical embeddings and new techniques helpful for bridging this gap is the main goal of this work. To describe the problem domain in more detail, we use the following classification: Specification languages may be:

1. **process oriented**, i.e., their focus of description is the behavior, usually described as possible sequences (traces) of states or communication events,

2. **data oriented**, i.e., their focus of description is the structure of data a system processes, its states, and individual steps the system performs when making a transition from one state to another, and

3. **object-oriented**, which is essentially a data-oriented specification approach where object-oriented data structuring techniques such as inheritance and subtyping are emphasized.

Examples for process-oriented specification languages are temporal or modal logics (such as LTL, CTL, \(\mu\)-calculus [15]) or process-algebras (such as CCS [34] or CSP [45]). Examples for data-oriented specification languages are VDM [27] or Z [47], examples for the object-oriented language class are Object-Z [46] or UML/OCL [40, 41].

### 3.3. Challenges of a Shallow Embedding of UML/OCL

Producing a shallow embedding of the key features of object-oriented modeling in HOL is the technically most challenging enterprise in this work, but also the one with the greatest potential of use in software engineering. A shallow embedding in HOL must capture the essence of OCL with respect to subtyping and inheritance in a type system that does not provide a notion of subtypes, and provide means for extensibility and reuse to capture the pragmatics of object orientation. Moreover, a formalization must capture that object-oriented specification is deeply intertwined with the notion of state, i.e., a map of object-references to objects (abstractions of pieces of memory) and its possible state transitions. Technically, these constraints have the form of class invariants or pre and postconditions of methods; OCL in class diagram is thus a typical data-oriented formal modelling technique.

We consider the following example: Since path expressions resulting from UML class-diagrams are basic elements of the OCL language, one can state that the attribute \(a\) of an object \(self\) must be 5 in the pre state: \(self@pre.a = 5\). With respect to a state transition, we may state that \(a\) increases during a transition: \(self@pre.a = self.a + 1\).

Thus, since expressions in OCL do not only compute values, but also contain operations that refer to the pre and post state \((\sigma, \sigma_{pre})\), the semantics of an expression \(\phi\) depends on such state pairs: \(I[\phi](\sigma, \sigma_{pre})\) [41] Definition A.30]. The standard also introduces \(I[\phi]_\sigma\), i.e., a semantic interpretation on only one state. This

29
version is used for precondition and invariant expressions. For simplification reasons, we only use the former version; invariant and precondition expressions are sufficiently characterized syntactically by the requirement that they must not contain any \$pre in paths. For our purpose of a machine-representable, shallow embedding for OCL, we make a further simplification and omit an explicit semantic function \(I\).

This can be done by viewing \(\phi\) as a function from \((\sigma, \sigma_{\text{pre}})\) to the semantic value of \(I[\phi](\sigma, \sigma_{\text{pre}}) = \phi(\sigma, \sigma_{\text{pre}})\). Technically, this means that we have to lift over the context any semantic function occurring in \(\phi\), e.g., \(- = -\) or \(- + -\) in the example above, over the states \(\tau = (\sigma, \sigma_{\text{pre}})\). More precisely, the addition \(- + -\) of type \([\text{Integer}, \text{Integer}] \Rightarrow \text{Integer}\) in the sense of the standard must be lifted over the context \(\tau\), i.e., the corresponding operation \(- + -\) in HOL-OCL must have the type \((\tau \Rightarrow \text{Integer}) \Rightarrow (\tau \Rightarrow \text{Integer}) \Rightarrow \tau \Rightarrow \text{Integer}\). When introducing the type synonym \(V_{\tau}(\alpha)\) for \(\tau \Rightarrow \alpha\), this type transformation can be made explicit: the HOL-OCL type for the OCL type above is \([V_{\tau}(\text{Integer}), V_{\tau}(\text{Integer})] \Rightarrow V_{\tau}(\text{Integer})\). We call \(\tau\) also the context of this type transformation, which is classified as “semi-canonical” translation (see Section 3.4). It turns out that the complete set of OCL operators, be it from the core logic or be it from the quite rich library, can be syntactically constructed as semi-canonical translations. This includes operators with non-trivial binding-structure such as the \texttt{let}-construct, or the \texttt{iterators} (corresponding to \texttt{fold}-like operators known from functional languages).

A further complication of a shallow embedding of OCL is due to the fact, that paths into the state may be undefined, and therefore all functions in expressions may have undefined results. Technically, this means that we have to extend all types by an additional \(\bot\) element—which leads to another “semi-canonical” type transformation—but for the expression semantics, the logic, and the calculi, this has dramatic consequences: Many rules can only be applied for “defined” values, which results in particular case splits and side-conditions in thousands of lemmas and rules. These side-conditions must be established by more or less complex side-calculi; for the example of undefinedness, for example, we need rules that infer facts like “if \(a + b\) is defined, \(a\) and \(b\) must be defined.” Thus, although considered semantically fairly trivial in many research communities, a proper treatment of definedness in the sense of the standard is usually avoided in deduction systems over OCL-like or VDM-like languages because of the size and complexity of the side-calculi.

Beyond the typical problems concerning undefinedness and states, the most challenging part of HOL-OCL as a shallow embedding consists in a particular semantic understanding of the key-notions UML state diagrams. This implies a notion of typed state, covering concepts such as static and dynamic types in systems, and combining this with the practical need of extensibility of the object-type system and modular theories over it. In the end, the theory also offers a new perspective on methods and late-binding method invocation. However, a modular treatment of state diagrams requires a kind of “semantic compiler” converting it into a semantic theory over the types, their relation, their properties with respect to object construction and destruction, etc.
3.4. An Overview over Embedding Techniques

To put HOL-OCL as an embedding into perspective, we define several notions for their classification. As already mentioned, we call a syntax translation:

- **canonical**, if and only if the non-terminals (or types) of the object language can be mapped one-to-one to type constructors in the `HOL` representation,
- **semi-canonical**, if and only if the non-terminals (or types) of the object language can be mapped to type expressions (possibly containing free type variables),
- **pre-compiled**, if and only if the non-terminals (or types) of the object language were mapped to type expressions according to their context in the term-language.

As an example for a canonical logical embedding, consider `HOL-CSP`\textsuperscript{[49]}. Here, the syntactical category of a "process over an alphabet \(\Sigma\)" can be directly represented by a type-constant \((\alpha)\textit{process}\), which is represented by the semantic domains of \(\text{CSP}\) (traces, failures, divergences). Binding of summation operators can be represented directly by \textit{higher-order abstract syntax} (HOAS), as well as the fixedpoint operator. Derived calculi allow for equivalence proofs of processes (even over infinite alphabets) via fixedpoint induction.

As an example for a pre-compiled translation, consider the HOL-Z embedding \textsuperscript{[11]}. While most operators from Z’s “mathematical toolkit” can be compiled canonically, the expressions for the schema calculus must be pre-compiled. In particular, a schema expression \(A\) may be mapped to a function \(\alpha_1, \ldots, \alpha_n \Rightarrow \text{bool}\), where both the \(\alpha_i\) and the \(n\) depend on previous declarations.

We turn now to a classification of type systems resulting from an embedding function `embedding : \(L \Rightarrow \text{HOL}\)` mapping expressions of an object-language \(L\) to expressions in HOL. We assume the existence of predicates `welltyped\_L` (assuring that an expression of language \(L\) is welltyped with respect to type discipline) and `welltyped\_hol` (assuring that a \(\text{HOL}\)-expression is welltyped with respect to the simple-type type-system including parametric polymorphism called \(\lambda^\circ\).

Then we can characterize a type translation underlying an embedding as

- **approximate**, if and only if for any \(e\), `welltyped\_hol(\text{embedding} \ e)` is implied by `welltyped\_L(e)`,
- **tight**, if and only if the type translation is approximative and we have additionally for any \(e\), `welltyped\_L(e)` is implied by `welltyped\_hol(\text{embedding} \ e)`.

Thus, if an embedding is tight, a possible implementation for a type-checker consists in applying the `embedding`-function and trying to type-check its result in HOL; an error on the converted term indicates the existence of a type error on the original term. Note, however, that the practical usability of such a conceptual implementation is usually very limited, in particular for semi-canonical or pre-compiled languages, since the error messages gained by this process are hard to decipher for users not familiar with the semantic details of the embedding.
### Chapter 3. Foundations

<table>
<thead>
<tr>
<th>Example</th>
<th>Process-Oriented</th>
<th>Data-Oriented</th>
<th>Object-Oriented</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOL-CSP</td>
<td>HOL-Z</td>
<td>HOL-OCL</td>
<td></td>
</tr>
<tr>
<td>Syntax</td>
<td>canonical</td>
<td>pre-compiled</td>
<td>OCL semi-canonical, HOAS</td>
</tr>
<tr>
<td>Typing</td>
<td>tight</td>
<td>approximate</td>
<td>tight</td>
</tr>
<tr>
<td>Semantics</td>
<td>denotational semantics, complex side-calculi</td>
<td>fairly trivial</td>
<td>complex side-calculi, three-valued logics, theory morphisms</td>
</tr>
</tbody>
</table>

| Table 3.1.: Comparing Logical Embeddings |

On this basis, we can compare logical embeddings like HOL-CSP [49], HOL-Z [11] and the present HOL-OCL in Tab. 3.1. The reason for the non-tightness of the Z embedding lies in a mere technicality: the Z type-system supports \( n \)-ary tuples or records. They are distinct to their (isomorphic) representation as nested pairs: \((a, b, c)\) has not the same type as \((a, (b, c))\). Since the latter is the representation of the former in HOL-Z, an expression like \((a, b, c) = (a, (b, c))\) can be typed after applying the embedding function although it cannot be typed with the Z type discipline.

Some explanation for the remarks in the line summarizing semantic features: in a shallow embedding, it is necessary to express syntactic constraints (e.g., for admissibility as in the case of fixpoint-induction, or continuity in the case of process-refinement, or state-passing in the case of rewriting in OCL) semantically, i.e., by second or third-order predicates expressing conditions that were otherwise characterized by inductively defined subsets of the syntax. These semantic predicates result in side-conditions which can be established by derived rules having a similar form and purpose than the inductive rules of a sub-language definition (for example, the admissibility rules characterize formulae built over logical constants, \( _\land, _\lor \) and universal quantification; thus, existential quantification or negation are ruled out except that they occur in the construction of constant terms). However, their semantic construction leads sometimes to unexpected generalizations and often improves the insight into their logical nature than their (traditional) syntactic counterparts.
Chapter 4.

Faithfully Representing \textbf{UML/OCL}

In the first two sections of this core chapter on our formalization of UML and OCL semantics, we refine our overall goal for a faithful formal semantics with respect to the standard into several sub-goals and then present an overall architecture of HOL-OCL meeting these goals. The subsequent sections are concerned with various aspects of this architecture.

4.1. A Note About Standard Compliance

We claim that we provide a semantic representation compliant with the OCL standard semantics definition. In this section, we make our claim more precise, in particular we have to discuss to which parts we claim to be compliant. First, the OCL standard is divided into normative parts and informative, i.e., not normative, parts. The semantics\textsuperscript{1} of the standard appears in the following chapters of [41]:

Chapter 7 “OCL Language Description”: This informative chapter motivates the use of OCL and introduces it in an informal way, mostly by showing examples. We used this chapter mainly for catching the intentions of the standard in cases where the other parts of the standard are unclear or contradictory.

Chapter 10 “Semantics Described using UML”: This normative chapter describes the “semantics” of OCL using the UML itself. Merely an underspecified “evaluation” environment is presented. Nevertheless, some of the information presented in this chapter is helpful for formalizing the standard.

Chapter 11 “The OCL Standard Library”: This normative chapter is, in our opinion, the best source of the normative part of the standard describing the intended semantics of OCL. It describes the semantics of the OCL expressions as requirements (in form of pairs of pre- and postconditions) they must fulfill. Overall, we prove these requirements for our embedding and thus show that our embedding satisfies these requirements.

Appendix A “Semantics”: This informative appendix defines the syntax and semantics of OCL formally in a textbook style paper-and-pencil notion. It is mostly based on [44].

\textsuperscript{1}A nice overview of the different usages of the word “semantics” is given in [22].
Chapter 4. Faithfully Representing \textit{UML/OCL}

Overall, we see the semantic foundations of the standard critical for several reasons:

1. The normative part of the standard does not contain a formal semantics of the language.

2. The consistency and completeness of the formal semantics given in “Appendix A” is not checked formally.

3. There is no proof, neither formal nor informal, that the formal semantics given in the informative “Appendix A” satisfies the requirements given in the normative chapter 10.

Nevertheless, we think the \textit{OCL} standard \cite{41} (“ptc/03-10-14”) is mature enough to serve as a basis for a machine-checked semantics and formal tools support.

When we claim to be compliant to the standard, we do not mean that we converted “literally” the “Semantics” chapter of the \textit{OCL} standard \cite{41 appendix A} into an Isabelle theory. The deviations from the standard can be grouped into the following six classes:

**Making the standard more precise:** The most important point here is the need for a typed set theory as meta-language for the description of the data-universe and the concepts “model” and “signature” left implicit in the standard: Formalizing this in \textit{HOL} is neither possible nor desirable, since consistency can no longer be guaranteed. Another issue in this line is that collection types have “smashed semantics” in \textit{HOL-OCL} (see subsection 4.7.1).

**Presentational issues:** This covers our decision to turn \textit{OCL} into a shallow embedding, as well as our decision to use a combinator style presentation for the bulk of semantic definitions both for conceptual and technical reasons. In section 4.5, we show in detail why these formulations are equivalent to the ones used in the standard.

**Generalizations:** This covers for example our decision to use an infinite collection type $\text{Set}_\tau$, since logical connections between, e.g., $\rightarrow \text{IsType}$ and class invariants can therefore be satisfactorily treated inside an own typed set theory in \textit{OCL} (see section 4.9).

**Repairing glitches:** The standard contains—as can be expected for a large semi-formal document—several errors in local definitions which were revealed during our formalization. Such cases are marked by with a danger sign on the margin throughout this document, and our definitions can be seen as our proposal for repair.

**Suggesting Extensions:** In some cases we see our proposals as an extension of the standard, these cases are marked with an exclamation sign on the margin.

**Proofs for Compliance Requirements:** The \textit{OCL} standard contains a collection of formal requirements in its mandatory part with no established link to the informative “Appendix A” of the standard \cite{41}. We provide formal proofs for the compliance of our \textit{OCL} semantics with these requirements (see section 4.6).
4.2. Building-Blocks of the HOL-OCL Architecture

Providing alternative mathematical syntax: Being the first who did substantial proof work in OCL, we early noticed the need for a compact, mathematical notation for OCL specifications as alternative to the programming-language like notation used in the OCL 2.0 standard. However, we accept the latter one in our front-ends, and as an alternative input format in the proof engine, too. This proceeding can be seen as generalization and is also covered by the standard, see Appendix A.

4.2. Building-Blocks of the HOL-OCL Architecture

In section 3.3, we have already seen that HOL-OCL can be decomposed in an UML part concerned with a typed object store and underlying object universes on the one hand and the OCL part just assuming abstract contexts on the other. This decomposition gives a natural basis for a separation of concern.

Before describing architectural issues in more detail, one general remark on terminology is appropriate here: The UML standard makes a clear separation between operations and operation specifications on the one hand and methods on the other; the former are entirely a specification construct, the latter an implementation construct. The UML allows an operation to have several methods, even in different programming languages. Consequently, methods are out of the scope of our work so far. Further, we distinguish operations from operation specifications by viewing the former as mathematical functions, the latter as relations.

With respect to the OCL part, we have to provide:

- A technique for giving semantics to basic (value) types of OCL, i.e., Boolean, Integer, Set and collection types such as Set, or Sequence.

- A technique for giving semantics for built-in operations over contexts, capturing arithmetics, logic and collection type theories.

- A technique for giving semantics for user-defined operations.

With respect to the UML part (resulting in a semantics for path expressions), we have to provide:

- A mechanism to generate formal theories of typed object structures associated to classes and their relationships (e.g., inheritance).

- A technique for giving semantics for user-defined operations in the context of classes, leading also to a formal semantics of path expressions. In principle, this constitutes an embedding of a subset of the UML foundation package [40].

- And last but not least, we have to bring both embeddings together, i.e., generating semantics for invariants and operation specifications consisting of pre and post conditions.

Further, we aim for mechanisms providing modularization and extensibility:
Chapter 4. Faithfully Representing UML/OCL

- The object store should allow for modular proofs, i.e., one should be able to add new classes without the need of re-proving the properties of existing classes.

- The embedding of OCL should be easily useable with another kind of object store, e.g., one idea is to use OCL for a Java-like object store allowing, e.g., a distinction between \( \bot \) and the “null” reference (pointer).

- The object-store should be useable without OCL, e.g., for a programming language description that allows for method definitions associated to an operation; thus, one could verify a method with respect to its operation specification in a Hoare-logic style of reasoning.

In this chapter we present techniques and concepts; the concrete collection of theories implementing them is contained in Appendix B.

Each of the mentioned techniques and encoding mechanisms can be organized into level, which were built in their core by formally defined theory morphisms called layer, in particular:

**Level 0:** This level defines the groundwork for the embeddings. It consists out of two layers:

- **Defining new Datatypes:** In this layer, we define HOL types, in particular auxiliary types for classes.

- **Datatype Adaption:** In this layer, the HOL datatypes are adapted as needed, e.g., we glue basic datatypes together to objects or extend all datatypes by an special “undefined” element.

In summary, this level defines all datatypes and provides a extensible object store.

**Level 1:** This adds, respectively adapts, the functional behavior and finalizes the embeddings. It consists out of two layers:

- **Functional Adaption:** This layer adapts and extend the functional behavior of our embeddings, e.g., it defines the strictness of operations and defines the semantics of operations invocations in the context of our object store.

- **Embedding Adaption:** This layer adds infrastructure for handling contexts.

In summary, this level provides an embedding of core OCL (i.e., there are only OCL formulae without context declarations) and an embedding of an extensible object store with operation invocation.

**Level 2:** This level combines the two embeddings, i.e., it introduces the context of OCL formulae and defines the semantics of objects and method invocations with respect to the validity of the corresponding preconditions, postconditions and invariants.

An overview of this architecture is shown in Figure 4.1 and will describe both, levels and layers, in more detail in the following, in particular in section 4.7.
4.3. Formal Preliminaries for Representing Semantics in $\text{HOL}$

First of all, we use the usual notation for Cartesian product $\alpha \times \beta$ and sum types $\alpha + \beta$. Recall that polymorphic type variables were represented by Greek letters. The theory of these type constructors is developed in the $\text{HOL}$ library and provides the constructor $(x, y)$ for pairs and the projections $\text{fst}$ and $\text{snd}$. The constructors for sum are $\text{Inl}$ and $\text{Inr}$; the projection is hidden in the “pattern match function”

$$\text{sumCase}(f, g, x) = \begin{cases} f(k) & \text{if } x = \text{Inl}
k \\ g(k) & \text{if } x = \text{Inr}
k \end{cases}.$$ 

In OCL, the notion of explicit undefinedness plays a fundamental role, both for the logical and non-logical expressions: c

Some expressions will, when evaluated, have an undefined value. For instance, typecasting with $\text{oclAsType()}$ to a type that the object does not support or getting the $\text{->first()}$ element of an empty collection will result in undefined.

(OCL Specification [41], page 15)

Thus, concepts like $\text{definedness}$ and $\text{strictness}$ play a major role in the OCL. We used Isabelle’s concept of a $\text{type class}$ to specify the class of all types bot that contain the undefinedness element $\bot$. Additionally, we required from this class the postulate “all OCL types must have one element different from the undefined value” to rule out certain pathological cases revealed during the proofs. For all types in this class, concepts such
Chapter 4. Faithfully Representing UML/OCL

as definedness

\[ \text{def}(x :: \alpha :: \bot) \equiv (x \neq \bot) \]

or strictness of a function

\[ \text{isStrict}(f) \equiv (f \bot) = \bot \]

are introduced. We define a combinator strictify by

\[ \text{strictify } f(x) \equiv \begin{cases} \bot & \text{if } x = \bot \\ f(x) & \text{else} \end{cases} \]

with type \((\alpha :: \bot) \rightarrow \beta :: \bot) \rightarrow \alpha \rightarrow \beta\).

The operator strictify yields a strict version of an arbitrary function \(f\) defined over the type class \(\bot\).

Further, we use the type constructor \(\tau \uparrow\) that assigns to each type \(\tau\) a type lifted by \(\bot\), for which we also write \(\tau \bot\). Since any type in \(\text{HOL}\) contains at least one element, each type \(\tau \bot\) is in fact in the type class \(\bot\). The function \(\upcase\) : \(\alpha \rightarrow \alpha \bot\) denotes the injection, the function \(\downcase\) : \(\alpha \rightarrow \alpha \bot\) its inverse for defined values. The case distinction function is defined by:

\[ \upCase(f, c, x) = \begin{cases} c & \text{if } x = \bot \\ f(k) & \text{if } x = k \end{cases} \]

We will complete our formalization section of the machinery specific to our shallow embedding by the type synonym \(V_\tau(\alpha)\) already mentioned in Section 3.3 and some combinators that capture the semantical essence of context lifting. The type synonym \(V_\tau(\alpha)\) is defined by:

\[ V_\tau(\alpha) = \tau \rightarrow \alpha \]

On the expression level, context lifting combinators fining the distribution of contexts are defined as follows:

\[ \begin{align*}
\text{lift}_0 f & \equiv \lambda \tau. f \\
\text{lift}_1 f & \equiv \lambda X \tau. f(X \tau) \\
\text{lift}_2 f & \equiv \lambda X Y \tau. f(X \tau)(Y \tau)
\end{align*} \]

with type \((\alpha \rightarrow \beta) \rightarrow V_\tau(\alpha) \rightarrow V_\tau(\beta)\), and

\[ \begin{align*}
\text{lift}_0 f & \equiv \lambda \tau. f \\
\text{lift}_1 f & \equiv \lambda X \tau. f(X \tau) \\
\text{lift}_2 f & \equiv \lambda X Y \tau. f(X \tau)(Y \tau)
\end{align*} \]

The types of these combinators reflect their purpose: they “lift” operations from \(\text{HOL}\) to semantic functions that are operations on contexts.

Operations constructed by context lifting enjoy the property, that the context is just passed, not changed. We call an operation context passing if it satisfies exactly this property. This is expressed formally as follows:

\[ \text{cp}(P) \equiv (\exists f. \forall X \tau. P X \St \equiv f(X \tau) \tau) \rightarrow \text{bool} \]

Context invariance of expressions will turn out to be a key concept allowing for converting an equivalence on \(\text{OCL}\) expressions into a congruence; thus cp will play a major role in side-calculi for \(\text{OCL}\).

The fundamental theory for undefinedness, elementary strictness combinators, lift-combinators and cp is developed in subsection B.3.1.
4.4. Encoding Standard \textsc{OCL} Operations

The standard contains “principles” for the semantics of the operations. Consider the example:

In general, an expression where one of the parts is undefined will itself be undefined. \hspace{1cm} (\textit{OCL} Specification [41], page 15)

In other words, one could rephrase this semantic principle as “all operations are strict,” be it standard or user-defined operations. The \textsc{OCL} standard requires as default for all operations to be \textit{strict}, both for the case of built-in like the \texttt{\_ + \_} on \texttt{Integer}, or user defined operations declared in class diagrams. Other “principles” are hidden in the semantic definitions; for example the passing of the context. Since we have to define around hundred operators, it is tempting to cover these underlying principles in combinators once and forall, both for conceptual and technical reasons (as we will see in section 4.7 in more detail). For the combinators introduced in section 4.3, it is now straight forward to meet the semantic principles. For the new types \texttt{Boolean} (subsection B.4.2 “\textsc{OCL} Boolean”) and \texttt{Integer} (subsection B.4.6 “\textsc{OCL} Integer”), for example, a representation as types from the \textsc{HOL} library looks as follows:

\begin{verbatim}
Boolean = bool \bot,
Integer = int \bot,
Boolean_\tau = V_\tau(\texttt{Boolean}),
Integer_\tau = V_\tau(\texttt{Integer}).
\end{verbatim}

These definitions are contained in theories subsection B.4.14. These type definitions by type synonyms are typical for our semi-canonical type translation.

Basic constant definitions for \texttt{T,F,\_} in \texttt{Boolean}, or 0,1, etc., in \texttt{Integer}, using the lifting combinators of section 4.3 is straight-forward:

\begin{verbatim}
\bot \equiv \text{lift}_0(\bot) \hspace{1cm} \text{with type Boolean}_\tau,
\texttt{T} \equiv \text{lift}_0(\texttt{true}) \hspace{1cm} \text{with type Boolean}_\tau,
\texttt{F} \equiv \text{lift}_0(\texttt{false}) \hspace{1cm} \text{with type Boolean}_\tau,
\bot \equiv \text{lift}_0(\bot) \hspace{1cm} \text{with type Integer}_\tau,
0 \equiv \text{lift}_0(0) \hspace{1cm} \text{with type Integer}_\tau, \text{and}
1 \equiv \text{lift}_0(1) \hspace{1cm} \text{with type Integer}_\tau.
\end{verbatim}

In fact, the definition for undefinedness is done for the \textit{polymorphic constant} \texttt{\_}, expressing the fact that undefinedness is omnipresent in all types of the \textsc{OCL} language. Furthermore, we use within the theories the mathematical syntax; a translation table can be found in Appendix A.
Chapter 4. Faithfully Representing \texttt{UML/\texttt{OCL}}

An example for a strict boolean operation is the logical negation:

\[ \neg \equiv \text{lift}_1(\text{strictify}(\lambda \_ \circ \neg \circ \_)) \quad \text{with type } \text{Boolean} \rightarrow \text{Boolean}. \]

From this definition, the usual logical laws for a strict negation are derived:

\[ \neg \bot = \bot \quad \neg \top = \top \quad \neg \neg \bot = \bot \]

A typical example for strict binary operation is the addition on integers; all other unary and binary operators of the theory of the follow this scheme of a constant definition:

\[ \_ + \_ \equiv \text{lift}_2(\text{strictify}(\lambda x. \text{strictify}(\lambda y. \_ x + \_ y))). \]

From these definitions, computational rules on numbers can be derived, which perform computations like \(3 + 4\) on the basis of binary representations; thus, computations of this kind can be handled fairly efficiently by the Isabelle rewriter. This representation technique for numbers is by no means new, it is merely a standard in Isabelle and adapted for these new types.

The encoding of the operations along the scheme described above is the default encoding; cases requiring special treatment are non-strict operators as well of higher-order constructs like quantifiers and the iterators of the \texttt{OCL} language similar to \texttt{fold} in functional programs:

These iterator expressions always have a collection expression as their source, as is defined in the well-formedness rules \ldots \cite[page 149]{OCL}.

Non-strict constructs such as \(\partial \text{self}\) or \(\not\partial \text{self}\) were defined via context lifting from the definedness predicate \texttt{def} introduced in section 4.3, without using the strictness combinator.

4.5. Textbook vs. Combinator Style Semantics of Operations

As mentioned previously, we use a combinator-style presentation rather than a textbook-style presentation as used in the \texttt{OCL} standard, both for reasons of conciseness as well as better amenability techniques. It is formally shown in our \texttt{Isabelle} theories that from our definitions, the requirements \cite[Chapter 11 (normative)]{OCL} of the standard follow. In this section, we give an alternative reason for this: namely, we formally show that our semantics is equivalent to (a formalized version of) the semantics given standard \cite[appendix A (non normative)]{OCL}.

The \texttt{OCL} 2.0 standard presents a definition scheme for all \textit{strict basic operations} just by one example. For the \texttt{+} operator on integers, it looks as follows: \texttt{OCL} \cite[page}{OCL}
4.5. Textbook vs. Combinator Style Semantics of Operations

This definition is presented as:

\[ I(+)({i_1}, {i_2}) = \begin{cases} 
  i_1 + i_2 & \text{if } i_1 \neq \bot \text{ and } i_2 \neq \bot, \\
  \bot & \text{otherwise.}
\end{cases} \]

This semantic function for basic operations is integrated in the more general semantic interpretation function for OCL expressions in

\[ I \llbracket e \rrbracket : \text{Env} \rightarrow I(t) \]

Let Env be the set of environments \( \tau = (\sigma, \beta) \). The semantics of an expression \( e \in \text{Expr}_t \) is a function \( I \llbracket e \rrbracket : \text{Env} \rightarrow I(t) \) that is defined as follows.

iv. \( I \llbracket w(e_1, \ldots, e_n) \rrbracket \tau = I(w)(\tau)(I \llbracket e_1 \rrbracket(\tau), \ldots, I \llbracket e_n \rrbracket(\tau)) \)

(\text{OCL Specification \[41\], page A-26, definition A.30})

There are two more semantic interpretation functions; one concerned with path expressions (i.e., attribute and navigation expressions [41, Definitions A.21]), and one concerning the interpretation of pre and postconditions \( \tau \models P \) which is used in two different variants.

To show the equivalence of the two formalization styles, we re-introduce a kind of “explicit semantic function” into our shallow embedding. Of course, which with respect to HOL-semantics, this is just the identity. \( \text{Sem}[E] \tau \) can be thought of as the fusion of the two semantic functions \( I(o) \) and \( I[E] \):

\[ \text{Sem}[x] \equiv x \quad \text{with type } \alpha \Rightarrow \alpha. \]

The definitions and exemplary proofs shown here are contained in theory subsection B.4.2.

Now we show for our first strict operation in OCL, the not operator, that it is in fact an instance of the standards definition scheme:

\[ \text{Sem}[\neg X] \gamma = \begin{cases} 
  \neg \text{Sem}[X] \gamma \downarrow & \text{if } \text{Sem}[X] \gamma \neq \bot, \\
  \bot & \text{otherwise.}
\end{cases} \]

This is formally proven as lemma “not_faithfully_represented” in the theory subsection B.4.2. The proof is trivial and canonical: it consists of the unfolding of all combinator definitions (they are just abbreviations of re-occurring patterns in the textbook style definitions!) and the semantic function Sem which is merely a syntactic marker in our context.

For the binary example of the integer addition, one proceeds analogously and receives as result:

\[ \text{Sem}[X + Y] \gamma = \begin{cases} 
  \text{Sem}[X] \gamma + \text{Sem}[Y] \gamma \downarrow & \text{if } \text{Sem}[X] \gamma \neq \bot \text{ and } \text{Sem}[Y] \gamma \neq \bot, \\
  \bot & \text{otherwise.}
\end{cases} \]

(4.1)

This is formally proven in subsection B.4.2.

In the following, we summarize the differences between the OCL standards textbook definitions and our combinator-style approach:

41
Chapter 4. Faithfully Representing UML/OCL

1. The standard [41, chapter A] assumes an “untyped set of values and objects” as semantic universe of discourse. Since we reuse the types from the HOL library to give boolean, integers and reals a semantics, meta-expressions like \{true, false\} \cup \{⊥\} used in the standard are simply illegal in our interpretation. This makes the injections \_\_ and projections \_\_ necessary.

2. The semantic functions in the standard are split into \(I(x), I[e]\_{\tau}, I_{\text{Att}}[e]\_{\tau}\) and \(\tau \models P\). Since we aim at a shallow embedding (which ultimately suppresses the semantic interpretation function), we prefer to fuse all these semantic functions into one.

3. The environment \(\tau\) in the sense of the standard is a pair of a variable map and a state pair. The variable map is superfluous in a shallow embedding (binding is treated by HOL itself), our contexts \(\tau\) just comprises the pair of pre and post state, thus an implementation of our notion of context.

4.6. Compliance to the Standards OCL Requirements

As already described, the semantics of OCL is spread over several chapters in the OCL standard. For example, with respect to undefinedness, it is stated that:

In general, an expression where one of the parts is undefined will itself be undefined. There are some important exceptions to this rule, however. First, there are the logical operators:

- True OR-ed with anything is True
- False AND-ed with anything is False
- False IMPLIES anything is True
- anything IMPLIES True is True

The rules for OR and AND are valid irrespective of the order of arguments and they are valid whether the value of the other sub-expression is known or not.

(OCL Specification [41], page 15)

which implies explicitly that OCL is based on a strong Kleene/uniLogic. Thus, most operators of the logical type like \_\_ and \_\_ (written \_\_\_\_) are explicitly stated exceptions from the “all operations are strict” principle.

In the normative part [41, chapter II], requirements were formally stated on the standard operations of OCL; the question, if these requirements are met by the informative semantics description[appendix A] has not been systematically investigated. A

Although, for most of the logical connective this can be settled by rephrasing the requirement given in form of a truth table [41, page A-12, Table A.2], there is a contradiction with respect to the truth table for IMPLIES and the requirement given in the normative part of the standard [41, page 139].

It is a contribution of our work that we can in fact formally prove the requirements are met by our semantics. In the case of the logical connectives, compliance to the standard is proven by deriving lemmas representing the complete truth table as required in the standard. Further, we also prove the normative requirements, and
4.7. Organizing the Embedding into Layer

thus connect the informative formal semantics with the normative requirements of the standard. Moreover, lemmas were derived for special calculi allowing for automated reasoning in OCL (see chapter 5).

With respect to the requirements of the standard [41, chapter 11], e.g., for isEmpty:

\[
\text{isEmpty}() : \text{Boolean} \\
\text{Is self the empty collection?} \\
\text{post: result} = (\text{self} \rightarrow \text{size}() = 0) \\
\text{(OCL Specification [41], page 141)}
\]

we prove formally requirement satisfaction lemmas:

\[
\vdash \partial (\text{self} \rightarrow \text{size}()) \\
\text{self} \rightarrow \text{isEmpty}() = (\text{self} : (\alpha \text{ Set}_{\tau}) \rightarrow \text{size}() = 0). \\
\text{(4.1)}
\]

Instead of using operation specifications, we prefer their reformulation as algebraic properties that are directly usable in proofs. The constraint \(\vdash \partial (\text{self} \rightarrow \text{size}())\) (the size of the set must be defined) is a tribute to our extension of the standard to infinite sets; it has the effect to constrain this specification to finite sets, i.e., to the domain the requirement is intended to hold.

4.7. Organizing the Embedding into Layer

In the previous sections we developed a standard representation technique for OCL operations. In this section, we will revise and generalize this technique to meet a particular technical problem of our approach.

The conservative embedding approach for yielding semantics for a large language such as OCL must provide derivations for several thousand “folklore” theorems to be practically relevant. In this section, we present an approach for deriving the mass of these theorems mechanically from the existing HOL library. The approach assumes a structured theory morphism mapping library types and library functions to new types and new functions of the specification language (i.e., OCL) while uniformly modifying some semantic properties. It turns out that the technique also greatly facilitates the technical organization of the automated generation of theories from class diagrams (see section 4.9).

The key idea is to represent the structure of the theory morphism by the semantic combinators \(_1, \text{V} (\_), \text{strictify} (\_), \text{lift} (\_), \text{lift} (\_)_0, \text{lift} (\_)_1, \text{lift} (\_)_2, \text{lift} (\_)_3\) introduced in the previous sections. We say that a theory morphism is layered, if in each form of conservative extension the following decomposition into elementary theory morphisms (the layer) is possible:

1. for type synonyms \((\alpha_1, \ldots, \alpha_m)T\), there must be type constructors \(C_1\) to \(C_n\) such that

\[
(\alpha_1, \ldots, \alpha_m)T = C_n \left( \ldots (C_1(T)) \right)
\]
Chapter 4. Faithfully Representing UML/OCL

<table>
<thead>
<tr>
<th>HOL</th>
<th>Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>\textit{bool}</td>
<td>\textit{set}</td>
</tr>
<tr>
<td>( \land, \lor = \ldots )</td>
<td></td>
</tr>
<tr>
<td>( X \land Y = Y \land X )</td>
<td>( A \cup B = A \cup B )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Type Adaption</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Functional Adaption</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Embedding Adaption</th>
</tr>
</thead>
</table>

**Figure 4.2.** Derivation of the OCL library

2. for conservative type definitions \((\alpha_1, \ldots, \alpha_m)T\), there must be functions \(C_1\) to \(C_n\) such that

\[
(\alpha_1, \ldots, \alpha_m)T = \left\{ x : C_n\left( \cdots \left( C_1(T') \right) \right) \mid P(x) \right\}
\]

3. for constant definitions \(c\), there must be functions \(E_1\) to \(E_n\) such that:

\[
c = (E_n \circ \cdots \circ E_1)(c')
\]

where each \(C_i\), or \(E_i\) are (type constructor) expressions build from semantic combinators of layer \(S_i\) and \(T'\). Where \(c'\) is a construct from the meta logic. A layer \(S_i\) is represented by a specification defining the semantic combinators, i.e., constructs that perform the semantic transformation from meta-level definitions to object-level definitions. In Figure 4.2, we show a classification for such layers.

In the following sections, we will present a collection of layers and their combinators in more detail. We will associate the semantic combinators one by one to the specific layers and collect them in a distinguished variable \(\textit{SemCom}\). Finally, we will put them together for our example [OCL] and describe generic theorem proving techniques that exploit the layering of the theory morphism for [OCL].
4.7. Organizing the Embedding into Layer

4.7.1. Datatype Adaption

Datatype adaption establishes the link between meta-level types and object-level types and meta-level constants to object-level constants. While meta-level definitions in libraries of existing theorem prover systems are geared toward good tool support, object-level definitions tend to be geared to a particular computational model, such that the gap between these two has to be bridged. For example, in Isabelle/HOL, the head-function applied to an empty list is defined to yield an arbitrary but fixed element; in a typical executable object-language such as SML, Haskell or OCL, however, this function should be defined to yield an exception element that is treated particularly. Thus, datatype adaption copes with such failure elements, the introduction of boundaries (as maximal and minimal numbers in machine arithmetics), congruences on raw data (such as smashing; see below) and the introduction of additional semantic structure on a type such as $\alpha :: \text{bot}$, or similarly, complete partial orders [36].

Now, revising the definition (cf. section 4.4):

\[
\text{Boolean} = \text{bool}_\bot, \quad \text{and} \\
\text{Boolean}_\tau = V_\tau(\text{Boolean}),
\]

we easily recognize the layer structure of these definitions.

We turn now to the semantical function combinators of this layer. We identify them in the injection $\llbracket \_ \rrbracket$ and the projection $\llbracket \_ \rrbracket$. We mark them as combinators by including them in the specific set: $\llbracket \_ \rrbracket, V(\_), \text{strictify} \_\_\_\_, \llbracket \_ \rrbracket, \text{lift}0, \text{lift}1, \text{lift}2, \text{lift}3 \in \text{SemCom}$.

As another example for a congruence construction, we will show the smashing on sets, which occurs in the semantics of SML or OCL for example. In a language with semantic domains providing $\bot$-elements, the question arises how they are treated in type constructors like product, sum, list or sets. Two extremes are known in the literature; for products, for example, we can have:

\[
(\bot, X) \neq \bot \\
\{a, \bot, b\} \neq \bot
\]

or:

\[
(\bot, X) = \bot \\
\{a, \bot, b\} = \bot
\]

The latter variant is called smashed product and smashed set. The semantics chapters make no clear decision here; since OCL tends to define its constructs towards executability and proximity of object-oriented programming languages such as Java, we opt for smashed collection semantics. The constant definition for the semantic combinator smash reads as follows:

\[
\text{smash } f \ X \equiv \text{if } f \bot X \text{ then } \bot \text{ else } X
\]

On this basis, the collection type $\text{Set}$, for example, is built via the type definition:

\[
\alpha \text{ Set} = \{X :: (\alpha :: \text{bot set}_\bot) | \bot \notin X\}
\]

\[\text{In fact, in the theories, the equivalent formulation as semantic combinators (smash}(\lambda xX. x \in X)X = X \text{ is used instead of } \bot \notin X)\]
and the type synonym:

$$\alpha \text{ Set}_\tau = V_\tau(\alpha \text{ Set})$$

As a consequence of this definitions, sets in HOL-OCL may be infinite which allows representing the syntactic category of types as sets in HOL-OCL.

This quotient construction identifies all sets containing $\bot$ in one class which is defined to be the $\bot$ of the type $\alpha$ set. All other sets were injected into an own class. Thus, an embedding of smashed sets into the class bot can be done as via the (overloaded) constant definition:

$$\bot \equiv \text{AbsSet} \bot$$

The injection \text{AbsSet} (together with the projection \text{RepSet}) is a consequence of the conservative type definition above (cf. section 2.1).

For nested OCL types such as $\text{Set(\text{Set(Integer)})}$, the HOL type is $\text{Integer Set Set}_\tau$ and not $\text{Integer}_\tau, \text{Set}_\tau, \text{Set}_\tau$ since context lifting is only necessary on the topmost level for each argument of an operation.

We “mark” the semantic combinators smash, $\bot : \alpha \text{ Set}$, AbsSet, RepSet by including them into \text{SemCom}.

**4.7.2. Functional Adaption**

Functional adaption is concerned with the semantic transformation of a meta-level function into an object-level operation. Functional adaption may involve, for example, the

- strictification of an operation, i.e., its result is undefined if one of its arguments is undefined,
- late-binding invocation semantics for operations. This semantic conversion process is necessary for converting a function into an operation using dynamic overloading.

Technically, this is achieved by the \text{strictify} combinator already introduced in section 4.3. Overloading and late-binding can be introduced by the combinators \text{invoke} and \text{invokeS} described in this section.

As an example for strictification, we present a definition of a built-in operation over a non-trivial datatype adaption, OCL’s union on sets. An intermediate version can now be defined as strictified version of HOL’s union over the smashed type $\alpha \text{ Set}$:

$$\text{union} \equiv \text{strictify}(\lambda X. \text{strictify}(\lambda Y. \text{AbsSet}(\text{\RepSet} X \cup \text{\RepSet} Y)))$$

with type $[\alpha : \text{bot Set}, \alpha \text{ Set}] \Rightarrow \alpha \text{ Set}$.

The, from object-oriented programming languages, well-known concept of method-overloading is not yet fully supported by OCL. We believe, this is more or less due to some accidental circumstances:
1. The UML standard [40, chapter 4.4.1] requires that operation names are unique within the same namespace. Albeit, the UML standard allows one to (explicitly) overwrite methods, i.e., implementation of operations.

2. The OCL standard [41, chapter 7.3.41] restricts the use of the precondition and postcondition declarations to operations or other behavioral features. Sadly, all OCL tools we know of do not support the specification of preconditions and postconditions for methods.

3. Whereas the OCL standard speaks on several places from operation calls, it does not give an hints how operation overloading should be solved, neither does it explain in details concepts like operation (method) calls or operation (method) invocations.

Bringing these together, one has to conclude, that operation overloading, and thus late-binding, is underspecified, or even not supported in OCL. Nevertheless, we think that overwriting inherited operations or methods is a very important feature of object-orientation and thus should be supported by the OCL. Thus we already provide the theoretical foundations for supporting late-binding (and thus overloading of operations) within HOL-OCL, nevertheless a concrete syntax for specifying this has to be worked out.[3]

As many object-oriented languages provide a particular call-scheme for functions, called method invocation which increases the reusability of code. Moreover, many object-oriented programming languages such as Java assume a particular overload-resolution strategy for invocations; this well-known construction in programming language theory is called late-binding. Since we believe that future versions will overcome the self-restriction to operation calls, and since the UML definition expresses at several places a clear preference for overloading operations, we will discuss in this document and partially implement in HOL-OCL a late-binding semantics of method invocation.

The treatment of late-binding requires a particular pre-compilation step concerning the declaration of overloaded-methods discussed in section 4.13 in more detail; in this section, we will concentrate on the callee-aspect of method invocations, i.e., how to represent sub-expressions occurring in post conditions representing an invocation of a user-defined operation specification:

<table>
<thead>
<tr>
<th>context</th>
<th>$A::m(a_1:t_1, \ldots, a_n:t_n):t$</th>
</tr>
</thead>
<tbody>
<tr>
<td>pre:</td>
<td>...</td>
</tr>
<tr>
<td>post:</td>
<td>...</td>
</tr>
</tbody>
</table>

In an “invocation,” e.g., a sub-expression $a.m(a_1, \ldots, a_n)$, the semantic value of the “dynamic type” (see section 4.9 for more details) of $self$ is detected, i.e., a set of “objects” whose structure is to be discussed later. This “type” helps to lookup the concrete operation specification in the table. This specification can be turned into a function (just by picking some function satisfying the specification) which is applied
Chapter 4. Faithfully Representing UML/OCL

to a as first argument (together with the other arguments). This semantics is captured in the \(n\)-indexed family of analogous `invoke` and `invokeS` semantic combinators; the former define call-by-name semantics, the latter call-by-value semantics satisfying the general strictness principle of OCL. Since `invokeS` can be realized on top of `invoke` as usual, we concentrate on the former.

The `invoke`-combinator is defined for the case \(n = 1\), for example, as follows:

\[
\text{invoke} C t a \ result \equiv
\lambda \tau. \begin{cases} 
\text{arbitrary} & \text{if } t \ (\text{Least } X. X \in \text{dom } t \land C(a \ \tau) \in X) = \text{None} \\
 f a \ result \ \tau & \text{if } t \ (\text{Least } X. X \in \text{dom } t \land C(a \ \tau) \in X) = \text{Some } f.
\end{cases}
\]

Here, Least is a HOL operator selecting the least set of a set of sets, that satisfies a certain property. In this case, this property is that self (suitably converted by a casting function \(C\), see 4.9 for details) is contained in one of the domains of the lookup table \(\text{tab}_m\) generated during the processing of the declaration discussed in section 4.13, i.e., some set (of objects) characterizing a type. For such an element of the domain of the lookup table, the specification of the operation is selected and returned.

The conversion \(C\) will be instantiated by a suitable “coercion” of a dynamic type to a class type to be discussed later (see section 4.9). Such a conversion is known to the pre-parser from the OCL types.

The process of selecting an arbitrary, but fixed function from a specification (i.e., a relation) is handled by the Choose-combinator omitted here. It is defined essentially as the context-lifting of the HOL Hilbert-Operator \(\varepsilon x. P x\) that just gives one result element satisfying \(P\); if this does not exist, the Hilbert-Operator picks an arbitrary element of this type.

Thus, the semantic code for the call-by-value invocation \(c.m(a_1, \ldots, a_n)\) is given by:

\[
\text{Choose}(\text{invokeS } C_{[A]} \ \text{tab}_m \ c \ a_1 \ldots \ a_n)
\]

where \(c\) is assumed as an object of class \(C\) and to have a subtype of \(A\) and \(C_{[A]}\) is a casting-function that converts \(C\) objects to \(A\) objects.

4.7.3. Embedding Adaption for Shallow Embedding

Semantic combinators for embedding adaptions are related to the embedding technique itself, namely the lifting/\textit{over} contexts. Recalling section 3.1 any function \(o\) with type \(T_1, \ldots, T_n \rightarrow T_{n+}\) of the object-language has to be transformed to a function:

\[
I[o] \quad \text{with type } [V_\tau(T_1), \ldots, V_\tau(T_n)] \Rightarrow V_\tau(T_{n+1}).
\]

As an example for a binary function like the built-in operation \(\cup\) (based on union defined in subsection 4.7.2), we present its constant definition:

\[
\cup \equiv \text{lift}_2 \text{union} \quad \text{with type } [(\alpha :: \text{bot}) \ \text{Set}_\tau, \alpha \ \text{Set}_\tau] \Rightarrow \alpha \ \text{Set}_\tau.
\]

\(^4\)It is a methodological issue to avoid this situation; i.e., a notion of a consistent OCL specification is needed which can be reduced to proof obligations. Such a proof methodology is discussed in a future version of this document.
4.8. Extensible Universes in Typed Meta-Language

Summing up the intermediate results of the local theory morphisms (i.e., the layers) in the previous subsections, the definition of our running example $\bigcup$ is given directly by:

$$\bigcup \equiv \text{lift}_2\left(\text{strictify}(\lambda X. \text{strictify}(\lambda Y. \text{AbsSet}[\text{RepSet} X \cup \text{RepSet} Y]))\right)$$

One easily recognizes our standard definition scheme, having AbsSet and RepSet as additional semantic combinators. During mechanical lifting of HOL theorems to OCL theorems (such as $A \cup B = B \cup A$), these operators require proofs for the invariance of the underlying quotient constructions; i.e., in this example, it must be proved that the union on representations of OCL sets will again be representations of an OCL set, (i.e., HOL sets not containing $\perp$).

4.8. Extensible Universes in Typed Meta-Language

The standard [H1, appendix A] uses naive set theory and an informal notion of “model” (in the sense of mathematical model theory) over a signature given by an informal class model. It implicitly assumes one big universe for values and objects (where undefinedness elements are just there . . .) and algebras over it without any concern of existence and consistency.

The standard cannot be formalized in this form in Isabelle, neither in an untyped set theory like Isabelle/ZF or a typed set theory underlying Isabelle/HOL; major efforts to make the foundations precise will have to be invested in both options. But since OCL is a typed language at the end, and since we wanted to have type-issues handled by the Isabelle type-checker and not inside the logic representation, it seemed for us also most natural to use a typed meta-language and typed set theory for this. In particular, in a shallow embedding, there should be a typed representation for each OCL expression, where the OCL type corresponds one-to-one to an HOL type (although not necessarily vice versa). Nevertheless, even our object universe construction should preserve the intentions of the standard, in the sense that general laws reflecting inheritance and subtyping on sets of objects can be derived. If possible, there should be no change of the users perspective of the OCL language, although its foundations have been worked out more precisely.

Recall that the OCL language specifies states and relations over them. The states are object structures, abstract representations of pieces of memory that were linked via references to each other. Formally, an object structure can be represented by a state $\tau$ mapping references or object id’s oid’s to objects, i.e., tuples of elementary values like integers or strings or object identifiers to other objects in the object structure. The type of these tuples corresponds to the type of the class they are belonging to; the components of the tuple correspond to the attributes of a class. The type of such an object structure is therefore oid $\Rightarrow \%$.

Instead of constructing a “universe of all objects” (which is either untyped or “too large” for a (simply) typed set theory, where all type sums must be finite), one could think of generating an object universe for each given class diagram. Ignoring subtyping
and inheritance for a moment, this would result in a universe \( U_0 \) = \( A + B + C \) for some class diagram with the classes \( A \), \( B \) and \( C \). Unfortunately, such a construction is not extensible: If we add a new class to an existing class diagram, say \( D \), then the “obvious” construction \( U_1 = A + B + C + D \) results in a different type to \( U_0 \), turning the two object structure types and all values constructed over them into something incomparable. This has quite dramatic consequences: such a representation rules out a modular, incremental construction of larger object systems as used in the UML standard document itself, for example. Properties, that have been proven over \( U_0 \) will not hold over \( U_1 \); practically, this means that all proof scripts will have to be rerun over an extended universe. Since even library proofs would have to be rerun (in current HOL-OCL, this takes about half an hour ...), such an approach is unfeasible.

Our solution to the problem is to use parametric polymorphisms for families for universes \( U_i \) (see Fig. 4.3 for a first overview of this idea), where the families stand for the “possible class diagram extensions”. Further, we extend the scheme sketched above by assigning to Classes not directly objects, but merely object extensions. This “incremental” object view (also used in many implementations) allows for the representation of object inheritance and leads, as we will see, to a smooth integration of object subtyping into the world of parametric polymorphism.

### 4.9. Encoding Object Structures

#### 4.9.1. The Basics

Recall that object universes are the core of our notion of state, which is the building block of our notion of context \( \tau \), which is again the building block of the semantic domain of HOL-OCL expressions: \( \tau \Rightarrow \alpha : \text{bot} \). In this section, we focus on families
4.9. Encoding Object Structures

of object universes $\mathcal{U}^i$, each of which corresponding to a class diagram. Each $\mathcal{U}^i$ comprises all value types (Real, Integer, String, Boolean, ...) and an extensible class type representation induced by a class hierarchy. To each class in a given class diagram, a class type is associated which represents the set of object instances or objects. The structure of a $\mathcal{U}^i$ is to provide a family of injections and projections to and from each class type. More precisely, if we assume a class $A$, this results in:

$$\text{mk}^{(0)}_A : \mathcal{U}^i \Rightarrow A,$$

and

$$\text{get}^{(0)}_A : A \Rightarrow \mathcal{U}^i,$$

allowing to inject any semantic value of OCL into some $\mathcal{U}^i$. Note, as we need also lifted version of these definitions, we will mark the different versions by different upper indexes. This in turn makes a family of states (containing “object systems”) possible:

$$\text{state} : \text{oid} \Rightarrow \mathcal{U},$$

from which concrete values may be accessed via an oid and then be projected via $\text{get}^{(0)}_A$. On this basis, the accessor functions composing OCL path expressions can be built.

The “families” of types and states are represented by parametric polymorphism in our approach. In the big picture, this encodes a subtype type system into the typed $\lambda$-calculus with parametric polymorphism underlying HOL in “shallow style” (c.f. [48]).

The extensibility of a universe type is reflected by “holes” (polymorphic variables), that can be filled when “adding” extensions to class objects which means adding subclasses to the class hierarchy. Our construction will ensure that $\mathcal{U}^{i+1}$ (corresponding to a particular class diagram) is just a type instance of $\mathcal{U}^i$ (where $\mathcal{U}^{(i+1)}$ is constructed by adding new classes to $\mathcal{U}^i$). Thus, properties proven over object systems “living” in $\mathcal{U}^i$ remain valid in $\mathcal{U}^{i+1}$.

The universe construction introduced so far follows the interpretation of object models given in the formal semantics of the standard:

Each object is uniquely determined by its identifier and vice versa. Therefore, the actual representation of an object is not important for our purposes.

(OCL Specification [41], page paragraph A.1.2.1)

The standard does not discuss constructors of objects. However, it is interesting to interpret this explicitly stated bijection between oids and object instances from the point of view of an operational semantics for them. There are essentially two choices:

1. an object constructor may have sharing semantics, i.e., the tuple of attribute values is searched in the global store; if existing, its reference into the store is returned, otherwise the tuple is entered into the state and associated to a fresh object identifier which is returned, or

Although, OCL includes the operation self.isNew() which, somehow, evaluates to true if self is a “fresh” object.

51
2. an object constructor may have creation semantics, i.e., generate a fresh object identifier and store it together with the tuple of attribute values in the store.

The former seems to be the underlying understanding of the original authors of \cite{[41], appendix A}. Even so, the author of the normative part always identifies objects by a reference to it, e.g.:

> If `self` is a reference to an object, then `self.property` is the value of the property `property` on `self`.  

(OCL Specification \cite{[41]}, page 15)

However, the latter view has the advantage to be closer to the usual programming language semantics of object constructors. Furthermore, in this setting, the reference to an object in the store can always be reconstructed which paves the way for reference equivalence as in Java or C++, and simple semantic definitions for `@pre` or referential equality (as discussed in definition 4.13).

Therefore, we provide, among others, one HOL-OCL configuration supporting non-referential universes and one supporting referential universes. Overall, we suggest to resolve this ambiguity in favor of the referential setting, which we also see as the default HOL-OCL configuration.

In our framework, the distinction between sharing semantics and creation semantics is reflected in two alternative universe constructions, namely the non-referential universe and the referential universe. In more detail, we can choose one of the following two types for `OclAny` and as basis for our universe construction:

\[
\alpha \text{OclAny} = \text{OclAny}_{\text{tag}} \times \alpha_{\perp} \quad \text{for building a non-referential universe, or} \\
\alpha \text{OclAny} = (\text{OclAny}_{\text{tag}} \times \text{oid}) \times \alpha_{\perp} \quad \text{for building a referential universe.}
\]

Where `OclAny_{type}` is an abstract datatype which makes the type for `OclAny` unique within our universe construction.

The “initial” universe type $\mathcal{U}_0^\alpha$ is defined as a sum of the built-in value types and the type `OclAny` (including all its extensions representing subtypes of `OclAny`):

\[
\mathcal{U}_0^\alpha = \alpha \text{OclAny} + \text{Values}.
\]

Since a class can be extended in several ways, the class hierarchy has a tree-like structure; where the leaves may be “holes.” Extending a universe type by instantiating the hole $\alpha$ is done as follows:

\[
\alpha \mapsto T \times \alpha_{\perp} + \beta
\]

where $T$ is the accumulative type of the attributes of the class extension and $\alpha_{\perp}$ represents the possible (future) extensions of this class. We present this idea in more formal detail in the next section.

---

52

---

6Technically, this different HOL-OCL configuration requires another theory for the basic type definition for `OclAny` (see subsection B.3.8 “Type Definition for `OclAny`” for details).
4.9. Encoding Object Structures

![Diagram showing a directed graph with nodes labeled as `Node` and `Cnode`, and attributes `depth()`, `i`, `left`, `right`, `color`.]

**Figure 4.4.:** Modelling Directed Graphs: Data Model

```plaintext
package digraph

class Node
def depth() = Integer
def i = Integer

def left = Node
def right = Node

class Cnode
color = Boolean
endclass

def inv range_of_i = self.i > 5

def inv: (not self.oclAsType(Node).left.oclIsUndefined() implies
      (not (self.oclAsType(Node).left.
        oclAsType(Cnode).color = self.color)))

and (not self.oclAsType(Node).right.oclIsUndefined() implies
      (not (self.oclAsType(Node).right.
        oclAsType(Cnode).color = self.color)))
endpackage
```

**Listing 4.1: Modelling Directed Graphs: OCL Specification**

### 4.9.2. The Formal Details of Encoding Object Structures

We will present the framework of our object encoding together with a small example: assume a class `Node` with an attribute `i` of type integer and two attributes `left` and `right` of type `Node`, and a derived class `Cnode` (thus, `Cnode` is a subtype of `Node`) with an attribute `color` of type `Boolean` (see Figure 4.4 and Listing 4.1 for details).

The `oclAsType()` expressions are not necessary since the OCL standard [41, p. 20] allows their syntactic omission. In OCL [41, p. 8], an invariant of class must evaluate to `true` for all instances (i.e., object of this class) at any time. Moreover, OCL is based on a three-valued logic. These two choices lead to several consequences:

1. Invariants must be valid, i.e., evaluate to `true` and are therefore defined.
2. From the definedness of the invariant and the strictness of `<>` follows the

---

7A more detailed discussion of a similar example can be found in section C.1.
Chapter 4. Faithfully Representing UML/\textit{OCL}

From the definedness of the invariant and the strictness of the equality follows that \texttt{self.color} must be defined, if the term \texttt{self.oclAsType(Node).left} or \texttt{self.oclAsType(Node).right} is defined.

4. From the definedness of the invariant and the strictness of the equality follows that \texttt{self.oclAsType(Node).left.oclAsType(Cnode).color} must be defined, if \texttt{self.oclAsType(Node).left} is defined. The case for \texttt{right} is symmetric.

5. From \texttt{self.oclAsType(Node).left.oclAsType(Cnode).color} being defined follows the definedness of \texttt{self.oclAsType(Node).left.oclAsType(Cnode)} and thus in this case \texttt{left} must be of type \texttt{Cnode}. Moreover, this means that \texttt{left} must fulfill the invariant for \texttt{Cnode}.

4.9.3. Type Constructions

In the following we define several type sets which all are subsets of the types of the \textit{HOL} type-system. This set, although denoted in usual set-notation, is a meta-theoretic construct, i.e., it cannot be formalized in \textit{HOL}. We start by defining all possible types for class attributes.

\textbf{Definition 4.1 (Attribute Types)} The set of attribute types \(\mathfrak{A}\) is defined inductively as follows:
1. \(\{\text{Boolean, Integer, Real, String, oid}\} \subset \mathfrak{A}\), and
2. \(\{a \text{ Set}, a \text{ Sequence}, a \text{ Bag}, a \text{ OrderedSet}\} \subset \mathfrak{A}\) for all \(a \in \mathfrak{A}\). \(\square\)

Attributes with class types, i.e., the attribute \texttt{left} of class \texttt{Node}, are encoded using the type \texttt{oid}. These object identifiers (i.e., references) will be resolved by accessor functions for a given state; an access failure will be reported by \(\bot\).

Similar to the description in the \textit{OCL} standard we represent the classes as a pairs of its attribute types which we extend by an an abstract datatype for each class which makes guarantees that each class type is unique. This gives a foundation for a strongly typed universe (with regard to the object-oriented type system).

\textbf{Definition 4.2 (Tag Types)} For each class \(C\) we assign a tag type \(t \in \mathfrak{T}\) which is just an abstract type used to make class types unique. The set \(\mathfrak{T}\) is called the set of tag types. \(\square\)

For class \texttt{Node} we assign an abstract datatype \texttt{Node}, with the only element \texttt{Node.key}, and we introduce the base type for classes:

\textbf{Definition 4.3 (Base Class Types)} The set of base class types \(\mathfrak{B}\) is defined as follows:
1. classes without attributes are represented by \((t \times \text{unit}) \in \mathfrak{B}\), where \(t \in \mathfrak{T}\) and \text{unit} is a special \textit{HOL} type denoting the empty product.
2. if \(t \in \mathfrak{T}\) is a tag type and \(a_i \in \mathfrak{A}\) for \(i \in \{0, \ldots, n\}\) then \((t \times a_0 \times \cdots \times a_n) \in \mathfrak{B}\). \(\square\)
4.9. Encoding Object Structures

Thus, the base object type of class \( \text{Node} \) is \( \text{Node}_1 \times \text{Integer} \times \text{oid} \times \text{oid} \) and of class \( \text{Cnode} \) is \( \text{Cnode}_1 \times \text{Boolean} \).

Without loss of generality, we assume in our object model a common supertype of all objects. In the case of OCL, this is \( \text{OclAny} \), in the case of Java this is \( \text{Object} \). This assumption is no restriction because such a common supertype can always be added to a given class structure without changing the overall semantics of the original object model.

**Definition 4.4 (OclAny)** Let \( \text{OclAny}_{\text{tag}} \in \mathcal{I} \) be the tag of the common supertype \( \text{OclAny} \) and \( \text{oid} \) the type of the object identifiers,

1. in the non-referential setting, we define \( \alpha_{\text{OclAny}} := (\text{OclAny}_{\text{tag}} \times \alpha_{\perp}) \).
2. in the referential setting, we define \( \alpha_{\text{OclAny}} := ((\text{OclAny}_{\text{tag}} \times \text{oid}) \times \alpha_{\perp}) \). □

Now we have all the foundations for defining the type of our family of universes formally:

**Definition 4.5 (Universe Types)** The set of all universe types \( U_{\text{ref}} \) resp. \( U_{\text{nonref}} \) (abbreviated \( U_x \)) is inductively defined by:

1. \( U_x^0 \in U_x \) is the initial universe type with one type variable (hole) \( \alpha \).
2. \( U_{(\alpha_{0},...,\alpha_{n},\beta_{1},...\beta_{m})} \in U_x \), \( n, m \in \mathbb{N} \), \( i \in \{0, ..., n\} \) and \( c \in \mathcal{B} \) then

\[
U_{(\alpha_{0},...,\alpha_{n},\beta_{1},...\beta_{m})} \left[ \alpha_{i} := \left( (c \times (\alpha_{n+1} + 1)) + \beta_{m+1} \right) \right] \in U_x
\]

This definition covers the introduction of “direct object extensions” by instantiating \( \alpha \)-variables.

3. \( U_{(\alpha_{0},...,\alpha_{n},\beta_{1},...\beta_{m})} \in U_x \), \( n, m \in \mathbb{N} \), \( i \in \{0, ..., n\} \), and \( c \in \mathcal{B} \) then

\[
U_{(\alpha_{0},...,\alpha_{n},\beta_{1},...\beta_{m})} \left[ \beta_{i} := \left( (c \times (\alpha_{n+1} + 1)) + \beta_{m+1} \right) \right] \in U_x
\]

This definition covers the introduction of “alternative object extensions” by instantiating \( \beta \)-variables. □

The initial universe \( U_x^0 \) represents the common supertype (i.e., \( \text{OclAny} \)) of all classes, i.e., a simple definition would be

\[
U_x^0 = \alpha_{\text{OclAny}}.
\]

Alternatively one can also encode values \( \text{Values} = \text{Real} + \text{Integer} + \text{Boolean} + \text{String} \) within the initial universe type, e.g.,

\[
U_x^0 = \alpha_{\text{OclAny}} + \text{Values}.
\]

For HOL-OCL we choose to represent also values within the universe which makes extensions possible that need to store values within the store. Thus we define the universes as follows:

**Definition 4.6 (Referential Universe Types)** The referential universe \( U_{\text{ref}} \) is constructed using the referential definition \( \alpha_{\text{OclAny}} := ((\text{OclAny}_{\text{tag}} \times \text{oid}) \times \alpha_{\perp}) \) in the definition of the initial universe:

\[
U_x^0 = \alpha_{\text{OclAny}} + \text{Real} + \text{Integer} + \text{Boolean} + \text{String}.
\]
Definition 4.7 (Non-Referential Universe Types) The non-referential universe $\mathcal{U}_{\text{nonref}}$ is constructed using the non-referential definition $\alpha \text{OclAny} := (\text{OclAny}_{\text{tag}} \times \alpha_\bot)$ in the definition of the initial universe:

\[ \mathcal{U}_0^0 = \alpha \text{OclAny} + \text{Real} + \text{Integer} + \text{Boolean} + \text{String}. \]

Extending the initial universe $\mathcal{U}_0^0(\alpha)$, in parallel, with the classes $\text{Node}$ and $\text{Cnode}$ leads to the following universe type:

\[ \mathcal{U}_1(\alpha_{\text{C}}, \beta_{\text{C}}, \beta_{\text{N}}) = \left( (\text{Node}_t \times \text{Integer} \times \text{oid} \times \text{oid}) \times ((\text{Cnode}_t \times \text{Boolean}) \times ((\alpha_{\text{C}})_{\bot} + \beta_{\text{C}})_{\bot} + \beta_{\text{N}}) \right) \text{OclAny} + \text{Values} \]

We pick up the idea of a universe representation without values for a class with all its extensions (subtypes). We construct for each class a type that describes a class and all its subtypes. They can be seen as “paths” in the tree-like structure of universe types, collecting all attributes in Cartesian products and pruning the type sums and $\beta$-alternatives.

Definition 4.8 (Class Type) The set of class types $\mathcal{C}$ is defined as follows: Let $\mathcal{U}$ be the universe covering, among others, class $C_n$, and let $C_0, \ldots, C_{n-1}$ be the supertypes of $C_n$, i.e., $C_1$ is inherited from $C_{i-1}$. The class type of $C_n$ is defined as:

1. $\forall C_i \in \mathcal{B}, i \in \{0, \ldots, n\}$ then
   \[ \mathcal{U}_n^0 = \left( C_0 \times \left( C_1 \times \ldots \times (C_n \times (C_{n-1})_{\bot})_{\bot} \right)_{\bot} \right) \in \mathcal{C}, \]

2. $\forall C_i \in \mathcal{C}$, where $\mathcal{U}_C$ is the set of universe types with $\mathcal{U}_n^0 = \mathcal{U}_n^0$.

Thus in our example we construct for the class type of class $\text{Node}$ the type

\[ ((\alpha_{\text{C}}, \beta_{\text{C}})) \text{Node} = \left( (\text{Node}_t \times \text{Integer} \times \text{oid} \times \text{oid}) \times ((\text{Cnode}_t \times \text{Boolean}) \times ((\alpha_{\text{C}})_{\bot} + \beta_{\text{C}})_{\bot} \right) \text{OclAny}, \]

and for $\text{CNode}$ the class type

\[ \alpha_{\text{C}} \text{ Cnode} = \left( (\text{Node}_t \times \text{Integer} \times \text{oid} \times \text{oid}) \times ((\text{Cnode}_t \times \text{Boolean}) \times ((\alpha_{\text{C}})_{\bot} \right) \text{OclAny}. \]

Here, $\alpha_{\text{C}}$ allows for extension with new classes by inheriting from $\text{Cnode}$ while $\beta_{\text{C}}$ allows for direct inheritance from $\text{Node}$. Alternatively, one could omit the lifting of the base types of the supertypes in the definition of class types. This would lead to:

\[ \mathcal{U}_n^0 = \left( C_0 \times \left( C_1 \times \ldots \times (C_n \times \alpha_{\bot}) \right) \right)_{\bot} \]

We see our definition as the more general one, since it allows for “partial objects” potentially relevant for other object-oriented semantics for programming languages.
4.9. Encoding Object Structures

For example Java, for which partial class objects may occur during construction. This paves the way for establishing the definedness of an object “lazy.” Furthermore, since the injections and projections are only built to define attribute accessors, partial objects are hidden from the OCL level.

In both cases the outermost \(⊥\) reflects that class objects may also be undefined, in particular after projection from some elements in the universe or from failing type casts. This choice has the consequence that constructor arguments may be undefined.

4.9.4. Treatment of Instances

For each class we provide injections and projects for each class. In the case of \texttt{OclAny} these definitions are quite easy, e.g., using the \texttt{Inl} constructors for type sums we can easily insert an \texttt{OclAny} object into the initial universe via

\[
\text{mk}^{(0)}_{\text{OclAny}} o = \text{Inl} o \quad \text{with type } \alpha \text{OclAny} \rightarrow \mathcal{U}^0_\alpha
\]

and the inverse function for constructing an \texttt{OclAny} object out of an universe can be defined as follows:

\[
\text{get}^{(0)}_{\text{OclAny}} u = \text{sumCase}(\lambda x. x, \lambda x. \varepsilon x. \text{true}, u) \quad \text{with type } \mathcal{U}^0_\alpha \rightarrow \alpha \text{OclAny}.
\]

In the general case, the definitions of the injections and projections is a little bit more complex, but follows the same schema: e.g., for the injections we have to find the “right” position in the type sum and insert the given object into that position. Using the following auxiliary functions

\[
\text{base} x = \begin{cases} b & \text{if } x = (a, b) \downarrow, \\ \text{down} & \text{otherwise}, \end{cases}
\]

\[
\text{sup} o = \text{fst} o \uparrow, \quad \text{and}
\]

\[
\text{FromL} x = \begin{cases} \text{sumCase}(\lambda x. x, \lambda x. x, \downarrow, \text{down, } x) & \text{if } x = v \downarrow, \\ \text{down} & \text{otherwise}, \end{cases}
\]

the injections for the classes \texttt{Node} and \texttt{Cnode} can be defined as follows:

\[
\text{get}^{(0)}_{\text{Node}} o = \text{get}^{(0)}_{\text{OclAny}} (\text{sup} o, \text{base}) \circ \text{Inl} o \downarrow \circ \text{base} o) \quad \text{and}
\]

\[
\text{mk}^{(0)}_{\text{Cnode}} o = \text{get}^{(0)}_{\text{Node}} (\text{sup} o, (\text{sup} \circ \text{base}) o, (\text{base} \circ \text{base} o) i \downarrow).
\]

And analogous for the projectors:

\[
\text{get}^{(0)}_{\text{Node}} u = ((\text{sup} o \circ \text{get}^{(0)}_{\text{OclAny}}) u, (\text{FromL} \circ \text{base} \circ \text{get}^{(0)}_{\text{OclAny}} u)), \quad \text{and}
\]

\[
\text{get}^{(0)}_{\text{Cnode}} u = ((\text{sup} o \circ \text{get}^{(0)}_{\text{Node}} u, (\text{sup} \circ \text{base} \circ \text{get}^{(0)}_{\text{Node}} u), (\text{FromL} \circ \text{base} \circ \text{base} o \circ \text{get}^{(0)}_{\text{Node}} u)), i \downarrow).
\]
Further, we define in a similar way projectors for all class attributes, e.g., for the attributes $i$ and $\text{self}$ of class $\text{Node}$ we generate:

$$
\text{self}.i^{(0)} \equiv \text{fst} \circ \text{snd} \circ \text{fst} \circ \neg \neg \circ \text{base} \ \text{self} \quad \text{with type } (\alpha_C, \beta_C) \ \text{Node} \to \text{int}, \text{ and}
$$

$$
\text{self}.\text{left}^{(0)} \equiv \text{fst} \circ \text{snd} \circ \text{snd} \circ \text{fst} \circ \neg \neg \circ \text{base} \ \text{self} \quad \text{with type } (\alpha_C, \beta_C) \ \text{Node} \to \text{oid}.
$$

In a next step, we define type test functions; for universe types we need functions for testing if a universe represents a specific type, i.e., we need to test that the corresponding extensions of the universe type are defined. For $\text{OclAny}$ we define:

$$
is\text{Univ}^{(0)}_{\text{OclAny}} u = \text{sumCase}(\lambda x. \text{true}, \lambda x. \text{false}, u) \quad \text{with type } \mathcal{U}_0^\alpha \to \text{bool}.
$$

For class types we define two type tests, an exact one that tests if an object is exactly of the given dynamic type and a more liberal one that tests if an object is of the given type or a subtype thereof. Testing the latter one, which is called kind in the OCL standard, is quite easy. We only have to test, that the base type of the object is defined, e.g., not equal to $\bot$:

$$
is\text{Kind}^{(0)}_{\text{OclAny}} o = \text{def} o \quad \text{with type } \alpha_{\text{OclAny}} \to \text{bool}.
$$

An object is exactly of a specific type, if it is of the given kind and the extension is undefined, e.g.:

$$
is\text{Type}^{(0)}_{\text{OclAny}} o = is\text{Kind}^{(0)}_{\text{OclAny}} \land \neg(\text{def} \circ \text{base}) o \quad \text{with type } \alpha_{\text{OclAny}} \to \text{bool}.
$$

The type tests for user defined classes are defined in a similar way by testing the corresponding extensions for definedness.

Finally, we define coercions, i.e., ways to type-cast classes along their subtype hierarchy. Thus we define for each class a cast to its direct subtype and to its direct supertype. We need no conversion on the universe types where the subtype relations are handled by polymorphism. Therefore we can define the type casts as simple compositions of projections and injections, e.g.:

$$
\text{Node}^{(0)}_{\text{Object}} = \text{get}^{(0)}_{\text{Object}} \circ \text{mk}^{(0)}_{\text{Node}} \quad \text{with type } (\alpha_1, \beta) \ \text{Node} \to \alpha_{\text{Any}} \ \text{OclAny},
$$

$$
\text{Object}^{(0)}_{\text{Node}} = \text{get}^{(0)}_{\text{Node}} \circ \text{mk}^{(0)}_{\text{Object}} \quad \text{with type } \alpha_{\text{Any}} \ \text{OclAny} \to (\alpha_1, \beta_1) \ \text{Node},
$$

where $\alpha_{\text{Any}} = (\alpha_1, \beta)$ $\text{Node} + \beta_{\text{Any}}$, i.e., the free type variable $\alpha_{\text{Any}}$ of $\alpha_{\text{Any}}$ $\text{OclAny}$ in the Universe $\mathcal{U}_{\text{Any}}^0$ is instantiated to match type of the $\mathcal{U}_{\text{Any}}^1(\alpha_1, \beta_1)$. These type-casts are changing the static type of an object, while the dynamic type remains unchanged, i.e., one can always re-cast an object to the type it was initially created.

Note, for a universe construction without values, e.g.,

$$
\mathcal{U}_0^\alpha = \alpha_{\text{OclAny}},
$$
the universe type and the class type for the common supertype are the same. In that case there is a particular strong relation between class types and universe types on the one hand and on the other there is a strong relation between the conversion functions and the injections and projections function. In more detail, see also Figure 4.5, one can understand the projections as a cast from the universe type to the given class type and the injections are inverse.

As a consequence, a theorem over class invariants (based finally on these projections, injections, casts, characteristic sets, etc.), it will remain valid even if we extend the universe via $\alpha$ and $\beta$ instantiations. In particular, this holds if we “finalize” classes by instantiating the $\alpha$’s and $\beta$’s related to this class by instantiating them by the unit type. We consider this fact as a solution to the long-standing problem of structured extensionally for object-oriented languages, enabling to represent “open world” and “closed world” assumptions as polymorphism on data universes.

4.9.5. Adaption to Higher Layers

The previous presented definitions are on the lowest layer, i.e., the introduction of new datatypes. Just as the HOL definition are adopted, over several layers, to match the OCL definitions, we have to adopt the new definitions for the UML core. For example,
Chapter 4. Faithfully Representing \textit{UML}, \textit{OCL}

after the functional and embedding adoptions, the accessor for the attributes \(i\) is:

\[
self.i^{(1)} \equiv \text{strictify} \circ \text{lift}_0(self.\ i^{(0)}) \quad \text{with type } (\alpha_C, \beta_C) \text{ Node}_r \rightarrow \text{Integer}_r,
\]

and for \texttt{left}:

\[
(self \ \tau).\ \texttt{left}^{(1)} \equiv \text{upCase}(\text{get}_{\text{Node}}^{(0)}, \bot, \text{fst} \ \tau \ (self \ \tau).\ \texttt{left}^{(0)})
\]

with type \((\alpha_C, \beta_C) \text{ Node}_r \rightarrow (\alpha_C, \beta_C) \text{ Node}_r\). The accessor for the \texttt{left} is somewhat more complicated as we have to resolve reference, i.e., note the change of types during adaption.

As already shown in these examples, we will use an upper index to distinguish the different definitions on different levels.

4.10. Faithful Representing \textit{UML} Object Structures

For backing our claim that the presented encoding of object structures models faithfully the concepts that are normally described as object-oriented (e.g., in the sense of programming language like Java or Smalltalk or the \textit{UML} standard \cite{uml_standard}), we prove several of the required properties. These theorems are proven for each class, e.g., during loading a specific \textit{UML} model. This is similar to other datatype packages in interactive theorem provers like Isabelle/\textit{HOL}. Further, these theorems are also a prerequisite for a successful reasoning over object structures.

First we prove some basic properties of our injections and projects, i.e., mainly that our conversion between universe representations and object representation is lossless. Therefore we show for very class \(C\) that

\[
isKind^{(0)}_C o \implies \text{get}^{(0)}_C (\text{mk}^{(0)}_C o) = o \quad \text{and} \quad \text{isUniv}^{(0)}_C u \implies \text{mk}^{(0)}_C (\text{get}^{(0)}_C u) = u.
\]

holds. Further, we show that the injection

\[
isType^{(0)}_C o \implies \text{isUniv}^{(0)}_C (\text{mk}^{(0)}_C o)
\]

results in a correct universe type and that the projection

\[
isUniv^{(0)}_C u \implies \text{isKind}^{(0)}_C (\text{get}^{(0)}_C u)
\]

results in the right class type. We also show the important subtyping relation, i.e., that injections a class \(C\) creates a universe type which is of the kind of the parent class \(P\):

\[
isKind^{(0)}_P o \implies \text{isUniv}^{(0)}_P (\text{mk}^{(0)}_C o),
\]

and that every universe of type \(C\) is also of the kind of the parent class \(P\):

\[
isUniv^{(0)}_C u \implies \text{isUniv}^{(0)}_P u.
\]
Moreover, we show that our definitions support lossless re-casting, i.e.,

\[
is\text{Kind}^{(0)}_C \text{self} \implies P^{(0)}(\text{Cl}_C^{(0)} \text{self}) = \text{self}
\]

4.11. A Constrained Object Store: Encoding Invariants

In this section, we bring \texttt{OCL} and \texttt{UML} together, i.e., we enrich the pure \texttt{UML} data model with invariants which supports the encoding of recursive object structures with class invariants. This constructions follows the spirit of the already presented scheme: we begin with a co-recursive construction of type sets (which can be seen as a kind of first level invariant) which later on define a second level construct, providing a representation that looks similar to people involved in object-oriented modeling.

4.11.1. A Co-Recursive Type and Kind Set Construction

In a setting with subtyping, we need two characteristic type sets, a sloppy one, the \textit{characteristic kind set}, and a fussy one, the \textit{characteristic type set}. We define these sets co-recursively. As basis for our co-recursive construction, we built for each invariant a “\texttt{HOL} representation,” i.e., in each formula where we replace recursively the logical connectives of \texttt{OCL} with them from \texttt{HOL} by requiring the validness of the subformula. This is done using the \textit{logical judgement} \( \tau \vdash P \) which means that the \texttt{OCL} formula \( P \) is valid (i.e., evaluates to \( \top \)) in context \( \tau \). This is explained in more detail in chapter 5.

As we want to use these invariants for a co-recursive construction we parametrize them over the current state \( \tau \), the object \texttt{self} and the type set \( C \) we are constructing.

Recall our previous example (see Figure 4.4 and Listing 4.1), where the class \texttt{Node} describes a potentially infinite recursive object structure. The invariant of class \texttt{Node} constrains the attribute \texttt{i} to values greater than 5. For this constraint, we generate

\[
\text{hol}_\text{inv}\_\text{range}\_\text{of}\_i\ \tau\ C\ \text{self}\ \equiv\ \tau \vdash \text{self}.i^{(1)} > 5
\]

Further, we generate the two invariants expressing the fact that \texttt{left} and \texttt{right} must be either undefined or of type \texttt{Node}:

\[
\begin{align*}
\text{hol}_\text{inv}\_\text{type}\_\text{left} & \ \tau \ C \ \text{self}\ \equiv\ \tau \vdash \emptyset \ \text{self}.\left^{(1)} \\
& \lor \tau \vdash \text{self}.\left^{(1)} \in (\lambda f. f\tau) \setminus C
\end{align*}
\]

\[
\begin{align*}
\text{hol}_\text{inv}\_\text{type}\_\text{right} & \ \tau \ C \ \text{self}\ \equiv\ \tau \vdash \emptyset \ \text{self}.\right^{(1)} \\
& \lor \tau \vdash \text{self}.\right^{(1)} \in (\lambda f. f\tau) \setminus C
\end{align*}
\]

Now we define a function for construction the kind set for \texttt{Node} which approximates
Chapter 4. Faithfully Representing UML/OCL

the set of possible instances of the class `Node` and its subclasses:

\[
\text{NodeKindF} :: U^1_{(\alpha_C, \beta_C, \beta_N)} \Rightarrow (\alpha_C, \beta_C) \text{ Node set} \\
\Rightarrow U^1_{(\alpha_C, \beta_C, \beta_N)} \Rightarrow (\alpha_C, \beta_C) \text{ Node set}
\]

\[
\text{NodeKindF} \equiv \lambda \tau. \lambda X. \{ \text{self} \mid \text{hol_inv_type_left } \tau X \text{self} \\
\wedge \text{hol_inv_type_left } \tau X \text{self} \\
\wedge \text{hol_inv_type_right } \tau X \text{self} \}
\]

By adding the conjunct \( \tau \models \text{isType}^{(1)} \text{Node} \text{self} \), we can construct another approximation function (which has obviously the same type as \( \text{NodeKindF} \)):

\[
\text{NodeTypeF} :: U^1_{(\alpha_C, \beta_C, \beta_N)} \Rightarrow (\alpha_C, \beta_C) \text{ Node set} \\
\Rightarrow U^1_{(\alpha_C, \beta_C, \beta_N)} \Rightarrow (\alpha_C, \beta_C) \text{ Node set}
\]

\[
\text{NodeTypeF} \equiv \lambda \tau. \lambda X. \{ \text{self} \mid (\text{self} \in (\text{NodeKindF} \tau X)) \\
\wedge \tau \text{isType}^{(1)} \text{Node} \text{self} \}
\]

Thus, the characteristic kind set for the class `Node` can be defined as the greatest fixedpoint over the function \( \text{NodeKindF} \):

\[
\text{NodeKindSet} :: U^1_{(\alpha_C, \beta_C, \beta_N)} \Rightarrow (\alpha_C, \beta_C) \text{ Node set} \\
\Rightarrow U^1_{(\alpha_C, \beta_C, \beta_N)} \Rightarrow (\alpha_C, \beta_C) \text{ Node set}
\]

\[
\text{NodeKindSet} \equiv \lambda \tau. (\text{gfp}(\text{NodeKindF} \tau)).
\]

For the characteristic type set we proceed analogously. Further, we prove automatically, using the monotonicity of the approximation functions, the point-wise inclusion of the kind and type sets:

\[
\text{NodeTypeSet} \subset \text{NodeKindSet}
\]

This property represents semantically the subtype relation. This kind of theorem remains valid if we add further classes in a class system.

Now we relate class invariants of subtypes to class invariants of supertypes. The core of the construction for characteristic sets taking the class invariants into account is a greatest fixedpoint construction (reflecting their co-algebraic properties). We proceed by defining a new approximation for an inherited class `Cnode` on the basis of the approximation function of the superclass:

\[
\text{CnodeF} \equiv \lambda \tau. \lambda X. \{ \text{self} \mid \text{self}^{(1)}_{[\text{Node}]} \in (\text{NodeKindF} \tau (\lambda o. \text{o}^{(1)}_{[\text{Node}]} \setminus X) \\
\wedge (\varphi \tau X \text{self}) \}
\]

where \( \varphi \) stand for the constraints specific to the subclass. Note \( \varphi \) must appropriately include \( \tau \models \text{self} \cdot \text{right}^{(1)} \in (\lambda f. f \tau) \setminus X \) to make the implicit recursion in the `Cnode` invariant explicit.

62
4.11. A Constrained Object Store

Similar to [42] we can handle mutual-recursive datatype definitions by encoding them into a type sum. However, we already have a suitable type sum together with the needed injections and projections, namely our universe type with the make and get methods for each class. The only requirement is, that a set of mutual recursive classes must be introduced “in parallel,” i.e., as one extension of an existing universe.

Our construction for type sets and kind sets provides for an object a tight connection between “being of a type” and “fulfilling its invariant,” i.e., the invariant for Node can be defined semantically as follows:

\[
\text{Node\_sem\_inv } self \equiv self \in \text{NodeKindSet } \text{ with type } (\alpha_C, \beta_C) \text{ Node } \rightarrow \text{Boolean}.
\]

4.11.2. Functional Adoption: Invariant Awareness

Using our invariant definition we can do the last step needed to combine our OCL embedding with our embedding of the UML core, i.e., we have to test if an object fulfills its invariant. This can easily done, e.g., for the accessor for attribute \( i \) of class Node we define:

\[
\text{self\_}i \equiv \text{if Node\_sem\_inv } self \text{ then self\_}i^{(1)} \text{ else } \bot \text{ endif }.
\]

All other, previously introduced definitions, are also adopted by wrapping them in an if-then-else-endif statement.

4.11.3. Defining Invariants

The semantic invariant definition previously introduced is not a representation an object-oriented modeler would expect. Therefore we define for each class a “user representation.” This representation is based on the accessor introduced in the last section, e.g., for Node we define:

\[
\text{Node\_defined } self \equiv \partial self ,
\]

\[
\text{Node\_inv\_range\_of\_i } self \equiv self\_i > 5 , \text{ and } \text{Node\_inv } self \equiv \text{Node\_defined } self \wedge \text{Node\_inv\_range\_of\_i } self .
\]

The constraint Node\_defined ensures the definedness of self, which allows us to prove the equivalence of both invariant representations, e.g., for Node we prove:

\[
\text{Node\_inv } self = \text{Node\_sem\_inv } self.
\]

Thus, we can provide the users of HOL-OCL an invariant representation that looks familiar to the OCL specification:

\begin{verbatim}
context Node
inv range_of_i : self\_i > 5
\end{verbatim}

Moreover, this representations allows proving of many system properties without the need of using co-recursive induction schemes.
Chapter 4. Faithfully Representing UML

4.12. An Object-Oriented Type-System

Within HOL-OCL we represent types via their characteristic set. Therefore, we lift both, the characteristic type set and characteristic kind set of each type (i.e., all basic types like Integer and also for all user defined types) introduced in subsection 4.11.1 to the OCL level. For doing so, we need to extend the OCL standard in two ways:

- The characteristic set, i.e., the set of all instances, can be infinite (e.g., for the type Integer). Therefore we use an infinite set theory for HOL-OCL. In subsection 5.6.3 we discuss the advantages of this setup in more detail.

- For supporting characteristic sets in front-end tools, we introduce two new operations:

  - `typeSetOf()` -- Returns all possible instances of self, this may be an infinite set. The Type T is equal to self.
    \[ OclType::typeSetOf()::Set(T) \]

  - `kindSetOf()` -- Returns all possible instances of self and its subtypes, this may be an infinite set. The Type T is equal to self.
    \[ OclType::kindSetOf()::Set(T) \]

For example, they allow one to specify, that the addition on Integers is associative:

\[ Integer::typeSetOf():->\forall x, y | (\neg x.oclIsUndefined() \land \neg y.oclIsUndefined()) \implies x + y = y + x \]

Our encoder will map the expression `type::typeSetOf()` and `type::kindSetOf()` directly to the corresponding type (kind) set.

4.13. Operation Invocations

We distinguish built-in operations (i.e., all library operations such as the logical operation \( \neg \), the arithmetical operation \( X + Y \) or the collection operation \( X \cup Y \)) and user-defined operations declared in class diagrams.

While built-in operations cannot be overloaded in HOL-OCL in order not to hamper algebraic reasoning on OCL expressions, user-defined operations can be overloaded which is considered as a main feature of object-oriented programming. However, as already discussed in subsection 4.7.2 the OCL 2.0 standard assumes that operation calls are statically known and makes therefore no statement on which overload resolution strategy is used; in earlier documents of the OCL semantics definition, it is suggested to users to be compliant to an arbitrary resolution strategy.
It is clearly feasible to make any static resolution strategy explicit in OCL by suitable \texttt{oclIsType()} or \texttt{oclIsKind()} tests on the arguments. However, as an experimental feature, we suggest to extend the OCL 2.0 standard by a dynamic late-binding strategy. In this section, we show how the semantics of strict operation invocations is encoded using the semantic combinator for strict invoke defined in 4.7.2.

### 4.13.1. The Invocation Encoding Scheme

**Initial Operation Definition**

In the following, we show the semantic representation scheme of invocation for user-defined operations by an example. We assume the three classes \(A\), \(B\) and \(C\), where \(C\) inherits from \(B\) and \(B\) inherits from \(A\), see Figure 4.5 on page 59 for an illustration of this scenario. Further, we assume that an operation \(m\), specified in the topmost class \(A\), with arguments \(a_1 :: T_1, \ldots, a_n :: T_n\), return type \(T\), the precondition \(P\), and postcondition \(Q\).

In the following, we will present declaration related infrastructure for invocations as introduced in subsection 4.7.2 more detail. We reconsider the scheme of an operation specification first: an operation \(m\), with arguments \(a_1 :: T_1, \ldots, a_n :: T_n\), return type \(T\), is declared by a pair of precondition and postcondition, thus, for each method we introduce a precondition and a postcondition:

\[
\text{pre self } a_1 \ldots a_n \text{ of type } [V_r(A), V_r(T_1), \ldots, V_r(T_n)] \Rightarrow \text{Boolean} \text{ and pre self } a_1 \ldots a_n \text{ result of type } [V_r(A), V_r(T_1), \ldots, V_r(T_n), V_r(T)] \Rightarrow \text{Boolean}.
\]

The precondition \(\text{pre}\) is a predicate function depending on the input parameter including the implicit input parameter \(\text{self}\). The postcondition \(\text{post}\) is a predicate function depending on the input parameter and the implicit \(\text{result}\) parameter. The implicit parameters \(\text{self}\) and \(\text{result}\) are defined in OCL they represent a common concept in object-oriented languages.

The standard defines the semantics of an operation specification by

\[
\tau_{\text{pre}} \models \text{pre self } a_1 \ldots a_n \land (\tau_{\text{pre}}, \tau_{\text{post}}) \models \text{post self } a_1 \ldots a_n \text{ result},
\]

assuming technically two different validity predicates \(\models\). We represent the former by the latter (replacing all accessors occurring in \(\text{pre}\) by their \(\@\text{pre}\)-variant) and slightly generalize to:

\[
S_m \text{ self } a_1 \ldots a_n \text{ result } \tau \models \tau \equiv \tau \models ((\text{pre self } a_1 \ldots a_n) \land (\text{post self } a_1 \ldots a_n \text{ result}))
\]

allowing to distinguish undefined specifications from contradictory ones. We will abbreviate this by \(S_m\) in the sequel.
Chapter 4. Faithfully Representing UML/OCL

Furthermore, we define the totalized operation specification:

\[
S_{m-tot} \text{self } a_1 \ldots a_n \text{ result } \tau \equiv \tau \models \text{if } \partial(\text{pre self } a_1 \ldots a_n) \land \text{pre self } a_1 \ldots, a_n \\
\text{then post self } a_1 \ldots a_n \text{ result} \\
\text{else } \emptyset \text{ result} \\
\text{endif}
\]

which can be used alternatively in HOL-OCL and which is preferable for methodological issues, namely for proofs of consistency of OCL specifications (not discussed in this document). We will abbreviate this by \(S_{m-tot}\) in the sequel.

Now, when processing the above part of the class declaration, the following HOL declaration of a lookup table \(\text{tab}_m\) is generated:

\[
\text{tab}_m : \{A \text{ set } \leftarrow [V_{\tau}(A), V_{\tau}(T_1), \ldots, V_{\tau}(T_n), V_{\tau}(T)] \Rightarrow \text{Boolean}_{\tau}\}
\]

Here, the arrow \(_\leftarrow _\) stands for the type of partial maps from the HOL library. The main difference of partial maps compared to total functions \(_\Rightarrow _\) is that partial functions have a domain operator \(\text{dom}\) with type \(\alpha \leftarrow \beta \Rightarrow \alpha \text{ set}\). Additionally, the axiom:

\[
\text{tab}_m \ A \equiv \text{Some}(S_m) \quad (4.2)
\]

or

\[
\text{tab}_{m-tot} \ A \equiv \text{Some}(S_{m-tot}) \quad (4.3)
\]

where \(A\) is the characteristic set of the class \(A\). In the concluding subsection, we will discuss the conservativity issue for this type of axioms which is similar, but technically unequal to a constant definition since the table is not defined once and for all, but pointwise for a finite set of arguments.

**Inheritance of Operation**

Now we consider the case, that the class \(B\) is declared, but operation \(m\) is not redeclared, i.e., inherited from class \(A\). This leads to the axioms:

\[
\text{tab}_m \ B \equiv \text{Some}(S_m) \quad (4.4)
\]

or

\[
\text{tab}_{m-tot} \ B \equiv \text{Some}(S_{m-tot}) \quad (4.5)
\]

Recall that due to our object universe construction, the type of \(B\) is an instance of the type of \(A\) even if the class \(B\) has been inserted into the system in a later stage than the compilation of \(A\), i.e., \(A\) and \(B\) live in different universes. Moreover, in the later universe, the property \(B \subset A\) holds and has been proven automatically.
4.13. Operation Invocations

**Operation Overriding**

Now we consider the case of an operation overriding, i.e., a new declaration, we introduce a new specification for the operation $m$ for class $C$ (and its subclasses) with precondition $P'$ and postcondition $Q'$. Again, see Figure 4.5 for details. Analogously to the overloading case, the two axioms:

$$\text{tab}_m B \equiv \text{Some}(S'_m)$$

or

$$\text{tab}_{m\text{-tot}} B \equiv \text{Some}(S'_{m\text{-tot}})$$

were constructed where $S'_m$ and $S'_{m\text{-tot}}$ were the operation specifications or totalized operation specifications as defined in 4.13.1.

4.13.2. Considering Conservativity

The axioms generated in the previous sections are conservative; however, they do not fit into one of the standard schemes such as constant definition (the argument of $\text{tab}_m$ and $\text{tab}_{m\text{-tot}}$ are a changing constant not allowed in this scheme). Rather, it is a finite family of constant definitions, where the overall type is refined from universe to universe. In the following, we characterize the syntax of this axiom scheme and sketch a proof of conservativity for it.

**Definition 4.9 (Finite Constant Definition Family)** A finite constant definition family is a theory extension $(\Sigma, A)$ where $\Sigma$ is a constant declaration $c :: \tau_1 \to \tau_2$ and $A$ is a finite sequence of axioms of the form $c \ D_1 \equiv E_1 \ldots c \ D_n \equiv E_n$ where $D_i$ and $E_i$ are closed expressions. One further optional rule, the catch-all rule, has the form: $X /\in \{D_1, \ldots, D_n\} \implies c \equiv E_{n+1}$. Furthermore, the following conditions must be satisfied:

1. $c$ does not occur in $E_1$.
2. $c$ does only occur in $E_j$ (in fact: in no defining expression $E$ in a definition except that the catch-all rule is known) in the form $c \ D_i$ with $i < j$.
3. The type of $c$ in axiom $j$ must be an instance of the type of $c$ in axiom $i$ with $i < j$.
4. All type variables occurring in any type of a subterm of $E_j$ must occur in the type of $c \ D_j$.
5. $D_j = D_k \implies j = k$, i.e., the $D_j$ must be pairwise disjoint.

The catch-all rule is used when a class is finalized, i.e., the class cannot be used as starting point for further inheritance.

**Theorem 4.1 (Conservativity)** A finite constant definition family is conservative, i.e., provided the original theory $(\Sigma, A)$ is consistent (“has models”), the theory $(\Sigma \cup \Sigma', A \cup A')$ extended by the extension $(\Sigma', A')$ is also consistent.
Chapter 4. Faithfully Representing UML/OCL

Proof In case that the catch-all rule is unknown, translate the constant definition family into a family of constant definitions with constants $c_{D_j}$. In case that the catch-all rule is known, the constant definition family can be replaced equivalently by the constant definition $c \ X \equiv \text{if } X = D_1 \text{ then } E_1 \text{ else ... else } E_{n+1}$.

The axioms above represent a constant definition family since partial maps $\alpha \rightarrow \beta$ are just a synonym for $\alpha \Rightarrow \beta$ option. The pairwise disjointness follows from the full inclusion of the characteristic sets assured by construction.

4.13.3. Limits to Recursive Invocations

Let us briefly reconsider why conservativity is fundamental for HOL-OCL: an UML/OCL model can be inconsistent in the sense that there is no state that satisfies all invariants or that a method produces a state contradicting the invariants. However, no axiom generated during the compilation of the UML/OCL model into Isabelle/HOL should introduce a logical inconsistency into the meta-logic HOL, i.e., reasoning in itself should never be corrupted. A proof over the consistency of an UML/OCL model in the above sense should be valid in any case, independent of any generated axiom. Therefore, we require that method definitions in class diagrams satisfy the constraints of a finite constant definition family.

This has consequences on the form of admissible recursive operation invocations in HOL-OCL: the conditions 1 and 2 in definition 4.9 rule out a general recursive invocation of the operation to be specified. Consider again the operation $m$ specified in class $C$, which overrides the operation $m$ already defined in class $A$. Assume that the postcondition of $m$ defined in class $C$ is given by

```
context C::m(a1:T1, ..., an:Tn): Integer
post: result = 1 + self.m(a1, ..., an)
and self.m(a1, ..., an).isDefined()
```

Following subsection 4.7.2, the operation invocation is represented by:

```
Choose(invokeS C[A] tab m self a1 ... an)
```

which conflicts with $tab_m$ directly to condition 2 of definition 4.9.

The example also shows why this kind of syntactic restriction is necessary: from $self.m(a1, ..., an) = 1 + self.m(a1, ..., an)$ and the definedness of the result one can infer $1 = 0$ in OCL and then false in HOL and then simply everything from there.

The OCL standard vaguely requires that recursions should always be terminating to rule out such kind of problems:

Underspecification of Recursion

The right-hand-side of this definition may refer to operations being defined (i.e., the definition may be recursive) as long as the recursion is not infinite.

(OCL Specification [41], page paragraph 7.5.2, pp.16)

and also:
For a well-defined semantics, we need to make sure that there is no infinite recursion resulting from an expansion of the operation call. A strict solution that can be statically checked is to forbid any occurrences [...] However, allowing recursive operation calls considerably adds to the expressiveness of OCL. We therefore allow recursive invocations as long as the recursion is finite. Unfortunately, this property is generally undecidable.

(OCL Specification [41], page A-31)

Unfortunately, in a proof-environment we have to be sufficiently more specific than this. Furthermore, HOL-OCL is designed to live with the open-world assumption, i.e., with the potential extensibility of object universes, as a default; further restrictions such as finalizations of class diagrams or a self-restriction to Liskov’s Principle may be added on top, but the system in itself does not require them. This has the consequence that even in the following version:

```plaintext
context C::m(a1:T1,..., an:Tn): Integer
  post: result = if a1.p() then 1 + self.m(a1.q(),... , an) else 0 endif
```

the termination for the invocation `self.m(a1.q(),...,an)` is fundamentally unknown (even if `p` and `q` are known and terminating): a potential overriding may destroy the termination of this recursive scheme.

In form of a pre-translation process, operation specifications with a limited form of recursive invocations can be converted into the format that satisfies the constraints of a finite constant definition family. These limited forms are assumed to occur in the postcondition `Q'` and can be listed as follows:

- calls to superclass operations, i.e., `(self.asType(A)).m(x1,...,xn)`, or
- direct recursive well-founded invocations, i.e., `(self.asType(C)).m(x1,...,xn)`.

The former invocation can be translated simply into `Choose(S_m self x1 ... xn)` or `Choose(S_m-tot self x1 ... xn)`. The latter is based on the theory of well-founded orders and the well-founded recursor `wfrec` in Isabelle/HOL and so to speak an application of the standard HOL methodology to OCL. We assume the following version:

```plaintext
context C::m(a1:T1,..., an:Tn): Integer
  post: result = if a1.p() then 1 + (self.asType(C)).m(a1.q(),... , an) else 0 endif
```
Chapter 4. Faithfully Representing UML/OCL

The idea is to abstract away the occurrence of the recursive call:

\[
\begin{align*}
\text{post}_{\text{rec}} f \text{ self } a_1 \ldots a_n \text{ result } & \equiv \text{ result } \triangleq \text{ if } a_1.p() \\
& \quad \text{ then } 1 + (f \ a_1.q)() \ldots a_n \\
& \quad \text{ else } 0 \\
& \quad \text{ endif}
\end{align*}
\]

and to build the operation specification notions on top of it: Let

\[
S_{m-\text{rec}} f \text{ self } a_1 \ldots a_n \text{ result } \tau \equiv \tau \models \left( \text{ pre self } a_1 \ldots a_n \\
\& \text{ post}_{\text{rec}} f \text{ self } a_1 \ldots a_n \text{ result} \right)
\]

and

\[
S_{m-\text{tot-rec}} f \text{ self } a_1 \ldots a_n \text{ result } \tau \equiv \tau \models \text{ if } \partial(\text{ pre self } a_1 \ldots a_n) \& \text{ pre self } a_1 \ldots a_n \\
\quad \text{ then } \text{ post}_{\text{rec}} f \text{ self } a_1 \ldots a_n \text{ result} \\
\quad \text{ else } \nexists \text{ result} \\
\quad \text{ endif}
\]

then, for direct recursive calls, the operation specifications are defined as \(S_m \equiv \text{ Wfrec } M S_{m-\text{rec}} \) or \(S_{m-\text{tot}} \equiv \text{ Wfrec } M S_{m-\text{tot-rec}}\) where \text{ Wfrec } is the context-lifted version of \text{ wfrec } and \(M\) is an ordering (such as \(x < y\) restricted on positive integers).

If this ordering is well-founded, from this definition, the original user-specified post-condition follows from this definition. Since the critical call is now incorporated into the well-founded recursion construction, the definition is conservative; and provided the user gives a suitable ordering, it can be shown that the desired specification follows from the constructed definitions.

Alternatively, in case of a finalized class, an invocation

\[
\text{ invokeS C tab}_m \text{ self } a_1 \ldots a_n
\]

can by replaced by the case-switch:

\[
\text{ if } \text{ self } \rightarrow \text{ IsType}(A) \text{ then } S \text{ else if } \ldots \text{ else } S''
\]

Summing up, conservativity implies that only limited forms of recursive invocations are admissible in HOL-OCL. In an open world (no class finalization so far), only operation calls can be treated, in a closed world (the class hierarchy has been finalized), an invocation can be expanded to a case-switch considering the dynamic type of \text{ self} over calls.


Historically, object-oriented systems are equipped with a variety of different “equalities” \[30\]. Answering the question if two objects are equal is not so obvious: e.g., are

two objects equal only if their object identifier is equal (are they the same object?) or are two objects equal if their values are equal, or are they equal if they are observably equivalent with respect to the accessor functions? In the following we will use this problem as a linchpin to discuss the differences between a referential universe and a non-referential universe.

Whereas in traditional specification formalism the equality is defined over values, the most basic equality over objects is the reference quality or identity equality which is also the kind of equality that is usually provided as a default, i.e., “built-in,” equality in object-oriented languages. Thus, there is usually a fundamental difference between values and objects.

**Definition 4.10 (Value Types)** The set of *value types* \( \mathcal{V} \) is defined inductively as follows:

1. \( \{ \text{Boolean, Integer, Real, String} \} \subseteq \mathcal{V} \), and
2. \( \{ v \text{ Set}, v \text{ Sequence}, v \text{ Bag}, v \text{ OrderedSet} \} \subseteq \mathcal{V} \) for all \( v \in \mathcal{V} \). □

**Definition 4.11 (Values)** An instance of a value type, e.g., \( x :: v \) with \( v \in \mathcal{V} \) is called *value*. □

Normally one expects that an equality is an equivalence relation.

**Definition 4.12 (Equivalence Relation)** An *equivalence relation* \( _\sim \) is a binary relation over a set \( S \) for which the following properties hold:

- Reflexivity: \( a \sim a \), for all \( a \in S \).
- Symmetry: \( a \sim b \) if and only if \( b \sim a \), for all \( a, b \in S \).
- Transitivity: if \( a \sim b \) and \( b \sim c \) then \( a \sim c \), for all \( a, b, c \in S \). □

Now we introduce in an abstract way the basic qualities of object-oriented systems, we ignore undefinedness in these definitions. In a second step, we will show, that the handling of undefinedness is orthogonal and can be combined with any of the following equalities.

Most object-oriented languages have the concepts of references or object identifiers where a reference uniquely identifies an object. Thus it seems a natural choice to use these references for defining an equality, namely the reference quality.

**Definition 4.13 (Reference Equality)** The *reference equality* or *identity equality* is defined as follows:

1. Two values are reference equal, if they are of the same type and represent the same value.
2. Two objects are reference equal, if their object identifiers (references) are equal. □

Thus, the reference equality tests if two objects represent in fact the same object in a store. If we want to test, if two objects are identical (i.e., they represent the same value) we have two options: a shallow and a deep one:

**Definition 4.14 (Shallow Value Equality)** The *shallow value equality* or just *value equality* is defined as follows:
Chapter 4. Faithfully Representing UML/OCL

1. Two values are shallow value equal, if they are of the same type and represent the same value.

2. Two objects are shallow value equal, if they are of the same type and all attributes with value types are pairwise shallow value equal.

This definition is not recursive, hence the name shallow equality. The main idea behind the shallow equality is to compare two singular objects as values. In contrast to this, we can define the deep value equality for comparing the values of two object structures.

Definition 4.15 (Deep Value Equality) The deep value equality is defined as follows:

1. Two values are deep value equal, if they are of the same type and represent the same value.

2. Two objects are deep equal, if they are of the same type and
   a) all attributes with value types are pairwise deep value equal.
   b) all attributes with type oid (object type) are pairwise deep value equal if they objects represented by the object identifiers are deep value equal.

Summarizing, we have already three different equalities:

1. the reference equality which checks if two objects are in fact the same object,
2. the shallow value equality which compares the values of the attributes on the first level, and
3. the deep value equality which compares recursively the object structure comparing the equality of the corresponding parts.

Assuming a setting, where all values and oid are defined, i.e., the classical two-valued view, each of them is an equivalence relation on objects. It seems to be obvious that that in a universe without undefinedness definition 4.15 refines definition 4.14 and definition 4.14 refines definition 4.13. Thus, two objects, that are reference equal are also shallow equal and deep equal. But if we have undefined values and object it is not clear how these equalities relate to each other. First, in a world with undefinedness we can apply the concept of strictness to equivalence relations:

Taking undefinedness into account, e.g., values and references can be undefined, the setting gets more complicated. First we generalize the concept of equivalence relations by introducing equivalence operators.

Definition 4.16 (Equivalence Operators) An equality operator $\sim$ is a binary operator that satisfies the following properties for a state $\tau$ and a context-passing $P$:

- Quasi-reflexivity:
  
  $\vdash_{\partial} x$

  $\vdash_{\tau} x \sim x$

- Quasi-symmetry:

  $\vdash_{\tau} x \sim y$  
  $\vdash_{\tau} y \sim x$

  $\vdash_{\tau} x \vdash_{\tau} y$

- Quasi-transitivity:
  \[
  \tau \vDash \partial x \quad \tau \vDash \partial y \quad \tau \vDash \partial z \quad \tau \vDash x \sim y \quad \tau \vDash y \sim z
  \]
  \[
  \tau \vDash x \sim z
  \]

- Quasi-substitutivity:
  \[
  \tau \vDash \partial x \quad \tau \vDash \partial y \quad \tau \vDash x \sim y \quad \tau \vDash P(x)
  \]
  \[
  \tau \vDash P(y)
  \]

This definition uses the logical judgement \( \tau \vDash P \) which means that the \( \text{OCL} \) formula \( P \) is valid (i.e., evaluates to \( T \)) in context \( \tau \); this judgement is defined and discussed at length in chapter 5.

In the following, we characterize certain classes of three-valued equality operators.

**Definition 4.17 (Strong Equality)** An equality operator is called a *strong equality* if it satisfies the property:

\[
(\perp \triangleq \perp) = T.
\]

This equality operation is quasi-reflexive, quasi-symmetric, quasi-transitive and quasi-substitutive even for undefined values which explains its outstanding importance in deduction.

Applying the concept of strictness to an equality operator results in the following definition:

**Definition 4.18 (Strict Equality)** An equality operator is called *strict equality* if it evaluates to undefined whenever one of its arguments is undefined, i.e., if the following properties hold:

\[
(o \triangleq \perp) = \perp, \quad (\perp \triangleq o) = \perp, \quad \text{and} \quad (\perp \triangleq \perp) = \perp.
\]

Strictly speaking, these last definitions are merely algebraic *characterizations* and not definitions. These operation symbols were characterized by some properties, but they are obviously not defined up to isomorphism. In our context, two interpretations of the equalities into the semantic domain of universes are of particular importance: when comparing objects, we can define the equality operation via \( \text{HOL} \)-equality in the object representation in the referential or the non-referential universe (when comparing values, we compare them via \( \text{HOL} \)-equality anyway; see subsection B.4.3 for technical details).

Thus, the concept of strictness is orthogonal to the semantics of equality if the arguments are defined. Thus we can combine this with all of our previous equality variants. In principle this results in six different equalities for the object logic (see also Table 4.1). Albeit, with respect to the interpretation of the equality operators (assuming only objects in the range of the state whose reference field just contains the reference to the object in the store), strong and strict equality operators both coincide with referential equality since we have a bijective mapping between the values of an object and the object identifier. As a consequence, the advantage of a non-referential universe is its potential for efficient implementations of strict and strong equality for an executable fragment of \( \text{OCL} \).
Chapter 4. Faithfully Representing UML/OCL

<table>
<thead>
<tr>
<th></th>
<th>strict</th>
<th>strong (non-strict)</th>
</tr>
</thead>
<tbody>
<tr>
<td>referential equality</td>
<td>(o_1 \doteq o_2)</td>
<td>(o_1 \doteq o_2)</td>
</tr>
<tr>
<td>shallow value equality</td>
<td>(o_1 \doteq o_2)</td>
<td>(o_1 \doteq o_2)</td>
</tr>
<tr>
<td>deep value equality</td>
<td>(o_1 \doteq o_2)</td>
<td>(o_1 \doteq o_2)</td>
</tr>
</tbody>
</table>

Table 4.1.: Equalities in an Object-oriented Setting

<table>
<thead>
<tr>
<th>(\models)</th>
<th>(\models)</th>
<th>(\models)</th>
<th>(\models)</th>
<th>(\models)</th>
<th>(\models)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\models)</td>
<td>(\models)</td>
<td>(\models)</td>
<td>(\models)</td>
<td>(\models)</td>
<td>(\models)</td>
</tr>
</tbody>
</table>

\[
\begin{array}{c}
\tau \models o_1 = o_2 \quad \checkmark \quad \checkmark \quad \checkmark \quad \checkmark \\
\tau \models o_1 \doteq o_2 \quad \checkmark \quad \checkmark \quad \checkmark \quad \checkmark \\
\tau \models o_1 \doteq o_2 \quad \checkmark \quad \checkmark \quad \checkmark \quad \checkmark \\
\tau \models o_1 \doteq o_2 \quad \checkmark \quad \checkmark \quad \checkmark \quad \checkmark \\
\tau \models o_1 \doteq o_2 \quad \checkmark \quad \checkmark \quad \checkmark \quad \checkmark \\
\tau \models o_1 \doteq o_2 \quad \checkmark \quad \checkmark \quad \checkmark \quad \checkmark \\
\end{array}
\]

Table 4.2.: Comparing Equalities (non-referential universe)

The OCL standard defines equality as the strict equality over values \([41]\, \text{Sec. A.2.2}\), and since objects are values, but object identifiers are not distinguished from object values \([41]\, \text{Definition A.10}\) we choose the strict reference quality \(\doteq\) as the default OCL equality. In addition, we provide both referential equalities and for each class both shallow value equalities. The deep value equalities can be defined by the user within HOL-OCL at the \(\text{HOL}\)-level, if needed.

Note, besides smashed sets and unsmashed sets, we could also define smashed objects (i.e., an undefined attribute would result in an undefined object) and unsmashed objects. This would also influence the relations between the different equalities, i.e., compare Table 4.2 with Table 4.3.

Finally, we report on some strange effect of the \texttt{self.OclIsNew()}\)-operator in the non-referential universe which can be seen as a non-standard behavior: if we assume a class \(A\) with an attribute \(i\) and if we assume the natural specification of the creation-method:

\[
\text{context } A::create(val:Integer):Boolean \\
\text{post: self.OclIsNew()} \text{ and self.i = val}
\]

This operation specification is not satisfiable if the objects has already been created and exists already in the store—this makes the whole concept of \texttt{self.OclIsNew()}\)-operator quite useless in the non-referential universe interpretation of the OCL 2.0 standard.
4.15. Specifying Frame Properties

The OCL does not guarantee that an operation only modifies the path-expressions mentioned in the postcondition, i.e., it allows arbitrary relations from pre states to post states. For most applications this is too general: there must be a way to express that parts of the state do not change during a system transition, i.e., to specify the frame properties of system transition. Thus we suggest to extend OCL one to specify the frame properties explicitly:

\[ \text{Set}{} \rightarrow \text{modifiedOnly}() \]

where \( S \) is a set of object identifiers (i.e., a set of OclAny objects). This also allows recursive operations to collect the set of objects that are potentially changed within a recursive data structure. Obviously, similar to \( \text{@pre} \) the use of \( \rightarrow \text{modifiedOnly}() \) is restricted to postconditions.

The semantics for \( \rightarrow \text{modifiedOnly}() \) can be defined in HOL-OCL quite easily. First we define a predicate oidOf for accessing the object identifier of an object:

\[
\text{oidOf} \, \tau \, X \equiv (\{ x. (\tau \, x) = \text{Some}(\text{mkOclAny} \, X) \})
\]

which allows a uniform definition of \( \rightarrow \text{modifiedOnly}() \) for the referential universe and the non-referential universe:

\[
\text{X} \rightarrow \text{modifiedOnly}() \equiv \lambda (\tau, \tau'). \\
\forall i \notin (\bigcup (\text{oidOf} \, \tau)^{-1} \text{RepSet}(X(\tau, \tau'))). \tau \, i = \tau' \, i.
\]

Thus requiring \( \text{Set}{} \rightarrow \text{modifiedOnly}() \) in a postcondition of an operation allows for stating explicitly that an operation is a query in the sense of the OCL standard, i.e., the \text{isQuery} property is true. Further, constructs like

\[
\text{Set}\{x,y\} \rightarrow \text{modifiedOnly}() \text{ and } \text{Set}\{z\} \rightarrow \text{modifiedOnly}()
\]

Table 4.3.: Comparing Equalities (referential universe)
Chapter 4. Faithfully Representing **UML, OCL**

is semantically the *intersection* of the argument lists, and thus equivalent to the term `Set{}->modifiedOnly()`, i.e., “nothing is changed.”
Chapter 5.

Calculi

One contribution of HOL-OCL is the development of proof calculi for OCL. Having a conservative embedding of OCL in HOL, one might ask why this is necessary. Of course, one could always unfold the definitions, thus converting an OCL formula into a HOL expression, and try to prove the latter. However, this is not an effective proof technique, analogously to the fact that the Turing machine is not necessarily an effective means to simulate an up-to-date microprocessor. Abstract, human-readable statements on OCL formulae are both important for the human user performing interactive proof as well as automated decision- or normalization procedures for certain fragments of OCL. To this means, appropriate logical statements have to be conceived that were linked via derived inference rules (i.e., formally proven in Isabelle/HOL) to each other, such that their use in a programmed tactic process finally yields the necessary automated support for effective interactive proof.

As the OCL standard does not provide any calculi we had to develop them based on previous works [28, 20] for three valued logics and own considerations and experiences with previous interactive proof environments [11]. We extended these works to support of UML-like data-models and we also developed a tool-supported methodology. One central point of the OCL semantics presented in the in the OCL standard [41, appendix A] is the notion of local validity judgements:

\[(\tau_{\text{pre}}, \tau_{\text{post}}) \vDash Q \iff I[Q](\tau_{\text{pre}}, \tau_{\text{post}}) = \text{true}\]  

(OCL Specification [41], page A.33)

We use this as a basis of our calculi and generalize this form of judgements to:

\[(\tau \vdash P) \equiv (I[P](\tau) = \text{true}), \quad (5.1a)\]
\[(\tau \vdash_F P) \equiv (I[P](\tau) = \text{false}), \quad \text{and} \quad (5.1b)\]
\[(\tau \vdash_{\perp} P) \equiv (I[P](\tau) = \perp), \quad (5.1c)\]

As a shorthand for all three variants, we will write \(\tau \vDash_x P\) for \(x \in \{\perp, F, T\}\). When omitting the index, we assume T as default (which will turn out to be complete). Moreover, we generalize local validity judgements to a notion of global or universal judgments:

\[(\vDash_x P) \equiv (\forall \tau. \tau \vDash_x P) \quad (5.2)\]
Chapter 5. Calci

In principle, reasoning over OCL formulae can either be based on a decomposition strategy of judgements or on exploiting equivalences between formulae or judgements over them; in the latter case, the transport of knowledge of contexts is a major technical issue in reasoning over OCL\(^1\) which turns out to be even more important (i.e., more fundamental) than reasoning over definedness of subterms.

In the following sections, we will explore the potential of deduction via equivalences, in section 5.9 we will discuss a tableaux calculus that can process proof states built from judgements on a completely different way.

5.1. A Theory of Basic Judgement

Following the previous definitions, we can easily check the following link between judgements and equalities:

\[
(\tau \vdash A) = (A \tau = \text{true}) = (A \tau = \text{T}) \quad (5.3)
\]

The following analogous equations reveal that only one kind of judgements is needed, as canonical form we take the validity judgement:

\[
(X = \bot) = (\vdash \not\tau X) \\
(X = \text{F}) = (\vdash \neg X) \\
(X = \text{T}) = (\vdash X) \\
(X \tau = \bot \tau) = (\tau \vdash \not\tau X) \\
(X \tau = \text{F} \tau) = (\tau \vdash \neg X) \\
(X \tau = \text{T} \tau) = (\tau \vdash X) \quad (5.4a-e)
\]

Applied from right to left, these theorems reveal also the character of judgements as rewrite-rules that can be used by automatic rewriting procedures. From these equalities, the base cases for judgements follow directly:

\[
\neg(\vdash \bot) \quad (5.5a) \\
\neg(\vdash \text{F}) \quad (5.5b) \\
\vdash \text{T} \quad (5.5c) \\
\neg(\tau \vdash \bot) \quad (5.5d) \\
\neg(\tau \vdash \text{F}) \quad (5.5e) \\
\tau \vdash \text{T} \quad (5.5f)
\]

A last fundamental fact of judgements is related to the three-valuedness of OCL, i.e., non quatrium datur:

\[
(\tau \vdash A) \lor (\tau \vdash \neg A) \lor (\tau \vdash \not\tau A) \quad (5.6)
\]

With this fact, a defined formula can be converted into formulae which are true or which are false; this gives rise for six corresponding case-split lemmas.

\(^1\)there is a notable similarity to labelled deduction systems [16, 51].
5.2. Basic Equivalences and Congruences

In principle, we distinguish four equivalences over OCL formulae; one of them is already a congruence.

**UC:** Universal (Formula) Congruence. This congruence requires that two formulae \( A \) and \( B \), both of type \( \text{Boolean} \), agree in all contexts \( \tau \) and in all three truth values of type \( \text{Boolean} \). They have the form

\[
A = B \quad \text{or} \quad A_1 = B_1 \quad \cdots \quad A_n = B_n \quad A_{n+1} = B_{n+1}.
\]

**LE:** Local (Formula) Equivalence. This equivalence requires that two formulae agree on all three truth values of \( \text{Boolean} \) in a specific context \( \tau \): They have the form

\[
A \tau = B \tau \quad \text{or} \quad H_1 \quad \cdots \quad H_n \quad A_{n+1} \tau = B_{n+1} \tau.
\]

Premises can have the form \( A \tau = B \tau \) or instances of this scheme such as \( \tau \models x \ A \).

**UJE:** Universal Judgement Equivalence. This equivalence requires that for all contexts \( \tau \) agree on one value \( \tau \) from \( \text{Boolean} \). They have the form \( \models x \ A = \models x \ A \) or horn-clauses over them.

**LJE:** Local Judgement Equivalence. This equivalence requires that two formulae agree on a specific truth value \( \tau \) of type \( \text{Boolean} \) in a specific context \( \tau \): \( \tau \models x \ A = \tau \models x \ A \) or horn-clauses over them.

Since all three possible kinds of judgements \( \models x \ A \) (universal) respectively \( \tau \models x \ A \) (local) called validity, invalidity and undefinedness, can be converted into each other, we can choose just one of them, validity, as representative. We will abbreviate \( \models \tau \ A \) or \( \tau \models x \ A \) by \( \models A \) or \( \models A \) resp.

The **UJE**-format is only of notational interest: it is not possible to build a complete calculus using only **UJE**-rules. While the rule:

\[
\frac{\models \partial A \quad \models \partial B}{(\models A \land B) = ((\models A) \land (\models B))}
\]  

is in fact valid (due to distribution of universal quantification over \( \land \)), but even an analogue version for the OCL disjunction, however, does not hold.

The **LE**-format, however, is flexible enough to build both practical relevant conversion calculi as well as (relative) complete calculi. Consider:

\[
\frac{\tau \models x \ A \quad \tau \models x \ B}{(\tau \models x \ A \land B) = ((\tau \models x \ A) \land (\tau \models x \ B))}
\]  

Since all three possible kinds of judgements \( \models x \ A \) (universal) respectively \( \tau \models x \ A \) (local) called validity, invalidity and undefinedness, can be converted into each other, we can choose just one of them, validity, as representative. We will abbreviate \( \models \tau \ A \) or \( \tau \models x \ A \) by \( \models A \) or \( \models A \) resp.
Chapter 5. Calculi

as a propositional equivalence or
\[
(\tau \models \forall x \in S. A \land B) = (\forall x. (\tau \models x \in S) \rightarrow (\tau \models A)) \land (\forall x. (\tau \models x \in S) \rightarrow (\tau \models B))
\]  
(5.8)

as a predicative equivalence.

Since judgements are propositional and LJE’s can be decomposed into implications from left-to-right and from right-to-left, there is another line to automated reasoning over OCL-formulae: they can be turned into a tableau calculus (the local judgement tableaux calculus, LTC, see section 5.9).

Unfortunately, there is a trade-off between completeness of the various calculi based on these equivalences and deductive efficiency. UC is the only congruence that can be directly processed by Isabelle’s simplifier; normalizations in UC can be computed relatively efficiently. While UC comprises several thousands of rules (among them, the strictness and computational rules of operators) it does not form a complete calculus for principle reasons: Some properties in OCL are inherently context dependent, in particular when referring to paths. Others are difficult to formalize in the form of the straight-jacket of a universal congruence. On the other end of the spectrum, since local judgements are simply propositions, they are extremely flexible. When extending LJE’s to equivalences over propositional (predicative) formulae, it is not difficult at all to convert them into a fairly abstract but still provably complete calculus with analytic rules (rules whose application yield to an equivalent transformation of the proofstate. Their use is “safe” in the sense that no logical content is lost.)

With respect to LTC it is well-known that the complexity for tableaux-based reasoning in Kleene-Logic is unfavorably high [19]. However, the logic is only one little fragment of the overall problem of building decision procedures in OCL. Most operations are strict, and from the data-invariants, definedness of many literals can be inferred, such that large fragments of the language are in fact two-valued. Furthermore, we do not only have the logic but also a rich datatype theory with collection types which give the overall language a flavour in its own. As consequence, a good combination of all these types of calculi is a prerequisite for automated reasoning for practically relevant reasoning work in OCL.

5.3. Reasoning on Context-Passing Predicate \( \text{cp} \)

In the following, we discuss the first side-calculus, the reasoning over context-passingness or \( \text{cp} \). Revising the definition

\[
\text{cp} :: (V_\tau(\alpha) \Rightarrow V_\tau(\beta)) \Rightarrow \text{bool}
\]

\[
\text{cp}(P) \equiv (\exists f. \forall X\tau. P \ X \ X = f(X\tau)\tau)
\]

(5.9)  
(5.10)

presented in section 4.3, one might wonder why this quite arcane definition is so pivotal for reasoning in OCL. An answer can be drawn from the following lemma:

\[
A \tau = B \tau \quad \text{cp} \ P
\]

\[
P \ A \tau = P \ B \tau
\]

(5.10)
5.4. Reasoning on Undefinedness and Definedness

Definedness and undefinedness are indeed opposite concepts in OCL, i.e., they satisfy the “classical” rule for all $X$ in all types:

$$\tau \vdash \not\emptyset X \lor \tau \vdash \not\emptyset X$$

(5.16)
Chapter 5. Calculi

This gives, of course, rise for case-split techniques that can be applied automatically in UJE or LJE calculi. However, since OCL is biased towards strict operations, the use of undefinedness in deduction is easier than its counterpart.

Undednedness can be propagated throughout a proof state via forward reasoning and exploited via rewriting. The forward reasoning part is covered by rules like:

\[
\tau \models \emptyset X \quad \text{cp} \quad P
\]
\[
P X \tau = P \perp \tau
\] (5.33)

and several variants used for technical purposes. Having replaced some term \(X\) by \(\perp\), strictness rules like \(f \perp Y\) or \(f Y \perp\) can reduce the size of subgoals drastically.

We now focus on the far more involved treatment of definedness. The core of reasoning over definedness is in fact representable in an UC calculus. It is summarized in Equation 5.2(a). This rule set contains also a class of rules for "strict standard operations \(f\). With this set of operations, we refer to operations that had been defined by constant definitions of the form:

\[
f \equiv \text{lift}_2(\text{strictify}(\lambda x. \text{strictify}(\lambda y. g \ x y)))
\] (5.34)

As in the case of the generation of cp-inference rules, we exploit the combinator-style definitions of the standard operators here and generate this type of rules in pre-computation steps once and for all.

The power and the main drawback of this type of UC-based calculus stems from the rules listed in Equation 5.2(b). They result in the generation of numerous case splits, which may be inappropriate in most deductions: if we know, that all variables in a subgoal are defined (and this is an important special case that we can achieve by initial case-splits done once and for all), simple conditional rules leading to direct backward-chaining are sufficient.

By the way, this strong definedness calculus can be extended to quantifiers as follows\(^2\):

\[
\text{cp} \quad P
\]
\[
\partial(\forall x \in S, P x) = \partial S \land ((\exists x \in S, (\neg P x)) \lor (\forall x \in S, (\partial P x)))
\] (5.35)

To overcome this drawback, we derived the following alternative rule-set listed in Equation 5.2(c). It reduces the burden of applicability to the question, if the definedness of a term can be derived. We will discuss in section 5.10 how this can be assured by prior normal form computations. By the way, the \(\tau \models \partial x\)-part in the last rule is strictly speaking redundant (as we will see when we discuss the Set-theory in more detail), but facilitates the establishment of \(\tau \models \partial P x\) since this additional assumption will be used if \(x\) occurs in (the instance of) \(P x\).

\(^2\)The analogous rule for existential quantification is omitted here.
### 5.4. Reasoning on Undefinedness and Definedness

#### (a) Core Definedness Rules

\[
\begin{align*}
\partial F &= T \\
\partial \bot &= F \\
\partial (\neg X) &= \partial X \\
\partial (X \land \partial X) &= T \\
\partial X \triangleq Y &= T \\
\partial f X &= \partial X \\
\end{align*}
\]

(5.17) \hspace{1cm} (5.18) \hspace{1cm} (5.19) \hspace{1cm} (5.20) \hspace{1cm} (5.21) \hspace{1cm} (5.22) \hspace{1cm} (5.23)

for all strict standard operations \(f\)

#### (b) Strong Definedness Rules

\[
\begin{align*}
\partial (\text{if } X \text{ then } Y \text{ else } Z \text{ endif}) &= \partial X \land (X \land \partial Y \lor \neg X \land \partial Z) \\
\partial (X \land Y) &= \partial X \land \partial Y \lor \partial X \land \neg X \lor \partial Y \land \neg Y \\
\partial (X \rightarrow Y) &= \partial X \land \partial Y \lor \partial X \land \neg X \lor \partial Y \land \neg Y \\
\partial (X \lor Y) &= \partial X \land \partial Y \lor \partial X \land \neg X \lor \partial Y \land Y \\
\end{align*}
\]

(5.24) \hspace{1cm} (5.25) \hspace{1cm} (5.26) \hspace{1cm} (5.27)

#### (c) Weak Definedness Rules

\[
\begin{align*}
\tau \models \partial X & \quad \tau \models \partial Y \quad \tau \models \partial Z \\
\tau \models \partial (\text{if } X \text{ then } Y \text{ else } Z \text{ endif}) \\
\tau \models \partial X & \quad \tau \models \partial Y \\
\tau \models \partial (X \rightarrow Y) \\
\tau \models \partial X & \quad \tau \models \partial Y \\
\tau \models \partial (X \lor Y) \\
\tau \models \partial (X \land Y) \\
\end{align*}
\]

(5.28) \hspace{1cm} (5.29) \hspace{1cm} (5.30) \hspace{1cm} (5.31)

\[\text{cp } P \]

\[
\begin{align*}
(\tau \models \partial (\forall x \in S \cdot Px)) &= (\tau \models \partial S \land ((\exists x. \tau \models x \in S \land \neg \tau \models Px) \\
&\lor (\forall x. \tau \models \partial x \land \tau \models x \in S \rightarrow \tau \models \partial Px)))
\end{align*}
\]

(5.32)

**Table 5.2.** The Definedness Calculi
Chapter 5. Calculi

5.5. Logical Bridges Between UC, LE, LJE, and LTC

The following characterizations between statements in these logical formats hold:

\[ (A = B) = (\forall \tau. A \tau = B \tau) \] (5.36)

\[ (A = B) = \left( (\forall \tau. (\tau \models A) = (\tau \models B)) \land (\forall \tau. (\tau \models \neg A) = (\tau \models \neg B)) \right) \] (5.37)

\[ (A \tau = B \tau) = \left( (\tau \models A) = (\tau \models B) \right) \land (\forall \tau. (\tau \models \neg A) = (\tau \models \neg B)) \] (5.38)

\[ (A \tau = B \tau) = \left( (\tau \models A) = (\tau \models B) \right) \land (\forall \tau. (\tau \models \neg A) = (\tau \models \neg B)) \] (5.39)

\[ (A \models A = (\tau \models B)) \land ((\tau \models \neg A) = (\tau \models \neg B)) \] (5.40)

\[ (\tau \models (a \triangleq b)) = (a \tau = b \tau) \] (5.41)

The two variants Equation 5.38 and Equation 5.40 implicitly exploit Equation 5.6: If two formulae agree in two truth-values, they have also to agree on the third. There is a third variant that is omitted here.

The characterization Equation 5.41 justifies an own tableaux calculus on the basis of local judgements. This rule is the “entry point” into section 5.9.

The rule Equation 5.42 also shows the connection of strong equality to local formula equivalence LE.

5.6. The Logics

5.6.1. Reasoning over Strong and Strict Equality

The strong equality satisfies the usual properties except the Leipnitz rule (substitutivity); instead, the slightly weaker form Equation 5.42 of substitutivity (for context passing contexts P) holds. This side-constraint is not surprising, since since Equation 5.42 shown in section 5.5 we know that strong equality and global equivalence are semantically equivalent.

\[ \tau \models a \triangleq a \] (5.42)

\[ \tau \models a \triangleq b \]

\[ \tau \models b \triangleq a \] (5.42)

\[ \tau \models a \triangleq b \quad \tau \models b \triangleq c \]

\[ \tau \models a \triangleq c \] (5.42)

\[ \tau \models a \triangleq b \quad \tau \models P a \quad cp \]

\[ \tau \models P b \] (5.42)
The following lemmas show that strict equality is indeed convertible into strong equality and is a stronger equality:

\[ \tau \vDash \partial a \quad \tau \vDash \partial b \]

\[ (a \equiv b)\tau = (a \triangleq b)\tau \quad (5.42) \]

\[ \tau \vDash a \triangleq b \]

\[ \tau \vDash a \triangleq b \quad (5.42) \]

5.6.2. Core-Logic (Boolean)

With core-logic of OCL we refer to the sub-language consisting of the logical connectives \( \neg \), \( \land \), \( \lor \), etc., which we also call the propositional fragment of OCL (although the underlying semantics is strictly speaking not propositional but Strong Kleene Logic SKL). The core-logic is contained in subsection B.4.2. Besides the computational rules like \( \bot \land F = F \), the core-logic enjoys a lattice-like structure with the rules shown in Equation 5.3(a).

In Equation 5.3(b), the rules are shown that deal with “logical reasoning” related to implication. Note, however, that the UC-rules do not form a complete calculus. The problem is (obviously) hidden in the only conditional rule, which has to be rephrased as LE-rule to achieve completeness. Unfortunately, this conditional rule corresponds to “assumption” and is therefore particularly vital in deduction. The Boolean case-split rule in Equation 5.3(c) is interesting for automated reasoning. Consequent case-splits over all Boolean variables yields a proof procedures of sufficient power, as can be seen for many facts in the basic library.

5.6.3. Set Theory and Logics

Set theory is the theory of membership \( x \in S \) on the one hand and set constructions like comprehensions (corresponding to the \( \rightarrow \text{select}() \)-construct in OCL) on the other.

In OCL, we have a typed form of a set theory which rules out, for example, Russel’s Paradox. With respect to typedness, OCL’s set theory is more related to HOL’s set theory, but more distant to ZF. Undefinedness, on the other hand, is a distinguishing feature of OCL’s set theory: Inclusion of elements in a set may result in an undefined set or in a set, that just contains undefined elements. As mentioned in subsection 4.7.1, we opt for a smashed sets semantics; the OCL standard is not clear with this respect.

On the deduction level, smashed semantics boils down to the following rule:

\[ \tau \vDash x \in S \]

\[ (\tau \vDash \emptyset x) \land (\tau \vDash \emptyset S) \quad (5.61) \]

This has the consequence, that whenever we eliminate a universal or existential OCL quantification, we know that the variable over which a quantifier ranges is defined. In itself, this is also useful to deduce that the body of a quantifier is defined—which it will usually not.
Chapter 5. Calculi

(a) Lattice

\[
\begin{align*}
F \land X &= F \quad (5.43) \\
T \land X &= X \quad (5.44) \\
T \lor X &= T \quad (5.45) \\
F \lor X &= X \quad (5.46) \\
X \op X &= X \quad (5.47) \\
X \op (Y \land Z) &= (X \op Y) \land (X \op Z) \quad (5.49) \\
\end{align*}
\]

where \( \op \in \{ \land, \lor \} \) (5.50)

\[
\begin{align*}
\neg (\neg X) &= X \quad (5.51) \\
(X \lor Y) \land Z &= (X \land Z) \lor (Y \land Z) \quad (5.52) \\
Z \land (X \lor Y) &= (Z \land X) \lor (Z \land Y) \quad (5.53) \\
(X \land Y) \lor Z &= (X \lor Z) \land (Y \lor Z) \quad (5.54) \\
Z \lor (X \land Y) &= (Z \lor X) \land (Z \lor Y) \quad (5.55) \\
\neg (X \lor Y) &= \neg (X) \lor \neg (Y) \quad (5.57) \\
\neg (X \land Y) &= \neg (X) \land \neg (Y) \quad (5.58)
\end{align*}
\]

(b) Logic

\[
\begin{align*}
X \rightarrow F &= \neg X \quad (5.59a) \\
F \rightarrow X &= T \quad (5.59b) \\
\partial(X) &= T \quad (5.59c) \\
(X \rightarrow X) &= T \\
(X \rightarrow (Y \land Z)) &= (X \rightarrow Y) \land (X \rightarrow Z) \quad (5.59d) \\
(X \rightarrow (Y \lor Z)) &= (X \rightarrow Y) \lor (X \rightarrow Z) \quad (5.59e) \\
(X \land Y) \rightarrow Z &= X \rightarrow (Y \rightarrow Z) \quad (5.59f) \\
(X \lor Y) \rightarrow Z &= (X \rightarrow Z) \land (Y \rightarrow Z) \quad (5.59g) \\
X \rightarrow (Y \rightarrow Z) &= Y \rightarrow (X \rightarrow Z) \quad (5.59h)
\end{align*}
\]

(c) Boolean Case-Split

\[
\begin{align*}
P \perp = P' \perp & \quad P \top = P' \top & \quad P \bot = P' \bot & \quad \cp(P) = \cp(P') \\
\hline
P \rightarrow X &= P' \rightarrow X \quad (5.60)
\end{align*}
\]

Table 5.3: The UCL Core-Calculus ("Propositional Calculus")
Further, we allow sets to be infinite. This generalization has the advantage, that general Sets can be used to represent the syntactic category of “types” in the standard as “characteristic sets” in HOL-OCL and enables the possibility to reason over them. From the pragmatics point of view, this also allows for quantifications of sets of “values” in the sense of OCL 2.0. For example, it is possible in HOL-OCL (see section 4.12 for details) to express the commutativity law on Integers inside OCL as follows:

\[
\text{Integer.typeSetOf()} \rightarrow \forall (x, y \mid \text{not } x. \text{oclIsUndefined()} \\
\text{and} \\
\text{not } y. \text{oclIsUndefined()} \\
\text{implies} \\
x + y = y + x)
\]

In an infinite set theory, each OCL type can be assigned to a characteristic set. Based on the characteristic sets for the base types Integer, Real, Boolean, String, we have defined set constructors \( \text{Set} : \alpha :: \perp \text{Set} \Rightarrow \alpha \text{ Set Set} \) that mimick the semantic effect of type constructors. The construction assures that characteristic sets are always defined objects \( \partial \text{Integer} = \mathbb{T}, \ldots, \partial X = \mathbb{T} \Rightarrow \partial \text{Set}(X) = \mathbb{T} \) etc.

Infiniteness of a set in the OCL can be naturally expressed by testing if the cardinality of the set is defined:

\[
\partial ||\text{Boolean}|| = \mathbb{T} \quad \partial ||\text{Integer}|| = \mathbb{F} \tag{5.62}
\]

In contrary, finiteness of sets paves the way for an induction-scheme in HOL-OCL.

In the following, we discuss the core of the collection theories at the example of the set theory. We ommit the type constraints from this presentation which enforce that the overloaded symbols are in fact interpreted as operations on sets.

Quantifiers and set constructors in OCL have a highly operational character with respect to undefinedness; in the standard, quantifiers were defined via iterators, hence fold-like constructs which also reflect the behaviour in case of undefinedness. This represents a particular challenge for deduction; on the other hand, similar languages like Spec# or VDM have the same characterizations, too, and the problem needs to be resolved for the forthcoming generation of “light-weight”-specification languages that are semantically “operation-like” and therefore closer to programming languages.

The combinator-based definition:

\[
\forall x \in S, P x \equiv \lambda x. \text{if def}(S \tau) \text{then } \forall x \in \text{set'}(\text{RepSequence}(S \tau)), P(\text{lift}_0 x) \tau = (\text{true}_\tau) \text{then } \text{true}_\tau \\
\text{else if } \exists x \in \text{set'}(\text{RepSequence}(S \tau)), P(\text{lift}_0 x) \tau = (\text{false}_\tau) \text{then } \text{false}_\tau \\
\text{else } \perp
\]

turns out to be equivalent (for the finite case) to the operational formulation of the
Chapter 5. Calculi

standard:

\[
\tau \models \partial \| S \|
\]

\[
(\forall x \in S. P \, x) \tau = (S^{-} \text{iterate}(x; y = T \,(P \, x) \land y)) \tau
\] (5.63)

Of course, we are interested for the general case of infinite sets. As general UC-rules, we have:

\[
\forall x \in \bot. P \, x = \bot
\] (5.64)

\[
\exists x \in \bot. P \, x = \bot
\] (5.65)

\[
\forall x \in \emptyset. P \, x = T
\] (5.66)

\[
\exists x \in \emptyset. P \, x = F
\] (5.67)

\[
\tau \models \partial X \quad \tau \models \partial a \quad \text{cp} \ P
\]

\[
(\forall x \in X^{-} \text{including}(a). P \, x) \tau = ((P \, a) \land (\forall x \in X. P \, x)) \tau
\] (5.68)

\[
\tau \models \partial X \quad \tau \models \partial Y
\]

\[
(\forall x \in (X \cup Y). P \, x) \tau = ((\forall x \in X. P \, x) \land (\forall x \in Y. P \, x)) \tau
\] (5.69)

The latter two rules allow for the elimination of quantifications over known finite sets via computation.

Besides, there is a tableau calculus for quantifier elimination can be directly derived from the rules in Equation 5.4(b).

The core of OCL set theory is the relation between the element-hood and the set comprehension (_ ->select( _ | _)) and the relation to equality, i.e., a form of set
5.7. Arithmetic Computational Rules

An important source of deduction is computation. Computation is needed when \( \tau \models 3 + 5 \neq 4 \) is refuted. So far, we have only used declarative concepts to introduce numbers; the question arises how this can be used for computation, and even: how can this be used fairly efficiently in deduction.

This problem is by no means new and deeply intertwined with the existing solution in Isabelle/HOL. In the HOL library, a type bin for binary two’s complement representation has been introduced—by classical, conservative means. Now, the Isabelle parser is configured to parse a literal like 3 to bitstring representation representing \((101)_2\). Further, an axiomatic class num is defined providing a function declaration numberOf :: bin \( \Rightarrow \alpha::\text{num} \) that can be overloaded for each type declared to be an instance of class num. Thus, for new datatypes, just a new function is defined that converts a bitstring representation to this new type. In the library, such a conversion has been provided, for example, for int. Based on this definitions, suitable rules have been derived that perform the integer operations like addition on the two’s complement representation directly; these rules can be directly processed by the simplifier.

With respect to the types Integer_\(\tau\), Real_\(\tau\) and String_\(\tau\), we can proceed analogously. For example, after declaring Integer_\(\tau\) to be an instance of num, we provide the following definition numberOf for the representation conversion:

\[
(\text{numberOf} :: \text{bin} \Rightarrow \text{Integer}_\(\tau\)) b \equiv \text{lift}_0((\text{numberOf} :: \text{bin} \Rightarrow \text{int}) b)
\]

This means, that the “new” numberOf with type bin \( \Rightarrow \text{Integer}_\(\tau\) is the context-lifted, \(\bot\)-lifted version of the “old” numberOf on integers. From this definition, among others,
the following facts follow:

\[ \partial \text{numberOf}(a) = T \]  \hspace{1cm} (5.75)

\[ \text{numberOf}(a) + \text{numberOf}(b) = \text{numberOf}(a + b) \] \hspace{1cm} (5.76)

\[ \text{numberOf}(a) \cdot \text{numberOf}(b) = \text{numberOf}(a \cdot b) \] \hspace{1cm} (5.77)

\[ \neg \text{iszero}(\text{numberOf}(a - 2b)) \]

\[ \frac{((\text{numberOf}(a) \triangleq (\text{numberOf}(b)))) = F} {\text{ numberOf}(a - 2b))} \] \hspace{1cm} (5.78)

Thus, besides definedness-related computations (“all values are defined”), computations in OCL were mapped directly to computations in the underlying meta-logic HOL. This setup enables the standard simplifier of Isabelle to refute judgements like

\[ \tau \vdash 3 + 2 \equiv 7 \] \hspace{1cm} (5.79)

fully automatic, i.e., without user interaction.

5.8. Converting OCL to HOL

For a fragment of OCL that is built for expressions that are always defined, the following “conversion” of OCL formula into standard HOL formulae over local judgements equivalences \( \text{LJE} \) are possible. The propositional part of the translation is described in Equation 5.4(a), the predicative part in Equation 5.4(b). The rules for the other collection types are accordingly.

5.9. The Judgement Tableaux Calculus LTC

The conversion technique discussed in section 5.8 requires reasoning on side-conditions such as \( \text{cp} P \) or definedness \( \partial X \). The question arises, if this can be avoided when performing a logical decomposition of the OCL formulae directly.

The tableaux methodology is one of the most popular approaches to design and implement proof-procedures. While originally geared towards first-order theorem proving, in particular for non-clausal formulae accommodating equality, renewed research activity is being devoted to investigating tableaux systems for intuitionistic, modal, temporal and many-valued logics, as well as for new families of logics, such as non-monotonic and sub-structural logics. Many of these recent approaches are based on a special labeling technique on the level of judgments, called labeled deduction [16, 51]. Of course, labeling can also be embedded into a higher-order, classical meta-logic. Being a special case of a many-valued logic, tableaux calculi for SKL based on labeled deduction have been extensively studied [29, 20, 19]. In this section, we present an experimental tableaux calculus for the predicative fragment of OCL, i.e., for SKL roughly following [29]. It is designed to be processed by Isabelle’s generic proof procedures, which are geared towards natural deduction.
5.10. Towards Automated Deduction in HOL-OCL

(a) Propositional Conversion

\[
\begin{align*}
\tau \models \partial A & \quad \Rightarrow \quad (\tau \models \neg A) = (\neg \tau \models A) \\
\tau \models \partial A & \quad \tau \models \partial B \\
\tau \models A \land B & \quad \Rightarrow \quad (\tau \models \tau \models A \land \tau \models B) \\
\tau \models A \lor B & \quad \Rightarrow \quad (\tau \models \tau \models A \lor \tau \models B) \\
\tau \models A \rightarrow B & \quad \Rightarrow \quad (\tau \models \tau \models A \rightarrow \tau \models B)
\end{align*}
\]

(5.80) (5.81) (5.82) (5.83)

(b) Predicative Conversion

\[
\begin{align*}
\tau \models \partial (S :: (\beta :: \text{bot}) \text{Set}_\tau \text{ cp } P & \quad \Rightarrow \quad (\forall x. \tau \models x \in S \rightarrow \tau \models P x) \\
\tau \models \partial (S :: (\beta :: \text{bot}) \text{ Set}_\tau \text{ cp } P & \quad \Rightarrow \quad (\exists x. \tau \models x \in S \land \tau \models (P x))
\end{align*}
\]

(5.84) (5.85)

Table 5.4.: The OCL to HOL Conversion Rules

Tableau proofs may be viewed as trees where the nodes are lists of formulae. Tableau rules extend the leaves of a tree by a new subtree, i.e., by adding leaves below, where the latter case is called “branching” and is used for case splits. Classical tableau rules are purely analytic: each rule captures the full logical content of the expanded connective. Backtracking from a rule application is never necessary. The goal of the process is to construct trees in a deterministic manner, where the leaves can eventually all be detected as “closed,” i.e., a logical contradiction is detected. This last step, however, may be combined with the non-deterministic search for a substitution making this contradiction possible.

The LTC appears in Table 5.5(a).

5.10. Towards Automated Deduction in HOL-OCL

In the current HOL-OCL distribution, only two major OCL-related proof procedures have been implemented:

- OCL_hypsubst
- OCL_subst

They mimic the Isabelle standard tactics hypsubst and subst and serve as an abstract interface to the various rules that express local congruences, strict and strong
Chapter 5. Calculi

(a) Definedness Introduction and Elimination

\[
\begin{array}{c}
\tau \models \partial(A) & \forall \tau \models \partial(A) \\
\forall \tau \models \neg \partial(A) & \forall \tau \models \neg \partial(A)
\end{array}
\]

(b) Negation

\[
\begin{array}{c}
\tau \models \neg \neg A & \forall \tau \models \neg \neg A \\
\forall \tau \models A & \forall \tau \models A
\end{array}
\]

(c) Conjunction Introduction and Elimination

\[
\begin{array}{c}
\tau \models A \land B & \forall \tau \models A \land B \\
\forall \tau \models \neg (A \land B) & \forall \tau \models \neg (A \land B)
\end{array}
\]

(d) Contradictions

\[
\begin{array}{c}
\tau \models A \land \neg A & \forall \tau \models A \land \neg A \\
\forall \tau \models A \land \neg A & \forall \tau \models A \land \neg A
\end{array}
\]

Table 5.5.: The Core of \text{LTC}
5.10. Towards Automated Deduction in HOL-OCL

For the moment, this tactic setup allows for a step-by-step reasoning using the rules of the logic and UC-rules (including computational rules) in the Isabelle simplifier. Provided that sufficient information on the definedness of free variables is available in a proof state, this enables a conversion to HOL formulae with the rules discussed in section 5.8 possible. A converted formula can be treated by the standard Isabelle proof procedures like safe_tac, blast_tac and auto_tac possibly intertwined with OCL_hypsubst. This covers to a certain extent logical reason automatically.

However, the situation is clearly not satisfactory for larger, application oriented proof projects in OCL so far. Here is a list of the most painful shortcomings when comparing it with proofs in “pure” Isabelle/HOL:

- The library on datatypes and on datatype-oriented rules is far from being sufficiently developed.
- An arithmetic decision procedure such as arith_tac is missing.
- All rules of the LE-format are not usable by the simplifier. Since the complete core calculus and many datatype-oriented rules are in this format, the proof engineer is limited to elementary proof techniques excluding the simplifier whenever these rules are involved in a proof.
- Rules of the LE-format are also excluded from the classical reasoner, i.e., the fast_tac, blast_tac and auto_tac procedures.
- A combined automatic tactic integrating all these local procedures like the auto_tac-procedure.

Partly, the situation is comparable to HOL 10 years ago—and a fair comparison to similar logical languages has to take into account that the development of HOL libraries and proof procedures needed this time. For OCL the development of proof procedures and, more critical, the technical support of formal methods based on OCL is still at the beginning. The latter will have to cope with path-expressions, modifies-clauses, and refinement-like situations.

In the following, we will summarize our ideas about potential future tactics to reason over OCL automatically.

With respect to arithmetic, besides a step-by-step reasoning, only the following paths to use automated procedures seem to be viable: defined arithmetic terms have to be converted (by unfolding semantic combinators and blowing away the cascades of definedness-conditions) into pure HOL arithmetic formulae and reuse the existing procedure (the adaption approach). Alternatively, arith_tac must be rewritten to cope with definedness issues (the re-engineering approach).

With respect to rewriting, we see (besides the not very attractive re-engineering approach) the following techniques to adapt to existing Isabelle technology:

**Proof-object transformation.** Since one can instantiate the simplifier with new equalities obeying the Leipnitz rule, one can run it in an unsafe-mode without

equalities and congruences hidden in local judgements as pointed out in section 5.1.
checking the cp-side conditions. Proof-objects generated in an unsafe mode could be extended to “full” proof objects where the missing parts are reconstructed. It remains to be explored how costly this approach would be (in development time as well as runtime; previous experience (blast_tac) suggests that at least the runtime costs are insignificant).

Making context-passing explicit. One can transform proof-states and rules in a format where context-passingness is encoded directly at all positions in a term. As a consequence, the simplifier can process the transformed rules directly. Additionally to the conversion tactics that perform this term-transformation in forward and backward proof, the major changes for this technique boil down to the management of transformed and un-transformed rule-sets used by the simplifier and auto_tac.

It is worth to present the letter option a bit more in detail:

\[
\text{cp } P \\
\frac{P \times \tau = P(\text{lift}_o(X \tau)) \tau}{P \times \tau}
\] (5.93)

One can also annotate any redex $X$ explicitly with the context it is referring to. This leads to a linear blowup on the size of terms. On such redeces, LE-rules match directly and can be processed by the simplifier. To enable the simplification of assumptions of a rewriting rule, this technique requires a pre-computation on all rules which should be hidden from the user.

Depending on the decision for the simplification, it is either possible to adopt tableaux calculi for the classical reasoning (however, first experiments showed that the built-in strategies are not compatible with three-valued logic) or to convert a proof-goal to a HOL-formula to be processed by standard classical reasoning.

At present, we consider the latter strategy for an automatic setup as more promising. Thus, an auto_tac could proceed as follows:

1. general logical simplification and normalization with the UC calculi,

2. performing a definedness case-split on all free variables in a subgoal, which are not already known to be defined or undefined. Moreover, for all potentially undefined subterms (like $1 \text{ div } 0$), a suitable case-split is generated,

3. using OCL_hypsubst, all $\bot$ were propagated and simplified,

4. a conversion to HOL-formulae is performed (following the rules in 5.8), extended by rules converting equalities on collection types, and simplifying path expressions along their structure,

5. making cp explicit (see above),

6. and apply standard auto_tac.
We call the first three phases the *splintering* of an OCL formula, the resulting sub-goals are the *splinters*. In principle, there may be exponential many splinters depending on the number of free variables in the formula. Variables bound by OCL quantifier are implicitly defined due to smashed collection semantics. However, due to the fact that expressions are usually built from strict operators, this growth is unlikely in practice. The subsequent phases will deeply interact with the datatype specific rules of the library.
Chapter 5. Calculi
Chapter 6.

The HOL-OCL System Architecture

6.1. An Architectural Overview

HOL-OCL is integrated into a framework [10], which among others provides a model repository, su4sml, written in SML. For a quick overview over main system components of HOL-OCL see Figure 6.1. HOL-OCL is based on the SML interface of Isabelle/HOL and the UML/OCL model repository. As front-end, HOL-OCL provides a special instance of ProofGeneral [5] and a LaTeX based documentation generation.

In this chapter, we will briefly present the main components of the HOL-OCL core system, namely:

- our datatype package, or encoder, which encodes UML/OCL models into HOL-OCL, i.e., from a user’s perspective it provides the XMI import facilities.
- the HOL-OCL library which provides the core theorems needed for verification and also provides a formal semantics for OCL.
- the theory morpher which derives many of the core OCL theorems by “lifting” them based on the corresponding theorems already proven for HOL.

As further background, we will also give a short introduction of the model repository su4sml.

6.2. The Model Repository: su4sml

The Model Repository su4sml [10] provides an interface to models expressed in the UML core (mainly class diagrams and state machines) and OCL. OCL expressions naturally translate into an abstract datatype in SML, as shown in Listing 6.1 and Listing 6.2. This abstract datatype is modeled closely following the standard OCL 2.0 metamodel. In addition to these datatype definitions, the repository structure defines a couple of normalization functions, for example for converting association ends into attributes with corresponding type, together with an invariant expressing the cardinality constraint.

For class models (see Listing 6.3), su4sml resembles the tree structure given by the “containment hierarchy.” For example, a class contains attributes, operations, or
Chapter 6. The HOL-OCL System Architecture

Figure 6.1.: Overview of the HOL-OCL architecture

Listing 6.1: su4sml: Representing OCL types

```sml
signature REP_OCL_TYPE = sig
  type Path = string list
  datatype OclType = Integer | Real | String | Boolean (* Primitive Types *)
                   | OclAny | OclVoid
                   | Set of OclType | Sequence of OclType
                   | OrderedSet of OclType | Bag of OclType
                   | Collection of OclType
                   | Classifier of Path (* user-defined classifiers *)
                   | DummyT (* dummy type for untyped expressions *)
end
```
6.2. The Model Repository: su4sml

Listing 6.2: su4sml: Representing OCL expressions

signature REP_OCL_TERM = sig
include REP_OCL_TYPE

datatype OclTerm =
  | Literal of string * OclType (* literal with type *)
  | CollectionLiteral of CollectionPart list * OclType (* content with type *)
  | If of OclTerm * OclType (* condition *)
      * OclTerm * OclType (* then *)
      * OclTerm * OclType (* else *)
      * OclType (* result type *)
  | AssociationEndCall of OclTerm * OclType (* source *)
      * Path (* assoc.-enc *)
      * OclType (* result type *)
  | AttributeCall of OclTerm * OclType (* source *)
      * Path (* attribute *)
      * OclType (* result type *)
  | OperationCall of OclTerm * OclType (* source *)
      * Path (* operation *)
      * (OclTerm * OclType) list (* parameters *)
      * OclType (* result type *)
  | OperationWithType of OclTerm * OclType (* source *)
      * string * OclType (* type parameter *)
      * OclType (* result type *)
  | Variable of string * OclType (* name with type *)
  | Let of string * OclType (* variable *)
      * OclTerm * OclType (* rhs *)
      * OclTerm * OclType (* in *)
  | Iterate of (string * OclType) list (* iterator variables *)
      * string * OclType * OclTerm (* result variable *)
      * OclTerm * OclType (* source *)
      * OclType (* result type *)
  | Iterator of string (* name of iterator *)
      * (string * OclType) list (* iterator variables *)
      * OclTerm * OclType (* source *)
      * OclTerm * OclType (* iterator.body *)
      * OclType (* result type *)
  and CollectionPart = CollectionItem of OclTerm * OclType (* element with type *)
  | CollectionRange of OclTerm (* first *)
      * OclTerm (* last *)
      * OclType (* type of range *)

end
Chapter 6. The HOL-ocl System Architecture

```ml
signature REP_CORE = sig

  type Scope
  type Visibility
  type operation = { name : string,
                     precondition : (string option * OclTerm) list,
                     postcondition : (string option * OclTerm) list,
                     arguments : (string * OclType) list,
                     result : OclType,
                     isQuery : bool,
                     scope : Scope,
                     visibility : Visibility }

  type associationend = { name : string,
                         aend_type : OclType,
                         multiplicity : (int * int) list,
                         ordered : bool,
                         visibility : Visibility,
                         init : OclTerm option }

  type attribute = { name : string,
                     attr_type : OclType,
                     visibility : Visibility,
                     scope : Scope,
                     stereotypes : string list,
                     init : OclTerm option }

datatype Classifier = Class of { name : Path,
                                  parent : Path option,
                                  attributes : attribute list,
                                  operations : operation list,
                                  associationends : associationend list,
                                  invariant : (string option * OclTerm) list,
                                  stereotypes : string list,
                                  interfaces : Path list,
                                  activity_graphs : ActivityGraph list}
  | Interface of { ... } (* similar to class *)
  | Enumeration of { ... }
  | Primitive of { ... }
end
```

Listing 6.3: su4sml: Representing the UML core
6.3. The Encoder: An Object-oriented Datatype Package

Encoding object-oriented data structures in HOL as needed for HOL-OCL, is a tedious and error-prone activity, which should be automated. In this section, we give an overview of the su4sml-based datatype package we implemented to automate this process. In the theorem prover community, a datatype package \[33\] is a module that allows one to introduce new datatypes and automatically derive certain properties over them. A (conservative) datatype package has two main tasks:

1. generate all required (conservative) constant definitions, and
2. prove as much (interesting) properties over the generated definitions as possible automatically behind the scenes.

For our datatype package, we use the possibility to build SML programs performing symbolic computations over formulae in a logically safe way.

In the following, we give a brief overview what our package does. The datatype package is implemented on top of the su4sml interface on one hand and on top of the Isabelle core on the other (see Listing 6.4 for details). During the encoding, our datatype packages extends the given theory by a HOL-OCL-representation of the given UML/OCL model. This is done in an extensible way, i.e., classes can be added later on to an existing theory preserving all proven properties. The obvious tasks of the datatype package are:

1. declare HOL types for the classifiers of the model,
2. encode the core data model into HOL, and
3. encode the OCL specification and combine it with the core data model.

Listing 6.4: The Top-level Interface of the Repository Encoder

```ml
signature REP_ENCODER =
 sig
  type mdr = { theory : theory,
               universe : typ,
               classifiers : Classifier list }
  val add_classifiers : Classifier list -> mdr -> mdr
 end
```

We also decided to ignore associations as such. We only represent their association ends, again as part of the participating classifiers.

Overall, the top-level data structures (see Listing 6.1-6.3) of su4sml are inspired by the metamodels of OCL [41, Chapter 8] and UML [40] and readers familiar with these metamodels should recognize the similarities.
In fact, the most important task is probably not that obvious: The package has to generate formal proofs that the generated encoding of object-structures is a faithful representation of object-orientation (e.g., in the sense of the UML standard [40], or Java). These theorems have to be proven for each model during its encoding phase. Among many other properties, our package proves for each pair of classes $A$ and $B$ where $B$ is a generalization of $A$ the following facts:

$$\frac{\text{self.oclIsType}(B)}{\text{self.oclIsKind}(A)}.$$ (6.1)

as well as the more complicated property:

$$\frac{\text{self.oclIsDefined()}}{\text{self.oclIsType}(B)} \quad \frac{\text{self.oclAsType}(A).oclAsType(B).oclIsDefined()}{\text{and self.oclAsType}(A).oclAsTypeB.oclIsType(B)}.$$ (6.2)

Listing 6.5 presents a simplified version of the SML function `cast_class_id` that proves the property (6.2). The expression starting in line 5 generates a type-checked instance of the current theorem to prove with respect to the current class (and its parent). Readers familiar with LCF-style theorem provers will recognize the “proof script” in lines 10 to 23. Finally, the function registers the proven theorem in Isabelle’s theorem database. Logical rules like (6.1) or (6.2) or co-induction schemes given by class invariants constitute the object-oriented datatype theory of a given class diagram and represent the basic weapon for proofs over them, in particular verifications of UML/OCL specifications. Stating these rules could be achieved by adding axioms (i.e., unproven facts) during the encoding process, which is definitively easier to implement. Instead, our datatype package generates entirely conservative definitions and derives these rules from them; this also includes the definition of recursive class invariants, which are in itself not conservative (see section 4.11 for details).

This strategy, i.e., stating entirely conservative definitions and formally proving the datatype properties for them, ensures two very important properties:

1. our encoding fulfills the required properties, otherwise the proofs would fail, and
2. doing all definitions conservatively together with proving all properties ensures the consistency of our model (provided that HOL is consistent and Isabelle/HOL is a correct implementation).

To get a feeling for the amount of work needed, the import of the “Company” model (including the OCL specification) presented in the OCL standard [41] Chapter 7 generates 1147 conservative definitions and proven theorems, the larger “Royals and Loyal” model [52] model generates 2472 conservative definitions and proven theorems.

\footnote{1\text{inherited from}}
6.4. The HOL-OCL-Library

An important part of HOL-OCL is a collection of Isabelle theory files describing the formalization in detail. These theories also contain new proof procedures (tactics) written in SML. These theory files are extensively documented in Appendix B in the appendix, the developed tactics are also described in section 9.3.

6.5. The Theory-Morpher

The theory morpher provides automatic support lifting theorems from the HOL level to the HOL-OCL level. This is based on our organization of the, i.e., library function definitions for our typed shallow embedding in a layered theory morphism. The theory morpher, or lifter is in principle a tactic-based program that lifts meta-level theorems to their object-level counterparts and meta-level prover configurations to object-level ones.

Our approach can be seen as an attempt to liberate the shallow embedding technique from the “point-wise-definition-style” in favor of more global semantic transformations from one language level to another. We abstracted the underlying conceptual notions into a generic framework that shows that the overall technique is applicable in a wide range of embeddings in type systems; embedding-specific dependencies arise only from the specifications of semantic combinator (the layers), and technology specific dependencies from the used tactic language.

Listing 6.5: Proving Cast and Re-Cast (simplified)
Chapter 6. The HOL-OCL System Architecture

In the present version, the tactic proof engine cannot handle data adaption invariants which limits its potential to 10%. However, this limitation will be overcome soon.
Part III.

System Description
Chapter 7.

Installing HOL-OCL

7.1. Prerequisites

HOL-OCL is built on top of Isabelle/HOL-Complex, version 2005, thus you need an working installation of Isabelle 2005. At the moment, HOL-OCL requires an Isabelle based on SML/NJ [6] to be full functional.\(^1\) We strongly recommend also to install the generic proof assistant front-end Proof General \(^2\). The overall system architecture is depicted in Figure 7.1. For doing larger applications, you should install a complete tool-chain comprising a CASE\(^3\)-Tool, e.g., ArgoUML, and an OCL type-checker (from the Dresden OCL\(^2\) toolkit) for generating type-correct UML/OCL models in a comfortable way (see Figure 9.1 for an overview of the proposed HOL-OCL work flow).

7.2. Installation

In the following we will give a brief guide how to install the prerequisites for an HOL-OCL base system (i.e., HOL-OCL and Isabelle), please refer to the respective documentation for details. We will not describe how to install the CASE-tool and the OCL type checker, but we recommend to install them in any case. We have tested our XMI import using the following setup:

\(^1\)The XMI import uses internally the Word32 structure which is not supported by Poly/ML [4].
\(^2\)Currently HOL-OCL was only tested on GNU/Linux systems on the i386 architecture, please report your experiences when you try to install HOL-OCL on a different operating system or architecture.

\[Figure 7.1.: \text{Overview of the High-level System Architecture of HOL-OCL}\]
Chapter 7. Installing HOL-OCL

- A recent version (0.20 or higher) of the CASE tool “ArgoUML” (http://argouml.tigris.org/).
- The type checker “Dresden-OCL 1.1” for OCL 2.0 (http://dresden-ocl.sf.net). Our toolchain only relies on the “Parser GUI” which can be started using the command

  ```
  java -jar ocl20parsertools.jar
  ```

  within the top-level directory of the Dresden OCL 2 toolkit. Alternatively, a command-line version of the type-checker is available:

  ```
  java -cp ocl20parsertools.jar tudresden.oocl20.core.parser.OCL20CLI
  ```

7.2.1. Installation from Source

SML and Isabelle

1. Download a recent version of sml/NJ [6] install it following its documentation. We recommend version 110.56 which can be downloaded from http://www.smlnj.org/dist/working/110.56/index.html.

2. Download the Isabelle 2005 source code[3] from the from the Isabell web-site (http://isabelle.in.tum.de/dist/packages.html), after unpacking the Isabelle source, replace the file src/Pure/defs.ML with contrib/defs.ML which is part of the HOL-OCL distribution[4]. After that you can follow the normal instructions for building Isabelle. Note that you need to build the HOL-Complex image, i.e., you have to call

  ```
  $ISABELLE_HOME/build -m HOL-Complex HOL
  ```

3. Finally install a version of Proof General that supports Isabelle 2005, e.g. we strongly recommend a 3.6 pre-release. E.g., download http://proofgeneral.inf.ed.ac.uk/releases/ProofGeneral-3.6pre051004.tar.gz and follow the supplied instructions.

Installing HOL-OCL

In the following we assume that you have a running Isabelle 2005 environment including the Proof General based front-end. The installation of HOL-OCL requires the following steps:

1. Unpack the HOL-OCL distribution, e.g.:

   ```
   tar zxfv holocl-0.9.0.tar.gz
   ```

   [3] Note that you cannot use the pre-compiled heap images as they are based on Poly/ML.

   [4] This fixes a performance bug in Isabelle 2005 which renders our XMI import unusable.
7.2. Installation

This will create a directory holocl-0.9.0 containing the HOL-OCL distribution.

2. Check the settings in the configuration file holocl-0.9.0/make.config. If you can use the isatool tool from Isabelle on the command line, the default settings should work.

3. Change into the src directory

    cd holocl-0.9.0/src

and build the HOL-OCL heap image for Isabelle by calling

    isatool make

4. HOL-OCL queries the environment variable $HOLOCL_HOME for finding runtime configurations. Thus you have to set this variable pointing to the top-level directory of your HOL-OCL installation.

5. Finally, you need to extend your ~/.emacs file with the following lines:

    (add-to-list 'load-path (concat (getenv "HOLOCL_HOME") "/etc/"))
    (load "x-symbol-holocl-startup") ;; Proof General extension
    ;; for HOL-OCL

This will make Proof General aware of the new syntax and commands provided by HOL-OCL. Further, if you are using GNU Emacs, you can also add the following lines to your ~/.emacs file:

    (require 'ocl) ;; simple mode for editing
    ;; OCL files

This will provide syntax highlighting for plain OCL specifications.

7.2.2. Using Debian Packages

Installing HOL-OCL on an Debian GNU/Linux on a i386 architecture should be straightforward. Just add the IsaMorph apt-repository to the sources of your package manager, e.g. by adding the following lines

# IsaMorph repository
deb-src http://kisogawa.inf.ethz.ch/isamorph/debian stable main
deb http://kisogawa.inf.ethz.ch/isamorph/debian stable main

to /etc/apt/sources.list file. Please replace stable by the distribution you are using (we provide packages for all three flavours, i.e., stable, testing or unstable). After that, update your package list, i.e., by executing

    aptitude update
Chapter 7. Installing HOL-OCL

Now install a complete (eventually you have to install other logics, if you need them) Isabelle setup by executing

\texttt{aptitude install x-symbol proofgeneral-misc isabelle \ isabelle-thy-hol-complex}

and HOL-OCL by executing

\texttt{aptitude install hol-ocl}

This should give you a running installation of sml/NJ Isabelle, Proof General and last but not least, HOL-OCL in its default configuration (based on smashed sets and a referential universe). If you need a different setup, please install HOL-OCL from source and change the configuration in the \texttt{make.config} file.

7.3. Starting

Regardless of the installation method you are using, you should now be able to start HOL-OCL using the command:\textsuperscript{5}

\texttt{Isabelle -L HOL-OCL}

As HOL-OCL provides new top-level commands, the -L HOL-OCL is \textit{mandatory}. After a few seconds you should see a Emacs window similar to the one shown in Figure 7.2.

\textsuperscript{5}If you installed the Debian packages, you can also start HOL-OCL using the command \texttt{hol-ocl} or start HOL-OCL using the menu entry of your favourite desktop environment.
7.3. Starting

Figure 7.2: A HOL-OCL session Using the Isar Interface of Isabelle
Chapter 7. Installing HOL-OCL
Chapter 8.

Limitations of HOL-OCL

In this chapter we give a brief overview of the supported OCL/UML subset and current limitations of HOL-OCL.

8.1. The Supported UML Subset

HOL-OCL aims for supporting a relevant subset of the “UML Core” module, i.e., more sloppy: the subset needed to express UML class diagrams.¹ The most restricting limitations are:

- **Enumeration** are not supported, but planned for a future release.
- **Associations** are represented by their associations ends (with additional constraints). Direct association support (i.e., as relations) is planned.
- **Association classes** are not supported, support is planned together with the direct support for associations.
- Qualifiers for **association ends** are not supported.
- **Ordered associations ends** have the type **Sequence** by the Dresden OCL Toolkit which is thus also the type used by HOL-OCL. In contrast, the UML standard [40, p. 3-71] requires the representation as **OrderedSet** (i.e., the elements of the set have an ordering, but duplicates are still prohibited).

Further note that the UML standard [40, p. 5-10] defines the following primitive datatypes: **Integer**, **UnlimitedInteger**, **String**, and **Enumerations**. We consider these datatypes different from the datatypes defined in the OCL standard [41], e.g. HOL-OCL supports the OCL types **Integer**, **Real**, **String**, and **Boolean** (the datatype **enumeration** is not supported at the moment). During modeling, we advise you to place the OCL datatypes in a package called **UML_OCL** (as proposed by the UML standard version 1.4).

¹Support for dynamic diagram types, i.e., activity charts or state charts is planned for a future release.
Chapter 8. Limitations of HOL-OCL

8.2. The Supported OCL Subset

8.2.1. OCL Syntactical Variants

In general, the OCL standard introduces a lot of syntactical variants to reduce the amount of text one has to write, i.e., bound variables do not need to be annotated with a concrete type, or can even be omitted. For example, the following to invariants are only syntactical different:

\[
\begin{align*}
\text{context } & A: \\
\text{inv: } & \text{self.b->select(i=5)} \\
\text{inv: } & \text{self.b->select(a | a.i =5 )}
\end{align*}
\]

At the moment, our tool chain does not support all these variants, in particular, one has to make bound variable explicit and has to annotate them with type information:

\[
\begin{align*}
\text{context } & A: \\
\text{inv: } & \text{self.b->select(b:B| b.i = 5)}
\end{align*}
\]

Furthermore, introducing alternative names for self, i.e.:

\[
\begin{align*}
\text{context } & \text{foo:A:} \\
\text{inv: } & \text{foo.i = 5}
\end{align*}
\]

is currently not supported.

8.2.2. OCL context declarations

The OCL standard [41, pp. 157] introduces the different context declarations, which are handled by HOL-OCL as follows:

\textbf{inv}: fully supported.

\textbf{pre}: fully supported.

\textbf{post}: fully supported.

\textbf{init}: are supported by converting them into an invariant, e.g.

\[
\begin{align*}
\text{context } & A: \\
\text{init: } & \text{self.x = 5}
\end{align*}
\]

will be converted into

\[
\begin{align*}
\text{context } & A: \\
\text{inv: } & \text{self.oclIsNew() implies self.x = 5}
\end{align*}
\]

Note, this formulae can be considered as non-standard with regards to the OCL standard but is valid in HOL-OCL.
8.2. The Supported OCL Subset

**def:** not supported due to Dresden OCL (will be supported after Dresden OCL is fixed), i.e., for HOL-OCL there is no difference between statements defined (graphical) within the case tool or as OCL formulae.

**derive:** not supported due Dresden OCL (will be supported after Dresden OCL is fixed), i.e., for HOL-OCL there is no difference between statements defined (graphical) within the case tool or as OCL formulae.

**body:** supported by converting them into a post condition, e.g.

```
context A::f():Integer
body: 5
```

will be converted into

```
context A::f():Integer
post: result = 5
```

**guard:** not supported, support will be developed once we support dynamic diagram types.

### 8.2.3. OCL Types

OCL introduces a variety of pre-defined types (and meta-types), for some of them certain restrictions apply within HOL-OCL. In more detail:

- The type OclVoid is modeled implicit, for details see the lifting construction and the handling of the type class bot.
- The type OclMessage is not support, support for it will be eventually developed together with the support for dynamic diagram types (e.g. activity charts).
- **Enumeration** are not supported, but planned for a future release.
- The types OclModelElementType and OclType are modeled implicit, respectively replaced by the type of the characteristic set (of a type).
- The enumeration OclModelElement is not supported, respectively modeled implicit.
- The type Tuple (respectively TupleType) is not yet supported. Support for tuples is planned for a future release.
- The type OrderedSet is not yet supported by the Dresden OCL Toolkit but is supported by HOL-OCL. If you want to use OrderedSet you have to enter the corresponding constraints directly into HOL-OCL.
8.2.4. Predefined Properties

OCL introduces a variety of pre-defined properties and operations, for some of them certain restrictions apply within HOL-OCL. In more detail:

- **OclInState** is not supported at the moment; it will be eventually developed together with the support for dynamic diagram types (e.g., state charts and activity charts).

- The generic “\texttt{\textit{-\textsl{iterate()}}}” expression is at the moment not supported by the XMI import. Nevertheless, it can be entered directly within HOL-OCL. The predefined iterator expressions, e.g., \texttt{\textit{-\textsl{one}}} or \texttt{\textit{select}}, are fully supported.

- Collection literals, e.g., \texttt{\textit{Set{1,3,4,9}}} or \texttt{\textit{Sequence{1,\ldots,42}}} are at the moment not supported by the XMI import. Nevertheless, they can be entered directly within HOL-OCL.

8.3. Reporting Bugs

If you find a bug in HOL-OCL, please send electronic mail to \texttt{hol-ocl@brucker.ch}. Include the version number, which you can find by running the \texttt{\textit{info()}} in the interactive HOL-OCL environment. Also include in your message the output that the program produced and the output you expected.

If you have other questions, comments or suggestions about HOL-OCL, contact the author via electronic mail to \texttt{hol-ocl@brucker.ch}. The authors will try to help you out, although they may not have time to fix your problems.
Chapter 9.

A HOL-OCL Reference Manual

9.1. The Basic Workflow

HOL-OCL allows one to reason formally over UML/OCL specifications. The overall HOL-OCL work-flow (see Figure 9.1 for an overview) is divided into two phases:

Modelling Phase: During the modeling and design phase one formalizes the (often informal given) requirements. The result of this phase should be a formal model of the software system being built (in our case, formalized using UML/OCL). Technically, the modelling phase is twofold:

1. design your (data) model using a CASE tool, e.g., ArgoUML and export it in XMI format.
2. refine your data model by adding OCL constraints using the Dresden OCL Toolkit. Export your refined model (including the OCL formulae in XMI format).

Verification Phase: In the analyzing and verification phase, the UML/OCL model is formally explored using an Isar-based environment. Such a formal analysis can for example aim towards proving the consistency (i.e., there exists a system that fulfills the requirements of the model), security of safety. Further, the model can be further improved, i.e., by doing formal refinements.

In the following, we will give a brief overview of the modelling phase and describe the verification phase in more detail.

9.2. The Modelling Phase

In this section, we give a brief overview of the modelling phase, i.e., we concentrate ourselves on describing the most important tasks and pitfalls of this phase. Please refer to the manuals of your CASE tool and Dresden OCL for more information about the technical details of the modelling phase.

Overall, the modeling phase is split into two parts:

CASE-Tool (e.g., ArgoUML) \hspace{2cm} XMI data model \hspace{2cm} Dresden-\textit{OCL} formal specification \hspace{2cm} HOL-\textit{OCL} proofs

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{hol-ocl_workflow.png}
\caption{The HOL-OCL Workflow}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{argouml_data_model.png}
\caption{Using ArgoUML for Data Modelling}
\end{figure}
9.2. The Modelling Phase

```ocl
package RoyalLoyal

context LoyaltyAccount::isEmpty(): Boolean
    pre: true
    post: result = (points = 0)

context LoyaltyAccount::points: Integer
    init: 0

class LoyaltyAccount
    inv
    Transactions: transactions.points
        ->exists(p: Integer | p = 500)
endpackage
```

**Listing 9.1:** A OCL Specification (Excerpt of the Royals and Loyals Model)

1. Modelling the data model (based on the diagrammatic UML notions) using a CASE tool, e.g., ArgoUML (see Figure 9.2). We assume that the reader is familiar with the CASE tool he is using. The result of this process should be an XMI file that can be imported into the Dresden OCL 2 toolkit. Our tool-chain requires the following organization of your model:

   - The complete model should be placed into a top-level UML package. This package is ignored by the Dresden OCL 2 Toolkit.
   - Within the top-level package you can specify arbitrary packages for your models.
   - The top-level package should contain a UML package called UML_OCL that contains all OCL datatypes (i.e., the OCL library). All basic datatypes, e.g., Integer, should be taken from this package.

   Please have a look at the examples provided by the HOL-OCL distribution for details.

2. Modelling and type-checking the OCL specification. The Dresden OCL 2 Toolkit uses a simple text format for the OCL specification, e.g., see Item 9.1 for an example. The type-checker (included in the “Parser Tool”) of the Dresden OCL 2 toolkit can now be used to type-check such a OCL specification against a given data model. This can be either done using a graphical interface (see Figure 9.3) in the following way:

   a) Click on the “Model” tab and load your UML model by clicking on “Load XMI” (either stored as XMI or ArgoUML’s native format (.zargo).

   b) Click on the “Constraint” tab and load your OCL specification.

Figure 9.3: Using the Dresden OCL Parser and Type-checker

c) Click on the “CST” tab and click on “Parse(CS)”. This will parse the concrete syntax of your OCL specification, i.e., up to now, no type-checking is involed.

d) If the last step succeeds, i.e., you see a parse tree of the concrete syntax, click on the “ASTGen log” tab and click on “Generate”. This will generate type-check your OCL specification.

e) If the type-checking succeeds without errors, you can export (by clicking on “Export XMI”) a XMI file containing both, the UML and OCL part of your model. This XMI file can be loaded into HOL-OCL.

Alternatively, you can type-check your models on the command-line using the following syntax:

```java
java -cp ocl20parsertools.jar tudresden.oc120.core.parser.OCL20CLI \
   --outfile output.xmi input.xmi input.ocl
```

where input.xmi is your data model (either in XMI format or ArgoUML’s native format), input.ocl is your OCL specification, and output.xmi the file where (after successful type-checking) the output is written to.

9.3. Using HOL-OCL: The Verification Phase

In this section we give a brief overview of HOL-OCL related extension of the Isar [53] proof language. We also use a presentation similar to the one in the Isar Reference
9.3. Using HOL-OCL: The Verification Phase

theory royals_and_loyals
  imports OCL
begin
  load_xmi "royals_and_loyals_ocl.xmi"
end

Listing 9.2: A simple HOL-OCL Theory File

Manual [53], e.g. “missing” non-terminals (e.g., ⟨goalspec⟩) of our syntax diagrams are defined in [53].

9.3.1. Getting Started

For using HOL-OCL you have to build your Isabelle theories (i.e. test specifications) on top of the theory UML_OCL (plain UML/OCL) or OCL (UML/OCL with extensions) instead of Main. A sample theory is shown in Listing 9.2.

9.3.2. Loading XMI files

A well-typed UML/OCL models can be imported using the load_xmi command, e.g.:

load_xmi "royals_and_loyals_ocl.xmi"

9.3.3. Canonizing Hypotheses

Similar to hypsubst_tac on the HOL level, HOL-OCL provides ocl_hybsubst_tac for the elimination of variables A within OCL equality assumptions. The format of these equalities is quite general here, a number of equalities stated implicitly is also handled:

1. \( A = t \) and \( t = A \) (as in standard hyp_subst_tac),
2. \( A \tau = t \tau, t \tau = A \tau \) (local congruences),
3. \( \tau \vdash \emptyset A, \vdash \emptyset A \) (local and global undefinedness),
4. \( \tau \vdash \neg A, \vdash \neg A \) (local and global falsities),
5. \( \tau \vdash A \triangleleft t, \tau \vdash t \triangleleft A, \vdash A \triangleleft t, \vdash t \triangleleft A \) (local and global strong equalities), and
6. \( \tau \vdash A \equiv t, \tau \vdash A \equiv t \equiv A \equiv t \vdash A \equiv t \equiv A \equiv t \) (local and global strict equalities).

The syntax for the command reads as follows:

ocl_hybsubst_tac \( \vdash ⟨goalspec⟩ \vdash \)
9.3.4. One-Step-Rewriting

The major limitation of canonization as described in the previous section is that it is restricted to variables - on the other hand, the canonization can apply an equality from left to right and from right to left. In contrast, rewriting (actually in this context: narrowing) proceeds only from left to right, but admitting simplification of non-variable terms.

The possible formats of implicit equalities look similarly as the list in ocl_hypsubst:

1. \( \tau \models \emptyset \text{lhs}, \models \emptyset \text{lhs} \) (local and global undefinedness; replaces lhs by \( \bot \)),
2. \( \tau \models \emptyset \text{lhs}, \models \emptyset \text{lhs} \) (local and global definedness; replaces \( \emptyset \text{lhs} \) by \( \top \)),
3. \( \tau \models \neg \text{lhs}, \models \neg \text{lhs} \) (local and global falsities; replaces \( \emptyset \text{lhs} \) by \( \bot \)),
4. \( \tau \models \text{lhs} \models \text{lhs} \) (local and global validities; replaces lhs by \( \top \)),
5. \( \text{lhs} \tau = t \tau \) (local congruences),
6. \( \models \text{lhs} \triangleq t \) (local and global strong equalities), and
7. \( \tau \models \text{lhs} \doteq t \) (local and global strict equalities).

The syntax for the command reads as follows:

```
ocl_subst ⟨goalspec⟩ ⟨‐(‐(‐no_asm_use ‐))⟩ ⟨‐(‐no_asm_simp ‐)⟩ (‐no_concl_simp) thmlist
```

With the attribute specification, the range of the possible rewrite-step can be limited. Specifying no_asm_use excludes assumptions in a goal from rewriting, no_asm_simp excludes them from being rewritten. By no_asm_concl, the rewriting of the conclusion can be prevented. The method accepts a direct specification of a goal to be rewritten, and a list of theorems hat can be used for rewriting (possibly empty).

The method fails if no redex can be found; thus, by using the repetition operator, a simple exhaustive rewriting process can be formulated.

9.3.5. Automated Proof-Procedures

As an equivalent to auto ...

```
ocl_auto ⟨‐(‐(‐nat ‐)(‐nat ‐))⟩ ⟨‐(‐clasimpmod ‐)⟩
```
9.4. Extending HOL-OCL

In this section we explain commands that are useful for extending HOL-OCL, i.e., they are more thought for developers than for users.

Exploiting theory morphisms: The theory lifting mechanism is used on a “per operator” basis, e.g.:

\[ \text{ocl_setup_op [OclIncludes, OclExcludes]} \]

The procedure performs at present no sophisticated ocl-specific machinery.
Chapter 10.

Case Studies

10.1. Encoding a Stack in UML/OCL

theory stack
imports OCL
begin

We use the class diagram presented in Fig. 10.1 together with the following OCL formulae shown in Listing 10.1.

load_xmi stack_ocl.xmi

An interesting system property would be

\[
\vdash s_0 \implies (\text{push } s_0 e_0 s_1) \implies ((\text{top } s_1 e_1) \land (e_1 \equiv e_0))
\]

or

\[
\vdash s_0 \implies \text{size}(s_0) \geq \text{size}(\text{pop } s_0)
\]

Note that such system properties specified in HOL-OCL allow the use of operations that are not side-effect free (e.g. push)

end

Figure 10.1.: Modelling a Stack: Data Model
package Stack

context Stack::pop(): Stack
pre notEmpty: isEmpty() = false
post topElementRemoved: top() <> self.top@pre()
post: elements = elements@pre->subSequence(2, self@pre->size())
post: elements->size() = elements@pre->size() -1

context Stack::top(): ElemType
pre notEmpty: isEmpty() = false
post: result = elements->first()
-- post: self=self@pre

context Stack::push(e: ElemType): Stack
post pushedElemTypeIsOnTop: top() = e
post: elements = elements@pre->prepend(e)
post: result = self

context Stack::isEmpty(): Boolean
post: result = (elements->size() <> 0)

endpackage

Listing 10.1: Modelling a Stack: OCL specification
Part IV.

Appendix
Appendix A.

The Syntax of OCL

OCL, being advertised with the slogan “Mathematical Foundation, But No Mathematical Symbols” [52], is normally written using a concrete syntax that is inspired by object-oriented programming languages. To give a first impression of this syntax to readers unfamiliar with it, we present a core fragment of OCL using Extended Backus-Naur Form (EBNF) notation (see Tab. A.1). This fragment in particular omits many syntactic variants resulting from naming expressions. This simplified concrete syntax used to denote our examples contains some redundancies: the variant expr->simpleName is semantically equivalent with dereferencing expr.simpleName, it is a tribute to the OCL convention to distinguish the application of operations on collections such as X->union(Y). In principle, this also holds for the prefix and infix operators. However, the semantics of this applications may be call-by-name or call-by-need; this is handled for each operator individually.

Whereas this textual notation pleases the people coming from object-oriented programming languages, it looks awkward for people coming from the mathematics and formal methods field. Especially for proof work, there seems a need for a compact, mathematical notation. Thus we developed a mathematics-oriented OCL syntax, as an alternative to the programming-language like notation used in the OCL 2.0 standard. For example, compare the textual presentation of the proof rule:

\[
\tau \models S \rightarrow \text{includes}(x) \quad \tau \models \neg(P \ x) \quad \text{cp} \ P
\]
\[
\tau \models (S \rightarrow \text{forall}(x \mid P(x)) \rightarrow \text{IsDefined()})
\]
(A.1)

to its presentation in mathematical notation:

\[
\tau \models x \in S \quad \tau \models \neg(P \ x) \quad \text{cp} \ P
\]
\[
\tau \models \partial(\forall x \in S . P(x)).
\]
(A.2)

Clearly, both syntax’s have their advantages and disadvantages and therefore we support both of them in HOL-OCL.

In Table A.2 we provide a brief comparison between the different concrete OCL syntax’s, namely the syntax as proposed in the OCL standard, our textual notation that tries to follows the standard syntax as close as possible, and finally our new mathematical syntax. The table follows the OCL library presentation from the standard [11, Chapter 11], constructs that are not supported by HOL-OCL are written in a gray typeface, e.g. ooclIsInState(s).
### Appendix A. The Syntax of OCL

Table A.1: Formal Grammar of OCL (fragment)
Table A.2.: Comparison of different concrete syntax variants for OCL

<table>
<thead>
<tr>
<th>OCL (standard)</th>
<th>mathematical HOL-OCL</th>
<th>textual HOL-OCL</th>
</tr>
</thead>
<tbody>
<tr>
<td>x = y</td>
<td>x ≡ y</td>
<td>x == y</td>
</tr>
<tr>
<td>x &lt;&gt; y</td>
<td>x ≠ y</td>
<td>x &lt;&gt; y</td>
</tr>
<tr>
<td>x ≤ y</td>
<td>x ≤ y</td>
<td>x ≦ y</td>
</tr>
<tr>
<td>x ≥ y</td>
<td>x ≥ y</td>
<td>x ≧ y</td>
</tr>
<tr>
<td>ooclIsNew()</td>
<td>ooclIsNew()</td>
<td>ooclIsNew()</td>
</tr>
<tr>
<td>ooclIsUndefined()</td>
<td>ooclIsUndefined()</td>
<td>ooclIsUndefined()</td>
</tr>
<tr>
<td>ooclAsType(t)</td>
<td>ooclAsType(t)</td>
<td>ooclAsType(t)</td>
</tr>
<tr>
<td>ooclIsType(t)</td>
<td>ooclIsType(t)</td>
<td>ooclIsType(t)</td>
</tr>
<tr>
<td>ooclIsKindOf(t)</td>
<td>ooclIsKindOf(t)</td>
<td>ooclIsKindOf(t)</td>
</tr>
<tr>
<td>ooclIsInState(s)</td>
<td>ooclIsInState(s)</td>
<td>ooclIsInState(s)</td>
</tr>
<tr>
<td>o.allInstances()</td>
<td>o.allInstances()</td>
<td>o.allInstances()</td>
</tr>
<tr>
<td>o.hasReturned()</td>
<td>o.hasReturned()</td>
<td>o.hasReturned()</td>
</tr>
<tr>
<td>o.result()</td>
<td>o.result()</td>
<td>o.result()</td>
</tr>
<tr>
<td>o.isSignalSent()</td>
<td>o.isSignalSent()</td>
<td>o.isSignalSent()</td>
</tr>
<tr>
<td>o.isOperationCall()</td>
<td>o.isOperationCall()</td>
<td>o.isOperationCall()</td>
</tr>
</tbody>
</table>

Continued on next page
# Appendix A. The Syntax of OCL

<table>
<thead>
<tr>
<th>OCL</th>
<th>mathematical HOL-OCL</th>
<th>textual HOL-OCL</th>
</tr>
</thead>
<tbody>
<tr>
<td>x.div(y)</td>
<td>x div y</td>
<td>x -&gt; div(y)</td>
</tr>
<tr>
<td>x.mod(y)</td>
<td>x mod y</td>
<td>x -&gt; mod(y)</td>
</tr>
<tr>
<td>x.max(y)</td>
<td>max(x, y)</td>
<td>x -&gt; max(y)</td>
</tr>
<tr>
<td>x.min(y)</td>
<td>min(x, y)</td>
<td>x -&gt; min(y)</td>
</tr>
<tr>
<td>s.size()</td>
<td>∥s∥</td>
<td>s -&gt; size()</td>
</tr>
<tr>
<td>s.concat(z)</td>
<td>s ∧ z</td>
<td>s -&gt; concat(z)</td>
</tr>
<tr>
<td>s.substring(i,j)</td>
<td>s.substring(i, j)</td>
<td>s -&gt; substring(i, j)</td>
</tr>
<tr>
<td>s.toInteger()</td>
<td>s.toInteger()</td>
<td>s -&gt; toInteger()</td>
</tr>
<tr>
<td>s.toReal()</td>
<td>s.toReal()</td>
<td>s -&gt; toReal()</td>
</tr>
<tr>
<td>s.toUpper()</td>
<td>s.toUpper()</td>
<td>s -&gt; toUpper()</td>
</tr>
<tr>
<td>s.toLower()</td>
<td>s.toLower()</td>
<td>s -&gt; toLower()</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Boolean</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>⊨ p</td>
<td>Valid p</td>
<td></td>
</tr>
<tr>
<td>⊨ true</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>⊨ false</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>x or y</td>
<td>x ∨ y</td>
<td></td>
</tr>
<tr>
<td>x xor y</td>
<td>x ⊕ y</td>
<td></td>
</tr>
<tr>
<td>x and y</td>
<td>x ∧ y</td>
<td></td>
</tr>
<tr>
<td>not x</td>
<td>¬ x</td>
<td></td>
</tr>
<tr>
<td>x implies y</td>
<td>x → y</td>
<td></td>
</tr>
<tr>
<td>x 1 implies y</td>
<td>x 1 → y</td>
<td></td>
</tr>
<tr>
<td>x 2 implies y</td>
<td>x 2 → y</td>
<td></td>
</tr>
<tr>
<td>x or y</td>
<td>x or y</td>
<td></td>
</tr>
<tr>
<td>x xor y</td>
<td>x xor y</td>
<td></td>
</tr>
<tr>
<td>x and y</td>
<td>x and y</td>
<td></td>
</tr>
<tr>
<td>not x</td>
<td>not x</td>
<td></td>
</tr>
<tr>
<td>if c then x else y endif</td>
<td>if c then x else y endif</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Collection</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>X-&gt;size()</td>
<td>∥X∥</td>
<td>X -&gt; size()</td>
</tr>
<tr>
<td>X-&gt;includes(y)</td>
<td>y ∈ X</td>
<td>X -&gt; includes(y)</td>
</tr>
<tr>
<td>X-&gt;excludes(y)</td>
<td>y ∉ X</td>
<td>X -&gt; excludes(y)</td>
</tr>
<tr>
<td>X-&gt;count(y)</td>
<td>X -&gt; count()</td>
<td></td>
</tr>
<tr>
<td>X-&gt;includesAll(Y)</td>
<td>X ⊆ Y</td>
<td>X -&gt; includesAll(Y)</td>
</tr>
<tr>
<td>X-&gt;excludesAll(Y)</td>
<td>X ⊄ Y</td>
<td>X -&gt; excludesAll(Y)</td>
</tr>
<tr>
<td>X-&gt;isEmpty()</td>
<td>X = ∅</td>
<td>X -&gt; isEmpty()</td>
</tr>
<tr>
<td>X-&gt;notEmpty()</td>
<td>X ≠ ∅</td>
<td>X -&gt; notEmpty()</td>
</tr>
<tr>
<td>X-&gt;sum()</td>
<td>X -&gt; sum()</td>
<td></td>
</tr>
<tr>
<td>X-&gt;product(Y)</td>
<td>X × Y</td>
<td>X -&gt; product(Y)</td>
</tr>
<tr>
<td>X-&gt;exists(e:T</td>
<td>P(e))</td>
<td>e ∈ X.P(e)</td>
</tr>
<tr>
<td>X-&gt;forall(e:T</td>
<td>P(e))</td>
<td>∀ e ∈ X.P(e)</td>
</tr>
<tr>
<td>X-&gt;isUnique(e:T</td>
<td>P(e))</td>
<td>X -&gt; isUnique(e : T</td>
</tr>
<tr>
<td>X-&gt;any(e:T</td>
<td>P(e))</td>
<td>X -&gt; any(e : T</td>
</tr>
<tr>
<td>X-&gt;one(e:T</td>
<td>P(e))</td>
<td>X -&gt; one(e : T</td>
</tr>
<tr>
<td>X-&gt;collect(e:T</td>
<td>P(e))</td>
<td>[e ∈ X</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>OCL</th>
<th>mathematical HOL-OCL</th>
<th>textual HOL-OCL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set{}</td>
<td>$\emptyset$</td>
<td>${}$</td>
</tr>
<tr>
<td>X-&gt;union(Y)</td>
<td>$X \cup Y$</td>
<td>$X \rightarrow \text{union}(Y)$</td>
</tr>
<tr>
<td>X = Y</td>
<td>$X \equiv Y$</td>
<td>$X \equiv Y$</td>
</tr>
<tr>
<td>X-&gt;intersection(Y)</td>
<td>$X \cap Y$</td>
<td>$X \rightarrow \text{intersection}$</td>
</tr>
<tr>
<td>X-&gt;complement(Y)</td>
<td>$X \backslash Y$</td>
<td>$X \rightarrow \text{complement}(Y)$</td>
</tr>
<tr>
<td>X - Y</td>
<td>$X - Y$</td>
<td>$X - Y$</td>
</tr>
<tr>
<td>X-&gt;including(y)</td>
<td>$y \in X$</td>
<td>$X \rightarrow \text{includes}(y)$</td>
</tr>
<tr>
<td>X-&gt;excluding(y)</td>
<td>$y \notin X$</td>
<td>$X \rightarrow \text{excludes}(y)$</td>
</tr>
<tr>
<td>X-&gt;symmetricDifference(Y)</td>
<td>$X \oplus Y$</td>
<td>$X \rightarrow \text{symmetricDifference}(Y)$</td>
</tr>
<tr>
<td>X-&gt;count(y)</td>
<td>$X \rightarrow \text{count}(y)$</td>
<td>$X \rightarrow \text{count}(y)$</td>
</tr>
<tr>
<td>X-&gt;flatten()</td>
<td>$|X|$</td>
<td>$X \rightarrow \text{flatten}()$</td>
</tr>
<tr>
<td>X-&gt;asSet()</td>
<td>$X \rightarrow \text{asSet}()$</td>
<td>$X \rightarrow \text{asSet}()$</td>
</tr>
<tr>
<td>X-&gt;asOrderedSet()</td>
<td>$X \rightarrow \text{asOrderedSet}()$</td>
<td>$X \rightarrow \text{asOrderedSet}()$</td>
</tr>
<tr>
<td>OrderedSet{}</td>
<td>${}$</td>
<td>${}$</td>
</tr>
<tr>
<td>X-&gt;append(y)</td>
<td>$X : y$</td>
<td>$X \rightarrow \text{append}(y)$</td>
</tr>
<tr>
<td>X-&gt;prepend(y)</td>
<td>$y : X$</td>
<td>$X \rightarrow \text{prepend}(y)$</td>
</tr>
<tr>
<td>X-&gt;insertAt(i,y)</td>
<td>$X \rightarrow \text{insertAt}(i,y)$</td>
<td>$X \rightarrow \text{insertAt}(i,y)$</td>
</tr>
<tr>
<td>X-&gt;subOrderedSet(i,j)</td>
<td>$X \rightarrow \text{subOrderedSet}(i,j)$</td>
<td>$X \rightarrow \text{subOrderedSet}(i,j)$</td>
</tr>
<tr>
<td>X-&gt;at(i)</td>
<td>$#^i X$</td>
<td>$X \rightarrow \text{at}(i)$</td>
</tr>
<tr>
<td>X-&gt;indexOf(y)</td>
<td>$X \text{?}(y)$</td>
<td>$X \rightarrow \text{indexOf}(y)$</td>
</tr>
<tr>
<td>X-&gt;first()</td>
<td>$#1 X$</td>
<td>$X \rightarrow \text{first}()$</td>
</tr>
<tr>
<td>X-&gt;last()</td>
<td>$#^$ X</td>
<td>$X \rightarrow \text{last}()$</td>
</tr>
<tr>
<td>Bag{}</td>
<td>${}$</td>
<td>${}$</td>
</tr>
<tr>
<td>X = Y</td>
<td>$X = Y$</td>
<td>$X = Y$</td>
</tr>
<tr>
<td>X-&gt;union(Y)</td>
<td>$X \cup Y$</td>
<td>$X \rightarrow \text{union}(Y)$</td>
</tr>
<tr>
<td>X-&gt;complement(Y)</td>
<td>$X \backslash Y$</td>
<td>$X \rightarrow \text{complement}(Y)$</td>
</tr>
<tr>
<td>X-&gt;including(y)</td>
<td>$y \in X$</td>
<td>$X \rightarrow \text{includes}(y)$</td>
</tr>
<tr>
<td>X-&gt;excluding(y)</td>
<td>$y \notin X$</td>
<td>$X \rightarrow \text{excludes}(y)$</td>
</tr>
<tr>
<td>X-&gt;count(y)</td>
<td>$X \rightarrow \text{count}(y)$</td>
<td>$X \rightarrow \text{count}(y)$</td>
</tr>
<tr>
<td>X-&gt;flatten()</td>
<td>$|X|$</td>
<td>$X \rightarrow \text{flatten}()$</td>
</tr>
<tr>
<td>X-&gt;asBag()</td>
<td>$X \rightarrow \text{asBag}()$</td>
<td>$X \rightarrow \text{asBag}()$</td>
</tr>
<tr>
<td>X-&gt;asSequence()</td>
<td>$X \rightarrow \text{asSequence}()$</td>
<td>$X \rightarrow \text{asSequence}()$</td>
</tr>
<tr>
<td>X-&gt;asSet()</td>
<td>$X \rightarrow \text{asSet}()$</td>
<td>$X \rightarrow \text{asSet}()$</td>
</tr>
<tr>
<td>X-&gt;asOrderedSet()</td>
<td>$X \rightarrow \text{asOrderedSet}()$</td>
<td>$X \rightarrow \text{asOrderedSet}()$</td>
</tr>
</tbody>
</table>

Continued on next page
## Appendix A. The Syntax of OCL

<table>
<thead>
<tr>
<th>OCL</th>
<th>mathematical HOL-OCL</th>
<th>textual HOL-OCL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequence{}</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
<tr>
<td>X-&gt;count()</td>
<td>X-&gt;count(y)</td>
<td>X-&gt;count(y)</td>
</tr>
<tr>
<td>X = Y</td>
<td>X = Y</td>
<td>X = Y</td>
</tr>
<tr>
<td>X-&gt;union(Y)</td>
<td>X ∪ Y</td>
<td>X-&gt;union(Y)</td>
</tr>
<tr>
<td>X-&gt;flatten()</td>
<td>X \llceil \rceil Y</td>
<td>X-&gt;flatten()</td>
</tr>
<tr>
<td>X-&gt;append(y)</td>
<td>X::y</td>
<td>X-&gt;append y</td>
</tr>
<tr>
<td>X-&gt;prepend(y)</td>
<td>y:X</td>
<td>X-&gt;prepend y</td>
</tr>
<tr>
<td>X-&gt;insertAt(i,y)</td>
<td>X-&gt;insertAt(i,y)</td>
<td>X-&gt;insertAt(i,y)</td>
</tr>
<tr>
<td>X-&gt;subSequence(i,j)</td>
<td>X-&gt;subSequence(i,j)</td>
<td>X-&gt;subSequence(i,j)</td>
</tr>
<tr>
<td>X-&gt;at(i)</td>
<td>˝i X</td>
<td>X-&gt;at(i)</td>
</tr>
<tr>
<td>X-&gt;indexOf(y)</td>
<td>X ˝?y</td>
<td>X-&gt;indexOf(y)</td>
</tr>
<tr>
<td>X-&gt;first()</td>
<td>˝1 X</td>
<td>X-&gt;first()</td>
</tr>
<tr>
<td>X-&gt;last()</td>
<td>˝$ X</td>
<td>X-&gt;last()</td>
</tr>
<tr>
<td>X-&gt;including(y)</td>
<td>y ∈ X</td>
<td>X-&gt;includes(y)</td>
</tr>
<tr>
<td>X-&gt;excluding(y)</td>
<td>y ̸∈ X</td>
<td>X-&gt;excludes(y)</td>
</tr>
<tr>
<td>X-&gt;asBag()</td>
<td>X-&gt;asBag()</td>
<td>X-&gt;asBag()</td>
</tr>
<tr>
<td>X-&gt;asSequence()</td>
<td>X-&gt;asSequence()</td>
<td>X-&gt;asSequence()</td>
</tr>
<tr>
<td>X-&gt;asSet()</td>
<td>X-&gt;asSet()</td>
<td>X-&gt;asSet()</td>
</tr>
<tr>
<td>X-&gt;asOrderedSet()</td>
<td>X-&gt;asOrderedSet()</td>
<td>X-&gt;asOrderedSet()</td>
</tr>
<tr>
<td>X-&gt;select(e:T</td>
<td>P(e))</td>
<td>{e ∈ X</td>
</tr>
<tr>
<td>X-&gt;reject(e:T</td>
<td>P(e))</td>
<td>{e ∈ X</td>
</tr>
<tr>
<td>X-&gt;collectNested(e:T</td>
<td>P(e))</td>
<td>{ {e ∈ X</td>
</tr>
<tr>
<td>X-&gt;sortedBy(e:T</td>
<td>P(e))</td>
<td>X-&gt;sortedBy(e:T</td>
</tr>
</tbody>
</table>

let e=x in P(s) end

| let e = x in P(s) end | let e = x then P(s) end |
Appendix B.
Isabelle Theories

B.1. Introduction

In this chapter we present the Isabelle theories of HOL-OCL. The main dependencies are shown in Fig. 1.1 on the next page. HOL-OCL is build on top of Isabelle [HOL].

This chapter was automatically generated by Isabelle, i.e., it is a formal document: all definitions and theorems presented here were checked and formally proven by Isabelle. Nevertheless, we took the privilege of omitting theory some parts, in particular part's concerning the setup of the styntax engine, the interface to Isar the implementation of several tactics, the lifter, and the datatype package. Thus, in this chapter we present the semantic foundation of HOL-OCL. If you are also interested in the technical details of the implementation, please read the source code which is included in the HOL-OCL distribution.

B.1.1. HOL-OCL Configurations

Note, HOL-OCL can be built in different configurations, e.g., one can choose between non-referential and referential universes and between smashed and unsmashed collection types:

Universe: One issue to be raised here is the semantics of equality: are two objects equal only if their object identifier is equal or are two objects equal if their values are equal? The OCL semantics is not specific here since equality is defined as equality over values [41, Sec. A.2.2], and since objects are values, but object identifiers are not distinguished from object values [41, Definition A.10]. However, since many object-oriented programming languages are centered around referential equality (which gave the motivation to opt for the latter in [7]), HOL-OCL can be configured such that the above definition leads to referential equality.

non-referential: here objects are just identified with their values, i.e., two objects are equal if and only if all their attributes are equal.

referential universe: here a referential equality is present, which is the strong equality for “boxed types” (that is Real, Boolean, String) and an equality on the reference to a value.

---

More precise, HOL-OCL is build on top of Isabelle/HOL/Complex but only to support real numbers. If you don’t need them, HOL-OCL should be build just fine on top of a plain Isabelle/HOL.
Appendix B. Isabelle Theories

Figure B.1.: Session Graph
This manual describes HOL-OCL with referential universes. We recommend the use of referential universes.

This option has effects on the theory OCL_OclAny_type.

Collections: OCL [4] Sec. A.2.5.2] allows for collections to include ⊥, i.e. the constructor of sets and the membership tests are non-strict. This has several undesired consequences for executability and proof support. Thus we provide two collection libraries:

smashed collections: smashing data-structures is a key-concept in denotational semantics [35] [54]. For example, pairs are smashed if (a, ⊥) is identified with ⊥ as in e.g. Java or SML or, with respect to sets, {a, ⊥} = ⊥.

unsmashed collections: In this configuration all collection types can contain the element ⊥.

This manual describes HOL-OCL with smashed collections. We recommend the use of smashed collections.

This option has effects on the following theories: OCL_Bag.thy, OCL_OrderedSet.thy, OCL_Set.thy, OCL_Bag_type.thy, OCL_OrderedSet_type.thy, OCL_Set_type.thy, OCL_CharacteristicSet.thy, OCL_Sequence.thy, OCL_Collection_requirements.thy, and OCL_Sequence_type.thy.

The “recommended configuration” is more developed and contains more deductive support.

B.1.2. Notational Remarks

For presentational reasons, we used in the previous chapters for a few constructs a “Formal Syntax” that looks somewhat more “mathematical” than the syntax of Isabelle. To help readers that are not familiar with the syntax of Isabelle/HOL we compare the (already introduced) “Formal Syntax” with the Isabelle syntax used in this chapter in Table B.1.

B.2. Overview

The remainder of this chapter are the Isabelle theories using the \LaTeX-based presentation facilities of Isabelle. We structured the theory presentation in this chapter into the following subsections:

Foundations: In this section, we introduce the foundations of HOL-OCL, namely the concept of lifting and the basic datatype definitions.

Library: In this section, we introduce the OCL datatypes presented in [41] Chapter 11 and prove basic properties over them. Especially, we prove that our definitions fulfill the requirements presented in the OCL standard [41] Chapter 11.
Appendix B, Isabelle Theories

### Formal Syntax vs. Isabelle Syntax

<table>
<thead>
<tr>
<th>Formal Syntax</th>
<th>Isabelle Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ A_1 \ldots A_n ] \implies C ]</td>
<td>[ [A_1; \ldots; A_n] \implies C ]</td>
</tr>
<tr>
<td>[ \text{sumCase}(f, g, x) = \begin{cases} f(k) &amp; \text{if } x = \text{Inl} \ k \ g(k) &amp; \text{if } x = \text{Inr} \ k \end{cases} ]</td>
<td>[ \text{case } x \text{ of Inl } k \implies f(k)</td>
</tr>
<tr>
<td>[ \text{upCase}(f, c, x) = \begin{cases} c &amp; \text{if } x = \bot \ f(k) &amp; \text{if } x = k \downward \end{cases} ]</td>
<td>[ \text{case } x \text{ of } k \downward \implies f(k)</td>
</tr>
<tr>
<td>[ V_x(\alpha) ]</td>
<td>[ (r, \alpha) \text{ VAL} ]</td>
</tr>
<tr>
<td>[ \text{Sem}[(_)] ]</td>
<td>[ \text{semfun } _ ]</td>
</tr>
</tbody>
</table>

Table B.1.: Comparison of the formal syntax and the Isabelle syntax

**State:** In this section, the concept of state and constructive concepts like proof calculi are presented.

**Requirements:** In this section, the proof (or disproof) of the requirements of [41, Chapter 11].

**OCL:** This section just contains the final OCL theory that should be used as basis for case studies, i.e., it it the HOL-OCL main theory.

### B.3. Foundations

#### B.3.1. The Theory of Lifting and its Combinators

```isabelle
theory Lifting
imports Main
begin

Besides the infrastructure for handling undefinedness, this theory also provides the basis for data type embedding smashing and context lifting including the generic core of theorems.

The main purpose of this theory is to provide a generic theory of undefinedness. The Isabelle standard mechanism for such a generic data type is the class mechanism. The standard method is to declare a class to which all related operations are associated.

**A Generic Theory of Undefinedness**

Since the very first OCL publications [39] explicit undefinedness is part of the language, both for the logic and the basic values, e.g., [39, 7.4.9 Undefined Values] states (this is similarity stated in [41, page 15]):

138
Whenever an OCL expression is being evaluated, there is a possibility that one or more of the queries in the expression are undefined. If this is the case, then the complete expression will be undefined. There are two exceptions to this for the Boolean operators:

- True OR-ed with anything is True
- False AND-ed with anything is False

The above two rules are valid irrespective of the order of the arguments and the above rules are valid whether or not the value of the other sub-expression is known.

(OCL Specification [39], page 7-11)

This requirement postulates the strictness of all operations (except for the logic) and rules out a modeling of undefinedness via Hilbert-Operators and underspecification (e.g., as done for Z [26] in Isabelle/HOL-Z [11]).

**classes**

\[
\text{bot0} \subseteq \text{ord}
\]

**consts**

\[
UU :: \alpha :: \text{bot0}
\]

**syntax**

\[
UU :: \alpha :: \text{bot0} \quad (\bot)
\]

**axclass**

\[
\text{bot} \subseteq \text{bot0}
\]

**nonEmpty**

\[
\exists x. x \neq \bot
\]

**constdefs**

\[
\text{DEF} :: \alpha :: \text{bot} \Rightarrow \text{bool}
\]

\[
\text{DEF} x \equiv (x \neq \bot)
\]

\[
\text{isStrict} :: (\alpha :: \text{bot} \Rightarrow \beta :: \text{bot}) \Rightarrow \text{bool}
\]

\[
isStrict f \equiv (f \bot = \bot)
\]

\[
\text{strictify} :: (\alpha :: \text{bot} \Rightarrow \beta :: \text{bot}) \Rightarrow \alpha \Rightarrow \beta
\]

\[
\text{strictify} f x \equiv \text{if } x = \bot \text{ then } \bot \text{ else } f x
\]

\[
\text{smash} :: ([\beta :: \text{bot}, \alpha :: \text{bot}] \Rightarrow \text{bool}, \alpha) \Rightarrow \alpha
\]

\[
\text{smash} f X \equiv \text{if } f \bot X \text{ then } \bot \text{ else } X
\]

**Semantic Constructions: Liftings, Functions, Products**

We introduce now the lifting construction (see Winskel [54, p.131]) by a type constructor defined as free data type:

**datatype**

\[
\alpha \text{ up} = \text{lift } \alpha \mid \text{down}
\]

**constdefs**

\[
\text{drop} :: \alpha \text{ up} \Rightarrow \alpha
\]
Appendix B. Isabelle Theories

drop x ≡ case x of lift v ⇒ v | down ⇒ ⊥ x. True

syntax
@lift :: 'α ⇒ 'α up (\_|_\}\
Lifting.drop :: 'α up ⇒ 'α (\^_\^)

syntax (xsymbols)
@lift :: 'α ⇒ 'α up (\_|_\)
Lifting.drop :: 'α up ⇒ 'α (\^_\^)

translations
|_a_ ⇒ lift a
|^a^ ⇒ drop a

instance up :: (zero) zero
  by intro_classes
instance up :: (one) one
  by intro_classes
instance up :: (plus) plus
  by intro_classes
instance up :: (minus) minus
  by intro_classes
instance up :: (times) times
  by intro_classes
instance up :: (inverse) inverse
  by intro_classes

Semantic Constructions: Liftings of Type Constructors

The class is then propagated across lifting, function space and cartesian products.

instance up :: (type) ord
  by intro_classes
arities up :: (type) bot
instance fun :: (type,ord) ord
  by intro_classes
arities fun :: (type,bot) bot
instance * :: (ord,ord) ord
  by intro_classes
instance + :: (ord,ord) ord
  by intro_classes
arities * :: (bot,bot) bot
arities + :: (bot,bot) bot

defs
UU_up_def[simp]: ⊥ ≡ down
UU\_fun\_def[simp]: \bot \equiv (\lambda x. \bot)

UU\_pair\_def[simp]: \bot \equiv (\bot, \bot)

UU\_sum\_def[simp]: \bot \equiv (\text{Inl} \bot)

\begin{verbatim}
instance \text{up} :: (type) bot
   by intro_classes

instance \text{fun} :: (type, bot) bot
   by intro_classes

instance * :: (bot, bot) bot
   by intro_classes

instance + :: (bot, bot) bot
   by intro_classes

Semantic Constructions Dealing with Context Lifting
\end{verbatim}

```
types (\tau, \bot) VAL = \tau \Rightarrow \bot

instance \text{fun}::(type,zero) zero
   by intro_classes

instance \text{fun}::(type,one) one
   by intro_classes

instance \text{fun}:: (type,plus) plus
   by intro_classes

instance \text{fun}:: (type,minus) minus
   by intro_classes

instance \text{fun}:: (type,times) times
   by intro_classes

instance \text{fun}:: (type,inverse) inverse
   by intro_classes

instance \text{fun}:: (type,ord) ord
   by intro_classes
```

constdefs
\begin{verbatim}
lift0 :: \alpha \Rightarrow (\tau, \alpha) VAL
lift0 \equiv \lambda c. \lambda s. c

lift1 :: (\alpha \Rightarrow \beta) \Rightarrow (\tau, \alpha) VAL \Rightarrow (\tau, \beta) VAL
lift1 \equiv (\lambda f X \tau. f (X \tau))

lift2 :: ([\alpha, \beta] \Rightarrow \gamma) \Rightarrow ([\tau, \alpha] VAL, [\tau, \beta] VAL) \Rightarrow ([\tau, \gamma] VAL
lift2 \equiv (\lambda f X Y \tau. f (X \tau) (Y \tau))

lift3 :: ([\alpha, \beta, \gamma] \Rightarrow \delta) \Rightarrow ([\tau, \alpha] VAL, [\tau, \beta] VAL, [\tau, \gamma] VAL) \Rightarrow [\tau, \delta] VAL
lift3 \equiv (\lambda f X Y Z \tau. f (X \tau) (Y \tau) (Z \tau))

\end{verbatim}

cp :: ([\tau, \alpha] VAL, \tau) \Rightarrow \beta \Rightarrow bool
cp(P) \equiv (\exists f. \forall X \tau. P X \tau = f (X \tau) \tau)
```

\begin{verbatim}
syntax
\end{verbatim}
Appendix B. Isabelle Theories

\[
\begin{align*}
lift0 &:: \alpha \Rightarrow (\tau, \alpha) \text{ VAL} \\
lift1 &:: (\alpha \Rightarrow (\tau, \beta) \Rightarrow (\sigma, \alpha) \text{ VAL } \Rightarrow (\sigma, \beta) \text{ VAL} \\
lift2 &:: (\tau, \alpha) \text{ VAL } \Rightarrow (\tau, \beta) \text{ VAL } \Rightarrow (\tau, \gamma) \text{ VAL} \\
lift3 &:: (\tau, \alpha) \text{ VAL } \Rightarrow (\tau, \beta) \text{ VAL } \Rightarrow (\tau, \gamma) \text{ VAL }
\end{align*}
\]

A Generic Theory of Undefinedness, Strictness, and Smashing

Lemma not_DEF_UU [simp]: \(\neg \text{DEF}(\bot)\)
by (simp (no_asm) add: DEF_def)

Lemma not_DEF_X: \((\neg \text{DEF} X) = (X = \bot)\)
by (simp (no_asm) add: DEF_def)

Lemma exists_DEF: \(\exists x. \text{DEF}(x)\)
by (simp add: DEF_def nonEmpty)

Lemma isStrict_strictify [simp]: isStrict(strictify f)
by (simp add: isStrict_def strictify_def)

Lemma strict2a_UU [simp]: strictify f \(\bot = \bot\)
by (simp (no_asm) add: strictify_def)

Lemma strict2b_UU [simp]: strictify f \(\bot X = \bot\)
by (simp (no_asm) add: strictify_def UU_fun_def)

Restrictiveness versus Definedness

Lemma DEF_strictify_DEF_args2 :
\[
\text{DEF } (\text{strictify } (\lambda x. \text{strictify } (f x)) X Y) \Rightarrow \text{DEF } X \land \text{DEF } Y
\]
apply (simp add: strictify_def DEF_def)
apply (case_tac X = \bot)
apply auto
done

Lemma DEF_strictify_DEF_fun :
\[
[ \forall X. \text{DEF}(f X) ; \text{DEF } X ] \Rightarrow \text{DEF(strictify } f X)
\]
by (simp add: strictify_def DEF_def)

Lemma DEF_strictify_DEF_args :
\[
\text{DEF(strictify } f X) \Rightarrow \text{DEF } f \land \text{DEF } X
\]
by (simp add: strictify_def DEF_def, auto)

142
B.3. Foundations

**Lemma** isStrict-compose :

\[ \text{isStrict } f \text{ isStrict } g \implies \text{isStrict } (f \circ g) \]

by \( \text{simp add: isStrict_def o_def} \)

**Lemma** smash_strict (simp):

\[ \text{smash } f \bot = \bot \]

by \( \text{simp (no_asm add: smash_def)} \)

**Lemma** smashed_sets_nonempty (simp):

\[ \bot : \{X. \text{smash } f X = X\} \]

by \( \text{simp (no_asm)} \)

This lemmas are useful for proofs of non-emptiness of type-definition based on smashed collection types.

**A Theory of Undefinedness and Strictness in Lifted Types**

**Lemma** not_down_exists_lift :

\[ x \neq \text{down} = (\exists y. x = \downarrow y) \]

by \( \text{induct_tac } x, \text{auto} \)

**Lemma** not_down_exists_lift2 :

\[ x \neq \bot = (\exists y. x = \downarrow y) \]

by \( \text{induct_tac } x, \text{auto} \)

**Lemma** drop_lift (simp):

\[ \downarrow f = f \]

by \( \text{simp add: drop_def UU_up_def} \)

**Lemma** drop_down (simp):

\[ \downarrow \bot = (\epsilon x. \text{True}) \]

by \( \text{simp add: drop_def} \)

**Lemma** drop_down2 (simp):

\[ \downarrow \text{down} = (\epsilon x. \text{True}) \]

by \( \text{simp add: drop_def} \)

**Lemma** not_DEF_down (simp):

\[ \neg \text{DEF} (\text{down}) \]

by \( \text{simp (no_asm add: DEF_def)} \)

**Lemma** DEF_lift (simp):

\[ \text{DEF} (\downarrow x) \]

by \( \text{simp (no_asm add: DEF_def)} \)

**Lemma** DEF_X_up :

\[ \text{DEF}(X::'a up) = (\exists x. X = \downarrow x) \]

by \( \text{simp add: not_down_exists_lift DEF_def} \)

**Lemma** not_DEF_X_up :

\[ \neg \text{DEF}(X::'a up) = (X = \bot) \]

by \( \text{simp (no_asm add: DEF_def)} \)

**Lemma** DEF_fun_lift (simp):

\[ \text{DEF}(\lambda x. f x) \]
Appendix B. Isabelle Theories

apply (simp (no_asm) add: DEF_def)
apply (rule notI)
apply (drule fun_cong)
apply simp
done

lemma DEF_fun_fun_lift [simp]: DEF (λ x y. f x y)
apply (simp (no_asm) add: DEF_def)
apply (rule notI)
apply (drule fun_cong)
apply (drule fun_cong)
apply simp
done

lemma lift_defined : ⊥∉ X → X ≠ ⊥
  by (auto)

A Generic Theory of Strictness

lemma strict2c_UU [simp]: strictify f down = down
  by (simp (no_asm) add: strictify_def)

lemma strict2d_UU [simp]: strictify f down X = down
  by (simp (no_asm) add: strictify_def)

lemma strict2e_UU [simp]: strictify (λ x. strictify (f x)) (X::′α::bot) ⊥ = ⊥
  by (simp add: strictify_def)

lemma strict2f_UU [simp]: strictify (λ x. strictify (f x)) (X::′α::bot) down = down
  by (simp add: strictify_def)

lemma strict2_DEF [simp]: DEF X ⇒ strictify f X = f X
  by (simp add: strictify_def, auto)

lemma strict3_DEF [simp]: DEF X; DEF Y ⇒ strictify(λ X. strictify (f X)) X Y = f X Y
  by (simp add: strictify_def, auto)

Generic Undefinedness-Reduction Rules for 2-Lifted Strict Operations

lemma lift1b_undef [simp]: lift1 (strictify f) ⊥ = ⊥
  by (simp add: lift1_def)

lemma lift2b_undef1a [simp]: lift2 (strictify(λ x. strictify(f x))) (X::′a::(′b::bot)) ⊥ = ⊥
  by (simp add: lift1_def lift2_def)

lemma lift2b_undef2a [simp]: lift2 (strictify(λ x. strictify(f x))) (X::′τ::(′b::bot)) ⊥ = ⊥
B.3. Foundations

by (simp add: lift1_def lift2_def)

lemma lift1_undef_fw: \( g \equiv \text{lift1}(\text{strictify } f) \Rightarrow g \bot = \bot \)
by (simp del: UU_fun_def)

lemma lift2_undef1_fw: \( g \equiv \text{lift2}(\text{strictify}(\lambda x. \text{strictify}(f x))) \Rightarrow g \bot X = \bot \)
by (simp del: UU_fun_def)

lemma lift2_undef2_fw: \( g \equiv \text{lift2}(\text{strictify}(\lambda x. \text{strictify}(f x))) \Rightarrow g X \bot = \bot \)
by (simp del: UU_fun_def)

Generic Theorems on Context Lifted Combinators

lemma cp_charn: \([A \tau = B \tau; \text{cp } P] \Rightarrow P A \tau = P B \tau \)
by (auto simp: cp_def)

lemma cp_by_cpify: \(\text{cp } P = (\forall X \tau. P X \tau = P (\text{lift0} (X \tau)) \tau) \)
by (auto simp: cp_def lift0_def, rule exI, assumption)

lemma cp_lift0 simp, intro!: \(\text{cp}(\text{lift0} c) \)
by (simp add: cp_def lift0_def, fast)

lemma cp_eq simp, intro!: \(\text{cp} P \Rightarrow P \lambda u ub. P u ub = P' u ub \)
by (auto simp: cp_def)

lemma cp_const simp, intro!: \(\text{cp} (\lambda X. c) \)
by (simp add: cp_def, fast)

lemma cp_id simp, intro!: \(\text{cp} (\lambda X. X) \)
by (simp add: cp_def, fast)

lemma cp_compose simp, intro!: \(\text{cp} P \Rightarrow \text{cp} (P o P') \)
apply (simp add: cp_def o_def)
apply (erule exE)
apply (erule exE)
apply (simp (no_asm_simp))
apply fast
done

lemma cp_compose2: \([cp P; cp P'] \Rightarrow \text{cp} (\lambda x. P (P' x)) \)
by (simp add: cp_def o_def, auto)

lemma cp_lift1 simp: \(\text{cp} P \Rightarrow \text{cp} (\lambda X. \text{lift1} f (P X)) \)
apply (simp add: cp_def lift1_def)
Appendix B. Isabelle Theories

apply (erule exE)
apply (simp (no_asm_simp))
apply fast
done

lemma cp_lift2 [simp]:
  \[\text{cp } P;\; \text{cp } P' \implies \text{cp } (\lambda X. \text{lift}_2 \; f \; (P \; X) \; (P' \; X))\]
apply (simp add: cp_def lift2_def)
apply (erule exE)
apply (erule exE)
apply (simp (no_asm_simp))
apply fast
done

lemma cp_lift3 [simp]:
  \[\text{cp } P;\; \text{cp } P';\; \text{cp } P'' \implies \text{cp } (\lambda X. \text{lift}_3 \; f \; (P \; X) \; (P' \; X) \; (P'' \; X))\]
apply (simp add: cp_def lift3_def)
apply (erule exE)+
apply (simp (no_asm_simp))
apply fast
done

lemma cp_lift0/fw: \(f \equiv \text{lift}_0 \; g \implies \text{cp } f\)
by (simp add: lift0_def cp_def)

lemma cp_lift1/fw [simp]:
  \([f \equiv \text{lift}_1 \; g; \; \text{cp } P] \implies \text{cp } (\lambda X. \; f \; (P \; X))\]
by (simp add: cp_def lift1_def, auto)

lemma cp_lift2/fw :
  \([f \equiv \text{lift}_2 \; g; \; \text{cp } P; \; \text{cp } P'] \implies \text{cp } (\lambda X. \; f \; (P \; X) \; (P' \; X))\]
by (simp add: cp_def lift2_def, auto)

lemma cp_lift3/fw :
  \([f \equiv \text{lift}_3 \; g; \; \text{cp } P; \; \text{cp } P'; \; \text{cp } P''] \implies \text{cp } (\lambda X. \; f \; (P \; X) \; (P' \; X) \; (P'' \; X))\]
by (simp add: lift3_def cp_def,auto)

lemma ocl_undef_split : \(X \; \tau = \bot \vee (\exists \; a. \; X \; \tau = \langle a \rangle)\)
by (simp add: UU_up_def,simp add: not_down_exists_lift [symmetric])

lemma ocl_cp_undef_split: \([\text{cp } P; \; \text{cp } P'; \; \bot = P' \; \bot; \; X \neq \bot \implies \text{cp } P \; X = P' \; X]\]
\[\implies \text{cp } (P \; X = P' \; X)\]
B.3. Foundations

by (simp add: UU_fun_def, auto)

lemma ocl_cp_subst :
  \[ X \tau = X' \tau; P X \tau = C; cp P \] \[ \implies P X' \tau = C \]
by (simp add: cp_def, auto)

lemma ocl_cp_subst2 :
  \[ X \tau = X' \tau; P X' \tau = P' X' \tau; cp P; cp P' \] \[ \implies P X \tau = P' X \tau \]
by (simp add: cp_def, auto)

lemma ocl_cp_subst3 :
  \[ X \tau = X' \tau; P X' \tau = P' X' \tau; cp P; cp P' \] \[ \implies P X \tau = P' X \tau \]
by (simp add: cp_def, auto)

lemma drop_lift_idem simp: (\[ \begin{array} {c} x \end{array} \]) = x
by (simp_all split add: up.split)

lemma lift_drop_idem simp: [DEF(\[ x \])] = (\[ x \]) = x
apply (simp_all add: drop_def DEF_def not_down_exists_lift auto)
done

lemma DEF_set_charn : (\forall x \in X \cdot DEF x) = (\bot \notin X)
by (simp add: DEF_def, auto)

lemma cp_option_case :
[cp P; cp P'; cp (\lambda X \tau . (\lambda x. P'' x X \tau))] \[ \implies cp (\lambda X \tau . \text{case } (P X \tau) \text{ of } \text{None } \Rightarrow P' X \tau \mid \text{Some } x \Rightarrow P'' x X \tau) \]
apply (simp add: cp_def)
apply (auto)

apply (rule_tac x=\lambda C \tau . \text{case } (f C \tau) \text{ of } \text{None } \Rightarrow (fa C \tau) \mid \text{Some } x \Rightarrow (fb C \tau) x \text{ in exf})
apply (auto)
apply (rotate_tac 1)
apply (erule allE)
apply (rotate_tac -1)
apply (erule allE)
apply (rule sym)
apply (assumption)

apply (rule_tac t=\lambda x. P'' x X \tau \text{ in subst})
apply (rotate_tac 2)
apply (erule allE)

147
Appendix B. Isabelle Theories

apply (rotate_tac \-1)
apply (erule allE)
apply (rule sym)
apply (assumption)
apply (rule refl)
done

Higher-order Context-passingness

This theory is intended to develop higher-order rewriting for LJE-rewriting, i.e., rewriting in the body of iterators or quantifiers with respect to strong equality. This part of the theory is still under development.

constdefs

cp0 :: ((\'\tau, \'\alpha) VAL \rightarrow \'\beta) \Rightarrow bool
 cp0 P ≡ ∀ Q \tau. P Q \tau = P (lift0 (Q \tau)) \tau

cp1 :: ((\'\tau, \'\alpha) VAL \Rightarrow (\'\tau, \'\beta) VAL \Rightarrow (\'\tau, \'\gamma) VAL) \Rightarrow bool
 cp1 P ≡ ∀ Q \tau. P Q \tau = P (λ x. (lift0 (Q x \tau))) \tau

cp2 :: ((\'\tau, \'\alpha) VAL \Rightarrow (\'\tau, \'\beta) VAL \Rightarrow (\'\tau, \'\gamma) VAL \Rightarrow (\'\tau, \'\delta) VAL) \Rightarrow bool
 cp2 P ≡ ∀ Q \tau. P Q \tau = P (λ x y. (lift0 (Q x y \tau))) \tau

Building a ruleset to unfold all cp-ness definitions

lemmas ss_cp_defs = cp_def cp0_def cp1_def cp2_def

The functional behaviour of lift0. This rule is sometimes useful in a proof.

lemma lift0_apply: lift0 X \tau = X
by (simp add: lift0_def)

The rules to "cp-unfold" a term by hand

lemma cp0_unfold:
[ cp0 P; Q \tau = R \tau ] \Longrightarrow P Q \tau = P (lift0 (R \tau)) \tau
apply (unfold cp0_def, erule_tac x=Q in allE, erule_tac x=\tau in allE)
by (simp add: lift0_apply)

lemma cp1_unfold:
[ cp1 P; \\\(\lambda x. Q x \tau = R x \tau \) ] \Longrightarrow P Q \tau = P (λ x. lift0 (R x \tau)) \tau
apply (unfold cp1_def, erule_tac x=Q in allE, erule_tac x=\tau in allE)
by (simp add: lift0_apply)

lemma cp2_unfold:
[ cp2 P; \\\(\lambda x y. Q x y \tau = R x y \tau \) ] \Longrightarrow P Q \tau = P (λ x y. lift0 (R x y \tau)) \tau
apply (unfold cp2_def, erule_tac x=Q in allE, erule_tac x=\tau in allE)
by (simp add: lift0_apply)
The rules to “cp-fold” a term by hand

**Lemma cp0_fold:**
\[
\text{cps} \begin{array}{l}
P; \ Q \tau = R \tau \\
\end{array} \Rightarrow P (\text{lift}_0 \ (Q \tau)) \tau = P R \tau \\
\text{by (erule cp0_unfold[symmetric], simp)}
\]

**Lemma cp1_fold:**
\[
\text{cps} \begin{array}{l}
\forall x. \ Q x \tau = R x \tau \\
\end{array} \Rightarrow P \ (\lambda x. \text{lift}_0 \ (Q x \tau)) \tau = P R \tau \\
\text{by (erule cp1_unfold[symmetric], simp)}
\]

**Lemma cp2_fold:**
\[
\text{cps} \begin{array}{l}
\forall x \ y. \ Q x y \tau = R x y \tau \\
\end{array} \Rightarrow P \ (\lambda x y. \text{lift}_0 \ (Q x y \tau)) \tau = P R \tau \\
\text{by (erule cp2_unfold[symmetric], simp)}
\]

Rules to Establish cp

**Lemma cp0_const [simp]:**
\[
\text{cp0} \ (\lambda x. \ P) \\
\text{by (simp add: cp0_def)}
\]

**Lemma cp0_id [simp]:**
\[
\text{cp0} \ (\lambda x. \ x) \\
\text{by (simp add: cp0_def lift0_apply)}
\]

**Lemma cp0_app:**
\[
\text{cp0} \ (\lambda x. \ P x y) \\
\text{cp0} \ (\lambda x. \ P x) \\
\text{cp0} \ (\lambda x. \ P x x) \\
\text{apply (unfold cp0_def, clarify)} \\
\text{apply (rule trans, rule_tac P = (\lambda x. \ P x ?Y) and \tau=\tau in cp0_unfold)} \\
\text{apply (erule cp0_1_P, refl)} \\
\text{apply (erule cp0_2_P, refl)} \\
\text{apply (rule refl)} \\
\text{done}
\]

**Lemma cp0_of_cp0:**
\[
\text{cp0} \ (\lambda x. \ Q x) \\
\text{cp0} \ (\lambda x. \ P x) \\
\text{cp0} \ (\lambda x. \ P (Q x)) \\
\text{apply (unfold cp0_def, clarify)} \\
\text{apply (rule sym, rule trans, rule_tac P = (\lambda x. \ P x) and \tau=\tau in cp0_unfold)} \\
\text{apply (erule cp0_P, refl)} \\
\text{apply (rule_tac P = (\lambda x. \ Q x) and \tau=\tau in cp0_fold)} \\
\text{apply (rule cp0_Q, refl)} \\
\text{apply (rule refl)} \\
\text{done}
\]
Appendix B. Isabelle Theories

lemma cp0_of_cp1:
  assumes cp1_P: cp1 P
  and cp0_1_Q: \( \forall a. \text{cp0} (\lambda x. Q x a) \)
  shows \( \text{cp0} (\lambda x. P (Q x)) \)
  apply (unfold cp0_def, clarify)
  apply (rule trans, rule_tac P=(\lambda x. P x) and \( \tau=\tau \) in cp1_unfold)
  apply (rule cp1_P, rule refl)
  done

lemma cp0_of_cp2:
  assumes cp2_P: cp2 P
  and cp0_1_Q: \( \forall a b. \text{cp0} (\lambda x. Q x a b) \)
  shows \( \text{cp0} (\lambda x. P (Q x ?X ?Y)) \)
  apply (unfold cp0_def, clarify)
  apply (rule trans, rule_tac P=(\lambda x. P x) and \( \tau=\tau \) in cp2_unfold)
  apply (rule cp2_P, rule refl)
  done

In the following, we prove the cp1 rules.

lemma cp1_const [simp]: cp1 \( (\lambda x. P) \)
  by (simp add: cp1_def)

This rule corresponds to cp0_id. It has the same structure except for the constant evaluation which is of course not needed for a nullary argument.

lemma cp1_const_eval [simp]: cp1 \( (\lambda x. x X) \)
  by (simp add: cp1_def lift0_apply)

lemma cp1_app:
  assumes cp1_1_P: \( \forall y. \text{cp1} (\lambda x. (P x y)) \)
  and cp1_2_P: \( \forall x. \text{cp1} (P x) \)
  shows \( \text{cp1} (\lambda x. P x x) \)
  apply (unfold cp1_def, clarify)
  apply (rule trans, rule_tac P=(\lambda x. P x ?Y) and \( \tau=\tau \) in cp1_unfold)
  apply (rule cp1_1_P, rule refl)
  apply (rule refl)
  done
lemma \textit{cp1_of_cp0}:
assumes \textit{cp0\_P}: \textit{cp0 P}
and \textit{cp1\_Q}: \textit{cp1 Q}
shows \textit{cp1 (λ x. \textit{P (Q x)})}
apply(unfold \textit{cp1\_def}, clarify)
apply(rule trans, rule_tac \textit{P=(λ x. \textit{P x}) and \textit{τ=τ in cp0\_unfold}})
apply(rule \textit{sym}, rule trans, rule_tac \textit{P=(λ x. \textit{P x}) and \textit{τ=τ in cp0\_unfold}})
apply(rule \textit{cp0\_P}, rule refl)
apply(rule sym, rule trans, rule_tac \textit{P=(λ x. \textit{P x}) and \textit{τ=τ in cp0\_fold}})
apply(rule \textit{cp0\_P})
apply(rule refl)
done

lemma \textit{cp1_of_cp1}:
assumes \textit{cp1\_P}: \textit{cp1 P}
and \textit{cp1\_1\_Q}: \forall a. \textit{cp1 (λ x. \textit{Q x a})}
shows \textit{cp1 (λ x. \textit{P (Q x)})}
apply(unfold \textit{cp1\_def}, clarify)
apply(rule trans, rule_tac \textit{P=(λ x. \textit{P x}) and \textit{τ=τ in cp1\_unfold}})
apply(rule \textit{sym}, rule trans, rule_tac \textit{P=(λ x. \textit{P x}) and \textit{τ=τ in cp1\_unfold}})
apply(rule \textit{cp1\_P}, rule refl)
apply(rule sym, rule trans, rule_tac \textit{P=(λ x. \textit{P x}) and \textit{τ=τ in cp1\_fold}})
apply(rule \textit{cp1\_P})
apply(rule sym, rule trans, rule_tac \textit{P=(λ x. \textit{P x}) and \textit{τ=τ in cp1\_fold}})
apply(rule \textit{cp1\_P})
apply(rule refl)
done

lemma \textit{cp1_of_cp2}:
assumes \textit{cp2\_P}: \textit{cp2 P}
and \textit{cp1\_1\_Q}: \forall a b. \textit{cp1 (λ x. \textit{Q x a b})}
shows \textit{cp1 (λ x. \textit{P (Q x)})}
apply(unfold \textit{cp1\_def}, clarify)
apply(rule trans, rule_tac \textit{P=(λ x. \textit{P x}) and \textit{τ=τ in cp2\_unfold}})
apply(rule \textit{sym}, rule trans, rule_tac \textit{P=(λ x. \textit{P x}) and \textit{τ=τ in cp2\_unfold}})
apply(rule \textit{cp2\_P}, rule refl)
apply(rule sym, rule trans, rule_tac \textit{P=(λ x. \textit{P x}) and \textit{τ=τ in cp2\_fold}})
apply(rule \textit{cp2\_P})
apply(rule sym, rule trans, rule_tac \textit{P=(λ x. \textit{P x}) and \textit{τ=τ in cp2\_fold}})
apply(rule \textit{cp1\_1\_Q}, rule refl)
apply(rule refl)
done

\textit{cp2 rules}

lemma \textit{cp2\_const \_simp}: \textit{cp2 (λ x. \textit{x \_P})}
by(simp add: \textit{cp2\_def})

lemma \textit{cp2\_const\_eval \_simp}: \textit{cp2 (λ x. \textit{x \_X \textit{Y})}
by(simp add: \textit{cp2\_def lift0\_apply})
Appendix B. Isabelle Theories

lemma cp2_app:
  assumes cp2_1_P: \( \forall y. \text{cp2}(\lambda x. (P x y)) \)
  and cp2_2_P: \( \forall x. \text{cp2}(P x) \)
  shows \( \text{cp2}(\lambda x. P x x) \)
  apply (unfold cp2_def, clarify)
  apply (rule trans, rule_tac P=\( \lambda x. P x ?Y \) and \( \tau=\tau \) in cp2_unfold)
  apply (rule_tac P=\( \lambda x. P ?X x \) and \( \tau=\tau \) in cp2_unfold)
  apply (rule refl)
  done

lemma cp2_of_cp0:
  assumes cp0_P: \( \text{cp0}(P) \)
  and cp2_Q: \( \text{cp2}(Q) \)
  shows \( \text{cp2}(\lambda x. P(Q x)) \)
  apply (unfold cp2_def, clarify)
  apply (rule trans, rule_tac P=\( \lambda x. P x \) and \( \tau=\tau \) in cp0_unfold)
  apply (rule_tac P=\( \lambda x. P x \) and \( \tau=\tau \) in cp0_unfold)
  apply (rule sym, rule trans, rule_tac P=\( \lambda x. P x \) and \( \tau=\tau \) in cp0_unfold)
  apply (rule cp0_P)
  apply (rule_tac P=\( \lambda x. Q x \) and \( \tau=\tau \) in cp2_fold)
  apply (rule refl)
  done

lemma cp2_of_cp1:
  assumes cp1_P: \( \text{cp1}(P) \)
  and cp2_1_Q: \( \forall a b. \text{cp2}(\lambda x. Q x a b) \)
  shows \( \text{cp2}(\lambda x. P(Q x)) \)
  apply (unfold cp2_def, clarify)
  apply (rule trans, rule_tac P=\( \lambda x. P x \) and \( \tau=\tau \) in cp1_unfold)
  apply (rule_tac P=\( \lambda x. P x \) and \( \tau=\tau \) in cp1_unfold)
  apply (rule sym, rule trans, rule_tac P=\( \lambda x. P x \) and \( \tau=\tau \) in cp1_unfold)
  apply (rule cp1_P)
  apply (rule_tac P=\( \lambda x. Q x ?X \) and \( \tau=\tau \) in cp2_fold)
  apply (rule cp2_1_Q, rule refl)
  apply (rule refl)
  done

lemma cp2_of_cp2:
  assumes cp2_P: \( \text{cp2}(P) \)
  and cp2_1_Q: \( \forall a b. \text{cp2}(\lambda x. Q x a b) \)
  shows \( \text{cp2}(\lambda x. P(Q x)) \)
  apply (unfold cp2_def, clarify)
  apply (rule trans, rule_tac P=\( \lambda x. P x \) and \( \tau=\tau \) in cp2_unfold)
  apply (rule_tac P=\( \lambda x. P x \) and \( \tau=\tau \) in cp2_unfold)
  apply (rule sym, rule trans, rule_tac P=\( \lambda x. P x \) and \( \tau=\tau \) in cp2_unfold)
  apply (rule cp2_P)
B.3. Foundations

apply (rule_tac P = (\lambda x. Q x ?X ?Y) and \tau = \tau in cp2_fold)
apply (rule cp2_1_Q, rule refl)
apply (rule refl)
done

Deciding cp using cp_unfold

By converting a term into explicit cp-representation one can also decide all context-pasingness questions. Since the tactic uses a stepwise unfolding it can deal with cases where simp combined with chain rules for cp-ness does not work. These are cases where currently the rule cp_compose2 is applied by hand. The decision using cp_unfold works as follows:

1. apply cp_unfold
2. if one of the rules cp0_cp_unfolded, cp1_cp_unfolded, or cp2_cp_unfolded matches were done otherwise the cp-ness proposition is false (assuming that the simpset of cp_unfold is complete with respect to the set of OCL operations)

lemma cp0_cp_unfolded:
cp0 (\lambda x. P (lift0 (\tau x)) \tau)
by (simp add: cp0_def lift0_apply)

lemma cp1_cp_unfolded:
cp1 (\lambda Q. P (\lambda x. lift0 (Q x)) \tau)
by (simp add: cp1_def lift0_apply)

lemma cp2_cp_unfolded:
cp2 (\lambda Q. P (\lambda x y. lift0 (Q x y)) \tau)
by (simp add: cp2_def lift0_apply)

Higher-Order lifting construction

constdefs
  lift1' :: [(\tau \Rightarrow \beta), \alpha \Rightarrow \beta, \gamma \Rightarrow \eta] \Rightarrow \gamma \Rightarrow \eta
  lift1' a1 \equiv (\lambda f x \tau. f (a1 x \tau))

  lift2' :: [(\alpha \Rightarrow \gamma, \beta \Rightarrow \gamma, \gamma \Rightarrow \eta)] \Rightarrow \alpha \Rightarrow \beta \Rightarrow \gamma \Rightarrow \eta
  lift2' a1 a2 \equiv (\lambda f x y \tau. f (a1 x f (a2 y \tau))

  lift3' :: [(\eta \Rightarrow \gamma, \alpha \Rightarrow \beta, \gamma \Rightarrow \delta)] \Rightarrow \gamma \Rightarrow \delta
  lift3' a1 a2 a3 \equiv (\lambda f x y z. f (a1 x f (a2 y f (a3 z \tau)))

  lift_arg0 :: (\tau \Rightarrow \beta) \Rightarrow (\tau \Rightarrow \beta)
  lift_arg0 \equiv id

  lift_arg1 :: ((\tau \Rightarrow \gamma) \Rightarrow (\tau \Rightarrow \delta)) \Rightarrow (\tau \Rightarrow (\gamma \Rightarrow \delta))
  lift_arg1 \equiv (\lambda f x \tau. f (lift0 x) \tau)
Appendix B. Isabelle Theories

\[
\begin{align*}
\text{lift\_arg2} &:: ([\alpha\Rightarrow\beta, \gamma\Rightarrow\delta]) \Rightarrow ([\eta, \alpha, \gamma] \Rightarrow \eta) \\
\text{lift\_arg2} &\equiv (\lambda f \tau x y. f (\text{lift}_0 x) (\text{lift}_0 y) \tau)
\end{align*}
\]

Rulesets to unfold the whole lifting constructions

\[
\text{lemmas ss\_lifting} = \text{lift1\_def lift2\_def lift3\_def} \\
\quad \text{lift1\_def lift2\_def lift3\_def} \\
\quad \text{lift\_arg0\_def lift\_arg1\_def lift\_arg2\_def} \\
\quad \text{DEF\_def strictify\_def isStrict\_def} \\
\quad \text{smash\_def}
\]

\[
\text{lemmas ss\_lifting\'} = \text{lift0\_def ss\_lifting}
\]

The Link to the old Combinator Set.

Note, \text{lift1}, \text{lift2}, \text{lift3} are special cases of these general combinators.

\[
\text{lemma lift1\_by\_lift1\': lift1} = (\text{lift1\'} lift_0)
\]
by(simp add: lift1\_def lift1\_def lift\_arg0\_def)

\[
\text{lemma lift2\_by\_lift2\': lift2} = (lift2\' lift_0 lift_0)
\]
by(simp add: lift2\_def lift2\_def lift\_arg0\_def)

\[
\text{lemma lift3\_by\_lift3\': lift3} = (lift3' lift_0 lift_0 lift_0)
\]
by(simp add: lift3\_def lift3'\_def lift\_arg0\_def)

Forward rules for the currently used constructions:

As we have in the section about \text{cp\_unfold}, transforming a term into explicit \text{cp}\-representation is very powerful. Its foundation is \text{cp\_unfold} which relies on a simplifier set containing all context-passingess predicates for every argument of every \text{OCL} operation. These set can be created by putting all forward rules from below whose first assumption is unifyable with the definition of the \text{OCL} function into this set.

The \text{fw\_OCL\_cp0\_chain} rules are the old \text{OCL\_cp} rules who can be put into the standard simplifier set.

Context-passingness by construction

ML \langle
\text{local}
val cpR\_prover\_simpset = simpset() addsimps ((thms ss\_lifting\') @ (thms ss\_cp\_defs))
\text{in}

fun cpR\_prover\_mk\_name (goal,arity,position,lifting) =
  let val \text{\_name, name\_prefix = mk\_name arity position lifting}
  val \text{thm = prove\_goalw (the\_context()) \[] goal}
  \text{(fn prems => \[ALLGOALS simp\_tac (cpR\_prover\_simpset
\text{end)}}
B.3. Foundations

```
addsrims prems))

in (store_thm(rname.thm), rname, name_prefix)
end
end

pointwise context-passingness rules

ML ⟨local

fun mk_name_cpR arity position lifting =
  let val name_prefix = OCL_cp ^ (Int.toString arity) ^ _
    ^ (Int.toString position) ^ _
in (fw_ ^ name_prefix ^ lifting, name_prefix) end
in
val cpR_thms = map (cpR_prover mk_name_cpR) [
(f ⊢ lift1 P ⇒ cp0 f, 0, 1, lift1),
(f ⊢ (lift1’ lift_arg0) P ⇒ cp0 f, 0, 1, lift1’),
(f ⊢ lift2 P ⇒ cp0 (λ x. f x Y), 0, 1, lift2),
(f ⊢ lift2 P ⇒ cp0 (λ x. f X x), 0, 2, lift2),
(f ⊢ (lift2’ lift_arg0 aY) P ⇒ cp0 (λ x. f x Y), 0, 1, lift2’),
(f ⊢ (lift2’ aX lift_arg0) P ⇒ cp0 (λ x. f X x), 0, 2, lift2’),
(f ⊢ (lift2’ aX lift_arg1) P ⇒ cp1 (λ x. f X x), 1, 2, lift2’),
(f ⊢ (lift2’ aX lift_arg2) P ⇒ cp2 (λ x. f X x), 2, 2, lift2’),
(f ⊢ lift3 P ⇒ cp0 (λ x. f x Y Z), 0, 1, lift3),
(f ⊢ lift3 P ⇒ cp0 (λ x. f X x Z), 0, 2, lift3),
(f ⊢ lift3 P ⇒ cp0 (λ x. f X x Z), 0, 3, lift3),
(f ⊢ (lift3’ lift_arg0 aY aZ) P ⇒ cp0 (λ x. f x Y Z), 0, 1, lift3’),
(f ⊢ (lift3’ aX lift_arg0 aZ) P ⇒ cp0 (λ x. f X x Z), 0, 2, lift3’),
(f ⊢ (lift3’ aX aY lift_arg0) P ⇒ cp0 (λ x. f X Y x), 0, 3, lift3’),
(f ⊢ (lift3’ aX aY lift_arg1 aZ) P ⇒ cp1 (λ x. f X x Z), 1, 2, lift3’),
(f ⊢ (lift3’ aX aY lift_arg2 aZ) P ⇒ cp2 (λ x. f X x Z), 2, 2, lift3’)
] end

pointwise cp_fold rules

ML ⟨local

fun mk_name_cpR_fold arity position lifting =
  let val name_prefix = OCL_cp ^ (Int.toString arity) ^ _fold_
    ^ (Int.toString position) ^ _
in (fw_ ^ name_prefix ^ lifting, name_prefix) end
in
val cpR_fold_thms = map (cpR_prover mk_name_cpR_fold) [
(f ⊢ lift1 P ⇒ f (lift0 (X τ)) τ = f X τ, 0, 1, lift1),
```

155
Appendix B. Isabelle Theories

(f ≡ (lift1' lift_arg0) P \Rightarrow f (lift0 (X \tau)) \tau = f X \tau, 0, 1, lift1'),

(f ≡ lift2 P \Rightarrow f (lift0 (X \tau)) Y \tau = f X Y \tau, 0, 1, lift2),
(f ≡ lift2 P \Rightarrow f X (lift0 (Y \tau)) \tau = f X Y \tau, 0, 2, lift2),

(f ≡ (lift2' lift_arg0 aY) P \Rightarrow f (lift0 (X \tau)) Y \tau = f X Y \tau, 0, 1, lift2'),
(f ≡ (lift2' aX lift_arg0) P \Rightarrow f X (lift0 (Y \tau)) \tau = f X Y \tau, 0, 2, lift2'),
(f ≡ (lift2' aX lift_arg1) P \Rightarrow f X (\lambda x. lift0 (Y x \tau)) \tau = f X Y \tau, 1, 2, lift2'),
(f ≡ (lift2' aX lift_arg2) P \Rightarrow f X (\lambda x y. lift0 (Y x y \tau)) \tau = f X Y \tau, 2, 2, lift2').

(f ≡ lift3 P \Rightarrow f (lift0 (X \tau)) Y Z \tau = f X Y Z \tau, 0, 1, lift3),
(f ≡ lift3 P \Rightarrow f X (lift0 (Y \tau)) Z \tau = f X Y Z \tau, 0, 2, lift3),
(f ≡ lift3 P \Rightarrow f X Y (lift0 (Z \tau)) \tau = f X Y Z \tau, 0, 3, lift3),

(f ≡ (lift3' lift_arg0 aY aZ) P \Rightarrow f (lift0 (X \tau)) Y Z \tau = f X Y Z \tau, 0, 1, lift3'),
(f ≡ (lift3' aX lift_arg0 aZ) P \Rightarrow f X (lift0 (Y \tau)) Z \tau = f X Y Z \tau, 0, 2, lift3'),
(f ≡ (lift3' aX aY lift_arg0) P \Rightarrow f X Y (lift0 (Z \tau)) \tau = f X Y Z \tau, 0, 3, lift3'),
(f ≡ (lift3' aX lift_arg2 aZ) P \Rightarrow f X (\lambda x y. lift0 (Y x y \tau)) Z \tau = f X Y Z \tau, 2, 2, lift3').

Unary OCL operations: old lifting construction.

lemma fw_OCL_cp0_chain0_lift1:
  assumes f_def: f ≡ lift1 P
  and cp0_X: cp0 X
  shows cp0 (\lambda x. f (X x))
  by(insert cp0_X, simp add: f_def cp0_def lift1_def lift0_apply)

lemma fw_OCL_cp0_chain0_lift1):
  assumes f_def: f ≡ (lift1' lift_arg0) P
  and cp0_X: cp0 X
  shows cp0 (\lambda x. f (X x))
  by(insert cp0_X, simp add: f_def cp0_def lift_arg0_def lift1'_def lift0_apply)

Binary OCL operations: old lifting construction.

lemma fw_OCL_cp0_chain00_lift2:
  assumes f_def: f ≡ lift2 P
  and cp0_X: cp0 X
  and cp0_Y: cp0 Y
  shows cp0 (\lambda x. f (X x) (Y x))
  by(insert cp0_X cp0_Y,
       simp add: f_def cp0_def lift2_def lift0_apply)
lemma fw_OCL_cp0_chain00_lift2':
assumes f_def: f \equiv (lift2' lift_arg0 lift_arg0) P
and \( cp0_X : cp0 X \)
and \( cp0_Y : cp0 Y \)
shows \( cp0 (\lambda x. f (X x) (Y x)) \)
by (insert cp0_X cp0_Y,
simp add f_def cp0_def lift_arg0_def lift2'_def lift0_apply)

lemma fw_OCL_cp0_chain01_lift2':
assumes f_def: f \equiv (lift2' lift_arg0 lift_arg1) P
and \( cp0_X : cp0 X \)
and \( \forall a. cp0 (\lambda x. Y x a) \)
shows \( cp0 (\lambda x. f (X x) (Y x)) \)
by (insert cp0_X cp0_Y,
simp add f_def cp0_def lift_arg0_def lift_arg1_def lift2'_def lift0_apply)

lemma fw_OCL_cp0_chain02_lift2':
assumes f_def: f \equiv (lift2' lift_arg0 lift_arg2) P
and \( cp0_X : cp0 X \)
and \( \forall a b. cp0 (\lambda x. Y x a b) \)
shows \( cp0 (\lambda x. f (X x) (Y x)) \)
by (insert cp0_X cp0_Y,
simp add f_def cp0_def lift_arg0_def lift_arg2_def lift2'_def lift0_apply)

Tertiary OCL operations: \texttt{->iterate} and \texttt{if}.

lemma fw_OCL_cp0_chain000_lift3:
assumes f_def: f \equiv lift3 P
and \( cp0_X : cp0 X \)
and \( cp0_Y : cp0 Y \)
and \( cp0_Z : cp0 Z \)
shows \( cp0 (\lambda x. f (X x) (Y x) (Z x)) \)
by (insert cp0_X cp0_Y cp0_Z,
simp add f_def cp0_def lift3_def lift0_apply)

lemma fw_OCL_cp0_chain000_lift3':
assumes f_def: f \equiv (lift3' lift_arg0 lift_arg0 lift_arg0) P
and \( cp0_X : cp0 X \)
and \( cp0_Y : cp0 Y \)
and \( cp0_Z : cp0 Z \)
shows \( cp0 (\lambda x. f (X x) (Y x) (Z x)) \)
by (insert cp0_X cp0_Y cp0_Z,
simp add f_def cp0_def lift_arg0_def lift3'_def lift0_apply)

lemma fw_OCL_cp0_chain020_lift3':
assumes f_def: f \equiv (lift3' lift_arg0 lift_arg2 lift_arg0) P
and \( cp0_X : cp0 X \)
and \( \forall a b. cp0 (\lambda x. Y x a b) \)
and \( cp0_Z : cp0 Z \)
shows \( cp0 (\lambda x. f (X x) (Y x) (Z x)) \)
Appendix B. Isabelle Theories

by (insert cp0_X cp0_Y cp0_Z, simp add: f_def cp0_def lift_arg0_def lift_arg2_def lift3_def)

Chain rules for \( cp \) usable by \texttt{simp} or \texttt{fast}.

Unary OCL operations: old lifting construction.

lemma \( \texttt{fw}\_\texttt{OCL}\_\texttt{cp}\_\texttt{chain0} \_\texttt{lift1} \!\!: \)
assumes \( f \equiv (\texttt{lift1} \!\! \texttt{lift}\_\texttt{arg0}) \ P \)
and \( \texttt{cp}\_\texttt{X} \!: \texttt{cp} \ X \)
shows \( \texttt{cp} \ (\lambda \ x. \ f \ (X \ x)) \)
by (insert \( \texttt{cp}\_\texttt{X} \), simp add: \texttt{f_def} \texttt{cp_by_cpify} \texttt{lift_arg0_def} \texttt{lift0_apply})

Binary OCL operations: old lifting construction.

lemma \( \texttt{fw}\_\texttt{OCL}\_\texttt{cp}\_\texttt{chain00} \_\texttt{lift2} \!\!: \)
assumes \( f \equiv (\texttt{lift2} \!\! \texttt{lift}\_\texttt{arg0} \texttt{lift}\_\texttt{arg0}) \ P \)
and \( \texttt{cp}\_\texttt{X} \!: \texttt{cp} \ X \)
and \( \texttt{cp}\_\texttt{Y} \!: \texttt{cp} \ Y \)
shows \( \texttt{cp} \ (\lambda \ x. \ f \ (X \ x) \ (Y \ x)) \)
by (insert \( \texttt{cp}\_\texttt{X} \texttt{cp}\_\texttt{Y} \), simp add: \texttt{f_def} \texttt{cp_by_cpify} \texttt{lift_arg0_def} \texttt{lift0_apply})

lemma \( \texttt{fw}\_\texttt{OCL}\_\texttt{cp}\_\texttt{chain01} \_\texttt{lift2} \!\!: \)
assumes \( f \equiv (\texttt{lift2} \!\! \texttt{lift}\_\texttt{arg0} \texttt{lift}\_\texttt{arg1}) \ P \)
and \( \texttt{cp}\_\texttt{X} \!: \texttt{cp} \ X \)
and \( \texttt{cp}\_\texttt{Y} \!: \lambda \ a. \texttt{cp} \ (\lambda \ x. \ Y \ x \ a) \)
shows \( \texttt{cp} \ (\lambda \ x. \ f \ (X \ x) \ (Y \ x)) \)
by (insert \( \texttt{cp}\_\texttt{X} \texttt{cp}\_\texttt{Y} \), simp add: \texttt{f_def} \texttt{cp_by_cpify} \texttt{lift_arg0_def} \texttt{lift2_def} \texttt{lift0_apply})

lemma \( \texttt{fw}\_\texttt{OCL}\_\texttt{cp}\_\texttt{chain02} \_\texttt{lift2} \!\!: \)
assumes \( f \equiv (\texttt{lift2} \!\! \texttt{lift}\_\texttt{arg0} \texttt{lift}\_\texttt{arg2}) \ P \)
and \( \texttt{cp}\_\texttt{X} \!: \texttt{cp} \ X \)
and \( \texttt{cp}\_\texttt{Y} \!: \lambda \ a \ b. \texttt{cp} \ (\lambda \ x. \ Y \ x \ a \ b) \)
shows \( \texttt{cp} \ (\lambda \ x. \ f \ (X \ x) \ (Y \ x)) \)
by (insert \( \texttt{cp}\_\texttt{X} \texttt{cp}\_\texttt{Y} \), simp add: \texttt{f_def} \texttt{cp_by_cpify} \texttt{lift_arg0_def} \texttt{lift2_def} \texttt{lift0_apply})

Tertiary OCL operations: \( \texttt{iterate} \) and \( \texttt{if} \).

lemma \( \texttt{fw}\_\texttt{OCL}\_\texttt{cp}\_\texttt{chain000} \_\texttt{lift3} \!\!: \)
assumes \( f \equiv (\texttt{lift3} \!\! \texttt{lift}\_\texttt{arg0} \texttt{lift}\_\texttt{arg0} \texttt{lift}\_\texttt{arg0}) \ P \)
and \( \texttt{cp}\_\texttt{X} \!: \texttt{cp} \ X \)
and \( \texttt{cp}\_\texttt{Y} \!: \texttt{cp} \ Y \)
and \( \texttt{cp}\_\texttt{Z} \!: \texttt{cp} \ Z \)
shows \( \texttt{cp} \ (\lambda \ x. \ f \ (X \ x) \ (Y \ x) \ (Z \ x)) \)
by (insert \( \texttt{cp}\_\texttt{X} \texttt{cp}\_\texttt{Y} \texttt{cp}\_\texttt{Z} \), simp add: \texttt{f_def} \texttt{cp_by_cpify} \texttt{lift_arg0_def} \texttt{lift3_def} \texttt{lift0_apply})

lemma \( \texttt{fw}\_\texttt{OCL}\_\texttt{cp}\_\texttt{chain020} \_\texttt{lift3} \!\!: \)
assumes \( f \_\text{def} : f \equiv (\text{lift3} \\text{liftarg0} \\text{liftarg2} \\text{liftarg0}) \ P \)
and \( cp\_X : cp \ X \)
and \( cp\_Y : \forall \ a \ b. \ cp (\lambda \ x. \ Y \ x \ a \ b) \)
and \( cp\_Z : cp \ Z \)
shows \( cp (\lambda \ x. \ f (X \ x) (Y \ x) (Z \ x)) \)
by (insert \( cp\_X \ cp\_Y \ cp\_Z \),
\( \text{simp add: } f\_\text{def} \ cp\_by\_cpify \ \text{liftarg0}\_\text{def} \ \text{liftarg2}\_\text{def} \ \text{lift3}\_\text{def} \))

Note, ll of these rules are registered for the use with \text{ocl_setup_op} in the theory \text{OCLL\_Kernel}.

cp\( \theta \) is equivalent to what we already have with \( cp \). Thus it is currently added to the simpset to allow for a decision of \( cp\theta\)-questions based on the machinery already built for deciding \( cp\)-questions. This will change when the theories are cleaned up.

\textbf{Accessing Type Sums}

\textbf{constdefs}

\( \text{FromL} \) :: \((\alpha + \beta) \uparrow \Rightarrow \alpha \uparrow \)
\( \text{FromL} \ x \equiv \text{case} \ x \ \text{of} \ \text{lift} \ v \Rightarrow (\sum\_\text{case} (\lambda \ x. \ x) \ (\lambda \ x. \ down) \ v) \)
\( | \down \Rightarrow down \)

\textbf{constdefs}

\( \text{FromR} \) :: \((\alpha + \beta) \uparrow \Rightarrow \beta \uparrow \)
\( \text{FromR} \ x \equiv \text{case} \ x \ \text{of} \ \text{lift} \ v \Rightarrow (\sum\_\text{case} (\lambda x. \ x) \ (\lambda x. \ down) \ v) \)
\( | \down \Rightarrow down \)

\textbf{lemma} \text{FromL\_UU} [simp]: \text{FromL} \ \bot = \bot
by (simp add: \text{FromL\_def} )

\textbf{lemma} \text{FromR\_UU} [simp]: \text{FromR} \ \bot = \bot
by (simp add: \text{FromR\_def} )

\textbf{lemma} \text{FromL\_down} [simp]: \text{FromL} \ down = \down
by (simp add: \text{FromL\_def} )

\textbf{lemma} \text{FromR\_down} [simp]: \text{FromR} \ down = \down
by (simp add: \text{FromR\_def} )

\textbf{lemma} \text{FromL\_lift\_Inl\_id} [simp]: \text{FromL} \ \text{Inl} \ x = x
by (simp add: \text{FromL\_def} )

\textbf{lemma} \text{FromR\_lift\_Inr\_id} [simp]: \text{FromR} \ \text{Inr} \ x = \text{lift} \ x
by (simp add: \text{FromR\_def} )

\textbf{lemma} \text{FromR\_Inl\_UU} [simp]: \text{FromR} \ \text{Inl} \ x = \bot

159
Appendix B. Isabelle Theories

by (simp add: FromR_def)

lemma FromL_Inr_UU [simp]: FromL \(\mathbf{L} \mathbf{L} x \mathbf{L} = \perp\)
by (simp add: FromL_def)

lemma h1: DEF (FromL(x)) \(\implies\) \(\mathbf{L} \mathbf{L} \mathbf{L} x \mathbf{L} = x\)
apply (simp add: FromL_def lift_drop_idem)
apply (case_tac x, simp add: lift_drop_idem drop_lift_idem, auto)
done

lemma h2: DEF (FromL(x)) \(\implies\) \(\mathbf{L} \mathbf{L} \mathbf{L} x \mathbf{L} = \mathbf{L} \mathbf{L} x \mathbf{L}\)
apply (simp add: FromL_def)
apply (case_tac x, simp add: lift_drop_idem drop_lift_idem, auto)
done

lemma DEF_FromL_exists_Inl: DEF (FromL x) = \(\exists\ y. x = \mathbf{L} \mathbf{L} \mathbf{L} y \mathbf{L}\)
apply (simp add: FromL_def)
apply (case_tac x, simp, auto)
done

lemma DEF_FromR_exists_drop_Inr: DEF (FromR x) = \(\exists\ y. x = \mathbf{L} \mathbf{L} \mathbf{L} y \mathbf{L}\)
apply (simp add: FromR_def lift_drop_idem)
apply (case_tac x, simp add: lift_drop_idem drop_lift_idem, auto)
done

lemma FromL_Inl_inv [simp]: (FromL \(\mathbf{L} \mathbf{L} x \mathbf{L} = \mathbf{L} \mathbf{L} X \mathbf{L}\)) = \(X = \mathbf{L} \mathbf{L} x \mathbf{L}\)
apply (auto)
done

lemma FromR_Inr_inv [simp]: (FromR \(\mathbf{L} \mathbf{L} x \mathbf{L} = \mathbf{L} \mathbf{L} X \mathbf{L}\)) = \(X = \mathbf{L} \mathbf{L} x \mathbf{L}\)
apply (auto)
done

lemma Inv_FromR_drop: DEF (FromR(x)) \(\implies\) Inv \(\mathbf{L} \mathbf{L} \mathbf{L} x \mathbf{L} = \mathbf{L} \mathbf{L} x \mathbf{L}\)
apply (simp add: FromR_def lift_drop_idem)
apply (case_tac x, simp add: lift_drop_idem drop_lift_idem, auto)
done
B.3. Foundations

lemma DEF_FromR_exits_Inr: DEF (FromR x) = (∃ y. x = Inr y)
apply (simp add: FromR_def)
apply (case_tac x, simp, auto)
done

lemma DEF_FromLD : DEF(FromL x)⇒ DEF(x)
apply (simp add: DEF_def FromL_def not_down_exists_lift)
apply (case_tac x, simp, simp)
done

lemma DEF_FromRD : DEF(FromR x)⇒ DEF(x)
apply (simp add: DEF_def FromR_def not_down_exists_lift)
apply (case_tac x, simp, simp)
done

end

B.3.2. The OCL Kernel

theory OCL_Kernel
imports $HOLOCL_HOME/src/Lifting
begin

Global Syntax Infrastructure

In the theory files, this section contains the SML code for setting up the infra-structure for switching between mathematical and other notations for OCL.

ocl_setup_op

In the theory files, this section contains the SML code that implements the rulebase for the context-passingness rules that are registered to the simplifier to decide cp-ness in proofs without the help of ocl_cp_unfold or ocl_simp.

Definition of the Isar interface to ocl_setup_op

In the theory files, this section contains the SML code that sets up the isar syntax for command setup_op.

Setting up the Rulebase for cp-reasoning.
Appendix B. Isabelle Theories

In the theory files, this section contains the SML code that sets up the rulebase for the context-passingness rules that are registered to the simplifier to decide cp-ness questions in interactive proofs without the help of ocl_cp_unfold or ocl_simp.

Registering the cp-rules used to decide cp-ness questions in cp_unfold and the cp-fold rules used to convert a term in explicit cp-representation to a term in implicit cp-representation.

end

B.3.3. Type Definition for OclUndefined

theory OCL_Undefined
  imports $HOLOCL_HOME/src/OCL_Kernel
begin

As previously mentioned, all types, let it be basic types or class types, my contain the element ⊥ denoting undefinedness. In classifier types, this can be interpreted as equivalent in unboxed types to a null-reference. Therefore, there is a universal constant in [OCL] called ⊥, that is constructed as follows:

constdefs
  OclUndefined :: ('a,'b::bot) VAL
  OclUndefined ≡ lift0 ⊥

syntax
  _OclUndefined_std :: ('a,'b::bot) VAL (OclUndefined)

syntax
  _OclUndefined_ascii :: ('a,'b::bot) VAL (undef)

syntax
  _OclUndefined_math :: ('a,'b::bot) VAL (⊥)

Rules describing the effect of strictify on the OCL level

lemma fw_OCL_undef_1_lift1':
  assumes f_def: f ≡ (lift1' lift_arg0) (strictify P)
  shows f OclUndefined = OclUndefined
  by(simp add: f_def OclUndefined_def ss_lifting')
  binary rules

lemma fw_OCL_undef_1_lift2':
  assumes f_def: f ≡ (lift2' lift_arg0 lift_arg0) (strictify P)
  shows f OclUndefined Y = OclUndefined

162
B.3. Foundations

by (simp add: f_def OclUndefined_def ss_lifting)

lemma fw_OCL_undef_1_lift2_01:
  assumes f_def: f ≡ (lift2' lift_arg0 lift_arg1) (strictify P)
  shows f OclUndefined Y = OclUndefined
by (simp add: f_def OclUndefined_def ss_lifting)

lemma fw_OCL_undef_2_lift2_00:
  assumes f_def: f ≡ (lift2' lift_arg0 lift_arg0) (λ x. strictify (P x))
  shows f X OclUndefined = OclUndefined
by (simp add: f_def OclUndefined_def ss_lifting)

tertiary rules

lemma fw_OCL_undef_1_lift3_000:
  assumes f_def: f ≡ (lift3' lift_arg0 lift_arg0 lift_arg0) (strictify P)
  shows f OclUndefined Y Z = OclUndefined
by (simp add: f_def OclUndefined_def ss_lifting)

lemma fw_OCL_undef_1_lift3_020:
  assumes f_def: f ≡ (lift3' lift_arg0 lift_arg2 lift_arg0) (strictify P)
  shows f OclUndefined Y Z = OclUndefined
by (simp add: f_def OclUndefined_def ss_lifting)

lemma fw_OCL_undef_2_lift3_000:
  assumes f_def: f ≡ (lift3' lift_arg0 lift_arg0 lift_arg0) (λ x y. strictify (P x y))
  shows f X Y OclUndefined = OclUndefined
by (simp add: f_def OclUndefined_def ss_lifting)

lemma fw_OCL_undef_2_lift3_020:
  assumes f_def: f ≡ (lift3' lift_arg0 lift_arg2 lift_arg0) (λ x y. strictify (P x y))
  shows f X Y OclUndefined = OclUndefined
by (simp add: f_def OclUndefined_def ss_lifting)

end

B.3.4. Type Definition for Boolean

theory OCL_Boolean_type
imports $HOLOCL_HOME/src/OCL_Kernel
begin

This theory is the prototype for a basic type definition in OCL. The value types are defined by extending the basic HOL types with the bottom element ⊥.

types
  Boolean_0 = bool up
  'a Boolean = ('a, Boolean_0) VAL

end
Appendix B. Isabelle Theories

B.3.5. Type Definition for Integer

theory OCL_Integer_type
imports $HOLOCL_HOME/src/OCL_Kernel
begin

The value types are defined by extending the basic $\text{HOL}$ types with the bottom element $\perp$.

types
  Integer_0 = int up
  'a Integer = ('a, Integer_0) VAL

translations
  a Integer ⇢ ('a, Integer_0) VAL

end

B.3.6. Type Definition for Real

theory OCL_Real_type
imports $HOLOCL_HOME/src/OCL_Kernel Complex_Main
begin

The value types are defined by extending the basic $\text{HOL}$ types with the bottom element $\perp$.

types
  Real_0 = real up
  'a Real = ('a, Real_0) VAL

translations
  a Real ⇢ ('a, Real_0) VAL

end

B.3.7. Type Definition for String

theory OCL_String_type
imports $HOLOCL_HOME/src/OCL_Kernel
begin

The value types are defined by extending the basic $\text{HOL}$ types with the bottom element $\perp$.

end
B.3. Foundations

\[
\text{types} \\
\text{String_0} = \text{string up} \\
{'}a \text{ String} = ('a, \text{String_0}) \text{ VAL}
\]

\[
\text{translations} \\
{'}a \text{ String} \leftarrow (a, \text{String_0}) \text{ VAL}
\]

B.3.8. Type Definition for OclAny

theory OCL_OclAny_type
imports $\text{HOOLCL_HOME/src/Lifting}$
begin

typedecl oid

arities
oid :: bot

datatype OclAny_key = OclAny

types OclAny_type = OclAny_key × oid

This definition of OclAny_type results in a “referential universe”, i.e., a universe where a referential equality is present. A referential equality is the strong equality for “boxed types” (that is Real, Boolean, String) and an equality on the reference to a value. Since our universe construction is designed to mirror the subtype discipline of OCL, i.e., objects are records of a certain type, the reference to an object must be stored in the object itself in our model, namely at the first position of the record.

If OCL expressions refer to states, where all objects contain the reference to itself in the state, the logical equality co-incides with a referential equality.

types
{'}a OclAny_ext = (OclAny_type × {'}a up)
{'}a OclAny_0 = ({'a OclAny_ext) up

Alternative we could define which would allow an additional ‘exception’ element with a non-strict behavior. This would model something like a null reference (or pointer) known from object-oriented programming languages.

translations
a OclAny_0 <= (type) ((OclAny_key * oid) * a up)up

types
{'st,'a)OclAny = {'st, 'a OclAny_0) VAL

lemma [simp]: DEF (obj::({'a)OclAny_0)) =
(fst(fst(drop(obj)))) = OclAny_key,OclAny)

apply (auto simp: DEF_def not_down_exits_lift)
apply (case_tac a)

165
Appendix B. Isabelle Theories

apply (assumption)
done
end

B.3.9. Type Definition for Collections

theory OCL_Collection_type
imports $HOLOCL_HOME/src/OCL_Kernel
begin
axclass collection < bot
end

B.3.10. Type Definition for Set

theory OCL_Set_type
imports $HOLOCL_HOME/src/library/collection/OCL_Collection_type
begin
typedef 'a Set_0 = {X::('a::bot) set up.
(smash (\x X. DEF X & x \in drop X) X) = X}
apply (rule_tac x=\bot in exI)
by (simp add: smash_def)

instance Set_0 :: (type) ord
  by intro_classes
arities Set_0 :: (type) collection
defs UU_Set_def: \bot \equiv Abs_Set_0 down
end

B.3.11. Type Definition for Sequence

theory OCL_Sequence_type
imports $HOLOCL_HOME/src/library/collection/OCL_Collection_type List
begin
In contrast to other collections, the collection Sequence is indeed implemented by finite lists. Consequently, size is defined for all defined sequences.

typedef 'a Sequence_0 = {X::('a::bot) list up.
(smash (\x X. DEF X & x \in set 'X) X) = X}
by (rule_tac x=\bot in exI, simp add: smash_def)
B.3. Foundations

arities  Sequence_0 :: (type) collection

defs    UU_Sequence_def. ⊥ ≡ Abs_Sequence_0 down

The HOL type constructor for representing OCL sequence types is defined as follows:

types  ('st,'b) Sequence = ('st, 'b Sequence_0) VAL

end

B.3.12. Type Definition for Bag

theory OCL_Bag_type
imports  $HOLOCL_HOME/src/library/collection/OCL_Collection_type
         Multiset
begin  typedef  'a Bag_0 = {X::('a::bot) multiset up.
               (smash (λx X. DEF X & x:# drop X) X) = X}
      by (rule_tac x=⊥ in exI)
      apply (simp add: smash_def)
      instance Bag_0 :: (type) ord
      by intro_classes
      arities Bag_0 :: (type) bot
      arities Bag_0 :: (type) collection
      defs    UU_Bag_def. ⊥ ≡ Abs_Bag_0 down
      types  ('st,'b) Bag = ('st, 'b Bag_0) VAL
      end

B.3.13. Type Definition for OrderedSet

theory OCL_OrderedSet_type
imports  $HOLOCL_HOME/src/library/collection/OCL_Collection_type
         List
begin  typedef  'a OrderedSet_0 = {X::('a::bot) list up.
               (smash (λ x X. DEF X & (distinct 'X' −→ x ∈ set 'X')) X) = X}
      by (rule_tac x=⊥ in exI, simp add: smash_def)
      instance OrderedSet_0 :: (type) ord

167
Appendix B. Isabelle Theories

by intro_classes

arities  OrderedSet_0 :: (type) bot
arities  OrderedSet_0 :: (type) collection

defs    UU_OrderedSet_def: ⊥ ≡ Abs_OrderedSet_0 down

types   ('a,'b) OrderedSet = ('a, 'b OrderedSet_0) VAL

end

B.3.14. The OCL Universe

theory OCL_Universe imports
  Datatype
  $HALOCL_HOME/src/library/basic/OCL_Boolean_type
  $HALOCL_HOME/src/library/basic/OCL_String_type
  $HALOCL_HOME/src/library/basic/OCL_Real_type
  $HALOCL_HOME/src/library/basic/OCL_Integer_type
  $HALOCL_HOME/src/library/basic/OCL_Undefined
  $HALOCL_HOME/src/library/basic/OCL_OclAny
  $HALOCL_HOME/src/library/collection/$COLLECTION/OCL_OrderedSet_type
  $HALOCL_HOME/src/library/collection/$COLLECTION/OCL_Bag_type

Note, the definitions of OclAny differs, depending if HOL-OCL is was built with a referential universe or not[2].

Foundations of the Universe Construction

The universe $U$ is a family of universe types which comprise all value types (Real, Integer, String, Boolean, ...) and an extendible class type representation induced by a class hierarchy. The concepts of the universe construction has been presented in Chapt. 4.

The “initial” universe type $U_0$ is built as sum of the built-in value types and the type OclAny (including all its extensions representing subtypes of OclAny).

types
  values  = Real_0 + Integer_0 + Boolean_0 + String_0
  'a U    = ('a OclAny_0) + values

types

B.3. Foundations

\[(a,T) \text{ cl}_\text{ext} = (T \times a \text{ up})\]
\[(a,b,T) \text{ ext} = (a,T)\text{cl}_\text{ext} + b\]

The following setup of Isabelle's syntax engine helps when presenting types corresponding to OCL types:

**translations**
\[
a U <= (\text{type}) (\text{OclAny}_0 \ a) + (\text{Real}_0 + \text{Integer}_0 + \text{Boolean}_0 + \text{String}_0)
\]
\[
\text{Real}_0 <= (\text{type}) \text{ real up}
\]
\[
\text{Integer}_0 <= (\text{type}) \text{ int up}
\]
\[
\text{String}_0 <= (\text{type}) \text{ char list up}
\]
\[
\text{Boolean}_0 <= (\text{type}) \text{ bool up}
\]

**Constants in and Operations on the Universe**

The test operations for “beeing a Real” in a universe type were provided as follows:

**constdefs**
\[
sup :: ((a \times b) \text{ up} \Rightarrow a
\]
\[
sup \ \text{obj} \equiv \text{fst}(\text{drop}\text{(obj)})
\]
\[
\text{base} :: (a \times b \text{ up} \Rightarrow b \text{ up}
\]
\[
\text{base} \ x \equiv \text{case} x \ \text{of lift} (a,b) => b
\]
\[
| \text{down} => \text{down}
\]

**constdefs**
\[
\text{refbase} :: (a \times b \times c \text{ up} \Rightarrow c \text{ up}
\]
\[
\text{refbase} \ x \equiv \text{case} x \ \text{of lift} (a,(b,c)) => c \ | \text{down} => \text{down}
\]

**constdefs**
\[
\text{ref_of} :: (a \times b \times c \text{ up} \Rightarrow b
\]
\[
\text{ref_of} \ x \equiv \text{fst}(\text{snd}\text{drop}(x))
\]

**lemma** \(\text{DEF}_\text{baseD} [\text{simp}]: \text{DEF}(\text{base}(\text{obj})) \Rightarrow \text{DEF}(\text{obj})\)
\text{apply } (\text{simp add: DEF_def base_def not_down_exists_lift})
\text{apply } (\text{cases obj, simp})
\text{apply } (\text{auto})
\text{done}

**lemma** \(\text{DEF}_\text{baseD2} [\text{simp}]: \text{DEF}(\text{base}(\text{obj})) \Rightarrow \text{DEF}(\text{snd}\text{drop}(\text{obj}))\)
\text{apply } (\text{simp add: DEF_def base_def not_down_exists_lift})
\text{apply } (\text{cases obj, simp})
\text{apply } (\text{auto})
\text{done}

**lemma** \(\text{base_snd_drop}: \text{DEF}(\text{base}(\text{obj})) \Rightarrow \text{base}(\text{obj}) = \text{snd}(\text{drop}(\text{obj}))\)
\text{apply } (\text{simp add: DEF_def base_def not_down_exists_lift})
\text{apply } (\text{cases obj, simp})
\text{apply } (\text{auto})
\text{done}
Appendix B. Isabelle Theories

lemma DEF_refbaseD [simp]: \( \text{DEF}\text{(refbase(obj))} \Rightarrow \text{DEF}\text{(obj)} \)
apply (simp add: DEF_def refbase_def not_down_exists_lift)
apply (cases obj, simp)
apply (auto)
done

lemma DEF_refbaseD2 [simp]: \( \text{DEF}\text{(refbase(obj))} \Rightarrow \text{DEF}\text{(snd\text{(drop(obj))})} \)
apply (simp add: DEF_def refbase_def not_down_exists_lift)
apply (cases obj, simp)
apply (auto)
done

lemma refbase_snd_drop: \( \text{DEF}\text{(refbase(obj))} \Rightarrow \text{refbase}\text{(obj)} = \text{snd}\text{(snd\text{(drop(obj))})} \)
apply (simp add: DEF_def refbase_def not_down_exists_lift)
apply (cases obj, simp)
apply (auto)
done

lemma base_UU [simp]: \( \text{base} \bot = \bot \)
by (simp add: base_def )

lemma base_down [simp]: \( \text{base} \downarrow = \downarrow \)
by (simp add: base_def)

lemma base_snd_lift [simp]: \( \text{base} \text{(lift(a,X))} = X \)
by (simp add: base_def)

lemma refbase_UU [simp]: \( \text{refbase} \bot = \bot \)
by (simp add: refbase_def)

lemma refbase_down [simp]: \( \text{refbase} \downarrow = \downarrow \)
by (simp add: refbase_def)

lemma refbase_snd_lift [simp]: \( \text{refbase}\text{(lift(a,(b,X)))} = X \)
by (simp add: refbase_def)

types 'a OCLtype = 'a U set

constdefs noext :: 'a => ('a x 'b up)
noext x = (x, \bot)

lemma fst_noext_id [simp]: \( \text{fst\text{(noext x)}} = x \)
B.4. Library

apply (simp (no_asm) add: noext_def)
done

lemma snd_noext_UU [simp]: snd (noext x) = ⊥
  apply (simp (no_asm) add: noext_def)
done

end

B.4. Library

B.4.1. The OCL let expression

theory OCL_Let
imports "$HOLOCL_HOME/src/Lifting"
begin

The OCL let expression is a purely syntactical abbreviation (see [41, p. A-26]) therefore it can be directly mapped to the HOL let.

constdefs
  OclLet :: ((′a,′b) VAL, (′a,′b) VAL ⇒ (′a,′b::bot) VAL) ⇒ (′a,′b) VAL
  OclLet ≡ Let

syntax _OclLet_std :: ((′a,′b) VAL,(′a,′b) VAL ⇒ (′a,′b::bot) VAL ⇒ (′a,′b) VAL
  ((let (_)/ in (_)/end) 15)

syntax _OclLet_ascii :: ((′a,′b) VAL,(′a,′b) VAL ⇒ (′a,′b::bot) VAL ⇒ (′a,′b) VAL
  ((let (_)/ in (_)/end) 15)

syntax (xsymbols)

_OclLet_math :: ((′a,′b::bot) VAL ⇒ (′a,′b) VAL
  ((let (_)/ in (_)/end) 15)

end

B.4.2. OCL Boolean

theory OCL_Boolean
imports "$HOLOCL_HOME/src/OCL_Universe
  "$HOLOCL_HOME/src/OCL_Let
begin

end
The Characteristic Set of the Type Boolean

Case distinction over a boolean

```isabelle
class boolean_cases_sem

assumes undefC: \( x = \bot \Rightarrow R \)
and trueC: \( x = True \Rightarrow R \)
and falseC: \( x = False \Rightarrow R \)

shows \( R \)

apply (rule disjE)
prefer 2 apply (erule undefC)
prefer 2 apply (rule disjE)
prefer 2 apply (rotate_tac \( \neg \neg \), erule trueC)
prefer 2 apply (rotate_tac \( \neg \neg \), erule falseC)
apply (auto simp: not_down_exists_lift)
done

class is_Boolean_0

constdefs
  is_Boolean_0 :: \( 'a \Rightarrow bool \)
  is_Boolean_0 \equiv sum_case (\( \lambda x. False \))
  ((sum_case (\( \lambda x. False \))
    (sum_case (\( \lambda x. False \))
      (sum_case (\( \lambda x. True \))(\( \lambda x. False \)))))

class get_Boolean_0

constdefs
  get_Boolean_0 :: \( 'a \Rightarrow \text{Boolean}_0 \)
  get_Boolean_0 \equiv sum_case (\( \lambda x. \epsilon x. True \))
  ((sum_case (\( \lambda x. \epsilon x. True \))
    (sum_case (\( \lambda x. \epsilon x. True \))
      (sum_case (\( \lambda x. x \))(\( \lambda x. \epsilon x. True \)))))

class mk_Boolean_0

constdefs
  mk_Boolean_0 :: \( \text{Boolean}_0 \Rightarrow 'a \)
  mk_Boolean_0 \equiv \text{Inr} \circ \text{Inr} \circ \text{Inr} \circ \text{Inl}

lemma get_mk_Boolean_id_0: get_Boolean_0 (mk_Boolean_0 \( x \)) = \( x \)

apply (simp add: get_Boolean_0_def mk_Boolean_0_def)
done

lemma is_mk_Boolean_0: is_Boolean_0 (mk_Boolean_0 \( x \)) = True

apply (simp add: is_Boolean_0_def mk_Boolean_0_def)
done

lemma mk_get_Boolean_id_0: is_Boolean_0 \( x \) \( \Rightarrow \) mk_Boolean_0 (get_Boolean_0 \( x \)) = \( x \)

apply (simp add: get_Boolean_0_def mk_Boolean_0_def is_Boolean_0_def)
apply (case_tac \( x \), simp, simp)
apply (case_tac \( b \), simp, simp)
apply (case_tac \( ba \), simp, simp)
apply (case_tac \( bb \), simp, simp)
done

constdefs
  \text{Boolean}_0 :: \( \tau \Rightarrow \text{Boolean}_0 \Rightarrow \text{Set}_0 \) VAL

\text{Boolean}_0 \equiv \text{lift}_0 (\text{Abs}_\text{Set}_0 \circ \text{lift} \cdot \text{UNIV}_\tau)
```

Semantics of Boolean expressions, i.e., the logical operators of the language. They build a Kleene-Logic, i.e., the usual algebraic laws hold. Moreover, all operators are context passing. This results in proof support based on extensive ternary case distinctions (\(P(X)\) holds iff \(P(\bot)\) and \(P(\top)\) and \(P(\bot)\)).

**OCL Boolean expressions**

**The Core of the Language**

These operators are defined via lifting principles from \(\text{HOL}\) (see [13]). A more textbook-like “definition” of \(\text{OCL}\) (following the standard) is derived in the theorem section.

**constdefs**

\(\text{OclIsDefined} :: \langle 'a, 'b::bot \rangle \text{VAL} \Rightarrow 'a \text{ Boolean} \)

\(\text{OclIsDefined} \equiv \text{lift}_1(\text{lift} \circ \text{DEF})\)

\(\text{OclTrue} :: 'a \text{ Boolean} \)

\(\text{OclTrue} \equiv \text{lift}_0(\bot_{\text{True}})\)

\(\text{OclFalse} :: 'a \text{ Boolean} \)

\(\text{OclFalse} \equiv \text{lift}_0(\bot_{\text{False}})\)

\(\text{OclNot} :: 'a \text{ Boolean} \Rightarrow 'a \text{ Boolean} \)

\(\text{OclNot} \equiv \text{lift}_1(\text{strictify}(\text{lift} \circ \text{Not} \circ \text{drop}))\)

**constdefs**

\(\text{OclAnd} :: \langle 'a \text{ Boolean}, 'a \text{ Boolean} \rangle \Rightarrow 'a \text{ Boolean} \)

\(\text{OclAnd} \equiv \text{lift}_2(\lambda x y. \text{if DEF } x \text{ then if DEF } y \text{ then } (\langle x \rangle \land (\langle y \rangle)) \text{ else if } \langle x \rangle \text{ then } \bot \text{ else } \bot_{\text{False}}) \text{ else if DEF } y \text{ then } \bot \text{ else } \bot_{\text{False}} \text{ else } \bot)\)

\(\text{OclIf} :: \langle 'a \text{ Boolean}, 'a::bot \rangle \text{VAL}, \langle 'a, 'a \rangle \text{VAL} \Rightarrow \langle 'a, 'a \rangle \text{VAL} \)

\(\text{OclIf} \equiv \text{lift}_3(\lambda x y z. \text{strictify}(\lambda a. \text{if } \langle a \rangle \text{ then } y \text{ else } z) x)\)

\(\text{OclSand} :: \langle 'a \text{ Boolean}, 'a \text{ Boolean} \rangle \Rightarrow 'a \text{ Boolean} \)

\(\text{OclSand} \equiv \text{lift}_2(\text{strictify}(\lambda x. \text{strictify}(\lambda y. (\langle x \rangle \land (\langle y \rangle)))))\)

The following statements represent the technical setup of Isabelle’s syntax engine for this core-language. All these technical setups can be ignored in first reading.
Appendix B. Isabelle Theories

**syntax**

- _OclIsDefined_std_ :: (′τ, α::bot) VAL ⇒ 'τ Boolean
  (→IsDefined() _) [60,60]
- _OclIsUndefined_std_ :: (′τ, α::bot) VAL ⇒ 'τ Boolean
  (→oclIsUndefined() _) [60,60]
- _OclTrue_std_ :: 'τ Boolean
  (true)
- _OclFalse_std_ :: 'τ Boolean
  (false)
- _OclNot_std_ :: 'τ Boolean ⇒ 'τ Boolean
  (not (_)) [59,59]
- _OclAnd_std_ :: ['τ Boolean, 'τ Boolean] ⇒ 'τ Boolean
  ((_ and _) [57,58])
- _OclIf_std_ :: ['τ Boolean, ('τ, b::bot) VAL, ('τ, b::bot) VAL] ⇒ ('τ, b) VAL
  ((if (_)/ then (_) /else (_) / endif) 15)
- _OclSand_std_ :: ['τ Boolean, 'τ Boolean] ⇒ 'τ Boolean
  ((_ sand _) [57,58,57])

**syntax**

- _OclIsDefined_ascii_ :: (′τ, α::bot) VAL ⇒ 'τ Boolean
  (isdef (_) [60,60])
- _OclIsUndefined_ascii_ :: (′τ, α::bot) VAL ⇒ 'τ Boolean
  (isundef (_) [60,60])
- _OclTrue_ascii_ :: 'τ Boolean
  (TRUE)
- _OclFalse_ascii_ :: 'τ Boolean
  (FALSE)
- _OclNot_ascii_ :: 'τ Boolean ⇒ 'τ Boolean
  (not (_)) [59,59]
- _OclAnd_ascii_ :: ['τ Boolean, 'τ Boolean] ⇒ 'τ Boolean
  ((_ and _) [57,58])
- _OclIf_ascii_ :: ['τ Boolean, ('τ, b::bot) VAL, ('τ, b::bot) VAL] ⇒ ('τ, b) VAL
  ((if (_)/ then (_) /else (_) / endif) 15)
- _OclSand_ascii_ :: ['τ Boolean, 'τ Boolean] ⇒ 'τ Boolean
  ((_ sand _) [57,58,57])

**syntax** (xsymbols)

- _OclIsDefined_math_ :: (′τ, α::bot) VAL ⇒ 'τ Boolean
  (∂ (_) [60,60])
- _OclIsUndefined_math_ :: (′τ, α::bot) VAL ⇒ 'τ Boolean
  (̸∂ (_) [60,60])
- _OclTrue_math_ :: 'τ Boolean
  (T)
- _OclFalse_math_ :: 'τ Boolean
  (F)
- _OclNot_math_ :: 'τ Boolean ⇒ 'τ Boolean
  (¬ (_) [59,59]
Is OCL Boolean Faithful to the OCL Standard?

In this section, we present background material and the proof work for the section 4.5.

constdefs

   semfun :: 'a ⇒ 'a (Sem [[( _ )]])
   Sem [[x]] ≡ x

We show for our first strict operation in OCL, the not operator, that it is in fact an instance of the standards definition scheme:

lemma not_fally_represented:
   Sem[[¬ X]] γ = (if Sem[[X]] γ ≠ ⊥
      then ¬ Sem[[X]] γ
      else ⊥)
by(simp add:OclNot_def
   DEF_def o_def
   lift0_def lift1_def lift2_def
   semfun_def)

The proof is trivial and canonic: it consists of the unfolding of all combinator definitions (they are just abbreviations of re-occurring patterns in the textbook style definitions used to make these patterns explicit!) and the semantic function which is a mere syntactic marker in our context.

The definition of basic operations for the special case of boolean operations is done by a truth table [41, table A 2, page A-12]. We represent this table for the elementary "and" case as following:

lemma and_fally_represented:
   Sem[[X ∧ Y]] γ =
   (if Sem[[X]] γ = False ∧ Sem[[Y]] γ = False
      then False
      else if Sem[[X]] γ = False ∧ Sem[[Y]] γ = True
      then False
      else if Sem[[X]] γ = True ∧ Sem[[Y]] γ = False
      then False
      else if Sem[[X]] γ = False ∧ Sem[[Y]] γ = ⊥
      then ⊥
      else if Sem[[X]] γ = True ∧ Sem[[Y]] γ = ⊥
      then ⊥
      else if Sem[[X]] γ = ⊥ ∧ Sem[[Y]] γ = False
      then False
      else if Sem[[X]] γ = ⊥ ∧ Sem[[Y]] γ = True
      then ⊥
      else if Sem[[X]] γ = ⊥ ∧ Sem[[Y]] γ = ⊥
      then ⊥
      else ⊥)
Appendix B. Isabelle Theories

apply(simp add:OclAnd_def
       DEF_def o_def strictify_def
       lift0_def lift1_def lift2_def
       semfun_def)

apply (cases X γ = down)
apply (cases Y γ = down)
apply (simp_all add: not_down_exists_lift)
by auto

For the operators or, xor, and implies, we refrain from an explicit proof of conformance with [41, table A 2, page A-12]. Instead, we preferred to define these operators as usual in terms of and and not. However, the subsequent lemmas OclUn-defined_or_True represent another way to directly check that our definitions meet the standard.

The Extended Core of the Language

constdefs
OclOr :: [′τ Boolean, ′τ Boolean] ⇒ ′τ Boolean
OclOr S T ≡ ¬(¬S ∧ ¬T)

OclSor :: [′τ Boolean, ′τ Boolean] ⇒ ′τ Boolean
OclSor S T ≡ ¬(¬S ˙∧ ¬T)

Alternative definitions for the use with ocl_setup_op:

lemma OclOr_alt_def: OclOr ≡ lift2 (λ x y. (if (DEF x)
     then (if (DEF y) then (⌜x⌝ ∨ ⌜y⌝)
               else (if ⌜x⌝ then True else ⊥))
     else (if (DEF y) then (⌜y⌝ else ⊥)
               else ⊥)))
apply(rule eq_reflection, (rule ext)+)
by(simp add: OclOr_def OclAnd_def OclNot_def ss_lifting)

lemma OclSor_alt_def: OclSor ≡ lift2 (strictify (λ x. strictify (λ y.⌜x⌝ ∨ ⌜y⌝)))
apply(rule eq_reflection, (rule ext)+)
by(simp add: OclSor_def OclNot_def OclSand_def ss_lifting')

syntax
_\_OclOr_std :: [′τ Boolean, ′τ Boolean] ⇒ ′τ Boolean
((\_or\_/) [53,54],[53])

_\_OclSor_std :: [′τ Boolean, ′τ Boolean] ⇒ ′τ Boolean
((\_sor\_/) [53,54],[53])

syntax
_\_OclOr_ascii :: [′τ Boolean, ′τ Boolean] ⇒ ′τ Boolean
((\_ or\_/) [53,54],[53])
There is an inconsistency between the normative part [41, Chapter 11] and the informative [41, Appendix A] the standard. For reasons discussed below, we chose the \textit{implies} version defined by [41, Table A-2, page A-12] and define the other version later.

\begin{verbatim}
constdefs
  OclSxor :: ['\tau Boolean, '\tau Boolean] ⇒ '\tau Boolean
  OclSxor S T ≡ (S ∨ T) ∧ ¬(S ∧ T)

  OclSimplies :: ['\tau Boolean, '\tau Boolean] ⇒ '\tau Boolean
  OclSimplies S T ≡ (∼S) ∨ T

  alternative definitions for the use with ocl_setup_op

lemma OclSxor_alt_def: OclSxor ≡ lift2 (λ x y.
  (if (DEF x)
   then (if (DEF y) then (⌜x⌝ ≠⌜y⌝)) else ⊥)
  else ⊥)
apply(simp add: OclSxor_def OclOr_alt_def OclAnd_def OclNot_def ss_lifting)

lemma OclSimplies_alt_def: OclSimplies ≡ lift2 (λ x y.
  (if (DEF x)
   then (if (DEF y) then (⌜x⌝ →⌜y⌝))
     else (⌜x⌝ then ⊥ else (True))
   else (if (DEF y) then (⌜y⌝ then (True))
     else ⊥))
apply(simp add: OclSimplies_def OclAnd_def OclNot_def
  OclOr_alt_def OclIsDefined_def ss_lifting)
\end{verbatim}

The truth for \textit{implies} does not fulfill the normative requirement.
appendix b. isabelle theories

apply (rule eq_reflection, (rule ext)+)
by (auto simp: OclSxor_def OclSor_def OclNot_def OclSand_def
     ss_lifting)

lemma OclSimples_alt_def:
OclSimples ≡ lift2 (strictify (λ x. strictify (λ y. (⌜x⌝ → ⌜y⌝))))
apply (rule eq_reflection, (rule ext)+)
by (simp add: OclSimplies_def OclSxor_def OclNot_def OclSand_def
     OclSor_def ss_lifting)

syntax
  _ OclXor_std :: ['τ Boolean, 'τ Boolean] ⇒ 'τ Boolean
    (_ xor/ _) [55,56,55]
  _ OclImplies_std :: ['τ Boolean, 'τ Boolean] ⇒ 'τ Boolean
    (_ implies/ _) [53,52,52]
  _ OclSxor_std :: ['τ Boolean, 'τ Boolean] ⇒ 'τ Boolean
    (_ sxor/ _) [55,56,55]
  _ OclSimples_std :: ['τ Boolean, 'τ Boolean] ⇒ 'τ Boolean
    (_ simplies/ _) [53,52,52]

syntax
  _ OclXor_ascii :: ['τ Boolean, 'τ Boolean] ⇒ 'τ Boolean
    (_ xor/ _) [55,56,55]
  _ OclImplies_ascii :: ['τ Boolean, 'τ Boolean] ⇒ 'τ Boolean
    (_ implies/ _) [53,52,52]
  _ OclSxor_ascii :: ['τ Boolean, 'τ Boolean] ⇒ 'τ Boolean
    (_ sxor/ _) [55,56,55]
  _ OclSimples_ascii :: ['τ Boolean, 'τ Boolean] ⇒ 'τ Boolean
    (_ simplies/ _) [53,52,52]

syntax
  _ OclXor_math :: ['τ Boolean, 'τ Boolean] ⇒ 'τ Boolean
    (_ ⊕/ _) [55,56,55]
  _ OclImplies_math :: ['τ Boolean, 'τ Boolean] ⇒ 'τ Boolean
    (_ −→/ _) [53,52,52]
  _ OclSxor_math :: ['τ Boolean, 'τ Boolean] ⇒ 'τ Boolean
    (_ ⌟⊕/ _) [55,56,55]
  _ OclSimplies_math :: ['τ Boolean, 'τ Boolean] ⇒ 'τ Boolean
    (_ ⌟−→/ _) [53,52,52]

An implies variant for three-valued logics introduced by Hähnle [18]:

constdefs
  OclImplies1 :: ['τ Boolean, 'τ Boolean] ⇒ 'τ Boolean
OclImplies1 S T ≡ ☐ S ∨ ☐ T

An implies variant for three-valued logics introduced by Hennicker et al [23]. This

178
variant is also the version actually used in the normative part of the standard.

**constdefs**

\[
\begin{align*}
OclImplies2 & : [\tau \text{ Boolean}, \tau \text{ Boolean}] \Rightarrow \tau \text{ Boolean} \\
OclImplies2 S T & \equiv (\neg S) \lor (S \land T)
\end{align*}
\]

Alternative definitions for the use with `ocl_setup_op`

**lemma** `OclImplies1_alt_def`:

\[
OclImplies1 \equiv \text{lift}_2 (\lambda x y. \\
(\text{if } \text{DEF } x \text{ then } (\text{if } [x] \text{ then } y \text{ else } \text{True}) \text{ else } \text{True}))
\]

**apply**(rule `eq_reflection`, (rule `ext`)+)

**by**(simp add: `OclImplies1_def OclAnd_def OclNot_def OclOr_alt_def OclIsDefined_def ss_lifting)

**lemma** `OclImplies2_alt_def`:

\[
OclImplies2 \equiv \text{lift}_2 (\lambda x y. \\
(\text{if } \text{DEF } x \text{ then } (\text{if } [x] \text{ then } y \text{ else } \text{True}) \text{ else } \bot))
\]

**apply**(rule `eq_reflection`, (rule `ext`)+)

**by**(simp add: `OclImplies2_def OclAnd_def OclNot_def OclIsDefined_def ss_lifting)

**syntax**

\[
\begin{align*}
\text{implies1}_\text{std} & : [\tau \text{ Boolean}, \tau \text{ Boolean}] \Rightarrow \tau \text{ Boolean} \\
(\text{implies1}/\_)[53,54,52] \\
\text{implies2}_\text{std} & : [\tau \text{ Boolean}, \tau \text{ Boolean}] \Rightarrow \tau \text{ Boolean} \\
(\text{implies2}/\_)[53,54,52]
\end{align*}
\]

**syntax**

\[
\begin{align*}
\text{implies1}_\text{ascii} & : [\tau \text{ Boolean}, \tau \text{ Boolean}] \Rightarrow \tau \text{ Boolean} \\
(\text{implies1}/\_)[53,54,52] \\
\text{implies2}_\text{ascii} & : [\tau \text{ Boolean}, \tau \text{ Boolean}] \Rightarrow \tau \text{ Boolean} \\
(\text{implies2}/\_)[53,54,52]
\end{align*}
\]

**syntax**

\[
\begin{align*}
\text{implies1}_\text{math} & : [\tau \text{ Boolean}, \tau \text{ Boolean}] \Rightarrow \tau \text{ Boolean} \\
(\text{implies1}/\_)[53,54,52] \\
\text{implies2}_\text{math} & : [\tau \text{ Boolean}, \tau \text{ Boolean}] \Rightarrow \tau \text{ Boolean} \\
(\text{implies2}/\_)[53,54,52]
\end{align*}
\]

**syntax**

\[
\begin{align*}
\text{implies1}_\text{std} & : \tau \text{ Boolean} \Rightarrow \tau \text{ Boolean} \\
(\text{implies1}/\_)[59,59] \\
\text{implies2}_\text{std} & : [\tau \text{ Boolean}, \tau \text{ Boolean}] \Rightarrow \tau \text{ Boolean} \\
(\text{implies2}/\_)[57,58,57] \\
\text{if}_\text{std} & : [\tau \text{ Boolean}, (\tau, \alpha :: \text{bot}) VAL, (\tau, \alpha :: \text{bot}) VAL] \Rightarrow (\tau, \alpha) VAL
\end{align*}
\]

179
Appendix B. Isabelle Theories

\[(\text{if } (_) \text{ then } (_) \text{ else } (_) \text{ endif}) 15\]

Setup of the Basics

lemma OclIsDefined_vs_DEF: \( \partial x = T \implies \text{DEF} (x \text{ St}) \)
apply (simp add: OclIsDefined_def lift1_def o_def OclTrue_def lift0_def)
apply (drule fun_cong [of _ _ St ])
apply (auto)
done

lemma DEF_vs_OclIsDefined:
assumes 1: \( (\forall \text{ St}. \text{DEF} (x \text{ St})) \)
show \( T = \partial x \)
apply (rule ext)
apply (simp add: OclIsDefined_def lift1_def o_def OclTrue_def lift0_def)
apply (rule 1)
done

ML_setup ⟨ ⟨val OclUndefined_def = get_def (theory OCL_Undefined) OclUndefined⟩⟩
ML ⟨ ⟨val lift3_def = get_def (theory Lifting) lift3
val lift2_def = get_def (theory Lifting) lift2
val lift1_def = get_def (theory Lifting) lift1
val lift0_def = get_def (theory Lifting) lift0
val cp_def = get_def (theory Lifting) cp⟩⟩
ML ⟨ ⟨val strictify_def = get_def (theory Lifting) strictify
val isStrict_def = get_def (theory Lifting) isStrict
val DEF_def = get_def (theory Lifting) DEF
val not_down_exists_lift = thm not_down_exists_lift
val up_split = thm up.split
val cp_lift0_fw = thm cp_lift0_fw
val cp_lift1_fw = thm cp_lift1_fw
val cp_lift2_fw = thm cp_lift2_fw
val cp_lift3_fw = thm cp_lift3_fw
val DEF_strictify_DEF_args = thm DEF_strictify_DEF_args
val DEF_strictify_DEF_args2 = thm DEF_strictify_DEF_args2
val lift1b_undef = thm lift1b_undef
val lift2_undef1a = thm lift2_undef1a
val lift2_undef2a = thm lift2_undef2a
val cp_compose2 = thm cp_compose2
val UU_fun_def = get_def (theory Lifting) UU_fun⟩⟩

180
B.4. Library

ML ⟨ ⟨
val OclIsDefined_def = thm OclIsDefined_def
val OclTrue_def = thm OclTrue_def
val OclFalse_def = thm OclFalse_def
val OclNot_def = thm OclNot_def
val OclAnd_def = thm OclAnd_def
val OclIf_def = thm OclIf_def
val OclOr_def = thm OCL_Boolean.OclOr_def
val OclXor_def = thm OCL_Boolean.OclXor_def
val OclImplies_def = thm OCL_Boolean.OclImplies_def
val OclImplies1_def = thm OCL_Boolean.OclImplies1_def
val OclImplies2_def = thm OCL_Boolean.OclImplies2_def)
⟩ ⟩

The Basic Laws for the Boolean Operators

ML_setup ⟨ ⟨
fun prover1 (goal,prems,name) =
let val thm = prove_goalw (the_context()) (DEF_def::strictify_def::o_def::
lift0_def::lift1_def::lift2_def::lift3_def::prems) goal
          (fn _ =>
             ALLGOALS(asm_full_simp_tac
                        (simpset())
                        addsplit’ [split_if,up_split]),
             ALLGOALS(asm_full_simp_tac
                        (simpset())
                        addsimps [not_down_exists_lif]),
                        auto_tac(claset(),simpset())))
          in bind_thm(name,thm);
          Addsimps[thm]
          end;
⟩ ⟩

ML_setup ⟨ ⟨
map prover1
[(| F = T, [OclIsDefined_def,OclTrue_def,OclFalse_def,OclUndefined_def],
   OclIsDefined___undef),
   (| T = T, [OclIsDefined_def,OclTrue_def,OclFalse_def,OclUndefined_def],
   OclIsDefined___True),
   (| F = T, [OclIsDefined_def,OclTrue_def,OclFalse_def,OclUndefined_def],
   OclIsDefined___False),
   (¬ T = T, [OclNot_def,OclTrue_def,OclFalse_def,OclUndefined_def],
   not___undef),
   (¬ F = T, [OclNot_def,OclTrue_def,OclFalse_def,OclUndefined_def],
   not___True),

   181
⟩ ⟩
Appendix B. Isabelle Theories

\[ \neg F = T, [\text{OclNot_def}, \text{OclTrue_def}, \text{OclFalse_def}, \text{OclUndefined_def}], \not\text{False} \];

This shows the following facts:

\[ \partial \bot = F \]
\[ \partial T = T \]
\[ \partial F = T \]
\[ \neg \bot = \bot \]
\[ \neg T = F \]
\[ \neg F = T \]

...which also prove the compliance with Table A.2 in the standard 2.0.

ML \textbf{\textbackslash{}*}

\texttt{map prover1}

\[ [\bot \land \bot = \bot, [\text{OclAnd_def}, \text{OclTrue_def}, \text{OclFalse_def}, \text{OclUndefined_def}], \text{undef}_\land_\text{undef}], \]
\[ (\bot \land T = \bot, [\text{OclAnd_def}, \text{OclTrue_def}, \text{OclFalse_def}, \text{OclUndefined_def}], \text{undef}_\land_\text{True}], \]
\[ (\bot \land F = F, [\text{OclAnd_def}, \text{OclTrue_def}, \text{OclFalse_def}, \text{OclUndefined_def}], \text{undef}_\land_\text{False}], \]
\[ (T \land \bot = \bot, [\text{OclAnd_def}, \text{OclTrue_def}, \text{OclFalse_def}, \text{OclUndefined_def}], \text{True}_\land_\text{undef}], \]
\[ (T \land T = T, [\text{OclAnd_def}, \text{OclTrue_def}, \text{OclFalse_def}, \text{OclUndefined_def}], \text{True}_\land_\text{True}], \]
\[ (T \land F = F, [\text{OclAnd_def}, \text{OclTrue_def}, \text{OclFalse_def}, \text{OclUndefined_def}], \text{True}_\land_\text{False}], \]
\[ (F \land \bot = F, [\text{OclAnd_def}, \text{OclTrue_def}, \text{OclFalse_def}, \text{OclUndefined_def}], \text{False}_\land_\text{undef}], \]
\[ (F \land T = F, [\text{OclAnd_def}, \text{OclTrue_def}, \text{OclFalse_def}, \text{OclUndefined_def}], \text{False}_\land_\text{True}], \]
\[ (F \land F = F, [\text{OclAnd_def}, \text{OclTrue_def}, \text{OclFalse_def}, \text{OclUndefined_def}], \text{False}_\land_\text{False}]]; \]

ML \textbf{\textbackslash{}*}

\texttt{map prover1}

\[ [\bot \lor \bot = \bot, [\text{OclOr_def}, \text{OclUndefined}_\lor_\text{undef}], \]
\[ (\bot \lor T = T, [\text{OclOr_def}, \text{OclUndefined}_\lor_\text{True}], \]
\[ (\bot \lor F = F, [\text{OclOr_def}, \text{OclUndefined}_\lor_\text{False}], \]
\[ (T \lor \bot = T, [\text{OclOr_def}, \text{True}_\lor_\text{undef}], \]
\[ (T \lor T = T, [\text{OclOr_def}, \text{True}_\lor_\text{True}], \]
\[ (T \lor F = T, [\text{OclOr_def}, \text{True}_\lor_\text{False}], \]
\[ (F \lor \bot = \bot, [\text{OclOr_def}, \text{False}_\lor_\text{False}], \]

182
\[
\begin{align*}
&\text{(F }\lor\text{ T }= \text{ T, [OclOr_def, False }\lor\text{ True)}, \\
&\text{(F }\lor\text{ F }= \text{ F, [OclOr_def, False }\lor\text{ False]); }
\end{align*}
\]
Appendix B. Isabelle Theories

\[\begin{align*}
&\{ (\bot \rightarrow \bot = \bot) :: \text{OclImplies2_def}, \ OclUndefined__implies2__undef, \\
&\{ (\bot \rightarrow T = T) :: \text{OclImplies2_def}, \ OclUndefined__implies2__True, \\
&\{ (\bot \rightarrow F = F) :: \text{OclImplies2_def}, \ OclUndefined__implies2__FALSE, \\
&\{ (T \rightarrow \bot = T) :: \text{OclImplies2_def}, \ OclUndefined__implies2__True, \\
&\{ (T \rightarrow F = F) :: \text{OclImplies2_def}, \ OclUndefined__implies2__False, \\
&\{ (F \rightarrow \bot = T) :: \text{OclImplies2_def}, \ OclUndefined__implies2__True, \\
&\{ (F \rightarrow T = T) :: \text{OclImplies2_def}, \ OclUndefined__implies2__False, \\
&\{ (F \rightarrow F = T) :: \text{OclImplies2_def}, \ OclUndefined__implies2__False, \\
\end{align*}\]

\[
\text{ML} \langle \langle \\
\text{map prover1} \langle \langle \\
\text{if } \bot \text{ then } Y \text{ else } Z \text{ endif} = \bot, \\
\text{if } T \text{ then } Y \text{ else } Z \text{ endif} = \langle Y::(\tau::\alpha::\text{bot}) \text{ VAL}, \\
\text{if } F \text{ then } Y \text{ else } Z \text{ endif} = \langle Z::(\tau::\alpha::\text{bot}) \text{ VAL}, \\
\rangle \rangle \rangle
\]

\text{All operators are contextpassing}

\textbf{lemmas} \ cp\_undef = OclUndefined\_def \ [\text{THEN} \ cp\_lift0\_fw, \ \text{standard}] \\
\textbf{lemmas} \ cp\_OclIsDefined = OclIsDefined\_def \ [\text{THEN} \ cp\_lift1\_fw, \ \text{standard}] \\
\textbf{lemmas} \ cp\_not = OclNot\_def \ [\text{THEN} \ cp\_lift1\_fw, \ \text{standard}] \\
\textbf{lemmas} \ cp\_and = OclAnd\_def \ [\text{THEN} \ cp\_lift2\_fw, \ \text{standard}] \\
\textbf{lemmas} \ cp\_if = OclIf\_def \ [\text{THEN} \ cp\_lift3\_fw, \ \text{standard}] \\
\text{declare} \ cp\_undef \ [\text{simp}, \ \text{intro}] \ \ cp\_OclIsDefined \ [\text{simp}, \ \text{intro}] \\
\ \ cp\_not \ [\text{simp}, \ \text{intro}] \ \ cp\_and \ [\text{simp}, \ \text{intro}] \\
\ \ cp\_if \ [\text{simp}, \ \text{intro}] \\

\text{ML} \langle \langle \\
\text{fun prover2 (goal,prems,name) =} \\
\text{let val thm = prove_goalw (the_context()) (prems) goal} \\
\text{(fn _ => [Fast_tac 1])} \\
\text{in bind_thm(name,thm);} \\
\text{AddSims[thm];} \\
\text{AddSIs [thm]} \\
\text{end;}
\rangle \rangle
\]
This shows the following facts: \[\llbracket cp ?P; cp ?P' \rrbracket = \Rightarrow cp (\lambda X. ?P X \lor ?P' X)\], \[\llbracket cp ?P; cp ?P' \rrbracket = \Rightarrow cp (\lambda X. ?P X \oplus ?P' X)\], \[\llbracket cp ?P; cp ?P' \rrbracket = \Rightarrow cp (\lambda X. ?P X \rightarrow ?P' X)\]

Proof Technique: High-level Trichometry on context passing contexts

lemma base_distinct:
\[
\begin{align*}
X \tau &= \bot \tau \lor X \tau = T \tau \lor X \tau = F \tau \\
\text{apply (simp add: OclUndefined_def lift0_def OclTrue_def OclFalse_def)} \\
\text{apply (auto)} \\
\text{apply (simp add: not_down_exists_lift)} \\
\text{apply (erule exE)} \\
\text{apply (auto)} \\
\text{done}
\end{align*}
\]

ML_setup ⟨ ⟨ val base_distinct = thm base_distinct ⟩ ⟩

ML_setup ⟨ ⟨
val prems = goalw (the_context()) []
  (X \tau = \bot \tau \lor X \tau = T \tau \lor X \tau = F \tau);
by (cut_facts_tac [base_distinct] 1);
by (Step_tac 1);
by (ALLGOALS (asm_full_simp_tac ((simpset()) addsimps
   [OclFalse_def,OclTrue_def,lift0_def,OclUndefined_def])));
qed distinct_1;

val prems = goalw (the_context()) []
  (X \tau = \bot \tau \lor X \tau = F \tau);
by (cut_facts_tac [base_distinct] 1);
by (Step_tac 1);
by (ALLGOALS (asm_full_simp_tac ((simpset()) addsimps
   [OclFalse_def,OclTrue_def,lift0_def,OclUndefined_def])));
qed distinct_2;

185
Appendix B. Isabelle Theories

val prems = goalw (the_context()) []
  \( \forall \tau \sim = \bot \Rightarrow (X \tau = T \tau \mid X \tau = F \tau) \);
by (cut_facts_tac [base_distinct] 1);
by (Step_tac 1);
by (ALLGOALS (asm_full_simp_tac (simpset() addsimps
  [OclFalse_def, OclTrue_def, isft0_def, OclUndefined_def])));
by (Fast_tac 1);
qed (distinct_3);

lemma cp_distinct_core:
  \[ cp P; cp P'; \]
  \[ \begin{array}{c}
    P \perp \tau = P' \perp \tau; \\
    P T \tau = P' T \tau; \\
    P F \tau = P' F \tau
  \end{array} \]
  \[ \Rightarrow \]
  \[ P X \tau = P' X \tau \]
apply (unfold cp_def)
apply (erule exE)
apply (erule exE)
apply (rotate_tac -2)
apply simp
apply (cut_tac X = X and \tau = \tau in base_distinct)
apply (erule disjE)
apply (erule_tac [2] disjE)
apply (auto)
done
ML "val cp_distinct_core = thm cp_distinct_core"

lemma cp_distinct_core_P:
  \[ cp P; cp P'; \]
  \[ \begin{array}{c}
    X \tau = \perp \Rightarrow P \perp \tau = P' \perp \tau; \\
    X \tau = T \tau \Rightarrow P T \tau = P' T \tau; \\
    X \tau = F \tau \Rightarrow P F \tau = P' F \tau
  \end{array} \]
  \[ \Rightarrow \]
  \[ P X \tau = P' X \tau \]
apply (unfold cp_def)
apply (erule exE)
apply (erule exE)
apply (rotate_tac -2)
apply simp
apply (cut_tac X = X and \tau = \tau in base_distinct)
apply (erule disjE)
apply (erule_tac [2] disjE)
apply (auto)
done
ML "val cp_distinct_core_P = thm cp_distinct_core_P"
B.4. Library

lemma local_validity_propagation1:
\[
\begin{align*}
X \tau &= \perp \tau; \\
\perp \tau &= P' \perp \tau; \\
\text{cp } P; \text{ cp } P' \\
\implies (P;:(\tau)\text{Boolean }\Rightarrow (\tau,'\alpha)\text{ VAL}) \ X \tau &= P' \ X \tau 
\end{align*}
\]
apply \( \text{rule_tac } P = P \text{ and } P' = P' \text{ in } \text{cp\_distinct\_core\_P} \)
apply auto
apply \( \text{simp\_all add: OclTrue\_def OclFalse\_def OclUndefined\_def lift0\_def} \)
done

ML \( \langle \langle \text{val local_validity_propagation1 = thm local_validity_propagation1 } \rangle \rangle \)

lemma local_validity_propagation2:
\[
\begin{align*}
X \tau &= T \tau; \\
T \tau &= P' T \tau; \\
\text{cp } P; \text{ cp } P' \\
\implies (P;:(\tau)\text{Boolean }\Rightarrow (\tau,'\alpha)\text{ VAL}) \ X \tau &= P' \ X \tau 
\end{align*}
\]
apply \( \text{rule_tac } P = P \text{ and } P' = P' \text{ in } \text{cp\_distinct\_core\_P} \)
apply auto
apply \( \text{simp\_all add: OclTrue\_def OclFalse\_def OclUndefined\_def lift0\_def} \)
done

ML \( \langle \langle \text{val local_validity_propagation2 = thm local_validity_propagation2 } \rangle \rangle \)

lemma local_validity_propagation3:
\[
\begin{align*}
X \tau &= F \tau; \\
F \tau &= P' F \tau; \\
\text{cp } P; \text{ cp } P' \\
\implies (P;:(\tau)\text{Boolean }\Rightarrow (\tau,'\alpha)\text{ VAL}) \ X \tau &= P' \ X \tau 
\end{align*}
\]
apply \( \text{rule_tac } P = P \text{ and } P' = P' \text{ in } \text{cp\_distinct\_core\_P} \)
apply auto
apply \( \text{simp\_all add: OclTrue\_def OclFalse\_def OclUndefined\_def lift0\_def} \)
done

ML \( \langle \langle \text{val local_validity_propagation3 = thm local_validity_propagation3 } \rangle \rangle \)

lemma cp_distinct:
\[
\begin{align*}
\text{cp } P; \text{ cp } P'; \\
P' F &= P' T; \\
P F &= \perp; \\
\implies P' X &= P' X 
\end{align*}
\]
apply \( \text{rule ext} \)
apply \( \text{drule_tac } f = P' \text{ and } x = x \text{ in } \text{fun\_cong} \)
apply \( \text{drule_tac } f = P \text{ and } x = x \text{ in } \text{fun\_cong} \)

187
Appendix B. Isabelle Theories

apply (drule_tac f = P F and x = x in fun_cong)
apply (rule cp_distinct_core)
back
apply (auto)
done

ML ⟨ ⟨ val cp_distinct = thm cp_distinct ⟩ ⟩

lemma cp_distinct1:
[ ⊥ X = T; cp P; cp P';
  P T = P' T;
  P F = P' F
] ⇒ P X = P' X
apply (unfold cp_def OclIsDefined_def o_def lift1_def)
apply (rule ext)
apply (drule_tac f = P T and x = x in fun_cong)
apply (drule_tac f = P F and x = x in fun_cong)
apply (drule_tac f = λc. DEF (X c) and x = x in fun_cong)
apply (erule exE)
apply (erule exE)
apply (rotate_tac −2)
apply simp
apply (cut_tac X = X and τ = x in base_distinct)
apply (erule disjE)
apply (erule_tac [2] disjE)
apply (simp)
apply (simp add: DEF_def lift0_def OclUndefined_def OclTrue_def)
apply (auto)
done

ML ⟨ ⟨ val cp_distinct1 = thm cp_distinct1 ⟩ ⟩

lemma cp_distinct2:
[ cp P; cp P';
  X X = ⊥ ⇒ P X = P' X;
  X X = T ⇒ P X = P' X;
  X X = F ⇒ P X = P' X
] ⇒ P X = P' X
apply (rule cp_distinct)
apply auto
done

ML ⟨ ⟨ val cp_distinct2 = thm cp_distinct2 ⟩ ⟩

The lemmas for st_transissibility allow for a new, high-level proof style based on
case-distinctions avoiding unfolding the definition of and, . . .

ML ⟨
fun Ocl_case_tac str n =
  EVERY (eres_inst_tac [(X,str)] cp_distinct1 n) ORELSE
  (res_inst_tac [(X,str)] cp_distinct n),
  TRY(Fast_tac n), TRY(Fast_tac n),
  Auto_tac]
⟩ ⟩

ML ⟨ ⟨
  fun prover3 (goal,dists,b,name) =
    let val thm =
      prove_goalw (the_context()) [] goal
        (fn _ => map (fn x => Ocl_case_tac x 1) dists)
      in bind_thm (name,thm);
      if b then Addsimps[thm] else ()
    end;
  ⟩ ⟩

ML ⟨ ⟨
  map prover3
  [(¬ X) = X, [X],true,not_not),
   (X ∧ X = X, [X],true,and_idem),
   (F ∧ X = F, [X],true,and_false_dominant_1),
   (X ∧ F = F, [X],true,and_false_dominant_2),
   (T ∧ X = X, [X],true,and_true_neutral_1),
   (X ∧ T = X, [X],true,and_true_neutral_2),
   (X ∧ Y = Y ∧ X, [X,Y],false,and_commute),
   (X ∧ (Y ∧ Z) = (X ∧ Y) ∧ Z,[X,Y,Z],false,and_assoc)]
⟩ ⟩

ML ⟨ ⟨
  map prover3
  [(X ∨ X = X,[X],true,or_idem),
   (X ∨ T = T,[X],true,or_true_dominant_1),
   (T ∨ X = T,[X],true,or_true_dominant_2),
   (X ∨ F = X,[X],true,or_false_neutral_1),
   (F ∨ X = X,[X],true,or_false_neutral_2),
   (X ∨ Y = Y ∨ X,[X,Y],false,or_commute),
   ((X ∨ Y) ∨ Z = X ∨ (Y ∨ Z),[X,Y,Z],false,or_assoc)];
⟩ ⟩

ML ⟨ ⟨
  map prover3
  [(((X ∨ Y) ∧ Z = (X ∧ Z) ∨ (Y ∧ Z),[Z,Y,X,X],false,and_or_distrib1),
    (Z ∧ (X ∨ Y) = (Z ∧ X) ∨ (Z ∧ Y),[Z,Y,X,X],false,and_or_distrib2),
    ((X ∧ Y) ∨ Z = (X ∨ Z) ∧ (Y ∨ Z),[Z,Y,X,X],false,and_or_distrib2)]
⟩ ⟩
Appendix B. Isabelle Theories

\[false, or_and_distrib1,\]
\[\begin{array}{c}
(Z \lor (X \land Y)) = (Z \lor X) \land (Z \lor Y), [Z,X,Y], \\
false, or_and_distrib2;\end{array}\]

\[\] \[\] \[\]

**ML**

\[
\begin{array}{c}
map prover3 \\
((\neg (X \lor \neg(Y)), [X,Y], false_de_morgan), \\
(\neg (X \land \neg(Y)), [X,Y], false_de_morgan1), \\
(\neg (X \lor \neg(Y)), [X,Y], false_de_morgan2); \\
\end{array}
\]

**ML**

\[
\begin{array}{c}
map prover3 \\
((\neg(X \land Y) = \neg(-X \lor \neg(Y)), [X,Y], true_zor_true_inverse_1), \\
((\neg-X \land \neg(Y)), [X,Y], true_zor_true_inverse_2), \\
((X \lor F = X, [X], true_zor_false_neutral_1), \\
((F \land X = X, [X], true_zor_false_neutral_2), \\
((X \land Y = Y \land X, [X,Y], false_zor_commute), \\
((X \lor Y) \land Z = X \lor (Y \land Z), \\
[X,Y,Z,Y,Z], false_zor_assoc); \\
\end{array}
\]

We will not include the or-generating rewrite rules into the rewriter since they do not "simplify" the situation. As rules, they are important, of course.

**ML**

\[
\begin{array}{c}
map prover3 \\
((\neg X, [X], true_implies_false), \\
((X \rightarrow T) = T, [X], true_implies_true1), \\
((X \neg\rightarrow \bot) = \neg X \lor \bot, [X], false_implies_undef), \\
((\neg F = X, [X], true_implies_true2), \\
((T \rightarrow X) = X, [X], true_implies_idem), \\
((\bot \rightarrow X) = X \lor \bot, [X], false_implies_undef2), \\
((X \rightarrow -X) = \neg X \lor X, [X], false_implies_idem1), \\
((X \rightarrow (Y \land Z)) = ((X \rightarrow Y) \land (X \rightarrow Z)), \\
[X,Y,Z,Z],false_implies_and), \\
((X \rightarrow (Y \lor Z)) = ((X \rightarrow Y) \lor (X \rightarrow Z)), \\
[X,Y,Z,Z],false_implies_or), \\
(((X \land Y) \rightarrow Z) = X \rightarrow (Y \rightarrow Z), \\
[Z,Y,X,Y,X],false_implies_orE), \\
(((X \lor Y) \rightarrow Z) = (X \rightarrow Z) \land (Y \rightarrow Z), \\
[Z,Y,X,Y,X,X,X,X],false_implies_orE), \\
((X \rightarrow (Y \rightarrow Z)) = Y \rightarrow (X \rightarrow Z), \\
[Z,Y,X,Y,X],false_implies_commute); \\
\end{array}
\]

**ML**

190
B.4. Library

map prover3

map prover3

ML

map prover3

The properties in comments, crucial for deduction, could not be proven. In fact, they do not hold due to the counter-examples:

lemma [ X=⊥; Y=T; Z=T ] ≥→
(X ∨ Y) (Y Z) ≠ (X Z) ∧ (Y Z)
apply(simp, auto simp: lift0_def OclUndefined_def OclTrue_def)
done

lemma [ X=⊥; Y=F ] ≥→
(X ∧ Y) (Y Z) ≠ (X Z)
apply(simp, auto simp: lift0_def OclUndefined_def OclTrue_def)
done

lemma [ X=⊥; Y=F ] ≥→
X (Y Z) ≠ Y (X Z)
apply(simp, auto simp: lift0_def OclUndefined_def OclTrue_def)
done

191
Appendix B. Isabelle Theories

All these higher logical arrangement rules do not hold for the standards definition \( ?S \rightarrow ?T \equiv \neg ?S \lor ?S \land ?T \) of the implication, in contrast to the "classical definition" \( ?S \rightarrow ?T \equiv \neg ?S \lor ?T \). Although the standards choice is feasible, in the light of these dramatic algebraic deficiencies, we qualify it as glitch from the deduction point of view and suggest to apply the definition used in the appendix.

For the completeness of our presentation, we show the properties of \textit{implies} introduced by Hähnle [18]:

\begin{verbatim}
ML ⨅
map prover3
\((\neg X) \lor X \land \neg X = T, \ [X], false, kleenical0)\)
\((\land X. \neg X = T \Rightarrow (X \lor \neg X) = T, \ [X], false, kleenical1)\)
\((\land X. \neg X = T \Rightarrow (\neg X \lor X) = T, \ [X], false, kleenical2)\)
\((\neg X \land X \land \neg X = F, \ [X], false, absurd0)\)
\((\land X. \neg X = T \Rightarrow (X \land \neg X) = F, \ [X], false, absurd1)\)
\((\land X. \neg X = T \Rightarrow (\neg X \land X) = F, \ [X], false, absurd2)\)
\((\neg (\neg X) \lor (X \rightarrow X) = T, \ [X], false, implies_assume)\)
\((\land X. \neg X = T \Rightarrow (X \rightarrow X) = T, \ [X], false, implies_assume)\)
\end{verbatim}

\begin{verbatim}
ML ⨅
map prover3
\((\forall X. \neg X = T \Rightarrow \neg (\neg X) = T, \ [X], true, isDefined_not)\)
\end{verbatim}
B.4. Library

\(\forall Z. [\partial X = T; \partial Y = T] \implies \partial (X \land Y) = T,\)
\([X], true, isDefined_and),

\(\forall Z. [\partial X = T; \partial Y = T] \implies \partial (X \lor Y) = T,\)
\([X], true, isDefined_or),

\(\forall Z. [\partial X = T; \partial Y = T] \implies \partial (X \oplus Y) = T,\)
\([X], true, isDefined_xor),

\(\forall Z. [\partial X = T; \partial Y = T] \implies \partial (X \rightarrow Y) = T,\)
\([X], true, isDefined_implies),

\(\forall X. [\partial X = T; \partial Y = T] \implies \partial (\text{if } \neg X \text{ then } Z \text{ else } Y) = (X \rightarrow Z) \land (\neg X \rightarrow Z),\)
\([X], false, if_to_implies]\)

\(\forall Z. [\partial X = T; \partial Y = T; \partial Z = T] \implies \partial (\text{if } X \text{ then } Y \text{ else } Z) = (X \rightarrow Y) \land (\neg X \rightarrow Z),\)
\([X], false, if_swap),

\(\forall Z. \partial X = T \implies (\text{if } X \text{ then } Y \text{ else } Z) = (X \rightarrow Y) \land (\neg X \rightarrow Z),\)
\([X], false, if_to_implies]\)

\(\forall A. [\partial X = T; \partial Y = T; \partial Z = T] \implies \partial (\text{if } X \text{ then } Y \text{ else } Z) = (X \rightarrow Y) \land (\neg X \rightarrow Z),\)
\([X], false, if_swap),

\(\forall Z. [\partial X = T; \partial Y = T; \partial Z = T] \implies \partial (\text{if } X \text{ then } Y \text{ else } Z) = (X \rightarrow Y) \land (\neg X \rightarrow Z),\)
\([X], false, if_swap),

\(\forall Z. [\partial X = T; \partial Y = T; \partial Z = T] \implies \partial (\text{if } X \text{ then } Y \text{ else } Z) = (X \rightarrow Y) \land (\neg X \rightarrow Z),\)
\([X], false, if_swap)
Appendix B. Isabelle Theories

apply (auto)
done

lemma lift1_strictify_is_isdef:
\[ \partial (\text{lift} \ 1 \ \text{strictify}(\lambda x. f \ x \ X)) \ X = \partial X \]
apply (unfold OclIsDefined_def lift1_def OclUndefined_def o_def)
apply (rule ext)
apply auto
apply (erule DEF_strictify_DEF_args)
apply auto
done

lemma lift2_strictify_is_isdef:
\[ \partial (\text{lift} \ 2 \ \text{strictify}(\lambda x. \text{strictify}(\lambda y. f \ x \ y)) \ X \ Y) = (\partial X \land \partial Y) \]
apply (rule ext)
apply auto
apply (erule DEF_strictify_DEF_args)
apply (erule_tac [2] DEF_strictify_DEF_args)
apply auto
done

declare lift1_strictify_is_isdef [simp] lift2_strictify_is_isdef [simp]

lemma lift1b_undef_fw:
f \equiv \text{lift} \ 1 \ \text{strictify}(g) \Longrightarrow f \bot = \bot
apply (unfold OclUndefined_def lift0_def)
apply (tactic \langle \{ fold_tac [UU_fun_def] \} \rangle)
apply (rule lift1b_undef)
done

lemma lift2_undef1a_fw:
f \equiv \text{lift} \ 2 \ \text{strictify}(\lambda x. \text{strictify}(g \ x)) \Longrightarrow f \bot (X::\tau \Rightarrow \alpha::\bot) = \bot
apply (unfold OclUndefined_def lift0_def)
apply (tactic \langle \{ fold_tac [UU_fun_def] \} \rangle)
apply (rule lift2_undef1a)
done

lemma lift2_undef2a_fw:
f \equiv \text{lift} \ 2 \ \text{strictify}(\lambda x. \text{strictify}(g \ x)) \Longrightarrow f(X::\tau \Rightarrow \alpha::\bot) \bot = \bot
apply (unfold OclUndefined_def lift0_def)
apply (tactic \langle \{ fold_tac [UU_fun_def] \} \rangle)
apply (rule lift2_undef2a)
done

194
B.4. Library

ML ⟨ ⟨ val lift2_undef2a_fw = thm lift2_undef2a_fw ⟩ ⟩

lemma lift1_strict_is_isdef_fw:
\[ f \equiv \text{lift1}(\text{strictify}(\lambda x. [g x])) \Rightarrow \partial(f X) = \partial X \]
by(auto)

lemma lift1_strictify_is_isdef_fw:
\[ f \equiv \text{lift1}(\text{strictify}(\lambda x. [g x])) \Rightarrow \partial(f X) = \partial X \]
by(auto)

lemma lift2_strict_is_isdef_fw:
\[ f \equiv \text{lift2}(\text{strictify}(\lambda x. \text{strictify}(\lambda y. [g (x y)]))) \Rightarrow \partial(f X Y) = (\partial X \land \partial Y) \]
by(auto)

lemma lift2_strictify_is_isdef_fw:
\[ f \equiv \text{lift2}(\text{strictify}(\lambda x. \text{strictify}(\lambda y. [g x y]))) \Rightarrow \partial(f X Y) = (\partial X \land \partial Y) \]
by(auto)

Definedness reasoning for the new lifting construction

ML ⟨ ⟨ val _ = let fun is_isdef_rules rname = let val rname' = \text{fw\_OCL\_is\_isdef\_lift}^rname \_0;\text{ assumes } f\_def: f \equiv (\text{lift}^rname\_0\_0\_0) (\text{strictify}(\lambda x. [g x]));\text{ shows } \partial(f X) = \partial X \text{ by(rule ext, simp add: f\_def OclIsDefined\_def ss\_lifting')}\text{ register rules for ocl\_setup\_op} \rangle ⟩ ⟩
Some basic laws for the \texttt{not} operator

\begin{enumerate}
\item \texttt{not\_injective} : \[ \neg X = \neg Y \implies X = Y \]
\begin{proof}
\begin{code}
\begin{verbatim}
by (drule_tac f = \lambda x. \neg x in \ arg\_cong, simp)
\end{verbatim}
\end{code}
\end{proof}
\item \texttt{not\_bijective}:
\begin{proof}
\begin{code}
\begin{verbatim}
by (auto intro!: not\_injective)
\end{verbatim}
\end{code}
\end{proof}
\end{enumerate}

Characterizations of logical operator definedness

\begin{enumerate}
\item \texttt{isDefined\_notD}:
\begin{proof}
\begin{code}
\begin{verbatim}
by (simp add: OclNot_def o_def lift1_strictify_is_isdef)
\end{verbatim}
\end{code}
\end{proof}
\end{enumerate}

ML setup
\begin{code}
\begin{verbatim}
ML_setup {
  map prover3 [(
    (\partial (\neg X) = (\partial X), \[X, true, isDefined notD\]),
    (\partial (X \& Y) = ((\partial X \& \partial Y) \lor (\partial X \& \neg X) \lor (\partial Y \& \neg Y)),
      \[X,Y,Y, false, isDefined andD\]),
    (\partial (X \lor Y) = ((\partial X \& \partial Y) \lor (\partial X \& X) \lor (\partial Y \& Y)),
      \[X,Y,Y, false, isDefined orD\]),
    (\partial (X \oplus Y) = (\partial X \& \partial Y), \[X,Y, false, isDefined xorD\]),
    (\partial (X \rightarrow Y) = (\partial X \& \partial Y) \lor (\partial X \& \neg X) \lor (\partial Y \& Y)),
      \[X,Y,Y, false, isDefined impliesD\]),
    (\partial (X \leftrightarrow Y) = \partial X \& (\neg (X \& \neg \partial Y)),
      \[X, false, isDefined implies2D\]),
    (\partial (if X then Y else Z endif) = (\partial X \& ((X \& \partial Y) \lor (\neg X \& \partial Z))),
      \[X, false, isDefined ifD\])];
\end{verbatim}
\end{code}
\end{proof}
\end{enumerate}

The set of rules above is of fundamental importance for the forward-reasoning of definedness expressions—it allows for computing for any core logic expression a DNF composed of boolean literals and text \texttt{is\_def}(X) terms (where \(X\) is either a Boolean \texttt{OCL} atom (variable) or a non Boolean expression (\texttt{if})). If the latter are composed by strict \texttt{OCL} operators, it can be further atomized to \texttt{is\_def}(X) atoms where \(X\) occurs in the expression.

Some generic laws for the \texttt{OCL} if operator

\begin{enumerate}
\item \texttt{if\_distrib\_strict}:
\begin{proof}
\begin{code}
\begin{verbatim}
[ cp P; isStrict P ] \implies
P(if X then (Y::(\tau,\alpha::bot) VAL) else Z endif) =
  (if X then ((P Y)::(\tau,\alpha::bot) VAL) else P Z endif)
apply (rule_tac X = X in cp\_distinct)
apply (rule_tac P = P in cp\_compose2)
apply auto
\end{verbatim}
\end{code}
\end{proof}
\end{enumerate}
apply (simp add: UU_fun_def OclUndefined_def isStrict_def lift0_def)
done

lemma if_distrib2 :
[\cp P; \\partial X = T ] \Longrightarrow
P (if X then (Y::('\tau', '\alpha::bot) VAL) else Z endif) =
(if X then ((P Y)::('\tau', '\beta::bot) VAL) else P Z endif)
apply (simp add: cp_def OclIf_def lift3_def, erule exE, rule ext)
apply (simp add: OclIsDefined_def DEF_def OclTrue_def
         lift0_def lift1_def o_def)
apply (drule_tac x = \tau in fun_cong, simp)
apply (simp only: not_down_exists_lift, erule exE)
apply simp
done

Final Setup
lemma and_left_idem : P \land (P \land Q) = P \land Q
  apply (subst and_assoc)
  apply (subst and_idem )
  apply (auto)
done
ML \<< val and_left_idem = thm and_left_idem >>

lemma or_left_idem: P \lor (P \lor Q) = P \lor Q
  apply (subst or_assoc \[symmetric\])
  apply (subst or_idem)
  apply (auto)
done
ML \<< val or_left_idem = thm or_left_idem >>

lemma and_left_assoc : X \land (Y \land Z) = Y \land (X \land Z)
  apply (simp add:and_assoc)
  apply (subst and_commute)
  apply simp
done

lemma or_left_assoc : X \lor (Y \lor Z) = Y \lor (X \lor Z)
  apply (simp add:or_assoc\[symmetric\])
  apply (subst or_commute)
  apply simp
done

Now we prepare a setup for Associativity, commutativity, and idempotency (ACI)
Appendix B. Isabelle Theories

rewriting of the boolean operators: These are:

\[ a \circ b = b \circ a \]  
\[ (a \circ b) \circ c = a \circ (b \circ c) \]  
\[ a \circ (b \circ c) = b \circ (a \circ c) \]  
\[ a \circ a = a \]  
\[ a \circ (a \circ b) = a \circ b \]

**lemmas** OCL_logic_ACI =

\text{and\_commute} and\_assoc \{symmetric\}
\text{and\_left\_assoc} and\_idem \{and\_left\_idem\}
\text{or\_commute} or\_assoc \{or\_left\_assoc\}
\text{or\_left\_idem}

**Boolean Relations**

**OCL Equalities**

In the non-referential universe the following defines the two default equalities. In the referential universe, these definitions define the referential equalities.

**constdefs** OclStrongEq :: \((\tau, \alpha :: \text{bot}) \text{VAL}, (\tau, \alpha) \text{VAL}) \Rightarrow \tau \text{ Boolean}

OclStrongEq \equiv \lambda x y. \{ x = y \}

OclStrictEq :: \((\tau, \alpha :: \text{bot}) \text{VAL}, (\tau, \alpha) \text{VAL}) \Rightarrow \tau \text{ Boolean}

OclStrictEq \equiv \lambda x y. \{ \text{strictify} \lambda x. \{ x = y \} \}

**consts**

OclStrongValueEq :: \((\tau, \alpha :: \text{bot}) \text{VAL}, (\tau, \alpha) \text{VAL}) \Rightarrow \tau \text{ Boolean}

OclStrictValueEq :: \((\tau, \alpha :: \text{bot}) \text{VAL}, (\tau, \alpha) \text{VAL}) \Rightarrow \tau \text{ Boolean}

OclStrongDeepValueEq :: \((\tau, \alpha :: \text{bot}) \text{VAL}, (\tau, \alpha) \text{VAL}) \Rightarrow \tau \text{ Boolean}

OclStrictDeepValueEq :: \((\tau, \alpha :: \text{bot}) \text{VAL}, (\tau, \alpha) \text{VAL}) \Rightarrow \tau \text{ Boolean}

**syntax**

\_OclStrongEq_std :: \((\tau, \alpha :: \text{bot}) \text{VAL}, (\tau, \alpha) \text{VAL}) \Rightarrow \tau \text{ Boolean}

\_OclStrictEq_std :: \((\tau, \alpha :: \text{bot}) \text{VAL}, (\tau, \alpha) \text{VAL}) \Rightarrow \tau \text{ Boolean}

\_OclStrongValueEq_std :: \((\tau, \alpha :: \text{bot}) \text{VAL}, (\tau, \alpha) \text{VAL}) \Rightarrow \tau \text{ Boolean}

\_OclStrictValueEq_std :: \((\tau, \alpha :: \text{bot}) \text{VAL}, (\tau, \alpha) \text{VAL}) \Rightarrow \tau \text{ Boolean}

198
B.4. Library

\[\text{OclStrongDeepValueEq_std :: } [(\tau, \alpha\::\text{bot}) \text{ VAL}, (\tau, \alpha) \text{ VAL}] \Rightarrow \tau \text{ Boolean} \]

\[(1_\sim \sim_\sim) \]

\[\text{OclStrictDeepValueEq_std :: } [(\tau, \alpha\::\text{bot}) \text{ VAL}, (\tau, \alpha) \text{ VAL}] \Rightarrow \tau \text{ Boolean} \]

\[(1_\sim \sim_\sim) \]

\text{syntax}

\[\text{OclStrongEq_ascii:: } [(\tau, \alpha\::\text{bot}) \text{ VAL}, (\tau, \alpha) \text{ VAL}] \Rightarrow \tau \text{ Boolean} \]

\[(1_{\sim\sim}) \]

\[\text{OclStrictEq_ascii:: } [(\tau, \alpha\::\text{bot}) \text{ VAL}, (\tau, \alpha) \text{ VAL}] \Rightarrow \tau \text{ Boolean} \]

\[(1_{\sim\sim}) \]

\[\text{OclStrongValueEq_ascii:: } [(\tau, \alpha\::\text{bot}) \text{ VAL}, (\tau, \alpha) \text{ VAL}] \Rightarrow \tau \text{ Boolean} \]

\[(1_{\sim\sim}) \]

\[\text{OclStrictValueEq_ascii:: } [(\tau, \alpha\::\text{bot}) \text{ VAL}, (\tau, \alpha) \text{ VAL}] \Rightarrow \tau \text{ Boolean} \]

\[(1_{\sim\sim}) \]

\[\text{OclStrongDeepValueEq_ascii:: } [(\tau, \alpha\::\text{bot}) \text{ VAL}, (\tau, \alpha) \text{ VAL}] \Rightarrow \tau \text{ Boolean} \]

\[(1_{\sim\sim}) \]

\[\text{OclStrictDeepValueEq_ascii:: } [(\tau, \alpha\::\text{bot}) \text{ VAL}, (\tau, \alpha) \text{ VAL}] \Rightarrow \tau \text{ Boolean} \]

\[(1_{\sim\sim}) \]

\text{syntax (xsymbols)}

\[\text{OclStrongEq_math:: } [(\tau, \alpha\::\text{bot}) \text{ VAL}, (\tau, \alpha) \text{ VAL}] \Rightarrow \tau \text{ Boolean} \]

\[(1_{\sim\sim}) \]

\[\text{OclStrictEq_math:: } [(\tau, \alpha\::\text{bot}) \text{ VAL}, (\tau, \alpha) \text{ VAL}] \Rightarrow \tau \text{ Boolean} \]

\[(1_{\sim\sim}) \]

\[\text{OclStrongValueEq_math:: } [(\tau, \alpha\::\text{bot}) \text{ VAL}, (\tau, \alpha) \text{ VAL}] \Rightarrow \tau \text{ Boolean} \]

\[(1_{\sim\sim}) \]

\[\text{OclStrictValueEq_math:: } [(\tau, \alpha\::\text{bot}) \text{ VAL}, (\tau, \alpha) \text{ VAL}] \Rightarrow \tau \text{ Boolean} \]

\[(1_{\sim\sim}) \]

\[\text{OclStrongDeepValueEq_math:: } [(\tau, \alpha\::\text{bot}) \text{ VAL}, (\tau, \alpha) \text{ VAL}] \Rightarrow \tau \text{ Boolean} \]

\[(1_{\sim\sim}) \]

\[\text{OclStrictDeepValueEq_math:: } [(\tau, \alpha\::\text{bot}) \text{ VAL}, (\tau, \alpha) \text{ VAL}] \Rightarrow \tau \text{ Boolean} \]

\[(1_{\sim\sim}) \]

\[\text{OclNeg:: } [\tau \text{ Boolean}, \tau \text{ Boolean}] \Rightarrow \tau \text{ Boolean} \]

\[(1_{/ <\sim > } ) \]

\text{translations}

\[X '<\sim ' Y \Rightarrow \sim(X \equiv Y)\]

Is HOL-OCL Faithful to the OCL standard (Part II)?

\text{lemma strictEq_factly_represented:}

\[\text{Sem}[X \equiv Y] \gamma = (\text{if } \sim \text{ Sem}[X] \gamma \neq \bot \land \sim \text{ Sem}[Y] \gamma \neq \bot \text{ then } \sim \text{ Sem}[X] \gamma \gamma = \sim \text{ Sem}[Y] \gamma \gamma \text{ else } \bot)\]

\text{apply (simp add: OclStrictEq_def)}

\[\text{DEF_def o_def}\]
This operator—the first binary operator of a strict operation—represents directly the definition scheme as imposed by [41, Definition A. 16]. The operators for Set, Bag, Integer and Real will follow this scheme.

B.4.3. OCL Logic Core

theory OCL_Logic_core
  imports \$HOLOC\_HOME/src/library/basic/OCL:Boolean
  uses \$HOLOC\_HOME/src/kernel_ext/isabelle_kernel_patch.ML
begin

Introduction

The purpose of this theory is to introduce the concept of OCL judgement (written $\tau \models \phi$) over a context $\tau$ and an OCL formula $\phi$ and to derive a number of mechanizable calculi for it. Here, a context is usually a system transition in OCL, i.e. a pair of two states $\tau = (\tau_{\text{pre}}, \tau_{\text{post}})$; however, since our theory on OCL does make perfect sense for generalizations such as "sequences of states" of Kripke structures, we prefer the more general notion of context to simple state pairs. A formula $\phi$ may contain paths such as "$\text{self.a.b}$" which were interpreted in $\tau$. The concept of a judgement occurs already in the standard in definition A.33 (Semantics of Operation Specifications). We turn it to the heart of deductive calculi for OCL. It will be the basis for equational calculi (both strict and strong equalities), congruences on formulas and local and global equivalences (terminology explained below) over judgements, and tableaux calculi over judgements.

All of them are integrated into tactic procedures that allow for automated proof state transformations even automated proofs over OCL formula. Finally, these SML-programmed tactics were bound to a specific Isar syntax.

Terminology

An OCL formula is globally valid (or just valid if its evaluation yields for all contexts (e.g., state transitions $(s, s')$, Kripke-structures, ...) true; an OCL formula is locally valid if this is the case for a specific context.

We have three different equational calculi for OCL forming the bare bones of automated deduction in OCL.

1. an universal congruence (on OCL formulae) (UC) is a (conditional) formula with an equality $E = E'$ as conclusion where $E$ and $E'$ has type $V_\alpha(\beta)$. These equalities hold for all contexts $\tau$ and can be processed directly by Isabelle's rewriter.
B.4. Library

2. A local equivalence ([LE]) is a (conditional) formula with an equality $E \tau = E' \tau$ as conclusion where $E$ and $E'$ has type $V_\alpha(\beta)$. These equalities hold only in some context $\tau$ of type $\tau$ (?) and can only be processed by the tactic OCL_rewriter tactic in subterms occurring in judgements and in the $E'$s in $E \tau = E' \tau$.

3. A local judgement equivalence ([LJE]) which states that two judgments over $\text{OCL}$ formulae must be equivalent in a particular context $\tau$, so $(\tau \models E) = (\tau \models E')$.

Recall that judgements require that the formula holds, i.e., evaluates to $\text{true}$. In contrast to [LE], the formulae must not agree on all three truth values.

The Theory of OCL Judgements

In the following, the notation for validity judgements is introduced:

constdefs
  OclValid :: 'a Boolean ⇒ bool
  OclValid P ≡ (P = T)
  OclLocalValid :: ['a, a Boolean] ⇒ bool
  OclLocalValid τ P ≡ (P τ = T τ)

syntax
  _OclValid_std :: 'a Boolean ⇒ bool
  _OclLocalValid_std: ['a,'a Boolean] ⇒ bool
  _OclValid_std τ P ≡ (P τ = T τ)

syntax
  _OclValid_ascii :: 'a Boolean ⇒ bool
  _OclLocalValid_ascii: ['a,'a Boolean] ⇒ bool
  _OclValid_ascii τ P ≡ (P τ = T τ)

syntax
  _OclValid_math :: 'a Boolean ⇒ bool
  _OclLocalValid_math: ['a,'a Boolean] ⇒ bool
  _OclValid_math τ P ≡ (P τ = T τ)

lemma cp_OclLocalValid[simp, intro!]:
  cp P ⇒ cp(λ X τ. τ ⊨ P X)
by(simp add: OclLocalValid_def)

The rules needed by cp_unfold.

lemma OCL_cp0_OclLocalValid: cp0 (λ x τ. τ ⊨ x)
by(simp add: OclLocalValid_def OclTrue_def ss_cp_def ss_lifting')
Appendix B. Isabelle Theories

lemma OCL_cp0_fold_OclLocalValid: \( \tau \models (\text{lift}0 (x \tau)) = (\tau \models x) \)
by (simp add: OclLocalValid_def OclTrue_def ss_cp_defs ss_lifting)

ML ⟨ ⟨
cpR_simpset := (!cpR_simpset) addsimps [thm OCL_cp0_OclLocalValid];
cpR_fold_simpset := (!cpR_fold_simpset) addsimps [thm OCL_cp0_fold_OclLocalValid];
⟩ ⟩

Generic Definedness Rules on Local Validity
lemma lift1_strictify_implies_LocalValid_defined: 
\( f \equiv \text{lift}1 (\text{strictify} (\lambda x. g x)) \)
\( \implies (\tau \models \partial (f X)) = (\tau \models \partial X) \)
apply (drule lift1_strictify_is_isdef_fw)
apply (rule_tac t = \partial (f X) in ssubst)
apply simp_all
done

lemma lift2_strictify_implies_LocalValid_defined: 
\( f \equiv \text{lift}2 (\text{strictify} (\lambda x. \text{strictify} (\lambda y. g x y))) \)
\( \implies (\tau \models \partial (f X Y)) = ((\tau \models \partial X) \land (\tau \models \partial Y)) \)
apply (drule lift2_strictify_is_isdef_fw)
apply (rule_tac t = \partial (f X Y) in ssubst, assumption)
apply (simp add: OclAnd_def OclTrue_def o_def
OclIsDefined_def lift0_def lift1_def lift2_def
OclLocalValid_def)
done

Semantic Representations of Validity
lemma localValid2sem: 
\( (\tau \models P) = (P \tau = \text{True}) \)
by (simp add: OclLocalValid_def OclTrue_def lift0_def)

lemma localValidNot2sem: 
\( (\tau \models \neg P) = (P \tau = \text{False}) \)
by (simp add: OclLocalValid_def OclNot_def OclTrue_def
strictify_def lift0_def lift1_def o_def
not_down_exists_lift, auto)

lemma localValidDefined2sem: 
\( (\tau \models \partial S) = \text{DEF}(S \tau) \)
by (simp add: OclLocalValid_def OclIsDefined_def strictify_def
o_def lift0_def lift1_def lift2_def
OclTrue_def OclFalse_def OclUndefined_def DEF_def)

lemma localValidUnDefined2sem: 
\( (\tau \models \not\partial S) = (S \tau = \bot) \)

202
B.4. Library

by (simp add: OclLocalValid_def OclIsDefined_def strictify_def o_def lift0_def lift1_def lift2_def OclNot_def OclTrue_def OclFalse_def OclUndefined_def DEF_def)

lemma localValidToNotFalse2sem:
  \(\tau \models P (x::b::type) \lor \varnothing(P x)\) = \(P x \tau \neq \downarrow \) by (simp add: OclLocalValid_def OclIsDefined_def strictify_def OclNot_def OclOr_def OclAnd_def o_def lift0_def lift1_def lift2_def OclTrue_def DEF_def not_down_exists_lift, auto)

lemma localValidToNotTrue2sem:
  \(\tau \models \neg P (x::b::type) \lor \varnothing(P x)\) = \(P x \tau \neq \downarrow \) by (simp add: OclLocalValid_def OclIsDefined_def strictify_def OclNot_def OclOr_def OclAnd_def o_def lift0_def lift1_def lift2_def OclTrue_def DEF_def not_down_exists_lift, auto)

lemma isUndefined_charn:
  \(X = \bot\) = \(\models \varnothing X\) apply (auto simp: OclValid_def) apply (simp add: OclUndefined_def OclTrue_def lift0_def lift1_def lift2_def o_def DEF_def OclIsDefined_def)
apply (rule ext) apply (drule_tac x = s in fun_cong) apply auto done

lemma is_FALSE_charn:
  \(X = \mathrm{\neg} F\) = \(\models \neg X\) by (auto simp: OclValid_def)

apply (auto simp: OclUndefined_def OclFalse_def OclTrue_def lift0_def lift1_def o_def OclIsDefined_def DEF_def OclNot_def strictify_def)
apply (rule ext) apply (drule_tac x = s in fun_cong) apply (case_tac X s = down) apply auto apply (simp add: not_down_exists_lift) apply auto done

lemma is_TRUE_charn:
  \(X = \top\) = \(\models X\) by (auto simp: OclValid_def)

Local and global validity statements are in fact complete in the sense that they can inherently express all three basic values of booleans. This foundational fact gives rise
to the idea to use these judgements both for tableaux and congruence-rewrite calculi.

Instead of representations in terms of semantic primitives, the local judgements can also be expressed on a more abstract level, i.e., in terms of global equivalences.

The following property reveals that strong equality is just mirrored by the HOL equality. Note that the strong equality is implicitly use also in the construction of sets—its choice is therefore highly critical. Depending on the layout of objects, i.e., the concrete object universe, this results in different properties. For the case of the referential universe and states only containing objects with reference to themselves in the state, logical equality coincides with referential equality.

\[ (X \tau = \bot \tau) = (\tau \models \neg X) \]

by \((simp add: OclLocalValid_def OclUndefined_def OclTrue_def lift0_def lift1_def o_def OclIsDefined_def DEF_def OclNot_def)\)

\[ (X \tau = \textbf{F} \tau) = (\tau \models \neg (X \tau)) \]

apply \((simp add: OclLocalValid_def OclUndefined_def OclTrue_def OclFalse_def lift0_def lift1_def o_def OclIsDefined_def DEF_def strictify_def OclNot_def)\)

apply auto
apply \((case_tac X St = down)\)
apply \((simp_all add: not_down_exists_lift)\)
apply auto
done

\[ (X \tau = \textbf{T} \tau) = (\tau \models X) \]

by \((simp add: OclLocalValid_def)\)

\[ (\tau \models x \triangleq y) = (x \tau = y \tau) \]

apply \((simp add: OclStrongEq_def OclLocalValid_def lift2_def OclTrue_def lift0_def)\)
done

The Standardization Rules of (Global) Validity Statements.

\[ OclTrue_is_Valid[simp]: \models \textbf{T} \]

by \((simp add: OclValid_def)\)

\[ OclFalse_is_Invalid[simp]: \neg (\models \textbf{F}) \]

apply \((simp add: OclValid_def OclTrue_def OclFalse_def lift0_def)\)

by \((unfold not_def, rule impI, drule fun_cong, simp)\)

\[ OclUndefined_is_Invalid[simp]: \neg (\models \bot) \]

204
The Standardization Rules of Local Validity Statements.

**lemma OclTrue_is_LocalValid [simp]:** \( \tau \vDash T \)

**by** (simp add: OclLocalValid_def)

**lemma OclFalse_is_LocalInvalid [simp]:** \( \neg (\tau \vDash F) \)

**by** (simp add: OclLocalValid_def OclTrue_def OclFalse_def lift0_def)

**lemma OclUndefined_is_LocalInvalid [simp]:** \( \neg (\tau \vDash \bot) \)

**by** (simp add: OclLocalValid_def OclTrue_def OclUndefined_def lift0_def)

On the basis of the standardization rules, the simplifier can already rule out a number of absurd validity statements:

**lemma isdef_congr [simp]:** \( (\tau \vDash \partial(\neg A)) = (\tau \vDash \partial(A)) \)

**by** simp

**lemma (\tau \vDash \partial(\neg A)) = (\tau \vDash \partial(A))**

**by** simp

**lemma \( \tau \vDash \partial(T) \)**

**by** simp

**lemma \( \tau \vDash \partial(F) \)**

**by** simp

**lemma \neg(\tau \vDash \partial(\bot))**

**by** simp

**lemma \neg(\tau \vDash \partial(T))**

**by** simp

**lemma \neg(\tau \vDash \partial(F))**

**by** simp

**lemma \( \tau \vDash \partial(\bot) \)**

**by** simp

**lemma \( \tau \vDash \partial(T) \)**

**by** simp

**Another Foundational Fact:** non_quatrium_datur

**lemma non_quatrium_datur: \( \tau \vDash A \lor (\tau \vDash \neg A) \lor (\tau \vDash \neg A) \)**

**apply** (simp add: isUndefined_charn_local [symmetric])

**apply** (simp add: is_FALSE_charn_local [symmetric])

**apply** (cut_tac base_distinct)

**apply** (auto simp: OclLocalValid_def)

**done**

**ML_setup** 

fun prover4 (goal, name) =  
let val thm = prove_goal (the_context())  
[OclFalse_def, OclTrue_def, OclUndefined_def, lift0_def]  
goal (fn _ => auto_tac (claset(), simpset()),  
TRY(drule fun_cong)),

205
Appendix B. Isabelle Theories

\begin{quote}
\texttt{
auto_tac(claset(),simpset())
}
\end{quote}

\begin{quote}
in \texttt{bind_thm(name,thm);}
Addsimps[thm]
end;
\end{quote}

\textbf{ML_setup} \langle \langle 
map prover4
\begin{quote}
\begin{itemize}
\item [(F \neq \bot, \text{\texttt{not\_FALSE\_undef}}),]
\item [(\bot \neq F, \text{\texttt{not\_undef\_FALSE}}),]
\item [(T \neq \bot, \text{\texttt{not\_TRUE\_undef}}),]
\item [(\bot \neq T, \text{\texttt{not\_undef\_TRUE}}),]
\item [(F \neq T, \text{\texttt{not\_FALSE\_TRUE}}),]
\item [(T \neq F, \text{\texttt{not\_TRUE\_FALSE}}),]
\item [(F \tau \neq \bot, \text{\texttt{not\_FALSE\_undef\_st}}),]
\item [(\bot \tau \neq F, \text{\texttt{not\_undef\_FALSE\_st}}),]
\item [(T \tau \neq \bot, \text{\texttt{not\_TRUE\_undef\_st}}),]
\item [(\bot \tau \neq T, \text{\texttt{not\_undef\_TRUE\_st}}),]
\item [(F \tau \neq T, \text{\texttt{not\_FALSE\_TRUE\_st}}),]
\item [(T \tau \neq F, \text{\texttt{not\_TRUE\_FALSE\_st}})];
\end{itemize}
\end{quote}
\rangle \rangle
\end{quote}

\textbf{lemma absurd1:} \llbracket \tau \models A; \tau \models \neg A \rrbracket \Longrightarrow R
\begin{quote}
by \texttt{(auto simp add: is\_FALSE\_charn\_local \{symmetric\},
\quad simp add: OclLocalValid\_def)}
\end{quote}

\textbf{lemma absurd1S:} \tau \models A \Longrightarrow \neg (\tau \models \neg A)
\begin{quote}
apply \texttt{(rule\_tac Pa = False in swap,simp\_all)}
by \texttt{(erule absurd1,simp)}
\end{quote}

\textbf{lemma absurd2:} \llbracket \tau \models A; \tau \models \partial A \rrbracket \Longrightarrow R
\begin{quote}
apply(\texttt{simp add: isUndefined\_charn\_local\{symmetric\}})
apply(\texttt{simp add: is\_TRUE\_charn\_local\{symmetric\}})
done
\end{quote}

\textbf{lemma absurd2S:} \tau \models A \Longrightarrow \neg (\tau \models \partial A)
\begin{quote}
apply \texttt{(rule\_tac Pa = False in swap,simp\_all)}
by \texttt{(erule absurd2,simp)}
\end{quote}

\textbf{lemma absurd3:} \llbracket \tau \models \neg A; \tau \models \partial A \rrbracket \Longrightarrow R
\begin{quote}
apply(\texttt{simp add: isUndefined\_charn\_local\{symmetric\}})
apply(\texttt{simp add: is\_FALSE\_charn\_local\{symmetric\}})
done
\end{quote}
lemma absurd3S: τ ⊨ ¬ A =⇒ (τ ⊨ A)
apply (erule_tac Pa = False in swap, simp_all)
by (erule absurd3, simp)

lemma absurd4: [ τ ⊨ ( κ A ) ] =⇒ R
by (simp add: OclLocalValid_def)

lemma absurd4S[simp]: ( τ ⊨ ( κ A ) )
by (simp add: OclLocalValid_def)

lemma absurd5: [ τ ⊨ ⊥ ] =⇒ R
by (simp add: OclLocalValid_def)

lemma absurd5S[simp]: ( τ ⊨ ⊥ )
by (simp add: OclLocalValid_def)

lemma absurd6: [ τ ⊨ F ] =⇒ R
by (simp add: OclLocalValid_def)

lemma absurd6S[simp]: ( τ ⊨ F )
by (simp add: OclLocalValid_def)

lemmas absurdE = absurd1 absurd2 absurd3 absurd4 absurd5 absurd6
lemmas absurdS = absurd1S absurd2S absurd3S absurd4S absurd6S absurd6S

declare absurdE [elim]

ML_setup ⟨⟨
val OCL_absurd_tac = best_tac (HOL_cs addEs
[(thm absurd1), (thm absurd2), (thm absurd3)])
⟩⟩

lemma not_valid: (¬ ( τ ⊨ A )) = (( (τ ⊨ ¬ A ) ∨ ( τ ⊨ A ))
apply (cut_tac τ = τ and A = A in non_quatrium_datur)
apply auto
done

lemma not_invalid: (¬ ( τ ⊨ ¬ A )) = (( (τ ⊨ A ) ∨ ( τ ⊨ A ))
by (cut_tac τ = τ and A = A in non_quatrium_datur, auto)

lemma not_isUndefined: (¬ ( τ ⊨ A )) = ( ( (τ ⊨ A ) ∨ ( τ ⊨ ¬ A ))
by (cut_tac τ = τ and A = A in non_quatrium_datur, auto)
lemma isUndefined_eq_not_isDefined[simp]:
\[\neg (\tau \models \partial A) = (\tau \models \neg \partial A)\]
apply auto
apply (drule not_valid [THEN iffD1], auto simp: OclLocalValid_def)
done

lemma not_isUndefined_eq_isDefined[simp]:
\[\neg (\tau \models \neg \partial A) = (\tau \models \partial A)\]
apply (subst isUndefined_eq_not_isDefined[symmetric])
apply (rule HOL.not_not)
done

lemma not_isUndefined2: \[(\tau \models \partial A) = (\tau \models A) \lor (\tau \models \neg A)\]
by (simp add: not_isUndefined[symmetric])

lemmas norm_validS =
not_valid
not_invalid
not_isUndefined
isUndefined_eq_not_isDefined
not_isUndefined_eq_isDefined

Global (Universal) vs. Local Validity
lemma global_vs_local_validity: \[(\forall \tau. (\tau \models A)) = (\models A)\]
by (auto simp:OclLocalValid_def OclValid_def,
rule ext,erule_tac x=x in allE, assumption)

lemma valid_intro: \[\models A\]
by (simp only:OclLocalValid_def OclValid_def)

lemma valid_elim: \[\tau \models A\]
by (simp only:OclLocalValid_def OclValid_def)

Universal Congruence vs. Judgement Equivalence
lemma equiv_I:
assumes a1: \[(\forall \tau. ((\tau \models A) = (\tau \models B)))\]
and a2: \[(\forall \tau. ((\tau \models \neg A) = (\tau \models \neg B)))\]
shows \[A = B\]
apply (rule ext)
apply (cut_tac \tau=x and A=A in non_quatium_datur)
apply (erule disjE)
apply (cut_tac [2] disjE)
apply (cut_tac \tau=I=x in a1 [THEN iffD1])
apply (cut_tac [4] \tau=I=x in a2 [THEN iffD1])
Absolute equivalence of OCL formula can be expressed in terms of absolute validity as follows:

**lemma equiv_D:**

\((A = B) = ((\forall \tau. (\tau \models A) = (\tau \models B)) ) \land (\forall \tau. ((\tau \models \emptyset A) = (\tau \models \emptyset B)))\)

by (auto intro!:equiv_I)

Local equivalence of OCL formula can be expressed in terms of local validity as follows:

**lemma equiv_D_local:**

\((A \tau B \tau) = ((\forall \tau. (\tau \models A) = (\tau \models B))) \land (\forall \tau. ((\tau \models \emptyset A) = (\tau \models \emptyset B)))\)

apply (auto)
apply (simp_all add: isUndefined_charn_local [symmetric])
apply (auto)
apply (simp_all only: not_valid)
apply auto
apply (simp_all add: is_FALSE_charn_local [symmetric])
apply (simp_all add: OclLocalValid_def)
done

**lemma equiv_I':**

assumes \(A: \land \tau. ((\tau \models A) = (\tau \models B))\)
and \(B: \land \tau. ((\tau \models \neg A) = (\tau \models \neg B))\)
shows \(A = B\)
apply (rule ext)
apply (cut_tac \tau = x and \(A = A\) in non_quatrium_datur, safe)
apply (cut_tac \tau1 = x in A [THEN iffD1])
apply (cut_tac \[\] \tau1 = x in B [THEN iffD1])
apply auto
apply (simp only: OclLocalValid_def)
apply (simp only: is_FALSE_charn_local [symmetric])
apply (cut_tac \tau = x and \(A = B\) in non_quatrium_datur)
apply (safe)
apply (drule A [THEN iffD2])
Appendix B. Isabelle Theories

apply (drule_tac [2] B THEN iffD2)
apply auto
apply (simp only: isUndefined_charn_local [symmetric])
done

lemma equiv_D':
(A = B) = ((\forall \tau. (\tau \models A) = (\tau \models B)) \land (\forall \tau. ((\tau \models \neg A) = (\tau \models \neg B))))
by(auto intro!:equiv_I')

lemma equiv_D'_local:
(A \tau = B \tau) = (((\tau \models A) = (\tau \models B)) \land (((\tau \models \neg A) = (\tau \models \neg B))))
apply (auto)
apply (simp_all add: is_FALSE_charn_local [symmetric])
apply (simp_all only: not_valid not_invalid is_FALSE_charn_local)
apply auto
apply (simp_all only: OclLocalValid_def)
done

The Theory of Strong and Strict Equality

The Setup: cp, strictness, definedness.
lemmas cp_strongEq = OclStrongEq_def [THEN cp_lift2_fw, standard]
lemmas cp_strictEq = OclStrictEq_def [THEN cp_lift2_fw, standard]
declare cp_strongEq [intro!] cp_strictEq [intro!]

lema isDefined_strongEq iff simp:[| \\models X \equiv Y |]
by(auto simp: OclIsDefined_def OclStrongEq_def
     lift2_def lift1_def lift0_def
     OclUndefined_def o_def OclTrue_def
     DEF_def OclValid_def)

lemmas isDefined_strictEq = OclStrictEq_def [THEN lift2_strictify_is_isdef_fw, standard]
lemmas OclUndefined__strictEq = OclStrictEq_def [THEN lift2_undef1a_fw, standard]
lemmas strictEq__undef = OclStrictEq_def [THEN lift2_undef2a_fw, standard]
declare isDefined_strictEq [simp]
OclUndefined__strictEq [simp]
strictEq__undef [simp]

Properties of Strong Equality
lemma StrongEq_notvalid [simp]:
B.4. Library

\[ \tau \models \partial x, \tau \models \partial y \implies (x \triangle y) \tau = \mathcal{F} \tau \]

by (simp add: localValidDefined2sem localValidUnDefined2sem DEF_def OclStrongEq_def OclFalse_def lift0_def lift2_def)

lemma StrongEq_notvalid2[simp]:
\[ \tau \models \partial x, \tau \models \partial y \implies (x \triangle y) \tau = \mathcal{F} \tau \]
by (auto simp: localValidDefined2sem localValidUnDefined2sem DEF_def OclStrongEq_def OclFalse_def lift0_def lift2_def)

lemma StrongEq_valid_undef:
\[ \tau \models \partial x, \tau \models \partial y \implies (x \triangle y) \tau = \mathcal{T} \tau \]
will be proven in |OCL.Logic| by: by (ocl_hypsubst, simp)

oops

lemma strictEq_is_strongEq_LE:
\[ \tau \models \partial a, \tau \models \partial b \implies (a \triangle b) \tau = (a \triangle b) \tau \]
by (simp add: OclStrongEq_def OclStrictEq_def OclTrue_def o_def OclIsDefined_def lift0_def lift1_def lift2_def OclLocalValid_def)

In the theory files, this section contains the SML code that implements OCL_normal_tac.

lemma strictEq_is_strongEq[simp]:
\[ \models \partial a; \models \partial b \implies a \triangle b = a \triangle b \]
by (tactic OCL_normal_tac (get_local_clasimpset ctxt)
(thenstrictEq_is_strongEq_LE) 1)

lemma isDefined_if_valid:
\[ \tau \models A \implies \tau \models \partial A \]
by (rule classical,
    auto simp: OclTrue_def OclIsDefined_def lift0_def lift1_def lift2_def o_def OclLocalValid_def)

lemma localvalid_strictEq_implies_localvalid_strongEq:
\[ \tau \models a \triangle b \implies \tau \models a \triangle b \]
apply (frule isDefined_if_valid,
simp only: OclStrictEq_def)
apply (THEN lift2_strictify_implies_LocalValid_defined)
done
Appendix B. Isabelle Theories

lemma \texttt{strongEq\_subst}:  
\[ [a \triangleq b = \text{T}; P a = \text{T}; cp P] \rightarrow P b = \text{T} \]  
apply (unfold OclStrongEq\_def OclTrue\_def lift0\_def lift1\_def lift2\_def)  
apply (rule ext)  
apply (drule_tac x = s in fun_cong)  
apply (drule_tac x = s in fun_cong)  
apply (simp add: cp\_def)  
apply (erule exE)  
apply (rotate\_tac -1)  
apply simp  
done

lemma \texttt{strongEq\_refl\_UC\_simp} : (a \triangleq a) = \text{T}  
apply (rule ext)  
by (simp add: OclStrongEq\_def OclTrue\_def lift0\_def lift2\_def)

lemma \texttt{strongEq\_refl} \(\triangleright a \triangleq a \text{ by simp}

lemma \texttt{strictEq\_refl\_UC\_simp} :  
\[(\neq \partial) a \]  
by simp

lemma \texttt{strongEq\_sym} :  
\(\models a \triangleq b \models b \triangleq a\)  
apply (unfold OclStrongEq\_def OclTrue\_def lift0\_def lift2\_def OclValid\_def)  
apply (rule ext)  
apply (drule_tac x = \tau in fun_cong)  
apply simp  
done

lemma \texttt{strongEq\_trans} :  
\[ (a \triangleq b; b \triangleq c) \rightarrow a \triangleq c \]  
apply (unfold OclStrongEq\_def OclTrue\_def lift0\_def lift2\_def OclValid\_def)  
apply (rule ext)  
apply (drule_tac x = \tau in fun_cong)  
apply (drule_tac x = \tau in fun_cong)  
apply simp  
done

lemma \texttt{strongEq\_refl\_locak} : \(\triangleright a \triangleq a \text{ by simp add: OclStrongEq\_def OclLocalValid\_def OclTrue\_def lift0\_def lift2\_def})

lemma \texttt{strongEq\_sym\_locak} : \(\triangleright a \triangleq b \models \tau \triangleq b \triangleq a\)
Lemma \(\text{strongEq\_trans\_local}\):  
\[
\begin{array}{c}
\preceq\tau a b ; \preceq\tau b c \Rightarrow \preceq\tau a c
\end{array}
\]

Extensionality must swap parameters and therefore looks quite inelegant ...

Lemma \(\text{strongEq\_ext\_local}\):  
\[
\begin{array}{c}
\forall x. \preceq\tau f x g x \Rightarrow \preceq\tau (\lambda X. f X) (\lambda X. g X)
\end{array}
\]

Technical Substitution Lemmas (for tactics)

Lemma \(\text{strongEq1}\):  
\[
\begin{array}{c}
\preceq\tau X Y ; \preceq\tau P Y ; \preceq\tau P X
\end{array}
\]

by (drule \text{strongEq\_sym\_local})
Appendix B. Isabelle Theories

```
erule strongEq_subst_local simp

lemmas strongEq1_rev = strongEq1[OF strongEq_sym_local]

lemma strongEq2:
[\tau \models X \triangleq Y; (\tau \models P Y) = (\tau \models P' Y); cp P; cp P']
implies (\tau \models P X) = (\tau \models P' X)
apply (rule iffI)
apply (rule_tac X=X in strongEq1, simp_all, drule sym, simp)
apply (erule strongEq1_rev, simp_all)
apply (rule_tac X=X in strongEq1, simp_all)
apply (simp, erule strongEq1_rev, simp_all)
done

lemmas strongEq2_rev = strongEq2[OF strongEq_sym_local]

lemma strongEq3:
[\tau \models X \triangleq Y; P Y \tau = P' Y \tau; cp P; cp P']
implies P X \tau = P' X \tau
apply (rule_tac P=P and P'=P' in ocl_cp_subst3, simp_all)
apply (simp add: OclLocalValid_def OclStrongEq_def strictify_def o_def lift0_def lift1_def lift2_def OclNot_def OclTrue_def OclFalse_def OclUndefined_def DEF_def)
done

lemmas strongEq3_rev = strongEq3[OF strongEq_sym_local]

lemma strongEq1_fw:
[\tau \models P X; \tau \models Y \triangleq X; cp P]
implies \tau \models P Y
by (erule strongEq1, simp)

lemma strongEq2_fw:
[(\tau \models P X) = (\tau \models P' X); \tau \models Y \triangleq X; cp P; cp P']
implies (\tau \models P X) = (\tau \models P' X)
by (erule strongEq2, simp_all)

lemma strongEq3_fw:
[P X \tau = P' X \tau; \tau \models Y \triangleq X; cp P; cp P']
implies P Y \tau = P' Y \tau
by (erule strongEq3, simp_all)

lemma strongEq1_fw2:
[\tau \models P X; \tau \models X \triangleq Y; cp P]
implies \tau \models P Y
by (erule strongEq1_rev, simp)

lemma strongEq2_fw2:
[(\tau \models P X) = (\tau \models P' X); \tau \models X \triangleq Y; cp P; cp P']
implies (\tau \models P X) = (\tau \models P' X)
by (erule strongEq2_rev, simp_all)

214
```
B.4. Library

lemma strongEq3_fw2:
\[ P \tau = P' X \tau; \tau \vdash X \triangleq Y; cp P; cp P' \] \implies P Y \tau = P' Y \tau
by (erule strongEq3_rev, simp_all)

Automated Canonization and Rewriting in OCL

OCL offers a number of equivalences: From strict and strong equality, we have three
types of congruences/equivalences, such that reasoning about them is tedious and must
be tactically supported. The ultimate goal of this section is to work out two tactic
procedures for this purpose that pursue this goal. As basis for these tactic procedures,
a number of rules and rule variants must be derived, whose existence is merely justified
by deduction technical reasons.

validity propagation rules

lemmas strictEq1 = strongEq1 [OF localvalid_strictEq_implies_localvalid_strongEq]
lemmas strictEq2 = strongEq2 [OF localvalid_strictEq_implies_localvalid_strongEq]
lemmas strictEq3 = strongEq3 [OF localvalid_strictEq_implies_localvalid_strongEq]

lemmas strictEq1_rev = strictEq1_rev [OF localvalid_strictEq_implies_localvalid_strongEq]
lemmas strictEq2_rev = strictEq2_rev [OF localvalid_strictEq_implies_localvalid_strongEq]
lemmas strictEq3_rev = strictEq3_rev [OF localvalid_strictEq_implies_localvalid_strongEq]

lemma subst_LJ_TRUE:
\[ \tau \vdash X; \tau \vdash P \top; cp P \] \implies \tau \vdash P X
apply (simp add: OclLocalValid_def, drule sym)
apply (erule_tac P = P in ocl_cp_subst.auto)
done

lemma subst_LJ_TRUE_fw:
\[ \tau \vdash X; \tau \vdash P X; cp P \] \implies \tau \vdash P \top
apply (simp add: OclLocalValid_def)
apply (erule_tac P = P in ocl_cp_subst)
apply auto
done

lemma subst_LJ_TRUE_fw_rev:
\[ \tau \vdash P X; \tau \vdash X; cp P \] \implies \tau \vdash P \top
apply (simp add: OclLocalValid_def)
apply (erule_tac P = P in ocl_cp_subst) back back

215
Appendix B. Isabelle Theories

apply auto
done

lemma subst_LE_TRUE:
\[ [\tau \models X; P \top \tau = P' \top \tau; cp P; cp P'] \Rightarrow P X \tau = P' X \tau \]
apply(rule local_validity_propagation2 [simplified is_TRUE_charn_local]) back
by auto

lemma subst_LE_TRUE-fw:
\[ [\tau \models X; P X \tau = P' X \tau; cp P; cp P'] \Rightarrow P \top \tau = P' \top \tau \]
apply(simp add: OclLocalValid_def)
apply(rule trans, rule sym)
apply(erule_tac \tau = \tau and P = P in cp_charn, simp)
apply(rule trans, assumption)
apply(erule_tac \tau = \tau and P = P' in cp_charn, simp)
done

lemma subst_LE_TRUE-fw_rev:
\[ [P \top X :: a \Rightarrow Boolean_0 \tau = P' \top X \tau; \tau \models X; cp P; cp P'] \Rightarrow P \top \tau = P' \top \tau \]
by(erule subst_LE_TRUE_fw, auto)

lemma subst_LJE_TRUE:
\[ [\tau \models X; (\tau \models P \top \tau) = (\tau \models P' \top \tau); cp P; cp P'] \Rightarrow (\tau \models P X) = (\tau \models P' X) \]
by(erule subst_LE_TRUE, auto)

lemma subst_LJE_TRUE-fw:
\[ [\tau \models X; (\tau \models P X) = (\tau \models P' X); \tau \models X; cp P; cp P'] \Rightarrow (\tau \models P \top \tau) = (\tau \models P' \top \tau) \]
by(erule subst_LE_TRUE-fw, auto)

lemma subst_LJE_TRUE-fw_rev:
\[ [(\tau \models P X) = (\tau \models P' X); \tau \models X; cp P; cp P'] \Rightarrow (\tau \models P \top \tau) = (\tau \models P' \top \tau) \]
by(erule subst_LJE_TRUE-fw, auto)

lemma subst_TRUE_LJE:
\[ [\tau \models X; cp P] \Rightarrow (\tau \models P X) = (\tau \models P \top) \]
apply(auto)
apply(erule subst_LJ_TRUE-fw, auto)
apply(erule subst_LJ_TRUE, auto)
done

216
lemma subst_LJ_FALSE:
\[ \begin{align*}
\mathbb{L} & \vdash \neg X; \mathbb{L} \vdash P F; \text{cp } P \implies \mathbb{L} \vdash P X \\
\text{apply} & \hspace{1em} \text{(drule is\_FALSE\_chern\_local [THEN iffD2])} \\
\text{apply} & \hspace{1em} \text{(rotate\_tac \(-I\))} \\
\text{apply} & \hspace{1em} \text{(drule sym)} \\
\text{apply} & \hspace{1em} \text{(simp add: OclLocalValid\_def)} \\
\text{apply} & \hspace{1em} \text{(erule_tac P = P in ocl\_cp\_subst)} \\
\text{apply} & \hspace{1em} \text{auto} \\
\text{done}
\end{align*} \]

lemma subst_LJ_FALSE/fw:
\[ \begin{align*}
\mathbb{L} & \vdash \neg X; \mathbb{L} \vdash P X; \text{cp } P \implies \mathbb{L} \vdash P F \\
\text{apply} & \hspace{1em} \text{(drule is\_FALSE\_chern\_local [THEN iffD2])} \\
\text{apply} & \hspace{1em} \text{(rotate\_tac \(-I\))} \\
\text{apply} & \hspace{1em} \text{(simp add: OclLocalValid\_def)} \\
\text{apply} & \hspace{1em} \text{(erule_tac P = P in ocl\_cp\_subst)} \\
\text{apply} & \hspace{1em} \text{auto} \\
\text{done}
\end{align*} \]

lemma subst_LJ_FALSE/fw_rev:
\[ \begin{align*}
\mathbb{L} & \vdash P X; \mathbb{L} \vdash \neg X; \text{cp } P \implies \mathbb{L} \vdash P F \\
\text{apply} & \hspace{1em} \text{(erule subst_LJ_FALSE/fw)} \\
\text{apply} & \hspace{1em} \text{auto} \\
\text{done}
\end{align*} \]

lemma subst_LE_FALSE:
\[ \begin{align*}
\mathbb{L} & \vdash \neg X; \mathbb{L} \vdash P F; \text{cp } P = \text{cp } P' \implies \mathbb{L} \vdash P X = P' X \\
\text{apply} & \hspace{1em} \text{(rule local\_validity\_propagation3 [simplified is\_FALSE\_chern\_local])} \\
\text{back} & \hspace{1em} \text{(erule subst_LJ_FALSE/fw, auto)} \\
\text{done}
\end{align*} \]

lemma subst_LE_FALSE-fw:
\[ \begin{align*}
\mathbb{L} & \vdash \neg X; \mathbb{L} \vdash P X; \text{cp } P = \text{cp } P' \implies \mathbb{L} \vdash P F = P' F \\
\text{apply} & \hspace{1em} \text{(simp only: is\_FALSE\_chern\_local[symmetric])} \\
\text{apply} & \hspace{1em} \text{(rule trans, rule sym)} \\
\text{apply} & \hspace{1em} \text{(erule_tac P = P in cp\_charn, simp)} \\
\text{apply} & \hspace{1em} \text{(rule trans, assumption)} \\
\text{apply} & \hspace{1em} \text{(erule_tac P = P in cp\_charn, simp)} \\
\text{done}
\end{align*} \]

lemma subst_LE_FALSE-fw_rev:
\[ \begin{align*}
\mathbb{L} & \vdash P X (\tau :: 'a) = P' X \tau; \mathbb{L} \vdash \neg \bar{X}; \text{cp } P; \text{cp } P' \implies \mathbb{L} \vdash P F = P' F \\
\text{by} & \hspace{1em} \text{(erule subst\_LE\_FALSE\_fw, auto)} \\
\text{done}
\end{align*} \]

lemma subst_LJE_FALSE:
\[ \begin{align*}
\mathbb{L} & \vdash \neg X; \mathbb{L} \vdash P F = (\tau \vdash P' F); \text{cp } P; \text{cp } P' \implies (\tau \vdash P X) = (\tau \vdash P' X) \\
\text{by} & \hspace{1em} \text{(erule subst\_LE\_FALSE, auto)} \\
\text{done}
\end{align*} \]
Appendix B. Isabelle Theories

lemma subst_LJE_FALSE_fw:
\[ \begin{align*}
\tau \models \neg X; (\tau \models P X) & \Rightarrow (\tau \models P F) = (\tau \models P' F) \\
\text{by (erule subst_LE_FALSE_fw, auto)}
\end{align*} \]

lemma subst_LJE_FALSE_fw_rev:
\[ \begin{align*}
\tau \models P X; \tau \models \neg X; cp P; cp P' & \Rightarrow (\tau \models P F) = (\tau \models P' F) \\
\text{by (erule subst_LJE_FALSE_fw, auto)}
\end{align*} \]

lemma subst_FALSE_LJE:
\[ \begin{align*}
\tau \models \neg X; cp P & \Rightarrow (\tau \models P X) = (\tau \models P F) \\
\text{apply (auto)}
\end{align*} \]

lemma subst_LJ_undef:
\[ \begin{align*}
\tau \models \neg X; \tau \models P \bot; cp P & \Rightarrow (\tau \models P X) \\
\text{apply (rule_tac P = P and \tau = \tau in ocl_cp_subst)}
\end{align*} \]

lemma subst_LJ_undef_fw:
\[ \begin{align*}
\tau \models \neg X; \tau \models P \bot; cp P & \Rightarrow (\tau \models P \bot) \\
\text{apply (erule subst_LJ_undef, auto)}
\end{align*} \]

lemma subst_LJ_undef_rev:
\[ \begin{align*}
\tau \models P \bot; \tau \models \neg X; cp P & \Rightarrow (\tau \models P X) \\
\text{by (erule subst_LJ_undef_fw, auto)}
\end{align*} \]

lemma subst_LE_undef:
\[ \begin{align*}
\tau \models \neg X; P \bot; \tau = P' \bot; cp P; cp P' & \Rightarrow P X \tau = P' X \tau \\
\text{apply (rule_tac P=P and \tau=\tau in ocl_cp_subst3)}
\end{align*} \]
apply (simp_all)
apply (simp add: OclLocalValid_def OclIsDefined_def strictify_def OclNot_def o_def lift0_def lift1_def lift2_def OclTrue_def DEF_def OclUndefined_def)
done

lemma subst_LE_undef_fw:
  \[ \tau \not\models \emptyset(X) \land \tau = \tau' \land \tau \models P \land \tau' \models P' \land \tau \]
apply (rule_tac P=P and \tau=\tau in ocl_cp_subst3)
apply (simp_all)
apply (simp add: OclLocalValid_def OclIsDefined_def strictify_def OclNot_def o_def lift0_def lift1_def lift2_def OclTrue_def DEF_def OclUndefined_def)
done

lemma subst_LE_undef_fw_rev:
  \[ \tau \models \emptyset(X) \land \tau = \tau' \land \tau \models P \land \tau \models P' \land \tau \]
by (erule subst_LE_undef_fw, auto)

lemma subst_LJE_undef:
  \[ \tau \models \emptyset(X) \land \tau = \tau' \land \tau \models P \land \tau' \models P' \land \tau \models P \land \tau' \models P' \land \tau \]
by (erule subst_LE_undef, auto)

lemma subst_LJE_undef_fw:
  \[ \tau \models \emptyset(X) \land \tau = \tau' \land \tau \models P \land \tau' \models P' \land \tau \models P \land \tau' \models P' \land \tau \]
by (erule subst_LJE_undef_fw, auto)

lemma subst_LJE_undef-fw_rev:
  \[ \tau \models \emptyset(X) \land \tau = \tau' \land \tau \models P \land \tau \models P' \land \tau \models P \land \tau' \models P' \land \tau \]
by (erule subst_LJE_undef-fw, auto)

lemma subst_LJE_undef:
  \[ \tau \models \emptyset(X) \land \tau = \tau' \land \tau \models P \land \tau \models P' \land \tau \models P \land \tau' \models P' \land \tau \]
apply (auto)
apply (erule subst_LJE_undef, auto)
apply (erule subst_LJE_undef, auto)
done

lemmas strictEq1-fw2 = strongEq1-fw2
  \[ OF \_ localvalid_strictEq_implies_localvalid_strongEq \]
lemmas strictEq2-fw2 = strongEq2-fw2
  \[ OF \_ localvalid_strictEq_implies_localvalid_strongEq \]
lemmas strictEq3-fw2 = strongEq3-fw2
  \[ OF \_ localvalid_strictEq_implies_localvalid_strongEq \]
lemmas strictEq1-fw = strongEq1-fw
  \[ OF \_ localvalid_strictEq_implies_localvalid_strongEq \]
Appendix B. Isabelle Theories

lemmas strictEq2_fw = strongEq2_fw
OF localvalid_strictEq_implies_localvalid_strongEq

lemmas strictEq3_fw = strongEq3_fw
OF localvalid_strictEq_implies_localvalid_strongEq

Implementation of OCL_hyp_subst_tac

These rules give some ideas for automation:

1. OCL_norm_tac computes local norm of validities: \( \vdash A \implies B \) is converted \( \tau \vdash A \implies \tau \vdash B \). This is done forward and backward style.

2. OCL_absurd_tac should decide if a subgoal is OCL absurd.

3. OCL_hyp_subst_tac for variables or parameters A, which uses:
   \[
   \begin{align*}
   A = t, t = A & \quad \text{(standard hyp_subst_tac)} \quad \text{(B.6)} \\
   A \tau = t \tau, t \tau = A & \quad \text{(local congruences)} \quad \text{(B.7)} \\
   \vdash \partial A, \tau \vdash \partial A & \quad \text{(undefinednesses local and global)} \quad \text{(B.8)} \\
   \vdash \neg A, \tau \vdash \neg A & \quad \text{(falsities local and global)} \quad \text{(B.9)} \\
   \vdash A \triangleq t, \tau \vdash A \triangleq t & \quad \text{(strong equalities local and global)} \quad \text{(B.10)} \\
   \tau \vdash A \triangleq t, \tau \vdash A \triangleq t & \quad \text{(B.11)}
   \end{align*}
   \]

4. OCL_def_hyp_split_tac:
   - atomizes definedness hypotheses, e.g., \( \partial(f A B) = \partial A \land \partial B \) ...
   - case-splits undefinedness hypothesis \( \partial(f A B) = \partial(A) \lor \partial(B) \) ...
   - and performs safe_tac and OCL_hyp_subst_tac. (but no global simplification afterwards in order to do not too much in a black box.

5. OCL_simp and OCL_asm_simp. New rewriter that can cope with \( \_ \triangleq \_ \) and \( \_ = \_ \) and its specific format of the subst rule. Future: use standard rewriter with a fake subst rule on OCL, transform the proof objects and refeed this into the kernel?

6. integrate into simp-procedure as looper or subgoaler.


B.4. Library

Testing OCL_hyp_subst_tac

lemma \([ \tau \models A; \tau \models \neg B; \tau \models A \land B ; \tau \models \emptyset B ] \implies \tau \models A \land B \land C\]
by(tacticOCL_hyp_subst_tac (get_local_clasimpset ctxt) 1, simp)

lemma \([ \tau \models A; \tau \models A \land B ; \tau \models \emptyset B; (\tau \models A) = (\tau \models C) ] \implies A \models B \tau\]
by(tacticOCL_hyp_subst_tac (get_local_clasimpset ctxt) 1, simp)

lemma \(!\tau A . \models \tau A; \tau \models A \land B ; \tau \models \emptyset B; (\tau \models A) = (\tau \models C) ] \implies A \models B \tau\]
by(tacticOCL_hyp_subst_tac (get_local_clasimpset ctxt) 1, simp)

lemma \([ \tau \models A; \tau \models D \triangleq E ; \tau \models D \triangleq I ] \implies \tau \models A \land E \triangleq I\]
by(tacticOCL_hyp_subst_tac (get_local_clasimpset ctxt) 1, simp)

lemma \([ \tau \models A; \tau \models E \triangleq D ; \tau \models I \triangleq E ; \tau \models I \triangleq D ] \implies \tau \models A \land E \triangleq I\]
by(tacticOCL_hyp_subst_tac (get_local_clasimpset ctxt) 1, simp)

lemma \([ \tau \models A; \tau \models \neg B; \tau \models I \triangleq E; A \models B \tau; \tau \models D \models I; \tau \models D \models E ] \implies \tau \models A \land B\]
apply(tacticOCL_hyp_subst_tac (get_local_clasimpset ctxt) 1)
apply(simp)
done

lemma \([ \tau \models A; \tau \models B; \tau \models E \triangleq I; \tau \models I \models E; \tau \models \emptyset B ] \implies \tau \models A \land B\]
by(tacticOCL_hyp_subst_tac (get_local_clasimpset ctxt) 1, simp)

Testing OCL_subst_tac

lemma isDefined_cong5 : \((\emptyset X \lor \emptyset X) = T\)
apply (rule ext, case_tac x= \emptyset (X))
apply (tacticOCL_subst_tac(false, false, false)
[get_local_clasimpset ctxt] 1, simp_all)
apply (tacticOCL_subst_tac(false, false, false)
[get_local_clasimpset ctxt] 1, simp_all)
done

Some more Absurdities

lemma not_isDefined_if_isUndefined:
\(\tau \models \emptyset A \implies (\neg (\tau \models \emptyset A))\)
by auto

221
Appendix B. Isabelle Theories

lemma non_tertium_datur_if_isDefined:
  \[ \tau \models \partial A; \tau \models A \Longrightarrow P; \tau \models \neg A \Longrightarrow P \] \Longrightarrow P
  by (cut_tac \tau = \tau and A = A in non_quatrium_datur, auto)

lemma isDefined_if_valid:
  \tau \models A \Longrightarrow \tau \models \partial A
  by (rule classical, auto)

lemma isDefined_if_invalid:
  \tau \models \neg A \Longrightarrow \tau \models \partial A
  by (rule classical, auto)

Trichotomy Specialized for if

lemma if_trichotomy:
  \[ \tau \models P \bot; \tau \models P Y; \tau \models P Z; cp P \] \Longrightarrow
  \tau \models P (if X then Y else Z endif)
  apply (simp add: OcIValid_def)
  apply (rule_tac P = \lambda x. P (if \exists Y then Y else Z endif) in cp_distinct_core)
  apply auto
  apply (rule_tac P = P in cp_compose2)
  apply auto
  done

lemma if_trichotomyE:
  \[ \tau \models P (if X then Y else Z endif);
      \tau \models P \bot \Longrightarrow R;
      \tau \models P Y \Longrightarrow R;
      \tau \models P Z \Longrightarrow R;
      cp P \] \Longrightarrow R
  apply (cut_tac \tau = \tau and A = X in non_quatrium_datur)
  apply safe
  apply (drule_tac \exists subst_LJ_undef_fw)
  prefer 3
  apply (assumption)
  apply (rule_tac \exists P = P in cp_compose2, simp_all)
  apply (drule_tac \exists subst_LJ_FALSE_fw)
  prefer 2
  apply (assumption)
  apply (drule subst_LJ_TRUE_fw)
  back
  apply (assumption)
  apply auto
  apply (rule_tac \exists P = P in cp_compose2)

222
apply (rule_tac P = P in cp_compose2)
apply auto
done

lemmas OclIf_LJE[simp] =
  subst_TRUE_LJE[of _ _ λX. if X then Y else Z endif, simplified]
  subst_FALSE_LJE[of _ _ λX. if X then Y else Z endif, simplified]
  subst_undef_LJE[of _ _ λX. if X then Y else Z endif, simplified]

A Weak (Propositional) \([\text{LJE}]\) Calculus for Propositional OCL

The weak propositional \([\text{LJE}]\) gives rise to a fairly promising decision procedure for a fragment of OCL:

- blow away quantifiers
- infer from inclusions of variables the invariants
- infer from the invariants the definedness of variables
- all remaining variables occurring in formula: case-splitting over definedness, congruence closure over undefinednesses,
- simp_all: universal congruences
- simp_all: weak propositional \([\text{LJE}]\)
- blast_tac.

Weak \([\text{LJE}]\) Calculus means here that everything is restricted to defined expressions.

lemma localValidNot2not :
  \[
  [\tau \models \varnothing A] \Longrightarrow (\tau \models \neg A) = (\neg (\tau \models A))
  \]
  by(auto elim!: non_tertium_datur_if_isDefined)

lemma localValidAnd2conj :
  \[
  [\tau \models \varnothing A; \tau \models \varnothing B] \Longrightarrow (\tau \models A \land B) = ((\tau \models A) \land (\tau \models B))
  \]
  apply(auto elim!: non_tertium_datur_if_isDefined)
  by(tactic.ALLGOALS(\text{OCL_hyp_subst_tac (get_local_clasimpset ctxt)},simp_all))
Appendix B. Isabelle Theories

lemma localValidOr2disj:
\[ \llbracket \tau \models \partial A; \tau \models \partial B \rrbracket \Rightarrow (\tau \models A \lor B) = ((\tau \models A) \lor (\tau \models B)) \]
apply (auto elim! : non_tertium_datur_if_isDefined)
by (tacticALLGOALS (OCL_hyp_subst_tac (get_local_clasimpset ctxt)), simp_all)

lemma localValidImplies2impl:
\[ \llbracket \tau \models \partial A; \tau \models \partial B \rrbracket = (\tau \models A \rightarrow B) = ((\tau \models A) \rightarrow (\tau \models B)) \]
by (simp add: OclImplies_def localValidNot2not localValidAnd2conj)

lemma isDefined_notI:
\[ \llbracket \tau \models \partial A \rrbracket = \Rightarrow \tau \models \partial (\neg A) \]
by simp

lemma isDefined_andI:
\[ \llbracket \tau \models \partial A; \tau \models \partial B \rrbracket = \Rightarrow \tau \models \partial (A \land B) \]
apply (auto elim! : non_tertium_datur_if_isDefined)
apply (tacticALLGOALS (OCL_hyp_subst_tac (get_local_clasimpset ctxt)))
apply (simp_all)
done

lemma isDefined_orI:
\[ \llbracket \tau \models \partial A; \tau \models \partial B \rrbracket = \Rightarrow \tau \models \partial (A \lor B) \]
apply (auto elim! : non_tertium_datur_if_isDefined)
apply (tacticALLGOALS (OCL_hyp_subst_tac (get_local_clasimpset ctxt)))
apply (simp_all)
done

lemma isDefined_xorI:
\[ \llbracket \tau \models \partial A; \tau \models \partial B \rrbracket = \Rightarrow \tau \models \partial (A \oplus B) \]
apply (auto elim! : non_tertium_datur_if_isDefined)
apply (tacticALLGOALS (OCL_hyp_subst_tac (get_local_clasimpset ctxt)))
apply (simp_all)
done

lemma isDefined_impliesI:
\[ \llbracket \tau \models \partial A; \tau \models \partial B \rrbracket = \Rightarrow \tau \models \partial (A \rightarrow B) \]
apply (auto elim! : non_tertium_datur_if_isDefined)
apply (tacticALLGOALS (OCL_hyp_subst_tac (get_local_clasimpset ctxt)))
apply (simp_all)
done

lemma isDefined_implies2I:
\[ \llbracket \tau \models \partial A; \tau \models \partial B \rrbracket = \Rightarrow \tau \models \partial (A \rightarrow B) \]
apply (auto elim! : non_tertium_datur_if_isDefined)
apply (tacticALLGOALS (OCL_hyp_subst_tac (get_local_clasimpset ctxt)))
apply (simp_all)
done

lemma localValidImplies22impl:
\[ \llbracket \tau \models \partial A; \tau \models \partial B \rrbracket = \Rightarrow (\tau \models A \rightarrow B) = ((\tau \models A) \rightarrow (\tau \models B)) \]
by (simp add: OclImplies2_def localValidNot2not isDefined_andI localValidOr2disj localValidAnd2conj)
Isar Interface Setup

This part of the so-called thymorpher generates a number of rules and a specific setup for all operators given to him. This includes (all examples are for the case of the weak (strict) equality here.

1. context passingness rules (cp) for all unary and binary operators, e.g.:

\[ \text{cpP; cpP}' \Rightarrow \text{cp}(\lambda X.PX = P'X) \]

These rules were used both as simplifier rules as well as safe introduction rules.

2. all undefinedness reduction rules (unary and binary case), e.g.:

\[ \bot \triangleq X = \bot \text{ and } X \triangleq \bot = \bot \]

These rules were used as global simplifier rules.

3. universal congruences for definedness, e.g.:

\[ \partial X \triangleq Y = \partial X \land \partial Y \]

4. the local judgement equivalence for definedness, e.g.:

\[ \tau \vdash \partial(X \triangleq Y) = (\tau \vdash \partial X \land \tau \vdash \partial Y) \]

This equality is used for optimized reasoning over definedness inside some OCL-tactics.

Definition of ocl_subst

In the theory files, this section contains the Isar setup code for ocl_subst.

Definition of ocl_auto

In the theory files, this section contains the Isar setup code for ocl_auto.

end

B.4.4. OCL Logic

theory OCL_Logic
  imports $HOLOCL_HOME/src/OCL_Logic_core
begin
Appendix B. Isabelle Theories

Testing and Demonstrations of Main Tactics

Automatic Generation of $\mathbf{UC}$ Variants of Global Equivalence Theorems

ML

\[
\begin{align*}
& \text{thm } OCL\_cp\_OclStrictEq \\
& \quad OCL\_undef\_1\_OclStrictEq \\
& \quad OCL\_undef\_2\_OclStrictEq \\
& \quad OCL\_is\_def\_OclStrictEq \\
& \quad OCL\_is\_defopt\_OclStrictEq
\end{align*}
\]

\[
\begin{align*}
& \text{thm } OclIsDefined\_def \\
& \quad ocl\_setup\_op\{OclIsDefined\} \\
& \quad ocl\_setup\_op\{OclStrongEq\} \\
& \quad ocl\_setup\_op\{OclAnd, OclNa\} \\
& \quad ocl\_setup\_op\{OclOr\_alt, OclXor\_alt\} \\
& \quad ocl\_setup\_op\{OclImplies\_alt, OclImplies1\_alt, OclImplies2\_alt\} \\
& \quad ocl\_setup\_op\{OclSand, OclSor\_alt, OclSxor\_alt\} \\
& \quad ocl\_setup\_op\{OclSimplies\_alt\} \\
& \quad ocl\_setup\_op\{OclIf\}
\end{align*}
\]

Test of ocl\_hypsubst

lemma ![τ ⊨ A; τ ⊨ −B; τ ⊨ A ∧ B; τ ⊨ Ø B] ⇒ τ ⊨ A ∧ B
by (ocl\_hypsubst [1], simp)

lemma ![τ ⊨ A; τ ⊨ A ∧ B; τ ⊨ Ø B; (τ ⊨ A) = (τ ⊨ C)] ⇒ A τ = B τ
by (ocl\_hypsubst, simp)

lemma !!τ A. ![τ ⊨ A; τ ⊨ A ∧ B; τ ⊨ Ø B; (τ ⊨ A) = (τ ⊨ C)] ⇒ A τ = B τ
by (ocl\_hypsubst, simp)

lemma ![τ ⊨ A; τ ⊨ D ⊮ E; τ ⊨ D ⊮ I] ⇒ τ ⊨ A ∧ E ⊮ I
by (ocl\_hypsubst, simp)

lemma ![τ ⊨ A; τ ⊨ D ⊮ E; τ ⊨ I ⊮ D] ⇒ τ ⊨ A ∧ E ⊮ I
by (ocl\_hypsubst, simp)

lemma ![τ ⊨ A; τ ⊨ E ⊮ D; τ ⊨ I ⊮ D] ⇒ τ ⊨ A ∧ E ⊮ I
by (ocl\_hypsubst, simp)

lemma ![τ ⊨ A; τ ⊨ −B; τ ⊨ E ⊮ I; τ ⊨ I ⊮ E; τ ⊨ E ⊮ I; τ ⊨ I ⊮ E] ⇒ τ ⊨ A ∧ B
by (ocl\_hypsubst, simp)

Test of ocl\_subst

lemma (Ø X ∨ Ø X) = T
apply (rule ext, case_tac x ⊨ Ø(x))
apply (ocl\_subst (no_asm_simp), simp_all)

226
apply (ocl_subst (no_asm_use)(no_asm_simp)(no_concl_simp) | ocl_subst)
apply (simp)
done

lemma StrongEq_valid_undef :
  \[ \{ \tau \models \varnothing \} x \equiv y \Rightarrow (x \triangleq y) \tau = T \tau \]
by (ocl_hypsubst, simp)

The following lemma explains strong equality entirely in terms of OCL in the sense of the standard, i.e., by using definedness and strict equality, which is the default. Due to strongEq_charn ((\tau \models \exists x \triangleq y) = (\exists x \models \exists y)), the outstanding importance of strong equality becomes obvious. The following lemma explains, why its reformulation in standard operators is possible, but tedious, and represents a post-hoc justification for the introduction strong equality.

lemma strongEq_charn2 :
  (x \triangleq y) = (if \partial x \land \partial y then x \equiv y else if \not\partial x \land \not\partial y then T else F endif)
apply (rule ext, case_tac xa \models \partial (x))
by (ocl_subst, simp_all)

Strong and Weak Definedness Calculi

lemma isDefined_cong5 : (\partial X \lor \not\partial X) = T
apply (rule ext, case_tac x \models \partial (X))
by (ocl_subst, simp_all)

lemma isDefined_cong6 : (\not\partial X \lor \partial X ) = T
apply (rule ext, case_tac x \models \partial (X))
by (ocl_subst, simp_all)

lemma isDefined_cong7 : (\partial X \lor \not\partial X \lor Z) = T
apply (rule ext, case_tac x \models \partial (X))
by (ocl_subst, simp_all)

lemma isDefined_cong8 : (\not\partial X \lor \partial X \lor Z) = T
apply (rule ext, case_tac x \models \partial (X))
Appendix B. Isabelle Theories

by (ocl_subst, simp_all, ocl_subst, simp)

lemma isDefined_cong9 : \( \emptyset X \land \emptyset X = F \)
apply (rule ext, case_tac x \( \vdash \emptyset (X) \))
by (ocl_subst, simp_all, ocl_subst, simp)

lemma isDefined_cong10 : \( \emptyset X \land \emptyset X = F \)
apply (rule ext, case_tac x \( \vdash \emptyset (X) \))
by (ocl_subst, simp_all, ocl_subst, simp)

lemma isDefined_cong11 : \( \emptyset X \land \emptyset X \land Z = F \)
apply (rule ext, case_tac x \( \vdash \emptyset (X) \))
by (ocl_subst, simp_all, ocl_subst, simp)

lemma isDefined_cong12 : \( \emptyset X \land \emptyset X \land Z = F \)
apply (rule ext, case_tac x \( \vdash \emptyset (X) \))
by (ocl_subst, simp_all, ocl_subst, simp)

lemmas core_definedness = OclIsDefined__False OclIsDefined__True OclIsDefined__undef
isDefined_idem isDefined_notD0
isDefined_cong4 isDefined_cong8 isDefined_cong1
isDefined_cong11 isDefined_cong12
isDefined_strongEq [THEN is_TRUE_charn[THEN iffD2]]
isDefined_strictEq

lemmas strong_definedness = core_definedness
isDefined_ifD0 isDefined_andD0 isDefined_impliesD0 isDefined_orD0

lemmas weak_definedness = core_definedness

isDefined_if isDefined_implies
isDefined_or isDefined_and

thm weak_definedness
thm strong_definedness
thm strictEq.is_strongEq.LE

lemmas weak_prop_LJE =
OclTrue.is_Valid OclFalse.is_Invalid OclUndefined.is_Invalid
OclTrue.is_LocalValid absurd6S absurd5S

228
These previous equivalences demonstrate, why a “global judgement equivalence” calculation does not make sense. Desirable versions of these rules would be:

\[ \vdash \neg A \iff (\vdash \neg A) \quad (B.12) \]
\[ \vdash A \lor B \iff (\vdash A) \lor (\vdash B) \quad (B.13) \]
\[ \vdash A \rightarrow B \iff (\vdash A) \rightarrow (\vdash B) \quad (B.14) \]

This is not achievable since the logical disjunction does not disperse over the universal quantifier hidden in the global validity statement.

Thus, a “global judgement equivalence” is not closed under global validity, such that any complete reasoning must be broken down on local judgements sooner or later.

end
### Appendix B. Isabelle Theories

**begin instance up :: (number)number ..**
**instance fun:: (type,number)number ..**

#### OCL Ordering Interface

This is only a syntactic interface for the ordering operators in OCL. Concrete definitions are provided in the structures Integer and Real.

**consts**

- `OclLe :: [(a,b) VAL, (a,b) VAL] => 'a Boolean`
- `OclLess :: [(a,b) VAL, (a,b) VAL] => 'a Boolean`
- `OclGe :: [(a,b) VAL, (a,b) VAL] => 'a Boolean`
- `OclGreater :: [(a,b) VAL, (a,b) VAL] => 'a Boolean`

**syntax**

- `_OclLe_std :: [(a,b) VAL, (a,b) VAL] => 'a Boolean`
  
- `_OclLess_std :: [(a,b) VAL, (a,b) VAL] => 'a Boolean`
  
- `_OclGe_std :: [(a,b) VAL, (a,b) VAL] => 'a Boolean`
  
- `_OclGreater_std :: [(a,b) VAL, (a,b) VAL] => 'a Boolean`

**syntax (xsymbols)**

- `_OclLe_ascii :: [(a,b) VAL, (a,b) VAL] => 'a Boolean`
  
- `_OclLess_ascii :: [(a,b) VAL, (a,b) VAL] => 'a Boolean`
  
- `_OclGe_ascii :: [(a,b) VAL, (a,b) VAL] => 'a Boolean`
  
- `_OclGreater_ascii :: [(a,b) VAL, (a,b) VAL] => 'a Boolean`

- `_OclLe_math :: [(a,b) VAL, (a,b) VAL] => 'a Boolean`
  
- `_OclLess_math :: [(a,b) VAL, (a,b) VAL] => 'a Boolean`
  
- `_OclGe_math :: [(a,b) VAL, (a,b) VAL] => 'a Boolean`
  
- `_OclGreater_math :: [(a,b) VAL, (a,b) VAL] => 'a Boolean`

**end**

---

230
B.4.6. **OCL Integer**

theory OCL_Integer
imports
$HOLOCL_HOME/src/library/basic/OCL_Numerals
begin

consts
  is_Integer_0 :: 'a U ⇒ bool
  is_Integer_0 ≡ sum_case (λx. False)
    (sum_case (λx. True)(λx. False))
  get_Integer_0 :: 'a U ⇒ Integer_0
  get_Integer_0 ≡ sum_case (λx. x. True)
    (sum_case (λx. x. True))
  mk_Integer_0 :: Integer_0 ⇒ 'a U
  mk_Integer_0 ≡ Inr ◦ Inr ◦ Inl

lemma get_mk_Integer_id_0 [simp]:
  get_Integer_0 (mk_Integer_0 x) = x
  apply (simp add: get_Integer_0_def mk_Integer_0_def)
  done

lemma is_mk_Integer_0 [simp]:
  is_Integer_0 (mk_Integer_0 x) = True
  apply (simp add: is_Integer_0_def mk_Integer_0_def)
  done

lemma mk_get_Integer_id_0 [simp]:
  is_Integer_0 x =⇒ mk_Integer_0 (get_Integer_0 x) = x
  apply (simp add: get_Integer_0_def mk_Integer_0_def is_Integer_0_def)
  apply (case_tac x, simp, simp)
  apply (case_tac b, simp, simp)
  done

consts
  Integer_0 :: ('st, Integer_0 Set_0) VAL
  Integer_0 ≡ lift0(Abs_Set_0 [λUNIV.]

defs
  Zero_ocl_int_def: 0 ≡ lift0( _0::int )
  One_ocl_int_def: 1 ≡ lift0( _1::int )

lemma OCL_is_def_Zero_ocl_int [simp]:
  OclIsDefined_def Zero_ocl_int [simp]:
  apply(rule ext)
  apply(simp add: OclIsDefined_def Zero_ocl_int_def OclTrue_def ss_lifting')
  done

lemma OCL_is_def_One_ocl_int [simp]:
  OclIsDefined_def One_ocl_int [simp]:
  apply(rule ext)
Appendix B. Isabelle Theories

apply (simp add: OclIsDefined_def One_ocl_int_def OclTrue_def ss_lifting')
done

defs (overloaded)

number_of_def : (number_of :: bin ⇒ 'a Integer)
≡ λ b. lift0 (number_of::bin ⇒ int) b )

defs

plus_def: op + ≡ lift2 (strictify (λ x::Integer_0. strictify (λ y. ((⌜x⌝) + (⌜y⌝)))))

minus_def: op − ≡ lift2 (strictify (λ x::Integer_0. strictify (λ y. ((⌜x⌝) − (⌜y⌝)))))

times_def: op * ≡ lift2 (strictify (λ x::Integer_0. strictify (λ y. ((⌜x⌝) * (⌜y⌝)))))

ocl_setup_op[plus, minus, times]

lemma plus_zero: (X::'a Integer) + 0 = X
by (rule ext, simp add: plus_def Zero_ocl_int_def ss_lifting')

lemma plus_commute: (X::'a Integer) + Y = Y + X
by (rule ext, simp add: plus_def ss_lifting')

defs

OclLe_def: OclLe ≡ lift2 (strictify (λ x::Integer_0. strictify (λ y. ((⌜x⌝) <= (⌜y⌝)))))

OclLess_def: OclLess ≡ lift2 (strictify (λ x::Integer_0. strictify (λ y. ((⌜x⌝) < (⌜y⌝)))))

OclGe_def: OclGe ≡ lift2 (strictify (λ x::Integer_0. strictify (λ y. (¬((⌜x⌝) <= (⌜y⌝))))))

OclGreater_def: OclGreater ≡ lift2 (strictify (λ x::Integer_0. strictify (λ y. (¬((⌜x⌝) < (⌜y⌝))))))

ocl_setup_op[OclLe, OclLess, OclGe, OclGreater]

lemma OclGe_elim [simp]: OclGe (X::'a Integer) Y = OclLe Y X
apply (rule ext)
apply (case_tac x = ⊥(X), simp_all, ocl_hypsubst [2], simp_all)
apply (case_tac x = ⊥(Y), simp_all, ocl_hypsubst [2], simp_all)
apply (simp add: OclGe_def OclLe_def
                OclIsDefined_def strictify_def OclLocalValid_def)
B.4. Library

apply (simp add: Orderings.linorder_not_less)
done

lemma OclGreater_elim[simp]: OclGreater (X::'a Integer) Y = OclLess Y X
apply (rule ext)
apply (case_tac x ⊨ ∂(X), simp_all, ocl_hypsubst [2], simp_all)
apply (case_tac x ⊨ ∂(Y), simp_all, ocl_hypsubst [2], simp_all)
apply (simp add: OclGreater_def OclLess_def OclIsDefined_def strictify_def OclLocalValid_def
  o_def lift0_def lift1_def lift2_def OclTrue_def OclUndefined_def DEF_def)
apply (simp add: Orderings.linorder_not_le)
done

consts

OclMod :: ['a Integer, 'a Integer] ⇒ 'a Integer
  (_ -> mod'( _ ') [66.65]65)

OclDiv :: ['a Integer, 'a Integer] ⇒ 'a Integer
  (_ -> div'( _ ') [66.65]65)

OclRound :: 'a Integer ⇒ 'a Integer
Appendix B. Isabelle Theories

\[ (_ \rightarrow \text{round } ) [66] \]

\textbf{OclFloor} :: 'a Integer \Rightarrow 'a Integer
\[ (_ \rightarrow \text{floor } ) [66] \]

\textbf{OclMin} :: ['a Integer, 'a Integer] \Rightarrow 'a Integer
\[ (_ \rightarrow \text{min } ) [66,65]65 \]

\textbf{OclMax} :: ['a Integer, 'a Integer] \Rightarrow 'a Integer
\[ (_ \rightarrow \text{max } ) [66,65]65 \]

\textbf{OclAbs} :: 'a Integer \Rightarrow 'a Integer
\[ (_ \rightarrow \text{abs } ) [66] \]

\textbf{OclNegative} :: 'a Integer \Rightarrow 'a Integer
\[ (- \_ [66]) \]

defs

\textbf{OclRound_def}: SELF \rightarrow \text{round } () \equiv SELF
\textbf{OclFloor_def}: SELF \rightarrow \text{floor } () \equiv SELF

defs

\textbf{OclMod_def}: OclMod \equiv lift2 (\text{strictify } (\lambda x::\text{Integer}_0. \text{strictify } (\lambda y. \text{if } \downarrow y = 0 \text{ then down else } \downarrow (\downarrow x ) \mod (\downarrow y ) ) ))
\textbf{OclDiv_def}: OclDiv \equiv lift2 (\text{strictify } (\lambda x::\text{Integer}_0. \text{strictify } (\lambda y. \text{if } \downarrow y = 0 \text{ then down else } \downarrow (\downarrow x ) \div (\downarrow y ) ) ))
\textbf{OclMin_def}: SELF \rightarrow \text{min } (I) \equiv \text{if } (\text{SELF } \leq I) \text{ then SELF else I endif}
\textbf{OclMax_def}: SELF \rightarrow \text{max } (I) \equiv \text{if } (\text{SELF } \geq I) \text{ then SELF else I endif}
\textbf{OclAbs_def}: OclAbs \equiv lift1 (\text{strictify } (\lambda x::\text{Integer}_0. \downarrow \text{abs } (\downarrow x ) ) )
\textbf{OclNegative_def}: OclNegative \equiv lift1 (\text{strictify } (\lambda x::\text{Integer}_0. \downarrow (- \downarrow x ) ) )

\textbf{ocl_setup_op } [\text{OclMod, OclDiv, OclAbs, OclNegative}]

\textbf{Computational Rules}

Foundational rule over Integer values in \textbf{OCL
lemma Integer_values_defined[simp];
\[ \partial\ (\text{number_of :: bin} \Rightarrow 'a \text{ Integer}) \ a) = T \]
apply (rule ext)
by (simp add: number_of_def
      OclIsDefined_def strictify_def
      o_def lift0_def lift1_def lift2_def
      OclTrue_def OclUndefined_def DEF_def)

These two elementary cases are required by the standard:

lemma div_zero: \( x \div \text{div}(0 \ ) = \bot \)
apply (rule ext)
apply (simp add: OclDiv_def Zero_ocl_int_def
      OclIsDefined_def strictify_def
      o_def lift0_def lift1_def lift2_def
      OclTrue_def OclUndefined_def DEF_def)
done

lemma mod_zero: \( x \mod \text{mod}(0 \ ) = \bot \)
apply (rule ext)
apply (simp add: OclMod_def Zero_ocl_int_def
      OclIsDefined_def strictify_def
      o_def lift0_def lift1_def lift2_def
      OclTrue_def OclFalse_def OclUndefined_def DEF_def)
done

lemma plus_compute [simp];
\[ ((\text{number_of :: bin} \Rightarrow 'a \text{ Integer}) \ a) + ((\text{number_of :: bin} \Rightarrow 'a \text{ Integer}) \ b) = \text{number_of (bin_add a b)} \]
apply (rule ext)
apply (simp add: number_of_def plus_def
      OclIsDefined_def strictify_def
      o_def lift0_def lift1_def lift2_def
      OclTrue_def OclFalse_def OclUndefined_def DEF_def)
done

lemma 3 + 4 = (7::'a Integer) by simp

lemma times_compute [simp];
\[ ((\text{number_of :: bin} \Rightarrow 'a \text{ Integer}) \ a) \ast ((\text{number_of :: bin} \Rightarrow 'a \text{ Integer}) \ b) = \text{number_of (bin_mult a b)} \]
apply (rule ext)
apply (simp add: number_of_def times_def
      OclIsDefined_def strictify_def
      o_def lift0_def lift1_def lift2_def
      OclTrue_def OclFalse_def OclUndefined_def DEF_def)
done
Appendix B. Isabelle Theories

lemma minus_compute [simp]:
  \[(\text{number_of}: \text{bin} \Rightarrow \text{a Integer}) \ a - ((\text{number_of}: \text{bin} \Rightarrow \text{a Integer}) \ b) =
  (\text{number_of} ((\text{bin_add} \ a \ (\text{bin_minus} \ b))))\]
apply (rule ext)
apply (simp add: number_of_def minus_def
  OclIsDefined_def strictify_def
  o_def lift0_def lift1_def lift2_def
  OclTrue_def OclFalse_def OclUndefined_def DEF_def)
done

lemma strong_eq_compute [simp]:
  \[\neg \text{iszero}((\text{number_of}: \text{bin} \Rightarrow \text{int})(\text{bin_add} \ a \ (\text{bin_minus} \ b))) \Rightarrow
  (((\text{number_of}: \text{bin} \Rightarrow \text{a Integer}) \ a) \neq ((\text{number_of}: \text{bin} \Rightarrow \text{a Integer}) \ b)) = \text{F}\]
apply (rule ext)
apply (simp add: number_of_def OclStrongEq_def
  OclIsDefined_def strictify_def
  o_def lift0_def lift1_def lift2_def
  OclTrue_def OclFalse_def OclUndefined_def DEF_def)
done

lemma strict_eq_compute [simp]:
  \[\neg \text{iszero}((\text{number_of}: \text{bin} \Rightarrow \text{int})(\text{bin_add} \ a \ (\text{bin_minus} \ b))) \Rightarrow
  (((\text{number_of}: \text{bin} \Rightarrow \text{a Integer}) \ a) = ((\text{number_of}: \text{bin} \Rightarrow \text{a Integer}) \ b)) = \text{F}\]
apply (rule ext)
apply (simp add: number_of_def OclStrictEq_def
  OclIsDefined_def strictify_def
  o_def lift0_def lift1_def lift2_def
  OclTrue_def OclFalse_def OclUndefined_def DEF_def)
done

lemma \[\tau \models 3 \triangleq C ; \tau \models C + 2 \triangleq (7: \text{a Integer})\] \Rightarrow \tau \models A \land B
apply ocl_hypsubst
apply simp
done

end

B.4.7. OCL Real

theory OCL_Real

236
imports
$HOLOCL_HOME/src/library/basic/OC\textunderscore Numerals$

begin constdefs
  is\_Real\_0 :: 'a U ⇒ bool
  is\_Real\_0 ≡ sum\_case (λx. False) (sum\_case (λx. True) (λx. False))

  get\_Real\_0 :: 'a U ⇒ Real\_0
  get\_Real\_0 ≡ sum\_case (λx. ϵ x x True) (λx. ϵ x x True)

  mk\_Real\_0 :: Real\_0 ⇒ 'a U
  mk\_Real\_0 ≡ Inr o Inl

lemma get\_mk\_Real\_id\_0 : get\_Real\_0 (mk\_Real\_0 x) = x
  apply simp add: get\_Real\_0_def mk\_Real\_0_def
  done

lemma is\_mk\_Real\_0 : is\_Real\_0 (mk\_Real\_0 x) = True
  apply simp add: is\_Real\_0_def mk\_Real\_0_def
  done

lemma mk\_get\_Real\_id\_0 : is\_Real\_0 x =⇒ mk\_Real\_0 (get\_Real\_0 x) = x
  apply simp add: mk\_Real\_0_def is\_Real\_0_def
  apply case_tac x, simp, simp
  done

constdefs
  Real\_0 :: ('st, Real\_0 Set\_0) VAL
  Real\_0 ≡ lift0 (Abs\_Set\_0 ⌞ lift ' UNIV ⌘)

defs
  OclZero\_def : 0 ≡ lift0 (λ:real ⌞ 0 ⌘ UNIV)

  OclOne\_def : 1 ≡ lift0 (λ:real ⌞ 1 ⌘)

defs
  plus\_def : op + ≡ lift2 (strictify (λ x::Real\_0. strictify (λ y.
    (⌜x⌝ + (⌜y⌝))))

  minus\_def : op − ≡ lift2 (strictify (λ x::Real\_0. strictify (λ y.
    (⌜x⌝ − (⌜y⌝))))

  times\_def : op * ≡ lift2 (strictify (λ x::Real\_0. strictify (λ y.
    (⌜x⌝ ∗ (⌜y⌝))))

ocl\_setup\_op [plus, minus, times]

consts
  OclRound :: 'a Real ⇒ 'a Integer (⌜_⌞ round' ⌘) [66]
  OclFloor :: 'a Real ⇒ 'a Integer (⌜_⌞ floor' ⌘) [66]

  OclMin :: ('a Real, 'a Real) ⇒ 'a Real (⌜_⌞ min' ⌘) [66,65] [65]
  OclMax :: ('a Real, 'a Real) ⇒ 'a Real (⌜_⌞ max' ⌘) [66,65] [65]
Appendix B. Isabelle Theories

\textbf{OclDivide} :: [\textit{a Real}, \textit{a Real}] => \textit{a Real}
\hspace{1cm} (\_ \rightarrow divide(\_ \_)[66,65]65)

\textbf{OclAbs} :: \textit{a Real} => \textit{a Real}
\hspace{1cm} (\_ \rightarrow abs(\_)[60])

\textbf{OclNegative} :: \textit{a Real} => \textit{a Real}
\hspace{1cm} (\_ \rightarrow [60])

\textbf{defs}
\textbf{OclDivide def}:
\hspace{1cm} OclDivide \equiv lift\textsubscript{2}(\text{strictify}(\lambda x::\text{Real}_0. \text{strictify}(\lambda y::\text{Real}_0. (\_ / \_))))

\textbf{defs}
\textbf{OclLe def}:
\hspace{1cm} OclLe \equiv lift\textsubscript{2}(\text{strictify}(\lambda x::\text{Real}_0. \text{strictify}(\lambda y. (\_ \_))))

\textbf{OclLess def}:
\hspace{1cm} OclLess \equiv lift\textsubscript{2}(\text{strictify}(\lambda x::\text{Real}_0. \text{strictify}(\lambda y. (\_<\_))))

\textbf{OclGe def}:
\hspace{1cm} OclGe \equiv lift\textsubscript{2}(\text{strictify}(\lambda x::\text{Real}_0. \text{strictify}(\lambda y. (\_ \_<\_))))

\textbf{OclGreater def}:
\hspace{1cm} OclGreater \equiv lift\textsubscript{2}(\text{strictify}(\lambda x::\text{Real}_0. \text{strictify}(\lambda y. (\_ \_<\_))))

\textbf{OclMin def}:
\hspace{1cm} SELF \rightarrow\rightarrow\text{min}(I) \equiv if (SELF \_<=\_ I) then SELF else I endif

\textbf{OclMax def}:
\hspace{1cm} SELF \rightarrow\rightarrow\text{max}(I) \equiv if (SELF \_>=\_ I) then SELF else I endif

\textbf{OclAbs def}:
\hspace{1cm} OclAbs \equiv lift\textsubscript{1}(\text{strictify}(\lambda x::\text{Real}_0. (abs(\_))))

\textbf{OclNegative def}:
\hspace{1cm} OclNegative \equiv lift\textsubscript{1}(\text{strictify}(\lambda x::\text{Real}_0. (\_ )))

\textbf{ocl_setup_op} [OclMax, OclMin, OclNegative]
\textbf{ocl_setup_op} [OclLe, OclLess, OclGe, OclGreater]

end

\textbf{B.4.8. OCL String}

\textbf{theory OCL\_String}

238
begin constdefs

is_String_0 :: 'a U ⇒ bool
is_String_0 ≡ sum_case (λx. False)
(sum_case (λx. False)
(sum_case (λx. False)
(sum_case (λx. False)(λx. True)))))

get_String_0 :: 'a U ⇒ String_0
get_String_0 ≡ sum_case (λx. ϵ x. True)
(sum_case (λx. ϵ x. True)
(sum_case (λx. ϵ x. True)
(sum_case (λx. ϵ x. True)(λx. x))))

mk_String_0 :: String_0 ⇒ 'a U
mk_String_0 ≡ Inr ◦ Inr ◦ Inr o Inr

lemma get_mk_String_id_0: get_String_0 (mk_String_0 x) = x
apply (simp add: get_String_0_def mk_String_0_def)
done

lemma is_mk_String_0: is_String_0 (mk_String_0 x) = True
apply (simp add: is_String_0_def mk_String_0_def)
done

lemma mk_get_String_id_0: is_String_0 x =⇒ mk_String_0 (get_String_0 x) = x
apply (simp add: get_String_0_def mk_String_0_def is_String_0_def)
apply (case_tac x, simp, simp)
apply (case_tac ba, simp, simp)
apply (case_tac bb, simp, simp)
done

constdefs

String_0 :: (′st, String_0 Set_0) VAL
String_0 ≡ lift0(Abs_Set_0(⌜UNIV⌟))

consts

OclConcat :: ['a String, 'a String] ⇒ 'a String
OclToLower :: 'a String ⇒ 'a String
OclToUpper :: 'a String ⇒ 'a String
stringsize :: 'a String ⇒ 'a Integer
OclSubstring :: ['a String, 'a Integer, 'a Integer] ⇒ 'a String

defs

OclConcat_def: OclConcat ≡ lift2(strictify(λ x::String_0. strictify(λ y. _ _ _)))
stringsize_def: stringsize ≡ lift1(strictify(λ x::String_0. int(size (⌜x⌟))))
OclSubstring_def:OclSubstring ≡ lift3(strictify(λ x::String_0.
Appendix B. Isabelle Theories

\begin{verbatim}
strictify(\lambda l:\text{Integer}_0. \\
\lambda u:\text{Integer}_0. \\
\downarrow \text{(List.take} \text{nat}((\lceil u \rceil - \lceil T + 1::\text{int} \rceil)) \\
\text{List.drop} \text{nat}((\lceil T - 1::\text{int} \rceil) \lceil s \rceil) \downarrow))
\end{verbatim}

end

B.4.9. **OCL** Collection

\textbf{theory} \textit{OCL Collection} \\
\textbf{imports} $\text{HOLOCL_HOME/} \text{src/library/basic/OCL_Integer}$ \\
\begin{verbatim}
begin \\
\text{The purpose of this theory is to provide the syntactic framework for the abstract} \\
\text{class \textit{Collection} in the sense of the standard. It is defined by the Isabelle type class} \\
\text{“collection”. We require that collections must always have a bottom element.} \\
\text{Unfortunately, this implementation by the type class “collection” is an approxima-} \\
\text{tion (a type constructor class would be more appropriate, but is not available in the} \\
\text{Isabelle type system). Consequently, in lemmas the concrete type instances for oper-} \\
\text{ators resulting from the abstract class must be given; the types inferred by Isabelle} \\
\text{automatically are too coarse and can lead to dead ends in proofs (definitions can not} \\
\text{be unfolded).}

\textbf{The Syntax of Abstract Operations}

\text{The core operation} \textit{size} (which may be undefined if and only if the collection is infinitely} \\
\text{large), \text{select, collect, includes and any.}

\textbf{Operations on all Collection Types}

\textbf{consts} \\
\textit{OclSize} :: \text{\langle \tau,\alpha::\text{collection} \rangle VAL} \Rightarrow \tau \text{ Integer} \\
\textit{OclCount} :: \text{\langle \tau,\beta::\text{collection} \rangle VAL,\langle \tau,\alpha::\text{bot} \rangle VAL} \Rightarrow \tau \text{ Integer} \\
\textit{OclIncludes} :: \text{\langle \tau,\beta::\text{collection} \rangle VAL,\langle \tau,\alpha::\text{bot} \rangle VAL} \Rightarrow \tau \text{ Boolean} \\
\textit{OclExcludes} :: \text{\langle \tau,\beta::\text{collection} \rangle VAL,\langle \tau,\alpha \rangle VAL} \Rightarrow \tau \text{ Boolean} \\
\textit{OclIncluding} :: \text{\langle \tau,\beta::\text{collection} \rangle VAL,\langle \tau,\alpha \rangle VAL} \Rightarrow \langle \tau,\beta \rangle VAL \\
\textit{OclExcluding} :: \text{\langle \tau,\beta::\text{collection} \rangle VAL,\langle \tau,\alpha \rangle VAL} \Rightarrow \langle \tau,\beta \rangle VAL \\
\textit{OclFlatten} :: \text{\langle \tau,\alpha::\text{collection} \rangle VAL} \Rightarrow \langle \tau,\beta::\text{bot} \rangle VAL \\
\textit{OclSum} :: \text{\langle \tau,\alpha::\text{collection} \rangle VAL} \Rightarrow \tau \text{ Integer} \\
\textit{OclAsSet} :: \text{\langle \tau,\alpha::\text{collection} \rangle VAL} \Rightarrow \langle \tau,\beta::\text{collection} \rangle VAL \\
\textit{OclAsSequence} :: \text{\langle \tau,\alpha::\text{collection} \rangle VAL} \Rightarrow \langle \tau,\beta::\text{collection} \rangle VAL
\end{verbatim}
B.4. Library

\[\text{OclAsBag} :: (\tau, \alpha::\text{collection}) \text{VAL} \Rightarrow (\tau, \beta::\text{collection}) \text{VAL}\]
\[\text{OclAsOrderedSet} :: (\tau, \alpha::\text{collection}) \text{VAL} \Rightarrow (\tau, \beta::\text{collection}) \text{VAL}\]
\[\text{OclIncludesAll} :: [(\tau, \alpha::\text{collection}) \text{VAL}, (\tau, \alpha) \text{VAL}] \Rightarrow \tau \text{ Boolean}\]
\[\text{OclExcludesAll} :: [(\tau, \alpha::\text{collection}) \text{VAL}, (\tau, \alpha) \text{VAL}] \Rightarrow \tau \text{ Boolean}\]
\[\text{OclIsEmpty} :: (\tau, \alpha::\text{collection}) \text{VAL} \Rightarrow \tau \text{ Boolean}\]
\[\text{OclNotEmpty} :: (\tau, \alpha::\text{collection}) \text{VAL} \Rightarrow \tau \text{ Boolean}\]
\[\text{OclComplement} :: (\tau, \beta::\text{collection}) \text{VAL} \Rightarrow (\tau, \beta') \text{VAL}\]
\[\text{OclUnion} :: [(\tau, \beta::\text{collection}) \text{VAL}, (\tau, \beta) \text{VAL}] \Rightarrow (\tau, \beta) \text{VAL}\]
\[\text{OclCollectionRange} :: [(\tau, \alpha) \text{VAL}, (\tau, \alpha) \text{VAL}] \Rightarrow (\tau, \beta) \text{VAL}\]

**syntax**

\[\text{OclSize\_std} :: (\tau, \alpha::\text{collection}) \text{VAL} \Rightarrow \tau \text{ Integer}\]
\[\text{OclCount\_std} :: [(\tau, \beta::\text{collection}) \text{VAL}, (\tau, \alpha::\text{bot}) \text{VAL}] \Rightarrow \tau \text{ Integer}\]
\[\text{OclIncludes\_std} :: [(\tau, \beta::\text{collection}) \text{VAL}, (\tau, \alpha) \text{VAL}] \Rightarrow \tau \text{ Boolean}\]
\[\text{OclExcludes\_std} :: [(\tau, \beta::\text{collection}) \text{VAL}, (\tau, \alpha::\text{bot}) \text{VAL}] \Rightarrow \tau \text{ Boolean}\]
\[\text{OclFlatten\_std} :: (\tau, \alpha::\text{collection}) \text{VAL} \Rightarrow (\tau, \beta::\text{collection}) \text{VAL}\]
\[\text{OclSum\_std} :: (\tau, \alpha::\text{collection}) \text{VAL} \Rightarrow (\tau, \beta::\text{collection}) \text{VAL}\]
\[\text{OclAsSet\_std} :: (\tau, \alpha::\text{collection}) \text{VAL} \Rightarrow (\tau, \beta::\text{collection}) \text{VAL}\]
\[\text{OclAsSequence\_std} :: (\tau, \alpha::\text{collection}) \text{VAL} \Rightarrow (\tau, \beta::\text{collection}) \text{VAL}\]
\[\text{OclAsBag\_std} :: (\tau, \alpha::\text{collection}) \text{VAL} \Rightarrow (\tau, \beta::\text{collection}) \text{VAL}\]
\[\text{OclAsOrderedSet\_std} :: (\tau, \alpha::\text{collection}) \text{VAL} \Rightarrow (\tau, \beta::\text{collection}) \text{VAL}\]
\[\text{OclIncludesAll\_std} :: [(\tau, \alpha::\text{collection}) \text{VAL}, (\tau, \alpha::\text{collection}) \text{VAL}] \Rightarrow \tau \text{ Boolean}\]
\[\text{OclExcludesAll\_std} :: [(\tau, \alpha::\text{collection}) \text{VAL}, (\tau, \alpha::\text{collection}) \text{VAL}] \Rightarrow \tau \text{ Boolean}\]
\[\text{OclIsEmpty\_std} :: (\tau, \alpha::\text{collection}) \text{VAL} \Rightarrow \tau \text{ Boolean}\]
Appendix B. Isabelle Theories

\begin{itemize}
\item \texttt{OclNotEmpty\_std} \rightarrow (\tau, \alpha::\texttt{collection}) \rightarrow (\texttt{Boolean}) [66]
\item \texttt{OclIncluding\_std} \rightarrow (\tau, \alpha::\texttt{bot}) \rightarrow (\tau, \beta::\texttt{collection}) [66]
\item \texttt{OclIncluding\_std} \rightarrow (\tau, \alpha::\texttt{bot}) \rightarrow (\tau, \beta::\texttt{collection}) [66]
\item \texttt{OclExcluding\_std} \rightarrow (\tau, \alpha::\texttt{bot}) \rightarrow (\tau, \beta::\texttt{collection}) [66]
\item \texttt{OclComplement\_std} \rightarrow (\tau, \beta::\texttt{collection}) \rightarrow (\tau, \beta::\texttt{collection}) [66]
\item \texttt{OclAsSet\_ascii} \rightarrow (\tau, \alpha::\texttt{collection}) \rightarrow (\tau, \beta::\texttt{collection}) [66]
\item \texttt{OclAsSequence\_ascii} \rightarrow (\tau, \alpha::\texttt{collection}) \rightarrow (\tau, \beta::\texttt{collection}) [66]
\item \texttt{OclAsBag\_ascii} \rightarrow (\tau, \alpha::\texttt{collection}) \rightarrow (\tau, \beta::\texttt{collection}) [66]
\item \texttt{OclAsOrderedSet\_ascii} \rightarrow (\tau, \alpha::\texttt{collection}) \rightarrow (\tau, \beta::\texttt{collection}) [66]
\item \texttt{OclIncludes\_std} \rightarrow (\tau, \alpha::\texttt{collection}) \rightarrow (\tau, \alpha::\texttt{collection}) [66]
\item \texttt{OclSize\_ascii} \rightarrow (\tau, \alpha::\texttt{collection}) \rightarrow (\tau, \alpha::\texttt{collection}) [66]
\item \texttt{OclCount\_ascii} \rightarrow (\tau, \alpha::\texttt{collection}) \rightarrow (\tau, \alpha::\texttt{collection}) [66]
\item \texttt{OclExcludes\_ascii} \rightarrow (\tau, \alpha::\texttt{collection}) \rightarrow (\tau, \alpha::\texttt{collection}) [66]
\item \texttt{OclIncludes\_ascii} \rightarrow (\tau, \alpha::\texttt{collection}) \rightarrow (\tau, \alpha::\texttt{collection}) [66]
\item \texttt{OclAsOrderedSet\_ascii} \rightarrow (\tau, \alpha::\texttt{collection}) \rightarrow (\tau, \alpha::\texttt{collection}) [66]
\end{itemize}

242
B.4. Library

_ OclExcludesAll_ascii :: \(\tau, \alpha::\text{collection} \) \(\text{VAL, } \tau, \alpha::\text{collection} \) \(\text{VAL} \Rightarrow \tau \ \text{Boolean} \)
\(_ \rightarrow \text{excludesAll}'(\_') \) \([66,65]65\)

_ OclIsEmpty_ascii :: \(\tau, \alpha::\text{collection} \) \(\text{VAL} \Rightarrow \tau \ \text{Boolean} \)
\(_ \rightarrow \text{isEmpty}'(\_') \) \([66]\)

_ OclNotEmpty_ascii :: \(\tau, \alpha::\text{collection} \) \(\text{VAL} \Rightarrow \tau \ \text{Boolean} \)
\(_ \rightarrow \text{notEmpty}'(\_') \) \([66]\)

_ OclIncluding_ascii :: \(\tau, \beta::\text{collection} \) \(\text{VAL, } \tau, \alpha::\text{bot} \) \(\text{VAL} \Rightarrow (\tau, \beta) \text{ VAL} \)
\(_ \rightarrow \text{including}'(\_') \)

_ OclExcluding_ascii :: \(\tau, \beta::\text{collection} \) \(\text{VAL} \Rightarrow (\tau, \beta) \text{ VAL} \)
\(_ \rightarrow \text{excluding}'(\_') \)

_ OclComplement_ascii :: \(\tau, \beta::\text{collection} \) \(\text{VAL} \Rightarrow (\tau, \beta) \text{ VAL} \)
\(_ \rightarrow \text{complement}'(\_') \)

_ OclUnion_ascii :: \(\tau, \beta::\text{collection} \) \(\text{VAL, } (\tau, \beta)\text{ VAL} \Rightarrow (\tau, \beta) \text{ VAL} \)
\(_ \rightarrow \text{union}'(\_') \) \([66,65]65\)

_ OclIntersection_ascii :: \(\tau, \beta::\text{collection} \) \(\text{VAL, } (\tau, \beta)\text{ VAL} \Rightarrow (\tau, \beta) \text{ VAL} \)
\(_ \rightarrow \text{intersection}'(\_') \) \([71,70]70\)

syntax (zsymbols)

_ OclSize_math :: \(\tau, \alpha::\text{collection} \) \(\text{VAL} \Rightarrow \tau \ \text{Integer} \)
\(_ \left\| \_ \right\| \) \([66]\)

_ OclCount_math :: \(\tau, \beta::\text{collection} \) \(\text{VAL, } \tau, \alpha::\text{bot} \) \(\text{VAL} \Rightarrow \tau \ \text{Integer} \)
\(_ \rightarrow \text{count} \_ \) \([66,65]65\)

_ OclIncludes_math :: \(\tau, \alpha::\text{collection} \) \(\text{VAL} \Rightarrow \tau \ \text{Boolean} \)
\(_ \in \_ \) \([66,65]65\)

_ OclExcludes_math :: \(\tau, \alpha::\text{bot} \) \(\text{VAL} \Rightarrow (\tau, \beta::\text{collection} \) \(\text{VAL} \Rightarrow \tau \ \text{Boolean} \)
\(_ \notin \_ \) \([66,65]65\)

_ OclFlatten_math :: \(\tau, \alpha::\text{collection} \) \(\text{VAL} \Rightarrow (\tau, \beta::\text{collection} \) \(\text{VAL} \Rightarrow \tau \ \text{Integer} \)
\(_ \left\| \_ \right\| \) \([66]\)

_ OclSum_math :: \(\tau, \alpha::\text{collection} \) \(\text{VAL} \Rightarrow \tau \ \text{Integer} \)
\(_ \rightarrow \text{sum}() \_ \) \([66]\)

_ OclAsSet_math :: \(\tau, \alpha::\text{collection} \) \(\text{VAL} \Rightarrow (\tau, \beta::\text{collection} \) \(\text{VAL} \Rightarrow \tau \ \text{Integer} \)
\(_ \rightarrow \text{asSet}() \_ \) \([66]\)

_ OclAsSequence_math :: \(\tau, \alpha::\text{collection} \) \(\text{VAL} \Rightarrow (\tau, \beta::\text{collection} \) \(\text{VAL} \Rightarrow \tau \ \text{Integer} \)

Appendix B. Isabelle Theories

\ ((_OclAsBag_math \ (\tau, \alpha::collection) \ VAL \Rightarrow \ (\tau, \beta::collection) \ VAL \))
\ ((_OclAsOrderedSet_math \ (\tau, \alpha::collection) \ VAL \Rightarrow \ (\tau, \beta::collection) \ VAL \))
\ ((_OclIncluding_math \ (\tau, \alpha::collection) \ VAL \Rightarrow \ (\tau, \beta::collection) \ VAL \))
\ |_OclNotEmpty_math |_OclAsBag_math
\ |_OclIncludesAll_math _OclAsOrderedSet_math
\ |_OclComplement_math _OclExcluding_math
\ |_OclIsEmpty_math _OclAsBag_math
\ |_OclAppend_std (\tau, \alpha::collection) \ VAL \Rightarrow \ (\tau, \beta::collection) \ VAL
\ |_OclPrepend_std (\tau, \alpha::collection) \ VAL \Rightarrow \ (\tau, \beta::collection) \ VAL

Operations on Collection Types with Ordering

consts
\ \text{OclAppend} :: (\tau, \alpha::collection) \ VAL \Rightarrow (\tau, \beta::collection) \ VAL
\ \text{OclPrepend} :: (\tau, \alpha::collection) \ VAL \Rightarrow (\tau, \beta::collection) \ VAL
\ \text{OclInsertAt} :: (\tau, \alpha::collection) \ VAL \Rightarrow (\tau, \beta::collection) \ VAL
\ \text{OclAt} :: (\tau, \alpha::collection) \ VAL \Rightarrow (\tau, \beta::collection) \ VAL
\ \text{OclIndexOf} :: (\tau, \alpha::collection) \ VAL \Rightarrow (\tau, \beta::collection) \ VAL
\ \text{OclFirst} :: (\tau, \alpha::collection) \ VAL \Rightarrow (\tau, \beta::collection) \ VAL
\ \text{OclLast} :: (\tau, \alpha::collection) \ VAL \Rightarrow (\tau, \beta::collection) \ VAL

syntax
\ \text{OclPrepend_std} :: (\tau, \alpha::collection) \ VAL \Rightarrow (\tau, \beta::collection) \ VAL
\ \text{OclAppend_std} :: (\tau, \alpha::collection) \ VAL \Rightarrow (\tau, \beta::collection) \ VAL
B.4. Library

(_ ->append '(_ ') [66,65,65]

_OclInsertAt_std :: [(τ, α::bot)Sequence, τ Integer, (τ, α) VAL] => (τ, α) VAL
(_ ->insertAt '(_ ') [66,65,65])

_OclAt_std :: [(τ, α::collection) VAL, τ Integer] => (τ, β) VAL
(_ ->at '(_ ') [66,65])

_OclIndexOf_std :: [(τ, α::collection) VAL, (τ, β) VAL] => τ Integer
(_ ->indexOf '(_ ') [66,65])

_OclFirst_std :: (τ, α::collection) VAL => (τ, β) VAL
(_ ->first() [66])

_OclLast_std :: (τ, α::collection) VAL => (τ, β) VAL
(_ ->last() [66])

syntax

_OclPrepend_ascii :: [(τ, (α::collection)) VAL, (τ, β::bot) VAL] => (τ, α) VAL
(_ ->prepend '(_ ') [66,65,65])

_OclAppend_ascii :: [(τ, (α::collection)) VAL, (τ, β::bot) VAL] => (τ, α) VAL
(_ ->append '(_ ') [66,65,65])

_OclInsertAt_ascii :: [(τ, (α::bot)Sequence, τ Integer, (τ, α) VAL] => (τ, α) VAL
(_ ->insertAt '(_ ') [66,65,65])

_OclAt_ascii :: [(τ, α::collection) VAL, τ Integer] => (τ, β) VAL
(_ ->at '(_ ') [66,65])

_OclIndexOf_ascii :: [(τ, α::collection) VAL, (τ, β) VAL] => τ Integer
(_ ->indexOf '(_ ') [66,65])

_OclFirst_ascii :: (τ, α::collection) VAL => (τ, β) VAL
(_ ->first() [66])

_OclLast_ascii :: (τ, α::collection) VAL => (τ, β) VAL
(_ ->last() [66])

syntax (xsymbols)

_OclPrepend_math :: [(τ, (α::collection)) VAL, (τ, β::bot) VAL] => (τ, α) VAL
(_ ->prepend '(_ ') [66,65,65])

_OclAppend_math :: [(τ, (α::collection)) VAL, (τ, β::bot) VAL] => (τ, α) VAL
(_ ->append '(_ ') [66,65,65])

_OclInsertAt_math :: [(τ, (α::bot)Sequence, τ Integer, (τ, α) VAL] => (τ, α) VAL
(_ ->insertAt '(_ ') [66,65,65])

_OclAt_math :: [(τ, α::collection) VAL, τ Integer] => (τ, β) VAL
(_ ->at '(_ ') [66,65])

_OclIndexOf_math :: [(τ, α::collection) VAL, (τ, β) VAL] => τ Integer
(_ ->indexOf '(_ ') [66,65])

_OclFirst_math :: (τ, α::collection) VAL => (τ, β) VAL
(_ $1 [66])

_OclLast_math :: (τ, α::collection) VAL => (τ, β) VAL
(_ $8 [66])

Operations on Collection Types without Ordering
consts

OclIntersection:: [(τ, β::collection) VAL, (τ, β) VAL] => (τ, β) VAL
Appendix B. Isabelle Theories

syntax

\_OclIntersection\_std:: [(\'=\tau, \'=\beta::collection) VAL, (\'=\tau, \'=\beta) VAL] \Rightarrow (\'=\tau, \'=\beta) VAL

(\_ \rightarrow intersection(\_ \_)) [71, 70] 70

syntax

\_OclIntersection\_ascii:: [(\'=\tau, \'=\beta::collection) VAL, (\'=\tau, \'=\beta) VAL] \Rightarrow (\'=\tau, \'=\beta) VAL

(\_ \rightarrow intersection(\_ \_)) [71, 70] 70

syntax (xsymbols)

\_OclIntersection\_math:: [(\'=\tau, \'=\beta::collection) VAL, (\'=\tau, \'=\beta) VAL] \Rightarrow (\'=\tau, \'=\beta) VAL

(\_ \cap \_ ) [71, 70] 70

The Syntax of Iterators

This section contains the operators of OCL involving binding, which as subsumed under the category “iterators” in the standard. Since we use a shallow embedding, we heavily use higher-order abstract syntax (HOAS) here.

However, quantifiers were not defined on the basis of iterate in HOL-OCL. This is since iterate is undefined for all infinite collections, in contrast to quantifiers, which do not necessarily have computational content.

consts

OclForAll : [(\'=\tau, \'=\beta::collection) VAL, (\'=\tau, \'=\alpha::bot) VAL \Rightarrow \'=\tau Boolean] \Rightarrow \'=\tau Boolean

OclSelect : [(\'=\tau, \'=\beta::collection) VAL, (\'=\tau, \'=\alpha::bot) VAL \Rightarrow \'=\tau Boolean]

\Rightarrow (\'=\tau, \'=\beta::collection) VAL

OclReject : [(\'=\tau, \'=\beta::collection) VAL, (\'=\tau, \'=\alpha::bot) VAL \Rightarrow \'=\tau Boolean]

\Rightarrow (\'=\tau, \'=\beta::collection) VAL

OclCollect : [(\'=\tau, \'=\gamma::collection) VAL,

(\'=\tau, \'=\alpha::bot) VAL \Rightarrow (\'=\tau, \'=\beta::bot) VAL]

\Rightarrow (\'=\tau, \'=\beta::collection) VAL

OclCollectNested : [(\'=\tau, \'=\gamma::collection) VAL,

(\'=\tau, \'=\alpha::bot) VAL \Rightarrow (\'=\tau, \'=\beta::bot) VAL]

\Rightarrow (\'=\tau, \'=\delta::collection) VAL

OclIterate : [(\'=\tau, \'=\gamma::collection) VAL,

[(\'=\tau, \'=\alpha::bot) VAL, (\'=\tau, \'=\beta::bot) VAL] \Rightarrow (\'=\tau, \'=\beta::bot) VAL,

(\'=\tau, \'=\beta::bot) VAL]

\Rightarrow (\'=\tau, \'=\beta::bot) VAL

246
B.4. Library

\begin{verbatim}
OclIsUnique ::= (\tau::\beta::\text{collection}) VAL, (\tau::\alpha::\text{bot}) VAL \rightarrow (\tau::\gamma::\text{bot}) VAL \rightarrow '\tau Boolean

OclOne ::= (\tau::\beta::\text{collection}) VAL, (\tau::\alpha::\text{bot}) VAL \rightarrow '\tau Boolean

OclAny ::= (\tau::\beta::\text{collection}) VAL, (\tau::\alpha::\text{bot}) VAL \rightarrow '\tau Boolean

\text{constdefs}
OclExists ::= [(\tau::\beta::\text{collection}) VAL, (\tau::\alpha::\text{bot}) VAL \rightarrow '\tau Boolean] \rightarrow '\tau Boolean

OclExists S P \equiv \neg\text{OclForAll} (\lambda x. \neg (P x))

\text{syntax}
_\text{OclForAll} = (\tau::\beta::\text{collection}) VAL \Rightarrow idt \Rightarrow '\tau Boolean
(_ \Rightarrow \text{forall} (\_ \_ \_)) [71,100,70,50]

_\text{OclExists} = (\tau::\beta::\text{collection}) VAL \Rightarrow idt \Rightarrow '\tau Boolean
(_ \Rightarrow \text{exists} (\_ \_ \_)) [71,100,70,50]

_\text{OclSelect} ::= (\tau::\beta::\text{collection}) VAL, (\tau::\alpha::\text{bot}) VAL \Rightarrow (\tau::\beta::\text{collection}) VAL
(_ \Rightarrow \text{select} (\_ \_ \_)) [71,100,70,50]

_\text{OclReject} ::= (\tau::\beta::\text{collection}) VAL, (\tau::\alpha::\text{bot}) VAL \Rightarrow (\tau::\beta::\text{collection}) VAL
(_ \Rightarrow \text{reject} (\_ \_ \_)) [71,100,70,50]

_\text{OclCollect} ::= (\tau::\beta::\text{collection}) VAL, (\tau::\alpha::\text{bot}) VAL \Rightarrow (\tau::\beta::\text{collection}) VAL
(_ \Rightarrow \text{collect} (\_ \_ \_)) [71,100,70,50]

_\text{OclCollectNested} ::= (\tau::\gamma::\text{collection}) VAL, (\tau::\alpha::\text{bot}) VAL \Rightarrow (\tau::\beta::\text{collection}) VAL
(_ \Rightarrow \text{collectNested} (\_ \_ \_)) [71,100,70,50]

_\text{OclIterate} ::= (\tau::\beta::\text{collection}) VAL, idt, idt, '\gamma, '\delta
\Rightarrow (\tau::\delta::\text{collection}) VAL
(_ \Rightarrow \text{iterate} (\_ \_ \_ \_ \_)) [71,100,70,50]

_\text{OclOne} ::= (\tau::\beta::\text{collection}) VAL, '\alpha \Rightarrow '\tau Boolean
(_ \Rightarrow \text{one} (\_ \_ \_)) [71,100,70,50]

_\text{OclIsUnique} ::= (\tau::\beta::\text{collection}) VAL, '\alpha \Rightarrow '\tau Boolean
(_ \Rightarrow \text{isUnique} (\_ \_ \_)) [71,100,70,50]

\text{syntax}
_\text{OclForAll} = (\tau::\beta::\text{collection}) VAL \Rightarrow idt \Rightarrow '\tau Boolean
\end{verbatim}

247
Appendix B. Isabelle Theories

(_ \rightarrow \text{forAll}(\_ | \_)) [71,100,70,50]

_OclExists_ascii :: \( (\tau, \beta :: \text{collection}) \text{ VAL} \Rightarrow \tau \text{ Boolean} \)

(_ \rightarrow \text{exists}(\_ | \_)) [71,100,70,50]

_OclSelect_ascii :: \( (\tau, \beta :: \text{collection}) \text{ VAL} \Rightarrow (\tau, \alpha :: \text{bot}) \text{ VAL} \)

\( \Rightarrow (\tau, \beta :: \text{collection}) \text{ VAL} \)

(_ \rightarrow \text{select}(\_ | \_)) [71,100,70,50]

_OclReject_ascii :: \( (\tau, \beta :: \text{collection}) \text{ VAL} \Rightarrow (\tau, \alpha :: \text{bot}) \text{ VAL} \)

\( \Rightarrow (\tau, \beta :: \text{collection}) \text{ VAL} \)

(_ \rightarrow \text{reject}(\_ | \_)) [71,100,70,50]

_OclCollect_ascii :: \( (\tau, \gamma :: \text{collection}) \text{ VAL} \Rightarrow (\tau, \gamma :: \text{collection}) \text{ VAL} \)

\( \Rightarrow (\tau, \delta :: \text{collection}) \text{ VAL} \)

(_ \rightarrow \text{collect}(\_ | \_)) [71,100,70,50]

_OclCollectNested_ascii :: \( (\tau, \gamma :: \text{collection}) \text{ VAL} \Rightarrow (\tau, \alpha :: \text{bot}) \text{ VAL} \)

\( \Rightarrow (\tau, \beta :: \text{collection}) \text{ VAL} \)

(_ \rightarrow \text{collectNested}(\_ | \_)) [71,100,70,50]

_OclIterate_ascii :: \( (\tau, \beta :: \text{collection}) \text{ VAL} \Rightarrow \text{idt} \Rightarrow (\tau, \gamma, \delta) \)

\( \Rightarrow (\tau, \beta :: \text{collection}) \text{ VAL} \)

(_ \rightarrow \text{iterate}(\_ | \_)) [71,100,70,50]

_OclOne_ascii :: \( (\tau, \beta :: \text{collection}) \text{ VAL} \Rightarrow \alpha \text{ VAL} \Rightarrow \tau \text{ Boolean} \)

\( \Rightarrow (\tau, \beta :: \text{collection}) \text{ VAL} \)

(_ \rightarrow \text{one}(\_ | \_)) [71,100,70,50]

_OclIsUnique_ascii :: \( (\tau, \beta :: \text{collection}) \text{ VAL} \Rightarrow \alpha \text{ VAL} \Rightarrow \tau \text{ Boolean} \)

\( \Rightarrow (\tau, \beta :: \text{collection}) \text{ VAL} \)

(_ \rightarrow \text{isUnique}(\_ | \_)) [71,100,70,50]

\textbf{syntax (xsymbols)}

_OclForAll_math :: \text{idt} \Rightarrow (\tau, \beta :: \text{collection}) \text{ VAL} \Rightarrow \tau \text{ Boolean} \)

\( (\forall \_ \in \_ | \_)) [71,100,70,50]

_OclExists_math :: \text{idt} \Rightarrow (\tau, \beta :: \text{collection}) \text{ VAL} \Rightarrow \tau \text{ Boolean} \)

\( (\exists \_ \in \_ | \_)) [71,100,70,50]

_OclSelect_math :: \( (\tau, \beta :: \text{collection}) \text{ VAL} \Rightarrow (\tau, \alpha :: \text{bot}) \text{ VAL} \Rightarrow \tau \text{ Boolean} \)

\( \Rightarrow (\tau, \beta :: \text{collection}) \text{ VAL} \)

(_ \rightarrow \text{select}(\_ | \_)) [71,100,70,50]

_OclReject_math :: \( (\tau, \beta :: \text{collection}) \text{ VAL} \Rightarrow (\tau, \alpha :: \text{bot}) \text{ VAL} \Rightarrow \tau \text{ Boolean} \)

\( \Rightarrow (\tau, \beta :: \text{collection}) \text{ VAL} \)

(_ \rightarrow \text{reject}(\_ | \_)) [71,100,70,50]

_OclCollect_math :: \( (\tau, \gamma :: \text{collection}) \text{ VAL} \Rightarrow (\tau, \alpha :: \text{bot}) \text{ VAL} \Rightarrow \tau \text{ Boolean} \)

\( \Rightarrow (\tau, \beta :: \text{collection}) \text{ VAL} \)

(_ \rightarrow \text{collect}(\_ | \_)) [71,100,70,50]

\textbf{248}
In principle, the following concepts could be defined—more or less directly as according to their specification in the standard—conservatively as constant definition, similarly to an abbreviation. However, we refrained from this possibility due to our theory-morpher technique, which requires as many as possible operator definitions in combinator format and derives the resulting properties from there. Consequently, we stated the requirements following from the standard simply as unproven lemmas and prove them later.

The following lemmas are unproven—they mirror the requirements in the standard and are intended as typechecked equivalents. These collection are proven on the basis of the concrete definitions in the concrete collection class theories.

One might wonder why the Isabelle-concept of an axiomatic class is not used here. The reason is that the underlying type concept of Isabelle (Order-Sorted Polymorphism in Isabelle) is too weak to express the connection between the type constructors to be specified and their content; in the subsequent declaration for example, there is no connection between \( \tau::\text{collection} \) and text \( \alpha::\text{bot} \) as there should be. These types in the abstract class are therefore quite rough approximations. As a consequence, axiomatic classes would easily require very general properties that can not be met by any concrete instance.

### Count

The standard requires the following definition:

**Lemma** \( \text{REQ}_{11.7.1.4} \):

\[
\text{self} \rightarrow \text{count}(\text{obj}) \equiv
\]
Appendix B. Isabelle Theories

\[ \text{self } \rightarrow \text{iterate(elem;acc=0 | if elem } \triangleq \text{ obj then acc } + 1 \text{ else acc endif)} \]

\text{oops}

Unfortunately, for the case of sets, this definition assumes that sets are “duplicate free lists” which is simply not the case in general, in particular if we admit infinite sets as in HOL-OCL.

Instead, we define the properties pointwise for each collection.

\textbf{Excludes}

The standard defines exclusion via \textit{->count}, which is possible, but messy with hindsight to a standard set theory:

\textbf{lemma} \textit{REQ11_7_1_3}:
\[ \text{self } \rightarrow \text{excludes(obj)} \equiv (\text{self } \rightarrow \text{count(obj)} \triangleq 0) \]

\text{oops}

\textbf{includesAll}

The definition of \textit{->includesAll} strictly follows the standard \textit{REQ11_7_1_5}:

\textbf{lemma} \textit{REQ11_7_1_5}:
\[ (\text{self } \rightarrow \text{includesAll(obj)}) \equiv \forall \text{elem} . (\text{self } \rightarrow \text{includes(elem))) } \]

\text{oops}

Unfortunately, this form of definition is \textit{not} conservative for type technical reasons: elem is too polymorphic and contains a free type variable not occurring in the lhs of this equation. Solution: \textit{->includesAll} must be defined individually on each concrete collection.

With the following three definitions, the situation is the same.

\textbf{lemma} \textit{REQ11_7_1_6}:
\[ (\text{self } \rightarrow \text{excludesAll(obj)}) \equiv \forall \text{elem} . (\text{self } \rightarrow \text{excludes(elem))) } \]

\text{oops}

\textbf{lemma} \textit{REQ11_7_1_7}:
\[ \text{isEmpty self } \equiv (\text{self } \rightarrow \text{size()} \triangleq 0) \]

\text{oops}

\textbf{lemma} \textit{REQ11_7_1_8}:
\[ \text{notEmpty X } \equiv \neg (\text{isEmpty}(X)) \]

\text{oops}

\textend

\textbf{B.4.10. OCL Sequence}

\texttt{theory} \texttt{OCL\_Sequence}

\texttt{imports}
\texttt{HOLOCL\_HOME/src/library/collection/OCL\_Collection}
\texttt{HOLOCL\_HOME/src/library/collection/HOL\_Collections\_ext}

\texttt{begin}

\texttt{250}
### Theorems needed in this theory but not belonging to it

#### Very often used simplifier sets

**Lemma** \( \text{DEF\_def\_both} \): 
\[
\text{DEF} \ X \equiv (\bot \neq X \land X \neq \bot)
\]
by (simp add: DEF\_def neq\_commute)

#### Lifting

**Lemma** \( \text{not\_down\_lift\_drop} \) [simp]: 
\[
x \neq \text{down} \implies \lfloor x \rfloor = x
\]
by (drule not\_down\_exists\_lift [THEN iffD1], auto)

#### Logic core

**Lemma** \( \text{and\_equiv\_sand} \): 
\[
\llbracket \tau \models \partial X; \tau \models \partial Y \rrbracket = \implies (X \land Y) \tau = (X \lor Y) \tau
\]
by (simp add: OclSand\_def OclAnd\_def localValid\_Defined\_2sem ss\_lifting)

**Lemma** \( \text{ocl\_if\_totally\_undefined} \) [simp]: 
\[
(\text{if} \ P \ \text{then} \bot \ \text{else} \bot \ \text{endif}) = \bot
\]
by (rule ext, simp add: OclIf\_def OclUndefined\_def ss\_lifting)

**Lemma** \( \text{if\_distrib\_defined} \): 
\[
\llbracket \tau \models \partial X; \tau \models \partial (P \land (\text{if} 
X \ \text{then} 
Y \ \text{else} 
Z \ \text{endif})) \rrbracket = \implies P(\text{if} \ X \ \text{then} \ Y \ \text{else} 
Z \ \text{endif}) \tau = (\text{if} \ X \ \text{then} 
P \ Y \ \text{else} 
P \ Z \ \text{endif}) \tau
\]
apply (auto simp: OclIf\_def localValid\_Defined\_2sem ss\_lifting)
auto

**Lemma** \( \text{if\_distrib\_strict\_alt} \): 
\[
\llbracket \tau \models (P \land (\text{if} \ X \ \text{then} 
Y \ \text{else} 
Z \ \text{endif})) \rrbracket = \implies (\text{if} \ X \ \text{then} 
(P \land (\text{if} \ X \ \text{then} 
Y \ \text{else} 
P \ Z \ \text{endif}))) \tau
\]
by (simp add: if\_distrib\_strict is\_Strict\_def OclUndefined\_def lift0\_def)

**Lemma** \( \text{if\_not} \): 
\[
(\text{if} \ X \ \text{then} 
Y \ \text{else} 
Z \ \text{endif}) = (\text{if} \ X \ \text{then} 
Z \ \text{else} 
Y \ \text{endif})
\]
by (rule ext, simp add: OclIf\_def OclNot\_def ss\_lifting)

**Some cp theory to simplify the later proofwork**

Adding currently missing cp-ness results to the simpset

**Lemmas** \( \text{cp\_hol\_simp} \) [simp,intro!]: \( \text{cp\_lift2} \) [simplified lift2\_def, of _ _ op \( \rightarrow \)]

**Lemmas** \( \text{cp\_hol\_and} \) [simp,intro!]: \( \text{cp\_lift2} \) [simplified lift2\_def, of _ _ op \( \land \)]
Appendix B. Isabelle Theories

lemmas cp_hol_or [simp,intro] = cp_lift2[simplified lift2.def, of _ op \lor]
lemmas cp_hol_not [simp,intro] = cp_lift1[simplified lift1.def, of _ \lambda x. \neg x]

lemma cp_or [simp,intro]: [ \[ cp P; cp P' \] \implies cp (\lambda X. (P X) \lor (P' X))
by(simp add: OclOr_def)

declare cp_strongEq [simp,intro]

lemma cp_sor [simp,intro]: [ \[ cp P; cp P' \] \implies cp (\lambda X. (P X) \lor (P' X))
by(simp add: OclSor_def)

lemma cp_sand [simp,intro]: [ \[ cp P; cp P' \] \implies cp (\lambda X. (P X) \land (P' X))
by(simp add: OclSor_def)

lemma cp_xor [simp,intro]: [ \[ cp P; cp P' \] \implies cp (\lambda X. (P X) \oplus (P' X))
by(simp add: OclSxor_def)

A very useful substitution rule

lemma cp_subst: [ \[ cp P \] \implies P (lift0 (x \tau)) \tau
by(subst (asm) cp_by_cpify, auto)

Setup of the environment

Special parameters

Properties of Datatype Adaption

The following rules are transformed versions of the automatically generated rules for
datatype adaption

lemma Abs_Sequence_0_inject_charn: [ (\bot::\tau = bot) \notin set x; (\bot::\tau = bot) \notin set y ] \implies ((Abs_Sequence_0 \down x) = (Abs_Sequence_0 \down y)) = (x = y)
by(subst Abs_Sequence_0_inject, simp_all add: OCL_Sequence_type.Sequence_0_def smash_def)

These are derived rules from the above one that allow the simplifier to detect false
assumptions which make a goal trivially true.

lemma Abs_Sequence_0_inject_absurd11 [simp]: [ \bot \notin set x ] \implies ((Abs_Sequence_0 \down) = (Abs_Sequence_0 \down x)) = False
by(subst Abs_Sequence_0_inject, simp_all add: OCL_Sequence_type.Sequence_0_def smash_def)

lemma Abs_Sequence_0_inject_absurd12 [simp]:
B.4. Library

\[ \bot \notin \text{set } x \implies ((\text{Abs}\_\text{Sequence}\_0(x)) = (\text{Abs}\_\text{Sequence}\_0 \downarrow)) = \text{False} \]
by (subst Abs\_Sequence\_0\_inject,
    simp\_all\ add: OCL\_Sequence\_type.Sequence\_0\_def smash\_def)

**Lemma** Abs\_Sequence\_0\_inject\_absurd21 [simp]:
\[ \bot \notin \text{set } x \implies (\bot = (\text{Abs}\_\text{Sequence}\_0(x))) = \text{False} \]
by (simp\_add: UU\_Sequence\_def)

**Lemma** Abs\_Sequence\_0\_inject\_absurd22 [simp]:
\[ ((\text{Abs}\_\text{Sequence}\_0(x)) = \bot) = \text{False} \]
by (simp\_add: UU\_Sequence\_def)

**Lemma** Abs\_Sequence\_0\_inverse\_charn1 [simp]:
\[ (\bot \notin \text{set } x) \implies \text{Rep}\_\text{Sequence}\_0(\text{Abs}\_\text{Sequence}\_0(x)) = x \]
by (subst Abs\_Sequence\_0\_inverse,
    simp\_all\ add: OCL\_Sequence\_type.Sequence\_0\_def smash\_def)

**Lemma** Abs\_Sequence\_0\_inverse\_charn2 [simp]:
\[ (\bot \notin \text{set } x) \implies \text{Rep}\_\text{Sequence}\_0(\text{Abs}\_\text{Sequence}\_0(x))^\downarrow = x \]
by (subst Abs\_Sequence\_0\_inverse,
    simp\_all\ add: OCL\_Sequence\_type.Sequence\_0\_def smash\_def)

**Lemma** Abs\_Sequence\_0\_cases\_charn:
\[ \text{assumes bottomCase: } [x = \bot] \implies P \]
\[ \text{assumes listCase : } \forall y. ([x = \text{Abs}\_\text{Sequence}\_0(y), \bot \notin \text{set } y] \implies P) \]
\[ \text{shows} \]
apply (rule_tac x = x in Abs\_Sequence\_0\_cases)
apply (case_tac y = \bot)
apply (rule bottomCase, simp\_add: UU\_Sequence\_def)
apply (frule not\_down\_exists\_lift2 [THEN iffD1])
apply (rule_tac y = "y" in listCase)
apply (auto simp: OCL\_Sequence\_type.Sequence\_0\_def smash\_def)
done

**Lemma** Abs\_Sequence\_0\_induct\_charn:
\[ \text{assumes bottomCase: } P \bot \]
\[ \text{assumes stepCase : } \forall y. ([\bot \notin \text{set } y] \implies P (\text{Abs}\_\text{Sequence}\_0(y))) \]
\[ \text{shows} \]
apply (rule_tac x = x in Abs\_Sequence\_0\_induct)
apply (rule_tac x = Abs\_Sequence\_0 y in Abs\_Sequence\_0\_cases\_charn)
apply (auto intro: bottomCase elim: stepCase)
done

These rules stem from the set theory, that was the first collection theory. It should actually be decided which of them are really needed anymore because the above rules cover most cases.

**Lemma** inj\_on\_Abs\_Sequence\_0\_injection
\[ \text{by (rule inj\_on\_inverse1, rule Sequence\_0.Abs\_Sequence\_0\_inverse, assumption)} \]

253
Appendix B. Isabelle Theories

**Lemma inj Rep Sequence**: \( \text{inj Rep Sequence 0} \)

```isar
to run
```

**Lemma smashed_sequence_charn**: \( (\bot \notin \text{set X}) = ((X) \in \text{Sequence 0}) \)

```isar
to run
```

**Lemma UU in smashed_sequence [simp]**: \( \bot \in \text{Sequence 0} \)

```isar
to run
```

**Lemma down in smashed_sequence [simp]**: \( \bot \in \text{Sequence 0} \)

```isar
to run
```

**Lemma mt in smashed_sequence [simp]**: \( (\emptyset) \in \text{Sequence 0} \)

```isar
to run
```

**Lemma DEF Abs Sequence**: \( \forall X. (\bot \notin \text{set X}) \implies \text{DEF} (\text{Abs Sequence 0} (X)) \)

```isar
to run
```

**Lemma DEF Rep Sequence**: \( \forall X. \text{DEF} X = \text{DEF} (\text{Rep Sequence 0} X) \)

```isar
to run
```

**Lemma not DEF Rep Sequence**: \( \forall X. \neg \text{DEF} X \implies \neg \text{DEF} (\text{Rep Sequence 0} X) \)

```isar
to run
```

**Lemma exists lift Sequence**: \( \forall X. \text{DEF} X \implies \exists c. \text{Rep Sequence 0} X = (c) \)

```isar
to run
```

**Lemma exists lift Sequence2**: \( \forall X. \text{DEF} X \implies \exists c. \bot \notin \text{set c} \land \text{Rep Sequence 0} X = (c) \)

```isar
to run
```

254
These two \textit{DEF\_X\_Sequence} lemmas are a central part in almost every proof that unfolds the OCL definitions. Furthermore they will also be used by the \texttt{thy\_morpher} to automatically lift theorems about HOL lists to theorems about OCL sequences.

Because in most cases both versions of the above theorems are used they are packed conveniently in this lemma.

And to enable a fast case splitting over (un)definedness of a specific sequence together with its semantic representation these two theorems are very useful. Note that there exists a \_0 version which does not require cp-ness. This \_0 version exists actually for almost all more complex theorems because not in all cases one has or can show cp-ness.

\textbf{B.4. Library}
Appendix B. Isabelle Theories

assumes defC: \( \forall c \in c.d. \ [ X \neq \bot; \bot \neq X \); 
(\bot \notin \text{set} c); (\bot \notin \text{set} d); 
\text{Rep\_Sequence\_0} X = \_c; \ 
X = \text{Abs\_Sequence\_0} \_d; \) \( \Longrightarrow \) P X
and undefC: \( [ X = \bot ] \Longrightarrow P X \)
shows P X
apply(rule Abs\_Sequence\_0_cases_charn, erule undefC)
apply(rule defC, auto)
done

lemma Sequence\_sem\_cases:
assumes defC: \( \forall c \in c.d. \ [ (X \tau) \neq \bot; \bot \neq (X \tau) \); 
(\bot \notin \text{set} c); (\bot \notin \text{set} d); 
\text{Rep\_Sequence\_0} (X \tau) = \_c; \ 
(X \tau) = \text{Abs\_Sequence\_0} \_d; \) \( \Longrightarrow \) P X \tau
and undefC: \( [ (X \tau) = \bot ] \Longrightarrow P X \tau \)
shows P X \tau
apply(rule_tac X = X in Sequence\_sem\_cases, rule cpP)
apply(rule Sequence\_sem\_cases_0)
apply(rule_defC prefer 7)
apply(rule_tac X = X in subst[OF cp_subst], rule cpP)
apply(rule undefC, simp_all)
done

And a version for the case that we’re reasoning over equalities of functions.

lemma Sequence\_sem\_cases\_ext:
assumes defC: \( \forall c \in c.d. \ [ (X \tau) \neq \bot; \bot \neq (X \tau) \); 
(\bot \notin \text{set} c); (\bot \notin \text{set} d); 
\text{Rep\_Sequence\_0} (X \tau) = \_c; \ 
(X \tau) = \text{Abs\_Sequence\_0} \_d; \) \( \Longrightarrow \) P X \tau = Q X \tau
and cpP: \( [ (X \tau) = \bot ] \Longrightarrow P X \tau = Q X \tau \)
and cpQ: \( [ (X \tau) = \bot ] \Longrightarrow P X \tau = Q X \tau \)
shows P X = Q X
apply(rule ext)
apply(rule savedInstanceStates[OF sym[OF cp_subst]], rule cpP)
apply(rule savedInstanceStates)
apply(rule_defC prefer 7)
apply(rule undefC)
apply(simp_all add: cpP cpQ)
done

These four lemmas are used by ocl\_setup\_op to reason about definedness:

lemma lift2\_strict\_is\_isdef\_fw\_Sequence\_Val:
assumes f\_def: \( f = \text{lift2}(\text{strictify}(\lambda x. \text{strictify}(\lambda y. \text{Abs\_Sequence\_0} \_g \text{Rep\_Sequence\_0} x y))) \)
and inv\_g: \( \forall a b. \ [ \bot \notin \text{set} a; (\bot \notin \text{set} b) \) \( \Longrightarrow \bot \notin \text{set} (g a b) \)
shows \( \partial(f X Y) = (\partial X \land \partial Y) \)
apply (rule ext)
apply (simp add: f_def OclIsDefined_def OclAnd_def 
  o_def ss_lifting)
apply (rule_tac X = X x in Sequence_sem_cases_0)
apply (rule impl, drule_tac b = (Y x) in inv_g)
apply (simp_all add: neq_commute)
done

lemma lift2_strict_is_isdef_fw_Sequence_Sequence:
  assumes f_def: \( f \equiv \text{lift2} (\text{strictify}(\lambda x. \text{strictify}(\lambda y. \text{Abs_Sequence_0} \langle g \langle \text{Rep_Sequence_0} x \rangle \rangle \langle g \langle \text{Rep_Sequence_0} y \rangle \rangle))) \)
  and inv_g: \( \forall a b. (\bot \notin \text{set} a; \bot \notin \text{set} b) \Longrightarrow \bot \notin \text{set} (g a b) \)
  shows \( \partial (f X Y) = (\partial X \land \partial Y) \)
apply (rule ext)
apply (simp add: OclIsDefined_def OclAnd_def 
  o_def ss_lifting)
apply (rule_tac X = X x in Sequence_sem_cases_0)
apply (rule_tac X = Y x in Sequence_sem_cases_0)
apply (rule impI, drule_tac b = ca in inv_g)
apply (simp_all add: neq_commute)
done

lemma lift2_strictify_implies_LocalValid_defined_Sequence_Val:
  assumes f_def: \( f \equiv \text{lift2} (\text{strictify}(\lambda x. \text{strictify}(\lambda y. \text{Abs_Sequence_0} \langle g \langle \text{Rep_Sequence_0} x \rangle \rangle \langle g \langle \text{Rep_Sequence_0} y \rangle \rangle))) \)
  and inv_g: \( \forall a b. (\bot \notin \text{set} a; \bot \notin \text{set} b) \Longrightarrow \bot \notin \text{set} (g a b) \)
  shows \( \tau \vdash \partial (f X Y) = (\tau \vdash \partial X \land \tau \vdash \partial Y) \)
apply (insert f_def)
apply (drule_tac X = X and Y = Y in lift2_strict_is_isdef_fw_Sequence_Val)
apply (rule inv_g, assumption+)
apply (simp add: OclAnd_def OclTrue_def o_def 
  OclIsDefined_def lift0_def lift1_def lift2_def 
  OclLocalValid_def)
done

lemma lift2_strictify_implies_LocalValid_defined_Sequence_Sequence:
  assumes f_def: \( f \equiv \text{lift2} (\text{strictify}(\lambda x. \text{strictify}(\lambda y. \text{Abs_Sequence_0} \langle g \langle \text{Rep_Sequence_0} x \rangle \rangle \langle g \langle \text{Rep_Sequence_0} y \rangle \rangle))) \)
  and inv_g: \( \forall a b. (\bot \notin \text{set} a; \bot \notin \text{set} b) \Longrightarrow \bot \notin \text{set} (g a b) \)
  shows \( \tau \vdash \partial (f X Y) = (\tau \vdash \partial X \land \tau \vdash \partial Y) \)
apply (insert f_def)
apply (drule_tac X = X and Y = Y in lift2_strict_is_isdef_fw_Sequence_Sequence)
apply (rule inv_g, assumption+)
apply (simp add: OclAnd_def OclTrue_def o_def 
  OclIsDefined_def lift0_def lift1_def lift2_def 
  OclLocalValid_def)
done
Appendix B. Isabelle Theories

Building a canonic representation of sequences

The empty sequence

constdefs
  OclMtSequence :: ('τ,'α::bot Sequence_0) VAL
  OclMtSequence ≡ lift0(Abs_Sequence_0 [[]]))

syntax
  _OclMtSequence_std :: ('τ,'α::bot) VAL ⇒ 'τ Boolean ([[]])
syntax
  _OclMtSequence_ascii :: ('τ,'α::bot) VAL ⇒ 'τ Boolean (mtSequence)
syntax (xsymbols)
  _OclMtSequence_math :: ('τ,'α::bot) VAL ⇒ 'τ Boolean ([[]])

lemma OCL_is_isdef_OclMtSequence [simp]:
  ⊨ ∅ [[]]
  by(simp add: OclValid_def OclIsDefined_def OclTrue_def
      OclMtSequence_def ss_lifting)

lemma OCL_is_defopt_OclMtSequence [simp]:
  τ ⊨ ∅ [[]]
  by(simp add: valid_elim)

And the ‘cons’ operation: including

defs

OclIncluding_def :
  OclIncluding ≡ lift2(strictify(λS. strictify (λe. Abs_Sequence_0
    (concat ['Rep_Sequence_0 S, |e []] ))))

ocl_setup_op [OclIncluding]

lemma OCL_is_def_OclIncluding:
  (τ ⊨ OclIncluding (X::('τ,'α::bot)Sequence) (Y::('τ,'α::bot)VAL)) = (∅ X ∧ ∅ Y)
  by(rule lift2_strict_is_isdef_fw_Sequence_Val[OF OclIncluding_def, simp])

lemma OCL_is_defopt_OclIncluding:
  (τ ⊨ OclIncluding (X::('τ,'α::bot)Sequence) (Y::('τ,'α::bot)VAL)) = ((τ ⊨ ∅ X) ∧ (τ ⊨ ∅ Y))
  by(rule lift2_strictify_implies_LocalValid_defined_Sequence_Val[OF OclIncluding_def, simp])

The syntax translation mkSequence builds our sequences

syntax
  @OclFinSequence :: args ⇒ ('τ,’α Sequence_0) VAL
  (mkSequence([_]))

translations
  mkSequence[x, xs] == OclIncluding (mkSequence[xs]) x
  mkSequence[x] == OclIncluding OclMtSequence x
B.4. Library

lemma test : mkSequence[1,2,3,4,5] = ?X oops

Relation of mtSequence and including

These two theorems should actually suffice to decide inequality of sequences

lemma including_notstrongeq_mtSequence[simp]:
(¬ ((X:(τ,α::bot)Sequence) ↠ including (a:(τ,α)VAL) ↑ [])) = T
apply(rule_tac X=X in SequenceSem_cases_ext)
apply(simp_all add: cp_strongEq)
done

lemma including_notstricteq_mtSequence[simp]:
\[ \tau \not\models \partial \((a::(\tau,\alpha::bot)VAL);\ \tau \not\models \partial \ (X::(\tau,\alpha::bot)Sequence) \) = \Rightarrow \ \tau \not\models (X\rightarrow\text{including } a) \langle\text{<}\rangle \ [\ [\ ]\ ]\]\napply(rule_tac X=X in SequenceSem_cases)
apply(simp_all add: cp_strictEq)
done

Case exhaustion over the canonic representation

lemma Sequence_cases_including_0:
assumes undefCase: \[ \llbracket (X::(\tau::bot Sequence_0) = \bot) \rrbracket \Rightarrow P \]
and mtCase: \[ \llbracket X = ([ ] \tau) \rrbracket \Rightarrow P \]
and stepCase: \[ \bigwedge \ (Y::(\tau::bot Sequence_0) (a::(\tau::bot)),\ \llbracket DEF Y; DEF a; X = (((lift0 Y) \rightarrow\text{including } (lift0 a)) \) \rrbracket \Rightarrow P \]
shows \[ P \]
apply(rule AbsSequence_0_cases_charn, rule undefCase)
apply(rule tac zs=y in rev_cases)
apply(rule mtCase)
apply(simp add: OclMtSequence_def ss_lifting')
apply(rule_tac Y=AbsSequence_0 ys and a=ya in stepCase)
apply(simp_all add: OclIncluding_def ss_lifting' neq_commute)
done

lemma Sequence_cases_including:
assumes undefCase : \[ \tau \models (X:(\tau,\alpha::bot)Sequence) \triangleq \bot \] \Rightarrow P \tau
and mtCase: \[ \tau \models X \triangleq [ ] \] \Rightarrow P \tau
and stepCase: \[ \bigwedge \ (Y:(\tau,\alpha::bot)Sequence) (a:(\tau,\alpha::bot)VAL),\ \llbracket \tau \models X \triangleq Y \rightarrow\text{including } a;\ \tau \models \partial Y;\ \tau \models \partial a \rrbracket \Rightarrow P \tau \]
Appendix B. Isabelle Theories

shows
apply (rule_tac X=X \ and \ \tau=\tau \ in \ Sequence_cases_including_0)
apply (rule undefCase) prefer 2
apply (rule mtCase) prefer 3
apply (rule stepCase, simp_all add: localValidDefined2sem)
apply (simp_all add: localValid2sem OclStrongEq_def OclUndefined_def ss_lifting)
done

Induction over the canonic representation

To simplify reasoning there exists a \_0 version which doesn’t pose any restrictions on the involved functions with regard to context-passingness.

lemma Sequence_induct_including_0:
assumes undefCase: P \bot
and mtCase: P (\[] \tau)
and stepCase: \forall (X::\tau::\bot Sequence_0) (a::\tau::bot).
\[ P X; DEF X; DEF a \Rightarrow (P ((OclIncluding (lift0 X) (lift0 a)) \tau)) \]
shows
apply (rule Abs_Sequence_0_induct_charn, rule undefCase)
apply (erule rev_mp)
apply (rule rev_induct)
apply (insert mtCase, simp add: OclMtSequence_def ss_lifting)
apply (auto)
apply (rotate_tac \-1, drule_tac a=x \ and \ X=Abs_Sequence_0 (xs in stepCase)
apply (erule DEF_Abs_Sequence)
apply (simp_all add: OclIncluding_def neq_commute ss_lifting)
done

lemma Sequence_induct_including:
assumes undefCase : P \bot
and mtCase: P \[] \tau
and stepCase: \forall (X:(\tau,\alpha::\bot)Sequence) (a:(\tau,\alpha::\bot)VAL).
\[ P X \tau; \tau \models \delta X; \tau \models \delta a \Rightarrow P (OclIncluding X a) \tau \]
and cpP: cp P
shows
apply (insert cpP)
apply (frule cp_by_cpfy[THEN iffD2])
apply (rule subst, rule sym)
apply (rule_tac x=X in cp_subst, simp)
apply (rule_tac \tau=\tau \ in \ Sequence_induct_including_0)
apply (insert undefCase)
apply (auto simp: OclUndefined_def intro!: mtCase)
apply (drule stepCase)
apply (simp_all add: localValidDefined2sem lift0_def)
done
A second sequence constructor on the OCL level

defs

OclCollectionRange_def :
OclCollectionRange ≡ lift2 (strictify (λ x::Integer. 0. strictify (λ y.
Abs_Sequence_0.map (λ z::nat. (int z + (∗x∗))
[0..<(nat (∗y∗) − (∗x∗) + 1)])))

ocl_setup_op [OclCollectionRange]

lemma OCL_is_defopt_OclCollectionRange [simp];
τ ⊨ ∅ ((OclCollectionRange (a::’a Integer)) b::(’a, Integer_0)Sequence) =
((τ ⊨ ∅ a) ∧ (τ ⊨ ∅ b))
apply(subgoal_tac ⊲ ∈ set (map (λ z. ((int z + (∗a∗) ])) [0..<(nat (’b τ ∗) − (’a τ))
+ 1)])
apply(auto simp: localValidDefined2sem OclCollectionRange_def ss_lifting)
done

lemma collectionRange_mtSequence_conv:
[ τ ⊨ (b::’a Integer) < (a::’a Integer) ] ⊢
OclCollectionRange a b τ = (\[[\tau],\tau\],\tau\](Sequence) τ
apply(case_tac τ ⊨ ∅ a, ocl_hypsubst, simp)
apply(case_tac τ ⊨ ∅ b, ocl_hypsubst, simp)
apply(simp add: localValidDefined2sem DEF_def_both, clarify)
apply(simp_all add: DEF_def OclCollectionRange_def OclMtSequence_def
OclLess_def localValid2sem ss_lifting)
done

lemma collectionRange_singleton_UC[simp];
OclCollectionRange a a = (\[[\tau],\tau\],\tau\](Sequence) ⇒including (a::’a, Integer_0) VAL
apply(erule ext, case_tac x ⊨ ∅(a), ocl_hypsubst, simp)
apply(simp add: OclCollectionRange_def OclMtSequence_def OclIncluding_def
localValidDefined2sem ss_lifting)
done

lemma collectionRange_expand_including:
[ τ ⊨ (a::’a Integer) ≤ b ] ⊢
((OclCollectionRange a b)::(’a, Integer_0)Sequence) τ =
(OclCollectionRange a (b − 1) ⇒including b τ
apply(subgoal_tac ⊲ ∉ set (map (λ z. ((int z + (∗a∗) ])) [0..<(nat (’b τ ∗) − (’a τ))
+ 1)])
apply(subgoal_tac ⊲ ∉ set (map (λ z. ((int z + (∗a∗) ])) [0..<(nat (’b τ ∗) − (’a τ)))]
apply(auto simp: OclCollectionRange_def OclIncluding_def
OclLe_def minus_def One_ocl_int_def localValid2sem ss_lifting)
apply(subst Abs_Sequence_0.inject_charn, auto)
apply(subgoal_tac (nat (’b τ ∗) − (’(a τ)) + 1)) = (nat (’b τ ∗) − (’(a τ)) + (nat 1))

B.4. Library
Appendix B. Isabelle Theories

apply(simp, arith)
done

The conversion operators

Sequence to sequence
defs

OclAsSequence_def :  
OclAsSequence ≡ id

lemma asSequence_identity[simp]:
OclAsSequence (S::('r,'a::bot)Sequence) = S
by(simp add: OclAsSequence_def)

Sequence to bag
defs

OclAsBag_def :
OclAsBag ≡ lift1 (strictify (λX. 
Abs_Bag_0 ⌞ multiset_of ⌜ Rep_Sequence_0 X ⌝ ⌝

ocl_setup_op [OclAsBag]

Sequence to ordered set
defs

OclAsOrderedSet_def :
OclAsOrderedSet ≡ lift1 (strictify (λX. 
Abs_OrderedSet_0 ⌜ rev (remdups (rev ⌜ Rep_Sequence_0 X ⌝)) ⌝

ocl_setup_op [OclAsOrderedSet]

Sequence to set
defs

OclAsSet_def :
OclAsSet ≡ lift1 (strictify (λX. Abs_Set_0 ⌜ set ⌜ Rep_Sequence_0 X ⌝)

ocl_setup_op [OclAsSet]

OclIterate
defs

OclIterate_def :
OclIterate ≡ (lift3' lift_arg0 lift_arg2 lift_arg0) (strictify (λ S P A. 
(foldl (λ x y. P y x) A (⌜Rep_Sequence_0 S⌝))))
The characteristic behaviour of iterate on the canonical representation

**lemma iterate_of_mtSequence[simp]:**

\[
\text{OclIterate ([]}::(\tau, \alpha::\text{bot})\text{Sequence})
\]

\[
(P::((\tau \Rightarrow \alpha) \Rightarrow ((\tau \Rightarrow 'c::\text{bot}) \Rightarrow (\tau \Rightarrow 'c)))
\]

\[
A = A
\]

apply(rule ext)
apply(subgoal_tac x ⊭ (∂[]))
apply(simp_all add: OclIterate_def OclIncluding_def OclMtSequence_def localValidDefined2sem ss_lifting)
done

**lemma iterate_of_including_0:**

assumes defS: \(\tau \vdash \partial(S::(\tau, (\alpha::\text{bot})\text{Sequence}))\)
and defx: \(\tau \vdash \partial(x::(\tau \Rightarrow (\alpha::\text{bot})))\)
shows \((\text{OclIterate (OclIncluding } S x P A) \tau) =

\((P (\text{lft0 (x }\tau)) (\text{lft0 ((OclIterate (S::((\tau, (\alpha::\text{bot})\text{Sequence})) P A) }\tau) \tau)) \tau)\)

apply(insert defS defx)
apply(frule_tac Y1=x in conjI[THEN OCL_is_defopt_OclIncluding[THEN iffD2]], assumption)
apply(simp add: localValidDefined2sem DEF_def)
apply(frule DEF_X_Sequence', clarify)
apply(simp add: OclIterate_def OclIncluding_def ss_lifting)
apply(frule DEF_X_Sequence', clarify, simp)
apply(subst (asm) Abs_Sequence_0_inject_charn, auto)
done

**lemma iterate_of_including:**

assumes defS: \(\tau \vdash \partial(S::(\tau, (\alpha::\text{bot})\text{Sequence}))\)
and defx: \(\tau \vdash \partial(x::(\tau \Rightarrow (\alpha::\text{bot})))\)
and cpP_1: \(\forall y. \text{cp (}(\lambda x. P x y)\))
and cpP_2: \(\forall x. \text{cp (}(P x \Rightarrow ((\text{OclIterate (S::((\tau, (\alpha::\text{bot})\text{Sequence})) P A) }\tau)) \tau)\)
apply(insert defS defx cpP_1 cpP_2)
apply(frule_tac x=x in iterate_of_including_0 and P=P and A=A in iterate_of_including_0)
apply(simp_all add: cp_by_cpify)
done

**lemma iterate_opt_of_including:**

assumes P_undef_1: \(!!y. \ P \perp y = \perp\)
and P_undef_2: \(!!x. \ P x \perp = \perp\)
and cpP_1: \(\forall x. \text{cp (}(\lambda y, cp (\lambda x. P x y)\))
and cpP_2: \(\forall x. \text{cp (}(P::(\tau, \alpha::\text{bot})\text{VAL} \Rightarrow (\tau', 'c::\text{bot})\text{VAL} \Rightarrow (\tau', 'c::\text{bot})\text{VAL}) x)\)
shows \((\text{OclIterate (OclIncluding } S x P A) =

\((P x (\text{OclIterate (S::((\tau, (\alpha::\text{bot})\text{Sequence})) P A}))\))\)

263
Appendix B. Isabelle Theories

apply(insert P_undef_1 P_undef_2 cpP_1 cpP_2)
apply(rule ext)
apply(case_tac xa = S)
apply(case_tac xa = x)
apply(rule iterate_of_including, simp_all)
apply(frule isUndefined_charn_local THEN iffD2)
apply(rule syn[OF trans], rule_tac A=x in cp_charn, simp, simp)
apply(frule isUndefined_charn_local THEN iffD2)
apply(rule trans, rule_tac A=S in cp_charn, simp, simp)
apply(rule syn[OF trans], rule_tac A=S in cp_charn)
apply(rule_tac P=P x in cp-compose2, simp_all)
done

The universal and fusion property

Fusion and universal theorems, as described in [25].

lemma iterate_universal_0:
  assumes g_CP: cp g
  and g_undef: g (λx.('α:'c::bot)Sequence) τ = (⊥::('τ::'c::bot)VAL) τ
  and g_mtSeq: g (OclMtSequence::('τ::'c::bot)Sequence) τ = A τ
  and g_incl: ∀ S x. [ τ ⊨ ∂ S; τ ⊨ ∂ x ] ⇒ g (OclIncluding S x) τ = P (lift0 (x τ)) (lift0 (g S τ)) τ
  shows g S τ = OclIterate S P::('τ::'c::bot)VAL ⇒ (τ::'c::bot)VAL ⇒ (τ::'c::bot)VAL) A τ
apply(rule_tac X=S in Sequence_induct_including)
apply(simp_all add: g_CP g_undef g_mtSeq)
apply(subst iterate_of_including_0, simp_all add: g_incl)
done

lemma iterate_universal:
  assumes g_CP: cp g
  and cpP_1: ∀ y. cp (λ x. P x y)
  and cpP_2: ∀ x. cp (P x)
  and g_undef: g ⊥ = (⊥::('τ::'c::bot)VAL) τ
  and g_mtSeq: g (OclMtSequence::('τ::'c::bot)Sequence) τ = A τ
  and g_incl: ∀ S x. [ τ ⊨ ∂ S; τ ⊨ ∂ x ] ⇒ g (OclIncluding S x) τ = P (x τ) (g S τ)
  shows g S τ = OclIterate S P::('τ::'c::bot)VAL ⇒ (τ::'c::bot)VAL ⇒ (τ::'c::bot)VAL) A τ
by(insert cpP_1 cpP_2 g_CP, rule iterate_universal_0, simp_all add: g_undef g_mtSeq g_incl cpP_by_cpfy)

lemma iterate_universal_0_opt:
  assumes g_CP: cp g
  and g_mtSeq: g (OclMtSequence::('τ::'c::bot)Sequence) τ = A τ
  and g_incl: ∀ S x. [ τ ⊨ ∂ S; τ ⊨ ∂ x ] ⇒ g (OclIncluding S x) τ = P (lift0 (x τ)) (lift0 (g S τ)) τ
  and defS: τ ⊨ ∂ S

264
shows \( g \ S \tau = \text{OclIterate} \ S \ (P; (\tau, \alpha :: \text{bot}) \text{VAL} \Rightarrow (\tau, \alpha :: \text{bot}) \text{VAL} \Rightarrow (\tau, \alpha :: \text{bot}) \text{VAL}) \) A \( \sigma \)
apply (insert defS, erule rev_mp)
apply (rule_tac X=S in Sequence_induct_including)
apply (simp_all add: g_cp g_mlSec)
apply (subst iterate_of_including_0, simp_all add: g_incl)
done

lemma iterate_universal_opt:
assumes g_cp: cp g
and cpP_1: \( \forall y. \, \text{cp} \ (x \cdot P \ x \ y) \)
and cpP_2: \( \forall x. \, \text{cp} \ (P \ x) \)
and g_mlSeq: \( \text{g} \ \text{OclMtSequence} \ (\forall \tau. \, (\alpha :: \text{bot}) \text{Sequence}) \) \( \tau \Rightarrow A \ \tau \)
and g_incl: \( \forall S \ x \cdot \left( \forall \tau. \, \tau \equiv \emptyset \ S ; \tau \equiv \emptyset \ x \right) \Longrightarrow \text{g} \ (\text{OclIncluding} \ S \ x) \tau = P \ x \ (g \ S) \tau \)
and defS: \( \sigma \equiv \emptyset \ S \)
shows \( g \ S \tau = \text{OclIterate} \ S \ (P; (\tau, \alpha :: \text{bot}) \text{VAL} \Rightarrow (\tau, \alpha :: \text{bot}) \text{VAL} \Rightarrow (\tau, \alpha :: \text{bot}) \text{VAL}) \) A \( \sigma \)
by (insert cpP_1 cpP_2 g_cp, rule iterate_universal_0_opt,
simp_all add: g_mlSeq g_incl cp_by_cpify)

lemma iterate_fusion_0_opt:
[| cp h; DEF (S \tau); h \ B \tau = A \ tau; \( \forall x. \forall y. \, h \ (Q \ (lift0 \ (x \ \tau)) \ (lift0 \ (y \ \tau))) \tau = P \ (lift0 \ (x \ \tau)) \ (lift0 \ (h \ y \ \tau)) \tau \) |] 
\( h \ (\text{OclIterate} \ (S; (\tau, \alpha :: \text{bot}) \text{Sequence}) \ (Q; (\tau, \alpha :: \text{bot}) \text{VAL} \Rightarrow (\tau, \alpha :: \text{bot}) \text{VAL} \Rightarrow (\tau, \alpha :: \text{bot}) \text{VAL}) \) \ B \( \tau \)
= \text{OclIterate} \ S \ (P; (\tau, \alpha :: \text{bot}) \text{VAL} \Rightarrow (\tau, \alpha :: \text{bot}) \text{VAL} \Rightarrow (\tau, \alpha :: \text{bot}) \text{VAL}) \ A \( \sigma \)
apply (rule iterate_universal_0_opt)
apply (rule_tac P=h in cp_compose2)
apply (simp_all)
apply (rule trans, rule_tac P=h in cp_subst, simp)
apply (subst iterate_of_including_0)
apply (simp_all add: cp_by_cpify validDefined2sem)
done

lemma iterate_fusion_opt:
[| cp h; \( \forall x. \, \text{cp} \ (P \ x) \); h \ B \tau = A \ tau; \( \forall x \ y. \, h \ (Q \ x \ y) \tau = P \ x \ (h \ y) \tau \) |] 
\( h \ (\text{OclIterate} \ (S; (\tau, \alpha :: \text{bot}) \text{Sequence}) \ (Q; (\tau, \alpha :: \text{bot}) \text{VAL} \Rightarrow (\tau, \alpha :: \text{bot}) \text{VAL} \Rightarrow (\tau, \alpha :: \text{bot}) \text{VAL}) \) \ B \( \tau \)
= \text{OclIterate} \ S \ (P; (\tau, \alpha :: \text{bot}) \text{VAL} \Rightarrow (\tau, \alpha :: \text{bot}) \text{VAL} \Rightarrow (\tau, \alpha :: \text{bot}) \text{VAL}) \ A \( \tau \)
Appendix B. Isabelle Theories

apply(route iterate_fusion_0_opt)
apply(assumption)+
apply(simp add: localValidDefined2sem)
apply(assumption)
apply(subgoal_tac h y τ = h (lift0 (y τ)) τ)
apply(simp)
apply(route trans)
apply(route_tac P=λ x. P ?X x in cp_subst)
apply(simp_all add: lift0_def cp_by_cpify)
done

lemma iterate_fusion_0:
[ cp h;
  h (\::(\', c::bot) VAL) τ = (\::(\', d::bot) VAL) τ;
  h B τ = A τ;
  \!\!x y. h (Q (lift0 (x τ)) (lift0 (y τ))) τ =
  P (lift0 (x τ)) (lift0 (h y τ) τ)
] \implies
h (OclIterate (S::(\::\', c::bot)Sequence)
  (Q::(\::\', c::bot) VAL ⇒ (\::(\', d::bot) VAL ⇒ (\::(\', c::bot) VAL) B) τ
= OclIterate S (P::(\::\', c::bot) VAL ⇒ (\::(\', d::bot) VAL ⇒ (\::(\', c::bot) VAL) A τ
apply(route iterate_universal_0)
apply(route_tac P=h in cp_compose2)
apply(simp_all)
apply(route trans, route_tac P=h in cp_subst, simp)
apply(subgoal iterate_of_including_0)
apply(simp_all add: cp_by_cpify)
done

lemma iterate_fusion:
[ cp h;
  \!\!x. cp (P x);
  h (\::(\', c::bot) VAL) τ = (\::(\', d::bot) VAL) τ;
  h B τ = A τ;
  \!\!x y. h (Q x y) τ = P x (h y) τ
] \implies
h (OclIterate (S::(\::\', c::bot)Sequence)
  (Q::(\::\', c::bot) VAL ⇒ (\::(\', c::bot) VAL ⇒ (\::(\', c::bot) VAL) B) τ
= OclIterate S (P::(\::\', c::bot) VAL ⇒ (\::(\', d::bot) VAL ⇒ (\::(\', c::bot) VAL) A τ
apply(route iterate_fusion_0)
apply(assumption)+
apply(subgoal_tac h y τ = h (lift0 (y τ)) τ)
apply(simp)
apply(route trans)
apply(route_tac P=λ x. P ?X x in cp_subst)
apply(simp_all add: lift0_def cp_by_cpify)
done
Further properties of iterate

Undeﬁniteness the second part

lemma OCL_undef_2_0clIterate [simp]:
assumes P_undef_2: \(\\forall x. P x \perp = \perp\)
shows \(\text{OclIterate}(S::(\tau::\alpha::\text{bot})\text{Sequence})\)
\((P::(\tau::\alpha::\text{bot})\text{VAL} \Rightarrow (\tau',c::\text{bot})\text{VAL} \Rightarrow (\tau',c::\text{bot})\text{VAL}) \perp = (\perp::(\tau',c::\text{bot})\text{VAL})\)
apply(insert P_undef_2, rule ext, rule sym)
apply(rule iterate_universal_0)
apply(simp_all add: lift0_def OclUndefined_def)
done

lemma OCL_is_defopt_OclIterate:
assumes defopt_P: \(\forall x y. (\tau \models \partial (P x y))\)
and cpP_1: \(\forall y. \text{cp}((\lambda x. P x y))\)
and cpP_2: \(\forall x. \text{cp}(P::(\tau::\alpha::\text{bot})\text{VAL} \Rightarrow (\tau',c::\text{bot})\text{VAL} \Rightarrow (\tau',c::\text{bot})\text{VAL}))\)
shows \(\tau \models \partial (\text{OclIterate}(S::(\tau::\alpha::\text{bot})\text{Sequence}) P A) = ((\tau \models \partial S) \land (\tau \models \partial A))\)
apply(insert defopt_P cpP_1 cpP_2)
apply(rule_tac X=S and \(\tau=\tau\) in Sequence_induct_including, simp_all)
apply(rule trans)
apply(rule_tac x=\((X->\text{including} a \rightarrow \text{iterate}(u;ua=A \mid (P u ua)))\) in cp_subst, simp)
apply(subst iterate_of_including)
apply(simp_all)
apply(subst OCL_is_defopt_OclIncluding)
apply(rule trans, rule sym)
apply(rule_tac x=(P a (OclIterate X P A)) in cp_subst, simp_all)
done

Forward rules to transfer properties about iterate to functions deﬁnable by iterate

For unary functions

lemma f1_by_iterate_cp:
assumes f_by_it: \(\forall S. (f::(\tau::\alpha::\text{bot})\text{Sequence})) =\)
\((\text{OclIterate} S (P::(\tau::\alpha::\text{bot})\text{VAL} \Rightarrow (\tau',c::\text{bot})\text{VAL} \Rightarrow (\tau',c::\text{bot})\text{VAL}) A)\)
and cpF: \(\text{cp} F\)
and cpF': \(\text{cp} F'\)
shows \(\text{cp}((\lambda X. (f ((F X)::(\tau::\alpha::\text{bot})\text{Sequence})))))\)
by(simp add: f_by_it cpF)

lemma f1_by_iterate_undef_1:
\(\forall S. f::(\tau::\alpha::\text{bot})\text{Sequence}) =\)
\((\text{OclIterate} S (P::(\tau::\alpha::\text{bot})\text{VAL} \Rightarrow (\tau',c::\text{bot})\text{VAL} \Rightarrow (\tau',c::\text{bot})\text{VAL}) A)\)
\(\Rightarrow\)
\(\Rightarrow\)
267
Appendix B. Isabelle Theories

\[ f \perp = \perp \]
by simp

**Lemma f1_by_iterate_defopt:**
\[
\text{assumes } f\_\text{by}_\text{it}: \bigwedge S. (f (S:\:\exists\,\tau,\alpha::\text{bot}\text{Sequence})) = (\text{OclIterate } S (P:\:\exists\,\tau,\alpha::\text{bot}) \text{VAL } \Rightarrow (\tau,\alpha::\text{bot}) \text{VAL } \Rightarrow (\tau,\alpha::\text{bot}) \text{VAL } A) \\
\text{and } \text{defopt}\_P: \forall x. (f = \partial (P x y)) \\
\text{and } cpP\_1: \bigwedge x. cp (\lambda x. P x y) \\
\text{and } cpP\_2: \bigwedge x. cp ((P:\:\exists\,\tau,\alpha::\text{bot}) \text{VAL } \Rightarrow (\tau,\alpha::\text{bot}) \text{VAL } \Rightarrow (\tau,\alpha::\text{bot}) \text{VAL } x) \\
\text{shows } (f = \partial(f (S:\:\exists\,\tau,\alpha::\text{bot}\text{Sequence}))) = ((f = \partial S) \land (f = \partial A)) \\
\text{by simp add: } f\_\text{by}_\text{it} \text{ OCL\_is\_defopt}\_\text{OclIterate} \text{ defopt}\_P cpP\_1 cpP\_2
\]

**Lemma f1_by_iterate_mSequence:**
\[
\bigwedge S. f (S:\:\exists\,\tau,\alpha::\text{bot}\text{Sequence}) = (\text{OclIterate } S (P:\:\exists\,\tau,\alpha::\text{bot}) \text{VAL } \Rightarrow (\tau,\alpha::\text{bot}) \text{VAL } \Rightarrow (\tau,\alpha::\text{bot}) \text{VAL } A) \\
\Rightarrow f [[]] = A \\
\text{by simp}
\]

**Lemma f1_by_iterate_including:**
\[
\text{assumes } f\_\text{by}_\text{it}: \bigwedge S. (f (S:\:\exists\,\tau,\alpha::\text{bot}\text{Sequence})) = (\text{OclIterate } S (P:\:\exists\,\tau,\alpha::\text{bot}) \text{VAL } \Rightarrow (\tau,\alpha::\text{bot}) \text{VAL } \Rightarrow (\tau,\alpha::\text{bot}) \text{VAL } A) \\
\text{and } \text{defS}: \tau = \partial(S:\:\exists\,\tau,\alpha::\text{bot})\text{Sequence}) \\
\text{and } \text{defx}: \tau = \partial(x; (\tau = \alpha::\text{bot})) \\
\text{and } cpP\_1: \bigwedge y. cp (\lambda x. P x y) \\
\text{and } cpP\_2: \bigwedge x. cp (P x) \\
\text{shows } (f (\text{OclIncluding } S x) \tau) = (P x (f S) \tau) \\
\text{by simp add: } f\_\text{by}_\text{it} \_\text{iterate\_of\_including} \text{ defS } \text{ defx } cpP\_1 \text{ cpP}\_2
\]

**Lemma f1_by_iterate_opt_including:**
\[
\text{assumes } f\_\text{by}_\text{it}: \bigwedge S. (f (S:\:\exists\,\tau,\alpha::\text{bot}\text{Sequence})) = (\text{OclIterate } S (P:\:\exists\,\tau,\alpha::\text{bot}) \text{VAL } \Rightarrow (\tau,\alpha::\text{bot}) \text{VAL } \Rightarrow (\tau,\alpha::\text{bot}) \text{VAL } A) \\
\text{and } P\_\text{undefined}\_1: \forall x. P \perp = \perp \\
\text{and } P\_\text{undefined}\_2: \forall x. P x \perp = \perp \\
\text{and } \neg cpP\_1: \bigwedge y. \neg cp (\lambda x. P x y) \\
\text{and } \neg cpP\_2: \bigwedge x. \neg cp (P x) \\
\text{shows } f (\text{OclIncluding } S x) = P x (f S) \\
\text{by simp add: } f\_\text{by}_\text{it} \_\text{iterate\_opt\_of\_including} \text{ P\_undefined\_1 P\_undefined\_2 cpP\_1 cpP}\_2
\]

**For binary functions**

This cp-ness result holds only for binary functions whose second argument is the neutral element of iterate. Currently the only function of this style is union.
lemma f2_by_iterate_cp:
assumes f2_by_iterate_st: \( \bigwedge S A. (f (S :: (\tau, \alpha :: \text{bot}) \text{Sequence}) A) \)
and \( \text{cpF} \colon \text{cp F} \)
and \( \text{cpF}^\prime \colon \text{cp F}^\prime \)
shows \( \lambda X. (f ((F \ X) :: (\tau, \alpha :: \text{bot}) \text{Sequence})) (F^\prime \ A)) \)
by(simp add: f2_by_iterate_defopt cpP)

lemma f2_by_iterate_undef_1:
\[ \bigwedge S A. f (S :: (\tau, \alpha :: \text{bot}) \text{Sequence}) A = \]
(\text{OclIterate} S (P :: (\tau, \alpha :: \text{bot}) \text{VAL} \Rightarrow (\tau, c :: \text{bot}) \text{VAL} \Rightarrow (\tau, c :: \text{bot}) \text{VAL}) A)
\[ \text{A} = \bot \]
by(simple)

lemma f2_by_iterate_undef_2:
assumes f2_by_iterate_st: \( \bigwedge S A. (f (S :: (\tau, \alpha :: \text{bot}) \text{Sequence}) A) \)
and \( \text{undef}_2 \colon \text{P} \quad \text{P} \quad x \quad \bot = \bot \)
shows \( f \quad \text{S} \quad \bot = \bot \)
by(simp add: f2_by_iterate_defopt cpP)

lemma f2_by_iterate_defopt:
assumes f2_by_iterate_st: \( \bigwedge S A. (f (S :: (\tau, \alpha :: \text{bot}) \text{Sequence}) A) \)
and \( \text{defopt} \colon \text{P} \quad \exists x. y. (\tau \equiv \partial (P \ x \ y)) \Rightarrow ((\tau \equiv \partial x) \land (\tau \equiv \partial y)) \)
and \( \text{cpP}^0 \colon \text{P} \quad \exists x. cp (\lambda x. P \ x \ y) \quad \text{VAL} \Rightarrow (\tau, c :: \text{bot}) \text{VAL} \Rightarrow (\tau, c :: \text{bot}) \text{VAL} \ x) \)
shows \( \tau \equiv \partial (f (S :: (\tau, \alpha :: \text{bot}) \text{Sequence}) A) = (\tau \equiv \partial (S) \land (\tau \equiv \partial A)) \)
by(simp add: f2_by_iterate_defopt_OclIterate_defopt_P cpP)

lemma f2_by_iterate_mtSequence:
\[ \bigwedge S A. f (S :: (\tau, \alpha :: \text{bot}) \text{Sequence}) A = \]
(\text{OclIterate} S (P :: (\tau, \alpha :: \text{bot}) \text{VAL} \Rightarrow (\tau, c :: \text{bot}) \text{VAL} \Rightarrow (\tau, c :: \text{bot}) \text{VAL}) A)
\[ \Rightarrow \]
\( f \quad \text{A} \quad \text{A} = \)
by(simple)

lemma f2_by_iterate_including:
assumes f2_by_iterate_st: \( \bigwedge S A. (f (S :: (\tau, \alpha :: \text{bot}) \text{Sequence}) A) \)
and \( \text{defS} \colon \tau \equiv \partial (S :: (\tau, \alpha :: \text{bot}) \text{Sequence}) \)
and \( \text{defx} \colon \tau \equiv \partial (x :: (\tau \Rightarrow \alpha :: \text{bot})) \)
and \( \text{cpP}^0 \colon \text{P} \quad \exists x. cp (\lambda x. P \ x \ y) \quad \text{VAL} \Rightarrow (\tau, c :: \text{bot}) \text{VAL} \Rightarrow (\tau, c :: \text{bot}) \text{VAL} \ x) \)
shows \( f (\text{OclIncluding} S \ x) A \ \tau = \ (P \ x \ (f \ S \ A) \ \tau) \)

B.4. Library
Appendix B. Isabelle Theories

by (simp add: f_by_it iterate_of_including defS defx cpP_1 cpP_2)

lemma f2_by_iterate_opt_including:
  assumes f_by_it: \( \forall S \ A. \ f(S::(\tau,\alpha::\text{bot})\text{Sequence}) \ A = \) (OclIterate S (P::(\tau,\alpha::\text{bot})\text{VAL} \Rightarrow (\tau,\text{c::bot})\text{VAL} \Rightarrow (\tau,\text{c::bot})\text{VAL}) \ A)
  and P_undef_1: !\ y. P \bot y = \bot
  and P_undef_2: !\ x. P x \bot = \bot
  and cpP_1: \( \forall y. \ cp (\lambda x. P x y) \)
  and cpP_2: \( \forall x. \ cp (P x) \)
  shows f (OclIncluding S x \ A) = P x (f S A)
  by (simp add: f_by_it iterate_opt_of_including P_undef_1 P_undef_2 cpP_1 cpP_2)

Union

defs

OclUnion_def :
OclUnion \equiv lift2(strictify(\lambda X. strictify(\lambda Y. Abs_Sequence_0 ((\' Rep_Sequence_0 X \oplus \' Rep_Sequence_0 Y))))))

ocl_setup_op [OclUnion]

lemma OCL_is_def_OclUnion:
(\partial(OclUnion (X::(\tau,\alpha::\text{bot})\text{Sequence}) \ Y) = (\partial X \land \partial Y)
apply (rule lift2_strict_is_isdef_fw_Sequence_Sequence [OF OclUnion_def])
apply (simp)
done

lemma OCL_is_defopt_OclUnion:
(\tau \models \partial(OclUnion (X::(\tau,\alpha::\text{bot})\text{Sequence}) \ Y)) = ((\tau \models \partial X) \land (\tau \models \partial Y))
apply (rule lift2_strictify_implies_LocalValid_defined_Sequence_Sequence [OF OclUnion_def])
apply (simp)
done

Its computational characterisation using iterate

lemma union_by_iterate:
((X::(\tau,\alpha::\text{bot})\text{Sequence}) \cup (Y::(\tau,\alpha::\text{bot})\text{Sequence})) =
(Y \rightarrow iterate(x\ y=X \mid y \rightarrow including (x::(\tau,\alpha::\text{bot})\text{VAL})))
apply (rule ext)
apply (rule iterate_universal, simp_all)
apply (rule_tac X=X in Sequence_sem_cases)
apply (simp add: OclUnion_def OclMtsSequence_def ss_lifting)
apply (simp add: OclUnion_def OclMtsSequence_def ss_lifting)
apply (simp_all add: localValidDefined2sem DEF_def)
apply (frule DEF_X_Sequence, clarify)
apply (rule_tac X=X in Sequence_sem_cases, simp_all)
apply (simp_all add: OclUnion_def OclIncluding_def ss_lifting' neq_commute)
B.4. Library

done

thm f2_by_iterate_including[OF union_by_iterate, simplified]

lemmas union_of_mtSequence1 [simp] = f2_by_iterate_mtSequence[OF union_by_iterate]

lemma union_of_mtSequence2 [simp]:
\[ \big[ \bigcup A = (A :: (\tau', \alpha::bot) Sequence) \big] \Rightarrow \text{OclMtSequence def OclUnion def ss_lifting} \]
done

lemmas union_of_including[simp] = f2_by_iterate_opt_including[OF union_by_iterate, simplified]

lemma union_assoc [simp]:
\[ (A \cup (B \cup C)) = ((A \cup B) \cup (C :: (\tau', \alpha::bot) Sequence)) \Rightarrow \text{OclUnion def ss_lifting} \]
done

Properties of iterate over a union of two sequences

lemma iterate_of_union [simp]:
\[ [ \tau \vdash \partial X ] \Rightarrow OclIterate ((X :: (\tau', \alpha::bot) Sequence) \cup Y) \]
\[ \text{OclIterate Y P (OclIterate X P A) } \tau \]
apply(case_tac \[ \tau \vdash \bot \ Y \])
apply(ocl_hypsubst, simp)
apply(simp add: localValidDefined2sem DEF_def)
apply(frule DEF_X_Sequence)
apply(rotate_tac 1, frule DEF_X_Sequence', clarify)
apply(simp add: OclUnion_def OclIterate_def ss_lifting)
done

lemma iterate_of_union_opt [simp]:
\[ [ A \forall x. P x \bot = \bot ] \Rightarrow OclIterate ((X :: (\tau', \alpha::bot) Sequence) \cup Y) \]
\[ (P :: (\tau', \alpha::bot) VAL \Rightarrow (\tau', c::bot) VAL) \Rightarrow (\tau', c::bot) VAL) A \]
\[ \text{OclIterate Y P (OclIterate X P A) } \tau \]
apply(rule ext)
apply(case_tac \[ \tau \vdash \partial X \])
apply(simp add: iterate_of_union)

271
Appendix B. Isabelle Theories

apply(simp add: sym[OF isUndefined_charn_local])
apply(rule_tac A1=X in trans[OF cp_charn], simp_all)
apply(rule_tac A2=X in sym[OF trans[OF cp_charn]], simp_all)
apply(simp)
done

lemma iterate_distrib_union:
  assumes mtC: B. g B A τ = B τ
and stepC: B x y. g B (P x y) τ = P x (g B y) τ
and cp2_g: x. cp (g x)
and cp2_P: x. cp (P x)
and defX: τ ⊩ ∂ X
and defY: τ ⊩ ∂ Y
shows OclIterate ((X::('τ,'α::bot)Sequence) ∪ Y)
  (P::('τ,'α::bot)VAL ⇒ ('τ,'c::bot)VAL ⇒ ('τ,'c::bot)VAL) A τ =
  g (OclIterate X P A (OclIterate Y P A) τ)
by(simp add: iterate_of_union defX defY cp2_g cp2_P mtC stepC)

lemma iterate_distrib_union_opt:
  assumes undefC: B. g B ⊥ = ⊥
and mtC: B. g B A τ = B τ
and stepC: B x y. g B (P x y) τ = P x (g B y) τ
and undef_2_P: x. P x ⊥ = ⊥
and cp2_g: x. cp (g x)
and cp2_P: x. cp (P x)
and defX: τ ⊩ ∂ X
and defY: τ ⊩ ∂ Y
shows f (X ∪ Y) τ = g (f X) (f Y) τ
by(simp add: f_by_it iterate_of_union_opt undef_2_P cp2_g cp2_P)

And the corresponding forward rules for unary functions

lemma f1_by_iterate_distrib_union:
  assumes f_by_it: S. (f (S::('τ,'α::bot)Sequence)) =
    (OclIterate S (P::('τ,'α::bot)VAL ⇒ ('τ,'c::bot)VAL ⇒ ('τ,'c::bot)VAL) A)
and mtC: B. g B A τ = B τ
and stepC: B x y. g B (P x y) τ = P x (g B y) τ
and cp2_g: x. cp (g x)
and cp2_P: x. cp (P x)
and defX: τ ⊩ ∂ X
and defY: τ ⊩ ∂ Y
shows f (X ∪ Y) τ = g (f X) (f Y) τ
by(simp add: f_by_it iterate_of_union defX defY cp2_g cp2_P mtC stepC)

lemma f1_by_iterate_distrib_union_opt:
B.4. Library

assumes \( f \) by it:
\[
\forall S. (\text{OclIterate } S : (\tau, \alpha :: \bot) \text{Sequence}) =
(\text{OclIterate } S : (\tau, \alpha :: \bot) \text{VAL} \Rightarrow (\tau, c :: \bot) \text{VAL} \Rightarrow (\tau, c :: \bot) \text{VAL}) A
\]
and undefC: \( \forall B. g B \bot = \bot \)
and mtC: \( \forall B. g B A = B \)
and stepC: \( \forall B x y. g B (P x y) = P (g B y) \)
and cp2_g: \( \forall x. \text{cp} (g x) \)
and cp2_P: \( \forall x. \text{cp} (P x) \)
shows \( f (X \cup Y) = g (f X) (f Y) \)
by (simp add: f_by_it iterate_distrib_union_opt undef_2_P cp2_g cp2_P undefC mtC stepC)

Append
defs

\text{OclAppend} \equiv \text{lift2} (\text{strictify} (\lambda S. \text{strictify} (\lambda e. \text{Abs_Sequence}_0
(\text{concat} (\text{Rep_Sequence}_0 S, [e])))
\]

ocl_setup_op \[OclAppend]\n
lemma append_including_UC [simp]:
\text{OclAppend} ((\tau, \alpha :: \bot) \text{Sequence}) (x :: (\tau, \alpha) \text{VAL}) = S \rightarrow \text{including} x
by (simp add: OclAppend_def OclIncluding_def)

Prepend
defs

\text{OclPrepend} \equiv \text{lift2} (\text{strictify} (\lambda S. \text{strictify} (\lambda e. \text{Abs_Sequence}_0
(e # \text{Rep_Sequence}_0 S)))
\]

ocl_setup_op \[OclPrepend]\n
lemma prepend_union_UC [simp]:
\text{OclPrepend} ((\tau, \alpha :: \bot) \text{Sequence}) (a :: (\tau, \alpha) \text{VAL}) = ([] \rightarrow \text{including} a) \cup X
apply (rule_tac X=X in Sequence_sem_cases_ext)
apply (simp_all)
apply (simp_all add: OclPrepend_def OclIncluding_def OclUnion_def
OclMtSequence_def ss_lifting neq_commute)
done

lemma test'': \( \text{OclPrepend} ((\tau, \alpha :: \bot) \text{Sequence}) (a :: (\tau, \alpha) \text{VAL}) (a :: (\tau, \alpha) \text{VAL}) \)
= bla
apply (simp) oops
Appendix B. Isabelle Theories

lemma OCL_is_def_OclPrepend:
\[ \partial(OclPrepend (X::('\tau', 'a::bot) Sequence) (Y::('\tau', 'a::bot) VAL)) = (\partial X \land \partial Y) \]
apply (rule lift2_strict_is_isdef_fw_Sequence_Val[OF OclPrepend_def])
apply (simp)
done

lemma OCL_is_defopt_OclPrepend:
\[ (\tau \models \partial(OclPrepend (X::('\tau', 'a::bot) Sequence) (Y::('\tau', 'a::bot) VAL))) = ( (\tau \models \partial X) \land (\tau \models \partial Y)) \]
apply (rule lift2_strictify_implies_LocalValid_defined_Sequence_Val[OF OclPrepend_def])
apply (simp)
done

Some sort of case exhaustion over prepend
lemma prepend_charn1:
\[ [\bot \notin \text{set } xs; xs \neq []] \Rightarrow \exists (S::('\tau', 'a::bot) Sequence_0) a. (Abs_Sequence_0 \langle \langle \rangle \rangle = (OclPrepend (lift0 S) ( (lift0 (a::'a))) \tau)) \]
apply (cases xs, simp_all)
apply (rule_tac x = Abs_Sequence_0 \langle \langle \rangle \rangle in exI)
apply (rule_tac x = lift0 a in exI)
apply (auto simp: OclMtSequence_def OclIncluding_def OclUnion_def ss_lifting')
done

lemma prepend_charn2:
\[ (\bot \notin \text{set } xs; xs \neq []) \Rightarrow \exists (S::('\tau', 'a::bot) Sequence) a. (Abs_Sequence_0 \langle \langle \rangle \rangle = (OclPrepend S (a::('\tau', 'a) VAL)) \tau) \]
apply (cases xs, simp_all)
apply (rule_tac x = lift0 (Abs_Sequence_0 \langle \langle \rangle \rangle) in exI)
apply (rule_tac x = lift0 a in exI)
apply (auto simp: OclMtSequence_def OclIncluding_def OclUnion_def ss_lifting')
done

Reverse induction on sequences: induction over prepend
lemma Sequence_induct_prepend_0:
assumes undefCase : P \bot
and mtCase : P (\bot \sigma)
and stepCase : \exists (S::('\tau', 'a::bot) Sequence_0) (x::'\tau::bot).
\[ P S; DEF S; DEF x \Rightarrow (P ((OclPrepend (lift0 S) (lift0 (x::'\tau))) \sigma)) \]
shows P (S::('\tau', 'a::bot) Sequence_0)
apply (rule Abs_Sequence_0_induct_charn, rule undefCase)
apply (erule rev_mp)
apply (induct_tac y)
apply (insert mtCase, simp add: OclMtSequence_def lift0_def)
apply (auto)
apply (rotate_tac -1, drule_tac x = a and S = Abs_Sequence_0 (list) in stepCase)
apply (erule DEF_Abs_Sequence)
apply (simp_all add: OclPrepend_def DEF_def neq_commute lift0_def lift2_def strictify_def)
done

lemma Sequence_induct_prepend:
assumes undefCase : P ⊥ τ
and mtCase : P [] τ
and stepCase : (\forall S :: (\tau :: τ,\alpha :: bot) Sequence. \forall x :: (\tau :: τ,\alpha :: bot) VAL. P S τ; \ tau \ tau \ tau \ x \ (\tau :: (\tau,\alpha) VAL)) τ
and cpP : cp P
shows (OclIterate (OclPrepend (x :: (\tau :: \tau,\alpha :: bot) VAL)) P A) τ = (OclIterate (S :: ((\tau,\alpha) VAL)) P (P x A)) τ
apply (insert cpP, simp)
apply (subst iterate_of_union)
apply (simp add: OCL_is_defopt_OclIncluding)
apply (erule_tac x = (OclIterate [] -> including x P A) in cp_charn)
done

iterate on prepend

iterate_of_prepend:
assumes defS : τ \ \tau (S :: (\tau :: (\tau,\alpha :: bot)) Sequence)
and defx : x :: (\tau :: (\tau \ ⇒ \ \alpha :: bot))
and cpP_1 : (\forall y :: (\tau :: \tau,\alpha :: bot). cp (\lambda x. P x y))
and cpP_2 : (\forall x :: \tau. cp P)
shows ((OclIterate (OclPrepend S (x :: (\tau,\alpha) VAL)) P A) τ) = ((OclIterate (S :: ((\tau,\alpha) bot) Sequence)) P (P x A)) τ
apply (insert defS defx cpP_1 cpP_2, simp)
apply (subst iterate_of_union)
apply (simp add: OCL_is_defopt_OclIncluding)
apply (rule_tac A = (OclIterate [] -> including x P A) in cp_charn)
done
Appendix B. Isabelle Theories

\text{OclIncludes\_def : } OclIncludes \equiv \text{lift2}\ (\text{strictify}\ (\lambda x. \ \text{strictify}\ (\lambda x. x \in \text{set} \ Rep\_Sequence\_0 X^1)))

\text{OclExcludes\_def : } OclExcludes \equiv \text{lift2}\ (\text{strictify}\ (\lambda X. \ \text{strictify}\ (\lambda x. x \notin \text{set} \ Rep\_Sequence\_0 X^1)))

\text{ocl\_setup\_op [OclIncludes, OclExcludes]}

\text{lemma includes\_ch1 :}
\text{(}\tau \models x \in S) \implies ((x \tau) \in \text{set} \ Rep\_Sequence\_0 (S \tau))
\text{apply (case_tac (S \tau) \neq \bot)}
\text{apply (case_tac (x \tau) \neq \bot)}
\text{apply (auto simp: OclIncludes\_def localValid2sem ss\_lifting) }
\text{done}

\text{lemma includes\_ch2 :}
\text{[ DEF (S \tau); (x \tau) \in \text{set} \ Rep\_Sequence\_0 (S \tau) ] \implies \tau \models x \in S}
\text{apply (unfold DEF\_def, frule DEF\_X\_Sequence')} 
\text{apply (auto simp: OclIncludes\_def localValid2sem ss\_lifting) }
\text{done}

\text{Higher Properties of includes and excludes}

\text{lemma excludes\_not\_includes [simp]:}
\text{x \notin X = \neg (x :: (\tau, 'a::bot) VAL) \in (X :: (\tau, 'a::bot) Sequence)}
\text{apply (rule ext)}
\text{apply (simp add: OclExcludes\_def OclIncludes\_def OclNot\_def ss\_lifting')} 
\text{done}

Currently a non-strict body is taken although a strict one is possible. This should be corrected as the experience has shown that strict functions are much nicer to work with.

\text{lemma includes\_by\_iterate:}
\text{a \in (X :: (\tau, 'a::bot) Sequence) =}
\text{OclIterate X (\lambda x. x :: (\tau, 'a::bot) VAL) y. (x \leadsto a) \lor y)
\text{(if (\partial a) then F else \bot endif)}}
\text{apply (rule ext)}
\text{apply (rule iterate\_universal, simp\_all)}
\text{apply (simp add: OclIncludes\_def OclMtSequence\_def OclFalse\_def
OclIf\_def OclIsDefined\_def OclUndefined\_def
ss\_lifting')} 
\text{apply (simp add: localValidDefined2sem DEF\_def)
apply (rule DEF\_X\_Sequence', clarify)
apply (auto simp: OclIncludes\_def OclIncluding\_def OclTrue\_def
OclSor\_def OclNot\_def OclSand\_def OclStrictEq\_def)

276
B.4. Library

ss_lifting' neq_commute)
done

lemmas includes_mtSequence[simp] = f1_by_iterate_mtSequence[OF includes_by_iterate]

thm f1_by_iterate_opt_including[OF includes_by_iterate, simplified]

lemma excludes_by_iterate:
a \notin (X::('τ, 'α::bot)Sequence) = 
OclIterate X (λ(x::('τ, 'α::bot)VAL. (x ' < >' a) \land y) 
(if (⊥ a) then T else ⊥ end)
apply(rule ext, simp add: includes_by_iterate)
apply(rule iterate_fusion, simp_all)
apply(simp_all add: OclNot_def OclTrue_def OclFalse_def OclIf_def OclSand_def OclSor_def OclUndefined_def ss_lifting' neq_commute)
done

containment in the empty list can be reduced to definedness

lemma includes_of_mtSequence[simp]:
\neg (τ \models ((x::('τ, 'α)VAL) ⊆ ([]):('τ, 'α::bot)Sequence))
by(simp add: OclIncludes_def OclMtSequence_def OclNot_def 
localValid2sem ss_lifting')

lemma includes_charn1_including[simp]:
\schema{\tau \models (a::('τ, 'α)VAL); \tau \models (X::('τ, 'α::bot)Sequence) \implies \tau \models a \in (X->including a)}
apply(simp only: localValidDefined2sem DEF_def)
apply(rule DEF_X_Sequence', clarify)
apply(simp add: localValid2sem OclIncludes_def OclIncluding_def 
ss_lifting' neq_commute)
done

lemma includes_charn2_including[simp]:
\schema{\tau \models (a::('τ, 'α)VAL); \tau \models (b::('τ, 'α)VAL); \tau \models a \in (X::('τ, 'α::bot)Sequence) \implies \tau \models a \in (X->including b)}
apply(case_tac X \tau \neq \bot)
apply(rule DEF_X_Sequence', clarify)
apply(simp_all only: localValidDefined2sem DEF_def)
apply(simp_all add: localValid2sem OclIncludes_def OclIncluding_def 
ss_lifting' neq_commute)
apply(drule neq_commute[THEN iffD1], simp)
done

lemma includes_of_collectionRange:
(x::('τ Integer)) \in ((OclCollectionRange a b)::('τ, Integer_0)Sequence) = 
((a::('τ Integer)) \leq x) \land (x \leq (b::('τ Integer)))
apply(rule ext)
apply (case_tac DEF (x xa), case_tac DEF (a xa), case_tac DEF (b xa))
apply (simp add: DEF_def_both, clarify)
apply (subgoal_tac ⊥ ∈ set (map (λz. ((int z) + ⌈(a xa)⌉)) [0..<nat (⌈(b xa)⌉ − ⌈(a xa)⌉) + 1]))
apply (auto simp add: DEF_def_both, arith)
apply (rule_tac x = nat (⌈(x xa)⌉ − ⌈(a xa)⌉) in image_eqI, auto)
done

lemma includes_of_union [simp]:
[ τ ⊨ ∅, τ ⊨ ∅ ] ⇒
(∀x. (∀y. ((∀z. ((∀w. (w ⊨ (x xa) ∧ w ⊨ (a xa)))) ∧ y) ⇒ (a xa) ⊨ X)) ⇒
(∀z. ((∀w. (w ⊨ (x xa) ∧ w ⊨ (a xa)))) ∧ y) ⇒ (a xa) ⊨ X)
apply (simp add: localValidDefined2sem DEF_def)
apply (frule DEF_X_Sequence)
apply (rotate_tac 1, frule DEF_X_Sequence, clarify)
apply (simp add: OclIncludes_def OclUnion_def OclOr_def OclAnd_def OclNot_def ss_lifting)
done

lemma test’’': τ ⊨ (1::'τ Integer) ∈ (mkSequence[1::'τ Integer]):('τ, Integer_0)Sequence
oops

lemma not_includes_of_mtSequence:
(τ ⊨ ¬ (x::('τ, 'α::bot) VAL) ∈ ([]::('τ, 'α::bot)Sequence)) = (τ ⊨ ∅)
by (simp add: localValidNot2sem localValidDefined2sem OclIncludes_def
OclMtSequence_def ss_lifting)

lemma mtSequence_Includes_of_OLD :
τ ⊨ ∅ ⇒
τ ⊨ (x::('τ, 'α::bot) VAL) ∉ ([]::('τ, 'α::bot)Sequence)
by (simp, ocl_subst, simp)

Note: this will be subsumed by OCL_is_defopt_OclIncludes if ocl_setup_op is
working correctly on collection types

Emptiness
defs

OclIsEmpty_def :
OclIsEmpty ≡ lift1 (strictify (λX. ((Rep_Sequence_0 X = []))))
B.4. Library

\[ \text{OclNotEmpty_def} : \]
\[ \text{OclNotEmpty} \equiv \text{lift1 (strictify (λX. ⌞(\text{Rep\_Sequence}_0 X) \neq [])}) \]

ocl_setup_op [OclIsEmpty, OclNotEmpty]

The normal form for emptiness testing:

we prefer a canonical form were notEmpty is written using isEmpty

\[ \text{lemma notEmpty_not_isEmpty_conv[simp]} : \]
\[ \not\emptyset (X::('τ, 'α::bot) Sequence) = \neg (\emptyset X) \]
\[ \text{apply(simp add: OclNotEmpty_def OclIsEmpty_def OclNot_def ss\_lifting')} \]
\[ \text{done} \]

further on the emptiness test is reduced to an equality to a constant

\[ \text{lemma isEmpty_stricteq_mtSequence_conv[simp]} : \]
\[ (\emptyset X) = (\emptyset (X::('τ, 'α::bot) Sequence)) \]
\[ \text{apply(rule_tac X x \not\emptyset in Sequence_sem_cases_ext)} \]
\[ \text{apply(simp_all add: OclIsEmpty_def OclMtSequence_def OclStrictEq_def Abs\_Sequence_0_inject_charn ss\_lifting')} \]
\[ \text{done} \]

Properties of emptiness:

\[ \text{lemma isEmpty_of_mSequence[simp]} : \]
\[ \vdash \emptyset [] \] by simp

\[ \text{lemma isEmpty_of_including[simp]} : \]
\[ [\vdash \emptyset (a::('τ,'α::bot) VAL); \vdash \emptyset (X::('τ, 'α::bot) Sequence)] \rightarrow [\vdash \emptyset (\emptyset (X->including a))] \] by simp

\[ \text{lemma isEmpty_union[simp]} : \]
\[ ((X::('τ, 'α::bot) Sequence) \cup Y) \equiv [] = (X \equiv []) \wedge (Y \equiv []) \] apply(rule_tac X=X in Sequence_sem_cases_ext)
\[ \text{apply(rule_tac X=Y in Sequence_sem_cases, simp_all)} \]
\[ \text{apply(simp_all add: OclUnion_def OclStrictEq_def OclMtSequence_def OclSand_def ss\_lifting\' Abs\_Sequence_0_inject\_charn)} \]
\[ \text{done} \]

\[ \text{lemma notEmpty_of_mSequence[simp]} : \]
\[ \vdash \neg (\emptyset []) \] by simp

279
Appendix B. Isabelle Theories

**lemma** notEmpty_of_including:

\[
\{ \tau \models \partial (a:('\tau,\alpha::bot)VAL) ; \tau \models \partial (X:('\tau,\alpha::bot)Sequence) \} \implies \\
\{ \tau \neq \emptyset (X\rightarrow including a) \}
\]

by(simp)

**Size**

defs

\[
OclSize_def : OclSize \equiv lift1 (strictify (\lambda X. \\
\text{int (Nat.size 'Rep.Sequence_0 X')})
\]

ocl_setup_op [OclSize]

**lemma** size_by_iterate:

\[
((self:('\tau,\alpha::bot)Sequence) \rightarrow size()) = \\
OclIterate self (\lambda (x:('\tau,\alpha::bot)VAL) (y:'\tau Integer). y + 1) \emptyset
\]

apply(rule ext)

apply(rule iterate_universal)

apply(simp_all)

apply(simp_all add: OclSize_def OclIterate_def plus_def OclMtSequence_def

  OclUndefined_def OclIncluding_def localValidDefined2sem

  OCL_Integer.ZERO_ocl_int_def OCL_Integer.ONE_ocl_int_def

  ss_lifting)

apply(frule DEF_X_Sequence')

apply(auto simp: neq_commute)

done

lemmas size_of_mtSequence[simp] = f1_by_iterate_mtSequence[OF size_by_iterate]

**lemma** size_of_including[simp]:

\[
\{ \tau \models \partial (x:('\tau,\alpha::bot)VAL) \} \implies \\
(((S:('\tau,\alpha::bot)Sequence) \rightarrow including x) ) \tau = (\|S\| + 1) \tau
\]

apply(case_tac \tau \neq \emptyset S)

apply(ocl_hypsubst, simp)

apply(simp add: f1_by_iterate_including[OF size_by_iterate, simplified])

done

**lemma** size_eq_zero_isEmpty_UC[simp]:

\[
(\|S:('\tau,\alpha::bot)Sequence\| \equiv 0) = (S \equiv [])
\]

apply(rule ext)

apply(case_tac \ S \ x \neq \bot)

apply(frule DEF_X_Sequence', clarify)

apply(simp_all add: OclSize_def OclStrictEq_def OclMtSequence_def

280
B.4. Library

\[ OCL\_Integer\_Zero\_ocl\_int\_def\ \text{Abs\_Sequence\_0\_inject\_charn} \]
\[ \text{localValid2sem\ ss\_lifting'} \]
\[ \text{done} \]

**Lemma** \( \text{size\_of\_union\ UC} \) [simp];
\[(\| (X::\{\tau,\alpha ::'bot\} Sequence) \cup Y)\|) = (\| X \| + \| Y \|)\]
\[\text{apply(rule f1\_by\_iterate\_distrib\_union\_opt[OF size\_by\_iterate, of op +, simplified])}\]
\[\text{apply(rule ext, simp add: plus\_def \text{Zero\_ocl\_int\_def} ss\_lifting')}\]
\[\text{apply(rule ext, simp add: plus\_def \text{One\_ocl\_int\_def} ss\_lifting')}\]
\[\text{done}\]

**Induction over two lists**

**Lemma** \( \text{Sequence\_induct2\_including\_0} \)
\[\text{assumes undefCase: } P \perp \perp \tau\]
\[\text{and equalsize: } \| (lift0 X) \| \tau = \| (lift0 Y) \| \tau\]
\[\text{and mtcase: } P (\| X \|) (\| Y \|)\]
\[\text{and stepcase: } \forall (X::\{\tau,\alpha ::'bot\} \text{Sequence}) (a::\{\tau,\alpha ::'bot\} \text{VAL}) (Y::\{\tau,\alpha ::'bot\} \text{Sequence}) (b::\{\tau,\alpha ::'bot\} \text{VAL}).\]
\[\text{shows } P (\| X \|) (\| Y \|) = \Rightarrow (P (\| (\text{OclIncluding} (lift0 X) (lift0 a)) \| \tau) (\| (\text{OclIncluding} (lift0 Y) (lift0 b)) \| \tau))\]
\[\text{apply(insert equalsize, erule rev\_mp)}\]
\[\text{apply(rule Abs\_Sequence\_0\_induct\_charn)}\]
\[\text{apply(erule rev\_mp)}\]
\[\text{apply(rule_tac x=X in Abs\_Sequence\_0\_induct\_charn)}\]
\[\text{apply(simp add: OclSize\_def ss\_lifting')}\]
\[\text{done}\]

**Lemma** \( \text{Sequence\_induct2\_including} \)
\[\text{assumes equalsize: } \tau \vdash \| X \| \triangleq \| Y \|\]
\[\text{and undefcase: } P \perp \perp \tau\]
\[\text{and mtcase: } P (\| \tau \|)\]
\[\text{and stepcase: } \forall (X::\{\tau,\alpha ::'bot\} \text{Sequence}) (a::\{\tau,\alpha ::'bot\} \text{VAL}) (Y::\{\tau,\alpha ::'bot\} \text{Sequence}) (b::\{\tau,\alpha ::'bot\} \text{VAL}).\]
\[281\]
Appendix B. Isabelle Theories

\[ P 
\begin{array}{llll}
X & Y & \tau & \vdash \partial \; X; \; \tau & \vdash \partial \; a; \; \tau & \vdash \partial \; Y; \; \tau & \vdash \partial \; b
\end{array}
\] \implies
\[ P \; (OclIncluding \; X \; a) \; (OclIncluding \; Y \; b) \; \tau \]

and
\[ cp_1 \; P \; \land \; \forall \; y. \; cp \; (\lambda \; x. \; P \; x \; y) \]

and
\[ cp_2 \; P \; \land \; \forall \; x. \; cp \; (P \; x) \]

shows
\[ P \; (X; \; (\tau, \alpha::bot).\text{Sequence}) \; (Y; \; (\tau, \alpha::bot).\text{Sequence}) \; \tau \]

apply (insert \( cp_1 \; P \; \land \; cp_2 \; P \), simp add: \( \text{cp_by_cpify} \))

apply (insert \( cp_1 \; P \; \land \; cp_2 \; P \))

apply (rule subst, rule sym, rule subst \( \tau \) \( \in \) \( cp_{\text{subst}} \), simp)

apply (rule subst, rule sym, rule subst \( \tau \) \( \in \) \( cp_{\text{subst}} \), simp)

apply (rule subst \( \tau \) \( \in \) \( \text{Sequence\_induct2\_including\_0} \), simp add: \( \text{lift0_def} \))

oops

Count
defs

\[ OclCount_{\text{def}} : OclCount \equiv \text{lift2} \; (\text{strictify} \; (\lambda \; X. \; \text{strictify} \; (\lambda \; x. \; (\text{int} \; (\text{Nat}_{\text{size}} \; \text{List}_{\text{filter}} \; (\text{op} = x) \; \text{Rep\_Sequence\_0} \; X)))) \]

ocl_setup_op \[ [OclCount] \]

Its computational characterisation by iterate
lemma count_by_iterate:
\[ ((S; \; (\tau, \alpha::bot)\text{Sequence}) \; \Rightarrow \text{count} ((a; \; (\tau, \alpha)\text{VAL}))) = \]
\[ (OclIterate \; S \; (\lambda \; (x; \; (\tau, \alpha::bot)\text{VAL}) \; (y; \; \tau) \; \text{Integer}). \text{if} \; (x \; = \; a) \; \text{then} \; (y \; + \; 1) \; \text{else} \; (y) \; \text{endif}) \]

apply (rule ext)

apply (rule OclIterate_universal)

apply (simp_all)

apply (simp_all add: OclMtSequence_def OclCount_def
\[ \text{OCL}\_\text{Integer} \_\text{Zero}_{\text{oocl\_int}} \_\text{int} \_\text{def} \_\text{OCL}\_\text{Integer} \_\text{One}_{\text{oocl\_int}} \_\text{def} \_\text{OclIf}_{\text{def}} \_\text{OclIsDefined}_{\text{def}} \_\text{OclUndefined}_{\text{def}} \_\text{OclStrictEq}_{\text{def}} \_\text{OclIncluding}_{\text{def}} \_\text{OclLocalValid}_{\text{def}} \_\text{plus}_{\text{def}} \_\text{OclTrue}_{\text{def}} \_\text{ss\_lifting}])

apply (frule DEF_X_Seq)

apply (auto simp: neg\_commute)

done

thm f1_by_iterate_including[OF count_by_iterate, simplified]

lemma count_of_mtSequence [simp]:
\[ \tau \; \vdash \; (\partial \; (x; \; (\tau, \alpha)\text{VAL})) \; \Rightarrow \]
\[ (([])\; (\tau, \alpha::bot)\text{Sequence}) \; \Rightarrow \text{count} \; x \; \tau \; = \; 0 \; \tau \]

by (simp add: count_by_iterate, ocl_subst, simp)

thm f1_by_iterate_including[OF count_by_iterate, simplified]

thm f1_by_iterate_opt_including[OF count_by_iterate, simplified]

282
thm f1_by_iterate_distrib_union[OF count_by_iterate, of op +, simplified]
thm f1_by_iterate_distrib_union_opt[OF count_by_iterate, of op +, simplified]

lemma plus_assoc1: \( (X::('\tau \text{Integer})) + Y) + Z = X + (Y + Z) \)
  by (rule ext, simp add: plus_def ss_lifting)

lemma plus_assoc2: \( (X::('\tau \text{Integer})) + (Y + Z) = Y + (X + Z) \)
  by (rule ext, simp add: plus_def ss_lifting)

lemmas plus_AC = plus_commute plus_assoc1 plus_assoc2

lemma plus_zero': simp]: \( (X::('\tau \text{Integer})) + 0 = X \land 0 + (X::('\tau \text{Integer})) = X \)
  by (rule conjI, (rule ext, simp add: plus_def ss_lifting' Zero_ocl_int_def)+)

lemma count_of_union [simp]:
  \( ((X::('\tau\alpha::\text{bot})Sequence) \cup Y) \rightarrow count (a::('\tau\alpha)VAL)) = ((X \rightarrow count a) + (Y \rightarrow count a)) \)
  apply (rule ext, case_tac x \\# a, ocl_hypsubst, simp)
  apply (case_tac x \\# X, ocl_hypsubst, simp)
  apply (case_tac x \\# Y, ocl_hypsubst, simp)
  apply (simp add: count_by_iterate)
  apply (ocl_subst)
  apply (simp add: iterate_distrib_union plus_AC if_distrib_strict_alt)
  done

lemma includes_by_count_UC[simp]:
  \( S \rightarrow count x > 0 = (x::('\tau\alpha::\text{bot})VAL) \in (S::('\tau\alpha::\text{bot})Sequence) \)
  apply (rule Sequence_sem_cases_ext, simp_all)
  apply (auto simp: OclIncludes_def OclCount_def OclGreater_def filter_empty_conv
         OclLess_def OclNot_def Zero_ocl_int_def ss_lifting')
  done

lemma excludes_by_count_UC[simp]:
  \( S \rightarrow count x \# 0 = \neg (x::('\tau\alpha::\text{bot})VAL) \in (S::('\tau\alpha::\text{bot})Sequence) \)
  apply (rule Sequence_sem_cases_ext, simp_all)
  apply (auto simp: OclIncludes_def OclCount_def OclStrictEq_def OclNot_def
         Zero_ocl_int_def ss_lifting' filter_empty_conv)
  done

Subsequence
constdefs
Appendix B. Isabelle Theories

\[ \text{OclSubSequence} :: [ ('\tau', '\alpha::bot) Sequence, '\tau Integer, '\tau Integer] = > ('\tau, '\alpha ) Sequence \]

\[ \text{OclSubSequence} \equiv \text{lift3} (\text{strictify} (\lambda S. \text{strictify} (\lambda l. \text{Abs\_Sequence\_0} \\
(\text{take} (\text{nat} ('u' - 'T' + 1))) \\
(\text{List.drop} (\text{nat} ('T' - 1))) \\
(\text{OclRep\_Sequence\_0} S)))))) \]

\[ \text{ocl\_setup\_op [OclSubSequence]} \]

Because the ocl\_setup\_op method doesn’t deal with \text{lift3} we have to setup the simple properties by ourselves.

\textbf{lemma OCL\_undef\_1\_OclSubsequence[simp]:}
\[ \text{OclSubSequence} ('\bot::('\tau, '\alpha::bot) Sequence) a b = '\bot \]
\[ \text{by (simp add: OclUndefined_def OclSubSequence_def ss\_lifting')} \]

\textbf{lemma OCL\_undef\_2\_OclSubsequence[simp]:}
\[ \text{OclSubSequence} (S::('\tau, '\alpha::bot) Sequence) '\bot b = '\bot \]
\[ \text{by (rule ext, simp add: OclUndefined_def OclSubSequence_def ss\_lifting')} \]

\textbf{lemma OCL\_undef\_3\_OclSubsequence[simp]:}
\[ \text{OclSubSequence} (S::('\tau, '\alpha::bot) Sequence) a '\bot = '\bot \]
\[ \text{by (rule ext, simp add: OclUndefined_def OclSubSequence_def ss\_lifting')} \]

\textbf{lemma OCL\_cp\_OclSubsequence[simp, intro!]:}
\[ [ \text{cp P; cp F; cp F}' ] \Longrightarrow \]
\[ \text{cp (\lambda X. OclSubSequence ((P X)::('\tau, '\alpha::bot) Sequence) (F X) (F}' X)) \]
\[ \text{by (simp add: OclSubSequence\_def)} \]

\textbf{Higher properties of subsequence}

Note: subsequence is in our case not undefined except for undefined arguments. To avoid undefinedness is quite favorable in general as it makes proofs simpler and reduces the side conditions to check. But our implementation still fulfills the requirements of the standard.

\textbf{lemma size\_of\_subsequence:}
\[ [ \tau = 'i \leq a; \tau = 'i \leq b - 'i; \tau = b \leq \|S\| ] \Longrightarrow \]
\[ \|\text{OclSubSequence} (S::('\tau, '\alpha::bot) Sequence) a b\| \tau = (b - a + 1) \tau \]
\[ \text{apply (rule_tac X=S in Sequence\_sem\_cases)} \]
\[ \text{apply (simp\_all add: localValid2sem)} \]
\[ \text{apply (case_tac b \tau \neq 'i, frule neq\_commute[THEN iffD1])} \]
\[ \text{apply (case_tac a \tau \neq 'i, rotate_tac -'i, frule neq\_commute[THEN iffD1])} \]
\[ \text{apply (auto simp: OclIncluding\_def OclSubSequence\_def OclSize\_def \}
One\_ocl\_int\_def plus\_def minus\_def ss\_lifting\]
\[ \text{Ocl\_def OclLess\_defnotin\_set\_takenotin\_set\_drop)} \]
\[ \text{apply (arith, case_tac ((b \tau) = down), simp\_all)} \]
\[ \text{done} \]
lemma subsequence_mtSequence_conv:
\[
\llbracket \tau \models \emptyset \wedge S := b < a \rrbracket \Rightarrow \\
(OclSubSequence (S::(\tau,\alpha::bot)Sequence) a b) \tau = [] \tau
\]
apply(rule_tac X=S in Sequence_sem_cases)
apply(simp_all add: localValidDefined2sem DEF_def)
apply(case_tac b \tau \neq \bot, frule neq_commute[THEN iffD1])
apply(case_tac a \tau \neq \bot, rotate_tac -1, frule neq_commute[THEN iffD1])
apply(auto simp: OclIncluding_def OclSubSequence_def OclMtSequence_def localValid2sem OclLess_def notin_set_take notin_set_drop ss_lifting)
done

Lemma OclInsertAt_def:

OclInsertAt def :
OclInsertAt \equiv lift3(strictify(\lambda S. strictify(\lambda i. strictify(\lambda x. Abs_Sequence_0(\frac{i \leq i}{i} \wedge \frac{i}{i} < (1+\text{int}(\text{Nat.size} Rep_Sequence_0 S)))) if (i \leq i \wedge i < (1+\text{int}(\text{Nat.size} Rep_Sequence_0 S)))) then concat [take (nat (op - i 1)) ("Rep_Sequence_0 S") [x], \
List.drop (nat (op - i 1)) ("Rep_Sequence_0 S")]) else \bot)))

ocl_setup_op [OclInsertAt]

Because the ocl_setup_op method doesn’t deal with lift3 we have to setup the simple properties by ourselves.

lemma OCL cp OclInsertAt[simp,intro!]:
\[
\llbracket cp P; cp F; cp F' \rrbracket \Rightarrow \\
cpy (\lambda X. OclInsertAt ((P X)::(\tau,\alpha::bot)Sequence) (F X) ((F' X)::(\tau,\alpha)VAL))
by(simp add: OclInsertAt_def)

lemma OCL undef_1_OclInsertAt[simp]:
OclInsertAt (\lambda::(\tau,\alpha::bot)Sequence) i (x::(\tau,\alpha)VAL) = \bot
by(simp add: OclUndefined_def OclInsertAt_def ss_lifting)

lemma OCL undef_2_OclInsertAt[simp]:
OclInsertAt (S::(\tau,\alpha::bot)Sequence) \bot (x::(\tau,\alpha)VAL) = \bot
by(rule ext, simp add: OclUndefined_def OclInsertAt_def ss_lifting)

lemma OCL undef_3_OclInsertAt[simp]:
OclInsertAt (S::(\tau,\alpha::bot)Sequence) \bot (\bot::(\tau,\alpha)VAL) = \bot
by(rule ext, simp add: OclUndefined_def OclInsertAt_def ss_lifting)

Higher properties of insertAt

lemma includes_of_insertAt:
\[
\llbracket \tau \models \emptyset (S::(\tau,\alpha::bot)Sequence) \Rightarrow \\
\llbracket \tau \models \emptyset (x::(\tau,\alpha)VAL) \rrbracket
\]

285
Appendix B. Isabelle Theories

\[ \tau \models I \leq i; \tau \models i \leq (|S| + 1) \implies \]
\[ \tau \models x \in \text{OclInsertAt} S i x \]
\[ \text{apply}(\text{rule_tac} X=S \text{ in Sequence_sem_cases}) \]
\[ \text{apply}(\text{simp_all add: localValidDefined2sem DEF_def}) \]
\[ \text{apply}(\text{case_tac} i \tau \neq \bot, \text{frule neq_commute}[THEN iffD1]) \]
\[ \text{apply}(\text{case_tac} x \tau \neq \bot, \text{rotate_tac} -1, \text{frule neq_commute}[THEN iffD1]) \]
\[ \text{apply}(\text{auto simp: OclInsertAt_def OclIncludes_def OclLe_def OclSize_def plus_def One_ocl_int_def ss_lifting}) \]
\[ \text{done} \]

\begin{itemize}
\item \textbf{lemma size_of_insertAt:}
\[ \tau \models \partial((OclAt \ S \ S) : \{\tau, \alpha :: \text{bot}\}) \]
\[ \tau \models I \leq i; \tau \models i \leq (|S| + 1) \implies \]
\[ \|\text{OclInsertAt} S i x\|\tau = (\|S::(\tau, \alpha)\text{Sequence}\| + 1) \tau \]
\[ \text{apply}(\text{rule_tac} X=S \text{ in Sequence_sem_cases}) \]
\[ \text{apply}(\text{simp_all add: localValidDefined2sem DEF_def}) \]
\[ \text{apply}(\text{case_tac} i \tau \neq \bot, \text{frule neq_commute}[THEN iffD1]) \]
\[ \text{apply}(\text{case_tac} x \tau \neq \bot, \text{rotate_tac} -1, \text{frule neq_commute}[THEN iffD1]) \]
\[ \text{apply}(\text{auto simp: OclInsertAt_def OclIncludes_def OclLe_def OclSize_def plus_def One_ocl_int_def ss_lifting}) \]
\[ \text{done} \]
\end{itemize}

at

defs

\begin{itemize}
\item \textbf{OclAt_def :}
\[ \text{OclAt} \equiv \text{lift2}(\text{strictify}(\lambda X. \text{strictify}(\lambda x. \text{if } \ceil{x} <\ 0 \lor \\text{int}(\text{Nat.size}'\text{Rep_Sequence}_0 X) < \ceil{x} \\\text{then} \bot \\\text{else } \text{Rep_Sequence}_0 X! \text{nat}(\ceil{x} - 1)))) \]
\end{itemize}

\begin{itemize}
\item \textbf{ocl_setup_op [OclAt]}
\end{itemize}

\begin{itemize}
\item \textbf{lemma at_lower_bound:}
\[ \tau \models i < 1 \implies \text{OclAt} (S::(\tau, \alpha :: \text{bot})\text{Sequence}) i \tau = (\bot::(\tau, \alpha)\text{VAL}) \tau \]
\[ \text{by}(\text{auto simp: localValid2sem OclLess_def OclAt_def OclLe_def OclInt_def One_ocl_int_def OclUndefined_def ss_lifting'}) \]
\end{itemize}

\begin{itemize}
\item \textbf{lemma at_upper_bound:}
\[ \tau \models |S| < i \implies \text{OclAt} (S::(\tau, \alpha :: \text{bot})\text{Sequence}) i \tau = (\bot::(\tau, \alpha)\text{VAL}) \tau \]
\[ \text{by}(\text{auto simp: localValid2sem OclLess_def OclAt_def OclLe_def OclInt_def OclSize_def OclUndefined_def ss_lifting'}) \]
\end{itemize}

\begin{itemize}
\item \textbf{lemma OCL_is_defopt_OclAt:}
\[ \tau \models I \leq i; \tau \models i \leq |S| \implies \]
\[ \tau \models \partial((\text{OclAt} (S::(\tau, \alpha :: \text{bot})\text{Sequence}) i)::(\tau, \alpha)\text{VAL}) = (\tau \equiv \partial S) \]
\end{itemize}

286
apply (case_tac i τ = ⊥)
apply (simp add: localValid2sem OclLe_def One_ocl_int_def ss_lifting)
apply (rule_tac X = S in Sequence_sem_cases, simp_all add: localValid2sem)
apply (auto simp: OclIsDefined_def OclAt_def OclLe_def One_ocl_int_def OclSize_def ss_lifting)
apply (simp add: in_set_conv_nth)
apply (erule_tac x = nat (⌜(i τ)⌝ − 1) in allE, arith)

done

lemma at_of_mtSequence[simp]:
OclAt (⊥ :: (′τ, ′α :: bot) Sequence) i = (⊥ :: (′τ, ′α) VAL)
by (rule ext, auto simp: OclAt_def OclMtSequence_def OclUndefined_def ss_lifting)

lemma at_last_of_including:
[ τ |= i = (∥S∥ + l) ] ===> OclAt (S :: (′τ, ′α :: bot) Sequence) ∼ including x i τ = (x :: (′τ, ′α) VAL) τ
apply (case_tac i τ = ⊥)
apply (simp add: localValid2sem OclStrictEq_def ss_lifting)
apply (case_tac τ ⊨ x ∉ ∂ x)
apply (ocl_hypsubst, simp)
apply (rule_tac X = S in Sequence_sem_cases)
apply (simp_all add: localValidDefined2sem DEF_def)
apply (frule neq_commute [THEN iffD1])
apply (rotate_tac 2, frule neq_commute [THEN iffD1])
apply (auto simp: OclAt_def OclIncluding_def OclSize_def localValid2sem OclStrictEq_def plus_def One_ocl_int_def ss_lifting)
apply (simp add: nth_append, arith)

done

lemma at_inside_of_including:
[ τ |= i ≠ i ≤ ∥S∥ ] ===> OclAt (S ∼ including (x :: (′τ, ′α :: bot) Sequence) i τ = (OclAt (S :: (′τ, ′α :: bot) Sequence) i τ))::′α)
apply (case_tac i τ = ⊥)
apply (simp add: localValid2sem OclLe_def ss_lifting)
apply (rule_tac X = S in Sequence_sem_cases)
apply (simp_all add: localValidDefined2sem DEF_def)
apply (frule neq_commute [THEN iffD1])
apply (auto simp: OclAt_def OclIncluding_def OclSize_def localValid2sem OclLe_def plus_def One_ocl_int_def ss_lifting)

done

lemma at_of_union1:
[ τ |= ∅ ⊆ S, τ |= i ≤ ∥S∥ ] ===>
Appendix B. Isabelle Theories

\texttt{OclAt (S1 U S2) i \tau =}
\texttt{((OclAt (S1::('\tau,\alpha::bot)Sequence) i \tau)::\alpha)}
\texttt{apply(rule_tac X=S1 in Sequence_sem_cases)}
\texttt{apply(rule_tac X=S2 in Sequence_sem_cases)}
\texttt{apply(simp_all add: localValidDefined2sem DEF_def)}
\texttt{apply(auto simp: OclAt_def OclUnion_def OclSize_def localValid2sem}
\texttt{ OclLe_def plus_def ss_lifting)}
\texttt{apply(simp add: nth_append, arith)}
\texttt{done}

\texttt{lemma at_of_union2:}
\texttt{[ \tau \models \|S1\| < i; \tau \models i \leq (\|S1\|+\|S2\|) ] \implies}
\texttt{OclAt (S1 U S2) i \tau =}
\texttt{((OclAt (S2::('\tau,\alpha::bot)Sequence) (i-\|S1\|) \tau)::\alpha)}
\texttt{apply(rule_tac X=S1 in Sequence_sem_cases)}
\texttt{apply(rule_tac X=S2 in Sequence_sem_cases)}
\texttt{apply(simp_all add: localValidDefined2sem DEF_def)}
\texttt{apply(auto simp: OclAt_def OclUnion_def OclSize_def minus_def localValid2sem}
\texttt{ OclLe_def OclLess_def plus_def ss_lifting)}
\texttt{apply(auto simp: nth_append, arith)}
\texttt{apply(subgoal_tac ((\text{nat} ((i \tau) \text{)} - 1)) - (\text{length c})) = (\text{nat} ((\text{nat} i \text{)} - (\text{int} (\text{length c)))) - 1))}
\texttt{apply(simp, arith)}
\texttt{done}

\texttt{lemma at_first_of_prepend:}
\texttt{[ \tau \models \partial S ] \implies}
\texttt{OclAt (OclPrepend (S::('\tau,\alpha::bot)Sequence) x) 1 \tau = (x::('\tau,\alpha) VAL) \tau}
\texttt{apply(case_tac \tau \models \emptyset x)}
\texttt{apply(ocl_hypsubst, simp)}
\texttt{apply(rule_tac X=S in Sequence_sem_cases)}
\texttt{apply(simp_all add: localValidDefined2sem DEF_def)}
\texttt{apply(rule neg_commute[THEN iffD1])}
\texttt{apply(auto simp: OclAt_def OclIncluding_def OclUnion_def OclSize_def localValid2sem}
\texttt{ OclMtSequence_def One_ocl_int_def ss_lifting)}
\texttt{done}

\texttt{lemma at_inside_of_prepend:}
\texttt{[ \tau \models \partial x; \tau \models 1 < i ] \implies}
\texttt{OclAt (OclPrepend (S::('\tau,\alpha::bot)Sequence) (x::('\tau,\alpha) VAL) (i-1) \tau =}
\texttt{((OclAt S (i - 1) \tau)::\alpha)}
\texttt{apply(case_tac \tau \models \emptyset S)}
\texttt{apply(ocl_hypsubst, simp_all)}
\texttt{apply(case_tac \tau \models \emptyset i)}
\texttt{apply(ocl_hypsubst, simp_all)}
\texttt{apply(rule_tac X=S in Sequence_sem_cases)}

288
B.4. Library

apply(simp_all add: localValidDefined2sem DEF_def)
apply(frule neq_commute[THEN iffD1])
apply(rotate_tac 2, frule neq_commute[THEN iffD1])
apply(case_tac τ ⊢ \|S\| + I < i)
apply(auto simp: OclAt_def OclIncluding_def OclUnion_def OclSize_def localValid2sem
OclMtSequence_def OclLess_def minus_def plus_def
One_ocl_int_def ss_lifting')
apply(subgoal_tac ((x τ) ≠ c) = ([x τ] @ c))
apply(simp only: nth_append)
apply(subgoal_tac ((\nat (\tau (i τ)) - I) - (Suc 0)) = (\nat (-2 + \tau (i τ))))
apply(auto, arith, arith)
done

lemma at_of_subsequence:
  \[ τ \vDash I \leq a; \tau \vDash a < b; \tau \vDash b \leq \|S\|; \tau \vDash I \leq i; \tau \vDash i \leq (a - b + I) \]\implies
OclAt (OclSubSequence (S::(\tau::\alpha::bot)Sequence) a b) i τ =
((OclAt S (a + i - 1) \tau)::\alpha)
apply(rule_tac X=S in Sequence_sem_cases)
apply(simp_all add: localValid2sem)
apply(case_tac τ ≠ ⊥, frule neq_commute[THEN iffD1])
apply(case_tac a ≠ ⊥, rotate_tac -l, frule neq_commute[THEN iffD1])
apply(case_tac b τ ≠ ⊥, rotate_tac -l, frule neq_commute[THEN iffD1])
apply(simp_all add: OclIncluding_def OclAt_def OclSubSequence_def
OclMtSequence_def OclLess_def minus_def plus_def
One_ocl_int_def plus_def minus_def ss_lifting'
OclLe_def OclLess_def notin_set_take notin_set_drop)
done

lemma at_of_insertAt_before:
  \[ τ \vDash \emptyset (x::(\tau::\alpha) VAL); τ \vDash i \leq (\|S\| + I); τ \vDash j < i \]\implies
OclAt (OclInsertAt (S::(\tau::\alpha::bot)Sequence) i x) j τ = ((OclAt S j τ)::\alpha)
apply(case_tac τ \vDash \emptyset S, ocl_hypsubst, simp)
apply(case_tac τ \vDash \emptyset i, ocl_hypsubst, simp)
apply(case_tac τ \vDash \emptyset j, ocl_hypsubst, simp)
apply(simp add: localValidDefined2sem DEF_def_both)
apply(clarify, frule DEF_X_Sequence', clarify)
apply(case_tac (I \leq \tau j))
apply(subgoal_tac ((\nat (\tau j) - I) < (length c)))
apply(auto simp: OclInsertAt_def OclAt_def OclLess_def OclSize_def plus_def
One_ocl_int_def ss_lifting' localValid2sem
OclMtSequence_def OclLe_def notin_set_take notin_set_drop nth_append)
apply(arith, arith)
done

lemma at_of_insertAt:
  \[ τ \vDash I \leq i; τ \vDash i \leq (\|S\| + I) \]\implies
OclAt (OclInsertAt (S::(\tau::\alpha::bot)Sequence) i (x::(\tau::\alpha) VAL)) i τ = x τ

289
Appendix B. Isabelle Theories

apply(case_tac τ = ∅ S)
apply(ocl_hypsubst, simp)
apply(rule_tac X=S in Sequence_sem_cases)
apply(simp_all add: localValidDefined2sem DEF_def)
apply(case_tac i τ ≠ ⊥, frule neq_commute[OF THEN iffD1])
apply(case_tac x τ ≠ ⊥, rotate_tac 1, frule neq_commute[OF THEN iffD1])
apply(auto simp: OclInsertAt_def OclAt_def OclLe_def OclSize_def plus_def
One_ocl_int_def ss_lifting' localValid2sem
notin_set_take notin_set_drop, arith)
apply(subgoal_tac (nat (⌜(i τ)⌝ − j)) = length (take (nat (⌜(i τ)⌝ − l) c))
rule_tac t = (nat (⌜(i τ)⌝ − l)) in subst back)
apply(rule syn, assumption, rule nth_append_length)
apply(simp, arith)
done

lemma at_of_insertAt_after:
[ τ = ∅ (x::τ α) VAL; τ ⊢ I ≤ i; τ ⊢ i ≤ (||S|| + l); τ ⊢ i < j ] =⇒
OclAt (OclInsertAt (S::(τ α::bot)Sequence) i x) j τ = ((OclAt S (j - l) τ)::'α)
apply(case_tac τ = ∅ S, ocl_hypsubst, simp)
apply(case_tac τ = ∅ i, ocl_hypsubst, simp)
apply(case_tac τ = ∅ j, ocl_hypsubst, simp)
apply(simp add: localValidDefined2sem DEF_def_both)
apply(clarify, frule OclX_Sequence', clarify)
apply(subgoal_tac (min (length c) (nat (⌜(i τ)⌝ − l))) = nat (⌜(i τ)⌝ − l))
apply(case_tac (((int (length c)) + l) < (⌜(j τ)⌝)))
apply(auto simp: OclInsertAt_def OclAt_def OclLess_def OclSize_def plus_def
One_ocl_int_def ss_lifting' localValid2sem minus_def
OclLe_def notin_set_take notin_set_drop nth_append)
apply(thin_tac ?P ≠ ?Q | thin_tac ?P = ?Q)+ apply(arith)
apply(thin_tac ?P ≠ ?Q | thin_tac ?P = ?Q)+ apply(arith)
apply(subgoal_tac (nat (⌜(j τ)⌝ − l)) − (nat (⌜(i τ)⌝ − l)) = Suc ((nat (⌜(j τ)⌝ − 2)) − (nat (⌜(i τ)⌝ − l))))
apply(simp)
apply(subst nth_drop)
apply(thin_tac ?P = ?Q, arith)
apply(subgoal_tac (nat (⌜(i τ)⌝ − l)) + ((nat (⌜(j τ)⌝ − 2)) − (nat (⌜(i τ)⌝ − l)))) =
(nat (−2 + (⌜(j τ)⌝)))
apply(simp)
apply(rotate_tac 2, thin_tac ?P, thin_tac ?P, arith)
apply(rotate_tac 2, thin_tac ?P, thin_tac ?P, arith)
done

IndexOf

defs

290
OclIndexOf_def:
OclIndexOf ≡ lift2(strictify(λX. strictify(λx. if x ∈ set Rep_Sequence_0 X then init(length (takeWhile (λ y. y ≠ x) Rep_Sequence_0 X)) + i) else ⊥))

ocl_setup_op [OclIndexOf]

lemma indexOf_excludes[simp]:
[| τ ⊨ ¬ ((x::(τ,α) VAL) ∈ (S::(τ,α::bot)Sequence)) |] ==⇒
OclIndexOf S x τ = ⊥
apply(rule_tac X=S in Sequence_sem_cases, simp_all)
apply(case_tac x τ = ⊥)
apply(simp_all add: OclIndexOf_def OclIncludes_def OclNot_def o_def
OclUndefined_def ss_lifting localValid2sem)
done

lemma notin_conv_all_noteq: a /∈ S = (∀ x ∈ S. x ≠ a)
by (auto)

lemma in_set_conv_first_decomp:
(x ∈ set xs) = (∃ ys zs. xs = ys @ x # zs ∧ x /∈ set ys)
apply(auto, erule rev_mp)
apply(rule length_induct, auto)
apply(rule in_set_conv_decomp[THEN iffD1], clarify)
apply(case_tac x ∈ set ys)
apply(erule_tac x=ys in allE, auto)
apply(rule_tac x=ysa in exI, simp)
done

In the standard self->at(i) = obj is written where it should be written like self->at(result) = obj. Furthermore the standard doesn’t specify that the returned index is the index of the first object that is equal to the searched one. This disables the combined use of indexOf and subsequence to visit all occurrences of a specific object.

lemma at_indexOf:
[| τ ⊨ (x::(τ,α) VAL) ∈ (S::(τ,α::bot)Sequence) |] ==⇒
OclAt S (OclIndexOf S x) τ = x τ
apply(rule_tac X=S in Sequence_sem_cases, simp_all)
apply(case_tac x τ ≠ ⊥)
apply(frule neq_commute[THEN iffD1])
apply(simp_all add: OclIndexOf_def OclIncludes_def OclNot_def OclAt_def
OclUndefined_def ss_lifting localValid2sem o_def)
apply(frule in_set_conv_first_decomp[THEN iffD1])
apply(clarify, simp add: notin_conv_all_noteq takeWhile_tail)
done
Appendix B. Isabelle Theories

First and Last
defs

OclFirst_def :  
OclFirst ≡ lift1 (strictify (λS. if ⌜Rep_Sequence_0 S⌝ = [] then ⊥ else hd (⌜Rep_Sequence_0 S⌝)))

OclLast_def :  
OclLast ≡ lift1 (strictify (λS. if ⌜Rep_Sequence_0 S⌝ = [] then ⊥ else List.last (⌜Rep_Sequence_0 S⌝)))

ocl_setup_op [OclFirst, OclLast]

lemma first_at_UC:  
OclFirst (S :: ′τ, ″α::bot″ Sequence) = ((OclAt S 1)::′τ, ″α::bot″ VAL)
apply(rule Sequence_sem_cases_ext, simp_all)
apply(auto simp: OclAt_def Zero_ocl_int_def One_ocl_int_def ss_lifting ″neq_Nil_conv″)
done

lemma first_of_mtSequence[simp]:  
OclFirst ([::′τ, ″α::bot″ Sequence]) = (⊥::′τ, ″α″ VAL)
by(simp add: first_at_UC)

lemma first_empty_of_including:  
[ τ ⊨ (S = [])] ⊢ OclFirst ((S::′τ, ″α::bot″ Sequence) =⇒ including (x::′τ, ″α″ VAL)) τ = ((x τ)::′α)
apply(rule_tac X=S in Sequence_sem_cases)
apply(simp_all add: localValidDefined2sem)
apply(case_tac c)
apply(auto simp: OclIncluding_def OclFirst_def OclNot_def OclStrictEq_def OclMtSequence_def ss_lifting ″neq_commute″)
done

Note: strange writing because of normal form of emptiness test

lemma first_not_empty_of_including:  
[ τ ⊨ ∅ x τ ⊨ ¬ (S = [])] ⊢ OclFirst ((S::′τ, ″α::bot″ Sequence) =⇒ including (x::′τ, ″α″ VAL)) τ = ((OclFirst S τ)::′α)
apply(rule_tac X=S in Sequence_sem_cases)
apply(simp_all add: localValidDefined2sem DEF_def)
apply(case_tac c)
apply(auto simp: OclIncluding_def OclFirst_def OclNot_def OclStrictEq_def OclMtSequence_def ss_lifting ″neq_commute″ localValid2sem)
done

292
lemma last_at_UC:
OclLast (S::('τ,'α::bot)Sequence) = ((OclAt S \parallel S)::('τ,'α)VAL)
apply(rule Sequence_sem_cases_ext, simp_all)
apply(auto simp: OclLast_def OclAt_def OclSize_def
Zero_ocl_int_def One_ocl_int_def
ss_lifting' last_conv_nth neq_Nil_conv)
done

lemma last_of_mtSequence[simp]:
OclLast ([]:('τ,'α::bot)Sequence) = (⊥::('τ,'α)VAL)
by(simp add: last_at_UC)

lemma last_empty_of_including:
[ τ ⊨ ∅ S ] ⇒
OclLast ([S::('τ,'α::bot)Sequence]→including (x:(('τ,'α)VAL)) τ =
((x τ)::'α)
apply(rule_tac X=S in Sequence_sem_cases)
apply(simp_all add: localValidDefined2sem DEF_def)
apply(simp add: OclIncluding_def OclLast_def
ss_lifting' neq_commute)
done

Forall
defs

OclForAll_def: OclForAll ≡ (λτ. (lift2' lift_arg0 lift_arg1)
(strictify( λS. (λP. if ∀ x ∈ set⇧(Rep_Sequence_0 S). P x = True
then True
else if ∃ x ∈ set⇧(Rep_Sequence_0 S). P x = False
then False
else False)))

ocl_setup_op [OclForAll]

Its computation characterisation by iterate
lemma forall_by_iterate:
(∀ x ∈ (S::('τ,'α::bot)Sequence). (P::('τ,'α::bot)VAL ⇒ 'τ Boolean) x) =
(S→iterate(x;y= T | (P x) ∧ y))
apply(rule ext)
apply(rule iterate_universal_0, simp_all)
apply(simp add: cp_by_cpify OclForAll_def lift0_def)
apply(simp_all add: OclForAll_def OclUndefined_def OclMtSequence_def)
Appendix B. Isabelle Theories

\textit{OclTrue_def} \textit{localValidDefined2sem} \textit{ss_lifting')}
\textbf{apply}(frule \textit{DEF_X_Sequence'}, clarify)
\textbf{apply}(frule \textit{neg_commute[THEN iffD1]})
\textbf{apply}(rotate_tac 1, frule \textit{neg_commute[THEN iffD1]})
\textbf{apply}(simp_all add: \textit{OclIncluding_def OclAnd_def ss_lifting'})
done

Derived properties from the relation to iterate
\textbf{lemma} \textit{OCL_undef_2_OclForAll}[simp]:
[\llbracket \tau \models \neg ((S::(\tau, 'alpha::bot)Sequence) = []) \rrbracket ] \implies
(\forall x \in S \cdot (\lambda x:(\tau, 'alpha)VAL. \bot) x) = \bot \tau
\textbf{apply}(rule_tac X = S in Sequence_sem_cases, simp_all)
\textbf{apply}(simp_all add: \textit{OclForAll_def OclUndefined_def OclMtSequence_def}
\textit{OclStrictEq_def OclNot_def localValid2sem}
o_def Abs_Sequence_0_inject_charn)
done

\textbf{lemmas} \textit{forall_of_mtSequence}[simp] = \textit{f1_by_iterate_mtSequence}[OF \textit{forall_by_iterate}]

\textbf{lemma} \textit{forall_including}[simp]:
[\llbracket \tau \models \partial (X::(\tau, 'alpha::bot)Sequence); \tau \models \partial Y \rrbracket ] \implies
(\forall x \in (X \cup Y) \cdot P (x:(\tau, 'alpha)VAL)) \tau = ((\forall x \in X \cdot P x) \land (\forall x \in Y \cdot P x)) \tau
\textbf{by}(simp add: \textit{forall_by_iterate} \textit{iterate_of_including})

\textbf{thm} \textit{f1_by_iterate_distrib_union}[OF \textit{forall_by_iterate}, of \textit{OclAnd}, simplified]

\textbf{lemma} \textit{forall_union}[simp]:
[\llbracket \tau \models \partial (X::(\tau, 'alpha::bot)Sequence); \tau \models \partial Y \rrbracket ] \implies
(\forall x \in (X \cup Y) \cdot P (x:(\tau, 'alpha)VAL)) \tau = ((\forall x \in X \cdot P x) \land (\forall x \in Y \cdot P x)) \tau
\textbf{apply}(simp add: \textit{forall_by_iterate})
\textbf{apply}(rule \textit{iterate_distrib_union})
\textbf{apply}(simp_all add: \textit{OCL_logic_ACI})
done

Introduction rules for \textit{ForAll}
\textbf{lemma} \textit{ForAll}:
\textbf{assumes} \textit{defS}: \tau \models \partial(S::(\tau, 'alpha::bot)Sequence)
\textbf{and} \textit{allP}: \forall x. \tau \models x \in S \implies \tau \models P x
\textbf{shows} \tau \models (\forall x \in S \cdot P(x::'alpha))
\textbf{apply}(insert \textit{defS})
\textbf{apply}(rule_tac X = S in Sequence_sem_cases)
\textbf{apply}(simp_all add: \textit{localValidDefined2sem DEFF_def})
\textbf{apply}(subgoal_tac (\forall x \in set c. P (\lambda x. x) = (\textit{True})))
\textbf{apply}(auto simp: \textit{OclForAll_def localValid2sem ss_lifting'})

294
B.4. Library

apply (rule_tac \(\tau_1 = \tau\) in localValid2sem \(\text{THEN iffD1}\), rule allP)
apply (auto simp: localValid2sem OclIncludes_def ss_lifting)
done

lemma notForAllI:
  assumes isin : \(\tau \models x \in (S::\langle\tau, (\alpha::bot)\rangle)\)Sequence
  and not : \(\tau \not\models \neg (P x)\)
  and cpP : cp P
  shows \(\tau \not\models \neg (\forall x \in S \cdot P(x; \tau \Rightarrow (\alpha::bot)))\)
apply (insert isin not cpP)
apply (rule_tac X in Sequence_sem_cases)
apply (simp_all add: localValidDefined2sem DEF_def)
apply (case_tac \(\neg (P x)\), frule neq_commute)
apply (case_tac x, rotate_tac -1, frule neq_commute)
apply (subgoal_tac \(\exists x \in (\set c). (P (\lambda s. x) \tau) = \langle False \rangle))
apply (simp_all add: OclForAll_def OclIncludes_def OclNot_def ss_lifting)
apply (rule_tac x = x \(\tau\) in bexI)
apply (rule_tac x = P \(\lambda \tau a. x\) \(\tau\) in boolean_cases_sem)
apply (rule_tac x = x \(\tau\) in bexI)
apply (rule_tac x = P \(\lambda \tau a. x\) \(\tau\) in boolean_cases_sem)
apply (rule_tac trans, rule_tac \(\tau = \tau\) in cp_subst)
apply (rule_tac \(\tau = \tau\) in simP add: lift0_def)
done

lemma undefForAllI2:
  assumes exUndef1: \(\tau \models x \in (S::\langle\tau, (\alpha::bot)\rangle)\)Sequence
  and exUndef2: \(\tau \not\models \emptyset (P x)\)
  and allP : \(\forall x. \tau \models x \in S \Rightarrow \tau \models (P x) \vee \emptyset (P x)\)
  and cpP : cp P
  shows \(\tau \not\models \emptyset (\forall x \in S \cdot P(x; \tau \Rightarrow (\alpha::bot)))\)
apply (insert exUndef1 exUndef2)
apply (frule isDefined_if_valid)
apply (drule OCL_is_defopt_OclIncludes \(\text{THEN iffD1}\))
apply (simp add: OclLocalValid_def OclIsDefined_def OclTrue_def OclForAll_def OclNot_def OclIncludes_def ss_lifting)
apply (erule conjE)
apply (frule DEF_X_Sequence', clarify)
apply (simp, safe)
apply (rule_tac \(\tau = \tau\) in bexI, simp_all) prefer 2
apply (rule_tac \(\tau = \tau\) in bexI, simp_all)
apply (subgoal_tac \(P (\lambda a. x) \tau = P x \tau\), simp)
apply (rule_tac \(\tau = \tau\) and \(P = P\) in cp_charn, simp add: cpP, rule cpP)

295
Appendix B. Isabelle Theories

apply(erule_tac Q = P (λτ. xa) τ = (False in contrapos_pp)
apply(rule_tac τ1 = τ in localValidToNotFalse2sem [THEN iffD1]) back
apply(rule allP)
apply(simp add: includes_charn2 DEF_def)
done

lemma isdefForAll2:
assumes exNot1: τ ⊨ x ∈ (S::(′τ,(′α::bot))Sequence)
and exNot2: τ ⊨ ¬ (P x)
and cpP : cp P
shows τ ⊨ δ(∀ x ∈ S. P(x::′τ ⇒ ′α::bot))
apply(insert exNot1 exNot2 cpP)
apply(drule_tac P=P in notForAllI, simp_all add: isDefined_if_invalid)
done

lemmas isdefForAll3 = ForAllI[THEN isDefined_if_valid]

Exists

Alternative definition for the use with ocl_setup_op

lemma OclExists_alt_def:
OclExists ≡ (lift2 ′lift_arg0 lift_arg1) (strictify (λ S. (λ P.
  if ∃ x ∈ set Rep_Sequence_0 S. P x = True
  then True
  else if ∀ x ∈ set Rep_Sequence_0 S. P x = False
  then False
  else ⊥))
apply(rule eq_reflection, (rule ext)+)
apply(simp add: OclExists_def forall_by_iterate
apply(auto)
oops

The relation to iterate

lemma exists_by_iterate:
(∃ x ∈ (source::′τ,(′α::bot))Sequence) • (P::′(′τ,(′α::bot))VAL ⇒ ′τ Boolean) x ) =
(source ->iterate(x; y= F | (P x) ∨ y))
apply(simp add: OclExists_def forall_by_iterate)
apply(rule ext, rule iterate_fusion_0, simp_all)
apply(simp add: OclNot_def OclOr_def OclAnd_def DEF_def
lift0_def lift1_def lift2_def strictify_def)
done

Derived properties from the relation to iterate

lemma OCL cp OclExists [simp, intro!]:
[ ∀ x. cp (P x); cp S ]
B.4. Library

\[ \Rightarrow cp(\lambda X. \exists Y \in ((S X)::(\tau,\alpha::bot)\text{Sequence}) \cdot P (Y::(\tau,\alpha)\text{VAL}) X) \]

by (simp add: exists_by_iterate)

lemmas exists_undef [simp] = f1_by_iterate_UNDEF_1[OF exists_by_iterate]
lemmas exists_empty [simp] = f1_by_iterate_mtSequence[OF exists_by_iterate, simplified]
thm f1_by_iterate_including[OF exists_by_iterate, simplified]
thm f1_by_iterate_opt_including[OF exists_by_iterate, simplified]

thm f1_by_iterate_UNDEF_1[OF exists_by_iterate]
thm f1_by_iterate_mtSequence[OF exists_by_iterate]
thm f1_by_iterate_including[OF exists_by_iterate, simplified]
thm f1_by_iterate_opt_including[OF exists_by_iterate, simplified]

Introduction rules for exist

lemma ExistsI:
assumes isin : \( \tau \models \exists x \in (S::(\tau,(\alpha::bot)\text{Sequence}) \cdot P x) \)
and not : \( \tau \not\models (P x) \)
and cpP : cp P
shows \( \tau \models (\exists x \in S/s\text{uaresmallsolid}P (x::\tau \Rightarrow \alpha::bot)) \)
by (auto simp: OclExists_def intro: notForAllI isin not cpP)

lemma NotExistsI:
assumes defS : \( \tau \not\models \emptyset(S::(\tau,(\alpha::bot)\text{Sequence}) \cdot P x) \)
and allP : \( \forall x. \tau \models x \in S \Rightarrow \tau \not\models \neg P x \)
shows \( \tau \models \neg (\exists x \in S \cdot P(x::\tau \Rightarrow \alpha::bot)) \)
by (auto simp: OclExists_def intro: ForAllI defS allP)

IncludesAll

defs

\[ OclIncludesAll \equiv \text{tfl2 } (\text{strictify } (\lambda X. \text{strictify } (\lambda Y. \text{set } \text{Rep_Sequence}_0 Y \subseteq \text{set } \text{Rep_Sequence}_0 X)) ) \]

ocl_setup_op [OclIncludesAll]

Its computational characterisation by iterate

This formulation should be replaced by one with a strict body to simplify reasoning
over it.

lemma includesAll_by_iterate:
OclIncludesAll X (Y::(\tau,\alpha::bot)\text{Sequence}) =
(Y \to iterate \( x y = \begin{cases} \text{if } (\emptyset X) \text{ then } Y \text{ else } \bot \end{cases} \mid ((x::(\tau,\alpha)\text{VAL}) \in X) \land y))
apply (rule ext)
Appendix B. Isabelle Theories

apply (rule iterate_universal_0 simp_all)
apply (simp add: OclIncludesAll_def OclMtSequence_def OclIsDefined_def
OclIf_def OclTrue_def OclUndefined_def ss_lifting)
apply (rule DEF_X_Sequencedefined2sem DEF_def)
apply (rule rotate_tac 1, frule neq_commute[THEN iffD1])
apply (simp add: localValidDefined2sem DEF_def)
apply (subst f1_by_iterate_distrib_union [OF includesAll_by_iterate])
apply (simp_all)
apply (ocl_subst simp)
apply (auto simp: OclIncludesAll_def OclSand_def OclIncludes_def
OclTrue_def localValidDefined2sem ss_lifting)
done

thm f1_by_iterate_undef_1 [OF includesAll_by_iterate]
lemmas includesAll_empty [simp] = f1_by_iterate_mtSequence [OF includesAll_by_iterate]
lemmas includesAll_including [simp] = f1_by_iterate_opt_including [OF includesAll_by_iterate, simplified]

thm includesAll_empty includesAll_including

lemma includesAll_union [simp]:
(\OclIncludesAll Z \((X::('\tau, 'a::bot)Sequence) \cup Y)\) =
(\OclIncludesAll Z X \land (\OclIncludesAll Z Y)
apply (rule ext)
apply (case_tac x \notin X, ocl_hypsubst, simp)
apply (case_tac x \notin Y, ocl_hypsubst, simp)
apply (case_tac x \notin Z, ocl_hypsubst, simp)
apply (subst f1_by_iterate_distrib_union [OF includesAll_by_iterate])
apply (simp_all)
apply (ocl_subst simp)
apply (auto simp: OclIncludesAll_def OclSand_def OclIncludes_def
OclTrue_def localValidDefined2sem ss_lifting)
done

lemma includesAll_by_forall:
[ \tau \equiv \partial (X::('\tau, 'a::bot)Sequence) ] \implies
(\OclIncludesAll X Y \tau = (\forall a \in Y \cdot ((a::('\tau, 'a)VAL) \in X)) \tau
apply (rule_tac X=X in Sequence_sem_cases)
apply (rule_tac X=Y in Sequence_sem_cases)
apply (simp_all add: localValidDefined2sem DEF_def)
apply (auto simp: OCL_Sequencedefined2sem OclStrongEq_def
OCL_Sequencedefined2sem OclIncludes_def ss_lifting' localValid2sem)
done

ExcludesAll
defs

OclExcludesAll_def:
OclExcludesAll \equiv \lift2 (\mapsto (\lambda X. \mapsto (\lambda Y. 298


B.4. Library

\[ \text{set } \{ \text{Rep\_Sequence\_0 } X \} \cap \text{set } \{ \text{Rep\_Sequence\_0 } Y \} = \{ \} \]
Appendix B. Isabelle Theories

\[ \text{OclExcludesAll X Y} \ \tau = (\forall a \in Y. ((a :: (\tau, \alpha) \text{VAL}) \notin X)) \ \tau \]

apply (rule_tac X=X in Sequence_sem_cases)
apply (rule_tac X=Y in Sequence_sem_cases)
apply (simp_all add: localValidDefined2sem DEF_def)
apply (auto simp: OCL_Sequence.OclForAll_def OCL_Sequence.OclExcludesAll_def OclStrongEq_def)

done

Select

defs

\[ \text{OclSelect_def: OclSelect} \equiv \text{(lift2' lift_arg0 lift_arg1)} \ (\text{strictify} \ (\lambda S P. \text{Abs_Sequence_0 (\text{List_filter} (\lambda x. P x = True)}) \ (\text{Rep_Sequence_0 S}))) \]

ocl_setup_op [OclSelect]

Its computational characterisation by iterate

lemma select_by_iterate:
\[(\forall x. (source :: (\tau, \alpha :: \text{bot}) \text{Sequence}) | (P :: (\tau, \alpha :: \text{bot}) \text{VAL} \Rightarrow \tau \text{ Boolean}) x)) = (source \rightarrow \text{iterate} \ (\text{iterator}; \text{result} = [] \ |
\text{if} (P \text{ iterator}) \text{then} (\text{OclIncluding result iterator}) \text{ else} \text{ (result) endif}))\]

apply (rule ext, rule iterate_universal_0, simp_all)
apply (simp add: OclSelect_def cp_by_cpify lift0_def)
apply (simp_all add: OclUndefined_def OclMtSequence_def OclSelect_def localValidDefined2sem ss_lifting)
apply (frule DEF_X_Sequence', clarify)
apply (frule neq_commute[THEN iffD1])
apply (rotate_tac 1, frule neq_commute[THEN iffD1])
apply (rule_tac x=P in boolean_cases_sem)
apply (simp_all add: OclIf_def OclIncluding_def ss_lifting')
done

Properties derived from the correspondence to iterate

lemmas select_of_mtSequence [simp] = f1_by_iterate_mtSequence[OF select_by_iterate]

lemma select_including [simp]:
\[ [\tau = \emptyset (x :: (\tau, \alpha :: \text{bot}) \text{VAL}); \text{cp} \ P] \Rightarrow \text{OclSelect} (S :: (\tau, \alpha) \text{Sequence} \rightarrow \text{including} \ x) \text{ P} \tau = (if (P x) \text{ then} (\text{OclSelect S P} \rightarrow \text{including} \ x \text{ else} (\text{OclSelect S P}) \text{ endif}) \tau)\]

apply (case_tac \tau = \emptyset S, ocl_hypsubst, simp)
apply (simp add: f1_by_iterate_including[OF select_by_iterate, simplified])
done

lemma select_including_strict [simp]:
B.4. Library

\[ P \bot = \bot; cp P \] \implies
\begin{align*}
OclSelect ((x:(\tau,\alpha::bot)\text{Val}))\ P \tau =

\begin{cases}
\mbox{if (P x) then (OclSelect S P) }\rightarrow\mbox{including x else (OclSelect S P)endif} & \tau
\end{cases}
\end{align*}

by(simp add: f1_by_iterate_opt_including[OF select_by_iterate, simplified])

\textbf{lemma} select\_union [simp]:
\begin{align*}
(OclSelect ((X:(\tau,\alpha::bot)\text{sequence}) \cup Y))\ (P:(\tau,\alpha)\text{Val} \Rightarrow \tau \text{Boolean}) =
\end{align*}
\begin{align*}
(OclSelect X P) \cup (OclSelect Y P)
\end{align*}

apply(subst f1_by_iterate_distrib_union_opt[OF select_by_iterate])

apply(simp_all)

apply(rule_tac X=B in Sequence_sem_cases_ext, simp_all)

apply(rule_tac X=y in Sequence_sem_cases, simp_all)

apply(case_tac x \tau \neq \bot, drule neq_commute[THEN ssD1])

apply(simp_all add: OclIf_def OclUnion_def OclIncluding_def ss_lifting')

\textbf{done}

\textbf{lemma} iterate\_of\_select:
assumes undef_1_Q \land y. Q \bot y = \bot

and undef_2_Q \land x. Q x \bot = \bot

and cp1_Q \land \alpha. cp (\lambda x. Q x y)

and cp2_Q \land x. cp (Q x)

and undef_1_P. P \bot = \bot

and cp_P. cp P

shows OclIterate (OclSelect (S:(\tau,\alpha::bot)\text{sequence}) P) \ Q A =
\begin{align*}
\mbox{OclIterate S } (\lambda x:(\tau,\alpha)\text{Val} \ y. \mbox{if (P x) then Q x y else y endif}) A
\end{align*}

apply(insert cp1_Q cp2_Q cp_P undef_1_P undef_2_Q undef_1_Q)

apply(rule ext)

apply(rule iterate_universal, simp_all add: select_by_iterate)

apply(subst iterate_opt_of_including, simp_all)

apply(rule_tac P=\lambda t. t x = ?Q in subst)

apply(rule sym[OF if_distrib_strict_all])

apply(simp_all add: iterate_opt_of_including)

\textbf{done}

\textbf{lemma} select\_of\_select:
assumes undef_1_P. P \bot = \bot

and undef_1_Q. Q \bot = \bot

and cp_P. cp P

and cp_Q. cp Q

shows OclSelect (OclSelect (S:(\tau,\alpha::bot)\text{sequence}) (P:(\tau,\alpha)\text{Val} \Rightarrow \tau \text{Boolean})) (Q:(\tau,\alpha)\text{Val} \Rightarrow \tau \text{Boolean}) =
\begin{align*}
\mbox{OclSelect S } (\lambda x. (P x) \land ((P x) \rightarrow (Q x)))
\end{align*}

by(simp add: select_by_iterate_iterate_of_select[simplified select_by_iterate]

undef_1_Q undef_1_P cp_P cp_Q if_contract)

\textbf{Reject}

defs

301
Appendix B. Isabelle Theories

\(\text{OclReject} \equiv (\text{lift2}' \text{lift_arg0 lift_arg1}) \text{(strictify } (\lambda S P.\ \text{if } \forall x \in \text{set } \text{rep_sequence}_0 S. \text{DEF} (P x) \text{ then } \text{Abs_sequence}_0 (\text{List.filter} (\lambda x. P x = \text{False})). \text{rep_sequence}_0 S)) \text{ else } \bot)\)

\text{ocl_setup_op [OclReject]}

\text{lemma reject_by_select: OclReject S P = (x : (S::('τ,'α::bot)sequence) | (P::('τ,'α::bot)val ⇒ 'τ boolean) x))}
\text{apply (rule ext, auto simp: OclReject_def OclNot_def OclSelect_def ss_lifting)}
\text{apply (subgoal_tac (λxa. ((P (λs. xa) x) = False)) = (λxa. (((P (λs. xa) x) ≠ down) ∧ (((P (λs. xa) x) ≠ down) ⇒ (¬(P (λs. xa) x))))))}
\text{apply (simp, rule ext)}
\text{apply (rule_tac x = P (λs. xa) x in boolean_cases, simp_all)}
done

\text{lemma reject_by_iterate: OclReject (source::('τ,'α::bot)sequence) (P::('τ,'α::bot)val ⇒ 'τ boolean) = (source \rightarrow\text{iterate}(\text{iterator}; \text{result} = []) | (¬ P \text{ iterator}) \text{then \text{OclIncluding \text{result \text{iterator}}} \text{ else \text{(result)}} \text{ endif}))}
\text{by (simp add: reject_by_select select_by_iterate)}

\text{Properties derived from the correspondence to iterate}
\text{lemma reject_of_union: (OclReject (X::('τ,'α::bot)sequence) ∪ Y (P::('τ,'α)val ⇒ 'τ boolean)) = (OclReject X P) ∪ (OclReject Y P)}
\text{by (simp add: reject_by_select)}

\text{Excluding}
\text{defs}
\(\text{OclExcluding} \equiv \text{lift2}' \text{strictify}(\lambda X. \text{strictify} (\lambda x. \text{Abs_sequence}_0 (\text{List.filter} (\lambda e. x ≠ e). \text{rep_sequence}_0 X)))\)

\text{ocl_setup_op [OclExcluding]}

\text{Its computational characteristic by iterate}
\text{lemma excluding_by_iterate: (OclExcluding (S::('τ,'α::bot)sequence) (x::('τ,'α)val)) = OclIterate S (λ (a::('τ,'α)val) y. \text{if } (a = x) \text{ then } y \text{ else } y \rightarrow\text{including a endif}) (if (∅ x) then [] else ⊥ endif)}
B.4. Library

apply(rule ext)
apply(rule iterate_universal, simp_all add: localValidDefined2sem DEF_def)
apply(simp add: OclMtSequence_def OclExcluding_def ss_lifting'
OclIf_def OclIsDefined_def OclUndefined_def)
apply(case_tac xa ⊭ ∂ x)
apply(ocl_hypsubst, simp_all add: localValidDefined2sem)
apply(frule DEF_X_Sequence', clarify)
apply(rotate_tac 1, frule neq_commute[THEN iffD1])
apply(simp add: OclExcluding_def OclIterate_def OclIf_def OclIncluding_def OclStrictEq_def ss_lifting')

done

lemmas excluding_empty [simp] = f1_by_iterate_converse_sequence[OF excluding_by_iterate]
lemmas excluding_including [simp] = f1_by_iterate_option_including[OF excluding_by_iterate, simplified]

lemma excluding_union [simp]; (((X::('τ', 'α::bot)Sequence) ∪ Y) ->excluding x) =
(X ->excluding x) ∪ (Y ->excluding x::('τ', 'α)VAL)
apply(rule ext, case_tac xa ⊭ ∂ x, ocl_hypsubst, simp)
apply(case_tac xa ⊭ ∂ x, ocl_hypsubst, simp)
apply(case_tac xa ⊭ ∂ Y, ocl_hypsubst, simp)
apply(simp add: localValidDefined2sem DEF_def)
apply(frule DEF_X_Sequence', clarify)
apply(rotate_tac 2, frule DEF_X_Sequence', clarify)
apply(simp add: OclExcluding_def OclUnion_def ss_lifting')

done

thm excluding_empty excluding_including excluding_union

Further propierties of excluding

lemma includes_of_excluding:
[ τ ⊭ ∂(x::('τ', 'α)VAL); τ ⊭ ∂(S::('τ', 'α::bot)Sequence) ] ==
(x ∈ (S ->excluding x)) τ = F τ
apply(simp add: localValidDefined2sem DEF_def both, clarify)
apply(frule DEF_X_Sequence', clarify)
apply(simp add: OclIncludes_def OclExcluding_def OclFalse_def ss_lifting')

done

lemma size_of_excluding:
\|((S::('τ', 'α::bot)Sequence) ->excluding x::('τ', 'α)VAL)\| =
\|S\| - OclCount S x
apply(rule Sequence_sem_cases_ext, simp_all)
apply(case_tac x τ \neq ⊥)
apply(frule neq_commute[THEN iffD1])
apply(simp_all add: OclSize_def OclExcluding_def OclCount_def
Appendix B. Isabelle Theories

```plaintext
minus_def ss_lifting
apply (induct_tac c, auto)
done

lemma excluding_by_select:
  [ τ ⊨ ∅ x ] ⇒
  ( ( S::(τ :: α :: bot)Sequence) ->excluding ( x:(τ :: α) VAL) ) τ =
  ( { a : S | (¬ ( a = x )) } ) τ
apply (rule_tac X=S in Sequence_induct_including)
apply simp
apply (simp, ocl_subst, simp)
apply (simp_all add: if_not)
apply (rule trans, rule_tac A=X->excluding x in cp_charn)
apply simp_all
done

Sum

Like collect sum is specified as mapping to other OCL functions ...this is because for
every type supporting plus, zero the sum function must be available and it make no
sense to add a new definition for every one of these
defs

OclSum_def : OclSum S ≡ OclIterate (S::(τ , Integer_0)Sequence) (λ x y. x + y) 0

thm OclSum_def
thm OclIterate_def

lemma sum_by_iterate: OclSum S = OclIterate (S::(τ , Integer_0)Sequence) (λ x y. x + y) 0
  by (simp add: OclSum_def)

lemma OCL cp OclSum [simp, intro!]:
               cp P ⇒ cp(λ S. (OclSum (P S::(τ , Integer_0)Sequence)))
  by (simp add: OclSum_def)

lemmas OCL undef 1 OclSum [simp] = f1_by_iterate_undef 1[OF sum_by_iterate]

lemmas sum_empty [simp] = f1_by_iterate_mtSequence[OF sum_by_iterate]

thm f1_by_iterate_including[OF sum_by_iterate, simplified]

lemmas sum_including [simp] = f1_by_iterate_opt_including[OF sum_by_iterate, simplified]

lemmas sum_union [simp] = f1_by_iterate_distrib_union_opt[OF sum_by_iterate, of op +, simplified plus_AC, simplified]
```

304
thm OCL_undef_1 OclSum sum_empty sum_including sum_union

One
defs

OclOne_def : OclOne ≡ (lift2' lift_arg0 lift_arg1) (strictify (λ S P.
  if ∀ x ∈ set 'Rep_Sequence_0 S. DEF (P x)
  then size (List.filter (λ x. P x = True) 'Rep_Sequence_0 S) = 1,
  else ⊥))

ocl_setup_op [OclOne]

Note that contrary to many other OCL functions it is not possible to represent the
one operation directly by an iterate. The reason for it is, that the internal state space
that is used has cardinality three whereas the state space of the output values has
cardinality two.

lemma one_by_size_of_select:
( OclOne (S::(τ,α::bot)Sequence) P ) =
∥ (x : S | P (x::(τ,α)) VAL) ∥ = 1
apply(rule_tac X = S in Sequence_sem_cases_ext)
apply(auto simp : OclSelect_def OclSize_def OclStrictEq_def cp_by_cpify
OclOne_def One_ocl_int_def ss_lifting)
done

lemma one_of_mtSequence [simp]:
OclOne ([]):(τ,α::bot)Sequence :: (τ Boolean) = F
apply(simp add: one_by_size_of_select)
apply(simp add: OclStrongEq_def OclFalse_def ss_lifting'
One_ocl_int_def Zero_ocl_int_def)
done

lemma one_singleton [simp]:
[ τ ⊨ ∂ (x:(τ,α) VAL); cp P ] ==>
OclOne ([]):(τ,α::bot)Sequence ->including x (P::(τ,α) VAL ⇒ ('τ Boolean)) τ
= P x τ
apply(simp only: one_by_size_of_select)
apply(rule trans)
apply(rule_tac A = [x : [] ->including x | (P x)] in cp_charn)
apply(simp_all)
apply(rule_tac A = P x τ in boolean_cases_sem)
apply(simp_all add: OclSize_def OclStrictEq_def OclIncluding_def OclMtSequence_def
OclIf_def One_ocl_int_def neq_commute
ss_lifting' localValidDefined2sem)
done
Appendix B. Isabelle Theories

**lemma** one_union [simp]:

\[ \text{OclOne} \left( \left( X \colon \left( \tau, \alpha \colon \text{bot} \right) \text{Sequence} \right) \cup Y \right) P = \left( \text{OclOne} X P \right) \oplus \left( \text{OclOne} Y \left( P \colon (\tau, \alpha) \text{VAL} \Rightarrow \tau \text{Boolean} \right) \right) \]

apply (rule ext)
apply (case_tac $x \in \varnothing X \text{ ocl_hypsubst}$, simp)
apply (simp add: OclSxor_def ss_lifting)
apply (case_tac $x \in \varnothing Y \text{ ocl_hypsubst}$, simp)
apply (simp add: one_by_size_of_select)
oops

IsUnique
defs

OclIsUnique_def :

\[ \text{OclIsUnique} \equiv (\text{lift2}'' \text{ lift_arg0 lift_arg1}) (\text{strictify} (\lambda S P .
if \forall x \in \text{set Rep_Sequence_0} S. \text{DEF} (P x)
then \text{distinct} (\text{map} (\lambda x. P x) (\text{Rep_Sequence_0} S)))
else \bot)) \]

ocl_setup_op [OclIsUnique]

**lemma** isUnique_by_forall:

\[ \text{OclIsUnique} \left( S \colon \left( \tau, \alpha \colon \text{bot} \right) \text{Sequence} \right) \left( P \colon (\tau, \alpha) \text{VAL} \Rightarrow (\tau, c \colon \text{bot}) \text{VAL} \right) = \text{OclIterate} S (\lambda x y. (\text{OclCount} (\text{OclCollectNested} S P) (P x)) \equiv 1) \land g \top \]

oops

Any
defs

OclAny_def :

\[ \text{OclAny} \equiv (\text{lift2}'' \text{ lift_arg0 lift_arg1}) (\text{strictify} (\lambda S P .
if \forall x \in \text{set Rep_Sequence_0} S. \text{DEF} (P x) \land
(\exists x \in \text{set Rep_Sequence_0} S. P x = \text{True})
then \text{hd} (\text{List.filter} (\lambda x. P x = \text{True}) (\text{Rep_Sequence_0} S))
else \bot)) \]

ocl_setup_op [OclAny]

**lemma** any_by_first_of_select:

\[ \text{OclAny} \left( S \colon (\tau, \alpha \colon \text{bot}) \text{Sequence} \right) \left( P \colon (\tau, \alpha) \text{VAL} \Rightarrow \tau \text{Boolean} \right) = \text{OclFirst} \left( (\text{OclAsSequence} (\text{OclSelect} S P)) \colon (\tau, \alpha) \text{Sequence} \right) \]

apply (rule_tac X=S in Sequence_sem_cases_ext, simp_all)
apply (auto simp: OclAny_def OclSelect_def OclFirst_def
\text{cp_by_cpify ss_lifting' filter_empty_conv})
done

306
lemma any_of_mtSequence[simp]:

\[ \text{OclAny} \left( \frac{\mid ::(\tau', \alpha::\bot)\text{Sequence} \quad (P::(\tau', \alpha)\text{VAL} \Rightarrow (\tau \text{ Boolean})) = \bot} \right) \]
by (simp add: any_by_first_of_select)

collectNested

defs

\[
\text{OclCollectNested_def:}
\]
\[ \text{OclCollectNested} \equiv (\text{lift2' lift_arg0 lift_arg1}) (\text{strictify} (\lambda S P. \\
\quad \text{if } \forall x \in \text{set} \left( \text{Rep_Sequence}_0 S \right) \text{. DEF} (P x) \\
\quad \text{then Abs_Sequence}_0 (\map (\lambda x. P x) \left( \text{Rep_Sequence}_0 S \right)) \\
\quad \text{else } \bot)) \]

ocl_setup_op [OclCollectNested]

lemma collectNested_by_iterate:

\[ ((\text{OclCollectNested} (X::(\tau', \alpha::\bot)\text{Sequence}) (P::(\tau', \alpha)\text{VAL} \Rightarrow (\tau', \epsilon)\text{VAL}))::(\tau', \epsilon::\bot)\text{Sequence}) = (X \rightarrow \text{iterate}(x, y=[] | y\rightarrow \text{including}(P x))) \]
apply (rule ext, rule iterate_universal_0, simp_all)
apply (simp add: OclCollectNested_def cp_by_cpyify lift0_def)
apply (simp_all add: OclUndefined_def OclMtSequence_def OclCollectNested_def localValidDefined2sem ss_lifting)
apply (frule DEF_X_Sequence', clarify)
apply (frule neq_commute[THEN iffD1])
apply (rotate_tac 1, frule neq_commute[THEN iffD1])
apply (auto simp: OclIncluding_def ss_lifting)
apply (subst (asm) Abs_Sequence_0_inject_absurd22, auto)
apply (subst Abs_Sequence_0_inverse_charn2, auto)
done

Properties derived from the correspondence to iterate

lemmas collectNested_of_mtSequence [simp] = f1_by_iterate_mtSequence[OF collectNested_by_iterate]

thm f1_by_iterate_including[OF collectNested_by_iterate, simplified]

lemmas collectNested_of_including [simp] = f1_by_iterate_opt_including[OF collectNested_by_iterate, simplified]

lemmas collectNested_of_union [simp] = f1_by_iterate_distrib_union_opt[OF collectNested_by_iterate, of OclUnion, simplified]

thm OCL_undef_1_OclCollectNested collectNested_of_mtSequence collectNested_of_including collectNested_of_union

Checking a general property of iterate... on foldl

This lemma could actually be made stronger because the two assumptions undef_1_P and cp_P are not needed. But they make the proof much simpler.
Appendix B. Isabelle Theories

**Lemma iterate_of_collectNested:**

**Assumes**
- **undef_1_Q:** \( \forall y. Q \bot y = \bot \)
- **undef_2_Q:** \( \forall x. Q x \bot = \bot \)
- **cp1_Q:** \( \forall y. \text{cp} (\lambda x. Q x y) \)
- **cp2_Q:** \( \forall x. \text{cp} (Q x) \)
- **undef_1_P:** \( P \bot = \bot \)
- **cp_P:** \( \text{cp} P \)

**Shows**
- \( \text{OclIterate} \left( (\text{OclCollectNested} (S::(\tau,\alpha::\text{bot})\text{Sequence}) (P::(\tau,\alpha::\text{bot})\text{VAL} \Rightarrow (\tau,\alpha::\text{bot})\text{VAL})):((\tau,\alpha)\text{Sequence}) Q A = \text{OclIterate} S (\lambda x y. Q (P x) y) A \right) \)

**Applying**
- **insert undef_1_Q undef_2_Q cp1_Q cp2_Q undef_1_P cp_P**
- **rule ext**
- **rule iterate_universal, simp_all**
- **rule_tac P′ = P in cp_compose2**
- **simp_all add: collectNested_by_iterate iterate_opt_of_including**

**Done**

**Definedness Rules**

**Lemma undefCollectNestedI:**

**Assumes**
- **exUndef1:** \( \tau \models x \in (C::(\tau,\alpha::\text{bot})\text{Sequence}) \)
- **exUndef2:** \( \tau \models \neg \partial (P::(\tau,\alpha::\text{bot})\text{VAL} \Rightarrow (\tau,\alpha::\text{bot})\text{VAL}) x \)
- **cp_P:** \( \text{cp} P \)

**Shows**
- \( \tau \models \neg \partial ((\text{OclCollectNested} C P)::(\tau,\alpha::\text{bot})\text{Sequence}) \)

**Applying**
- **insert exUndef1 exUndef2**
- **rule isDefined_if_valid**
- **substitution (asm) OCL_is_defopt_OclIncludes**
- **clarify, simp add: localValidDefined2sem DEF_def**
- **frule DEF_X_Sequence’, clarify’**
- **simp add: localValid2sem OclIsDefined_def OclNot_def OclCollectNested_def OclIncludes_def ss_lifting’**
- **clarify’**
- **erule_tac x = x \tau in ballE**
- **simp_all add: cp_by_cpify lift0_def’**

**Done**

**Flatten**

This definition is currently not complete as it deals only with the type sequence of sequences of some type. There must be written a tactic that defines all needed instances of flatten on the different types. See the summer thesis for further information about the problems around flatten.

**Defining**

\[ \text{OclFlatten} \equiv \text{liftI}(\lambda S. \text{Abs_Sequence}_0 \text{concat} (\text{map} (\lambda x. \text{Rep_Sequence}_0 x \tau) (\text{map} (\lambda y. \text{Rep_Sequence}_0 y S^0)))) \]
B.4. Library

ocl_setup_op [OclFlatten]

lemma OCL_is_defopt_OclFlatten [simp]:
(τ ⊨ (∥ X ∥):=('τ,′α:bot)Sequence)) = (∥ X ∥):=('τ,′α Sequence_0)Sequence))
apply(rule_tac X=X in Sequence_sem_cases, simp_all)
apply(simp_all add: localValidDefined2sem OclFlatten_def ss_lifting)
apply(apply(clarify)
apply(subst (asm) Abs_Sequence_0_inject_absurd22, auto)
apply(rule_tac x=a in Abs_Sequence_0_cases_charn, simp_all)
done

Its computational characteristic by iterate

lemma flatten_by_iterate:
((OclFlatten (X:=('τ,′α:bot)Sequence)):=('τ,′α)Sequence) =
(X->iterate(x; y[]= y ∪ ((x:=('τ,′α)Sequence))))
apply(rule ext, rule iterate_universal_0, simp_all)
apply(simp_all add: OclUndefined_def OclMtSequence_def OclFlatten_def
localValidDefined2sem ss_lifting)
apply(frule DEF_X_Sequence', clarify)
apply(frule neq_commute[THEN iffD1])
apply(rotate_tac 1, frule neq_commute[THEN iffD1])
apply(frule DEF_X_Sequence', clarify)
apply(simp add: OclUnion_def OclIncluding_def ss_lifting)
apply(subgoal_tac ⊥/∈ set (concat (map (λ x::′α Sequence_0).
(Rep_Sequence_0 x))) c))
apply(auto)
apply(rule_tac x=a in Abs_Sequence_0_cases_charn, auto)
done

Deriving the rules that follow from the correspondence to iterate

lemmas flatten_of_mtSequence [simp] = f1_by_iterate mtSequence[OF flatten_by_iterate]
lemmas flatten_of_including [simp] = f1_by_iterate_opt_including[OF flatten_by_iterate,
simplified]
lemmas flatten_of_union [simp] = f1_by_iterate_distrib_union_opt[OF flatten_by_iterate,
of OclUnion, simplified]

thm OCL_undef_1_OclFlatten flatten_of_mtSequence flatten_of_including flatten_of_union

functions applied to flatten

lemma f_of_flatten:
assumes g_by_iterate: g f X τ = OclIterate X (λ x y. h y (f x)) A τ
and f_union: ⋀ X Y. [ τ ⊨ ∅ X; τ ⊨ ∅ Y ] =⇒ f (X ∪ Y) τ = h (f X) (f Y) τ
and f_empty: f [] τ = (A:=('τ,′c:bot)VAL) τ
and f_undef: f ⊥ τ = ⊥ τ
and cp_f: cp f
and cp_f_h: ∩ y. cp (λ x. h x y)
Appendix B. Isabelle Theories

and
shows $f ((\{X:\langle\tau,\alpha\rangle Sequence_0\}::\langle\tau,\alpha::\text{bot}\rangle Sequence) \tau$ = $(g f X)::\langle\tau,\alpha::\text{bot}\rangle VAL) \tau$
apply(insert cp1_h cp2_h cp_f, subst g_by_iterate)
apply(rule_tac X=X and $\tau=\tau$ in Sequence_induct_including)
apply(simp_all add: f_undef f_empty f_union)
apply(subst iterate_of_including, simp_all)
apply(rule_tac X=X and $\tau=\tau$ in cp_charn, simp_all)
apply(rule cp_eq, rule_tac P=f in cp_compose2, simp_all)
done

lemma isEmpty_flatten:
$((\{X:\langle\tau,\alpha\rangle Sequence_0\}::\langle\tau,\alpha\rangle Sequence) = []) = ((\forall x \in X \cdot (x:\langle\tau,\alpha\rangle Sequence) = []))$
apply(rule ext, rule_tac X=X and $h=\text{OclAnd}$ in f_of_flatten)
apply(simp_all add: forall_by_iterate OCL_logic_ACI
and_equiv_sand[symmetric] OCL_is_defopt_OclStrictEq
del: OCL_is_def_OclStrictEq)
done

lemma includes_flatten:
$\{ \tau = \emptyset \cdot (a::\langle\tau,\alpha::\text{bot}\rangle VAL) \} \Longrightarrow$
$(a \in ((\{X:\langle\tau,\alpha\rangle Sequence_0\}::\langle\tau,\alpha\rangle Sequence)) \tau = (\exists Y \in X \cdot (a \in (Y::\langle\tau,\alpha\rangle Sequence)))) \tau$
apply(rule_tac X=X and $h=\text{OclOr}$ in f_of_flatten)
apply(simp_all add: includes_of_union exists_by_iterate)
apply(ocl_subst, simp add: OCL_logic_ACI)
done

lemma excludes_flatten:
$\{ \tau = \emptyset \cdot (a::\langle\tau,\alpha::\text{bot}\rangle VAL) \} \Longrightarrow$
$(a \notin ((\{X:\langle\tau,\alpha\rangle Sequence_0\}::\langle\tau,\alpha\rangle Sequence)) \tau = (\forall Y \in X \cdot (a \notin (Y::\langle\tau,\alpha\rangle Sequence)))) \tau$
apply(rule_tac X=X and $h=\text{OclAnd}$ in f_of_flatten)
apply(simp_all add: includes_of_union forall_by_iterate)
apply(ocl_subst, simp add: OCL_logic_ACI)
apply(rule trans, rule_tac A=$(a \in (X \cup Y))$ in cp_charn)
apply(rule includes_of_union, simp_all)
apply(simp add: OclAnd_def OclOr_def OclNot_def ss_lifting)
done

The current formulation is NOT true. But what is an elegant solution to it?

lemma includesAll_flatten:
$(\text{OclIncludesAll} X ((\{Y:\langle\tau,\alpha\rangle Sequence_0\}::\langle\tau,\alpha\rangle Sequence))) = (\forall Z \in Y \cdot (\text{OclIncludesAll} X (Z::\langle\tau,\alpha::\text{bot}\rangle Sequence)))$
oopsort{ooops}
oopsort{ooops}
The current formulation is NOT true. But what is an elegant solution to it?

**Lemma excludesAll_flatten:**
\[ (\text{OclExcludesAll } X ((\text{OclReject } Y (\text{\texttt{Sequence}_{\text{\texttt{\_}}0}\text{Sequence})))):(\tau,\alpha)\text{Sequence})) = (\forall\ Z \in\ Y \cdot (\text{OclExcludesAll } X (Z:(\tau,\alpha)::\text{bot}\text{Sequence}))) \]

*oops*

**Lemma forall_flatten:**
\[ (\forall\ y \in\ ((\text{OclReject } Y (\text{\texttt{Sequence}_{\text{\texttt{\_}}0}\text{Sequence})))):(\tau,\alpha)\text{Sequence}) \cdot P\ y) = (\text{OclForAll } X (\lambda\ Y::(\tau,\alpha)\text{Sequence}. (\forall\ y \in\ Y \cdot P\ (y:(\tau,\alpha)::\text{bot}\text{VAL})))) \]

apply(rt ext, rule_tac X=X and h=OclAnd in f_of_flatten)
apply(simp_all, simp_all add: forall_by_iterate OCL_logic_ACI)
done

**Lemma exists_flatten:**
\[ (\exists\ y \in\ ((\text{OclReject } Y (\text{\texttt{Sequence}_{\text{\texttt{\_}}0}\text{Sequence})))):(\tau,\alpha)\text{Sequence}) \cdot P\ y) = (\text{OclExists } X (\lambda\ Y::(\tau,\alpha)\text{Sequence}. (\exists\ y \in\ Y \cdot P\ (y:(\tau,\alpha)::\text{bot}\text{VAL})))) \]

by(simp add: OclExists_def forall_flatten)

**Lemma select_flatten:**
\[ \text{OclSelect } (\text{OclCollectNested } X (\lambda\ Y::(\tau,\alpha)\text{Sequence}). \text{OclSelect } Y\ P)):(\tau,\alpha)\text{Sequence}_{\text{\texttt{\_}}0}\text{Sequence}) = \]

apply(rt ext)
apply(rule_tac X=X and \tau=x in Sequence_induct_including, simp_all)
apply(rt trans)
apply(rule_tac A=\text{OclSelect } [\text{X}] P and \tau=x in cp_charn)
apply(simp_all)
done

**Lemma reject_flatten:**
\[ \text{OclReject } (\text{OclCollectNested } X (\lambda\ Y::(\tau,\alpha)\text{Sequence}). \text{OclReject } Y\ P)):(\tau,\alpha)\text{Sequence}_{\text{\texttt{\_}}0}\text{Sequence}) = \]

by(simp add: reject_by_select select_flatten)

By rewriting any to first_of_select it is clear what the result of any on a flattened sequence will be.

Currently there is no simplification rule for the equalities. I just can’t see a way how to represent the iterated comparison of a prefix of both sequences with its intertwined concatenations.

By rewriting one to size_of_select it is clear what the result of one on a flattened sequence will be.

**Lemma size_flatten:**
\[ \text{OclSum } ((\text{OclCollectNested } X (\text{OclSize}(\tau,\alpha)\text{Sequence}\Rightarrow \tau\text{ Integer}))):(\tau,\text{Integer}_{\text{\texttt{\_}}0}\text{Sequence}) \]

apply(rt ext)
Appendix B. Isabelle Theories

apply (rule_tac X=X and \( \tau = x \) in Sequence_induct_including, simp_all)
apply (rule trans)
apply (rule_tac A=\[ X \] and \( \tau = x \) in cp_charn)
apply (simp_all add: plus_AC)
done

lemma count_flatten:
\[ \tau \in \partial \alpha \implies \] \( \llbracket (X:(\tau,\alpha \ Sequence_0 \ Sequence_0)) \rrbracket : (\tau,\alpha :: \text{	exttt{bot}}\ Sequence) \rightarrow \text{count} \ (\alpha:(\tau,\alpha \ VAL)) \] \( \tau = \nabla \llbracket \llbracket \)\n
OclSum ((OclCollectNested X (\( \lambda (X:(\tau,\alpha)\ Sequence). X \rightarrow \text{count} \ a)\))::\( (\tau,\alpha \ Integer_0)\ Sequence) \) \( \tau \)
apply (rule_tac X=X and \( \tau = \tau \) in Sequence_induct_including, simp_all)
apply (rule trans)
apply (rule_tac A=\[ X \] \( \rightarrow \text{count} \ a \) ) and \( \tau = \tau \) in cp_charn
apply (simp_all add: plus_AC)
done

lemma sum_flatten:
\( \text{OclSum (OclCollectNested X (\( \lambda (X:(\tau,\alpha)\ Sequence). X \rightarrow \text{count} \ a)\))::(\tau,\alpha \ Integer_0)\ Sequence} = \nabla \llbracket \llbracket \)\n
OclSum ((OclCollectNested X (OclSum::(\( \tau,\alpha :: \text{	exttt{bot}}\ Sequence) \Rightarrow \tau \ Integer))::(\tau,\alpha \ Integer_0)\ Sequence) \) \( \tau \)
apply (rule ext)
apply (rule_tac X=X and \( \tau = \tau \) in Sequence_induct_including, simp_all)
apply (rule trans)
apply (rule_tac A=\[ X \] \( \rightarrow \text{sum}() \) \( \llbracket X \rrbracket \) ) and \( \tau = \tau \) in cp_charn
apply (simp_all add: plus_AC)
done

lemma excluding_flatten:
\[ \tau \in \partial x \implies \] \( \llbracket (X:(\tau,\alpha \ Sequence_0 \ Sequence_0)) \rrbracket : (\tau,\alpha :: \text{	exttt{bot}}\ Sequence) \rightarrow (x:(\tau,\alpha \ VAL) \) \( \tau = \nabla \llbracket \llbracket \)\n
OclExcluding ((OclCollectNested X (\( \lambda (Y:(\tau,\alpha)\ Sequence). OclExcluding Y x)\))::(\tau,\alpha \ Sequence_0)\ Sequence)) \) \( \tau \)
apply (rule_tac X=X and \( h = \text{OclUnion in f_of_flatten} \) )
apply (simp_all)
apply (ocl_subst)
apply (simp add: flatten_by_iterate iterate_of_collectNested)
done

lemma collectNested_flatten:
\( ((OclCollectNested ((\[ X :: (\tau,\alpha Sequence_0)\ Sequence))::(\tau,\alpha :: \text{	exttt{bot}}\ Sequence) \) \( (P::(\tau,\alpha \ VAL) \Rightarrow (\tau,\alpha :: \text{	exttt{bot}} \ VAL))::(\tau,\alpha \ Sequence) \) \( \nabla \llbracket \llbracket \)\n
OclCollectNested X (\( \lambda (Y:(\tau,\alpha)\ Sequence). (OclCollectNested Y P)::(\tau,\alpha Sequence_0)\ Sequence))::(\tau,\alpha \ Sequence_0)\ Sequence)\) \) \( \tau \)
apply (rule ext)
apply (rule_tac X=X and \( \tau = \tau \) in Sequence_induct_including, simp_all)
apply (rule trans)
apply (rule_tac A=OclCollectNested \[ X \] P ) and \( \tau = \tau \) in cp_charn

312
B.4. Library

apply (simp_all)
done

lemma test':
||(((X:(τ',α Sequence_0 Sequence_0)Sequence))::(τ',α Sequence_0)Sequence)
||::((τ',α::bot)Sequence))|| = h
apply (simp add: size_flatten collectNested_flatten sum_flatten)
oops

Sequence specific functions

These are: first, last, at, insertAt, index0f, subSequence

lemma last_empty [simp]:
OclLast ([]:(τ',α::bot)Sequence) = (⊥::(τ',α)VAL)
by (simp add: last_at_UC)

lemma last_including [simp]:
(⟦τ ⊨ ∂ S⟧ =⇒ OclLast (S::(τ',α::bot)Sequence) →including (x:(τ',α)VAL)⟧ τ = ((x τ)::'α)
apply (rule_tac X = S in Sequence_sem_cases)
apply (simp add: OclIncluding_def OclLast_def ss_lifting neq_commute)
done

lemma last_union:
(⟦τ ⊨ ∂ X; τ ⊨ (Y '<>' []⟧ =⇒ OclLast (X::(τ',α::bot)Sequence) ∪ Y) τ = ((OclLast Y)::(τ',α)VAL) τ
apply (rule_tac X = X in Sequence_sem_cases)
apply (rule_tac X = Y in Sequence_sem_cases, simp_all)
apply (auto simp: localValid2sem OclNot_def OclStrictEq_def OclMtSequence_def
OclUnion_def OclLast_def OclIsDefined_def ss_lifting')
done

lemma ForAllD:
assumes allP : τ ⊨ (∀ x ∈ C. P(x::'τ ⇒ 'α::bot))
and cpP : cp P
shows (λ x. τ ⊨ x ∈ (C::(τ,(α::bot))Sequence) ⇒ τ ⊨ P x)
apply (insert allP cpP)
apply (simp add: localValid2sem OclForAll_def OclNot_def OclIncludes_def
ss_lifting')
apply (simp add: strictify_def
split: split_if_asm)
apply (erule_tac x = x τ in ballE)
apply (simp_all add: cp_by_cpfy lift0_def)

313
Appendix B. Isabelle Theories

done

lemma isdefSelectI:
  assumes localDef: \( \forall x \in C \cdot (\sigma(P \ (x \colon (\tau', \alpha::\text{bot})\ 	ext{VAL}))) \)
  and \( \tau = \sigma \ (\text{OclSelect} \ (C\colon(\tau', \alpha::\text{bot})\text{Sequence}) \ P) \)
  shows \( \tau \vdash \sigma \ (\text{OclSelect} \ C \colon (\tau', \alpha::\text{bot})\text{Sequence}) \ P \)
apply(insert localDef)
apply(erule rev_mp)
apply(rule_tac X=C in Sequence_induct_including)
apply(simp_all, clarify)
oops

lemma last Flatten:
((OclLast (\(\llceil X\colon (\tau', \alpha\ 	ext{Sequence}\_\text{th Sequence})\rrceil\))\colon(\tau', \alpha\ 	ext{VAL}) =
OclLast (OclLast (OclSelect X \ (Y :: (\tau', \alpha\ 	ext{Sequence}) \ Y '<<' []))))\colon(\tau', \alpha\ 	ext{Sequence})
apply(rule ext)
apply(rule_tac X=\(X\) in Sequence_induct_including, simp_all)
apply(case_tac x \vdash \ (a '<<' []))
apply(rotate_tac \(-1\), subst (asm) is\_TRUE\_charn\_local[symmetric])
apply(simp_all)
apply(simp add: last\_union)
apply(rule_tac B=a in cp\_charn)
apply(rule last\_including)
apply(simp\_all)

prefer 2
apply(simp add: if\_not)
apply(subst (asm) localValidNot2not[symmetric])
apply(simp add: weak\_prop\_LJE)
apply(simp)
apply(rotate_tac \(-1\), ocl\_subst)
apply(simp add: weak\_prop\_LJE)
apply(rule_tac t=OclLast (\(\llceil X\rrceil\) \cup a) \ x and
\ x =\ OclLast (\(\llceil X\rrceil\)) \ x in subst)

apply(rotate_tac 1, thin_tac ?P)
apply(rule trans[symmetric])
apply(rule_tac A=a and B=[] in cp\_charn)
apply(simp add: OclLast\_def OclUnion\_def localValid2sem OclStrictEq\_def OclFlatten\_def
OclDefined\_def OclMtSequence\_def ss\_lifting)
apply(simp\_all)
oops
Collect

Note: Currently collectNested is only defined here but it should actually be polymorphically defined in the theory OCL_Collection. Furthermore the collect operation could be defined right there because it should be defined on the OCL level to avoid having to define collect over all different types like we have to do it for flatten.

Defining collect based on collectNested according to the standard defs

\[
\begin{align*}
\text{OclCollect_def} & : \\
(\text{OclCollect} & : ((\tau,\alpha:\text{bot})\text{Sequence}, ((\tau,\alpha) \text{VAL} \Rightarrow (\tau,\text{c::bot})\text{Sequence})) \Rightarrow (\tau,\text{c::bot})\text{Sequence}) \\
S P & \equiv \llbracket (\text{OclCollectNested} S P) : ((\tau,\text{c Sequence_0})\text{Sequence}) \rrbracket
\end{align*}
\]

\[
\begin{align*}
\text{OclCollect_Integer_def} & : \\
(\text{OclCollect} & : ((\tau,\alpha:\text{bot})\text{Sequence}, ((\tau,\alpha) \text{VAL} \Rightarrow \tau \text{Integer}) \Rightarrow \tau \text{Integer_0})\text{Sequence}) \\
S P & \equiv (\text{OclCollectNested} S P)
\end{align*}
\]

\[
\begin{align*}
\text{lemma collect_by_iterate:} \\
\llbracket P \perp = \perp ; cp P \rrbracket & \implies \\
((\text{OclCollect} (X : ((\tau,\alpha:\text{bot})\text{Sequence}) (P : ((\tau,\alpha) \text{VAL} \Rightarrow (\tau,\text{c::bot})\text{Sequence})) : ((\tau,\text{c})\text{Sequence}) \\
S P & \equiv (\text{OclCollectNested} S P)
\end{align*}
\]

\[
\begin{align*}
\text{lemma OCL_cp_OclCollect[simp,intro!]:} \\
\llbracket \lambda y. cp (\lambda x. P x y) ; cp S \rrbracket & \implies cp(\lambda X. (\text{OclCollect} ((S X) : ((\tau,\alpha : \text{bot})\text{Sequence}) \\
((P X) : ((\tau,\alpha) \text{VAL} \Rightarrow (\tau,\text{c})\text{Sequence}) : ((\tau,\text{c::bot})\text{Sequence}) \\
by(\text{simp add: OclCollect_def})
\end{align*}
\]

\[
\begin{align*}
\text{lemma OCL_undef_1_OclCollect[simp]:} \\
\text{OclCollect} (\perp : ((\tau,\alpha : \text{bot})\text{Sequence}) (P : ((\tau,\alpha) \text{VAL} \Rightarrow (\tau,\text{c})\text{Sequence}) = \\
(\perp : ((\tau,\text{c::bot})\text{Sequence}) \\
by(\text{simp add: OclCollect_def})
\end{align*}
\]

end
Appendix B. Isabelle Theories

B.4.11. OCL Bag

theory OCL_Bag
imports
  $HOLOCL_HOME/src/library/collection/smashed/OCL_Sequence
begin

Properties of the the Datatype Adaption

The following rules are transformed versions of the automatically generated rules for datatype adaption

lemma Abs_Bag_0_inject_absurd11 [simp]:
  \[ \text{count } x \bot = 0 \implies (\text{Abs} \_ \text{Bag} \_ 0 \text{ down} = (\text{Abs} \_ \text{Bag} \_ 0 \ (x)) = False \]
by (subst Abs_Bag_0_inject, simp_all add: OCL_Bag_type.Bag_0_def smash_def)

lemma Abs_Bag_0_inject_absurd12 [simp]:
  \[ \text{count } x \bot = 0 \implies ((\text{Abs} \_ \text{Bag} \_ 0 \ x) = (\text{Abs} \_ \text{Bag} \_ 0 \text{ down})) = False \]
by (subst Abs_Bag_0_inject, simp_all add: OCL_Bag_type.Bag_0_def smash_def)

lemma Abs_Bag_0_inject_absurd21 [simp]:
  \[ \text{count } x \bot = 0 \implies (\bot = (\text{Abs} \_ \text{Bag} \_ 0 \ x)) = False \]
by (simp add: UU_Bag_def)

lemma Abs_Bag_0_inject_absurd22 [simp]:
  \[ \text{count } x \bot = 0 \implies ((\text{Abs} \_ \text{Bag} \_ 0 \ x) = \bot) = False \]
by (simp add: UU_Bag_def)

lemma Abs_Bag_0_inject_charn [simp]:
  \[ \text{count } x \bot = 0 \implies ((\text{Abs} \_ \text{Bag} \_ 0 \ x) = (x) = False \]
by (simp_all add: OCL_Bag_type.Bag_0_def smash_def)

lemma Abs_Bag_0_inverse_charn [simp]:
  \[ (\text{count } x \bot = 0) \implies \text{Rep} \_ \text{Bag} \_ 0 (\text{Abs} \_ \text{Bag} \_ 0 \ x) = x \]
by (substruct Abs_Bag_0_inverse, simp_all add: OCL_Bag_type.Bag_0_def smash_def)

lemma Abs_Bag_0_inverse_charn2 [simp]:
  \[ (\text{count } x \bot = 0) \implies (\text{Rep} \_ \text{Bag} \_ 0 (\text{Abs} \_ \text{Bag} \_ 0 \ x))^\# = x \]
by (substruct Abs_Bag_0_inverse, simp_all add: OCL_Bag_type.Bag_0_def smash_def)

lemma Abs_Bag_0_cases_charn:
  assumes bottomCase : \[ x = \bot \implies P \]
  assumes listCase : \[ \forall y. (\exists x. (x = \text{Abs} \_ \text{Bag} \_ 0 y, \text{count} y \bot = 0 \implies P)) \]
  shows P
316
apply \( \text{rule_tac } x = x \text{ in } \text{Abs\_Bag\_0\_cases} \)
apply \( \text{case_tac } y = \perp \)
apply \( \text{rule bottomCase}, \text{simp add: UU\_Bag\_def} \)
apply \( \text{frule not\_down\_exists\_lift2 \[ \text{THEN iffD1} \]} \)
apply \( \text{rule_tac } y = \{ y \} \text{ in listCase} \)
apply \( \text{simp add: OCL\_Bag\_type, Bag\_0\_def smash\_def DEF\_def} \)
apply \( \text{case_tac (count } \{ y \} \perp = (0::\text{nat}) \) \)
done

lemma Abs\_Bag\_0\_induct\_charn:
assumes \( \text{bottomCase: } P \perp \)
assumes \( \text{stepCase: } \forall y. (\{ \text{count } y \perp = 0 \} \implies P \text{ (Abs\_Bag\_0 } y)) \)
shows \( P x \)
apply \( \text{rule_tac } x = x \text{ in } \text{Abs\_Bag\_0\_induct} \)
apply \( \text{auto intro! : bottomCase stepCase} \)
done

lemma inj\_on\_Abs\_Bag\_0 : inj\_on\_Abs\_Bag\_0 Bag\_0
by \( \text{rule inj\_on\_inverseI, rule Bag\_0\_inj\_on\_inverse, assumption} \)

lemma inj\_Rep\_Bag\_0 : inj\_Rep\_Bag\_0
by \( \text{rule inj\_on\_inverseI, rule Bag\_0\_Rep\_Bag\_0\_inverse} \)

lemma smashed\_bag\_charn:
(\text{count } X \perp = 0) = \( (\{ X \} \in \text{Bag\_0}) \)
by \( \text{unfold smash\_def Bag\_0\_def UU\_Bag\_def, auto} \)

lemma UU\_in\_smashed\_bag [simp]:
\( \perp \in \text{Bag\_0} \)
by \( \text{unfold smash\_def Bag\_0\_def UU\_Bag\_def, auto} \)

lemma down\_in\_smashed\_bag [simp]:
down \( \in \text{Bag\_0} \)
by \( \text{unfold smash\_def Bag\_0\_def UU\_Bag\_def, auto} \)

lemma mt\_in\_smashed\_bag[simp]:
(\{#\} ) \in \text{Bag\_0}
by \( \text{unfold smash\_def Bag\_0\_def, auto} \)

lemma DEF\_Abs\_Bag: \( \forall X. (\text{count } X \perp = 0) \implies \text{DEF (Abs\_Bag\_0 } \{ X \}) \)
apply \( \text{unfold DEF\_def UU\_Bag\_def, simp} \)
done

lemma DEF\_Rep\_Bag:
\( \forall X. \text{DEF } X \implies \text{DEF (Rep\_Bag\_0 } X \)
apply \( \text{unfold DEF\_def UU\_Bag\_def, auto} \)
apply \( \text{drule_tac } f = \text{Abs\_Bag\_0 } \text{ in arg_cong} \)

317
Appendix B. Isabelle Theories

apply (simp add: Rep_Bag_0_inverse) done

lemma not_DEF_Rep_Bag:
\(\forall X. \neg \text{DEF} X \equiv \neg \text{DEF} (\text{Rep}_\text{Bag}_0 X)\)
apply (unfold DEF_def UU_Bag_def, auto)
apply (simp add: Abs_Bag_0_inverse) done

lemma exists_lift_Bag:
\(\forall X. \text{DEF} X = \Rightarrow \exists c. \text{Rep}_\text{Bag}_0 X = (\langle c \rangle)\)
by (drule DEF_Rep_Bag, simp add: DEF_X_up)

lemma exists_lift_Bag2:
\(\forall X. \text{DEF} X = \Rightarrow \exists c. \text{count} c \bot = 0 \land \text{Rep}_\text{Bag}_0 X = (\langle c \rangle)\)
apply (frule exists_lift_Bag)
apply (auto simp: UU_Bag_def DEF_def)
apply (drule sym, rule swap)
apply assumption
apply (unfold not_def)
apply (subst (asm) smashed_bag_charn)
apply (simp add: Rep_Bag_0)
done

lemma Rep_Bag_cases:
\(\text{Rep}_\text{Bag}_0 X = \bot \lor (\exists c. \text{count} c \bot = 0 \land \text{Rep}_\text{Bag}_0 X = (\langle c \rangle))\)
apply (case_tac DEF X)
apply (drule exists_lift_Bag)
apply (drule_tac [2] not_DEF_Rep_Bag)
apply (simp_all add: DEF_def)
done

lemma DEF_X_Bag_0 : DEF(X) = (\exists c. \text{count} c \bot = 0 \land \text{Rep}_\text{Bag}_0 X = (\langle c \rangle))
apply (insert Rep_Bag_cases [of X], auto)
apply (drule exists_lift_Bag, auto)
apply (rule swap)
prefer 2
apply (rule not_DEF_Rep_Bag, auto)
done

The following lemma is crucial for thy_morpher:

lemma DEF_X_Bag : DEF X = (\exists c. \text{count} c \bot = 0 \land X = \text{Abs}_\text{Bag}_0 (\langle c \rangle))
apply (auto simp: DEF_Abs_Bag)
apply (simp add: DEF_X_Bag_0)
apply (erule exE, rule refl, auto)
apply (rule injD [OF inj_Rep_Bag_0])
apply (auto simp: smashed_bag_charn Abs_Bag_0_inverse)
done

This lemma is very convenient in simplifying unfolded definitions

lemma DEF_X_Bag':
\[
\begin{array}{l}
[ X \neq \bot ] \implies \\
(\exists c. \ (\text{count} \ c \bot = 0) \land (\text{Rep}_\text{Bag}_0 X = \{c\})) \
\land \\
(\exists c. \ (\text{count} \ c \bot = 0) \land (X = (\text{Abs}_\text{Bag}_0 \{c\})))
\end{array}
\]
apply (fold DEF_def)
apply (frule DEF_X_Bag [THEN iffD1])
apply (drule DEF_X_Bag_0 [THEN iffD1])
simp
done

lemma Bag_sem_cases_0:
assumes defC: \(\forall c \ d. [\ X \neq \bot; \ \bot \neq X;\) \ 
\ (\text{count} \ c \bot = 0); \ (\text{count} \ d \bot = 0); \ 
\text{Rep}_\text{Bag}_0 X = \{c\}; \ 
(X = \text{Abs}_\text{Bag}_0 \{d\}] \implies P X \) 
and undefC: \[ X = \bot \implies P X \) 
shows \(P X \)
apply (rule Abs_Bag_0_cases_charn, erule undefC)
apply (rule defC, auto)
done

lemma Bag_sem_cases:
assumes defC: \(\forall c \ d. [\ (X \tau) \neq \bot; \ \bot \neq (X \tau);\) \ 
\ (\text{count} \ c \bot = 0); \ (\text{count} \ d \bot = 0); \ 
\text{Rep}_\text{Bag}_0 (X \tau) = \{c\}; \ 
(X \tau) = \text{Abs}_\text{Bag}_0 \{d\}] \implies P X \tau \) 
and undefC: \[ (X \tau) = \bot \implies P X \tau \) 
and cpP: \(cp P \)
shows \(P X \tau \) 
apply (rule_tac P1=P in subst[OF sym[OF cp_subst]], rule cpP)
apply (rule Bag_sem_cases_0)
apply (rule_tac P1=P in subst[OF cp_subst], rule cpP)
apply (rule defC) prefer 7
apply (rule_tac P1=P in subst[OF cp_subst], rule cpP)
apply (rule undefC, simp_all)
done

lemma Bag_sem_cases_ext:
assumes defC: \(\forall c \ d. \tau. [\ (X \tau) \neq \bot; \ \bot \neq (X \tau);\) \ 
\ (\text{count} \ c \bot = 0); \ (\text{count} \ d \bot = 0); \ 
\text{Rep}_\text{Bag}_0 (X \tau) = \{c\}; \ 
(X \tau) = \text{Abs}_\text{Bag}_0 \{d\}] \implies P X \tau = Q X \tau \) 
and undefC: \(\forall \tau. [\ (X \tau) = \bot \implies P X \tau = Q X \tau \) 
and cpP: \(cp P \)
Appendix B. Isabelle Theories

and \( cpQ \): \( cp \ Q \)
shows \( P X = Q X \)
apply (rule ext)
apply (rule_tac X = X in Bag_sem_cases)
apply (rule defC) prefer 7
apply (rule undefC)
apply (simp_all add: cpP cpQ)
done

These four lemmas are used by ocl_setup_op to reason about definedness:

lemma lift2_strict_is_isdef-fw_Bag_Val:
assumes f_def: \( f \equiv \text{lift2}(\text{strictify}(\lambda x. \text{strictify}(\lambda y. \text{Abs_Bag}_0 \text{ Rep_Bag}_0 x^r y))) \)
and inv_g: \( \text{!} ! a b. ( \lfloor \text{count a } \bot = 0; (\bot ::\'a::bot) \neq b \rfloor \implies \text{count (g a b) } \bot = 0) \)
shows \( \partial(fX Y) = (\partial X \land \partial Y) \)
apply (simp add: f_def OclIsDefined_def OclAnd_def)
apply (rule ext)
apply (case_tac DEF (X \( \tau \))
apply (frule DEF_X_Bag_0 [THEN iffD1])
apply (auto simp: strictify_def DEF_def)
done

lemma lift2_strictify_implies_LocalValid_defined_Bag_Val:
assumes f_def: \( f \equiv \text{lift2}(\text{strictify}(\lambda x. \text{strictify}(\lambda y. \text{Abs_Bag}_0 \text{ Rep_Bag}_0 x^r \text{ Rep_Bag}_0 y^r))) \)
and inv_g: \( \text{!} ! a b. ( \lfloor \text{count a } \bot = 0; \text{count b } \bot = 0 \rfloor \implies \text{count (g a b) } \bot = 0) \)
shows \( \tau \models \partial(fX Y) = ((\tau \models \partial X) \land (\tau \models \partial Y)) \)
apply (insert f_def)

320
B.4. Library

apply (drule_tac X = X and Y = Y in lift2_strict_is_isdef_fw_Bag_Val)
apply (rule inv_g, assumption+)
apply (simp add: OclAnd_def OclTrue_def o_def
          OclIsDefined_def lift0_def lift1_def lift2_def
          OclLocalValid_def)
done

lemma lift2_strictify_implies_LocalValid_defined_Bag_Bag:
  assumes f_def: \( f \equiv \text{lift2}(\text{strictify}(\lambda x. \text{strictify}(\lambda y. \text{Abs_Bag_0 \ Rep_Bag_0 x \ Rep_Bag_0 y))) \)
          and inv_g: !\!a b. (! count a ⊥ = 0; count b ⊥ = 0 \implies count (g a b) ⊥ = 0)
shows \( (\tau \models \partial(f X Y) = ((\tau \models \partial X) \land (\tau \models \partial Y)) \)
apply (insert f_def)
apply (drule_tac X = X and Y = Y in lift2_strict_is_isdef_fw_Bag_Bag)
apply (rule inv_g, assumption+)
apply (simp add: OclAnd_def OclTrue_def o_def
          OclIsDefined_def lift0_def lift1_def lift2_def
          OclLocalValid_def)
done

The conversion operators

From bags to sequences

Informally speaking the AsSequence operation returns just some sequence that has exactly the same elements like the given bag.

Note: With the current definition it does not hold that bag->seq->oset = bag->set->oset. To get this behaviour one has to define AsSequence as some sequence that has the elements in the same order like the associated set converted to a sequence.
defs

OclAsSequence_def :
OclAsSequence ≡ lift1 (strictify (\lambda X. Abs_Sequence_0 \ list_of_multiset \ Rep_Bag_0 X'))

ocl_setup_op [OclAsSequence]

lemma OCL_is_defopt_OclAsSequence:
  \( (\tau \models \partial (((\text{self}:\text{Bag}) \rightarrow \text{asSequence})):((\text{a}, \text{b}:\text{bot})\text{Sequence}))) = (\tau \models \partial \text{self}) \)
apply (simp add: localValidDefined2sem OclAsSequence_def ss_lifting)
apply (rule impl, frule DEF_X_Bag', auto)
done

lemma OCL_is_def_OclAsSequence:
  \( (\partial (((\text{self}:\text{Bag}) \rightarrow \text{asSequence})):((\text{a}, \text{b}:\text{bot})\text{Sequence}))) = (\partial \text{self}) \)
apply (rule Bag_sem_cases_ext, simp_all)
apply (simp_all add: OclIsDefined_def OclAsSequence_def ss_lifting)
done
Appendix B. Isabelle Theories

Characterisation theorems of the conversion from bags to sequences

lemma OclAsSequence_charn_0:
assumes undefCase: P ⊥ ⊥ τ
and defCase: ∀xs. [[ "Rep_Bag_0 B" ]] = multiset_of xs; DEF B; ⊥ ∉ set xs ]] ⇒ P (λ s. (Abs_Sequence_0 xs)) (λ s. B) τ
shows P ((OclAsSequence (λ s. (B::'a::bot Bag_0)));(λ s. B) τ)
apply(insert undefCase)
apply(simp add: localValidDefined2sem OclIsDefined_def OclAsSequence_def OclUndefined_def ss_lifting)
apply(rule impl)
apply(rule DEF_X_Bag_0[THEN iffD1,simplified DEF_def,clarify])
apply(rule list_of_multisetI)
apply(rule defCase)
apply(simp_all add: localValidDefined2sem DEF_def mem_set_multiset_eq)
done

lemma OclAsSequence_charn:
assumes undefCase: P ⊥ ⊥ τ
and defCase: ∀xs. [[ "Rep_Bag_0 (B τ)" ]] = multiset_of xs; ⊥ ∉ set xs; τ ⊨ ∅B ]] ⇒ P (λ s. (Abs_Sequence_0 xs)) B τ
and cp1_P: ∀y. cp (λ x. P x y)
and cp2_P: ∀x. cp (λ x. P x)
shows P ((OclAsSequence (B::'a::bot Bag));(λ x. B) τ)
apply(rule subst, rule_tac x1 = B in sym[OF cp_subst])
apply(rule list_of_multisetI)
apply(rule defCase)
apply(simp_all add: localValidDefined2sem)
apply(rule subst)
apply(simp_all add: cp0_eq_cp cp2_P cp1_P lift0_def)
apply(rule_tac P=P in OclAsSequence_charn_0)
apply(insert undefCase, simp add: OclUndefined_def lift0_def)
apply(drule defCase, simp_all add: localValidDefined2sem)
apply(rule subst)
apply(rule_tac P=λ x St. (λ s. (Abs_Sequence_0 xs)) x) St and A=B in cp_charn)
apply(simp_all add: cp2_P)
done

Showing the distributivity over the equivalences

Note: Actually it should be possible to develop the theory about the inverse of multiset_of in a more general way by combining the results of Hilbert _Choice.thy and Multiset.thy. But I’m currently not using this approach because only few specifically tailored theorems are needed.

lemma count_filter_inv_multiset_of:
count M x = length (List.filter (λ y. y = x) (list_of_multiset M))
by(auto intro: list_of_multisetI simp: count_filter[symmetric])
B.4. Library

lemma bag2seq_holEq:
\[(\text{\texttt{X}}::(\texttt{'}a\texttt{,}b::\texttt{bot})\texttt{Bag}) = \text{\texttt{Y}}) = ((\text{\texttt{asSequence}}\texttt{(X)}::\texttt{(a,'b)Sequence}) = (\text{\texttt{asSequence}}\texttt{(Y)})\]
apply(auto simp: OclAsSequence_def ss_lifting' expand_fun_eq)
apply(erule_tac x\texttt{=}x in allE)
apply(case_tac X x \texttt{\#} \bot, frule DEF_X_Bag')
apply(auto)
apply(subst \texttt{(asm) Abs_Sequence_0_inject_charn, auto})
apply(subst multiset_eq_conv_count_eq+)
apply(subst count_filter_inv_multiset_of+)
apply(simp)
apply(auto)
done

lemma bag2seq_strictEq:
\[(\text{\texttt{X}}::(\texttt{'}a\texttt{,}b::\texttt{bot})\texttt{Bag}) =\text{\texttt{Y}}) = ((\text{\texttt{asSequence}}\texttt{(X)}::\texttt{(a,'b)Sequence}) = (\text{\texttt{asSequence}}\texttt{(Y)})\]
apply(rule ext)
apply(simp add: OclStrictEq_def OclAsSequence_def ss_lifting')
apply(rule impI)+
apply(frule DEF_X_Bag', rotate_tac 1)
apply(frule DEF_X_Bag', clarify, simp)
apply(subst Abs_Sequence_0_inject_charn, auto)
apply(subst multiset_eq_conv_count_eq+)
apply(subst count_filter_inv_multiset_of+)
apply(simp)
done

lemma bag2seq_strongEq:
\[(\text{\texttt{X}}::(\texttt{'}a\texttt{,}b::\texttt{bot})\texttt{Bag}) \texttt{\#} \text{\texttt{Y}}) = ((\text{\texttt{asSequence}}\texttt{(X)}::\texttt{(a,'b)Sequence}) \texttt{\#} (\text{\texttt{asSequence}}\texttt{(Y)})\]
apply(rule ext)
apply(auto simp: OclStrongEq_def OclAsSequence_def ss_lifting')
apply(frule DEF_X_Bag', clarify, simp)
apply(frule DEF_X_Bag', clarify, simp)
apply(frule DEF_X_Bag', rotate_tac 1)
apply(frule DEF_X_Bag', clarify, simp)
apply(subst \texttt{(asm) Abs_Sequence_0_inject_charn, auto})
apply(subst multiset_eq_conv_count_eq+)
apply(subst count_filter_inv_multiset_of+)
apply(simp)
done

lemmas ss_bag2seq = bag2seq_strictEq bag2seq_strongEq

Simplifying multiple conversions

asBag is the inverse of asSequence

lemma seq2bag_of_bag2seq_UC:
Appendix B. Isabelle Theories

\((\text{OclAsBag \((B::(\text{'a,\text{'b::bot})\text{Bag})):\text{('a,\text{'b::bot})\text{Sequence}})\)) = B\)

\text{apply (rule Bag_sem_cases_ext, simp_all)}

\text{apply (simp_all add: OclAsBag_def OclAsSequence_def ss_lifting')}

\text{done}

This blowup theorem can be quite useful for conversion proofs about functions that map from a collection type to the same collection type.

\text{lemmas blowup_bag2seq = seq2bag_of_bag2seq_UC}[symmetric]

From bags to bags
defs
\text{OclAsBag_def : OclAsBag(self::(\text{'a, \text{'b::bot})\text{Bag})):\text{('a,\text{'b::bot})\text{Bag}}) \equiv self}

\text{lemma bag2bag_id [simp]:}

\text{((OclAsBag \((B::(\text{'a,\text{'b::bot})\text{Bag})):\text{('a,\text{'b})\text{Bag})) = B\)

\text{by (simp add: OclAsBag_def)}}

From bags to ordered sets
defs

\text{OclAsOrderedSet_def :}

\text{OclAsOrderedSet \equiv lift1 (strictify (\lambda X. Abs_OrderedSet_0 (list_of_set (set_of (\text{Rep_Bag_0} X)))) )}

\text{ocl_setup_op [OclAsOrderedSet]}

From bags to sets
defs

\text{OclAsSet_def :}

\text{OclAsSet \equiv lift1 (strictify (\lambda X. Abs_Set_0 (set_of (\text{Rep_Bag_0} X))))}

\text{ocl_setup_op [OclAsSet]}

Building a canonic representation of bags

The empty bag
defs

\text{OclMtBag :: (\text{'a, \text{'b::bot})\text{Bag})):\text{('a,\text{'b::bot})\text{Bag}}) \equiv lift0(Abs_Bag_0(\{\#\}))}

\text{syntax _OclMtBag_std :: (\text{'a,\text{'b::bot})\text{Bag})):\text{('a,\text{'b::bot})\text{Bag}}) \Rightarrow \text{'a Boolean (Bag{})}

\text{syntax _OclMtBag_ascii :: (\text{'a,\text{'b::bot})\text{Bag})):\text{('a,\text{'b::bot})\text{Bag}}) \Rightarrow \text{'a Boolean (mtBag) }

\text{syntax (xsymbols)}

\text{ _OclMtBag_math :: (\text{'a,\text{'b::bot})\text{Bag})):\text{('a,\text{'b::bot})\text{Bag}}) \Rightarrow \text{'a Boolean (})}

\text{parse_translation \(\langle flat(map (emb trans_const) [OclMtBag]) \rangle\)}

\text{print_translation \(\langle map emb_print [OclMtBag] \rangle\)}
B.4. Library

Foundational Properties of MtBag

lemma OCL_is_isdef_OclMtBag [simp]:
\[ \vdash P \]
by (simp add: OclValid_def OclIsDefined_def OclTrue_def OclMtBag_def ss_lifting)

lemma OCL_is_defopt_OclMtBag [simp]:
\[ \tau \vdash P \]
by (simp add: valid_elim)

Relating the empty bag to its counterpart on Sequences

lemma bag2seq_mtSequence_mtBag_UC:
\[ (\emptyset :: (a, b) \text{Bag}) = (\text{OclAsBag} (\emptyset :: (a, b) \text{Sequence})) \]
by (simp add: OclAsSequence_def OclMtBag_def OclMtSequence_def ss_lifting)

lemmas ss_bag2seq = ss_bag2seq bag2seq_mtSequence_mtBag_UC [symmetric]
and vice versa

lemma seq2bag_mtBag_mtSequence_UC:
\[ (\text{OclAsBag} (\emptyset :: (a, b) \text{Sequence})) = (\emptyset :: (a, b) \text{Bag}) \]
by (simp add: OclAsSequence_def OclMtBag_def OclMtSequence_def ss_lifting)

lemmas ss_seq2bag = seq2bag_mtBag_mtSequence_UC [symmetric]

And the 'cons' operation: including def

\[
OclIncluding \quad \equiv \quad \text{lift2} \quad (\text{strictify} \quad (\lambda X. \quad \text{strictify} \quad (\lambda Y. \quad \text{Abs_Bag_0} \\ (\{\#Y\#\} \quad + \quad \{\text{Rep_Bag_0} \quad X\})))
\]

ocl_setup_op [OclIncluding]

lemma OCL_is_isdef_OclIncluding:
\[ \vdash (\text{OclIncluding} \quad (\text{X} :: (a, b) \text{Bag}) \quad (\text{Y} :: (a, b) \text{Sequence})) = (\vdash X \quad \land \quad \vdash Y) \]
by (rule lift2_strict_is_isdef_fw_Bag_Val [OF OclIncluding_def], simp add: neq_commute)

lemma OCL_is_defopt_OclIncluding:
\[ (\tau \vdash (\text{OclIncluding} \quad (\text{X} :: (a, b) \text{Bag}) \quad (\text{Y} :: (a, b) \text{Sequence}))) = ((\tau \vdash X) \quad \land \quad (\tau \vdash Y)) \]
by (rule lift2_strictify_implies_LocalValid_defined_Bag_Val [OF OclIncluding_def], simp add: neq_commute)

The syntax translation mkBag builds now our bags

syntax
@OclFinBag :: args ⇒ (a,b Bag_0) VAL (mkBag{\_})

325
Appendix B. Isabelle Theories

translations
\begin{align*}
\text{mkBag}(x, xs) &= \text{OclIncluding} (\text{mkBag}(xs)) x \\
\text{mkBag}(x) &= \text{OclIncluding} \text{ OclMtBag} x
\end{align*}

lemma \text{mkBag}\{1,1,0,1\} = \textit{?X}

translations on Bags to its counterpart on sequences

\[ ((\text{OclAsBag}\ S)::(\text{\'a,\'b,bot})\text{Bag}) \rightarrow \text{inclusion} \ x = \\
(\text{OclAsBag}\ ((\text{S)::(\text{\'a,\'b,bot})\text{Sequence}) \rightarrow \text{inclusion}\ (x::(\text{\'a,\'b})\text{VAL}))
\]
apply(rule\_tac\ X=S in Sequence\_sem\_cases\_ext, simp\ all)
apply(case\_tac\ x \tau \neq \bot, frule neq\_commute[THEN iff\_D1])
apply(simp\ all\ add: OCL\_Sequence.OclAsBag\_def OCL\_Sequence.OclIncluding\_def
OclIncluding\_def ss\_lifting' mem\_set\_multiset\_eq union\_ac)

\[ \text{done} \]

lemmas ss_seq2bag = ss_seq2bag seq2bag_including_UC

Singletons can be converted in any direction and don’t lose information

\[ ((\text{\{}\text{\}}::(\text{\'a,\'b,bot})\text{Sequence}) \rightarrow \text{inclusion} \ x = \\
(\rightarrow \text{asSequence}\) ((\text{\{}\text{\}}::(\text{\'a,\'b})\text{Bag}) \rightarrow \text{inclusion}\ (x::(\text{\'a,\'b})\text{VAL}))
\]
apply(rule\ ext)
apply(simp\ add: OclMtSequence\_def OclMtBag\_def OclIncluding\_def
OclAsSequence\_def OCL\_Sequence.OclIncluding\_def
ss\_lifting')

\[ \text{done} \]

lemmas ss_bag2seq = ss_bag2seq bag2seq_singleton[symmetric]

Further properties of including

\[ ((B::(\text{\'a,\'b,bot})\text{Bag}) \rightarrow \text{inclusion} \ a) \rightarrow \text{inclusion} \ b = \\
((B \rightarrow \text{inclusion}\ (\text{\text{\'{a,\'b}}})\text{VAL}) \rightarrow \text{inclusion}\ (a::(\text{\'a,\'b})\text{VAL}))
\]
apply(rule\_tac\ X=B in Bag\_sem\_cases\_ext, simp\ all)
apply(case\_tac\ DEF (a x), case\_tac\ DEF (a x))
apply(simp\ add: local\Valid\Defined\2sem DEF\_def\ both, clarify)
apply(simp\ all\ add: OclIncluding\_def union\_ac ss\_lifting')
\[ \text{done} \]

A second bag constructor on the OCL level

defs

\[ \text{Abs\_Bag\_0'}\multiset\_of\ (\text{map} (\lambda z::\text{nat}. (\text{int} z + \langle x^2 \rangle) [\theta <(\text{nat}\ (\langle y' - \langle x^2 + 1 \rangle))]))\]

326
B.4. Library

\texttt{ocl\_setup\_op [OclCollectionRange]}

\texttt{lemma OCL\_is\_defopt\_OclCollectionRange [simp]:}
\begin{verbatim}
\tau \models (OclCollectionRange (a::('a Integer)) b)::('a, Integer_0)Bag)
  = ((\tau \models \exists a) \land (\tau \models \exists b))
\end{verbatim}
\begin{verbatim}
apply(subgoal_tac count (multiset_of (map (\lambda z. ((int z) + \lfloor (a \tau) \rfloor) [0..<(nat ((\lfloor (b \tau) \rfloor - \lfloor (a \tau) \rfloor) + 1))]))) \isasymleq 0)
apply(auto simp: localValidDefined2sem OclCollectionRange_def ss_lifting)
done
\end{verbatim}

\textbf{Relating collectionRange on Bags to its counterpart on Sequences}

\texttt{lemma seq2bag\_collectionRange\_UC:}
\begin{verbatim}
((OclCollectionRange a b)::('a Integer) (b::('a Integer))::('a,Integer_0)Sequence)
apply(rule ext)
apply(case_tac x \isasymleq \isasymnexists a, ocl\_hypsubst, simp)
apply(case_tac x \isasymleq \isasymnexists b, ocl\_hypsubst, simp)
apply(simp add: localValidDefined2sem DEF_def_both, clarify)
apply(subgoal_tac \isasymnexists set (map (\lambda z. ((int z) + \lfloor (a x) \rfloor) [0..<(nat ((\lfloor (b x) \rfloor - \lfloor (a x) \rfloor) + 1))])
apply(auto simp: OCL\_Sequence.OclAsBag_def OclCollectionRange_def ss_lifting'
OCL\_Sequence.OclCollectionRange_def)
done
\end{verbatim}

\texttt{lemmas ss_seq2bag = ss_seq2bag seq2bag\_collectionRange\_UC}

\textbf{Further properties of collectionRange}

Having a cp-aware rewriter would be that nice...

\texttt{lemma collectionRange\_mtBag\_conv:}
\begin{verbatim}
[ \tau \models (b::'a Integer) < (a::'a Integer) ] \rightarrow
OclCollectionRange a b \tau = (\{\}::('a,Integer_0)Bag) \tau
\end{verbatim}
\begin{verbatim}
apply(simp add: ss_seq2bag)
apply(rule trans, rule_tac P=OclAsBag in cp\_chvn)
apply(rule OCL\_Sequence.collectionRange\_mtSequence\_conv)
apply(simp_all add: ss_seq2bag)
done
\end{verbatim}

\texttt{lemma collectionRange\_singleton\_UC[simp]:}
\begin{verbatim}
OclCollectionRange a a = \{\}::('a,Integer_0)Bag \isasymRightarrow (a::('a,Integer_0)VAL)
by(simp add: seq2bag\_collectionRange\_UC seq2bag\_including\_UC[symmetric]
seq2bag\_mtBag\_mtSequence\_UC)
\end{verbatim}

\texttt{lemma collectionRange\_expand\_including:}
Appendix B. Isabelle Theories

\[ \tau \models (a \cdot 'a \text{ Integer}) \leq b \] \[ \Rightarrow ((\text{OclCollectionRange a b}) \cdot (\text{Bag})) \tau = ((\text{OclCollectionRange a (b - 1)}) \cdot \text{including b} \) \]
apply (simp add: ss_seq2bag)
apply (rule trans, rule_tac P = OclAsBag in cp_charn)
apply (rule OCL_Sequence.collectionRange_expand_including, simp_all)
done

Iterate
defs

\[ \text{OclIterate}_\text{def} : \]
\[ \text{OclIterate} \equiv (\text{lift3}' \text{lift}_\text{arg0} \text{lift}_\text{arg2} \text{lift}_\text{arg0}) \text{ (strictify } (\lambda S P A. (\text{fold_multiset } (\lambda x y. P y x) A (\text{'Rep_Bag_0 S'})))) \]

ocl_setup_op [OclIterate]

Its characterisation on the empty bag

lemma iterate_charn_mtBag [simp]:
\[ (\text{OclIterate } (\text{OclIncluding B x}) P A) \tau = (P \cdot (\text{lift0 } (x' \tau)) \cdot \text{ (lift0 } (\text{OclIterate } (\text{B}) P A) \tau) \tau) \]
by (rule ext, simp add: ss_lifting OclIterate_def OclMtBag_def)

lemma iterate_charn_including:
\[ \text{assumes ordIndep}: \forall a b c. (P a (\text{lift0 } (P b c) \tau)) = (P b \cdot (\text{lift0 } (P a c) \tau)) \tau \]
\[ \text{and defB}: \tau \models \partial (B::('a,'b::'bot))\text{Bag} \]
\[ \text{and defx}: \tau \models \partial (x::('a \Rightarrow 'b::'bot)) \]
\[ \text{shows } (\text{OclIterate } (\text{OclIncluding B x}) P A) \tau = (P \cdot (\text{lift0 } (x' \tau)) \cdot (\text{OclIterate } (\text{B}) P A) \tau) \tau) \]
apply (insert defx defB ordIndep)
apply (simp add: localValidDefined2sem)
apply (frule DEF_X_Bag [THEN iffD1])
apply (frule DEF_X_Bag_0 [THEN iffD1])
apply (clarify)
apply (simp add: OclIncluding_def OclIterate_def ss_lifting'
\text{fold_multiset_union_rev}
\text{fold_multiset_union})
done

lemma iterate_charn_including:
\[ \text{assumes ordIndep}: \forall a b c. (P a (P b c)) = (P b (P a c)) \]
\[ \text{and cpP}_1: \forall y. P (\lambda x. P x y) \]
\[ \text{and cpP}_2: \forall x. P (P x) \]
\[ \text{and defB}: \tau \models \partial (B::('a,'b::'bot))\text{Bag} \]
\[ \text{and defx}: \tau \models \partial (x::('a \Rightarrow 'b::'bot)) \]
\[ \text{shows } (\text{OclIterate } (\text{OclIncluding B x}) P A) \tau ) = \]
(P x (OclIterate (B::('a,'b::bot)Bag) P A) \tau)
apply(rule sym[OF trans])
apply(rule_tac x=x in cp_subst, simp add: cpP_1)
apply(rule trans)
apply(rule_tac x=(B->iterate(u;ua=A | (P u ua))) in cp_subst)
apply(insert cpP_2, simp add: cp_by_cpify lift0_def)
apply(rule sym[OF iterate_charn_including_0])
apply(simp add: ordIndep cp_by_cpify)
apply(rule defB, rule defx)
done

lemma iterate_opt_charn_including:
assumes ordIndep: \forall a b c. (P a (P b c)) = (P b (P a c))
and P_undef_1: !!y. P \bot y = \bot
and P_undef_2: !!x. P x \bot = \bot
and cpP_1: \land y. cp (\lambda x. P x y)
and cpP_2: \land x. cp ((P::('a,'b::bot)VAL \Rightarrow ('a,'c::bot)VAL \Rightarrow ('a,'c::bot)VAL) x)
shows (OclIterate (OclIncluding B x) P A) = (P x (OclIterate (B::('a,'b::bot)Bag) P A))
apply(insert P_undef_1 P_undef_2 cpP_1 cpP_2 ordIndep)
apply(rule ext)
apply(case_tac xa \Rightarrow B)
apply(case_tac xa \Rightarrow x)
apply(rule iterate_charn_including, simp_all)
apply(rule isUndefined_charn_local[OF defD2])
apply(rule trans, erule_tac A=x in cp_charn, simp, simp)
apply(rule sym[OF trans], erule_tac A=x in cp_charn, simp, simp)
apply(rule isUndefined_charn_local[OF defD2])
apply(rule trans, erule_tac A=B in cp_charn, simp, simp)
apply(rule sym[OF trans], erule_tac A=B in cp_charn)
apply(rule_tac P=P x in cp_compose2, simp_all)
done

Forward rules for functions defined by iterate

lemma f_by_iterate_undef_1:
\[ \begin{array}{l}
\forall A. f (B::('a,'b::bot)Bag) = \\ OclIterate B (P::('a,'b::bot)VAL \Rightarrow ('a,'c::bot)VAL \Rightarrow ('a,'c::bot)VAL) A \end{array} \]
\Rightarrow f \bot = \bot
by(simp)

lemma f_by_iterate_mtBag:
\[ \begin{array}{l}
\forall A. f (B::('a,'b::bot)Bag) = \\ OclIterate B (P::('a,'b::bot)VAL \Rightarrow ('a,'c::bot)VAL \Rightarrow ('a,'c::bot)VAL) A;
\forall a b c. (P a (P b c)) = (P b (P a c));
\forall x. cp (P x) \end{array} \]
\Rightarrow f \bot = A
Appendix B. Isabelle Theories

by (simp)

lemma f_by_iterate_including:
assumes f_by_it: \( \bigwedge B. (f(B::(\text{'a,\text{'b:bot})Bag)) = \) 
and ordIndep: \( \forall a b c. (P a (P b c)) = (P b (P a c)) \)
and defB: \( \tau \vdash \partial(B::(\text{'a,\text{'b:bot})Bag)) \)
and defx: \( \tau \vdash \partial(x::(\text{'a \Rightarrow \text{'b:bot})) \)
and cpP_1: \( \bigwedge y. cp(\lambda x. P x y) \)
and cpP_2: \( \bigwedge x. cp(P x) \)
shows \( (f(OclIncluding B x) \tau) = (P x (f B) \tau) \)
by (simp add: f_by_it iterate_charn_including ordIndep defB defx cpP_1 cpP_2)

lemma f_by_iterate_opt_including:
assumes f_by_it: \( \bigwedge S. (f(S::(\text{'a,\text{'b:bot})Bag)) = \) 
and ordIndep: \( \forall a b c. (P a (P b c)) = (P b (P a c)) \)
and P_undef_1: \( \forall y. P \bot y = \bot \)
and P_undef_2: \( \forall x. P x \bot = \bot \)
and cpP_1: \( \bigwedge y. cp(\lambda x. P x y) \)
and cpP_2: \( \bigwedge x. cp(P x) \)
shows \( f(OclIncluding S x) \tau = (P x (f S) \tau) \)
by (simp add: f_by_it iterate_charn_including ordIndep P_undef_1 P_undef_2 cpP_1 cpP_2)

Conversion of iterate from bags to sequences

For iterates mapping from bags to a non-sequence

lemma iterate_bag2seq:
assumes ordIndep: \( \forall a b c. (P a (P b c)) = (P b (P a c)) \)
shows \( (OclIterate (B :: ((\text{'a,\text{'b:bot})Bag)) \)
\( (P::(\text{'a,\text{'b:bot})VAL \Rightarrow \) \( (\text{'a,\text{'c:bot})VAL \) \( (\text{'a,\text{'c:bot})VAL) \)
\( A) = \)
\( (OclIterate ((OclAsSequence B)::(\text{'a,\text{'b:bot})Sequence) P A) \)
apply (insert ordIndep, rule ext)
apply (simp add: OclAsSequence_def OclIterate_def OCL_Sequence.OclIterate_def ss_lifting)
apply (case_tac B x \( \neq \bot) \)
apply (frule DEF_X_Bag)
apply (auto simp: fold_multiset_def)
done

lemma iterate_seq2bag:
assumes ordIndep: \( \forall a b c. (P a (P b c)) = (P b (P a c)) \)
and cpP: \( \bigwedge x. cp(P x) \)
shows \( (OclIterate (S :: ((\text{'a,\text{'b:bot})Sequence)) \)
\( (P::(\text{'a,\text{'b:bot})VAL \Rightarrow \) \( (\text{'a,\text{'c:bot})VAL \) \( (\text{'a,\text{'c:bot})VAL) \)
330
B.4. Library

\[ A = (\text{OclIterate} ((\text{OclAsBag } S)::(\text{a,b})\text{Bag} ) P A) \]
apply (insert ordIndep \text{cpP}_2, \text{rule ext})
apply (simp add: \text{OCL\_Sequence}.\text{OclAsBag\_def} \text{OclIterate\_def} \text{OCL\_Sequence}.\text{OclIterate\_def} \text{ss\_lifting} \text{cp\_by\_cpify})
apply (case_tac \( S x \neq \bot \))
apply (frule \text{DEF\_X\_Sequence}', clarify)
apply (auto simp: \text{mem\_set\_multiset\_eq} \text{fold\_multiset\_def})
apply (rule list_of_multisetI)
apply (erule \text{foldl\_right\_order\_independent})
apply (simp)
done

and for iterates mapping from bags to bags. This lemma characterises the same property on lists and multisets and serves as a guide through the proof of the theorem on bags and sequences. Because there the view is a little bit obfuscated by the contextpassingness and undefinedness cases.

\begin{align*}
\text{lemma } & \text{foldl\_multiset2list2multiset:} \\
\text{assumes } & \text{mtC\_conv: } e = \text{multiset\_of } e' \\
\text{and } & \text{stepC\_conv: } f = (\lambda M a. \text{multiset\_of } (f' \text{ SOME } xs. M = \text{multiset\_of } xs \ a)) \\
\text{and } & \text{ordInsens\_f': } \forall \text{ xs ys a. } \[ \text{multiset\_of } xs = \text{multiset\_of } ys \] \Rightarrow \text{multiset\_of } (f' \text{ xs a}) = \text{multiset\_of } (f' \text{ ys a}) \\
\text{shows } & \text{foldl } f e x s = \text{multiset\_of } (\text{foldl } f' e' x s) \\
\text{apply } & \text{(simp add: mtC\_conv stepC\_conv)} \\
\text{apply } & \text{(rule sym)} \\
\text{apply } & \text{(rule_tac x = x in rev\_induct)} \\
\text{apply } & \text{(simp\_all)} \\
\text{apply } & \text{(rule ordInsens\_f', simp)} \\
\text{apply } & \text{(rule someI2\_ex)} \\
\text{apply } & \text{(rule surj\_multiset\_of \text{THEN} surjD), simp)} \\
\text{done}
\end{align*}

\begin{align*}
\text{lemma } & \text{iterate\_bag2seq2bag\_0:} \\
\text{assumes } & \text{ordIndepP: } \forall \ a b c \tau. \ (P a (\text{lift0 } (P b c \tau))) \tau = (P b (\text{lift0 } (P a c \tau))) \tau \\
\text{and } & \text{mtC\_conv: } A = \text{OclAsBag } A' \\
\text{and } & \text{stepC\_conv: } \forall \text{ x x' B. } P x B = \text{OclAsBag } (P' x (\text{OclAsSequence } B)) \\
\text{and } & \text{ordInsens\_P': } \forall \text{ S S' x \tau. } [ \text{OclAsBag } S \tau = ((\text{OclAsBag } S' \tau)\text{ : }'c:\text{bot } Bag_0) ] \\
\text{shows } & (\text{OclAsBag } (P' x S) \tau = ((\text{OclAsBag } (P' x S') \tau)\text{ : }'c:\text{bot } Bag_0) \\
\text{apply } & \text{(rule ext)} \\
\text{apply } & \text{(rule trans\text{|symmetric})} \\
\text{apply } & \text{(rule \text{cp\_subst}, simp add: OCL\_cp\_OclAsBag)}
\end{align*}
Appendix B. Isabelle Theories

apply (simp add: OclIterate_def OCL_Sequence.OclIterate_def ordIndepP)
apply (rule_tac P = λa. (P a b c) = (P b a c))
apply (simp add: mtC_conv)
apply (rule_tac P = (λx. (P x b c) = (P x a c)) and t = B in subst)
apply (simp add: ss_lifting)
apply (rule_tac P = (λx. (P x b c) = (P x a c)) and t = BOT in subst)
apply (simp add: OclAsSequence_def)
apply (frule DEF_X_Bag, clarify, simp)
oops

lemma iterate_bag2seq2bag:
assumes ordIndepP: ∀a b c. (P a (P b c)) = (P b (P a c))
and cpP_2: ∃x. cp (P x)
and mtC_conv: A = OclAsBag A'
and stepC_conv: ∀x. P x B = OclAsBag (P x (OclAsSequence B))
and ordInsens_P: ∀S S' x. (OclAsBag S x) = (OclAsBag S' x) ⇒ (OclAsBag S' x) = (OclAsBag S x)
shows (OclAsBag (P x S) x) = (OclAsBag (P' x S') x) = (OclAsBag (P' x S') x)
oops

Note: If one looks at the conversion theorems about union, including and so on one sees that asBag can be taken inside. The same theorem should hold on iterate. But currently I’m not sure about its use, because in all proofs about a conversion of iterate the “reformulation” theorems (the form: bag2seq2bag) are used.
I don’t know either if the “distributive” version is equally or more powerful. Therefore the following lemma after the lemmas illustrating the idea on multisets is currently left unproven.

lemma projection_of_foldl:
assumes projInsens_f: ∀xs ys a. (P xs = P ys) ⇒ P (f xs a) = P (f ys a)
shows P (foldl f e xs) =

332
B.4. Library

\[ \text{foldl } (\lambda \ a \ b. \ P \ (\text{SOME } \ y) \ a = P \ y) \ b) \ (P \ e) \ x \]
apply(rule_tac xs=\xs in rev_induct)
apply(simp_all)
apply(rule projInsens_f, simp)
apply(rule someI2, rule sym, simp_all)
done

lemma multiset_of_foldl:
assumes ordInsens_f \[ \land \ x \ y a. [\text{multiset}_\text{of } \ x = \text{multiset}_\text{of } \ y] \implies \text{multiset}_\text{of } (f \ x \ a) = \text{multiset}_\text{of } (f \ y \ a)
and ordIndep_f (\forall a \ b. c. ((f (f a) b) = (f (f a) b)))
shows multiset_of (foldl f e \xs) =
\begin{align*}
\text{foldl } (\lambda \ M \ a. \ \text{multiset}_\text{of } (f \ (\text{SOME } \ y). \ M = \text{multiset}_\text{of } \ y) \ a) \\
\text{multiset}_\text{of } e \\
\text{SOME } y. \ \text{multiset}_\text{of } \ x = \text{multiset}_\text{of } \ y
\end{align*}

oops

lemma iterate_seq2bag:
assumes ordIndepP (\forall a \ b. c. \ (P' a (P' b c)) = (P' b (P' a c)))
and P'_def (P' = (\lambda x. (B::('a::bot):Bag). OclAsBag (P x ((OclAsSequence B)::('a,c::bot:Bag))))
and cpP_2 (\land x. cp (P' x))
and ordInsens_p (\forall \ x. \ (\text{OclAsBag } S \ x \tau) = ((\text{OclAsBag } S' \ tau) :: 'c::bot Bag_0))
implies OclAsBag (P x \S) = ((OclAsBag (P x \S) :: 'c::bot Bag_0)
shows (OclIterate ((OclAsBag S)::('a,b::bot)Bag))
\begin{align*}
(\lambda x. (B::('a,c):Bag). OclAsBag (P x ((OclAsSequence B)::('a,c::bot:Sequence))))(A)
\end{align*}

oops

Union
defs

OclUnion_def : OclUnion \equiv lift2 (\lambda X. strictify (\lambda Y. Abs_Bag_0 ((\landRep_Bag_0 X + \landRep_Bag_0 Y)_y)))

ocl_setup_op [OclUnion]

lemma OCL_is_def_OclUnion:
\partial(OclUnion (X::('a,b::bot):Bag) Y) = (\partial X \land \partial Y)
apply(rule lift2_strict_is_isdef_fw_Bag_Bag[OF OclUnion_def])
Appendix B. Isabelle Theories

apply (simp)
done

lemma OCL_is_defopt_OclUnion:
  \((\tau \vDash \emptyset) (OclUnion (X::('a,'b::bot)Bag) Y)) = (\tau \vDash \emptyset X) \land (\tau \vDash \emptyset Y)\)
apply (rule lift2_strictify_implies_LocalValid_defined_Bag_Bag[of OclUnion_def])
apply (simp)
done

lemma union_seq2bag:
  \((-\text{asBag()} ((X::('a,'b::bot)Sequence) \cup Y) = (\text{-\text{asBag()} X}):(\text{\text{'a,'b}Bag}) \cup (\text{-\text{asBag()} Y}):(\text{\text{'a,'b}Bag})\)
apply (rule Sequence_sem_cases_ext, simp_all)
apply (rule_tac X=X in Sequence_sem_cases, simp_all)
apply (simp_all add: OCL_Sequence.OclUnion_def mem_set_multiset_eq OCL_Sequence.OclAsBag_def ss_lifting)
done

lemma union_bag2seq2bag:
  \((-\text{asBag()} ((\text{-\text{asSequence()} (X::('a,'b::bot)Bag)})::(\text{\text{'a,'b})Sequence}) \cup (\text{-\text{asSequence()} Y}))
= (X \cup Y)
by (simp add: union_seq2bag seq2bag_of_bag2seq_UC)

lemma union_by_iterate:
  \((\text{(X::('a,'b::bot)Bag}) \cup (Y::('a,'b::bot)Bag)) =
  (Y \rightarrow_{iterate(x;y=X \mid y \rightarrow_{including (x::('a,'b::bot)VAL} )})\)
apply (simp add: union_bag2seq2bag[symmetric] union_by_iterate)
oops

Intersection
defs

\text{OclIntersection_def} : OclIntersection \equiv \text{lift2}(\lambda X. \text{strictify} (\lambda Y. \text{Abs_Bag}_0 ((\text{\text{\text{'a,'b}Bag}) \cap (\text{\text{'a,'b}Bag})) ))\)

\text{ocl_setup_op [OclIntersection]}
We'll need a second definition for the mixed case of intersection between a set and a bag ... the same case holds for union.

Includes and excludes
defs

\text{OclIncludes_def} : OclIncludes \equiv \text{lift2}(\lambda X. \text{strictify} (\lambda x. \_ \text{\text{\text{\text{'a,'b}Bag}) \cap x}))\)
OclExcludes_def: OclExcludes ≡ lift2 (strictify (λX. strictify (λx. "count " Rep_Bag_0 X \ x = 0''' )))

ocl_setup_op [OclIncludes, OclExcludes]

We prefer a normal form where excludes is written as not includes

lemma excludes_not_includes [simp]:
  x \not\in X = \neg (x::('a,'b)VAL) ∈ (X::('a,'b:bot) Bag)
apply(rule Bag_sem_cases_ext, simp_all)
apply(simp_all add: OclExcludes_def OclNot_def OclIncludes_def ss_lifting)
done

Relating includes and excludes on Bags to their counterparts on Sequences

lemma includes_bag2seq:
  (a::('a,'b)VAL) ∈ (X::('a,'b:bot)Bag) =
  a ∈ ((OclAsSequence X)::('a,'b:bot)Sequence)
apply(rule ext)
apply(rule_tac B=X in OclAsSequence_charn)
apply(simp_all add: localValidDefined2sem DEF_def)
apply(rule DEF_X_Bag', clarify)
apply(simp add: OclIncludes_def OCL_Sequence.OclIncludes_def
          OCL_Sequence.OclAsBag_def ss_lifting mem_set_multiset_eq)
done

lemma excludes_bag2seq:
  (a::('a,'b)VAL) \not\in (X::('a,'b:bot)Bag) =
  a \not\in ((OclAsSequence X)::('a,'b:bot)Sequence)
by(simp add: includes_bag2seq)

building a simplifier set to expand all functions on bags to the ones on sets, if it is possible.

lemmas ss_bag2seq = ss_bag2seq includes_bag2seq excludes_bag2seq

and vice versa

lemma includes_seq2bag:
  (a::('a,'b)VAL) ∈ (X::('a,'b:bot)Sequence) =
  a ∈ ((OclAsBag X)::('a,'b)Bag)
apply(rule Sequence_sem_cases_ext, simp_all)
apply(simp_all add: OclIncludes_def OCL_Sequence.OclIncludes_def
          OCL_Sequence.OclAsBag_def ss_lifting mem_set_multiset_eq)
done

lemma excludes_seq2bag:
  (a::('a,'b)VAL) \not\in (X::('a,'b:bot)Sequence) =
Appendix B. Isabelle Theories

\[ a \notin ((\text{OclAsBag} X);(\text{a,b})\text{Bag}) \]
by (simp add: includes_seq2bag)

lemmas ss_seq2bag = ss_seq2bag includes_seq2bag excludes_seq2bag

Characterisation of includes on the semantic part

lemma includes_charn1 :
\[(\tau \models x \in S) \implies (\emptyset < \text{count } \text{Rep_Bag}_0 (S \tau) ) (x \tau)\]
apply (frule isDefined_if_valid)
apply (erule OCL_is_defopt_OclIncludes [THEN iffD1])
apply (simp add: OclLocalValid_def OclIsDefined_def strictify_def
OclNot_def OclIncludes_def o_def lift0_def lift1_def lift2_def
OclTrue_def OclFalse_def OclUndefined_def DEF_def)
done

lemma includes_charn2 :
\[ \llbracket \text{DEF}(S \tau); \emptyset < \text{count } \text{Rep_Bag}_0 (S \tau) \rrbracket (x \tau) = \implies \tau \models x \in S \]
apply (frule DEF_X_Bag [THEN iffD1], erule exE)
apply (simp add: OclLocalValid_def OclIsDefined_def strictify_def
OclNot_def OclIncludes_def o_def lift0_def lift1_def lift2_def
OclTrue_def OclFalse_def OclUndefined_def DEF_def)
apply (auto)
done

Higher Properties of includes and excludes

lemma includes_of_mtBag [simp]:
\[ \neg (\tau \models (x::(\text{a,b})\text{VAL}); (\tau \models (\text{a,b})\text{Bag})) \]
by (simp only: ss_bag2seq, rule includes_of_mSequence)

lemma includes_charn1_including[simp]:
\[ (\tau \models \partial (a::(\text{a,b})\text{VAL}); (\tau \models \partial (X::(\text{a,b})\text{Bag})) ) \implies \tau \models a \in (X \rightarrow\text{including} a) \]
apply (simp only: localValidDefined2sem DEF_def)
apply (frule DEF_X_Bag, clarify)
apply (simp add: localValid2sem OclIncludes_def OclIncluding_def
ss_lifting' neq_commute)
done

lemma includes_charn2_including[simp]:
\[ (\tau \models \partial (a::(\text{a,b})\text{VAL}); (\tau \models \partial (b::(\text{a,b})\text{VAL}); (\tau \models a \in (X::(\text{a,b})\text{Bag}) ) \implies \tau \models a \in (X \rightarrow\text{including} b) \]
apply (case_tac X \tau \neq \bot)
apply (frule DEF_X_Bag, clarify)

336
apply(simp_all only: localValidDefined2sem DEF_def)
apply(simp_all add: localValid2sem OclIncludes_def OclIncluding_def
 ss_lifting' neq_commute)
apply(drule neq_commute THEN_iffD1, simp)
done

It would be more favourable to have this theorem proven on sets first and lift it then
to all other collections. Because it doesn’t work to lift it in the other direction, from
sequences to bags, sets and ordered sets.

lemma includes_of_collectionRange:
(x::('a Integer)) ∈ ((OclCollectionRange a b)::('a Integer, 'a Integer) Bag) = 
((a::('a Integer)) ≤ x) ∧ (x ≤ (b::('a Integer)))
apply(rule ext)
apply(case_tac DEF (x xa), case_tac DEF (a xa), case_tac DEF (b xa))
apply(simp add: DEF_def_both, clarify)
apply(subgoal_tac count (multiset_of (map (λ z. ⌞ (int z) + ⌜(a xa)⌝) [0..<(nat ⌜(b xa)⌝ − ⌜(a xa)⌝ + 1]])) ⊥ = 0)
apply(auto simp add: OclIncludes_def OclCollectionRange_def OclLe_def
 OclSand_def OclNot_def ss_lifting)
apPLY(arith)
apPLY(rule_tac x = nat(⌜(x xa)⌝ − ⌜(a xa)⌝) in image_eqI, auto)
apPLY(simp add: count_filter)
done

lemma cp_sor [simp, intro!]: [ cp P; cp P' ] ⇒ cp (λ X. (P X) ∨ (P' X))
by(simp add: OclSor_def)

lemma includes_of_union [simp]:
((a::'a,b::bot) VAL) ∈ ((X::('a,b::bot)Bag) U Y) = 
((a ∈ X) ∨ (a ∈ Y))
apPLY(rule_tac X=X in Bag_sem_cases_ext, simp_all)
apPLY(rule_tac X=Y in Bag_sem_cases, simp_all)
apPLY(case_tac τ = Γ a, ocl_hypsubst, simp add: OclSor_def)
apPLY(simp add: localValidDefined2sem DEF_def_both, clarify)
apPLY(simp_all add: OclIncludes_def OclUnion_def OclSor_def
 OclSand_def OclNot_def ss_lifting)
done

lemma not_includes_of_mtBag:
(τ ⊨ ¬ (x::('a, b)VAL) ∈ ((x::('a,b::bot) Bag)) = (τ ⊨ ∅ x)
by(simp only: ss_bag2seq_not_includes_of_mtSequence)

Emptiness
defs
Appendix B. Isabelle Theories

\[ \text{OclIsEmpty} \equiv \text{lift1} (\text{strictify} (\lambda X. \{\#\} = \{\text{Rep_Bag}_0 X\})) \]

\[ \text{OclNotEmpty} \equiv \text{lift1} (\text{strictify} (\lambda X. \{\#\} \neq \{\text{Rep_Bag}_0 X\})) \]

\text{ocl_setup_op} [\text{OclIsEmpty, OclNotEmpty}]

we prefer a canonical form were notEmpty is written using isEmpty

\text{lemma notEmpty_not_isEmpty_conv [simp]:}
\begin{align*}
\not\emptyset(X;('a, 'b::bot)\ Bag) &= \neg (\not\emptyset X) \\
\text{apply (rule ext)} \\
\text{apply (simp add: OclNotEmpty_def OclIsEmpty_def OclNot_def ss_lifting) }
\end{align*}

done

Relating isEmpty and isNotEmpty on Bags to their counterparts on Sequences

\text{lemma isEmpty_bag2seq:}
\begin{align*}
\not\emptyset(X;('a, 'b::bot)\ Bag) &= \not\emptyset((\text{OclAsSequence} X);('a,('b::bot))\ Sequence) \\
\text{apply (rule ext)} \\
\text{apply (rule_tac B=X in OclAsSequence_charn, simp_all)} \\
\text{apply (simp_all add: localValidDefined2sem DEF_def)} \\
\text{apply (frule DEF_X_Bag', clarify)} \\
\text{apply (simp_all add: OclIsEmpty_def OclMtSequence_def mem_set_multiset_eq OclStrictEq_def ss_lifting') } \\
\text{apply (subst Abs_Sequence_0_inject_charn)} \\
\text{apply (auto simp: mem_set_multiset_eq)}
\end{align*}

done

\text{lemma isNotEmpty_bag2seq:}
\begin{align*}
\text{OclNotEmpty}(X;('a, 'b::bot)\ Bag) &= \text{OclNotEmpty}((\text{OclAsSequence} X);('a,('b::bot))\ Sequence) \\
\text{by (simp add: isEmpty_bag2seq)}
\end{align*}

\text{lemmas ss_bag2seq = ss_bag2seq isEmpty_bag2seq isNotEmpty_bag2seq}

from sequences to bags

\text{lemma isEmpty_seq2bag:}
\begin{align*}
\not\emptyset(X;('a, 'b::bot)\ Sequence) &= \not\emptyset((\text{OclAsBag} X);('a, 'b)\ Bag) \\
\text{apply (rule Sequence_sem_cases_ext, simp_all)} \\
\text{apply (simp_all add: OclIsEmpty_def OclStrictEq_def OclMtSequence_def OCL_Sequence OclAsBag_def ss_lifting' mem_set_multiset_eq)} \\
\text{apply (subst Abs_Sequence_0_inject_charn)}
\end{align*}

338
B.4. Library

apply (auto simp: mem_set_multiset_eq)
done

lemma isNotEmpty_seq2bag:
OclNotEmpty (X::(('a','b::bot)Sequence)) = OclNotEmpty ((OclAsBag X)::('a,('b::bot)Bag))
by (simp only: isNotEmpty_seq2bag notEmpty_not_isEmpty_conv OCL_Sequence.notEmpty_not_isEmpty_conv)

lemmas ss_seq2bag = ss_seq2bag isEmpty_seq2bag isNotEmpty_seq2bag

Further properties of the emptiness test

lemma isEmpty_stricteq_mtBag_conv [simp]:
(\ ⟨\ X \⟩) = ((X::('a,'b::bot)Bag) ≡ ⟨\⟩)
apply (rule ext)
apply (case_tac X x ≠⊥)
apply (frule DEF_X_Bag', clarify)
apply (simp_all add: OclIsEmpty_def OclMtBag_def OclStrictEq_def Abs_Bag_0_inject_charn ss_lifting)
apply (blast)
done

lemma isEmpty_of_mtbag:
τ ⊨ \ ⟨\⟩
by (simp)

lemma isEmpty_of_including:
\⟦ τ ⊨ ∂ (a::('a,'b)VAL); τ ⊨ ∂ (X::('a,'b::bot)Bag) \⟧ ⇒
τ ⊨ ¬(\ ⟨\⟩(X→including a))
oops

lemma notEmpty_of_mtbag:
τ ⊨ ¬(\ ⟨\⟩)
by (simp)

lemma notEmpty_of_including:
\⟦ τ ⊨ ∂ (a::('a,'b)VAL); τ ⊨ ∂ (X::('a,'b::bot)Bag) \⟧ ⇒
τ ⊨ \ ⟨\⟩(X→including a)
oops

Size
defs

OclSize_def ≡ (OclSize::('a,'b::bot Bag_0) VAL => 'a Integer) ≡
lift1 (strictify (λX. _int (size (⌜Rep_Bag_0 X⌝)))),)

ocl_setup_op [OclSize]
Appendix B. Isabelle Theories

Relating size on bags to its counterpart on sequences

lemma size_multiset_of: (size (multiset_of xs)) = (length xs)
  by (induct xs, auto)

lemma size_bag2seq: 
  (∥X :: (′a, ′b::bot)Bag∥) = 
  (∥((OclAsSequence X)::′a,′b::bot)Sequence∥)
  apply (rule ext)
  apply (rule_tac B=X in OclAsSequence_charn, simp_all)
  apply (frule DEF_X_Bag', clarify)
  apply (auto simp: OclSize_def OCL_Sequence.
  OclSize_def.
  OCL_Sequence.
  OclAsBag_def size_multiset_of ss_lifting)
  done

lemmas ss_bag2seq = ss_bag2seq size_bag2seq

lemma size_seq2bag: 
  (∥[X :: (′a, ′b::bot)Sequence∥) = 
  (∥((OclAsBag X)::′a,′b::bot)Bag∥)
  apply (rule Sequence_sem_cases_ext, simp_all)
  apply (auto simp: OclSize_def OCL_Sequence.
  OclSize_def.
  OCL_Sequence.
  OclAsBag_def size_multiset_of ss_lifting mem_set_multiset_eq)
  done

lemmas ss_seq2bag = ss_seq2bag size_seq2bag

Further properties of size

The real power of the proofs by conversion

lemma size_by_iterate: 
  (∥X :: (′a, ′b::bot)Bag∥) = 
  OclIterate X (λ (x::′a,′b::bot) VAL) (y::′a Integer. y + 1) 0
  by (simp add: ss_bag2seq OCL_Sequence.size_by_iterate iterate_bag2seq)

Count

defs

  OclCount_def : OclCount ≡ lift2 (strictify (λX. strictify (λx.
  int (count Rep_Bag_0 X')) x'))

ocl_setup_op [OclCount]

340
Relating count on bags to its counterpart on sequences

**Lemma count_bag2seq**:

\[
\begin{align*}
(X \cdot ('a', 'b': bot) Bag) \rightarrow count (a :: ('a', 'b') VAL) &= \\
((\rightarrow asSequence()) X) \cdot ('a', 'b': bot) Sequence \rightarrow count a
\end{align*}
\]

apply (rule ext)
apply (rule_tac B = X in OclAsSequence_charn, simp_all)
apply (auto simp: localValidDefined2sem DEF_def)
apply (frule DEF_X_Bag', clarify)
apply (auto simp: OclCount_def OCL_Sequence)
apply (induct_tac xs, simp_all)
done

lemmas ss_bag2seq = ss_bag2seq count_bag2seq

**Lemma count_seq2bag**:

\[
\begin{align*}
(X \cdot ('a', 'b': bot) Sequence) \rightarrow count (a :: ('a', 'b') VAL) &= \\
((\rightarrow asBag()) X) \cdot ('a', 'b': bot) Bag \rightarrow count a
\end{align*}
\]

apply (rule Sequence_sem_cases_ext, simp_all)
apply (auto simp: OCL_Sequence)
apply (induct_tac c, simp_all)
done

lemmas ss_seq2bag = ss_seq2bag count_seq2bag

Further properties of count

**Lemma count_by_iterate**:

\[
\begin{align*}
(X \cdot ('a', 'b': bot) Bag) \rightarrow count ((a :: ('a', 'b') VAL)) &= \\
(OclIterate X) (\lambda (x :: ('a', 'b': bot) VAL) (y :: 'a Integer). \text{if } (x \equiv a) \text{then } (y + 1) \text{ else } y \text{ endif})
\end{align*}
\]

apply (simp add: ss_bag2seq count_by_iterate)
apply (subst iterate_bag2seq, simp_all)
apply ((rule allI)+, rule ext)
apply (simp add: OclIf_def plus_def One_ocl_int_def)
done

**Lemma includes_by_count_UC**:

\[
(X \rightarrow count a) > \emptyset = (a :: ('a', 'b') VAL) \in (X \cdot ('a', 'b': bot) Bag)
\]

by (simp only: ss_bag2seq OCL_Sequence.includes_by_count_UC)

**Lemma excludes_by_count_UC**:

\[
\begin{align*}
\text{OclCount } S x \equiv \emptyset &= \neg ((x :: ('a', 'b') VAL) \in (S \cdot ('a', 'b': bot) Sequence))
\end{align*}
\]

by (simp only: ss_bag2seq OCL_Sequence.excludes_by_count_UC)
Appendix B. Isabelle Theories

Forall defs

\begin{align*}
\text{OclForAll} &= \text{lift2' lift_arg0 lift_arg1 (\strictify \land S. (\lambda P. \\
& \text{if } \forall x \in \text{set_of Rep_Bag_0 S}. P x = \text{True} \text{ then } \text{True} \\
& \text{else if } \exists x \in \text{set_of Rep_Bag_0 S}. P x = \text{False} \text{ then } \text{False} \\
& \text{else } \bot))}
\end{align*}

ocl_setup_op [OclForAll]

Relating forall on bags to its counterpart on sequences

\text{lemma forall_bag2seq:}

\begin{align*}
\forall x \in (X :: (('a,'b::bot)Bag)) \cdot P (x::('a => 'b)) &= \\
(\forall x \in ((\text{OclAsSequence X})::(('a,'b::bot)Sequence) \cdot P x)
\end{align*}

\text{apply(rule ext)}
\text{apply(rule_tac B = X in OclAsSequence_charn, simp_all)}
\text{apply(simp_all add: OclForAll_def OCL_Sequence OclUndefined_def OclAsSequence_def mem_set_multiset_eq cp_by_cpify ss_lifting' localValidDefined2sem)}
\text{done}

\text{lemmas ss_bag2seq = ss_bag2seq forall_bag2seq}

Further properties of forall

\text{lemma forall_by_iterate:}

\begin{align*}
(\forall x \in (B::('a,'b::bot)Bag)) \cdot (P::('a,'b::bot)VAL \Rightarrow 'a Boolean) x &= \\
(\forall x \in ((\text{OclAsSequence B})::(('a,'b::bot)Sequence) \cdot P x)
\end{align*}

\text{apply(simp add: forall_by_iterate ss_bag2seq)}
\text{apply(subst iterate_bag2seq simp_all add: and_assoc)}
\text{apply(simp add: and_commute)}
\text{done}

Exists

Relating exists on bags to its counterpart on sequences

\text{lemma exists_bag2seq:}

\begin{align*}
\exists x \in (B::('a,'b::bot)Bag) \cdot P (x::('a => 'b)) &= \\
(\exists x \in ((\text{OclAsSequence B})::(('a,'b::bot)Sequence) \cdot P x)
\end{align*}

\text{by(simp add: OclExists_def forall_bag2seq)}

\text{lemmas ss_bag2seq = ss_bag2seq exists_bag2seq}

Further properties of exists

\text{lemma exists_by_iterate:}

\begin{align*}
(\exists x \in (B::('a,'b::bot)Bag)) \cdot (P::('a,'b::bot)VAL \Rightarrow 'a Boolean) x &= \\
(\exists x \in ((\text{OclAsSequence B})::(('a,'b::bot)Sequence) \cdot P x)
\end{align*}

\text{by(simp add: exists_by_iterate ss_bag2seq)}
B.4. Library

apply (subst iterate_bag2seq, simp_all)
apply (subst or_commute)
apply (simp add: or_assoc)
apply (simp add: or_commute)
done

IncludesAll
defs

\( OclIncludesAll \_def: OclIncludesAll \equiv \text{lift2} (\lambda X. \text{strictify} (\lambda Y. \\
\set_of{\text{Rep\_Bag}_0 Y} \subseteq \set_of{\text{Rep\_Bag}_0 X})) \)

ocl\_setup\_op [OclIncludesAll]

Relating includesAll on bags to its counterpart ond sequences

lemma includesAll_bag2seq:
\( OclIncludesAll (X::('a,'b::bot)Bag) (Y::('a,'b)Bag) = \)
\( OclIncludesAll ((OclAsSequence X)::('a,'b)Sequence) ((OclAsSequence Y)::('a,'b)Sequence) \)
apply (rule ext)
apply (rule_tac B=X in OclAsSequence_charn, simp_all)
apply (rule_tac B=Y in OclAsSequence_charn, simp_all)
apply (simp add: OclAsSequence_def mem_set_multiset_eq
localValidDefined2sem ss_lifting')
done

lemmas ss\_bag2seq = ss\_bag2seq includesAll\_bag2seq

Further properties of includesAll

lemma includesAll\_by\_iterate:
\( OclIncludesAll X (Y::('a,'b::bot)Bag) = \)
\( \text{iterate}(x,y = \text{if } (\exists X) \text{ then } \top \text{ else } \bot \text{ endif } | ((x::('a,'b)VAL) \in X) \land y) \)
apply (simp add: includesAll\_by\_iterate ss\_bag2seq)
apply (subst iterate\_bag2seq)
apply (simp_all add: OCL\_is\_def OclAsSequence)
apply (auto, rule ext, auto simp: OclSand\_def ss\_lifting')
done

ExcludesAll
defs

\( OclExcludesAll \_def: OclExcludesAll \equiv \text{lift2} (\lambda X. \text{strictify} (\lambda Y. \\
\set_of{\text{Rep\_Bag}_0 X} \cap \set_of{\text{Rep\_Bag}_0 Y} = \{\}) \)

ocl\_setup\_op [OclExcludesAll]

343
Appendix B. Isabelle Theories

Relating excludesAll on bags to its counterpart ond sequences

\textbf{lemma} excludesAll\_bag2seq
\begin{align*}
\text{OclExcludesAll } (X; (\forall a,b. : \text{bot}) \text{Bag}) = \\
\text{OclExcludesAll } ((\text{OclAsSequence } X); (\forall a,b. : \text{Sequence}) ((\text{OclAsSequence } Y); (\forall a,b. : \text{Sequence})
\end{align*}
apply (rule ext)
apply (rule_tac B = X in \text{OclAsSequence}_\text{charn}, simp_all)
apply (rule_tac B = Y in \text{OclAsSequence}_\text{charn}, simp_all)
apply (simp add: \text{OclExcludesAll}_\text{def} \text{OCL\_Sequence.\OclExcludesAll}_\text{def} \text{OclAsSequence}_\text{def} \text{mem_set_multiset_eq} \text{localValidDefined2sem ss_lifting})
done

\textbf{lemmas} ss\_bag2seq = ss\_bag2seq excludesAll\_bag2seq

Further properties of excludesAll

\textbf{lemma} excludesAll\_by\_iterate:
\begin{align*}
\text{OclExcludesAll } (Y; (\forall a,b. : \text{bot}) \text{Bag}) = \\
(Y \rightarrow \text{iterate}(x; y = \text{if } (\partial X) \text{ then } \text{T} \text{ else } \text{⊥} \text{ endif} \mid ((x; (\forall a,b. : \text{VAL}) \notin X) \land y))
\end{align*}
apply (simp add: excludesAll\_by\_iterate ss\_bag2seq)
apply (subst iterate\_bag2seq)
apply (simp_all add: \text{OCL\_is\_def\_OclAsSequence})
apply (auto, rule ext, auto simp: \text{OclSand\_def ss_lifting})
done

Select
defs

\text{OclSelect\_def: } \text{OclSelect} \equiv (\text{lift2}_\text{lift\_arg0} \text{lift\_arg1}) (\text{strictify } (\lambda S P. \\
if \forall x \in \text{set} \text{ of } \text{Rep\_Bag}_0 S. \text{DEF} (P x) \text{ then } \text{Abs\_Bag}_0 (\text{MCollect} \text{Rep\_Bag}_0 S \lambda x. P x = \text{True}) \text{ else } \perp))

\textbf{ocl\_setup\_op [OclSelect]}

Relating select on bags to its counterpart on sequences

\textbf{lemma} select\_bag2seq2bag:
\begin{align*}
(\text{OclSelect } (X; (\forall a,b. : \text{bot}) \text{Bag}) (P; (\forall a,b. : \text{VAL} \Rightarrow \text{'a } \text{Boolean}) = \\
(\text{OclAsBag } (\text{OclSelect } ((\text{OclAsSequence } X); (\forall a,b. : \text{Sequence}) P)))
\end{align*}
apply (rule ext)
apply (case_tac X x \neq \perp)
apply (frule \text{DEF\_X\_Bag}', clarify)
apply (auto simp: \text{OclAsSequence\_def OCL\_Sequence.\OclAsBag\_def} \text{OclSelect\_def OCL\_Sequence.\OclSelect\_def} \text{ss\_lifting})
done

\textbf{lemmas} ss\_bag2seq2bag = select\_bag2seq2bag

344
Further properties of select lemma \selectbyiterate:

\[(\forall x : (B : ('a, 'b :: bot) Bag) \mid ((P : ('a, 'b :: bot) VAL \Rightarrow 'a Boolean) x)) =
(B \rightarrow iterate(x, y = \{\} | if (P x) then (y \rightarrow including x) else y endif))\]

oops

Reject def

\[OclReject \equiv (lift2' lift_arg0 lift_arg1) (strictify (\lambda S P, if \forall x \in set_of 'Rep_Bag_0 S. DEF (P x) then Abs_Bag_0 ('MCollect 'Rep_Bag_0 S) (\lambda x. P x = \{False\})) else \bot))\]

ocl_setup_op [OclReject]

Excluding def

\[OclExcluding \equiv lift2 (strictify (\lambda X. strictify (\lambda Y. Abs_Bag_0 ('MCollect Rep_Bag_0 X) (\lambda a. a \neq Y)))))\]

ocl_setup_op [OclExcluding]

Collect

Note currently this collect corresponds to a collectNested. This will be fixed later.

defs

\[OclCollect \equiv (\lambda S P. if DEF (S \tau) then if \forall x \in set_of 'Rep_Bag_0 S. DEF (P (\lambda x. x \tau)) then Abs_Bag_0 'Abs_multiset ((count 'Rep_Bag_0 S) o (inv (\lambda x. P (lift0 x))))) else \bot else \bot)\]

ocl_setup_op [OclCollect]

One def

\[OclOne \equiv (S : ('a, ('b :: bot) Bag) VAL) P \equiv\]
Appendix B. Isabelle Theories

\( \|((x : S \mid P (x::'a::type \Rightarrow 'b::bot)))\| = 1 \)

ocl_setup_op [OctOne]

Sum

Like collect sum is specified as mapping to other ocl functions ...this is because for every type supporting plus, zero the sum function must be available and it make no sense to add a new definition for every one of these

defs

\( OclSum \_ \text{def} : \)

\( OclSum S \equiv OclIterate (S:('a,'b:(bot,plus,zero))Bag) (\lambda x y. x + y) \theta \)

Complement

defs

\( OclComplement \_ \text{def} : OclComplement \equiv \text{lift1} (\text{strictify}(\lambda X. Abs\_Bag\_0 (\_ , -(\text{Rep\_Bag\_0 } X) - \{\#\bot\#\}))) \)

ocl_setup_op [OclComplement]

Stuff that should be moved into the right theory

end

B.4.12. OCL OrderedSet

theory OCL\_OrderedSet
imports

$\text{HOLOCL\_HOME/src/library/collection/smashed/OCL\_Sequence}$

begin

Properties of the Congruence inside the Datatype Adaption

The following rules are transformed versions of the automatically generated rules for datatype conversions.

lemma Abs\_OrderedSet\_inj_charn:
\[
[ (\bot::'a::bot) \notin \text{set } x; (\bot::'a::bot) \notin \text{set } y; \text{distinct } x; \text{distinct } y ] \Longrightarrow
((\text{Abs\_OrderedSet\_0 } (x)) = (\text{Abs\_OrderedSet\_0 } (y))) = (x = y)
\]

by(subst Abs\_OrderedSet\_0_inject,

\text{simp \_all \ add: OrderedSet\_0\_def smash\_def})
B.4. Library

lemma Abs_OrderedSet_0_inject_absurd11 [simp]:
  \[ \bot \notin \text{set } x; \text{distinct } x \] \implies ((Abs_OrderedSet_0 down) = (Abs_OrderedSet_0 \downarrow x)) = False
by (subst Abs_OrderedSet_0_inject, simp_all add: OrderedSet_0_def smash_def)

lemma Abs_OrderedSet_0_inject_absurd12 [simp]:
  \[ \bot \notin \text{set } x; \text{distinct } x \] \implies ((Abs_OrderedSet_0 \downarrow x) = (Abs_OrderedSet_0 down)) = False
by (subst Abs_OrderedSet_0_inject, simp_all add: OrderedSet_0_def smash_def)

lemma Abs_OrderedSet_0_inject_absurd21 [simp]:
  \[ \bot \notin \text{set } x; \text{distinct } x \] \implies (\bot = (Abs_OrderedSet_0 \downarrow x)) = False
by (simp add: UU_OrderedSet_def)

lemma Abs_OrderedSet_0_inject_absurd22 [simp]:
  \[ \bot \notin \text{set } x; \text{distinct } x \] \implies ((Abs_OrderedSet_0 \downarrow x) = \bot) = False
by (simp add: UU_OrderedSet_def)

lemma Abs_OrderedSet_0_inverse_charn:
  assumes bottomCase:
    \[ \bot \notin \text{set } x; \text{distinct } x \] \implies P
  assumes listCase:
    \[ \forall y. (\bot = (Abs_OrderedSet_0 \downarrow y); \bot \notin \text{set } y; \text{distinct } y) \] \implies P
  shows P
apply (rule_tac x=x in Abs_OrderedSet_0_cases)
apply (case_tac x = \bot)
apply (frule not_down_exists_lift2 [THEN iffD1])
apply (rule_tac y=y in listCase)
done

lemma Abs_OrderedSet_0_cases_charn:
  assumes bottomCase:
    \[ x = \bot \] \implies P
  assumes listCase:
    \[ \forall y. (x = (Abs_OrderedSet_0 \downarrow y); \bot \notin \text{set } y; \text{distinct } y) \] \implies P
  shows P
apply (rule_tac x=x in Abs_OrderedSet_0_cases)
apply (case_tac x = \bot)
apply (frule not_down_exists_lift2 [THEN iffD1])
apply (rule_tac y=y in listCase)
done

347
Appendix B. Isabelle Theories

```ml
lemma Abs_OrderedSet_0_induct_charn:
  assumes bottomCase : P ⊥
  assumes stepCase : \( \forall y. ([ \bot \notin set y, \text{distinct} y] \implies P (Abs\_OrderedSet_0 \langle y \rangle)) \)
  shows P x
  apply (rule_tac x=x in Abs_OrderedSet_0_induct)
  apply (rule_tac x=Abs_OrderedSet_0 y in Abs_OrderedSet_0_cases_charn)
  apply (simp_all add: bottomCase stepCase)
  done

lemma inj_on_Abs_OrderedSet: inj_on Abs_OrderedSet_0 OrderedSet_0
  by (rule inj_on_inverseI, rule OrderedSet_0.Abs_OrderedSet_0_inverse)

lemma inj_Rep_OrderedSet: inj Rep_OrderedSet_0
  by (rule inj_on_inverseI, rule OrderedSet_0.Rep_OrderedSet_0_inverse)

lemma smashed_orderedSet_charn:
  \((\bot \notin set X \land \text{distinct} X) = \langle \langle X \rangle \in \text{OrderedSet}_0 \rangle\)
  by (unfold smash_def OrderedSet_0_def UU_OrderedSet_def, auto)

lemma UU_in_smashed_orderedSet [simp]:
  \(\bot \in \text{OrderedSet}_0\)
  by (unfold smash_def OrderedSet_0_def UU_OrderedSet_def, auto)

lemma down_in_smashed_orderedSet [simp]:
  down \in \text{OrderedSet}_0
  by (unfold smash_def OrderedSet_0_def UU_OrderedSet_def, auto)

lemma mt_in_smashed_orderedSet [simp]:
  \(\langle \langle \rangle \rangle \in \text{OrderedSet}_0\)
  by (unfold smash_def OrderedSet_0_def UU_OrderedSet_def, auto)

lemma DEF_Abs_OrderedSet:
  \(\forall X. ([ \bot \notin set X, \text{distinct} X] \implies \text{DEF} (Abs\_OrderedSet_0 \langle X \rangle))\)
  apply (unfold DEF_def UU_OrderedSet_def, simp)
  done

lemma DEF_Rep_OrderedSet:
  \(\forall X. \text{DEF} X \implies \text{DEF} (\text{Rep\_OrderedSet}_0 X)\)
  apply (unfold DEF_def UU_OrderedSet_def, auto)
  apply (drule_tac f = Abs_OrderedSet_0 in arg_cong)
  apply (simp add: Rep_OrderedSet_0_inverse)
  done

lemma not_DEF_Rep_OrderedSet:
  \(\forall X. \neg \text{DEF} X \implies \neg \text{DEF} (\text{Rep\_OrderedSet}_0 X)\)
  apply (unfold DEF_def UU_OrderedSet_def, auto)
  apply (simp add: Abs_OrderedSet_0_inverse)
  done
```

348
lemma exists_lift_OrderedSet:
\[ X. \text{DEF} X \implies \exists c. \text{Rep\_OrderedSet\_0} X = (\{c\}) \]
by (drule DEF_Rep_OrderedSet, simp add: DEF_X_up)

lemma exists_lift_OrderedSet2:
\[ X. \text{DEF} X \implies \exists c. \bot /\in \text{set} c \land \text{distinct} c \land \text{Rep\_OrderedSet\_0} X = (\{c\}) \]
apply (frule exists_lift_OrderedSet)
apply (clarify, simp)
apply (erule exists_lift_OrderedSet2)
apply (erule swapped_ordinarySet_charn [THEN iffD2])
done

lemma Rep_OrderedSet_cases:
\[ \text{Rep\_OrderedSet\_0} X = \bot \lor (\exists c. \bot /\in \text{set} c \land \text{distinct} c \land \text{Rep\_OrderedSet\_0} X = (\{c\})) \]
apply (case_tac DEF_X)
apply (drule exists_lift_OrderedSet2)
apply (erule not_DEF_Rep_OrderedSet)
done

lemma DEF_X_OrderedSet_0: \[ \text{DEF} X = (\exists c. \bot /\in \text{set} c \land \text{distinct} c \land \text{Rep\_OrderedSet\_0} X = (\{c\})) \]
apply (auto simp: DEF_Abs_OrderedSet)
apply (simp add: DEF_X_OrderedSet_0)
apply (erule exE, rule exI, auto)
apply (erule injD [OF inj_Rep_OrderedSet])
apply (auto simp: smashed_ordinarySet_charn Abs_OrderedSet_0_inverse)
done

The following lemma is crucial for the theory morpher:

lemma DEF_X_OrderedSet: \[ \text{DEF} X = (\exists c. \bot /\in \text{set} c \land \text{distinct} c \land X = \text{Abs\_OrderedSet\_0} \{c\}) \]
apply (auto simp: DEF_Abs_OrderedSet)
apply (simp add: DEF_X_OrderedSet_0)
apply (erule exE, rule exI, auto)
apply (rule injD [OF inj_Rep_OrderedSet])
apply (auto simp: slashed_ordinarySet_charn Abs_OrderedSet_0_inverse)
done

This lemma is very convenient in simplifying unfolded definitions

lemma DEF_X_OrderedSet':
\[ X \neq \bot \implies (\exists c. (\bot /\in \text{set} c) \land (\text{distinct} c) \land (\text{Rep\_OrderedSet\_0} X = (\{c\})) \land (\exists c. (\bot /\in \text{set} c) \land (\text{distinct} c) \land (X = (\text{Abs\_OrderedSet\_0} (\{c\}))))) \]
apply (fold DEF_def)

349
Appendix B. Isabelle Theories

apply (frule DEF_X_OrderedSet[THEN iffD1])
apply (drule DEF_X_OrderedSet_0[THEN iffD1])
apply (simp)
done

lemma OrderedSet_sem_cases_0:
assumes defC: \( \forall c \ d. \ \{ X \neq \bot; \bot \neq X; \\
(\bot \notin \text{set} \ c); (\bot \notin \text{set} \ d); \\
\text{distinct} \ c; \text{distinct} \ d; \\
\text{Rep}_{\text{OrderedSet}_0} X = \{c\}; \\
X = \text{Abs}_{\text{OrderedSet}_0} \{c\} \} \Rightarrow P X \)
and undefC: \( \{ X = \bot \} \Rightarrow P X \)
sows P X
apply (rule Abs_OrderedSet_0_cases_charn, erule undefC)
apply (rule defC, auto)
done

lemma OrderedSet_sem_cases:
assumes defC: \( \forall c \ d. \ \{ (X \tau) \neq \bot; \bot \neq (X \tau); \\
(\bot \notin \text{set} \ c); (\bot \notin \text{set} \ d); \\
\text{distinct} \ c; \text{distinct} \ d; \\
\text{Rep}_{\text{OrderedSet}_0} (X \tau) = \{c\}; \\
(X \tau) = \text{Abs}_{\text{OrderedSet}_0} \{c\} \} \Rightarrow P X \tau \)
and undefC: \( \{ (X \tau) = \bot \} \Rightarrow P X \tau \)
and cpP: cp P
shows P X \tau
apply (rule_tac P2=P in subst[OF sym[OF cp_subst]], rule cpP)
apply (rule_tac P1=P in subst[OF cp_subst], rule cpP)
apply (rule defC, prefer 9)
apply (rule_tac P1=P in subst[OF cp_subst], rule cpP)
apply (rule undefC, simp_all)
done

lemma OrderedSet_sem_cases_ext:
assumes defC: \( \forall c \ d \ \tau. \ \{ (X \tau) \neq \bot; \bot \neq (X \tau); \\
(\bot \notin \text{set} \ c); (\bot \notin \text{set} \ d); \\
\text{distinct} \ c; \text{distinct} \ d; \\
\text{Rep}_{\text{OrderedSet}_0} (X \tau) = \{c\}; \\
(X \tau) = \text{Abs}_{\text{OrderedSet}_0} \{c\} \} \Rightarrow P \ X \tau = Q \ X \tau \)
and undefC: \( \{ (X \tau) = \bot \} \Rightarrow P \ X \tau = Q \ X \tau \)
and cpP: cp P
and cpQ: cp Q
shows P X = Q X
apply (rule ext)
apply (rule_tac X=X in OrderedSet_sem_cases)
apply (rule defC, prefer 9)
apply (rule undefC)

350
apply(simp_all add: cpP cpQ)
done

These four lemmas are used by ocl_setup_op to reason about definedness:

lemma lift2_strict_is_isdef_fu_OrderedSet_Val:
assumes  f_def: \( f \equiv \text{lif2}(\text{strictify}(\lambda x. \text{strictify}(\lambda y. \text{Abs}_{\text{OrderedSet}_0}(g \upharpoonright_{\text{Rep}_{\text{OrderedSet}_0}} x) y))) \)
and  inv_g1: \( !a b. \left[ \bot \notin \text{set} \ a; \ \text{distinct} \ a; \ (\bot \cup a \cup \text{bot}) \neq b \right] \Rightarrow \bot \notin \text{set} \ (a \cup b) \)
and  inv_g2: \( !a b. \left[ \bot \notin \text{set} \ a; \ \text{distinct} \ a; \ (\bot \cup a \cup \text{bot}) \neq b \right] \Rightarrow \text{distinct} \ (a \cup b) \)
sows  \((f X Y) = (\partial X \land \partial Y)\)
apply(rule ext)
apply(simp add: f_def OclIsDefined_def OclAnd_def 
a_def ss_lifting')
apply(rule_tac X=X in OrderedSet_sem_cases_0)
apply(rule impl, frule_tac b=(Y x) in inv_g1)
apply(drule_tac[\( \beta \)] b=(Y x) in inv_g2)
apply(simp_all add: neq_commute)
done

lemma lift2_strict_is_isdef_fu_OrderedSet_OrderedSet:
assumes  f_def: \( f \equiv \text{lif2}(\text{strictify}(\lambda x. \text{strictify}(\lambda y. \text{Abs}_{\text{OrderedSet}_0}(g \upharpoonright_{\text{Rep}_{\text{OrderedSet}_0}} x) y))) \)
and  inv_g1: \( !a b. \left[ \bot \notin \text{set} \ a; \ \text{distinct} \ a; \ (\bot \cup a \cup \text{bot}) \neq b \right] \Rightarrow \bot \notin \text{set} \ (a \cup b) \)
and  inv_g2: \( !a b. \left[ \bot \notin \text{set} \ a; \ \text{distinct} \ a; \ (\bot \cup a \cup \text{bot}) \neq b \right] \Rightarrow \text{distinct} \ (a \cup b) \)
sows  \((f X Y) = (\partial X \land \partial Y)\)
apply(rule ext)
apply(simp add: f_def OclIsDefined_def OclAnd_def 
a_def ss_lifting')
apply(rule_tac X=X in OrderedSet_sem_cases_0)
apply(rule impl, frule_tac b=(Y x) in inv_g1)
apply(drule_tac[\( \beta \)] b=(Y x) in inv_g2)
apply(simp_all add: neq_commute)
done

lemma lift2_strictify_implies_LocalValid_defined_OrderedSet_Val:
assumes  f_def: \( f \equiv \text{lif2}(\text{strictify}(\lambda x. \text{strictify}(\lambda y. \text{Abs}_{\text{OrderedSet}_0}(g \upharpoonright_{\text{Rep}_{\text{OrderedSet}_0}} x) y))) \)
and  inv_g1: \( !a b. \left[ \bot \notin \text{set} \ a; \ (\bot \cup a \cup \text{bot}) \neq b \right] \Rightarrow \bot \notin \text{set} \ (a \cup b) \)
and  inv_g2: \( !a b. \left[ \bot \notin \text{set} \ a; \ (\bot \cup a \cup \text{bot}) \neq b \right] \Rightarrow \text{distinct} \ (a \cup b) \)
sows  \((\tau \equiv (f X Y)) = ((\tau \equiv \partial X) \land (\tau \equiv \partial Y))\)
apply(insert f_def)
apply(drule_tac X=X and Y=Y in lift2_strict_is_isdef_fu_OrderedSet_Val)
apply(assumption)+
apply(simp_all add: OclAnd_def OclTrue_def a_def 
OclIsDefined_def lif0_def lif1_def lif2_def 
OclLocalValid_def)
done

351
Appendix B. Isabelle Theories

lemma lift2_strictify_implies_LocalValid_defined_OrderedSet_OrderedSet:
assumes f_def:
\[ f \equiv \text{lift2}(\text{strictify}(\lambda x. \text{strictify}(\lambda y. \text{Abs_OrderedSet_0} \, \text{rep_S_n_}\, \text{g} \, \text{Rep_OrderedSet_0} \, x \, \text{rep_S_n_}\, \text{Rep_OrderedSet_0} \, y)) \]
and inv_g1:
\[ !a \, b. (\emptyset \notin \text{set a}; \text{distinct a}; \emptyset \notin \text{set b}; \text{distinct b} \implies \emptyset \notin \text{set (g a b)}) \]
and inv_g2:
\[ !a \, b. (\emptyset \notin \text{set a}; \text{distinct a}; \emptyset \notin \text{set b}; \text{distinct b} \implies \text{distinct (g a b)}) \]
shows \( \tau \models \partial(f \, X \, Y) = ((\tau \models \partial X) \land (\tau \models \partial Y)) \)
apply(insert f_def)
apply(drule_tac X=X and Y=Y in lift2_strict_is_isdef_fw_OrderedSet_OrderedSet)
apply(assumption)+
apply(simp add: OclAnd_def OclTrue_def o_def OclIsDefined_def lift0_def lift1_def lift2_def OclLocalValid_def)
done

Building a canonic representation of orderedSets

The empty orderedSet

constdefs
OclMtOrderedSet :: ('a, 'b:bot OrderedSet_0) VAL
OclMtOrderedSet \equiv lift0(Abs_OrderedSet_0 (\emptyset))

syntax
\_OclMtOrderedSet_std :: ('a, 'b:bot) VAL \Rightarrow 'a Boolean (OrderedSet)
syntax
\_OclMtOrderedSet_ascii :: ('a, 'b:bot) VAL \Rightarrow 'a Boolean (mtOrderedSet)
syntax (xsymbols)
\_OclMtOrderedSet_math :: ('a, 'b:bot) VAL \Rightarrow 'a Boolean (\langle\rangle)
parse_translation \{ (\text{\_flat(map (\text{\_\_emb trans_const}) [OclMtOrderedSet]))} \}
print_translation \{ (\text{\_map \_\_emb_print [OclMtOrderedSet]}) \}

lemma OCL_is_isdef_OclMtOrderedSet [simp]:
\( \models \partial(\emptyset) \)
by(simp add: OclValid_def OclIsDefined_def OclTrue_def OclMtOrderedSet_def ss_lifting)

lemma OCL_is_defopt_OclMtOrderedSet [simp]:
\( \tau \models \partial(\emptyset) \)
by(simp add: valid_elim)

And the ‘cons’ operation: including def

OclIncluding_def :
OclIncluding \equiv \text{lift2}(\text{strictify}(\lambda S. \text{strictify}(\lambda e. \text{Abs_OrderedSet_0} \, \text{rep_S_n_}\, (\text{remdups (concat ['\text{Rep_OrderedSet_0} \, S', [e]]))))))

352
ocl_setup_op \{OclIncluding\}

**lemma OCL_is_def_OclIncluding:**
\[\partial (OclIncluding (X::('a', 'b':bot)OrderedSet) (Y::('a', 'b':bot) VAL)) = (\partial X \land \partial Y)\]
*by (rule lift2_strict_is_isdef_fw_OrderedSet_Val[\{OF OclIncluding_def\}, simp_all]*)

**lemma OCL_is_defopt_OclIncluding:**
\[\tau \models (\partial (OclIncluding (X::('a', 'b':bot)OrderedSet) (Y::('a', 'b':bot) VAL))) = (\tau \models \partial X \land (\tau \models \partial Y))\]
*by* (rule lift2_strictify_implies_LocalValid_defined_OrderedSet_Val[\{OF OclIncluding_def\}, simp_all]*)

The syntax translation *mkOrderedSet* builds now our *orderedSets*

**syntax**
\[
\text{@OclFinOrderedSet :: } \text{args} \Rightarrow ('a', 'b' \text{OrderedSet}_0) VAL\]

**translations**
\[
\begin{align*}
\text{mkOrderedSet}[x, xs] & \equiv \text{OclIncluding (mkOrderedSet[xs]) } x \\
\text{mkOrderedSet}[x] & \equiv \text{OclIncluding OclMtOrderedSet } x
\end{align*}
\]

**lemma test :** *mkOrderedSet\{1,2,3,4,5\} = ?X oops*

**Relation of mtOrderedSet and including**

These two theorems should actually suffice to decide inequality of orderedSets

**lemma including_notstrongeq_mtOrderedSet[simp]:**
\[
\begin{align*}
\tau \models & \partial (X::('a', 'b':bot)\text{OrderedSet}) \rightarrow \text{including } (a::('a', 'b') VAL) \not\equiv () \\
\text{apply} & (\text{rule_tac } X=X \text{ in OrderedSet\_sem\_cases\_ext}) \\
\text{apply} & (\text{simp\_all add: cp_strongEq}) \\
\text{apply} & (\text{simp\_all add: OclIncluding\_def OclMtOrderedSet\_def OclStrongEq\_def}) \\
\end{align*}
\]

**done**

**lemma including_notstricteq_mtOrderedSet[simp]:**
\[
\begin{align*}
\tau \models & \partial (X::('a', 'b':bot)\text{OrderedSet}) \not\equiv (X \rightarrow \text{including } a) \not\equiv () \\
\text{apply} & (\text{rule_tac } X=X \text{ in OrderedSet\_sem\_cases}) \\
\text{apply} & (\text{simp\_all add: cp_strongEq cp_strictEq localValidDefined2sem}) \\
\end{align*}
\]

**done**
Appendix B. Isabelle Theories

A second orderedSet constructor on the OCL level

\[ \text{OclCollectionRange} \equiv \text{lift2} (\text{strictify} (\lambda x : \text{Integer}_0. \text{strictify} (\lambda y. \text{Abs}_\text{OrderedSet}_0 (\text{map} (\lambda z : \text{nat}. ((\text{int} z) + (\text{nat} y) - (\text{nat} x) + 1)))))) \]

\\[ \text{ocl_setup_op [OclCollectionRange]} \]

\text{lemma OCL_is_defopt_OclCollectionRange [simp]:}
\tau \models \emptyset (\text{OclCollectionRange} (\text{a} :: (\text{a Integer}) \text{b} :: (\text{a, Integer}_0) \text{OrderedSet}) = ((\tau \models \emptyset \text{a}) \land (\tau \models \emptyset \text{b}))
\]

\text{oops}

\text{lemma collectionRange_mtOrderedSet_conv:}
[ \tau \models (\text{b} :: (\text{a Integer}) < (\text{a :: (a Integer)}) ] \implies
\text{OclCollectionRange} \text{a b } \tau = (\text{OclCollectionRange} (\text{a} :: (\text{a Integer}) \text{b} :: (\text{a, Integer}_0) \text{OrderedSet}) \tau
\]
\text{apply (case_tac } \tau \models \emptyset \text{a, ocl_hypsubst, simp)}
\text{apply (case_tac } \tau \models \emptyset \text{b, ocl_hypsubst, simp)}
\text{apply (simp add: localValidDefined2sem DEF_def_both, clarify)}
\text{apply (simp_all add: DEF_def OclCollectionRange_def OclMtOrderedSet_def }\text{OclLess_def localValid2sem ss_lifting')} 
\text{done}

\text{lemma collectionRange_singleton_UC [simp]:}
\text{OclCollectionRange} \text{a a } = (\text{a :: (a Integer)}) \models \emptyset (\text{a, Integer}_0) \text{OrderedSet} \rightarrow \text{including} (\text{OclCollectionRange}_\text{def OclMtOrderedSet_def OclIncluding_def }\text{OclLess_def localValid2sem ss_lifting'})
\text{done}

\text{lemma collectionRange_expand_including:}
[ \tau \models (\text{a :: (a Integer)} \leq \text{b}) ] \implies
(\text{OclCollectionRange} \text{a b} :: (\text{a, Integer}_0) \text{OrderedSet}) \tau = (\text{OclCollectionRange} \text{a (b - 1)} \rightarrow \text{including b } \tau
\]
\text{oops}

The conversion operators

\text{OrderedSet to sequence}

\text{defs}
\[ \text{OclAsSequence} \equiv \text{lift1} (\text{strictify} (\lambda X.} \]

354
B.4. Library

\[ Abs\_Sequence\_0\ (Rep\_OrderedSet\_0\ X) \]

ocl_setup_op [OclAsSequence]

**OrderedSet to bag**

**defs**

\[
\begin{align*}
OclAsBag\_def & : \\
OclAsBag & \equiv \text{lift1} (\text{strictify} (\lambda X. Abs\_Bag\_0 (\text{multiset\_of} (Rep\_OrderedSet\_0\ X'))) )
\end{align*}
\]

ocl_setup_op [OclAsBag]

**OrderedSet to orderedSet**

**defs**

\[
\begin{align*}
OclAsOrderedSet\_def & : \\
OclAsOrderedSet & \equiv \text{id}
\end{align*}
\]

**lemma** asOrderedSet_identity[simp]:

\[
\text{OclAsOrderedSet } (S::(a,b:\text{bot})\text{OrderedSet}) = S
\]

by (simp add: OclAsOrderedSet_def)

**OrderedSet to set**

**defs**

\[
\begin{align*}
OclAsSet\_def & : \\
OclAsSet & \equiv \text{lift1} (\text{strictify} (\lambda X. Abs\_Set\_0 (\text{set\_of} (Rep\_OrderedSet\_0\ X'))) )
\end{align*}
\]

ocl_setup_op [OclAsSet]

end

B.4.13. **OCL Set**

theory **OCL_Set**

imports

$\text{HOLOCL\_HOME}/\text{src}/\text{library}/\text{collection}/\text{smashed}/\text{OCL\_Bag}$

$\text{HOLOCL\_HOME}/\text{src}/\text{library}/\text{collection}/\text{smashed}/\text{OCL\_OrderedSet}$

begin

Is **OCL Set** Faithful to the **OCL Standard**?

Unlike the basic library theories, for this first and foundational "Collection"-type theory the question of faithfulness is not merely a syntactic matter (like fusing various
Appendix B. Isabelle Theories

semantic interpretation functions into one). In fact, it is not even trivial to answer. This is mainly for two reasons:

1. We generalize the concept of Set as required by OCL 2.0 to infinite sets.

2. We interpret the standard with respect to the question, if OclUndefind can be included in a set or not: we deny this question in this version of a set theory.

The first decision has the advantage, that general Sets can be used to represent the syntactic category of "types" in the standard as "characteristic sets" in HOL and enables the possibility to reason over them. From the pragmatics point of view, this also allows for quantifications of sets of "values" in the sense of OCL 2.0. For example, it is possible in HOL-OCL to express the commutativity law on Integers inside OCL.

The second decision is due to the fact that the standard avoids a clear statement to the nature of undefinedness in OCL. This led to two forms of interpretations by users and tool-developers: is OclUndefind just "null", so the null-reference, or is it a semantic construct denoting non-termination or exceptional behaviour? In the former sense, it is possible to include OclUndefind in a set, in the latter not. Admitting undefinedness in sets also has consequences in the inclusion operation and the elementhood test (including and includes). The operational behaviour of Java-implementations reflects the latter view, which we chose therefore as default. Semantically, this leads to a quotient construction (called "smashing" in the literature) which identifies \{x, ⊥\} with ⊥.

With respect to the question of faithfulness of our OCL semantics we have the following answers:

1. the required properties of OCL 2.0 should hold in our setting for finite sets, and

2. the subtle issue of ⊥s in sets is not mentioned at all in them.

Therefore, we show compliance in this sense by providing the individual proof for these "required properties". However, we will only use them in rare cases in definitions and provide a number of other properties for them that are more suited for automated reasoning.

Foundational Properties of the smash-construction

Global OCL type constructor for OCL Set types:

types    \text{\langle}'\tau, '\alpha\text{\rangle}\text{Set} = \text{\langle}'\tau, '\alpha\text{Set}_0\text{\rangle} Val

Properties of the Congruence inside the Datatype Adaption

lemma Abs_Set_inject_absurd11 [simp]:
[ ⊥ \notin x ] \Longrightarrow ((Abs_Set_0 down) = (Abs_Set_0 \downarrow x)) = False
by (subst Abs_Set_0_inject, simp_all add: OCL_Set_type.Set_0_def smash_def)

lemma Abs_Set_0_inject_absurd12 [simp]:
B.4. Library

\[
\begin{align*}
\llbracket \bot \notin x \rrbracket & \implies ((\text{Abs}_\text{Set}_0 (x)) = (\text{Abs}_\text{Set}_0 \downarrow)) = \text{False} \\
\text{by (subst Abs}_\text{Set}_0 \text{\_inject, simp\_all add: OCL\_Set\_type.Set}_0 \text\_def smash\_def)}
\end{align*}
\]

Lemma Abs\_Set\_0\_inject\_absurd21 [simp]:
\[
\llbracket \bot \notin x \rrbracket \implies (\bot = (\text{Abs}_\text{Set}_0 (x))) = \text{False} \\
\text{by (simp add: UU\_Set\_def)}
\]

Lemma Abs\_Set\_0\_inject\_absurd22 [simp]:
\[
\llbracket \bot \notin x \rrbracket \implies ((\text{Abs}_\text{Set}_0 (x) = \bot)) = \text{False} \\
\text{by (simp add: UU\_Set\_def)}
\]

Lemma Abs\_Set\_0\_inject\_charn:
\[
\llbracket (\bot::\alpha::\bot) \notin x; (\bot::\alpha::\bot) \notin y \rrbracket \implies ((\text{Abs}_\text{Set}_0 (x) = (\text{Abs}_\text{Set}_0 (y))) = (x = y)) \\
\text{by (subst Abs}_\text{Set}_0 \text\_inject, simp\_all add: OCL\_Set\_type.Set}_0 \text\_def smash\_def)}
\]

Lemma Abs\_Set\_0\_inverse\_charn1 [simp]:
\[
(\bot \notin x) \implies \text{Rep\_Set}_0 (\text{Abs}_\text{Set}_0 (x)) = x \\
\text{by (subst Abs}_\text{Set}_0 \text\_inverse, simp\_all add: OCL\_Set\_type.Set}_0 \text\_def smash\_def)}
\]

Lemma Abs\_Set\_0\_inverse\_charn2 [simp]:
\[
(\bot \notin x) \implies \text{Rep\_Set}_0 (\text{Abs}_\text{Set}_0 (x)) = x \\
\text{by (subst Abs}_\text{Set}_0 \text\_inverse, simp\_all add: OCL\_Set\_type.Set}_0 \text\_def smash\_def)}
\]

Lemma Abs\_Set\_0\_cases\_charn:
\[
\begin{align*}
\text{assumes bottomCase : } & [x = \bot] \implies P \\
\text{assumes listCase : } & \forall y. ([x = \text{Abs}_\text{Set}_0 (y) ; \bot \notin y] \implies P) \\
\text{shows } & P \\
\text{apply (rule_tac x=x in Abs\_Set\_0\_cases)} \\
\text{apply (case\_tac y = \bot)} \\
\text{apply (rule bottomCase, simp add: UU\_Set\_def)} \\
\text{apply (rule not\_down\_exists\_lift[THEN iffD1])} \\
\text{apply (rule_tac y="y" in listCase)} \\
\text{apply (auto simp: OCL\_Set\_type.Set}_0 \text\_def smash\_def)}
\end{align*}
\]
done

Lemma Abs\_Set\_0\_induct\_charn:
\[
\begin{align*}
\text{assumes bottomCase : } & P \bot \\
\text{assumes stepCase : } & \forall y. ([\bot \notin y] \implies P (\text{Abs}_\text{Set}_0 (y))) \\
\text{shows } & P \ x \\
\text{apply (rule_tac x=x in Abs\_Set\_0\_induct)} \\
\text{apply (rule_tac x=Abs\_Set\_0 y in Abs\_Set\_0\_cases\_charn)} \\
\text{apply (auto intrl: bottomCase elim: stepCase)}
\end{align*}
\]
done

357
Appendix B. Isabelle Theories

the rest

**Lemma inj_on_Abs_Set**: inj on Abs Set 0 OCL Set type Set 0

by (rule inj_on_inverseI, rule Set 0.Abs Set_0 inverse, assumption)

**Lemma inj_Rep_Set**: inj Rep Set 0

by (rule inj_on_inverseI, rule Set 0.Rep Set_0 inverse)

**Lemma smashed_set_charn**: \( \bot \notin X \Rightarrow (\{X\} \in OCL Set type Set 0) \)

by (unfold smash_def OCL Set type.Set 0 def UU_Set_def, auto)

**Lemma UU_in_smashed_set**: \( \bot \in OCL Set type Set 0 \)

by (unfold smash_def OCL Set type.Set 0 def UU_Set_def, auto)

**Lemma down_in_smashed_set**: down : OCL Set type Set 0

by (unfold smash_def OCL Set type.Set 0 def UU_Set_def, auto)

**Lemma mt_in_smashed_set**: \{\} \in OCL Set type Set 0

by (unfold smash_def OCL Set type.Set 0_def, auto)

Universal sets are never in OCL Set type.Set 0, since they must contain bottom elements (HOL’s type discipline forces UNIV to be of type ‘α::bot set) and therefore their smashed value is \( \bot \).

**Lemma UNIV_notin_smashed_set**: \( \bot \notin OCL Set type Set 0 \)

by (simp add: smash_def OCL Set type.Set 0_def)

In contrast, the set consisting of all 1-lifted elements is in OCL Set type.Set 0. This justifies the construction of characteristic sets for Boolean, Integer, Real, and String.

**Lemma liftUNIV_in_smashed_set**: lift ‘ UNIV \in OCL Set type Set 0

by (auto simp: smash_def OCL Set type.Set 0_def)

**Lemma DEF Abs Set**: \( \bot \notin X \Rightarrow DEF (Abs Set_0 (\{X\})) \)

by (simp add: DEF_def)

**Lemma DEF_Rep_Set**: DEF X \Rightarrow DEF (Rep Set_0 X)

apply (unfold DEF_def UU_Set_def,auto)
apply (drule_tac f = Abs Set_0 in arg_cong)
apply (simp add: Rep Set_0_inverse)
done

**Lemma not_DEF_Rep_Set**: \( \neg DEF X \Rightarrow \neg DEF (Rep Set_0 X) \)

apply (unfold DEF_def UU_Set_def,auto)
apply (simp add: Abs Set_0_inverse)
done

358
lemma exists_lift_Set: DEF X \implies \exists c. \Rep_Set_0 X = (\angle c \rangle)
by (drule DEF_Rep_Set,simp add: DEF_X_up)

lemma exists_lift_Set2: DEF X \implies \exists c. \bot \notin c \land \Rep_Set_0 X = (\angle c \rangle)
apply (frule exists_lift_Set)
apply (auto simp: smashed_set_charn)
apply (drule_tac \[2\] not_DEF_Rep_Set)
apply (simp_all add: DEF_def)
done

lemma Rep_Set_cases: \Rep_Set_0 X = \bot \lor (\exists c. \bot \notin c \land \Rep_Set_0 X = (\angle c \rangle))
apply (case_tac DEF X)
apply (drule exists_lift_Set2)
apply (simp_all add: Rep_Set_0)
apply (erule exE)
apply (rule exI)
apply (simp_all add: smashed_set_charn)
apply (rule injD [OF inj_Rep_Set])
apply (auto simp: Abs_Set_0_inverse)
done

lemma DEF_X_Set_0 : DEF X = (\exists c. \bot \notin c \land \Rep_Set_0 X = (\angle c \rangle))
apply (auto simp: DEF_Abs_Set smashed_set_charn)
apply (simp add: DEF_X_Set_0)
apply (rule not_DEF_Rep_Set, auto)
done

The following lemma is crucial for the theory morpher:

lemma DEF_X_Set: DEF X = (\exists c. \bot \notin c \land X = \Abs_Set_0 (\angle c \rangle))
apply (auto simp: DEF_Abs_Set smashed_set_charn)
apply (simp add: DEF_X_Set_0)
apply (erule exE, rule exI)
apply (simp_all add: Abs_Set_0_inverse)
done

lemma \[simp\]: \bot \notin ca \implies \Rep_Set_0 (\Abs_Set_0 (\lift ' \UNIV, \angle ca \rangle) = (\angle ca \rangle)
apply (rule Abs_Set_0_inverse)
apply (simp add: smash_def OCL_Set_type.Set_0_def)
done

lemma RepAbs_UNIV[\[simp\]]:
\Rep_Set_0 (\Abs_Set_0 (\lift \lift ' \UNIV, \angle ca \rangle) = (\lift ' \UNIV)
apply (simp_all add: Abs_Set_0_inverse liftUNIV_in_smashed_set)
done
Appendix B. Isabelle Theories

lemma Abs_Set_rangelift_DEF:\[simp\]:
DEF(Abs_Set_0.range lift)
by(auto simp: DEF_X_Set_0)

lemma DEF_X_Set':
\[
\begin{align*}
\text{DEF':} & \quad (X \neq \bot) \implies \\
& \quad (\exists c. \bot \notin c) \land (\text{Rep}_X c = (X\tau)) \\
& \quad (\exists d. \bot \notin d) \land (X = (\text{Abs}_X d))
\end{align*}
\]
apply(fold DEF_def)
apply(frule DEF_X_Set[THEN iffD1])
apply(drule DEF_X_Set_0[THEN iffD1])
apply(simp)
done

lemma Set_sem_cases_0:
assumes defC: \[\forall c d. (X \neq \bot) \land (\bot \notin c) \\
& \quad (\bot \notin d) \land (\text{Rep}_X c = (X\tau)) \\
& \quad (X = (\text{Abs}_X d)) \implies P X\]
and undefC: \[\forall c d. (X = \bot) \implies P X\]
sows P X
apply(rule Abs_Set_0_cases_charn, erule undefC)
apply(rule defC, auto)
done

lemma Set_sem_cases:
assumes defC: \[\forall c d. (X\tau \neq \bot) \land (\bot \notin c) \\
& \quad (\bot \notin d) \land (\text{Rep}_X c = (X\tau)) \\
& \quad (X\tau = (\text{Abs}_X d)) \implies P X\tau\]
and undefC: \[\forall c d. (X\tau = \bot) \implies P X\tau\]
and cpP: cp P
shows P X\tau
apply(rule_tac P2=P in subst[OF sym[OF cp_subst]], rule cpP)
apply(rule_tac P1=P in subst[OF cp_subst], rule cpP)
apply(rule defC) prefer 7
apply(rule_tac P1=P in subst[OF cp_subst], rule cpP)
apply(rule undefC, simp_all)
done

lemma Set_sem_cases_ext:
assumes defC: \[\forall c d. \tau. (X\tau \neq \bot) \land (\bot \notin c) \\
& \quad (\bot \notin d) \land (\text{Rep}_X c = (X\tau)) \\
& \quad (X\tau = (\text{Abs}_X d)) \implies P X\tau = Q X\tau\]

360
and undefC: \[ \forall \tau. (X \tau = \bot) \Rightarrow P X \tau = Q X \tau \]
and cpP: cp P
and cpQ: cp Q
shows \[ P X = Q X \]
apply(rule ext)
apply(rule_tac X=X in Set_sem_cases)
apply(rule defC) prefer 7
apply(rule undefC)
apply(simp_all add: cpP cpQ)
done

These four lemmas are used by ocl_setup_op to reason about definedness:

lemma lift2_strict_is_isdef_fw_Set_Val:
assumes f_def: \( f \equiv \text{lift2}(\text{strictify}(\lambda x. \text{strictify}(\lambda y. \text{Abs_Set_0} g \text{Rep_Set_0} x y))) \)
and inv_g: \( \forall a b. (\bot \in a; (\bot :: \alpha :: \text{bot}) \neq b) \Rightarrow \bot \in (g a b) \)
shows \( \partial(f X Y) = (\partial X \land \partial Y) \)
apply(simp add: f_def OclIsDefined_def OclAnd_def
\quad o_def lift0_def lift1_def lift2_def
\quad strictify_def DEF_def)
apply(rule ext)
apply(case_tac DEF (X \tau))
apply(erule DEF_X_Set_0 [THEN iffD1])
apply(auto simp: strictify_def DEF_def)
apply(drule_tac b=(Y \tau) in inv_g)
prefer 2
apply(drule DEF_Abs_Set, simp add: DEF_def, auto)
done

lemma lift2_strict_is_isdef_fw_Set_Set:
assumes f_def: \( f \equiv \text{lift2}(\text{strictify}(\lambda x. \text{strictify}(\lambda y. \text{Abs_Set_0} g \text{Rep_Set_0} x y))) \)
and inv_g: \( \forall a b. (\bot \in a; \bot \in b) \Rightarrow \bot \in (g a b) \)
shows \( \partial(f X Y) = (\partial X \land \partial Y) \)
apply(simp add: f_def OclIsDefined_def OclAnd_def
\quad o_def lift0_def lift1_def lift2_def
\quad strictify_def DEF_def)
apply(rule ext)
apply(case_tac DEF (X \tau))
apply(case_tac DEF (Y \tau))
apply(auto simp: strictify_def DEF_def)
apply(drule_tac b=ca in inv_g, assumption)
apply(rotate_tac -1)
apply(drule DEF_Abs_Set, simp add: DEF_def)
done

lemma lift2_strictify_implies_LocalValid_defined_Set_Val:
assumes f_def: \( f \equiv \text{lift2}(\text{strictify}(\lambda x. \text{strictify}(\lambda y. \text{Abs_Set_0} g \text{Rep_Set_0} x y))) \)
and inv_g: \( \forall a b. (\bot \in a; (\bot :: \alpha :: \text{bot}) \neq b) \Rightarrow \bot \in (g a b) \)
shows \( \partial(f X Y) = (\partial X \land \partial Y) \)
apply(simp add: f_def OclIsDefined_def OclAnd_def
\quad o_def lift0_def lift1_def lift2_def
\quad strictify_def DEF_def)
apply(rule ext)
apply(case_tac DEF (X \tau))
apply(case_tac DEF (Y \tau))
apply(auto simp: strictify_def DEF_def)
apply(drule DEF_X_Set_0 [THEN iffD1])
apply(auto simp: strictify_def DEF_def)
apply(drule_tac b=ca in inv_g, assumption)
apply(rotate_tac -1)
apply(drule DEF_Abs_Set, simp add: DEF_def)
done

361
Appendix B. Isabelle Theories

shows $(\tau \models \partial (f \times Y)) = ((\tau \models \partial X) \land (\tau \models \partial Y))$
apply(insert f_def)
apply(drule_tac X=X and Y=Y in lift2_strict_is_isdef_fw_Set_Val)
apply(rule inv_g, assumption+)
apply(simp add: OclAnd_def OclTrue_def o_def
            OclIsDefined_def lift0_def lift1_def lift2_def
            OclLocalValid_def)
done

lemma lift2_strictify_implies_LocalValid_defined_Set_Set:
assumes f_def: $f \equiv \text{lift2} (\text{strictify} (\lambda x. \text{Abs}_{\text{Set}}_0 (\text{list_of_set} (\text{Rep}_{\text{Set}}_0 X)))$)
and inv_g: $!a b. [ \bot \notin a; \bot \notin b \implies \bot \notin (g a b)]$
shows $(\tau \models \partial (f \times Y)) = ((\tau \models \partial X) \land (\tau \models \partial Y))$
apply(insert f_def)
apply(drule_tac X=X and Y=Y in lift2_strict_is_isdef-fw_Set_Set)
apply(rule inv_g, assumption+)
apply(simp add: OclAnd_def OclTrue_def o_def
            OclIsDefined_def lift0_def lift1_def lift2_def
            OclLocalValid_def)
done

The conversion operators

From sets to sequences
Because there is no ordering on the elements of the sets the *AsSequence* operator
chooses some sequence which has exactly the same elements as the set.
Because this is just some sequence the proof about statements containing the *AsSe-
quence* operator, have to show the same properties as one has to show for the general
Hilbert Choice operator.
defs

\begin{center}
\begin{align*}
\text{OclAsSequence} & \quad \equiv \text{lift1} (\text{strictify} (\lambda X. \text{Abs}_{\text{Sequence}}_0 (\text{list_of_set} (\text{Rep}_{\text{Set}}_0 X))) \\
\text{ocl_setup_op} & \quad [\text{OclAsSequence}]
\end{align*}
\end{center}

From sets to bags
defs

\begin{center}
\begin{align*}
\text{OclAsBag} & \quad \equiv \text{lift1} (\text{strictify} (\lambda X. \text{Abs}_{\text{Bag}}_0 (\text{multiset_of_set} (\text{Rep}_{\text{Set}}_0 X))) \\
\text{ocl_setup_op} & \quad [\text{OclAsBag}]
\end{align*}
\end{center}

From sets to ordered sets
defs

\begin{center}
\begin{align*}
\text{OclAsOrdered} & \quad \equiv \text{lift1} (\text{strictify} (\lambda X. \text{Abs}_{\text{Ordered}}_0 (\text{Rep}_{\text{Set}}_0 X))) \\
\text{ocl_setup_op} & \quad [\text{OclAsOrdered}]
\end{align*}
\end{center}
B.4. Library

\[
\text{OclAsOrderedSet} \equiv \text{lift1 (strictify (λX. Abs.OrderedSet_0 (list_of_set 'Rep.Set_0 X))})
\]

ocl_setup_op [OclAsOrderedSet]

lemma bag2seq2oset_eq_bag2set2oset:
\[
\begin{align*}
\text{asOrderedSet}() ((\text{asSequence()} (B::('τ,'α::bot)Bag))::('τ,'α)Sequence) &= \\
((\text{asOrderedSet()}) ((\text{asSet()} B)::('τ,'α)Set))::('τ,'α)OrderedSet
\end{align*}
\]
apply(rule ext)
apply(case_tac x ⊨ ∅ B, ocl_hypsubst, simp)
apply(simp add: localValidDefined2sem DEF_def_both, clarify)
apply(rule DEF_X_Bag', clarify)
apply(simp add: OCL_Bag.OclAsSequence_def OCL_Bag.OclAsSet_def
OCL_Sequence.OclAsOrderedSet_def
OCL_Set.OclAsOrderedSet_def ss_lifting')
apply(subst Abs_OrderedSet_0_inject_charn)
apply(simp_all add: rev_remdups rev_remstutter[symmetric])
done

lemma oset2seq2bag_eq_oset2set2bag:
\[
\begin{align*}
\text{asBag()} ((\text{asSequence()} (X::('τ,'α::bot)OrderedSet))::('τ,'α)Sequence) &= \\
((\text{asBag()}) ((\text{asSet()} X)::('τ,'α)Set))::('τ,'α)Bag
\end{align*}
\]
apply(rule OrderedSet_sem_cases_ext, simp_all)
apply(simp_all add: OCL_OrderedSet.OclAsSequence_def OCL_OrderedSet.OclAsSet_def
OCL_Sequence.OclAsBag_def
OCL_Set.OclAsBag_def ss_lifting')
done

From sets to sets
defs

\[
\begin{align*}
\text{OclAsSet} \equiv \text{id}
\end{align*}
\]

lemma set2set_id [simp]:
\[
((\text{OclAsSet} (B::('τ,'α::bot)Set))::('τ,'α)Set) = B
\]
by(simp add: OclAsSet_def)

The Definition of the Set Operators

The Powerset Operator
defs

\[
\begin{align*}
\text{Set} &:: ('st, ('α::bot) Set_0) VAL \Rightarrow ('st, 'α Set_0 Set_0) VAL \\
\text{Set} &\equiv \text{lift1 (strictify (λX. Abs.Set_0 (Abs.Set_0 o lift) 'x. x ⊆ 'Rep.Set_0 X))})
\end{align*}
\]

ocl_setup_op [Set]
Appendix B. Isabelle Theories

lemma Set_defined :
τ ⊨ ∅ X ⇒ τ ⊨ ∅(Set X)
apply(simp add: Set_def localValidDefined2sem)
apply (auto simp: strictify_def
    o_def lift0_def lift1_def lift2_def image_def
    OclTrue_def OclFalse_def OclUndefined_def)
apply (rule DEF_Abs_Set, simp)
apply (rule allI, rule impI)
apply (rule neq_commute[THEN iffD1])
apply (rule DEF_Abs_Set[symmetric])
apply (rule DEF_Abs_Set, simp)
apply (rule exists_lift_Set2, auto)
done

lemma Set_definedR :
(τ ⊨ ∅(Set X)) = (τ ⊨ ∅ X)
apply (auto simp: Set_defined)
oops

The Empty Set
constdefs
  OclMtSet :: (′τ, ′α::bot Set_0) VAL
  OclMtSet ≡ lift0(Abs_Set_0(⌞{}⌟))

syntax
  _OclMtSet_std :: (′τ, ′α::bot) VAL ⇒ ′τ Boolean ({} ()
syntax
  _OclMtSet_ascii :: (′τ, ′α::bot) VAL ⇒ ′τ Boolean (mtSet)
syntax (xsymbols)
  _OclMtSet_math :: (′τ, ′α::bot) VAL ⇒ ′τ Boolean (∅ ()

Foundational Properties of MtSet
lemma Abs_Set_Mt_DEF[simp]:
DEF(Abs_Set_0(⌞{}⌟))
by(simp add: DEF_X_Set_0)

lemma mtSet_DEFINED [simp]:
∅ T
by(simp add: localValidDefined2sem Abs_Set_Mt_DEF OclMtSet_def
  OclIsDefined_def lift1_def lift0_def OclTrue_def)

Foundational Properties of includes and excludes
defs

  OclIncludes_def : OclIncludes ≡ lift2 (strictify (λX. strictify (λx.

364
B.4. Library

\( \forall x \in \text{Rep}_0(X') \))

\textit{OclExcludes} def: \( \text{OclExcludes} \equiv \text{lift2} (\text{strictify} \ (\lambda X. \text{strictify} \ (\lambda x. x \notin \text{Rep}_0(X'))) \))

\texttt{ocl_setup_op [OclIncludes, OclExcludes]}

\textbf{lemma includes_charn1 :} \( (\tau \models x \in S) \implies (x \tau \in \text{Rep}_0(S \tau)) \)
\begin{itemize}
  \item \texttt{apply (frule isDefined_if_valid, \texttt{drule OCL_is_defopt_OclIncludes[THEN iffD1])}}
  \item \texttt{apply (simp add: OclLocalValid_def OclIsDefined_def strictify_def OclNot_def lift0_def lift1_def lift2_def OclTrue_def OclFalse_def OclUndefined_def DEF_def)}
\end{itemize}
\texttt{done}

\textbf{lemma includes_charn2 :} \( \left[ \text{DEF}(S \tau); x \tau \in \text{Rep}_0(S \tau) \right] \implies \tau \models x \in S \)
\begin{itemize}
  \item \texttt{apply (frule DEF_X_Set[THEN iffD1], erule exE)}
  \item \texttt{apply (simp add: OclLocalValid_def OclIsDefined_def strictify_def OclNot_def lift0_def lift1_def lift2_def OclTrue_def OclFalse_def OclUndefined_def DEF_def)}
\end{itemize}
\texttt{apply auto}
\texttt{done}

\textbf{Higher Properties of includes and excludes}

\textbf{lemma excludes_not_includes[simp]:}
\( x \notin X = \neg (x; ('\tau, 'a)\text{VAL}) \in (X; ('\tau, 'a;\text{bot}) \text{Set}) \)
\begin{itemize}
  \item \texttt{apply (rule ext)}
  \item \texttt{apply (simp add: OclExcludes_def OclIncludes_def)}
  \item \texttt{apply (simp only: OclNot_def)}
\end{itemize}
\texttt{done}

\textbf{lemma mtSet_Includes_charn :}
\( \tau \models \emptyset \models x \implies x; ('\tau, 'a)\text{VAL} \notin (\emptyset; ('\tau, 'a;\text{bot}) \text{Set}) \)
\begin{itemize}
  \item \texttt{apply (simp add: localValValidDefined2sem)}
  \item \texttt{apply (simp only: excludes_not_includes OclMtSet_def OclLocalValid_def OclIncludes_def lift0_def lift1_def lift2_def)}
\end{itemize}
\texttt{done}

365
Appendix B. Isabelle Theories

\[\text{strictify_def \ o_def OclNot_def OclTrue_def DEF_def}\]
\[\text{apply(simp add: Abs_Set_Mt_DEF [simplified DEF_def] strictify_def)}\]
\text{done}

\begin{itemize}
  \item \textbf{lemma} \textit{X in Set X}:
  \[\tau \models (S:(\tau,\alpha::\bot)Set) \implies \tau \models S \in (\text{Set } S)\]
  \text{oops}

  \item \textbf{lemma} \textit{mtSet in Set}:
  \[\tau \models (S:(\tau,\alpha::\bot)Set) \implies \tau \models (\emptyset:(\tau,\alpha::\bot)Set) \in (\text{Set } S)\]
  \text{oops}
\end{itemize}

\textbf{Consequences of Smashedness of Sets}

This is the characteristic property of smashed sets: if \textit{X ->includes(x)} is valid, we know that \textit{x} must be defined.

\begin{itemize}
  \item \textbf{lemma} \textit{smashed_sets_charn}:
  \[\tau \models (x::(\tau,\alpha)\text{VAL}) \in (X:(\tau,\alpha::\bot)Set) \implies \tau \models \partial x\]
  \text{apply(simp add: OclIncludes_def lift2_def lift1_def lift0_def}
  \text{strictify_def OclTrue_def OclIsDefined_def o_def OclLocalValid_def)}\]
  \text{apply(case_tac X \tau = \bot, auto)}
  \text{apply(simp add: strictify_def DEF_def)}
  \text{apply(case_tac x \tau = \bot, auto)}
  \text{done}
\end{itemize}

\textbf{Fundamental Theorem on (infinite) Sets}

\begin{itemize}
  \item \textbf{lemma} \textit{Set_Ext0}:
  \[\forall x::(\tau,\alpha)\text{VAL}. \tau \models \partial x \implies (x \in (S:(\tau,\alpha::\bot)Set)) \tau = (x \in T)\tau\]
  \text{apply(simp add: OclIncludes_def lift2_def lift1_def lift0_def}
  \text{strictify_def OclTrue_def OclIsDefined_def o_def OclLocalValid_def)}\]
  \text{apply(case_tac S \tau = \bot, auto)}
  \text{apply(case_tac T \tau = \bot, auto)}
  \text{apply(insert exists_DEF, auto)}
  \text{apply(case_tac T \tau = \bot, auto)}
  \text{apply(simp add: DEF_def[symmetric])}
  \text{apply(frule DEF_Rep_Set)}
  \text{apply(frule DEF_Rep_Set) back}
  \text{apply(simp add: DEF_X_Set)}
  \text{apply auto}
  \text{apply(rule_tac f = \lambda c. Abs_Set_0 \lhd \in arg_cong)}
  \text{apply(rule set_ext)}
  \text{apply(crule_tac x=\lambda r, xa in allE)}
  \text{apply(case_tac x=\bot, simp_all add: DEF_def[symmetric])}
\end{itemize}

366
apply \((\text{auto simp: DEF_def})\)
done

lemma \texttt{Set_Ext} :
assumes \(H : \forall x : ((\tau, 'a::bot)\text{Set})\). \tau \ni \varnothing \Rightarrow (x \in (S : (\tau, 'a::bot)\text{Set}))\tau = (x \in T)\tau\)
shows \(S \tau = T \tau\)
apply (\text{rule Set_Ext0}) back
by (\text{auto intro: } H)

Semantic Definitions of the Standard Set Operations
defs

\begin{align*}
\text{OclSize_def} & : (\text{OclSize : } (\tau, 'a::bot)\text{Set_0}) \text{VAL } \Rightarrow \tau \text{ Integer} \equiv \\
& (\text{lift1 (strictify (} \lambda X. \\
& \text{if infinite } Rep\text{._0 }X \text{ then } \bot \\
& \text{ else } (\text{int(card(} Rep\text{._0 }X \text{))))}}))
\end{align*}

\begin{align*}
\text{OclCount_def} & : \text{OclCount } \equiv \text{lift2 (strictify (} \lambda X. \text{strictify (} \lambda x. \\
& (\text{if } x \in Rep\text{._0 }X \text{ then int } 1 \\
& \text{ else int } 0)))))
\end{align*}

\begin{align*}
\text{OclIncludesAll_def} & : \text{OclIncludesAll } \equiv \text{lift2 (strictify (} \lambda X. \text{strictify (} \lambda Y . \\
& (\text{Rep\text{._0 }X \subseteq Rep\text{._0 }Y)))}
\end{align*}

\begin{align*}
\text{OclExcludesAll_def} & : \text{OclExcludesAll } \equiv \text{lift2 (strictify (} \lambda X. \text{strictify (} \lambda Y . \\
& (\text{Rep\text{._0 }X \cap Rep\text{._0 }Y} = \{}))
\end{align*}

\begin{align*}
\text{OclIsEmpty_def} & : \text{OclIsEmpty } \equiv \text{lift1 (strictify (} \lambda X. \\
& (\{} = Rep\text{._0 }X \}))
\end{align*}

\begin{align*}
\text{OclNotEmpty_def} & : \text{OclNotEmpty } \equiv \text{lift1 (strictify (} \lambda X. \\
& (\{} \neq Rep\text{._0 }X \}))
\end{align*}

defs

\begin{align*}
\text{OclSum_def} & : \text{OclSum (self : (} \tau, 'a::bot)\text{Set_0) VAL} \equiv \bot
\end{align*}

\texttt{ocl_setup_op [OclSize, OclCount, OclIncludesAll, OclExcludesAll, OclIsEmpty, OclNotEmpty]}

sum wrongly defined in the standard: idempotence
Appendix B. Isabelle Theories

defs

\begin{align*}
\text{Ocl Flatten def } & \quad \text{(Ocl Flatten : (}'\tau', 'a :: \text{bot Set}_0 \text{ Set}_0') \text{VAL } \Rightarrow ('\tau', 'a \text{ Set}_0) \text{VAL)} \\
& \equiv \text{lift1 (strictify (}\lambda X. \text{Abs Set}_0 (\bigcup (\text{Lifting drop } \circ \text{Rep Set}_0) '\text{Rep Set}_0 X'))) \\
\text{ocl_setup_op [Ocl Flatten]}
\end{align*}

defs

\begin{align*}
\text{Ocl Including def : Ocl Including } & \equiv \text{lift2 (strictify (}\lambda X. \text{strictify (}\lambda Y. \text{Abs Set}_0 (\_ \_ \_ \_ \_ Y))))
\end{align*}

\begin{align*}
\text{Ocl Excluding def : Ocl Excluding } & \equiv \text{lift2 (strictify (}\lambda X. \text{strictify (}\lambda Y. \text{Abs Set}_0 (\_ \_ \_ \_ \_ \_ \_ Y))))
\end{align*}

\begin{align*}
\text{Ocl Complement def : Ocl Complement } & \equiv \text{lift1 (strictify (}\lambda X. \text{Abs Set}_0 (\_ \_ \_ \_ \_ Y))))
\end{align*}

\begin{align*}
\text{Ocl Union def : Ocl Union } & \equiv \text{lift2 (strictify (}\lambda X. \text{strictify (}\lambda Y. \text{Abs Set}_0 (\_ \_ \_ \_ \_ Y)))}
\end{align*}

\begin{align*}
\text{Ocl Intersection def : Ocl Intersection } & \equiv \text{lift2 (strictify (}\lambda X. \text{strictify (}\lambda Y. \text{Abs Set}_0 (\_ \_ \_ \_ \_ Y)))}
\end{align*}

\begin{align*}
\text{ocl_setup_op [Ocl Including, Ocl Excluding, Ocl Complement, Ocl Union]}
\end{align*}

\begin{align*}
\text{ocl_setup_op [Ocl Intersection]}
\end{align*}

\begin{align*}
\text{declare } & \text{OCL cp_Ocl Intersection[simp,intro!]} \\
\text{Note that also sequencing of declarations are possible.}
\end{align*}

\begin{align*}
\text{syntax } & \quad \text{@OclFinSet } \quad \text{args } \Rightarrow ('\tau', 'a \text{ Set}_0) \text{VAL} \quad (\text{mkSet (}_\_))
\end{align*}

\begin{align*}
\text{lemma mkSet \{1,1,1,0,1\} = ?X oops}
\end{align*}

368
Properties of the Operations

Useful Lemmas (necessary in this theory)

**Lemma**: OclIntersection_idem

\[\text{simp}]: (\{S:'(\tau,\alpha:\bot)\Set\} \cap S) = S\]

**Proof**

1. Use rule `ext`
2. Case `\(\text{case\_tac } x \equiv \partial(S)\)`
3. Simplify `\(\text{simp\_all, ocl\_hyps\subst \[2\], simp\_all}\)`
4. Apply `ocl\_hypsubst \[2\]`, `simp\_all`
5. Apply `simp\_only: OclIntersection\_def`
6. `OclLocalValid\_def`, `OclIsDefined\_def`, `strictify\_def`
7. `OclNot\_def`, `OclTrue\_def`, `DEF\_def`
8. Apply `simp\_all` add `strictify\_def`, `lift\_drop\_idem`, `DEF\_def`, `symmetric`
9. `DEF\_Rep\_Set`, `Rep\_Set\_0\_inverse`

**Done**

**Lemma**: not_empty

\[\text{OclNotEmpty}(X: '\tau, 'alpha:\bot)\Set\) = \neg (\text{OclIsEmpty}(X))\]

**Proof**

1. Rule `ext`
2. Case `\(\text{case\_tac } x \equiv \partial(X)\)`
3. Simplify `\(\text{simp\_all}\)`
4. Apply `ocl\_hypsubst \[2\]`, `simp\_all`
5. Apply `rule\ sym`, `rule\ trans`
6. Apply `rule\ strictEq\_is\_strongEq\_LE`
7. `\(\text{simp}\_only: OclIsDefined\_def, OclTrue\_def, OclLocalValid\_def, OclMtSet\_def\)`
8. Apply `auto\ simp\: DEF\_def`
9. Rule `tac\ t = \{\}` in `ssubst`, `assumption`
10. `subst\ lift\_drop\_idem`
11. Rule `DEF\_Rep\_Set`
12. `auto\ simp\: DEF\_def, Rep\_Set\_0\_inverse`

**Done**

**Lemma**: OclIsEmpty_charn

\[\text{OclIsEmpty\_charn\ : OclIsEmpty}(X) = (X = \emptyset)\]

**Proof**

1. Rule `ext`
2. Case `\(\text{case\_tac } x \equiv \partial(X)\)`
3. `\(\text{simp\_all}\)`
4. `ocl\_hypsubst \[2\]`, `simp\_all`
5. Apply `rule\ sym`, `rule\ trans`
6. `rule\ strictEq\_is\_strongEq\_LE`
7. `\(\text{simp\_only: OclIsDefined\_def, OclTrue\_def, OclLocalValid\_def, OclMtSet\_def\)`
8. Apply `auto\ simp\: DEF\_def`
9. Rule `tac\ t = \{\}` in `ssubst`, `assumption`
10. `subst\ lift\_drop\_idem`
11. Rule `DEF\_Rep\_Set`
12. `auto\ simp\: DEF\_def, Rep\_Set\_0\_inverse`

**Done**
Appendix B. Isabelle Theories

lemma OclIsNotEmpty_local_charn_LJE :
  \( \tau \vdash OclIsNotEmpty_local_charn_LJE \)

apply (simp only: OclIsDefined_def OclTrue_def OclLocalValid_def
  OclNotEmpty_def OclIncludes_def
  OclIsEmpty_def OclStrongEq_def
  lift0_def lift1_def lift2_def
  strictify_def o_def not_def DEF_def
)
apply (simp)
apply (rule_tac x = \( c \in X \) in exI)
apply (simp add: strictify_def DEF_def)
done

Sets with defined size must be finite.

lemma finite_Sets :
  \( \tau \vdash OclIsNotEmpty_local_charn_LJE \) ==\>
  finite \( \Rep_Set_0 (\self \tau) \)
apply (simp add: OclIsDefined_def OclTrue_def lift0_def lift1_def lift2_def
  strictify_def o_def not_def DEF_def
)
apply (simp only: OclSize_def)
apply (simp add: lift0_def lift1_def lift2_def OclLocalValid_def
  strictify_def DEF_def UU_up_def)
apply (cases \( \self \tau \) = \bot)
apply (auto simp: OclLocalValid_def)
done

Sets with defined size must be defined.

lemma def_if_size_def :
  \( \tau \vdash OclIsNotEmpty_local_charn_LJE \) ==\>
  \( \tau \vdash def_if_size \)
apply (simp add: OclIsDefined_def OclTrue_def lift0_def lift1_def lift2_def
  strictify_def o_def not_def DEF_def
)
apply (simp only: OclSize_def)
apply (simp add: lift0_def lift1_def lift2_def OclLocalValid_def
  strictify_def DEF_def UU_up_def)
apply (cases \( \self \tau \) = \bot)
apply (auto simp: OclLocalValid_def)
done

lemma def_if_size_def_global :
  \( \tau \vdash OclIsNotEmpty_local_charn_LJE \) ==\>
  \( \tau \vdash def_if_size \)
apply (rule valid_intro)
apply (drule_tac \( \tau \) = \bot in valid_elim)

370
B.4. Library

apply (simp add: def_if_size_def)
done

lemma REQ_11_7_1_4_alt2:
  (self::('τ,'α::bot) Set) -> count((obj::('τ,'α) VAL)) =
  (if obj ∈ self then 1 else 0 endif)
apply (rule ext)
apply (simp add: OclCount_def OclIncludes_def OclIf_def OclStrictEq_def
          OCL_Integer.Zero_ocl_int_def OCL_Integer.One_ocl_int_def)
apply (simp only: lift0_def lift1_def lift2_def lift3_def
          strictify_def o_def not_def OclIsDefined_def OclTrue_def
          split_def split_if split)
done

Semantic Definitions of the Iterators

With "iterator", the standard attempts to subsume several vaguely related higher-order
concepts such as fold, map, filter and comprehensions. The quantifier ForAll is in fact
be defined via fold. Since this approach only works for finite sets, we do not follow the
standard here and give a more general definition, but show that this coincides with
the standards requirements for finite sets.

Universal Quantifiers
defs

OclForAll_def: OclForAll ≡ (lift2' lift_arg0 lift_arg1) (strictify( λ S. (λ P.
                        if ∀ x ∈ "Rep_Set_0 S". P x = "True" then "True"
                        else if ∃ x ∈ "Rep_Set_0 S". P x = "False"
                        then "False" else ⊥)))

ocl_setup_op[OclForAll]

lemma OclExists_UU1 [simp]:
  (∃ x ∈ (λ::('τ,'α::bot)Set) * P (x::('τ,'α) VAL)) = ⊥
by(simp add: OclExists_def)

lemma OclForAllMt [simp]:
  (∀ x ∈ (λ::('τ,'α::bot)Set) * P (x::('τ,'α::bot) VAL)) = T
by(simp add: OclForAll_def OclTrue_def OclMtSet_def ss_lifting)
Appendix B. Isabelle Theories

**lemma OclExistsMt [simp]:**

\[
\exists x \in (\emptyset::('\tau, '\alpha::bot))Set . P (x::('\tau, '\alpha::bot) VAL)) = F
\]

by (simp add: OclExists_def)

**lemma ForAllI:**

assumes \(\text{defS} : \tau \models \partial (S::('\tau, ('\alpha::bot))Set)\)
and \(\text{allP} : \forall x . \tau \models x \in S \Rightarrow \tau \models P x\)
shows \(\tau \models (\forall x \in S . P(x::'\tau \Rightarrow '\alpha::bot))\)

apply (insert defS)
apply (rule_tac X = S in Set_sem_cases)
apply (simp_all add: localValidDefined2sem DEF_def)
apply (auto simp: OclForAll_def localValid2sem ss_lifting)
done

**lemma notForAllI:**

assumes \(\text{isin} : \tau \models x \in (S::('\tau, ('\alpha::bot))Set)\)
and \(\text{not} : \tau \models \neg (P x)\)
and \(\text{cpP} : \text{cp P}\)
shows \(\tau \models \neg (\forall x \in S . P(x::'\tau \Rightarrow '\alpha::bot))\)

apply (insert isin not cpP)
apply (rule_tac X = S in Set_sem_cases)
apply (simp_all add: localValidDefined2sem DEF_def)
apply (auto simp: OclForAll_def OclIncludes_def OclNot_def ss_lifting)
done

**lemma ForAllD:**

assumes \(\text{allP} : \tau \models (\forall x \in S . P(x::'\tau \Rightarrow '\alpha::bot))\)
and \(\text{cpP} : \text{cp P}\)
shows \(\forall x . \tau \models x \in (S::('\tau, ('\alpha::bot))Set) \Rightarrow \tau \models P x\)

apply (insert allP cpP)
372
apply (simp add: localValid2sem OclForAll_def OclNot_def OclIncludes_def ss_lifting')
apply (simp add: strictify_def
    split: split_if_asm)
apply (erule_tac x = x τ in ballE)
apply (simp_all add: cp_by_cpify lift0_def)
done

lemma localValidForall2forall :
  assumes defS : \tau \vDash \partial (S::('τ,'α::bot) Set)
  and cpP : cp P
  shows (\tau \vDash \forall x \in S . P(x::'τ \Rightarrow 'α::bot)) =
    (\forall x . \tau \vDash x \in S \Rightarrow \tau \vDash P x)
apply (safe)
apply (drule ForAllD, simp_all add: cpP)
apply (rule ForAllI, simp_all add: defS)
done

lemma undefForAllI1:
  \[ \tau \vDash \nexists (S::('τ,'α::bot) Set) \]
  \[ \Rightarrow \tau \vDash \nexists (\forall \alpha \in S . P(x::'τ \Rightarrow 'α)) \]
  by (erule_tac P = \lambda X. (\nexists (\forall \alpha \in X . P x)) in subst_LJ_undef, simp_all)

lemma undefForAllI2:
  assumes exUndef1 : \tau \vDash x \in (S::('τ,'α::bot) Set)
  and exUndef2 : \tau \vDash \nexists (P x)
  and allP : \forall x . \tau \vDash x \in S \Rightarrow \tau \vDash (P x) \lor \nexists (P x)
  and cpP : cp P
  shows \tau \vDash \nexists (\forall x \in S . P(x::'τ \Rightarrow 'α::bot))
apply (insert exUndef1 exUndef2)
apply (frule isDefined_if_valid)
apply (drule OCL_is_defopt_OclIncludes[THEN iffD1])
apply (simp add: OclLocalValid_def OclIsDefined_def OclTrue_def
    OclForAll_def OclNot_def OclIncludes_def
    ss_lifting')
apply (erule conjE)
apply (frule DEF_X_Set', clarify)
apply (simp, safe)
apply (rule_tac x = x in bexI, simp_all prefer 2)
apply (rule_tac x = x τ in bexI, simp_all)
apply (subgoal_tac P (\tau a. x τ) \tau = P x τ, simp)
apply (rule_tac x = x τ in localValidToNotFalse2sem [THEN iffD1])
done

apply (simp_all add: includes_charn2 DEF_def)
done
Appendix B. Isabelle Theories

lemma isdefForAll2:
  assumes exNot1: \( \tau \models x \in (S::(\tau, (\alpha::bot))Set) \)
  and exNot2: \( \tau \models \neg (P x) \)
  and cpP : cp P
  shows \( \tau \models \partial(\forall x \in S \cdot P(x::\tau \Rightarrow \alpha::bot)) \)
apply(insert exNot1 exNot2 cpP)
apply(drule_tac P=P in notForAllI)
apply(simp_all add: isDefined_if_invalid)
done

lemma isDefinedForall_UC:
  assumes cpP : cp P
  shows \( (\partial(\forall x \in S \cdot P(x::\tau \Rightarrow \alpha::bot))) = ((\partial(S::(\tau, \alpha)Set)) \land ((\exists x \in S \cdot (\neg (P x))) \lor (\forall x \in S \cdot (\partial (P x))))) \)
oops

lemma isDefinedForall_LJE:
  assumes cpP : cp P
  shows \( (\tau \models \partial(\forall x \in S \cdot P(x::\tau \Rightarrow \alpha::bot))) = ((\tau \models \partial S) \land ((\exists x. (\tau \models x \in (S::(\tau, \alpha)Set)) \land (\neg (\tau \models P x))) \lor (\forall x. (\tau \models \partial x \land (\tau \models x \in S) \Rightarrow (\tau \models \partial (P x))))) \)
oops

lemmas isdefForAll3 = ForAll[THEN isDefined_if_valid]

lemma ExistsI:
  assumes isin : \( \tau \models x \in (S::(\tau, (\alpha::bot))Set) \)
  and not : \( \tau \models (P x) \)
  and cpP : cp P
  shows \( \tau \models (\exists x \in S \cdot P(x::\tau \Rightarrow \alpha::bot)) \)
by (auto simp:OclExists_def intro!: notForAll isin not cpP)

lemma NotExistsI:
  assumes defS: \( \tau \models \partial(S::(\tau, (\alpha::bot))Set) \)
  and allP : \( \forall x. \tau \models x \in S \Rightarrow (\tau \models \neg P x) \)
  shows \( \tau \models \neg(\exists x \in S \cdot P(x::\tau \Rightarrow \alpha::bot)) \)
by (auto simp:OclExists_def intro!: ForAll defS allP)

lemma ExistsD:

374
B.4. Library

assumes $ExP : \tau \vdash (\exists x \in S \cdot P(x) \Rightarrow (\alpha::bot))$
shows $\exists x. \tau \vdash x \in (S::(\tau,(\alpha::bot))Set) \land \tau \vdash (P x)$
apply (insert $ExP$)
apply (simp add: localValid2sem OclForAll_def OclNot_def OclIncludes_def OclExists_def o_def ss_lifting)
apply (simp add: strictify_def
split: split_if_asm)
apply (frule DEF_X_Set', clarify)
apply (rule_tac x = lift0 x in exI)
apply (auto simp: lift0_def not_down_exists_lift)
done

lemma localValidExists2exists:
assumes $cpP : cp \ P$
assumes $defS : \tau \vdash \partial(S::(\tau,(\alpha::bot))Set)$
shows $(\tau \vdash (\exists x \in S \cdot P(x) \Rightarrow (\alpha::bot))) = (\exists x. \tau \vdash x \in S \land \tau \vdash (P x))$
apply (safe)
apply (drule ExistsD, simp)
apply (auto intro!: ExistsI $cpP$)
done

lemmas weak_pred_LJE = weak_prop_LJE
localValidForall2forall
localValidExists2exists

thm weak_pred_LJE

Select and Collect
def $OclSelect\_def: OclSelect \equiv \ (\lift2' \ lift\_arg0 \ lift\_arg1) \ (\strictify (\lambda S P. \ if \ \forall x \in \italic{Rep\_Set\_0} S. DEF (P x) \ then \ Abs\_Set\_0 ((x\in\italic{Rep\_Set\_0} S. P x = \true)) \ else \ \bot))$

ocl_setup_op [OclSelect]

lemma SelectPartialUndef:
assumes $ainS : \tau \vdash a \in (S::(\tau,(\alpha::bot))Set)$
and $allP : \tau \vdash \emptyset(P a)$
and $cpP : cp \ P$
shows $((x : S \mid P (x) \Rightarrow (\alpha::bot))) \tau = \bot \tau$
apply (insert $ainS$ $allP$)
apply (frule isDefined_if_valid,
drule OCL\_iss\_defopt\_OclIncludes[THEN iffD1])
apply (simp add: OclSelect\_def OclIncluding_def OclUndefined_def OclLocalValid_def OclIsDefined_def OclTrue_def OclForAll_def OclNot_def OclIncludes_def)
Appendix B. Isabelle Theories

\[ ss\_lifting' \]
\begin{verbatim}
apply auto
apply (erule_tac x=a \in ballE, simp_all)
apply (subgoal_tac P (\x'. a \tau \tau = P a \tau, simp)
apply (rule_tac \tau=\tau and \P=P in cp_charn, simp add: cpP, rule cpP)
done

lemma SelectPartialUndef2 [simp]:
assumes ainS: \tau \models (a ::'\tau \Rightarrow '\alpha ::bot) \in (S::('\tau ::'\alpha ::bot)\Set)
shows ((\x:S | (\x. \bot)((\x::'\tau\Rightarrow '\alpha ::bot)))) \tau = \bot \tau
by (rule SelectPartialUndef, auto intro!: ainS)

lemma mem_OclSelect_eq:
assumes defS: \tau \models \partial(S::('\tau ::'\alpha ::bot)\Set)
and defa: \tau \models \partial(a::('\tau ::'\alpha ::bot))
and ainS: \tau \models a \in S
and allP: \\\ A x. \tau \models x \in S \supset \tau \models \partial(P x)
and cpP : cp P
shows (\tau \models a \in ((\x:S | P (x::'\tau\Rightarrow '\alpha ::bot))))
= (\tau \models P a)
apply (insert defS defa ainS)
apply (simp add: OclSelect_def OclIncluding_def OclUndefined_def
OclLocalValid_def OclIsDefined_def OclTrue_def
OclForAll_def OclNot_def OclIncludes_def
ss_lifting' o_def)
apply (frule DEF_X_Set', clarify)
apply (simp)
apply (rule_tac \tau=P a \tau in subst)
apply (rule sym, rule_tac \tau=P=P \and x=a in cp_subst, rule cpP)
apply (rule_tac \tau=P=P (lift0 (a \tau)) \tau in boolean_cases _sem)
apply (auto simp: lift0_def)
apply (rotate_tac -1, erule contrapos_pp)
apply (rule allP[simplified
OclLocalValid_def OclIsDefined_def OclTrue_def
OclForAll_def OclNot_def OclIncludes_def
ss_lifting', simplified])
apply (auto simp: strictify_def)
done

lemma nonmem_OclSelect:
assumes defS: \tau \models \partial(S::('\tau ::'\alpha ::bot)\Set)
and defa: \tau \models \partial(a::('\tau \Rightarrow '\alpha ::bot))
and anninS: \tau \not\tau \models a \in S
and cpP : cp P
shows \tau \not\tau \models a \in ((\x:S | P (x::'\tau\Rightarrow '\alpha ::bot))))
apply (insert defS defa anninS)
apply (simp add: OclSelect_def OclIncluding_def

376
\end{verbatim}
B.4. Library

apply (frule DEF_X_Set', clarify, simp)
done

lemma mem_Select.charn:
assumes defS: \( \tau \Vdash \partial(S:(\tau, (\alpha::\bot)) Set) \)
and defa: \( \tau \Vdash \partial(\alpha::(\tau \Rightarrow \alpha::\bot)) \)
and allP: \( \forall x. \tau \Vdash x \in S \implies \tau \Vdash \partial(P x) \)
and cpP: cp P
shows \( \tau \Vdash a \in ((x:S | P(x::\tau\Rightarrow 'alpha::bot))) = (\tau \Vdash P a \land \tau \Vdash a \in S) \)
by (intro mem_OclSelect_eq nonmem_OclSelect, simp_all add: allP defS defa cpP+)

lemma select_mem.charn:
assumes defT: \( \tau \Vdash \partial(T:(\tau, (\alpha::\bot)) Set) \)
shows \( (\{x:S | ((x::(\tau \Rightarrow 'alpha::bot)) \in T)\}) \tau = ((S::(\tau,\alpha) Set) \cap T) \tau \)
apply(insert defT)
apply(simp add: localValidDefined2sem DEF_def)
apply(frule DEF_X_Set', clarify)
apply(rule_tac X=S in Set_sem_cases, simp_all)
apply(simp_all add: OclSelect_def OclIncludes_def OclIntersection_def ss_lifting)
apply(safe)
apply(subst Abs_Set_0_inject_charn)
apply(auto)
done

lemma select_mem.charn_global[simp]:
assumes defT: \( \tau \Vdash \partial(T:(\tau, (\alpha::\bot)) Set) \)
shows \( (\{x:S | ((x::(\tau \Rightarrow 'alpha::bot)) \in T)\}) = ((S::(\tau,\alpha) Set) \cap T) \)
apply(rule ext, insert defT)
apply(rule select_mem.charn)
apply(auto simp: global_vs_local_validity[ symmetric])
done

lemma select_mem.charn_universal[simp]:
shows \( (\{x:S | ((x::(\tau \Rightarrow 'alpha::bot)) \in S)\}) = ((S::(\tau,\alpha) Set) \)

377
Appendix B. Isabelle Theories

apply (rule ext)
apply (case_tac x ⊨ ∂(S))
apply (simp_all, ocl_hypsubst \[Ω, simp_all\])
apply (rule trans)
apply (rule select_mem_charn)
apply (simp_all)
done

defs
OclCollect_def: OclCollect S P ≡ λ τ.
  if DEF (S τ) then
    if ∀ x ∈ \[Rep_Set_0 (S τ)\]. DEF (P (λτ. x) τ)
    then Abs_Set_0 (λx. P (λτ. x) τ) \[Rep_Set_0 (S τ)\] else ⊥
  else ⊥

Any and One
defs
OclAny_def : OclAny ≡ (lift2' lift_arg0 lift_arg1) (strictify (λ S P.
  if (∀ x ∈ \[Rep_Set_0 S\]. DEF (P x)) ∧
  (∃ x ∈ \[Rep_Set_0 S\]. P x = \[True\])
  then SOME x.(x ∈ \[Rep_Set_0 S\] ∧ P x = \[True\])
  else ⊥))

ocl_setup_op [OclAny]

defs
OclOne_def : OclOne ≡ (lift3' lift_arg0 lift_arg2 lift_arg0) (strictify (λ S P.
  if (finite \[Rep_Set_0 S\])
  then card \{x ∈ \[Rep_Set_0 S\]. P x = \[True\]\} = 1
  else ⊥))

ocl_setup_op [OclOne]

The iterator for Sets is not adequately defined in the standard (idempotence). This can be overcome by Paulson’s theory of the finite fold operator of sets: it is always defined, but only for bodies P that are \[ACI\], there is an unfold theorem.

This definition essentially captures the intention of the standard.

defs
OclIterate_def : OclIterate ≡ (lift3' lift_arg0 lift_arg2 lift_arg0) (strictify (λ S P A.
  if (finite \[Rep_Set_0 S\])
  then (fold_set (λ x y. P y x) A \[Rep_Set_0 S\])
  else ⊥))

378
Properties of iterate on sets

lemma iterate_infinite:
\( \tau \not\models \varnothing \) \( ( (X::(\tau,'_\alpha::bot)\text{Set}) ) \) \( \implies \)
\( \tau \not\models (\text{OclIterate} X (P::(\tau,'_\alpha) \text{ VAL} \Rightarrow (\tau,'_\beta \text{ VAL} \Rightarrow (\tau,'_\beta) \text{ VAL}) A) ) \)

apply(rule_tac X=X in Set_sem_cases, simp_all)
apply(case_tac finite c)
apply(simp_all add: localValidUnDefined2sem OclSize_def OclIterate_def ss_lifting)
done

Using this theorem all requirements proven about iterate on bags will carry over to iterate on \textit{finite} sets quite easily. Because they are actually equivalent in this case.

lemma iterate_set2bag:
\( \tau \not\models ( (X::(\tau,'_\alpha::bot)\text{Set}) ) \) \( \implies \)
\( \tau \not\models (\text{OclIterate} X (P::(\tau,'_\alpha) \text{ VAL} \Rightarrow (\tau,'_\beta \text{ VAL} \Rightarrow (\tau,'_\beta) \text{ VAL}) A) ) \)=
(\text{OclIterate} ((\text{asBag} X)::(\tau,'_\alpha::bot)\text{Bag}) P A)

apply(rule_tac X=X in Set_sem_cases, simp_all)
apply(case_tac finite c)
apply(simp_all add: OclSize_def OclIterate_def OclLocalValid_def
OclStrongEq_def OCL_Bag.OclIterate_def
fold_set_fold_multiset_conv OclAsBag_def OclTrue_def ss_lifting)
done

end

B.4.14. OclAny

theory OCL_OclAny
imports
\$HOLOCL\_HOME/src/library/collection/\$COLLECTION/OCL\_Set
begin

Level 0
setup \{ Theory.add_path UML\_OCL.level0 | \}

constdefs
mk\_OclAny :: 'a OclAny\_0 \Rightarrow 'a U
mk\_OclAny :: Inl
get\_OclAny :: 'a U \Rightarrow 'a OclAny\_0
get\_OclAny :: sum_case (\lambda x. x) (\lambda x. eps x. True)
is\_OclAny :: 'a OclAny\_0 \Rightarrow bool
is\_OclAny obj \equiv DEF(obj)
is\_OclAny_univ :: 'a U \Rightarrow bool

379
Appendix B. Isabelle Theories

is_OclAny_univ ≡ sum_case (λ x. True) (λ x. False)

lemma get_mk_OclAny_id: get_OclAny(mk_OclAny x) = x
by (simp add: get_OclAny_def mk_OclAny_def)

lemma mk_get_OclAny_id:
apply (simp add: get_OclAny_def mk_OclAny_def is_OclAny_univ_def)
done

lemma is_OclAny_univ_implies_is_get:
apply (simp add: get_OclAny_def mk_OclAny_def is_OclAny_def)
done

lemma is_mk_OclAny:
apply (simp add: is_OclAny_univ_def get_OclAny_def is_OclAny_def mk_OclAny_def)
done

setup ⟨ ⟨ Theory.add_path / ⟩ ⟩
Level 1
setup ⟨ ⟨ Theory.add_path UML_OCL.level1 ⟩ ⟩

constdefs
mk_OclAny :: ('τ, 'α OclAny_0) VAL ⇒ ('τ, 'α U) VAL
mk_OclAny ≡ lift1 level0.mk_OclAny
get_OclAny :: ('τ, 'α U) VAL ⇒ ('τ, 'α OclAny_0) VAL
get_OclAny ≡ lift1 level0.get_OclAny
is_OclAny :: ('τ, 'α OclAny_0) VAL ⇒ (τ)Boolean
is_OclAny ≡ lift1(strictify(lift o level0.is_OclAny))
is_OclAny_univ :: ('τ, 'α U) VAL ⇒ (τ)Boolean
is_OclAny_univ ≡ lift1(lift o level0.is_OclAny_univ)
OclAny :: ('τ, 'α OclAny_0 Set_0) VAL
OclAny ≡ lift0(Abs_Set_0 ⌞ lift ' UNIV ⌟)

lemma get_mk_OclAny_id :
τ≡ level1.is_OclAny_obj ⇒ level1.get_OclAny(level1.mk_OclAny_obj) = obj
apply (unfold level1.is_OclAny_univ_def level1.is_OclAny_def level1.get_OclAny_def
level1.mk_OclAny_def OclLocalValid_def)
apply (rule ext)
apply (simp add: lift1_def level0.get_mk_OclAny_id)
done

lemma mk_get_OclAny_id :

380
\(\tau \models \text{level1.is\_OclAny\_univ univ} \quad \text{implies} \quad \text{level1.mk\_OclAny (level1.get\_OclAny univ)} \quad \text{implies} \quad \text{level1.mk\_OclAny univ \text{OclLocalValid\_def}}\)

apply (frule isDefined_if_valid)
apply (frule localValidDefined2sem [THEN iffD1])
apply (unfold level1.is\_OclAny\_univ_def level1.is\_OclAny\_def level1.get\_OclAny\_def
level1.mk\_OclAny\_def OclLocalValid\_def)
apply(simp add: OclLocalValid\_def lift1\_def lift0\_def level0.mk\_OclAny\_id OclTrue\_def)
done

lemma is\_OclAny\_univ\_implies\_is\_get:
\[\text{DEF(level1.get\_OclAny univ } \tau); (\tau \models \text{level1.is\_OclAny\_univ univ}) \quad \Rightarrow \quad (\tau \models \text{level1.is\_OclAny (level1.get\_OclAny univ)})\]
apply (frule isDefined_if_valid)
apply (frule localValidDefined2sem [THEN iffD1])
apply (unfold level1.is\_OclAny\_univ\_def level1.is\_OclAny\_def level1.get\_OclAny\_def
level1.mk\_OclAny\_def OclLocalValid\_def)
apply(simp add: OclLocalValid\_def lift1\_def lift0\_def level0.is\_OclAny\_univ\_implies\_is\_get
OclTrue\_def strictify\_def DEF\_def )
done

lemma is\_mk\_OclAny:
\(\tau \models \text{level1.is\_OclAny\_obj} \quad \text{implies} \quad (\tau \models \text{level1.is\_OclAny\_univ (level1.mk\_OclAny\_obj)})\)
apply (frule isDefined_if_valid)
apply (frule localValidDefined2sem [THEN iffD1])
apply (unfold level1.is\_OclAny\_univ\_def level1.is\_OclAny\_def level1.get\_OclAny\_def
level1.mk\_OclAny\_def OclLocalValid\_def)
apply(simp add: OclLocalValid\_def lift1\_def lift0\_def OclTrue\_def strictify\_def DEF\_def )
apply(case_tac obj \(\tau = \text{down})
apply(auto simp: level0.is\_mk\_OclAny)
done

setup \(\langle \langle \text{Theory.add\_path /} \rangle \rangle\)

Level 2
setup \(\langle \langle \text{Theory.add\_path UML\_OCL} \rangle \rangle\)

constdefs
\(\text{mk\_OclAny} : (\tau , \alpha \text{OclAny}_0) \text{VAL} \Rightarrow (\tau , \alpha \text{U} ) \text{VAL}\)
\(\text{mk\_OclAny} \equiv \text{level1.mk\_OclAny}\)
\(\text{get\_OclAny} : (\tau , \alpha \text{U})\text{VAL} \Rightarrow (\tau , \alpha \text{OclAny}_0 ) \text{VAL}\)
\(\text{get\_OclAny} \equiv \text{level1.get\_OclAny}\)
\(\text{is\_OclAny} : (\tau , \alpha \text{OclAny}_0) \text{VAL} \Rightarrow (\tau )\text{Boolean}\)
\(\text{is\_OclAny} \equiv \text{level1.is\_OclAny}\)
\(\text{is\_OclAny\_univ} : (\tau , \beta \text{U} ) \text{VAL} \Rightarrow (\tau )\text{Boolean}\)
Appendix B. Isabelle Theories

\[ is\_OclAny\_univ \equiv level1.is\_OclAny\_univ \]
\[ OclAny \equiv \{\tau, \alpha\} OclAny_0 \ Set_0 \ VAL \]
\[ OclAny \equiv level1.OclAny \]

**Lemma** get_mk_OclAny_id:
\[ \tau \models UML\_OCL.is\_OclAny obj \Rightarrow UML\_OCL.get\_OclAny (UML\_OCL.mk\_OclAny obj) = obj \]
apply (unfold UML\_OCL.is\_OclAny_def UML\_OCL.get\_OclAny_def UML\_OCL.mk\_OclAny_def)
apply (simp add: level1.get\_mk\_OclAny\_id)
done

**Lemma** mk_get_OclAny_id:
\[ \tau \models UML\_OCL.is\_OclAny\_univ univ \Rightarrow UML\_OCL.mk\_OclAny (UML\_OCL.get\_OclAny univ) = \tau \]
apply (unfold UML\_OCL.is\_OclAny\_univ_def UML\_OCL.get\_OclAny_def UML\_OCL.mk\_OclAny_def)
apply (simp add: level1.mk\_get\_OclAny\_id)
done

**Lemma** is_OclAny_univ_implies_is_get:
\[ [\text{DEF}(UML\_OCL.get\_OclAny\_univ \tau); (\tau \models UML\_OCL.is\_OclAny\_univ \univ)] \Rightarrow (\tau \models UML\_OCL.is\_OclAny (UML\_OCL.get\_OclAny \univ)) \]
apply (unfold UML\_OCL.is\_OclAny\_univ_def UML\_OCL.get\_OclAny_def UML\_OCL.mk\_OclAny_def)
apply (simp add: level1.is\_OclAny\_univ\_implies\_is\_get)
done

**Lemma** is_mk_OclAny:
\[ \tau \models UML\_OCL.is\_OclAny \ obj \Rightarrow (\tau \models UML\_OCL.is\_OclAny\_univ (UML\_OCL.mk\_OclAny \ obj)) \]
apply (unfold UML\_OCL.is\_OclAny\_univ_def UML\_OCL.get\_OclAny_def UML\_OCL.mk\_OclAny_def)
apply (simp add: level1.is\_mk\_OclAny)
done

**Setup** \[ \langle [\text{Theory.add\_path \ _}] \rangle \]

Re-typing or Casting.

The standard describes an operation that “casts” an object to one of its subtypes. Note that our OCL-encoder provides for each new class an own definition for this polymorphic scheme.

**Consts**
\[ OclAsType :\{\tau, \alpha::\bot\} VAL \Rightarrow (\tau, \beta::\bot) VAL \]
\[ \_ \Rightarrow oclAsType\_\_ (\_ 66,65 65) \]
Checking Dynamic Types of “Kinds”

As a consequence of the difference between dynamic and static typing in object-oriented languages, a test for the “kind” of an object is provided. It checks for the dynamic type.

Note that this operator is in fact defined by our OCL encoder and uses the internally defined test functions.

constdefs
OclIsKindOf :: \((\tau, 'a::bot) \Rightarrow \tau\) = \(\lambda \_ \rightarrow \text{oclIsKindOf}(\_\_ \_)[66,65]65\)

OclIsKindOf self CharSet \equiv self \in CharSet

This simple fundamental definition is the fruit of our generalization of the OCL set theory.

constdefs
OclIsTypeOf :: \((\tau, 'a::bot) \Rightarrow \tau\) = \(\lambda \_ \rightarrow \text{oclIsTypeOf}(\_\_ \_)[66,65]65\)

OclIsTypeOf self NarrowCharSet \equiv self \in NarrowCharSet

B.4.15. CharactersticSets

theory OCL_CharactersticSet
imports
$HOLOCL_HOME/src/library/basic/OCL_Real
$HOLOCL_HOME/src/library/basic/OCL_String
$HOLOCL_HOME/src/library/OclAny/OCL_OclAny
begin

Embedding Characteristic Sets into OCL

lemma Integer_0_Defined [simp]:
\(\Rightarrow \text{Integer}_0\)

by (simp add: localValidDefined2sem Abs_Set_Mt_DEF Integer_0_def lift0_def)

lemma in_Integer_0:
\(\Rightarrow \exists x. ('a::Integer) \in (\text{Integer}_0::('a,\text{Integer}_0)\text{Set})\)

apply (simp add: OCL_Set.OclIncludes_def Integer_0_def localValidDefined2sem OclLocalValid_def OclIsDefined_def OclTrue_def
lifto_def lifti_def liftof_def strictify_def
Abs_Set_range_liftof_DEF[simplified DEF_def])

by (auto simp: DEF_def not_down_exists_lift)

lemma in_Integer_0R[simp]:

end
Appendix B. Isabelle Theories

\[
\begin{align*}
\tau \models (x : 'a \text{Integer}) \in (\text{Integer}_0 : ('a, \text{Integer}_0)\text{Set}) = \\
(\tau \models \partial x)
\end{align*}
\]

by (auto simp: in_\text{Integer}_0

OCL_Logic_core.isDefined_if_valid

THEN OCL_Set.OCL_is_defopt_OclIncludes

THEN iffD1])

The relevance of the latter type of rules become apparent if we look at the following example:

lemma test:
\[
(\forall x \in \text{Integer}_0 \cdot (x + (\text{OclNegative} x) \doteq 0)) = \top
\]

oops

First of all, such an expression is syntactically illegal in OCL. In Standard syntax, this is presented as

\[
\text{Integer}_0 \to \text{forall} (x \mid x + (-x) = 0)
\]

\text{Integer}_0 is considered a type name which is not part of the expression language; therefore, no quantification over them is possible in standard OCL. Since we interpret OCL types as sets in the sense of the OCL_Set theory, we can quantify and reason over it in HOL-OCL.

In particular, rule forAllI eliminates the quantifier and reduces this to

\[
\tau \models x \in \text{Integer}_0 \to (x + (\text{OclNegative} x) \doteq 0)) = \top \quad (B.15)
\]

which can be further simplified by in_\text{Integer}_0R to

\[
\tau \models \partial x \to (x + (-x) \doteq 0)) = \top \quad (B.16)
\]

This is a valid statement in OCL (although we omit the proof here). In contrast,

\[
(x + (-x) \doteq 0)) = \top \quad (B.17)
\]

in itself is not valid since \(x\) may be undefined. Thus, quantifiers range over defined values only (as one would expect). These theorems also implicitly state that the characteristic sets of the basic types are non-empty.

lemma Real_Defined [simp]:
\[
\tau \models \partial \text{Real}_0
\]

by (simp add: localValidDefined2sem Real_0_def lift0_def)

lemma in_Real_0:
\[
\tau \models \partial x \to
\]

\[
\tau \models (x : 'a \text{Real}) \in (\text{Real}_0 : ('a, \text{Real}_0)\text{Set})
\]

apply (simp add: OCL_Set.OclIncludes_def Real_0_def localValidDefined2sem

OclLocalValid_def OclUsDefined_def OclTrue_def

lift0_def lift1_def lift2_def strictify_def

Abs_Set.rangelift_DEF[simplified DEF_def])

384
by (auto simp: DEF_def not_down_exists_lift)

lemma in_RealR_0[simp]:
  (τ ⊩ (x::'a Real) ∈ (Real_0::('a,Real_0)Set)) =
  (τ ⊩ ∂ x)
by (auto simp: in_Real_0 isDefined_if_valid
          THEN OCL_Set.OCL_is_defopt_OclIncludes
          THEN iffD1)

lemma Boolean_Defined [simp]:
  τ ⊩ ∂ Boolean_0
by (simp add: localValidDefined2sem Boolean_0_def lift0_def)

lemma in_Boolean:
  τ ⊩ ∂ x =⇒
  τ ⊩ (x::'a Boolean) ∈ (Boolean_0::('a,Boolean_0)Set)
apply (simp add: OCL_Set.OclIncludes_def Boolean_0_def localValidDefined2sem
        OclLocalValid_def OclIsDefined_def OclTrue_def
        lift0_def lift1_def lift2_def strictify_def
        Abs_Set_rangeOclDef[simplified DEF_def])
by (auto simp: DEF_def not_down_exists_lift)

lemma String_0_Defined [simp]:
  τ ⊩ ∂ String_0
by (simp add: localValidDefined2sem String_0_def lift0_def)

lemma in_String_0:
  τ ⊩ ∂ x =⇒
  τ ⊩ (x::'a String) ∈ (String_0::('a,String_0)Set)
apply (simp add: OCL_Set.OclIncludes_def String_0_def localValidDefined2sem
        OclLocalValid_def OclIsDefined_def OclTrue_def
        lift0_def lift1_def lift2_def strictify_def
        Abs_Set_rangeOclDef[simplified DEF_def])
by (auto simp: DEF_def not_down_exists_lift)

lemma in_StringR[simp]:
  (τ ⊩ (x::'a String) ∈ (String_0::('a,String_0)Set)) =
Appendix B. Isabelle Theories

\[
(\tau \models \partial x)
\]
by (auto simp; in String_0
isaDefined_if_valid
[THEN OCL_Set.OCL_is_defopt_OclIncludes
[THEN iffD1]]
)

lemma OclAny_Defined [simp]:
\[\tau \models \partial OclAny\]
by(simp add: localValidDefined2sem OclAny_def level1.OclAny_def lift0_def)

lemma in_OclAny:
\[\tau \models \partial x \implies \tau \models (x :: (\'a,\'b) OclAny) \in (OclAny::(\'a,\'b OclAny_0)Set)\]
apply (simp add: OCL_Set.OclIncludes_def OclAny_def level1.OclAny_def localValidDefined2sem
OclLocalValid_def OclIsDefined_def OclTrue_def
lift0_def lift1_def lift2_def strictify_def
Abs_Set_rangelift_DEF[simplified DEF_def])
by (auto simp; DEF_def not_down_exists_lift)

lemma in_OclAnyR[simp]:
\[\tau \models (x :: (\'a,\'b) OclAny) \in (OclAny::(\'a,\'b OclAny_0)Set) = (\tau \models \partial x)\]
by (auto simp; in_OclAny
isaDefined_if_valid
[THEN OCL_Set.OCL_is_defopt_OclIncludes
[THEN iffD1]])

end

B.4.16. The \textbf{OCL} Library

theory OCL_Library
imports
\$HOLOCL_HOME/src/library/collection/$COLLECTION/OCL_CharactersticSet
begin

Datatype Conversions

consts
HolOclToReal :: 'a Integer => 'a Real (\_ => toReal(\' ) [66])
defs
HolOclToReal_def: HolOclToReal \equiv lift1(strictify(\lambda x:Integer_0.
\_ real (\"x\") ))
B.5. State

B.5.1. OCL State

theory OCL_State
imports $HOLOCL_HOME/src/library/OclAny/OCL_OclAny
begin
  'a state = oid → 'a
  's St = 's state × 's state
  ('a,'t) V = ('a St,'t) VAL

translations
  a state <= (type) oid ⇒ a option
  a St <= (type) (a state) × (s state)
  (a,t) V <= (type) a St ⇒ t

To sum up, the HOL types assigned to the key OCL types of the OCL standard are a context (st) indexed family of types. Recall: the contexts are a state relation or a Kripke-Structure over states over the universe.

Provided that we have a representation of class types generated from an UML class diagram, we can therefore translate any OCL type into an HOL-type achieving type soundness on the HOL-level.

Checking Freshness of Object Instances in the State.

constdefs
  OclIsNew :: ('a U St,'b:bot) VAL ⇒ ('a U St) Boolean
  OclIsNew obj ≡ (λ(s,s'). level0.mk_OclAny (((obj) ⇒ oclAsType(OclAny)) (s,s')) ∉ ran s ∧ level0.mk_OclAny (((obj) ⇒ oclAsType(OclAny)) (s,s')) ∈ ran s')

The OCL encoder must generate a coercion in order to make this operation applicable to any object of some class-type

Selecting the Objects living in a State.

consts
  OclAllInstances :: ('a U St,'b) VAL ⇒ ('a U St,'b Set_0) VAL
  OclAllInstancesAtpre :: ('a U St,'b) VAL ⇒ ('a U St,'b Set_0) VAL

defs
  OclAllInstancesString_def[simp]:
  OclAllInstances (self:('a U St,String_0) VAL) ≡ OclUndefined

  OclAllInstancesPreString_def[simp]:

end
Appendix B. Isabelle Theories

\[ \text{OclAllInstancesAtpre (self::'(a U St,String_0) VAL) } \equiv \text{OclUndefined} \]

**defs**

\[ \text{OclAllInstancesInteger_def[simp]:} \]
\[ \text{OclAllInstances (self::'(a U St,Integer_0) VAL) } \equiv \text{OclUndefined} \]

\[ \text{OclAllInstancesPreInteger_def[simp]:} \]
\[ \text{OclAllInstancesAtpre (self::'(a U St,Integer_0) VAL) } \equiv \text{OclUndefined} \]

**defs**

\[ \text{OclAllInstancesReal_def[simp]:} \]
\[ \text{OclAllInstances (self::'(a U St,Real_0) VAL) } \equiv \text{OclUndefined} \]

\[ \text{OclAllInstancesPreReal_def[simp]:} \]
\[ \text{OclAllInstancesAtpre (self::'(a U St,Real_0) VAL) } \equiv \text{OclUndefined} \]

**defs**

\[ \text{OclAllInstancesBoolean_def[simp]:} \]
\[ \text{OclAllInstances (self::'(a U St,Boolean_0) VAL) } \equiv \text{Boolean_0} \]

\[ \text{OclAllInstancesPreBoolean_def[simp]:} \]
\[ \text{OclAllInstancesAtpre (self::'(a U St,Boolean_0) VAL) } \equiv \text{Boolean_0} \]

And now the general case for all "objects", i.e. all instances of subclass OclAny:

**defs**

\[ \text{OclAllInstancesOclAny_def:} \]
\[ \text{OclAllInstances (self::'(a U St,'a OclAny_0) VAL) } \equiv \]
\[ \lambda(s,s'). \text{Abs_Set_0 (⌜level0.get_OclAny ' ran s⌝)} \]

\[ \text{OclAllInstancesPreOclAny_def:} \]
\[ \text{OclAllInstancesAtpre (self::'(a U St,'a OclAny_0) VAL) } \equiv \]
\[ \lambda(s,s'). \text{Abs_Set_0 (⌜level0.get_OclAny ' ran s⌝)} \]

The modifiedOnly() - clause and its Infrastructure

**constdefs**

\[ \text{OclOidOf :: 'a U state } \Rightarrow \text{'a OclAny_0 } \Rightarrow \text{oid set} \]
\[ \text{OclOidOf s X } \equiv \{x . (s x) = \text{Some(OCL_OclAny.mk_OclAny X)}\} \]

The oid Set is a tribute to non-referential universes where there may be different object identifiers in the store for the same object. The restriction to 'a OclAny_0 assures that the projection is only applicable to objects.

**constdefs**

\[ \text{OclModifiedOnly :: ('}a U St,'a OclAny_0) Set} \Rightarrow ('}a U St) Boolean \]
\[ \text{OclModifiedOnly X } \equiv \lambda(s,s'). \]
\[ \forall id \in (\text{OclOidOf s ''Rep_Set_0(X(s,s))})^\circ. \text{ s id } = \text{ s' id} \]

end
B.5.2. The OCL Calculi

theory OCL_Calculi
imports $HOLOCL_HOME/src/OCL_Library
begin

This theory develops some more experimental calculi for OCL such as the local judgement tableaux calculus (let!) or a particular congruence rewriting calculus. It is the basis of some more experimental proof procedures so far.

Some core tableaux calculus

The conceptual basis of this calculus is drawn from [28] where “labeled formulas” where introduced. These are:

- \( A^t \) (for \( A s = T s \)),
- \( A^f \) (for \( A s = F s \))
- \( A^u \) (for \( A s = \bot s \))

A “labeled clause” is then a set of labelled formulas (considered as disjunctions). In their notation, the crucial rules for labeled clauses are:

\[
\begin{align*}
C, (A \land B)^t & \quad C, (A \land B)^f & \quad C, (A \land B)^u \\
C, A^t & \quad C, A^f & \quad C, A^u \\
B^t & \quad B^f & \quad B^u
\end{align*}
\]

(B.18)

\[
\begin{align*}
C, (\neg A)^t & \quad C, (\neg A)^f & \quad C, (\neg A)^u \\
C, A^t & \quad C, A^f & \quad C, A^u
\end{align*}
\]

(B.19)

Tableau-calculi were implemented in Isabelle not on the basis of clauses, but on Horn formula \([A_1; \ldots; A_n] \Rightarrow B\) corresponding to \(\neg A_1, \ldots A_n, B\) in clause representation. The conclusion in the Horn-format is used with preference during proof search.

As a consequence, it is necessary to duplicate the set of rules into introduction- and elimination rules. Further, we use the validity normal form to represent negation; thus the handling of the not is different and has to be encoded into the rules (leading to further duplications of the rule sets), this is necessary in Isabelle’s representation of tableaux calculi anyway.

lemma and_TRUE_I:

\[
\begin{align*}
\begin{array}{c}
\tau \models A, \tau \models B \\
\end{array}
\Rightarrow \tau \models (A \land B)
\end{align*}
\]

by (erule subst_LJ_TRUE, erule subst_LJ_TRUE, auto)

lemma and_D1:

\[
\begin{align*}
\begin{array}{c}
\tau \models A \land B \\
\end{array}
\Rightarrow \tau \models A
\end{align*}
\]

apply (simp_all add: OclAnd_def OclLocalValid_def)
Appendix B. Isabelle Theories

\begin{verbatim}
DEF_def lift2_def split add
apply (case_tac A τ = down)
apply (simp_all add: OclTrue_def lift0_def)
apply (simp add: split_if_eq1)
apply (case_tac B τ = down)
apply (simp_all add: split_if_eq1 not_down_exists_lift)
apply (erule exE)
apply (erule exE)
apply (simp_all add: drop_lift)
done

lemma and_D2:
  [ τ ⊨ A ∧ B ] ⇒ τ ⊨ B
  by (rule and_D1, subst and_commute, assumption)

lemma and_TRUE_E:
  [ τ ⊨ (A ∧ B); τ ⊨ A; τ ⊨ B ] ⇒ R ] ⇒ R
  by (frule and_D1, drule and_D2, auto)

lemma and_congr'::
  (τ ⊨ (A ∧ B)) = ((τ ⊨ A) ∧ (τ ⊨ B))
  by (auto elim: and_TRUE_E and_D1 and_D2 intro: and_TRUE_I)

lemma not_and_undef_congr1[simp]:
  (τ ⊨ ¬ (⊥ ∧ B)) = (τ ⊨ ¬ B)
  apply (cut_tac τ = τ and A = B in non_quatrum_datur)
  apply auto
  apply (erule_tac subst_LJ_TRUE_fw, assumption, auto)
  apply (erule_tac subst_LJ_FALSE, auto)
  by (drule_tac subst_LJ_undef_fw, assumption, auto)

lemma or_undef_congr1[simp]:
  (τ ⊨ ⊥ ∨ B) = (τ ⊨ B)
  by (simp add: OclOr_def)

lemma not_and_undef_congr2[simp]:
  (τ ⊨ ¬ (B ∧ ⊥)) = (τ ⊨ ¬ B)
  by (subst and_commute, simp add: not_and_undef_congr1)

lemma or_undef_congr2[simp]:
  (τ ⊨ B ∨ ⊥) = (τ ⊨ B)
  by (simp add: OclOr_def)
\end{verbatim}

390
lemma and_undef_congr3 [simp]:
\( \neg (\tau \models \bot \land B) \)
apply (cut_tac \( \tau = \tau \) and \( A = B \) in non_quatium_datur)
apply auto
apply (drule_tac \( P = \lambda B. (\bot \land B) \) in subst_LJ_TRUE_fw_rev)
apply simp_all
by (drule_tac subst_LJ_undef_fw, assumption, auto)

lemma and_undef_congr4 [simp]:
\( \neg (\tau \models B \land \bot) \)
by (subst and_commute, simp add: not_and_undef_congr1)

lemma and_FALSE_I_core:
\llbracket (\tau \models \neg A) \lor (\tau \models \neg B) \rrbracket = \Rightarrow \tau \models \neg (A \land B)
by (auto elim: subst_LJ_FALSE)

lemmas and_FALSE_I = disjCI [THEN and_FALSE_I_core, standard]

lemma and_FALSE_I1:
\llbracket (\tau \models B) \lor (\tau \models \neg B) \rrbracket = \Rightarrow \tau \models \neg (A \land B)
by (rule and_FALSE_I, simp only: not_invalid)

lemma and_FALSE_E:
\llbracket \tau \models \neg (A \land B); \tau \models \neg A \Rightarrow R; \tau \models \neg B \Rightarrow R \rrbracket = \Rightarrow R
apply (cut_tac \( \tau = \tau \) and \( A = A \) in non_quatium_datur)
apply auto
apply (rotate_tac \(-1\))
apply (drule_tac \( P = \lambda Y St. (X \lor Y) \) in subst_LJ_FALSE_fw)
apply assumption
prefer 3
apply auto
done

lemma or_2_classic_disj:
\llbracket \tau \models \partial X; \tau \models \partial Y \rrbracket = \Rightarrow (\tau \models X \lor Y) = ((\tau \models X) \lor (\tau \models Y))
apply auto
deffer 1 apply (erule_tac \( P = \lambda X St. (X \lor Y) \) St in subst_LJ_TRUE)
prefer 3 apply (erule_tac \( P = \lambda Y St. (X \lor Y) \) St in subst_LJ_TRUE)
apply (auto simp; not_valid)
apply (rotate_tac \(-1\))
apply (drule_tac \( P = \lambda Y St. (X \lor Y) \) St in subst_LJ_FALSE_fw)
apply auto
done
Appendix B. Isabelle Theories

**lemma isdef_and_congr:**

\[
(τ ⊨ (X \land Y)) = ((τ ⊨ X \land τ X) \lor (τ ⊨ Y \land τ Y))
\]

apply (auto simp: isDefined_andD0 or_2_classic_disj or_2_classic_disj)
apply (simp_all add: or_2_classic_disj)
done

**lemma solution0:**

\[
[ ((τ ⊨ τ X) \land (τ ⊨ τ Y)) \lor ((τ ⊨ τ X) \land (τ ⊨ τ X)) \lor ((τ ⊨ τ Y) \land (τ ⊨ τ Y)) ]
\Rightarrow τ ⊨ (X \land Y)
\]
by (simp add: isdef_and_congr and_congr)

**lemma solution1:**

\[
[ ((τ ⊨ τ B) \land (τ ⊨ τ A)) \sim = T ]
\Rightarrow (τ ⊨ τ B) \land (τ ⊨ τ B)
\]
apply (simp add: OclLocalValid_def[symmetric])
apply (rule solution0)
apply (cases ~ τ ⊨ τ B \land ~ B, simp_all)
apply (cases ~ τ ⊨ τ A \land ~ A, simp_all)
apply (auto elim!: and_TRUE_E or_def)
done

**lemma solution2:**

\[
[ τ ⊨ (τ B \land ∼ B): τ ⊨ (τ A \land ∼ A) ]
\Rightarrow (τ ⊨ τ A) \land (τ ⊨ τ B)
\]
apply (rule solution1)
apply (simp only: OclLocalValid_def[symmetric] not_valid)
apply auto
done

**lemma isDefined_and_TRUE_E:**

\[
[ (τ ⊨ τ B) \lor (τ ⊨ τ B): (τ ⊨ τ A) \lor (τ ⊨ τ A) ]
\Rightarrow (τ ⊨ τ A) \land (τ ⊨ τ B)
\]
apply (rule solution2)
apply (auto elim!: and_FALSE_E and_TRUE_E simp add: isDefined_andD0 or_def)
done

**lemma solution3:**
B.5. State

\[
\begin{align*}
&\lbracket \neg (\tau \models \neg A) \lor \neg (\tau \models \neg B) \rbracket \implies (\tau \models \partial A); \\
&\lbracket \neg (\tau \models \neg A) \lor \neg (\tau \models \neg B) \rbracket \implies (\tau \models \partial B) \\
&\implies \tau \models \partial (A \land B)
\end{align*}
\]

apply (rule isDefined_and_TRUE_I)
apply (simp only: not_INVALID)
apply auto
done

lemma isDefined_and_TRUE_E:
\[
\begin{align*}
&\lbracket \tau \models \partial (A \land B); \\
&\lbracket \tau \models \partial A; \tau \models \partial B \rbracket \implies R; \\
&\tau \models \neg A \implies R; \\
&\tau \models \neg B \implies R \\
&\implies R
\end{align*}
\]

by (auto elim!: and_FALSE_E and_TRUE_E
simp add: isDefined_andD0 OclOr_def)

The following rule follows the principal equality:
\[
\tau \models \partial (A \land B) = \tau \models ((\partial A \lor \partial B) \land (\partial A \land \partial B))
\]  
(B.20)

Via isDefined_andD0, de_morgan1, and de_morgan2 one gets:
\[
= \tau \models (\neg A \land \neg B) \land (\neg A \land \neg B) 
\]  
(B.21)

lemma isDefined_and_FALSE_I:
\[
\begin{align*}
&\lbracket \neg (\tau \models \partial (A \land B)); \\
&\tau \models \neg (\partial A \land \neg A); \\
&\tau \models \neg (\partial B \land \neg B) \rbracket \\
&\implies \tau \models \partial (A \land B)
\end{align*}
\]

by (auto intro!: and_TRUE_I and_FALSE_I elim!: and_FALSE_E and_TRUE_E
simp add: isDefined_andD0 OclOr_def)

lemma isDefined_and_FALSE_I1:
\[
\begin{align*}
&\lbracket (\neg (\tau \models \partial A) \land \neg (\tau \models \neg B)) \lor \\
&\neg (\tau \models \neg A) \land \neg (\tau \models \neg B) \rbracket \\
&\implies \tau \models \neg (A \land B)
\end{align*}
\]

apply (rule isDefined_and_FALSE_I)
apply (simp_all add: not_valid)
apply (auto elim!: subst_LJ_undef subst_LJ_TRUE subst_LJ_FALSE subst_LJ_FALSE)
done

lemma isDefined_and_FALSE_I2:
\[
\begin{align*}
&\lbracket (\neg (\tau \models \neg A) \lor \neg (\tau \models \partial B)) \implies \tau \models \partial A; \\
&\neg (\tau \models \neg A) \land \neg (\tau \models \neg B) \implies (\tau \models \neg B) \\
&\implies \tau \models \partial (A \land B)
\end{align*}
\]

apply (rule isDefined_and_FALSE_I1)

lemma isDefined_and_FALSE_Id:
\[
\begin{align*}
&\lbracket (\neg A) \lor \neg (\tau \models \partial B) \implies \tau \models \partial A; \\
&\neg (\tau \models \neg A) \land \neg (\tau \models \neg B) \implies (\tau \models \neg B) \\
&\implies \tau \models \partial (A \land B)
\end{align*}
\]

apply (rule isDefined_and_FALSE_I1)

393
Appendix B. Isabelle Theories

apply(auto simp del: isDefined_if_valid isDefined_if_invalid)
done

lemma isDefined_and_FALSE_I3:
  assumes A: \((\tau \models \\emptyset B) \implies (\tau \models \neg A)\) \implies \tau \models \emptyset A
  and B: \((\tau \models \emptyset B) \implies (\tau \models \neg A)\) \implies \sim (\tau \models \neg B)
  shows \(\tau \models \emptyset (A \land B)\)
    apply (rule isDefined_and_FALSE_I2)
    apply (rule A)
    apply (rule_tac [2] B)
    apply auto
    done

lemma isDefined_and_FALSE_I4:
  \[\tau \models (\emptyset B) \implies (\tau \models \emptyset A); 
  \tau \models (\emptyset A) \implies (\tau \models A); 
  \tau \models (\emptyset B) \implies (\tau \models B) \]
  \implies \tau \models \emptyset (A \land B)
  apply (rule isDefined_and_FALSE_I)
  apply (rule and_FALSE_I)
  prefer 2
  apply (subst and_commute)
  apply (rule_tac and_FALSE_I)
  prefer 3
  apply (subst and_commute)
  apply (rule_tac and_FALSE_I)
  apply(auto simp del: isDefined_if_valid isDefined_if_invalid)
  done

lemma isDefined_and_FALSE_I5:
  \[(\tau \models \emptyset A) \lor (\tau \models \emptyset B); 
  (\tau \models \emptyset A) \lor (\tau \models A); 
  (\tau \models \emptyset B) \lor (\tau \models B) \]
  \implies \tau \models \emptyset (A \land B)
  apply(simp add: isDefined_andD0 de_morgan1 de_morgan2 
  and_congr' or_2_classic_disj)
  apply(auto elim!: subst_LJ_undef subst_LJ_TRUE subst_LJ_FALSE 
  simp del: isDefined_if_valid 
  not_isUndefined_eq_isDefined)
  done

lemma isDefined_and_FALSE_E:
  \[
  \tau \models \emptyset (A \land B); 
  \tau \models \emptyset A; \tau \models \emptyset B\] \implies R;
  \[
  \tau \models \emptyset A; \tau \models B\] \implies R;
  \[
  \tau \models A; \tau \models \emptyset B\] \implies R]
\[ \implies R \]
by (auto elim: and_TRUE_E and_FALSE_E simp add: isDefined_andD0 OclOr_def)

**lemmas** isDefined_TRUE_E = non_ternium_datur_if_isDefined

**lemma** isDefined_TRUE_I:
\[ \llbracket \tau \models A \lor (\tau \models \neg A) \rrbracket \implies \tau \models \partial A \]
apply (erule disjE)
apply (drule isDefined_if_valid)
apply (drule_tac [2] isDefined_if_invalid)
apply auto
done

**lemma** isDefined_TRUE_I1:
\[ \llbracket (\tau \models A) \lor (\tau \models (\neg \partial A)) \rrbracket \implies \tau \models (\partial A) \]
apply (rule isDefined_TRUE_I)
apply (auto simp del: isDefined_if_valid isDefined_if_invalid)
apply (simp only: not_valid not_not isDefined_notD0)
done

**lemma** not_not_E:
\[ \llbracket \neg \neg A \models \neg \neg A ; \tau \models A \implies R \rrbracket \implies R \]
by auto

**lemma** not_not_D:
\[ \tau \models \neg \neg A \implies \tau \models A \]
by auto

**lemma** not_not_I:
\[ \llbracket \tau \models A \rrbracket \implies \tau \models \neg \neg A \]
by auto

**lemma** isDefined_not_TRUE_E:
\[ \llbracket \tau \models \neg \partial (\neg A) \rrbracket \implies \tau \models \neg \partial A \]
by auto

**lemma** isDefined_not_TRUE_I:
\[ \llbracket \tau \models \neg \partial A \rrbracket \implies \tau \models \neg \partial (\neg A) \]
by auto

**lemma** isDefined_not_FALSE_E:
\[ \llbracket \tau \models \neg \partial (\neg A) \rrbracket \implies \tau \models \neg \partial A \]
by auto

**lemma** isDefined_not_FALSE_I:
\[ \llbracket \tau \models \neg \partial A \rrbracket \implies \tau \models \neg \partial (\neg A) \]
by auto
Appendix B. Isabelle Theories

Driven rules for the or

\textbf{lemma} or\_TRUE\_I\_core:\n\begin{align*}
\forall \tau \exists A, B. \; (\tau \models A) \vee (\tau \models B) & \implies \tau \models A \vee B \\
\text{apply (unfold OclOr\_def)} \\
\text{apply (rule and\_FALSE\_I\_core)} \\
\text{apply auto} \\
\text{done}
\end{align*}

\textbf{lemmas} or\_TRUE\_I = disjCI [THEN or\_TRUE\_I\_core, standard]

\textbf{lemma} or\_FALSE\_I:\n\begin{align*}
\forall \tau \exists A, B. \; (\tau \models \neg A) \wedge (\tau \models \neg B) & \implies \tau \models \neg (A \vee B) \\
\text{apply (unfold OclOr\_def)} \\
\text{apply (rule not\_not\_I)} \\
\text{apply (rule and\_TRUE\_I)} \\
\text{apply auto} \\
\text{done}
\end{align*}

\textbf{lemma} or\_TRUE\_E:\n\begin{align*}
\forall \tau \exists A, B, R. \; (\tau \models A \vee B) & \implies \tau \models R \\
\text{apply (unfold OclOr\_def)} \\
\text{apply (auto elim!: and\_TRUE\_E and\_FALSE\_E simp add: isDefined\_andD0 OclOr\_def)} \\
\text{done}
\end{align*}

\textbf{lemma} or\_FALSE\_E:\n\begin{align*}
\forall \tau \exists A, B, R. \; (\tau \models \neg (A \vee B)) & \implies \tau \models R \\
\text{apply (unfold OclOr\_def)} \\
\text{apply (auto elim!: and\_TRUE\_E and\_FALSE\_E simp add: isDefined\_andD0 OclOr\_def)} \\
\text{done}
\end{align*}

\textbf{lemma} isDefined\_or\_TRUE\_I:\n\begin{align*}
\forall \tau \exists A, B, R. \; ((\tau \models \emptyset A) \vee (\tau \models \emptyset B)) & \implies \tau \models \emptyset (A \vee B) \\
\text{apply (unfold OclOr\_def)} \\
\text{apply (rule isDefined\_not\_TRUE\_I)} \\
\text{apply (rule isDefined\_and\_TRUE\_I)}
\end{align*}
B.5. State

apply auto
done

lemma isDefined_or_FALSE_I1:
\[ \tau \models \emptyset B \implies \tau \not\models \emptyset A; \]
\[ \tau \models \emptyset A \implies \tau \models \neg A; \]
\[ \tau \models \emptyset B \implies \tau \models \neg B \]
\[ \implies (\tau \models \emptyset (A \lor B)) \]
apply (unfold OclOr_def)
apply (rule isDefined_not_FALSE_I)
apply (rule isDefined_and_FALSE_I4)
apply auto
done

lemma isDefined_or_FALSE_I:
\[ (\tau \models A) \lor \neg (\tau \models \emptyset B) \implies (\tau \models \emptyset A); \]
\[ (\tau \models A) \lor \neg (\tau \models \emptyset B) \implies \neg (\tau \models B) \]
\[ \implies (\tau \models \emptyset (A \lor B)) \]
apply (unfold OclOr_def)
apply (rule isDefined_not_FALSE_I)
apply (rule isDefined_and_FALSE_I)
apply (rule and_FALSE_I)
apply (rule isDefined_not_FALSE_I)
apply (rule_tac[2] isDefined_not_FALSE_I)
apply (rule_tac[3] isDefined_not_FALSE_I)
apply auto
apply (simp_all only: not_valid)
apply (auto simp: isDefined_if_valid)
done

lemma isDefined_or_FALSE_E:
\[ (\tau \models \emptyset (A \lor B)); \]
\[ (\tau \models \emptyset A; \tau \models \emptyset B) \implies R; \]
\[ (\tau \models \emptyset A; \tau \models \neg B) \implies R; \]
\[ (\tau \models \neg A; \tau \models \emptyset B) \implies R \]
\[ \implies R \]
apply (unfold OclOr_def)
apply (drule isDefined_not_FALSE_E)
apply (auto elim!: and_TRUE_E and_FALSE_E isDefined_and_FALSE_E
simp add: isDefined_andD0 OclOr_def)
done

lemma isDefined_or_TRUE_E:
\[ (\tau \models \emptyset (A \lor B)); \]

397
Appendix B. Isabelle Theories

\[
\begin{align*}
& \vdash \varnothing \models A; \varnothing \models \varnothing B \implies R; \\
& \varnothing \models B \implies R; \\
& \varnothing \models A \implies R \\
\end{align*}
\]
apply \(\text{unfold OclOr_def}\)
apply \(\text{drule isDefined\_not\_TRUE\_E}\)
apply \(\text{erule isDefined\_and\_TRUE\_E}\)
apply auto
done

\text{lemma \ strongEq\_distrib\_if1:}
\[\vdash \varnothing X \implies (A \models (\text{if } X \text{ then } Y \models B \text{ else } Z \models A \text{ endif}) = (\text{if } X \text{ then } Y \models A \text{ else } Z \models A \text{ endif}))\]
by (rule if\_distrib2, auto simp: OclValid_def OclLocalValid_def)

\text{lemma \ strongEq\_distrib\_if2:}
\[\vdash \varnothing X \implies ((\text{if } X \text{ then } Y \models B \text{ else } Z \models A \text{ endif}) = (\text{if } X \text{ then } Y \models A \text{ else } Z \models A \text{ endif}))\]
by (rule if\_distrib2, auto simp: OclValid_def OclLocalValid_def)

\text{lemma \ cp\_local\_valid [simp.intro]:}
cp P \implies cp (\lambda X. \tau. (\varnothing \models P X))
by (auto simp: OclValid_def OclLocalValid_def)

\text{lemma \ and\_congr:}
\[
\begin{align*}
& [(\varnothing \models A) \lor (\varnothing \models \varnothing A) \implies (\varnothing \models B) = (\varnothing \models B')] \\
& \implies (\varnothing \models A \land B) = (\varnothing \models A \land B') \\
& \text{apply (cut_tac } \tau = \tau \text{ and } A = A \text{ in non_quatrum_datur) } \\
& \text{apply (rule_tac } X = A \text{ in } \text{cp\_distinct\_core\_P) } \\
& \text{apply (auto simp: OclLocalValid\_def[symmetric])} \\
& \text{done}
\end{align*}
\]

\text{lemma \ and\_congr\_a:}
\[
\begin{align*}
& [(\varnothing \models \varnothing A; \varnothing \models A \implies (\varnothing \models B) = (\varnothing \models B')] \\
& \implies (\varnothing \models A \land B) = (\varnothing \models A \land B') \\
& \text{apply (rule and\_congr)} \\
& \text{apply auto} \\
& \text{done}
\end{align*}
\]

\text{lemma \ and\_congr\_b:}

398
B.5. State

\[ \tau \models \neg A; \tau \models \partial A \implies (\tau \models B) = (\tau \models B') \]
apply (rule and_congr)
apply auto
done

lemma not_congr:
\[ \tau = \tau' \implies (\tau \models \neg A) = (\tau \models \neg A') \]
apply (rule not_congr)
apply (subst equiv_D_local) back
apply auto
done

The relevance for automated deduction becomes apparent with the next rewrite rule, which boils down reductions in local congruences to check if the definedness is equivalent. This can be decomposed into two meta-implications; the advantage of this is presentation comes from the fact that such derivations are particularly easy and can be supported automatically by a forward-closure tactic for literals contained in valid definedness formulas. It has to be checked if the recomputation of these literals can be avoided.

lemma or_congr:
\[ \tau = \tau' \implies (\tau \models \partial A') \]
apply (rule_tac P = \lambda A \tau. (\tau \models \partial A) in ocl_cp_subst)
apply (rule sym, assumption)
apply (rule_tac P = \lambda B \tau. (\tau \models \partial B) in ocl_cp_subst)
apply auto
done

lemma or_congr0:
\[ (\tau \models \partial A) \quad (\tau \models \partial A') \]
apply (rule or_congr)

399
Appendix B. Isabelle Theories

apply (subst equiv_D_local) back
prefer 2
apply (subst equiv_D_local) back
apply (auto simp: OclLocalValid_def)
apply (auto simp: OclLocalValid_def[ symmetric])
done

lemma if_congr:
   [ \( \tau \models C \implies (\tau \models A) = (\tau \models A') \); 
     \( \tau \not\models C \implies (\tau \models B) = (\tau \models B') \) ]
   \implies ((\tau \models \text{if} C \text{ then } A \text{ else } B \text{ endif}) = 
     (\tau \models \text{if} C \text{ then } A' \text{ else } B' \text{ endif}))
apply (cut_tac \( \tau = \tau \) and \( A = A \) in non_quatrium_datur)
apply (rule_tac X = \( A \) in cp_distinct_core_P)
apply (auto simp: is_FALSE_charn_local OclLocalValid_def[ symmetric])
done

lemma implies_undef_congr[simp]:
   (\( \tau \not\models \bot \longrightarrow B \)) = (\( \tau \models B \))
by (simp add: OclImplies_def)

lemma implies_congr:
   [ (\( \tau \models A \)) \lor (\( \tau \not\models \emptyset \ A \)) \implies (\( \tau \models B \)) = (\( \tau \models B' \) ) ]
   \implies ((\( \tau \models \wedge \ A \longrightarrow B \)) = (\( \tau \models \wedge \ A \longrightarrow B' \)))
apply (cut_tac \( \tau = \tau \) and \( A = A \) in non_quatrium_datur)
apply (rule_tac X = \( A \) in cp_distinct_core_P)
apply (auto simp: isUndefined_charn_local OclLocalValid_def[ symmetric])
done

lemmas LEC = and_congr not_congr or_congr if_congr
       not_and_undef_congr1
       not_and_undef_congr2
       or_undef_congr1
       or_undef_congr2
       and_undef_congr3
       and_undef_congr4
       implies_undef_congr
end

B.5.3. Encoding of OCL Operations

theory OCL_Operation
imports
   $HOLOCL_HOME/src/OCL_Calculi
begin

400
Standard and Strict Method Invocation, and Recursion

The core primitives \texttt{OCL\_choose} and \texttt{OCL\_invoke}, its strict variant \texttt{OCL\_invokeS} are used to represent method.

\begin{verbatim}
consts OCL\_choose :: (\tau \Rightarrow \text{Boolean} \Rightarrow \tau) \Rightarrow (\tau \Rightarrow \tau)
OCL\_choose F \equiv (\lambda \tau. \text{SOME } x. \tau \Rightarrow \tau = \text{T} \tau)
lemma cp F \Rightarrow cp(OCL\_choose F)
apply(simp add: cp_def OCL\_choose_def)
apply safe
apply (rule exI, rule allI, rule allI)
apply (simp)
oops

consts OCL\_invoke :: (\tau \Rightarrow \text{Boolean} \Rightarrow \tau) \Rightarrow (\tau \Rightarrow \tau)
consts OCL\_invokeS :: (\tau \Rightarrow \text{Boolean} \Rightarrow \tau) \Rightarrow (\tau \Rightarrow \tau)

Instance for null-ary invocation with return value:
\begin{verbatim}
OCL\_invoke (C :: \tau \Rightarrow \text{a})
(tab :: \tau \Rightarrow \text{a} \Rightarrow \text{b} \Rightarrow \text{c})
(self :: \tau \Rightarrow \text{b}) (result :: \tau \Rightarrow \text{c})
\end{verbatim}
\end{verbatim}

\begin{verbatim}
defs OCL\_invoke0\_def :
  OCL\_invoke C tab self result \equiv
  \lambda St. (case tab (LEAST X. X \in \text{dom tab} \land C(self St) \in X) of
  None \Rightarrow \text{arbitrary}
  | Some f \Rightarrow f(self::\text{a} \Rightarrow \text{b})
  (result::\text{c} St)

defs OCL\_invoke0\_S\_def :
  OCL\_invokeS C tab self result \equiv
  (if \partial(self) then OCL\_invoke C tab self result else \bot endif)

lemma OCL\_invoke0\_S\_undef0[simp] :
  OCL\_invokeS C (tab::\text{c} \Rightarrow (\text{a} \Rightarrow \text{d} : \text{bot} \Rightarrow \text{c} \Rightarrow \text{e} : \text{bot} : \text{bot}) \Rightarrow \text{b} : \text{bot}) \Rightarrow \bot X
  = \bot
  by(simp add: OCL\_invoke0\_S\_def)

lemma OCL\_invoke0\_S\_is\_def :
  \partial(OCL\_invokeS C)
  (tab::\text{c} \Rightarrow (\text{a} \Rightarrow \text{d} : \text{bot} \Rightarrow \text{c} \Rightarrow \text{e} : \text{bot} : \text{bot} \Rightarrow \text{a} \Rightarrow \text{b} : \text{bot})
\end{verbatim}

\end{verbatim}
Appendix B. Isabelle Theories

```
self result) \implies
\begin{align*}
\vdash & \partial (\text{self}) \\
\text{by} & (\text{simp add: } \text{OCL\textunderscore invoke0S\textunderscore def isDefined\textunderscore ifD0 globalValidAnd2conj})
\end{align*}
```

Instance for binary invocation:

```
\text{OCL\textunderscore invoke} (C \text{::'} a \Rightarrow e) \\
(\text{tab ::' eset} \Rightarrow (s \Rightarrow' a) \Rightarrow (s \Rightarrow' b) \Rightarrow (s \Rightarrow' c) \Rightarrow s \Rightarrow d)(\text{self ::'} s \Rightarrow' a) \\
(a ::' s \Rightarrow' b)(b ::' s \Rightarrow' c)
```

```
\text{defs } \text{OCL\textunderscore invoke1\textunderscore def}:
\text{OCL\textunderscore invoke} C \text{tab self a result} \\
\equiv \lambda \tau . (\text{case tab } (\text{LEAST } X. X \in \text{dom tab} \land C(\text{self } \tau) \in X) \text{ of} \\
None \Rightarrow \text{arbitrary} \\
| \text{Some } f \Rightarrow f(\text{self ::'} \tau \Rightarrow'a) \\
(a ::' \tau \Rightarrow' b) (result ::' \tau \Rightarrow' c) \\
\text{defs } \text{OCL\textunderscore invoke1S\textunderscore def}:
\text{OCL\textunderscore invokeS} C \text{tab self a result} \\
\equiv (\text{if } \partial (\text{self}) \text{ and } \partial (a) \text{ then } \text{OCL\textunderscore invoke} C \text{tab } \text{self } (a ::' \tau \Rightarrow' b)(\text{result ::'} \tau \Rightarrow' c) \\
\text{else } \bot \text{ endif})
```

```
\text{lemma } \text{OCL\textunderscore invoke1S\textunderscore undef}\textunderscore simp] :
\text{OCL\textunderscore invokeS} C \\
(\text{tab ::' eset} \Rightarrow (s \Rightarrow' a \Rightarrow' b \Rightarrow' c \Rightarrow' d))(\text{self ::'} s \Rightarrow' a) \\
\text{by} (\text{simp add: } \text{OCL\textunderscore invoke1S\textunderscore def})
```

```
\text{lemma } \text{OCL\textunderscore invoke1S\textunderscore undef}\textunderscore simp] :
\text{OCL\textunderscore invokeS} C \\
(\text{tab ::' eset} \Rightarrow (\text{self ::'} \tau \Rightarrow' a \Rightarrow' b \Rightarrow' c \Rightarrow' d))(\text{self ::'} s \Rightarrow' a) \\
= \bot \\
\text{by} (\text{simp add: } \text{OCL\textunderscore invoke1S\textunderscore def})
```

```
\text{lemma } \text{OCL\textunderscore invoke2S\textunderscore is\textunderscore def}:
\vdash \partial (\text{OCL\textunderscore invokeS} C) \\
(\text{tab ::' eset} \Rightarrow (s \Rightarrow' a \Rightarrow' b \Rightarrow' c \Rightarrow' d))(\text{self ::'} s \Rightarrow' a) \\
\text{by} (\text{simp add: } \text{OCL\textunderscore invoke1S\textunderscore def isDefined\textunderscore ifD0 globalValidAnd2conj})
```

Instance for Binary Invocation:

```
\text{defs } \text{OCL\textunderscore invoke2\textunderscore def}:
```

B.5. State

OCL_invoke C tab self a b result
≡ λ St. (case tab (LEAST X. X ∈ dom tab ∧ C(self St) ∈ X) of
None ⇒ arbitrary
| Some f ⇒ f (self; s⇒'a)(a; s⇒'b)(b; s⇒'c)(result; s⇒'d) St )

defs

OCL_invokeCS_def:
OCL_invoke C tab self a b result
≡ (if (∂(self) and ∂(a)) and ∂(b)
then OCL_invoke C tab (self; s⇒'a; bot)
(a; s⇒'b; bot) (b; s⇒'c; bot)
(result; s⇒'d)
else ⊥
endif)

lemma OCL_invoke2S_undef0[simp] :
OCL_invoke C tab self a b result
= ⊥
by(simp add: OCL_invokeC_def)

lemma OCL_invoke2S_undef1[simp] :
OCL_invoke C tab self a b result
= ⊥
by(simp add: OCL_invokeC_def)

lemma OCL_invoke2S_undef2[simp] :
OCL_invoke C tab self a b result
= ⊥
by(simp add: OCL_invokeC_def)

lemma OCL_invoke2S_is_def:
≡ (∂(OCL_invoke C tab self a b result)
= (if (∂(self) and ∂(X) and ∂(Y)
X Y result)
by(simp add: OCL_invoke2S_def isDefined_ifD0 globalValidAnd2conj)
end
Appendix B. Isabelle Theories

B.5.4. The Object Constraint Language: OCL

theory UML_OCL
imports $HOLOCL_HOME/src/OCL_State $HOLOCL_HOME/src/OCL_Operation begin

The Theory-Morpher

In the theory file, this section contains an SML program implementing a theory morphism from HOL to HOL-OCL. It filters all combinator-based definitions in HOL-OCL, constructs a one-to-one constant symbol based signature morphism between the HOL and the HOL-OCL theory (modulo argument permutation), uses this signature morphism to translate HOL theorems to HOL-OCL proof goals and attempts to prove them with a generic case split tactic. For conceptual details, see [13].

end

B.6. Requirements

In this section, we present the requirements from the normative part of the OCL standard [41, Chapter 11] and prove (or disprove) that our embedding is faithful to these requirements.

At time of writing, this is work in progress and not all requirements are analyzed. This section will be improved in one of the next releases of HOL-OCL.

B.6.1. Requirements for OCL Primitive Types

theory OCL_Basic_requirements
imports $HOLOCL_HOME/src/OCL_Library
begin

This theory contains the requirements for the primitive types defined in the OCL standard library (Integer, Real, String, and Boolean) [41, Chapter 11.5].

Real

+ (r : Real) : Real

The value of the addition of self and r.

(11.5.1-a)
B.6. Requirements

- \( (r : \text{Real}) : \text{Real} \)  
  The value of the subtraction of \( r \) from \( \text{self} \).  
  (11.5.1-b)

* \( (r : \text{Real}) : \text{Real} \)  
  The value of the multiplication of \( \text{self} \) and \( r \).  
  (11.5.1-c)

- \( : \text{Real} \)  
  The negative value of \( \text{self} \).  
  (11.5.1-d)

/ \( (r : \text{Real}) : \text{Real} \)  
  The value of \( \text{self} \) divided by \( r \).  
  (11.5.1-e)

abs() : \text{Real}  
The absolute value of \( \text{self} \).  
(11.5.1-f)

\[ \text{post: } \begin{cases} \text{if } \text{self} < 0 \text{ then result} = - \text{self} \\ \text{else result} = \text{self} \end{cases} \]  
\text{endif}

lemma req_11_5_1-f:  
( \text{self} \rightarrow \text{abs}(\text{self})) = (\text{if} (\text{self} < 0) \text{ then OclNegative self else self endif})

floor() : \text{Integer}  
The largest integer which is less than or equal to \( \text{self} \).  
(11.5.1-g)

\[ \text{post: } (\text{result} \leq \text{self}) \text{ and } (\text{result} + 1 > \text{self}) \]

lemma req_11_5_1-g:  
\( \models ((\text{self} \rightarrow \text{floor}(\text{self})) \rightarrow \text{toReal}(\text{self}) \leq \text{self}) \text{ and } ((\text{self} \rightarrow \text{floor}(\text{self}) + 1) \rightarrow \text{toReal}(\text{self}) > \text{self}) \)

oops

round() : \text{Integer}  
The integer which is closest to \( \text{self} \). When there are two such integers, the largest one.  
(11.5.1-h)

\[ \text{post: } (\text{result} \rightarrow \text{abs}(\text{result}) < 0.5) \text{ or } ((\text{self} \rightarrow \text{result}).\text{abs}(\text{result}) = 0.5 \text{ and } (\text{result} > \text{self})) \]

lemma req_11_5_1-h: true

oops
Appendix B. Isabelle Theories

\textbf{max}(r : \text{Real}) : \text{Real} \hfill (11.5.1-i)
\begin{align*}
\text{The maximum of self and } r.
\end{align*}
\begin{align*}
\text{post}: & \quad \text{if self } \geq r \text{ then result } = \text{self} \\
& \quad \text{else result } = r \\
& \quad \text{endif}
\end{align*}

\textbf{min}(r : \text{Real}) : \text{Real} \hfill (11.5.1-j)
\begin{align*}
\text{The minimum of self and } r.
\end{align*}
\begin{align*}
\text{post}: & \quad \text{if self } \leq r \text{ then result } = \text{self} \\
& \quad \text{else result } = r \\
& \quad \text{endif}
\end{align*}

\textbf{<} (r : \text{Real}) : \text{Boolean} \hfill (11.5.1-k)
\begin{align*}
\text{True if self is less than } r.
\end{align*}
\begin{align*}
\text{post}: & \quad \text{result } = \neg (\text{self } \leq r)
\end{align*}

\textbf{>} (r : \text{Real}) : \text{Boolean} \hfill (11.5.1-l)
\begin{align*}
\text{True if self is greater than } r.
\end{align*}
\begin{align*}
\text{post}: & \quad \text{result } = \neg (\text{self } \leq r)
\end{align*}

\textbf{\leq} (r : \text{Real}) : \text{Boolean} \hfill (11.5.1-m)
\begin{align*}
\text{True if self is less than or equal to } r.
\end{align*}
\begin{align*}
\text{post}: & \quad \text{result } = ((\text{self } = r) \text{ or } (\text{self } < r))
\end{align*}

\textbf{\geq} (r : \text{Real}) : \text{Boolean} \hfill (11.5.1-n)
\begin{align*}
\text{True if self is greater than or equal to } r.
\end{align*}
\begin{align*}
\text{post}: & \quad \text{result } = ((\text{self } = r) \text{ or } (\text{self } > r))
\end{align*}

\textbf{Integer}

\textbf{-} : \text{Integer} \hfill (11.5.2-a)
\begin{align*}
\text{The negative value of self.}
\end{align*}
B.6. Requirements

\[ + (i : \text{Integer}) : \text{Integer} \]
The value of the addition of self and i.

\[ - (i : \text{Integer}) : \text{Integer} \]
The value of the subtraction of i from self.

\[ * (i : \text{Integer}) : \text{Integer} \]
The value of the multiplication of self and i.

\[ / (i : \text{Integer}) : \text{Real} \]
The value of self divided by i.

\[ \text{abs()} : \text{Integer} \]
The absolute value of self.

\[ \text{div}(i : \text{Integer}) : \text{Integer} \]
The number of times that i fits completely within self.

\[ \text{mod}(i : \text{Integer}) : \text{Integer} \]
The result is self modulo i.

\[ \text{max}(i : \text{Integer}) : \text{Integer} \]
The maximum of self an i.
### Appendix B. Isabelle Theories

**min(i : Integer) : Integer**  
(11.5.2-j)  
The minimum of self and i.  

| post: if self <= i then result = self  
else result = i  
endif |
|---|---|

**String**

**size() : Integer**  
(11.5.3-a)  
The number of characters in self.

**concat(s : String) : String**  
(11.5.3-b)  
The concatenation of self and s.  

| post: result.size() = self.size() + string.size()  
post: result.substring(1, self.size()) = self  
post: result.substring(self.size() + 1, result.size()) = s |
|---|---|

**substring(lower : Integer, upper : Integer) : String**  
(11.5.3-c)  
The sub-string of self starting at character number lower, up to and including character number upper. Character numbers run from 1 to self.size().  

| pre: 1 <= lower  
pre: lower <= upper  
pre: upper <= self.size() |
|---|---|

**toInteger() : Integer**  
(11.5.3-d)  
Converts self to an Integer value.

**toReal() : Real**  
(11.5.3-e)  
Converts self to a Real value.

**Boolean**
or (b : Boolean) : Boolean
True if either self or b is true.

xor (b : Boolean) : Boolean
True if either self or b is true, but not both.
post: (self or b) and not (self = b)

and (b : Boolean) : Boolean
True if both b1 and b are true.

not : Boolean
True if self is false.
post: if self then result = false
else result = true
endif

implies (b : Boolean) : Boolean
True if self is false, or if self is true and b is true.
post: (not self) or (self and b)

end

B.6.2. OCL Collection requirements

theory OCL_Collection_requirements
imports $HOLOCL_HOME/src/OCL_Library
begin
This theory contains the requirements for the collection types defined in the OCL standard library (Set, OrderedSet, Bag, and Sequence) [1] Chapter 11.7.

Collection
Appendix B. Isabelle Theories

size() : Integer  
The number of elements in the collection self.

<table>
<thead>
<tr>
<th>post: result = self-&gt;iterate(elem; acc : Integer = 0</th>
<th>acc + 1)</th>
</tr>
</thead>
</table>

Set

OrderedSet

Bag

<table>
<thead>
<tr>
<th>lemma req_bag_11_7_1-a:</th>
</tr>
</thead>
<tbody>
<tr>
<td>[</td>
</tr>
<tr>
<td>by(simp add: OCL_Bag.size_by_iterate)</td>
</tr>
</tbody>
</table>

Sequence

<table>
<thead>
<tr>
<th>lemma req_seq_11_7_1-a:</th>
</tr>
</thead>
<tbody>
<tr>
<td>[</td>
</tr>
<tr>
<td>by(simp add: OCL_Sequence.size_by_iterate)</td>
</tr>
</tbody>
</table>

includes(object : T) : Boolean  
True if object is an element of self, false otherwise.

| post: result = (self->count(object) > 0) |
|---|---|

Set

OrderedSet

Bag

<table>
<thead>
<tr>
<th>lemma req_bag_11_7_1-b:</th>
</tr>
</thead>
<tbody>
<tr>
<td>[(obj:('a,'b)VAL) \in (self::('a,'b::bot)Bag) = ((self-&gt;count obj) &gt; 0)]</td>
</tr>
<tr>
<td>by(simp only: OCL_Bag.includes_by_count_UC)</td>
</tr>
</tbody>
</table>

Sequence

<table>
<thead>
<tr>
<th>lemma req_seq_11_7_1-b:</th>
</tr>
</thead>
<tbody>
<tr>
<td>[(obj:('a,'b)VAL) \in (self::('a,'b::bot)Sequence) = ((self-&gt;count obj) &gt; 0)]</td>
</tr>
<tr>
<td>by(simp only: OCL_Sequence.includes_by_count_UC)</td>
</tr>
</tbody>
</table>
excludes(object : T) : Boolean

True if object is not an element of self, false otherwise.

post: result = (self -> count(object) = 0)

Set

OrderedSet

Bag

lemma req_bag_11_7_1-c:
((obj:`a',`b)VAL) \not\in (self:`a',`b:::bot)Bag) = ((self -> count obj) = 0)

oops

Sequence

lemma req_seq_11_7_1-c:
((obj:`a',`b)VAL) \not\in (self:`a',`b:::bot)Sequence) = ((self -> count obj) = 0)

by(simp)
Appendix B. Isabelle Theories

\textbf{count} (object : T) : Integer

The number of times that object occurs in the collection self.

| post: result = self \rightarrow iterate ( elem; acc : Integer = 0 |
| \hspace{1cm} if elem = object then acc + 1 else acc endif |

Set

OrderedSet

Bag

| lemma req_bag_11_7_1-d: |
| [ τ \models \partial (\text{obj}::(\text{a},\text{b})\text{VAL}) ] \Rightarrow |
| ((self::(\text{a},\text{b}::\text{bot})\text{Bag} \rightarrow \text{count} \text{ obj } ) \tau = |
| (self \rightarrow iterate (x; y=0 | (if (x \neq \text{obj}) \text{ then } (y + 1) \text{ else } \text{yendif})) \tau |
| by (simp add: OCL_Bag.count_by_iterate OCL_Bag.OclIterate_def |
| OclIf_def localValid2sem ss_lifting') |

Sequence

| lemma req_seq_11_7_1-d: |
| [ τ \models \partial (\text{obj}::(\text{a},\text{b})\text{VAL}) ] \Rightarrow |
| ((self::(\text{a},\text{b}::\text{bot})\text{Sequence} \rightarrow \text{count} \text{ obj } ) \tau = |
| (self \rightarrow iterate (x; y=0 | (if (x \neq \text{obj}) \text{ then } (y + 1) \text{ else } \text{yendif})) \tau |
| by (simp add: OCL_Sequence.count_by_iterate OCL_Sequence.OclIterate_def |
| OclIf_def localValid2sem ss_lifting') |
**B.6. Requirements**

**includesAll(c2 : Collection(T)) : Boolean**

Does self contain all the elements of c2?

**post: result = c2->forAll(elem | self->includes(elem))**

**Set**

If self = ⊥ and (obj = {}) then the left-hand side of the equation evaluates to ⊥ whereas the right-hand side evaluates to T.

**Wrong definition of the correspondence of includesAll and iterate**

**Lemma req_set_11_7_1-e:**

\[
((\text{self}:('\tau','\alpha::\text{bot})\text{Set}) \rightarrow \text{includesAll}(\text{obj}))
\]

\[
= (\text{obj} \rightarrow \text{forAll}(\text{elem} | (\text{self} \rightarrow \text{includes}(\text{elem}:'(\tau,'\alpha::\text{bot})\text{VAL})))) = \text{False}
\]

**apply(simp add: OclIncludes_def OclIncludesAll_def OclForAll_def lift0_def lift1_def lift2_def strictify_def DEF_def)**

**oops**

**OrderedSet**

**Lemma req_bag_11_7_1-e:**

\[
\left[ \tau \models \partial(\text{self}:('\alpha,'\beta::\text{bot})\text{Bag}) \right] \Rightarrow
\]

\[
(\text{OclIncludesAll self obj}) \tau = (\forall \text{elem} \in \text{obj} \cdot ((\text{elem}:'(\alpha,\beta)\text{VAL}) \in \text{self})) \tau
\]

**oops**

**Sequence**

**Lemma req_seq_11_7_1-e:**

\[
\left[ \tau \models \partial(\text{self}:('\alpha,'\beta::\text{bot})\text{Sequence}) \right] \Rightarrow
\]

\[
(\text{OclIncludesAll self obj}) \tau = (\forall \text{elem} \in \text{obj} \cdot ((\text{elem}:'(\alpha,\beta)\text{VAL}) \in \text{self})) \tau
\]

**apply(rule_tac X=\text{self} in Sequence_sem_cases)**

**apply(rule_tac X=\text{obj} in Sequence_sem_cases)**

**apply(simp_all add: localValidDefined2sem DEF_def)**

**apply(auto simp: OCL_Sequence.OclForAll_def OCL_Sequence.OclIncludesAll_def OclStrongEq_def)**

**OCL_Sequence.OclIncludes_def ss_lifting’ localValid2sem)**

**done**
Appendix B. Isabelle Theories

excludesAll(c2 : Collection(T)) : Boolean
Does self contain none of the elements of c2 ?

post: result = c2 -> forAll(elem | self -> excludes(elem))

Set

If self = ⊥ and obj = ∅ then the left-hand side of the equation evaluates to ⊥ whereas the right-hand side evaluates to T.

lemma req_set_11_7_1-f:
((self::(τ,α::bot)Set) −>excludesAll(obj))
= (obj −>forAll(elem | (self −>excludes((elem::(τ,α::bot)VAL)))))
apply(rule ext)
apply(simp add: OclExcludes_def OclExcludesAll_def OclForAll_def
lift0_def lift1_def lift2_def strictify_def DEF_def)
apply(auto)
oops

OrderedSet

Bag

lemma req_bag_11_7_1-f:
[τ ⊨ (self::(a,b::bot)Bag)] ➨
τ ⊨ (OclExcludesAll self obj) ≜ (∀ elem ∈ obj . ((elem::(a,b)VAL) ∉ self))
oops

Sequence

lemma req_seq_11_7_1-f:
[τ ⊨ (self::(a,b::bot)Sequence)] ➨
τ ⊨ (OclExcludesAll self obj) ≜ (∀ elem ∈ obj . ((elem::(a,b)VAL) ∉ self))
apply(rule_tac X=self in Sequence_sem_cases)
apply(rule_tac X=obj in Sequence_sem_cases)
apply(simp_all add: localValidDefined2sem DEF_def
OCL_Sequence.OclForAll_def
OCL_Sequence.OclExcludesAll_def OclStrongEq_def
OCL_Sequence.OclIncludes_def ss_lifting localValid2sem
OclNot_def)
done
is\texttt{Empty}() : Boolean

Is self the empty collection?

\textbf{post: }result = ( self \rightarrow \text{size}() = 0 )

\textbf{Set}

Due to our extension to infinite sets, the usual connection between is\texttt{Empty} and size holds only under a precondition

\textbf{lemma} REQ11_7_1_7:
\[
\emptyset = \partial (\text{self} \rightarrow \text{size}()) \\
\implies \text{self} \rightarrow \text{is\texttt{Empty}()} = (\text{self}:(\tau,\alpha:\text{bot}\texttt{Set}) \rightarrow \text{size}()) \equiv 0
\]
\textit{apply} (rule ext)
\textit{apply} (drule_tac \tau = x in valid\_elim)
\textit{apply} (subgoal_tac finite (Lifting.drop (Rep_Set_0 (self x))))
\textit{prefer} 2
\textit{apply} (erule finite\_Sets)
\textit{apply} (simp add: OclIs\texttt{Empty}\_def Ocl\texttt{Size}\_def Ocl\texttt{StrictEq}\_def OCL\_Integer.Zero\_ocl\_int\_def)
\textit{apply} (simp only: lift0\_def lift1\_def lift2\_def
straight\_def o\_def not\_def)
\textit{apply} (simp\_all (no\_asm\_use) add: UU\_fun\_def DEF\_def strictify\_def
split add: split\_if up\_split)
\textit{apply} (simp\_all only: lift0\_def lift1\_def lift2\_def
strictify\_def o\_def not\_def OclIs\texttt{Defined}\_def DEF\_def Ocl\texttt{True}\_def)
\textit{apply} auto
\textit{done}

\textbf{OrderedSet}

\textbf{Bag}

\textbf{lemma} req\_bag\_11\_7\_1\_g:
\[
(\emptyset = \emptyset) = || (\text{self}:(\tau,\alpha:\text{bot}\texttt{Bag}))|| \equiv 0
\]
\textit{apply}(rule Bag\_sem\_cases\_ext, simp\_all)
\textit{apply}(simp\_all add: OCL\_Bag.Ocl\texttt{Size}\_def OclMt\texttt{Bag}\_def Ocl\texttt{StrictEq}\_def
Zero\_ocl\_int\_def ss\_lifting’)
\textit{done}

\textbf{Sequence}

\textbf{lemma} req\_seq\_11\_7\_1\_g:
\[
(\emptyset = \emptyset) = || (\text{self}:(\tau,\alpha:\text{bot}\texttt{Sequence}))|| \equiv 0
\]
\textit{by} simp

\textbf{OrderedSet}

\textbf{Bag}

\textbf{lemma} req\_bag\_11\_7\_1\_g:
\[
(\emptyset = \emptyset) = || (\text{self}:(\tau,\alpha:\text{bot}\texttt{Bag}))|| \equiv 0
\]
\textit{apply}(rule Bag\_sem\_cases\_ext, simp\_all)
\textit{apply}(simp\_all add: OCL\_Bag.Ocl\texttt{Size}\_def OclMt\texttt{Bag}\_def Ocl\texttt{StrictEq}\_def
Zero\_ocl\_int\_def ss\_lifting’)
\textit{done}

\textbf{Sequence}

\textbf{lemma} req\_seq\_11\_7\_1\_g:
\[
(\emptyset = \emptyset) = || (\text{self}:(\tau,\alpha:\text{bot}\texttt{Sequence}))|| \equiv 0
\]
\textit{by} simp

\textbf{OrderedSet}

\textbf{Bag}

\textbf{lemma} req\_bag\_11\_7\_1\_g:
\[
(\emptyset = \emptyset) = || (\text{self}:(\tau,\alpha:\text{bot}\texttt{Bag}))|| \equiv 0
\]
\textit{apply}(rule Bag\_sem\_cases\_ext, simp\_all)
\textit{apply}(simp\_all add: OCL\_Bag.Ocl\texttt{Size}\_def OclMt\texttt{Bag}\_def Ocl\texttt{StrictEq}\_def
Zero\_ocl\_int\_def ss\_lifting’)
\textit{done}

\textbf{Sequence}

\textbf{lemma} req\_seq\_11\_7\_1\_g:
\[
(\emptyset = \emptyset) = || (\text{self}:(\tau,\alpha:\text{bot}\texttt{Sequence}))|| \equiv 0
\]
\textit{by} simp

\textbf{OrderedSet}

\textbf{Bag}

\textbf{lemma} req\_bag\_11\_7\_1\_g:
\[
(\emptyset = \emptyset) = || (\text{self}:(\tau,\alpha:\text{bot}\texttt{Bag}))|| \equiv 0
\]
\textit{apply}(rule Bag\_sem\_cases\_ext, simp\_all)
\textit{apply}(simp\_all add: OCL\_Bag.Ocl\texttt{Size}\_def OclMt\texttt{Bag}\_def Ocl\texttt{StrictEq}\_def
Zero\_ocl\_int\_def ss\_lifting’)
\textit{done}

\textbf{Sequence}

\textbf{lemma} req\_seq\_11\_7\_1\_g:
\[
(\emptyset = \emptyset) = || (\text{self}:(\tau,\alpha:\text{bot}\texttt{Sequence}))|| \equiv 0
\]
\textit{by} simp

\textbf{OrderedSet}

\textbf{Bag}

\textbf{lemma} req\_bag\_11\_7\_1\_g:
\[
(\emptyset = \emptyset) = || (\text{self}:(\tau,\alpha:\text{bot}\texttt{Bag}))|| \equiv 0
\]
\textit{apply}(rule Bag\_sem\_cases\_ext, simp\_all)
\textit{apply}(simp\_all add: OCL\_Bag.Ocl\texttt{Size}\_def OclMt\texttt{Bag}\_def Ocl\texttt{StrictEq}\_def
Zero\_ocl\_int\_def ss\_lifting’)
\textit{done}

\textbf{Sequence}

\textbf{lemma} req\_seq\_11\_7\_1\_g:
\[
(\emptyset = \emptyset) = || (\text{self}:(\tau,\alpha:\text{bot}\texttt{Sequence}))|| \equiv 0
\]
\textit{by} simp
Appendix B. Isabelle Theories

**notEmpty() : Boolean**

Is self not the empty collection?

**post:** \( \text{result} = (\text{self} \rightarrow \text{size()} \not= 0) \)

**Set**

**lemma** req_set_11_7_1-h:

\[ \text{OclNotEmpty}(X::\tau, a::\alpha::\bot\text{ Set}) = \neg (\text{OclIsEmpty}(X)) \]

**apply** (rule ext)

**apply** (simp add: OclNotEmpty_def OclIsEmpty_def OclNot_def)

**apply** (simp only: lift1_def lift2_def strictify_def o_def not_def)

**apply** (simp_all (no_asm_use) add: UU_fun_def DEF_def strictify_def split add: split_if upsplit)

**done**

**OrderedSet**

**Bag**

**lemma** req_bag_11_7_1-h:

\[ (\not= \emptyset \text{ self}) = (\| (\text{self}::a,b::\bot\text{ Bag})\|) \not= \emptyset \]

**by** (simp add: req_bag_11_7_1-h [symmetric])

**Sequence**

**lemma** req_seq_11_7_1-h:

\[ (\not= \emptyset \text{ self}) = (\| (\text{self}::a,b::\bot\text{ Sequence})\|) \not= \emptyset \]

**by** (simp add: req_seq_11_7_1-h [symmetric])
\textbf{B.6. Requirements}

\textbf{sum()} : T \hspace{1cm} (11.7.1-i)

The addition of all elements in self. Elements must be of a type supporting the +
operation. The + operation must take one parameter of type T and be both associ-
ative: \((a+b)+c = a+(b+c)\), and commutative: \(a+b = b+a\). Integer and Real fulfill this
condition.

\textbf{post}: result = self->iterate( elem; acc : T = 0 | acc + elem )

\textbf{Set}

\textbf{OrderedSet}

\textbf{Bag}

\textbf{lemma} req_bag_11_7_1-i:

\(\text{\texttt{sum() S} = ((S::'(a,'b::{bot,plus,zero})Bag}) \rightarrow_{iterate(x;y=0 \mid (x + y)))} \)

\textbf{by}(simp add: OCL_Bag.OclSum_def)

\textbf{Sequence}

\textbf{lemma} req_seq_11_7_1-i:

\(\text{\texttt{sum() S} = ((S::'(a,Integer_0)Sequence}) \rightarrow_{iterate(x;y=0 \mid (x + y)))} \)

\textbf{by}(simp add: OCL_Sequence.OclSum_def)

Note: That this requirement is not fulfilled completely as it currently
holds only for integers. But this will change in the future.
Appendix B. Isabelle Theories

\textbf{product(c2:: Collection(T2)) : Set(Tuple(first: T, second: T2))} \quad (11.7.1-j)

The cartesian product operation of self and c2.

\begin{verbatim}
result =
  self->iterate(e1; acc: Set(Tuple(first: T, second: T2)) = Set{} |
  c2->iterate(e2; acc2: Set(Tuple(first: T, second: T2)) = acc |
                    acc2->including (Tuple(first = e1, second = e2))))
\end{verbatim}

Set

OrderedSet

\textbf{Bag}

\textit{lemma} req_bag_11_7_1–j:

\begin{verbatim}
(OclProduct (self::('a,'b::bot)Bag) (c2::('a,'c::bot)Bag)) =
  (self->iterate(e1; acc=OclMtSet |
                    c2->iterate(e2; acc2=acc |
                               acc2->including (OclTuple e1 e2))))
\end{verbatim}

\textit{oops}

Sequence

\textit{lemma} req_seq_11_7_1–j:

\begin{verbatim}
(OclProduct (self::('a,'b::bot)Sequence) (c2::('a,'c::bot)Sequence)) =
  (self->iterate(e1; acc=OclMtSet |
                    c2->iterate(e2; acc2=acc |
                               acc2->including (OclTuple e1 e2))))
\end{verbatim}

\textit{oops}

Set

OrderedSet

Bag

\textbf{= (bag : Bag(T)) : Boolean} \quad (11.7.7-b)

True if self and bag contain the same elements, the same number of times.

\begin{verbatim}
result =
  (self->forall(elem | self->count(elem) = bag->count(elem)) and
   bag->forall(elem | bag->count(elem) = self->count(elem)))
\end{verbatim}
B.6. Requirements

union(bag : Bag(T)) : Bag(T)

The union of self and bag.

post: result -> forall( elem | result -> count(elem) = self -> count(elem) + bag -> count(elem))
post: self -> forall( elem | result -> count(elem) = self -> count(elem) + bag -> count(elem))
post: bag -> forall( elem | result -> count(elem) = self -> count(elem) + bag -> count(elem))

union(set : Set(T)) : Bag(T)

The union of self and set.

post: result -> forall( elem | result -> count(elem) = self -> count(elem) + set -> count(elem))
post: self -> forall( elem | result -> count(elem) = self -> count(elem) + set -> count(elem))
post: set -> forall( elem | result -> count(elem) = self -> count(elem) + set -> count(elem))

intersection(bag : Bag(T)) : Bag(T)

The intersection of self and bag.

post: result -> forall( elem | result -> count(elem) = self -> count(elem). min(bag -> count(elem)))
post: self -> forall( elem | result -> count(elem) = self -> count(elem). min(bag -> count(elem)))
post: bag -> forall( elem | result -> count(elem) = self -> count(elem). min(bag -> count(elem)))

intersection(set : Set(T)) : Set(T)

The intersection of self and set.

post: result -> forall( elem | result -> count(elem) = self -> count(elem). min(set -> count(elem)))
post: self -> forall( elem | result -> count(elem) = self -> count(elem). min(set -> count(elem)))
post: set -> forall( elem | result -> count(elem) = self -> count(elem). min(set -> count(elem)))
### Appendix B. Isabelle Theories

#### including(object : T) : Bag(T)

The bag containing all elements of self plus object.

**post**: result\(\rightarrow\)forall(elem | if elem = object then
  result\(\rightarrow\)count(elem) = self\(\rightarrow\)count(elem) + 1
else
  result\(\rightarrow\)count(elem) = self\(\rightarrow\)count(elem)
endif)

**post**: self\(\rightarrow\)forall(elem | if elem = object then
  result\(\rightarrow\)count(elem) = self\(\rightarrow\)count(elem) + 1
else
  result\(\rightarrow\)count(elem) = self\(\rightarrow\)count(elem)
endif)


#### excluding(object : T) : Bag(T)

The bag containing all elements of self apart from all occurrences of object.

**post**: result\(\rightarrow\)forall(elem | if elem = object then
  result\(\rightarrow\)count(elem) = 0
else
  result\(\rightarrow\)count(elem) = self\(\rightarrow\)count(elem)
endif)

**post**: self\(\rightarrow\)forall(elem | if elem = object then
  result\(\rightarrow\)count(elem) = 0
else
  result\(\rightarrow\)count(elem) = self\(\rightarrow\)count(elem)
endif)


#### count(object : T) : Integer

The number of occurrences of object in self.

420
B.6. Requirements

\textbf{flatten() : Bag(T2)}

If the element type is not a collection type this result in the same bag. If the element type is a collection type, the r is the bag containing all the elements of all the elements of self.

\textbf{post:}
\begin{verbatim}
result = if self.type.elementType.oclIsKindOf(CollectionType) then
  self->iterate(c; acc : Bag() = Bag{} | acc->union(c->asBag()) )
else
  self
endif
\end{verbatim}

\textbf{asBag() : Bag(T)}

A Bag identical to self. This operation exists for convenience reasons.

\textbf{post:} result = self

\textbf{asSequence() : Sequence(T)}

A Sequence that contains all the elements from self, in undefined order.

\textbf{post:}
\begin{verbatim}
result ->forAll(elem | self->count(elem)=result->count(elem))
post: self ->forAll(elem | self->count(elem)=result->count(elem))
\end{verbatim}

\textbf{asSet() : Set(T)}

The Set containing all the elements from self, with duplicates removed.

\textbf{post:}
\begin{verbatim}
result ->forAll(elem | self ->includes(elem))
post: self ->forAll(elem | result->includes(elem))
\end{verbatim}

\textbf{asOrderedSet() : OrderedSet(T)}

An OrderedSet that contains all the elements from self, in undefined order, with duplicates removed.

\textbf{post:}
\begin{verbatim}
result ->forAll(elem | self ->includes(elem))
post: self ->forAll(elem | result->includes(elem))
post: self ->forAll(elem | result->count(elem) = 1)
\end{verbatim}
Appendix B. Isabelle Theories

Sequence

\textbf{count(object : T) : Integer} \hspace{1cm} (11.7.5-a)
The number of occurrences of object in self.

\textbf{= (s : Sequence(T)) : Boolean} \hspace{1cm} (11.7.5-b)
True if self contains the same elements as s in the same order.

\begin{itemize}
  \item \textbf{post:}
    \begin{align*}
      & \text{result} = \text{Sequence} \{ 1..\text{self} \rightarrow \text{size}() \} \rightarrow \\
      & \text{forall} (\text{index} : \text{Integer} | \text{self} \rightarrow \text{at}(\text{index}) = \text{s} \rightarrow \text{at}(\text{index}))
    \end{align*}
    \text{and}
    \begin{align*}
      & \text{self} \rightarrow \text{size}() = \text{s} \rightarrow \text{size}()
    \end{align*}
\end{itemize}

\begin{itemize}
  \item \textbf{lemma req_11_7_5−b:}
    \begin{align*}
      & ((S1::(\text{\textasciitilde}a,\text{\textasciitilde}b::\text{bot})\text{Sequence}) \equiv S2) = \\
      & (\forall \text{i} \in ((\text{OclCollectionRange} 1 \| \text{S1}||):(\text{\textasciitilde}a,\text{Integer}_0)\text{Sequence}). ((\text{OclAt} \text{S1} \text{i}) \equiv (\text{OclAt} \text{S2} \text{i})) ) \land \\
      & ((\| \text{S1}|| \equiv \| \text{S2}||))
    \end{align*}
\end{itemize}

union (s : Sequence(T)) : Sequence(T) \hspace{1cm} (11.7.5-c)
The sequence consisting of all elements in self, followed by all elements in s.

\begin{itemize}
  \item \textbf{post:}
    \begin{align*}
      & \text{result} \rightarrow \text{size}() = \text{self} \rightarrow \text{size}() + \text{s} \rightarrow \text{size}() \\
      & \text{post:} \text{Sequence} \{ 1..\text{self} \rightarrow \text{size}() \} \rightarrow \\
      & \text{forall} (\text{index} : \text{Integer} | \text{self} \rightarrow \text{at}(\text{index}) = \text{result} \rightarrow \text{at}(\text{index}))
    \end{align*}
\end{itemize}

\begin{itemize}
  \item \textbf{lemma req_11_7_5−c−1:}
    \begin{align*}
      & \llbracket (\text{self}::(\text{\textasciitilde}a,\text{\textasciitilde}b::\text{bot})\text{Sequence}) \cup \text{s} \rrbracket \| = (\| \text{self}\| + \| \text{s}||)
    \end{align*}
  \item \textbf{by(simp)}
\end{itemize}

\begin{itemize}
  \item \textbf{lemma req_11_7_5−c−2:}
    \begin{align*}
      & \llbracket \tau \vdash \delta (\text{self}::(\text{\textasciitilde}a,\text{\textasciitilde}b::\text{bot})\text{Sequence}) \rrbracket \implies \\
      & \tau \vdash \forall \text{index} \in ((\text{OclCollectionRange} 1 \| \text{self}||):(\text{\textasciitilde}a,\text{Integer}_0)\text{Sequence}). (\text{OclAt} (\text{self} \cup \text{s} \text{ index}) \equiv (\text{OclAt} \text{self index}))
    \end{align*}
  \item \textbf{apply(rule OCL_Sequence.ForAll)}
  \item \textbf{apply(simp add: OCL_Sequence.OCL_is_defopt_OclCollectionRange)}
  \item \textbf{apply(simp add: OCL_Sequence.includes_of_collectionRange)}
  \item \textbf{oops}
\end{itemize}

\begin{itemize}
  \item \textbf{lemma req_11_7_5−c−3:}
    \begin{align*}
      & \llbracket \forall \text{index} \in ((\text{OclCollectionRange} 1 \| \text{s}||):(\text{\textasciitilde}a,\text{Integer}_0)\text{Sequence}). (\text{OclAt} \text{s index}) \equiv (\text{OclAt} (\text{self} \cup \text{s} \text{ index} + (\| \text{self}||)))
    \end{align*}
  \item \textbf{oops}
\end{itemize}
flatten() : Sequence(T2) \hspace{1cm} (11.7.5-d)

If the element type is not a collection type this result in the same self. If the element type is a collection type, the result is the sequence containing all the elements of all the elements of self. The order of the elements is partial.

\[
\text{post:} \\
\quad \text{result} = \begin{cases} \\
\quad \text{if self.type.elementType.oclIsKindOf(CollectionType)} \\
\quad \quad \text{then} \\
\quad \quad \quad \text{self->iterate(c; acc : Sequence() = Sequence{} |} \\
\quad \quad \quad \quad \quad \text{acc->union(c->asSequence() )}) \\
\quad \quad \text{else} \\
\quad \quad \quad \text{self} \\
\quad \end{cases}
\]

The postcondition in the standard is not typeable because it must have these two types at the same time which is not possible:

\[
(('a,'b::bot Sequence_0)Sequence) \Rightarrow ('a,'b)Sequence \\
('a,'b::bot)Sequence \Rightarrow ('a,'b)Sequence
\]

therefore we split the requirement into two parts:

1. characterises the case of a flatten of a sequence of sequences
2. characterises the case of a flatten of a sequence of a not collection type. This follows by definition of flatten on sequences of non collection types

\textbf{lemma} req_11_7_5-d-1:

\[
(fact:(a,b::bot Sequence_0)Sequence)\Rightarrow:(a,b)Sequence) = \\
(self->iterate(x,y=[] | (y \cup x)))
\]

\textit{by}(simp add: OCL_Sequence.flatten_by_iterate)
Appendix B. Isabelle Theories

append (object: T) : Sequence(T)  
(11.7.5-e)

The sequence of elements, consisting of all elements of self, followed by object.

| post: result -> size() = self -> size() + 1 |
| post: result -> at(result -> size() ) = object |
| post: Sequence(1..self -> size() )->forall(index : Integer | result -> at(index) = self -> at(index)) |

lemma req_11_7_5-e-1:
\[ \tau \models (\partial (\text{obj}::(\text{a},\text{b}::\text{bot})\text{VAL})) \implies (\|\text{OclAppend (self} :: (\text{a},\text{b})\text{Sequence}) \text{obj}\|\tau) = (\|\text{self\| + 1)} \tau) \]
by(simp)

lemma req_11_7_5-e-2:
\[ \tau \models (\partial (\text{self} :: (\text{a},\text{b}::\text{bot})\text{Sequence})) \implies (\text{OclAt (OclAppend self (obj} :: (\text{a},\text{b})\text{VAL})) ||\text{OclAppend self obj||} \tau) = (\text{obj} \tau) \]
apply(case_tac \( \tau \models \neg \partial \text{obj} \))
apply(ocl_hypsubst, simp_all)
apply(rule OCL_Sequence.at_last_of_including)
apply(rule subst, rule sym)
apply(rule_tac A=||self ->including obj || in cp_charn)
apply(rule OCL_Sequence.size_of_including)
apply(simp_all)
oops

lemma req_11_7_5-e-3:
\[ \forall \text{index} \in ((\text{OclCollectionRange 1 ||(self} :: (\text{a},\text{b}::\text{bot})\text{Sequence})))::(\text{a},\text{Integer_0})\text{Sequence}) \]
\[ \text{(OclAt self index) \models \text{OclAt (OclAppend self (obj} :: (\text{a},\text{b})\text{VAL}) \text{ index})} \]
oops
B.6. Requirements

prepend(object : T) : Sequence(T)

The sequence consisting of object, followed by all elements in self.

| post: result->size = self->size() + 1 |
| post: result->at(1) = object |
| post: Sequence{1..self->size()})->forall(index : Integer |
| self->at(index) = result->at(index + 1)) |

lemma req_11_7_5_f_1:
τ ⊨ (∂ (obj::('a','b':bot)VAL)) ⇒
(∥OclPrepend (self::('a','b)Sequence) obj∥) τ = (∥self∥ + 1) τ
apply(simp)
apply(rule trans)
apply(rule_tac A=∥S->including obj ∥ in cp_charn)
apply(rule OCL_Sequence.size_of_including)
apply(simp add: localValidDefined2sem)
apply(simp add: localValid2sem OCL_Sequence.OclSize_def OclStrictEq_def
One_ocl_int_def Zero_ocl_int_def plus_def ss_lifting)

oops

lemma req_11_7_5_f_2:
τ ⊨ (∂ (self::('a,'b':bot)Sequence)) ⇒
(OclAt (OclPrepend self (obj::('a,'b)VAL)) 1 τ) = (obj τ)
by(simp only: at_first_of_prepend)
lemma req_11_7_5_f_3:
∀ index ∈ ((OclCollectionRange 1 ||(self::('a,'b:bot)Sequence))::('a,Integer_0)Sequence)
·
(OclAt self index) = (OclAt (OclPrepend self (obj::('a,'b)VAL)) (index+1))

oops
Appendix B. Isabelle Theories

insertAt(index : Integer, object : T) : Sequence(T)

The sequence consisting of self with object inserted at position index.

post: result -> size = self -> size() + 1
post: result -> at(index) = object
post: Sequence{1..(index - 1)} -> forall(i : Integer | self -> at(i) = result -> at(i))
post: Sequence{(index + 1)..self -> size()) -> forall(i : Integer | self -> at(i) = result -> at(i + 1))

no preconditions about range of index. But they are surely needed because of the correspondence to at()
subSequence(lower : Integer, upper : Integer) : Sequence(T)  \((11.7.5-h)\)

The sub-sequence of self starting at number lower, up to and including element number upper.

\[
\begin{align*}
\text{pre} & : 1 \leq \text{lower} \\
\text{pre} & : \text{lower} \leq \text{upper} \\
\text{pre} & : \text{upper} \leq \text{self} \rightarrow \text{size}() \\
\text{post} & : \text{result} \rightarrow \text{size}() = \text{upper} - \text{lower} + 1 \\
\text{post} & : \text{Sequence} \{ \text{lower} .. \text{upper} \} \rightarrow \forall \text{index} \\
& \quad (\text{result} \rightarrow \text{at}(\text{index} - \text{lower} + 1) = \\
& \quad \quad \text{self} \rightarrow \text{at}(\text{index}))
\end{align*}
\]

**lemma** req_11_7_5−h−2:

\[
[\tau \models 1 \leq \text{lower}; \tau \models \text{lower} \leq \text{upper} - 1; \tau \models \text{upper} \leq \|\text{self}\|] \implies \\
\|\text{OclSubSequence (self; ('a,'b::bot)Sequence) lower upper}\| \tau = (\text{upper} - \text{lower} + 1)
\]

\by (simp add: size_of_subsequence)

**lemma** req_11_7_5−h−2:

\[
[\tau \models 1 \leq \text{lower}; \tau \models \text{lower} \leq \text{upper} - 1; \tau \models \text{upper} \leq \|\text{self}\|] \implies \\
\tau \models \forall \text{index} \in ((\text{OclCollectionRange lower upper});('a,Integer_0)Sequence) \cdot \\
(\text{OclAt (OclSubSequence self lower upper) (index} - \text{lower} + 1) \equiv \\
\text{OclAt (self; ('a,'b::bot)Sequence) index})
\]

**oops**

at(i : Integer) : T  \((11.7.5-i)\)

The i-th element of sequence.

\[
\begin{align*}
\text{pre} & : i \geq 1 \text{ and } i \leq \text{self} \rightarrow \text{size}() \\
\end{align*}
\]

**lemma** req_11_7_5−i:

\[
[\tau \models 1 \leq i; \tau \models i \leq \|\text{S}\|] \implies \\
(\tau \models \partial((\text{OclAt (S; ('a,'b::bot)Sequence) i});('a,'b)\text{VAL}))
\]

\apply (rotate_tac 1, frule isDefined_if_valid)

\apply (simp only: OCL_is_defopt_OclLe OCL_Sequence,OCL_is_defopt_OclSize OCL_is_defopt_OclAt)

\oops
## Appendix B. Isabelle Theories

### indexOf(obj : T) : Integer

The index of object `obj` in the sequence.

<table>
<thead>
<tr>
<th>pre</th>
<th>: self-&gt;includes(obj)</th>
</tr>
</thead>
<tbody>
<tr>
<td>post</td>
<td>: self-&gt;at(i) = obj</td>
</tr>
</tbody>
</table>

**lemma req_11_7_5-j:**

\[ \tau \vdash (\text{obj}::(\text{a},\text{b})\text{VAL}) \in (\text{self}::(\text{a},\text{b}:\text{bot})\text{Sequence}) \implies \]

\[ \text{OclAt self (OclIndexOf self obj)} \tau = \text{obj} \tau \]

*by* (simp add: at_indexOf)

### first() : T

The first element in self.

| post | : result = self->at(1) |

**lemma req_11_7_5-k:**

\[ \text{OclFirst (self}::(\text{a},\text{b}:\text{bot})\text{Sequence}) = ((\text{OclAt self 1})::(\text{a},\text{b})\text{VAL}) \]

*by* (rule first_at_UC)

### last() : T

The last element in self.

| post | : result = self->at(self->size() ) |

**lemma req_11_7_5-l:**

\[ \text{OclLast (self}::(\text{a},\text{b}:\text{bot})\text{Sequence}) = ((\text{OclAt self ||self||})::(\text{a},\text{b})\text{VAL}) \]

*by* (rule last_at_UC)

#### including(object : T) : Sequence(T)

The sequence containing all elements of self plus object added as the last element.

| post | : result = self.append(object) |

**lemma req_11_7_5-m:**

\[ \text{self->including (obj}::(\text{a},\text{b})\text{VAL}) = \text{OclAppend (self}::(\text{a},\text{b}:\text{bot})\text{Sequence)} \text{obj} \]

*by* (rule append_including_UC[symmetric])

---

428
B.6. Requirements

excluding(object : T) : Sequence(T)  (11.7.5-n)
The sequence containing all elements of self apart from all occurrences of object. The
order of the remaining elements is not changed.

post: result->includes(object) = false
post: result->size() = self->size() - self->count(object)
post: result = self->iterate(elem; acc : Sequence(T)
    = Sequence()
        if elem = object then acc else acc->append(elem) endif)

lemma req_11_7_5-n-1:
    [ \tau \models \partial(\text{obj}::('a,'b:\text{Sequence}) \land \tau(\text{self}::\text{Sequence})) ] \implies
    \tau(\text{self}->excluding \text{obj}) = \text{F} \tau
by(simp add: OCL_Sequence.includes_of_excluding)
lemma req_11_7_5-n-2:
    \| (\text{self}::\text{Sequence})->excluding (\text{obj}::\text{Sequence})\| = \| \text{self} \|
by(simp add: OCL_Sequence.size_of_excluding)
lemma req_11_7_5-n-3:
    [ \tau \models \partial(\text{obj}::\text{Sequence}) ] \implies
    \tau((\text{self}-->excluding \text{obj})) \tau =
    \text{OclAppend} \tau \text{acc} \tau\text{elem} \tau
by(simp add: OCL_Sequence.excluding_by_iterate localValid2sem
    OCL_Sequence.OclIterate_def OclIf_def ss_lifting')

asBag() : Bag(T)  (11.7.5-o)
The Bag containing all the elements from self, including duplicates.

post: result->forAll(elem | self->count(elem)=result->count(elem))
post: self->forAll(elem | self->count(elem)=result->count(elem))

lemma req_11_7_5-o-1:
    \forall elem : ((\text{asBag()} (\text{self}::\text{Sequence})):\text{Bag})
    \tau \models \partial(\tau(\text{self}::\text{Sequence}) \land \tau(\text{asBag()} \text{self}) \land \tau(\text{count elem}))
oops
lemma req_11_7_5-o-2:
    \forall elem : \tau \models \partial(\text{self}::\text{Sequence})
    \tau \models \partial(\tau(\text{self}::\text{Sequence}) \land \tau(\text{count elem}))
oops
Appendix B. Isabelle Theories

asSequence() : Sequence(T)  (11.7.5-p)
The Sequence identical to the object itself. This operation exists for convenience reasons.

\post: result = self

\begin{lemma}
\req_{11.7.5-p}:
\begin{align*}
((\Rightarrow \text{asSequence()} \ (\text{self}::{('a,'b::bot)Sequence})):('a,'b::bot)Sequence) = \text{self} \\
\text{by (simp)}
\end{align*}
\end{lemma}

asSet() : Set(T)  (11.7.5-q)
The Set containing all the elements from self, with duplicated removed.

\begin{verbatim}
| post: result ->forall(elem | self ->includes(elem))
| post: self ->forall(elem | result ->includes(elem))
\end{verbatim}

\begin{lemma}
\req_{11.7.5-q-1}:
\begin{align*}
\forall \ elem \in ((\Rightarrow \text{asSet()} \ (\text{self}::{('a,'b::bot)Sequence})):('a,'b Set_0)VAL) \\
((\text{elem}::{('a,'b)VAL}) \in \text{self})
\text{oops}
\end{align*}
\end{lemma}

\begin{lemma}
\req_{11.7.5-q-2}:
\begin{align*}
\forall \ elem \in (\text{self}::{('a,'b::bot)Sequence}) \cdot ((\text{elem}::{('a,'b)VAL}) \in ((\Rightarrow \text{asSet()} \ \text{self}::{('a,'b Set_0)VAL}))
\text{oops}
\end{align*}
\end{lemma}

asOrderedSet() : OrderedSet(T)  (11.7.5-r)
An OrderedSet that contains all the elements from self, in the same order, with duplicates removed.

\begin{verbatim}
| post: result ->forall(elem | self ->includes(elem))
| post: self ->forall(elem | result ->includes(elem))
| post: self ->forall(elem1, elem2 | self ->indexOf(elem1) < self ->indexOf(elem2) implies result ->indexOf(elem1) < result ->indexOf(elem2) )
\end{verbatim}

\begin{lemma}
\req_{11.7.5-r-1}:
\begin{align*}
\forall \ elem \in ((\Rightarrow \text{asOrderedSet()} \ (\text{self}::{('a,'b::bot)Sequence})):('a,'b OrderedSet_0)VAL) \\
((\text{elem}::{('a,'b)VAL}) \in \text{self})
\text{oops}
\end{align*}
\end{lemma}

\begin{lemma}
\req_{11.7.5-r-2}:
\begin{align*}
\forall \ elem \in (\text{self}::{('a,'b::bot)Sequence}) \cdot ((\text{elem}::{('a,'b)VAL}) \in ((\Rightarrow \text{asOrderedSet()} \ \text{self}::{('a,'b::bot OrderedSet_0)VAL}))
\text{oops}
\end{align*}
\end{lemma}

end
B.6. Requirements

B.6.3. OCL Iterator requirements

theory OCL_Iterator_requirements
imports
$HOLOCL_HOME/src/OCL_Library
begin

This theory contains the requirements for iterators defined in the OCL standard library [41, Chapter 11.9].

Collection

_exists_ (11.9.1-a)

Results in true if body evaluates to true for at least one element in the source collection.

\[
\text{source} \rightarrow \exists (\text{iterators} \mid \text{body}) = \\
\text{source} \rightarrow \text{iterate}(\text{iterators}; \text{result} : \text{Boolean} = \text{false} \\
\mid \text{result or body})
\]

Set

OrderedSet

Bag

\text{lemma req_bag_11_9_1-a:}

\((\exists x \in (\text{source}::(\text{a}, \text{b}::\text{bot})\text{Bag}) \cdot (P::(\text{a}, \text{b}::\text{bot})\text{VAL} \Rightarrow \text{a Boolean}) x) = \\
(\text{source} \rightarrow \text{iterate}(x;y=F \mid (P x) \lor y))

\text{by (rule OCL_Bag.exists_by_iterate)}

Sequence

\text{lemma req_seq_11_9_1-a:}

\((\exists x \in (\text{source}::(\text{a}, \text{b}::\text{bot})\text{Sequence}) \cdot (P::(\text{a}, \text{b}::\text{bot})\text{VAL} \Rightarrow \text{a Boolean}) x) = \\
(\text{source} \rightarrow \text{iterate}(x;y=F \mid (P x) \lor y))

\text{by (rule OCL_Sequence.exists_by_iterate)}

Appendix B. Isabelle Theories

**forAll**

Results in true if the body expression evaluates to true for each element in the source collection; otherwise, result is false.

| source -> forAll (iterators | body ) = |
|-----------------------------------------|
| source -> iterate (iterators ; result : Boolean = true |
| | result and body) |

**Set**

**OrderedSet**

**Bag**

*lemma* req_bag_11_9_1-b:

\(\forall x \in (\text{source} : (\text{a,b}: \text{bot} : \text{Bag}) \rightarrow \text{P} : (\text{a,b} : \text{bot} : \text{VAL} \Rightarrow \text{a Boolean}) x) =\)

\((\text{source} \rightarrow \text{iterate}(\text{x} \rightarrow \text{T} | \text{P} \land \text{y}))\)

*by* (rule OCL_Bag forall_by_iterate)

**Sequence**

*lemma* req_seq_11_9_1-b:

\(\forall x \in (\text{source} : (\text{a,b}: \text{bot} : \text{Sequence}) \rightarrow \text{P} : (\text{a,b} : \text{bot} : \text{VAL} \Rightarrow \text{a Boolean}) x) =\)

\((\text{source} \rightarrow \text{iterate}(\text{x} \rightarrow \text{T} | \text{P} \land \text{y}))\)

*by* (rule OCL_Sequence forall_by_iterate)

**isUnique**

Results in true if body evaluates to a different value for each element in the source collection; otherwise, result is false.

| source -> isUnique (iterators | body ) = |
|-----------------------------------------|
| source -> collect (iterators | Tuple { iter = Tuple { iterators }, value = body}) |
| -> forAll (x, y | (x.iter <> y.iter) |
| implies (x.value <> y.value)) |

isUnique may have at most one iterator variable.

**Set**

**OrderedSet**

**Bag**

**Sequence**
any

(11.9.1-d)

Returns any element in the source collection for which body evaluates to true. If there is more than one element for which body is true, one of them is returned. There must be at least one element fulfilling body, otherwise the result of this IteratorExp is OclUndefined.

\[
\text{source} \to \text{any} (\text{iterator} \mid \text{body}) = \\
\text{source} \to \text{select} (\text{iterator} \mid \text{body}) \to \text{asSequence()} \to \text{first()}
\]

any may have at most one iterator variable.

Set

OrderedSet

Bag

\text{lemma req\_bag\_11\_9\_1-d:}

\text{OCL\_Collection.OclAny (Source::('a', 'b':bot)Bag) (P::((('a', 'b':bot)VAL \Rightarrow 'a Boolean)) =}

\text{OclFirst ((\text{asSequence()} ([x : source \mid (P x)]):(('a', 'b':bot)Sequence))}

\text{oops}

Sequence

\text{lemma req\_seq\_11\_9\_1-d:}

\text{OCL\_Collection.OclAny (source::('a', 'b':bot)Sequence) (P::(('a', 'b':bot)VAL \Rightarrow 'a Boolean) =}

\text{OclFirst ((\text{asSequence()} ([x : source \mid (P x)]):(('a', 'b':bot)Sequence))}

\text{by(rule OCL\_Sequence.any\_by\_first\_of\_select)
Appendix B. Isabelle Theories

**one** (11.9.1-e)

Results in true if there is exactly one element in the source collection for which body is true.

\[
\text{source} \rightarrow \text{one} (\text{iterator} \mid \text{body}) = \text{source} \rightarrow \text{select} (\text{iterator} \mid \text{body}) \rightarrow \text{size}() = 1
\]

one may have at most one iterator variable.

**Set**

**OrderedSet**

**Bag**

\[\text{lemma req\_bag\_11\_9\_1-e:}\]

\[
(\text{OclOne (source::(’a,’b::bot)Bag) (P::(’a,’b::bot)VAL } \Rightarrow \text{’a Boolean)}) = \]

\[
(\parallel \{x : \text{source} \mid (P x)\} \parallel = 1)
\]

\[\text{by (simp add: OCL\_Bag.OclOne\_def)}\]

**Sequence**

\[\text{lemma req\_seq\_11\_9\_1-e:}\]

\[
(\text{OclOne (source::(’a,’b::bot)Sequence) (P::(’a,’b::bot)VAL } \Rightarrow \text{’a Boolean)}) = \]

\[
(\parallel \{x : \text{source} \mid (P x)\} \parallel = 1)
\]

\[\text{by (rule OCL\_Sequence.one\_by\_size\_of\_select)}\]
B.6. Requirements

**collect**

The Collection of elements which results from applying body to every member of the source set. The result is flattened. Notice that this is based on collectNested, which can be of different type depending on the type of source. collectNested is defined individually for each subclass of CollectionType.

\[
\text{source} \rightarrow \text{collect} \ (\text{iterators} \mid \text{body}) = \text{source} \rightarrow \text{collectNested} \ (\text{iterators} \mid \text{body}) \rightarrow \text{flatten()}
\]

collect may have at most one iterator variable.

**Set**

**OrderedSet**

**Bag**

**sequence**

**lemma** req_bag_11_7_4-f:

\[
\text{OclCollect } S \ P \equiv \llceil (\text{OclCollectNested } S \ P) \rrceil
\]

**oops**

**Sequence**

**lemma** req_seq_11_9_1-f:

\[
\text{OclCollect } S \ P \equiv \llceil (\text{OclCollectNested } S \ P) \rrceil
\]

**Set**

**Bag**

**Sequence**

**select(expression : OclExpression) : Sequence(T)**

(11.9.4-a)

The subsequence of the source sequence for which body is true.

\[
\text{source} \rightarrow \text{select} \ (\text{iterator} \mid \text{body}) =
\text{source} \rightarrow \text{iterate} \ (\text{iterator}; \text{result} : \text{Sequence(T)}\Rightarrow \text{Sequence}()) |
\text{if body then result} \rightarrow \text{including} \ (\text{iterator})
\text{else result}
\text{endif}
\]

select may have at most one iterator variable. **lemma** req_11_9_4-a:

\[
(\forall x : \text{(source}::\text{([a,b::bot]}\text{Sequence}) \mid (\text{P}::([a,b::bot]}\text{VAL} \Rightarrow a \text{ Boolean}) x)) =
(\text{source} \rightarrow \text{iterate} (\text{iterator}; \text{result} = []) |
\text{if (P iterator) then (OclIncluding result iterator) else result endif})
\]

**by**(rule OCL_Sequence.select_by_iterate)
Appendix B. Isabelle Theories

reject

The subsequence of the source sequence for which body is false.

source -> reject (iterator | body) =
source -> select (iterator | not body)

reject may have at most one iterator variable. **lemma** req_11_9_4-b:
OclReject source P = (\{x : (source::(′a,′b::bot)Sequence) | (¬ (P::(′a,′b::bot)VAL ⇒ ′a Boolean) x)\})
**by** (rule OCL_Sequence.reject_by_select)

collectNested

The Sequence of elements which results from applying body to every member of the source sequence.

source -> collect (iterators | body) =
source -> iterate (iterators; result : Sequence (body.type) = Sequence {} | result -> append (body ) )

collectNested may have at most one iterator variable. **lemma** req_11_9_4-c:
((OclCollectNested (source::(′a,′b::bot)Sequence) (P::(′a,"b)VAL ⇒ (′a,"c)VAL)::(′a,"c::bot)Sequence) =
(source ->iterate(iterators; result=[] | result ->including (P iterators)))
**by** (rule OCL_Sequence.collectNested_by_iterate)

sortedBy

Results in the Sequence containing all elements of the source collection. The element for which body has the lowest value comes first, and so on. The type of the body expression must have the < operation defined. The < operation must return a Boolean value and must be transitive i.e. if a < b and b < c then a < c.

source -> sortedBy (iterator | body) =
iterate (iterator ; result : Sequence(T) : Sequence {} |
if result ->isEmpty() then
result.append(iterator)
else
let position : Integer = result ->indexOf (result ->select (item | body (item) > body (iterator)) ->first())
in
result.insertAt(position, iterator)
endif

sortBy may have at most one iterator variable.

end
B.7. OCL

B.7.1. The Object Constraint Language: OCL

theory OCL
imports
$HOLOCL_HOME/src/UML_OCL
$HOLOCL_HOME/src/library/basic/OCL_Basic_requirements
$HOLOCL_HOME/src/library/collection/$COLLECTION/OCL_Collection_requirements
$HOLOCL_HOME/src/library/collection/$COLLECTION/OCL_Iterator_requirements
begin end
Appendix B. Isabelle Theories
Appendix C.

Encoding UML/OCL by Example

C.1. Encoding UML/OCL into HOL by Example

C.2. A Simple Example

In this section we present the details of our encoding by an tiny example. We use the class diagram presented in Figure C.1 together with the OCL specification shown in Listing C.1. Our Example consists only out of two classes with an inheritance relationship. Class A has one attribute i of type Integer that is constraint by an invariant. Further, class A has a method \( f(x:\text{Integer}):\text{Integer} \) which is described by a pre-condition and post-condition. Class B only has one attribute j of type B. Note that this is, in contrast to the attribute i of class A, an object type. In the following we describe which definition and theorems are generated during the import of this simple class diagram into HOL-OCL.

C.3. Importing UML/OCL models

UML/OCL models can be directly imported into HOL-OCL if they are available in XMI format, e.g.,

```plaintext
load_xmi encoding_example_ocl.xmi
```

```plaintext
package encoding

context A::i:Integer
  init: 42

context A
  inv: i >= 0

context A::f(x:Integer):Integer
  pre: x > 0
  post: result = x.div(i)
endpackage
```

Listing C.1: A simple Encoding Example: OCL specification
Appendix C. Encoding UML/OCL by Example

![Diagram](image)

**Figure C.1.:** A simple Encoding Example: Data Model

imports the UML/OCL specification of our example. During the import, different definitions and theorems are generated into the current theory context. HOL-OCL organizes these automatically generated stuff into a hierarchy of namespaces, i.e., in our example:

**UML_OCL:** This is the standard namespace for internal definitions, i.e., definitions that normally should not be needed by the users. This namespace is divided as follows:

- **univ.model:** contains the basic type definitions of classes and the type of the universe
- **level0.model:** contains the level 0 definitions of the model.
- **level1.model:** contains the level 1 definitions of the model.

**model:** It contains all definitions a user would expect, namely all the level 2 stuff which ties the UML and OCL part together.

In all namespaces, “model” is replaced by the top-level UML package of the encoded model, i.e., for our example “encoding”. Thus, in our example all level 0 definitions are defined within “UML_OCL.level0.encoding”.

### C.3.1. Encoding Level 0:

#### The Universe Type

The first major step of encoding classes into the base OCL universe is to construct the universe type, but first we have to construct the core types for classes. For each class
C.3. Importing UML/OCL models

we construct a "identifier" type which is crucial for our strong type discipline:

\[ UML\_OCL.univ.encoding.A\_key = A\_key \]

the base type of the class, describing its locally defined attributes

\[ UML\_OCL.univ.encoding.A\_base\_type = A\_key \times \text{Integer}_0 \]

the type of the class, describing the inherited type together with the base type

\[ UML\_OCL.univ.encoding.A\_type = A\_key \times \text{Integer}_0 \]

\[ 'a \ UML\_OCL.univ.encoding.A\_ext = (\text{OclAny}_\text{key} \times \text{oid}) \times ((A\_key \times \text{Integer}_0) \times 'a \ up) \ up \]

These types are analogous defined for the inherited class B:

\[ UML\_OCL.univ.encoding.B\_key = B\_key \]

\[ UML\_OCL.univ.encoding.B\_base\_type = B\_key \times \text{oid} \]

\[ UML\_OCL.univ.encoding.B\_type = (A\_key \times \text{Integer}_0) \times B\_key \times \text{oid} \]

\[ 'a \ UML\_OCL.univ.encoding.B\_ext = (\text{OclAny}_\text{key} \times \text{oid}) \times ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a \ up) \ up) \ up \]

Together with the pre-defined OCL universe type they build the basis for the model specific universe type:

\[ ('a, 'b, 'c) \ U\_encoding\_example = U ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a \ up + 'b) \ up + 'c) \]

Now we can encode types for classes represented in the universe, e.g. for class A:

\[ ('a, 'b) \ UML\_OCL.univ.encoding.A = \text{OclAny}_0 ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a \ up + 'b) \ up) \]

and for class B:

\[ 'a \ UML\_OCL.univ.encoding.B = \text{OclAny}_0 ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a \ up) \ up) \]

**Defining the Basic Methods over Classes**

For each class we define two type tests for objects, one for testing if a object is of a specific type or supertype (i.e., this test is true, if the object is of the given kind):

\[ UML\_OCL.level0.encoding.is\_A :: \]

\[ \text{OclAny}_0 ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a \ up + 'b) \ up) \Rightarrow \text{bool} \]

\[ \text{level0.encoding.is\_A} \equiv \text{DEF} \circ \text{base} \]
and one for testing if an object is exactly the requested type

\[
UML\_OCL.\text{level0.encoding.isType}_A :: \\
\text{OclAny}_0 \left( (A\_key \times \text{Integer}_0) \times (B\_key \times \text{oid}) \times 'a \text{ up} + 'b \text{ up} \right) \Rightarrow \text{bool} \\
\text{level0.encoding.isType}_A \equiv \\
\lambda \text{obj}. \text{level0.encoding.is}_A \text{ obj} \land \neg (\text{DEF} \circ \text{base} \circ \text{base}) \text{ obj}
\]

Further, we define a type for universe instances:

\[
UML\_OCL.\text{level0.encoding.is}_A\_univ :: \\
\text{U} \left( (A\_key \times \text{Integer}_0) \times (B\_key \times \text{oid}) \times 'a \text{ up} + 'b \text{ up} + 'c \right) \Rightarrow \text{bool} \\
\text{level0.encoding.is}_A\_univ \equiv \\
\text{level0.is}\_\text{OclAny}\_univ \equiv \text{univ} \land (\text{DEF} \circ \text{FromL} \circ \text{base} \circ \text{level0.get}_\text{OclAny}) \equiv \text{univ}
\]

Analogously we define for the inherited class B:

\[
UML\_OCL.\text{level0.encoding.is}_B :: \\
\text{OclAny}_0 \left( (A\_key \times \text{Integer}_0) \times (B\_key \times \text{oid}) \times 'a \text{ up} \right) \Rightarrow \text{bool} \\
\text{level0.encoding.is}_B \equiv \text{DEF} \circ \text{base} \circ \text{base}
\]

\[
UML\_OCL.\text{level0.encoding.isType}_B :: \\
\text{OclAny}_0 \left( (A\_key \times \text{Integer}_0) \times (B\_key \times \text{oid}) \times 'a \text{ up} \right) \Rightarrow \text{bool} \\
\text{level0.encoding.isType}_B \equiv \\
\lambda \text{obj}. \text{level0.encoding.is}_B \text{ obj} \land \neg (\text{DEF} \circ \text{base} \circ \text{base} \circ \text{base}) \text{ obj}
\]

\[
UML\_OCL.\text{level0.encoding.is}_B\_univ :: \\
\text{U} \left( (A\_key \times \text{Integer}_0) \times (B\_key \times \text{oid}) \times 'a \text{ up} + 'b \text{ up} + 'c \right) \Rightarrow \text{bool} \\
\text{level0.encoding.is}_B\_univ \equiv \\
\text{level0.encoding.is}_A\_univ \equiv \text{univ} \land \neg ((\text{DEF} \circ \text{FromL} \circ \text{base} \circ \text{base} \circ \text{level0.encoding.get}_A) \equiv \text{univ})
\]
We define a functions for embedding a class into the corresponding universe

\[
\text{level0.encoding.mk}_A :: \\
\text{OclAny}_0 ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a \text{ up} + b) \text{ up}) \\
\Rightarrow U ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a \text{ up} + b) \text{ up} + 'c)
\]

\[
\text{level0.encoding.mk}_A ?\text{obj} \equiv \\
\text{level0.mk}_\text{OclAny} \lbrack \text{sup} ?\text{obj}, (\text{lift} \circ \text{Inl} \circ \text{Lifting.drop} \circ \text{base}) ?\text{obj} \rbrack
\]

and one for extracting an object out of a given universe:

\[
\text{level0.encoding.get}_A :: \\
U ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a \text{ up} + b) \text{ up} + 'c) \\
\Rightarrow \text{OclAny}_0 ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a \text{ up} + b) \text{ up})
\]

\[
\text{level0.encoding.get}_A ?\text{univ} \equiv \\
\lbrack \text{sup} \circ \text{level0.get}_\text{OclAny} \rbrack ?\text{univ}, (\text{FromL} \circ \text{base} \circ \text{level0.get}_\text{OclAny}) ?\text{univ} \rbrack
\]

These two functions can also be understood as conversion between object types and universe types.

Analogous we define for the inherited class \(B\):

\[
\text{level0.encoding.mk}_B :: \\
\text{OclAny}_0 ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a \text{ up}) \text{ up}) \\
\Rightarrow U ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a \text{ up} + b) \text{ up} + 'c)
\]

\[
\text{level0.encoding.mk}_B ?\text{obj} \equiv \\
\text{level0.encoding.mk}_A \\
\lbrack \text{sup} ?\text{obj}, (\text{sup} \circ \text{base}) ?\text{obj}, (\text{lift} \circ \text{Inl} \circ \text{Lifting.drop} \circ \text{base} \circ \text{base}) ?\text{obj} \rbrack
\]

\[
\text{level0.encoding.get}_B :: \\
U ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a \text{ up} + b) \text{ up} + 'c) \\
\Rightarrow \text{OclAny}_0 ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a \text{ up}) \text{ up})
\]

\[
\text{level0.encoding.get}_B ?\text{univ} \equiv \\
\lbrack \text{sup} \circ \text{level0.encoding.get}_A ?\text{univ}, (\text{sup} \circ \text{base} \circ \text{level0.encoding.get}_A) ?\text{univ}, (\text{FromL} \circ \text{base} \circ \text{base} \circ \text{level0.encoding.get}_A) ?\text{univ} \rbrack
\]
Appendix C. Encoding UML/\texttt{OCL} by Example

For converting along type hierarchies (i.e. down-casting and up-casting) we provide for each class two functions for the conversion to the direct predecessor and direct successor in the class hierarchy:

\[
\text{UML} \_ \text{OCL}.\text{level0.encoding.A} \_2 \_\text{OclAny} ::
\]

\[
\text{OclAny} \_0 ((A \_\text{key} \times \text{Integer} \_0) \times ((B \_\text{key} \times \text{oid}) \times 'a \ up + 'b) \ up)
\Rightarrow \text{OclAny} \_0 ((A \_\text{key} \times \text{Integer} \_0) \times ((B \_\text{key} \times \text{oid}) \times 'a \ up + 'b) \ up + 'c)
\]

\[
\text{level0.encoding.A} \_2 \_\text{OclAny} \equiv \text{level0.get}_\text{OclAny} \circ \text{level0.encoding.mk}_A
\]

\[
\text{UML} \_ \text{OCL}.\text{level0.encoding.OclAny} \_2 \_A ::
\]

\[
\text{OclAny} \_0 ((A \_\text{key} \times \text{Integer} \_0) \times ((B \_\text{key} \times \text{oid}) \times 'a \ up + 'b) \ up + 'c)
\Rightarrow \text{OclAny} \_0 ((A \_\text{key} \times \text{Integer} \_0) \times ((B \_\text{key} \times \text{oid}) \times 'a \ up + 'b) \ up)
\]

\[
\text{level0.encoding.OclAny} \_2 \_A \equiv \text{level0.encoding.get}_A \circ \text{level0.encoding.mk}_\text{OclAny}
\]

Analogous we define for the inherited class B:

\[
\text{UML} \_ \text{OCL}.\text{level0.encoding.B} \_2 \_A ::
\]

\[
\text{OclAny} \_0 ((A \_\text{key} \times \text{Integer} \_0) \times ((B \_\text{key} \times \text{oid}) \times 'a \ up + 'b) \ up)
\Rightarrow \text{OclAny} \_0 ((A \_\text{key} \times \text{Integer} \_0) \times ((B \_\text{key} \times \text{oid}) \times 'a \ up + 'b) \ up)
\]

\[
\text{level0.encoding.B} \_2 \_A \equiv \text{level0.encoding.get}_A \circ \text{level0.encoding.mk}_B
\]

\[
\text{UML} \_ \text{OCL}.\text{level0.encoding.A} \_2 \_B ::
\]

\[
\text{OclAny} \_0 ((A \_\text{key} \times \text{Integer} \_0) \times ((B \_\text{key} \times \text{oid}) \times 'a \ up + 'b) \ up)
\Rightarrow \text{OclAny} \_0 ((A \_\text{key} \times \text{Integer} \_0) \times ((B \_\text{key} \times \text{oid}) \times 'a \ up) \ up)
\]

\[
\text{level0.encoding.A} \_2 \_B \equiv \text{level0.encoding.get}_B \circ \text{level0.encoding.mk}_A
\]

Finally, we provide accessor functions for the class attributes:

\[
\text{UML} \_ \text{OCL}.\text{level0.encoding.A}.i ::
\]

\[
\text{OclAny} \_0 ((A \_\text{key} \times \text{Integer} \_0) \times ((B \_\text{key} \times \text{oid}) \times 'a \ up + 'b) \ up) \Rightarrow \text{Integer} \_0
\]

\[
\text{level0.encoding.A}.i \equiv \text{snd} \circ \text{fst} \circ \text{Lifting.drop} \circ \text{base}
\]
Proving Properties

Already on this level, we can prove important properties of our encoding. For example, the following theorem “UML_OCL.level0.encoding.is_A_univ_implies_OclAny_univ” shows, that on the universe types, every object of class \(A\) is also an object of class \(OclAny\):

\[
\text{level0.encoding.is}_A \text{?obj} \implies \text{level0.is}_\text{OclAny}_\text{?obj}
\]

Using \(\text{get}_\text{mk}_A\_\text{id}\) and \(\text{get}_\text{mk}_A\_\text{id}\) we can convert “lossless” between our class type representation and universe representation, this is shown by “UML_OCL.level0.encoding.get\_mk\_A\_id”:

\[
\text{level0.encoding.is}_A \text{?obj} \implies \\
\text{level0.encoding.get}_A(\text{level0.encoding.mk}_A\text{?obj}) = \text{?obj}
\]

and “UML_OCL.level0.encoding.mk\_get\_A\_id”:

\[
\text{level0.encoding.is}_A \text{?univ} \implies \\
\text{level0.encoding.mk}_A(\text{level0.encoding.get}_A\text{?univ}) = \text{?univ}
\]

and “UML_OCL.level0.encoding.is\_A\_univ_implies_is\_get” shows that a successful type test on the universe types also implies a successful type test on the class types:

\[
\text{level0.encoding.is}_A \text{?univ} \implies \\
\text{level0.encoding.is}_A(\text{level0.encoding.get}_A\text{?univ})
\]

The theorem “UML_OCL.level0.encoding.is\_mk\_A” shows that the constructor creates an object that is of type \(A\):

\[
\text{level0.encoding.is}_A \text{?obj} \implies \\
\text{level0.encoding.is}_A\text{?univ}(\text{level0.encoding.mk}_A\text{?obj})
\]
Appendix C. Encoding UML/OCL by Example

and also satisfies the test of its super-type, e.g., OclAny. This is shown by the following theorem “UML_OCL.level0.encoding.is_OclAny_mk_A”:

\[
\text{level0.encoding.is}_A \ ?\ obj \Rightarrow \text{level0.is}_\text{OclAny}_\text{univ} \ (\text{level0.encoding.mk}_A \ ?\ obj)
\]

“UML_OCL.level0.encoding.cast_A_id” shows that we can successfully downcast objects:

\[
\text{level0.encoding.is}_A \ ?\ obj \Rightarrow \\
\text{level0.encoding.OclAny}_2 \ A \ (\text{level0.encoding.A}_2 \ OclAny \ ?\ obj) = \ ?\ obj
\]

Analogous, these properties are also shown for class B:

\[
\text{UML_OCL.level0.encoding.is}_B \text{ univ}_\text{implies}_A \text{ univ}:
\]

\[
\text{level0.encoding.is}_B \text{ univ} \ ?\ obj \Rightarrow \text{level0.encoding.is}_A \text{ univ} \ ?\ obj
\]

\[
\text{UML_OCL.level0.encoding.is}_B \text{ univ}_\text{implies}_is\_get:
\]

\[
\text{level0.encoding.is}_B \text{ univ} \ ?\ univ \Rightarrow \\
\text{level0.encoding.is}_B \ (\text{level0.encoding.get}_B \ ?\ univ)
\]

\[
\text{UML_OCL.level0.encoding.get}_\text{mk}_B \text{ id}:
\]

\[
\text{level0.encoding.is}_B \ ?\ obj \Rightarrow \\
\text{level0.encoding.get}_B \ (\text{level0.encoding.mk}_B \ ?\ obj) = \ ?\ obj
\]

\[
\text{UML_OCL.level0.encoding.is}_mk_B \ B:
\]

\[
\text{level0.encoding.is}_B \ ?\ obj \Rightarrow \\
\text{level0.encoding.is}_B \text{ univ} \ (\text{level0.encoding.mk}_B \ ?\ obj)
\]

\[
\text{UML_OCL.level0.encoding.is}_A \text{ mk}_B \ B:
\]

\[
\text{level0.encoding.is}_B \ ?\ obj \Rightarrow \\
\text{level0.encoding.is}_A \text{ univ} \ (\text{level0.encoding.mk}_B \ ?\ obj)
\]
C.3. Importing \textit{UML/OCL} models

\texttt{UML\_OCL.level0.encoding.mk\_get\_B\_id:}

\begin{verbatim}
level0.encoding.is\_B\_univ ?univ \Rightarrow
level0.encoding.mk\_B (level0.encoding.get\_B ?univ) = ?univ
\end{verbatim}

\texttt{UML\_OCL.level0.encoding.cast\_B\_id:}

\begin{verbatim}
level0.encoding.is\_B ?obj \Rightarrow
level0.encoding.A\_2\_B (level0.encoding.B\_2\_A ?obj) = ?obj
\end{verbatim}

C.3.2. Encoding Level 1:

The encoding on level 1 follows strictly the schema from level 0, i.e., we also start two type tests for objects, one for testing if a object is of a specific type or subtype (i.e., this test is true, if the object is of the given kind):

\texttt{UML\_OCL.level1.encoding.is\_A ::}

\begin{verbatim}
(state U ((A\_key × Integer\_0) × ((B\_key × oid) × 'a up + 'b) up + 'c)) ×
state U ((A\_key × Integer\_0) × ((B\_key × oid) × 'a up + 'b) up + 'c)
⇒ OclAny\_0 ((A\_key × Integer\_0) × ((B\_key × oid) × 'a up + 'b) up))
⇒ state U ((A\_key × Integer\_0) × ((B\_key × oid) × 'a up + 'b) up + 'c) ×
state U ((A\_key × Integer\_0) × ((B\_key × oid) × 'a up + 'b) up + 'c)
⇒ Boolean\_0
\end{verbatim}

level1.encoding.is\_A ≡ lift\_1 (strictify (lift \circ level0.encoding.is\_A))

and one for testing if a object is exactly the requested type

\texttt{UML\_OCL.level1.encoding.isType\_A ::}

\begin{verbatim}
(state U ((A\_key × Integer\_0) × ((B\_key × oid) × 'a up + 'b) up + 'c)) ×
state U ((A\_key × Integer\_0) × ((B\_key × oid) × 'a up + 'b) up + 'c)
⇒ OclAny\_0 ((A\_key × Integer\_0) × ((B\_key × oid) × 'a up + 'b) up))
⇒ state U ((A\_key × Integer\_0) × ((B\_key × oid) × 'a up + 'b) up + 'c) ×
state U ((A\_key × Integer\_0) × ((B\_key × oid) × 'a up + 'b) up + 'c)
⇒ Boolean\_0
\end{verbatim}

level1.encoding.isType\_A ≡ lift\_1 (strictify (lift \circ level0.encoding.isType\_A))
Further, we define a type for universe instances:

\[
UML_{OCL}.level1.encoding.is\_A\_univ ::
\]

\[
(state\_U ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a up + 'b) up + 'c) \times
\]

\[
state\_U ((A\_key \times Intege\_0) \times (B\_key \times oid) \times 'a up + 'b) up + 'c)
\]

\[
\Rightarrow U ((A\_key \times Intege\_0) \times (B\_key \times oid) \times 'a up + 'b) up + 'c)
\]

\[
\Rightarrow state\_U ((A\_key \times Intege\_0) \times (B\_key \times oid) \times 'a up + 'b) up + 'c) \times
\]

\[
state\_U ((A\_key \times Intege\_0) \times (B\_key \times oid) \times 'a up + 'b) up + 'c)
\]

\[
\Rightarrow Boolean\_0
\]

\[
level1.encoding.is\_A\_univ \equiv lift_1 (lift \circ level0.encoding.is\_A\_univ)
\]

Analogous we define for the inherited class B:

\[
UML_{OCL}.level1.encoding.is\_B ::
\]

\[
(state\_U ((A\_key \times Intege\_0) \times (B\_key \times oid) \times 'a up + 'b) up + 'c) \times
\]

\[
state\_U ((A\_key \times Intege\_0) \times (B\_key \times oid) \times 'a up + 'b) up + 'c)
\]

\[
\Rightarrow OclAny\_0 ((A\_key \times Intege\_0) \times (B\_key \times oid) \times 'a up) up)
\]

\[
\Rightarrow state\_U ((A\_key \times Intege\_0) \times (B\_key \times oid) \times 'a up + 'b) up + 'c) \times
\]

\[
state\_U ((A\_key \times Intege\_0) \times (B\_key \times oid) \times 'a up + 'b) up + 'c)
\]

\[
\Rightarrow Boolean\_0
\]

\[
level1.encoding.is\_B \equiv lift_1 (strictify (lift \circ level0.encoding.is\_B))
\]

\[
UML_{OCL}.level1.encoding.isType\_B ::
\]

\[
(state\_U ((A\_key \times Intege\_0) \times (B\_key \times oid) \times 'a up + 'b) up + 'c) \times
\]

\[
state\_U ((A\_key \times Intege\_0) \times (B\_key \times oid) \times 'a up + 'b) up + 'c)
\]

\[
\Rightarrow OclAny\_0 ((A\_key \times Intege\_0) \times (B\_key \times oid) \times 'a up) up)
\]

\[
\Rightarrow state\_U ((A\_key \times Intege\_0) \times (B\_key \times oid) \times 'a up + 'b) up + 'c) \times
\]

\[
state\_U ((A\_key \times Intege\_0) \times (B\_key \times oid) \times 'a up + 'b) up + 'c)
\]

\[
\Rightarrow Boolean\_0
\]

\[
level1.encoding.isType\_B \equiv lift_1 (strictify (lift \circ level0.encoding.isType\_B))
\]
C.3. Importing \texttt{UML/OCL} models

\[ \text{UML\_OCL.level1.encoding.is\_B\_univ ::} \]
\[ (\text{state } U \ ((A_{\text{key}} \times \text{Integer\_0}) \times ((B_{\text{key}} \times \text{oid}) \times 'a \text{ up} + 'b \text{ up} + 'c) \times) \]
\[ \Rightarrow U \ ((A_{\text{key}} \times \text{Integer\_0}) \times ((B_{\text{key}} \times \text{oid}) \times 'a \text{ up} + 'b \text{ up} + 'c)) \]
\[ \Rightarrow \text{OclAny\_0} \ ((A_{\text{key}} \times \text{Integer\_0}) \times ((B_{\text{key}} \times \text{oid}) \times 'a \text{ up} + 'b \text{ up})) \]
\[ \Rightarrow \text{state } U \ ((A_{\text{key}} \times \text{Integer\_0}) \times ((B_{\text{key}} \times \text{oid}) \times 'a \text{ up} + 'b \text{ up} + 'c) \times) \]
\[ \Rightarrow U \ ((A_{\text{key}} \times \text{Integer\_0}) \times ((B_{\text{key}} \times \text{oid}) \times 'a \text{ up} + 'b \text{ up} + 'c)) \]
\[ \Rightarrow \text{Boolean\_0} \]
\[ \text{level1.encoding.is\_B\_univ} \equiv \text{lift}_1 \ (\text{lift} \circ \text{level0.encoding.is\_B\_univ}) \]

We define a functions for embedding a class into the corresponding universe

\[ \text{UML\_OCL.level1.encoding.mk\_A ::} \]
\[ (\text{state } U \ ((A_{\text{key}} \times \text{Integer\_0}) \times ((B_{\text{key}} \times \text{oid}) \times 'a \text{ up} + 'b \text{ up} + 'c) \times) \]
\[ \Rightarrow \text{OclAny\_0} \ ((A_{\text{key}} \times \text{Integer\_0}) \times ((B_{\text{key}} \times \text{oid}) \times 'a \text{ up} + 'b \text{ up})) \]
\[ \Rightarrow \text{state } U \ ((A_{\text{key}} \times \text{Integer\_0}) \times ((B_{\text{key}} \times \text{oid}) \times 'a \text{ up} + 'b \text{ up} + 'c) \times) \]
\[ \Rightarrow U \ ((A_{\text{key}} \times \text{Integer\_0}) \times ((B_{\text{key}} \times \text{oid}) \times 'a \text{ up} + 'b \text{ up} + 'c)) \]
\[ \Rightarrow \text{level1.encoding.mk\_A} \equiv \text{lift}_1 \ \text{level0.encoding.mk\_A} \]

and one for extracting an object out of a given universe:

\[ \text{UML\_OCL.level1.encoding.get\_A ::} \]
\[ (\text{state } U \ ((A_{\text{key}} \times \text{Integer\_0}) \times ((B_{\text{key}} \times \text{oid}) \times 'a \text{ up} + 'b \text{ up} + 'c) \times) \]
\[ \Rightarrow U \ ((A_{\text{key}} \times \text{Integer\_0}) \times ((B_{\text{key}} \times \text{oid}) \times 'a \text{ up} + 'b \text{ up} + 'c)) \]
\[ \Rightarrow \text{state } U \ ((A_{\text{key}} \times \text{Integer\_0}) \times ((B_{\text{key}} \times \text{oid}) \times 'a \text{ up} + 'b \text{ up} + 'c) \times) \]
\[ \Rightarrow \text{OclAny\_0} \ ((A_{\text{key}} \times \text{Integer\_0}) \times ((B_{\text{key}} \times \text{oid}) \times 'a \text{ up} + 'b \text{ up} + 'c)) \]
\[ \Rightarrow \text{level1.encoding.get\_A} \equiv \text{lift}_1 \ \text{level0.encoding.get\_A} \]

These two functions can also be understood as conversion between object types and universe types.
Appendix C. Encoding UML/ocl by Example

Analogous we define for the inherited class B:

\[UML\_ocl.level1.encoding.mk\_B ::\]
\[(state\ U\ ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a\ up + \ b)\ up + \ 'c)\times state\ U\ ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a\ up + \ b)\ up + \ 'c)\Rightarrow OclAny\_0\ ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a\ up)\ up)\Rightarrow state\ U\ ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a\ up + \ b)\ up + \ 'c)\times state\ U\ ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a\ up + \ b)\ up + \ 'c)\Rightarrow U\ ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a\ up + \ b)\ up + \ 'c)\]

\[level1.encoding.mk\_B \equiv lift\_1\ level0.encoding.mk\_B\]

\[UML\_ocl.level1.encoding.get\_B ::\]
\[(state\ U\ ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a\ up + \ b)\ up + \ 'c)\times state\ U\ ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a\ up + \ b)\ up + \ 'c)\Rightarrow U\ ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a\ up + \ b)\ up + \ 'c)\Rightarrow state\ U\ ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a\ up + \ b)\ up + \ 'c)\times state\ U\ ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a\ up + \ b)\ up + \ 'c)\Rightarrow OclAny\_0\ ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a\ up)\ up)\Rightarrow state\ U\ ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a\ up + \ b)\ up + \ 'c)\times state\ U\ ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a\ up + \ b)\ up + \ 'c)\Rightarrow OclAny\_0\ ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a\ up + \ b)\ up + \ 'c)\]

\[level1.encoding.get\_B \equiv lift\_1\ level0.encoding.get\_B\]

For converting along type hierarchies (i.e. down-casting and up-casting) we provide
for each class two functions for the conversion to the direct predecessor and direct successor in the class hierarchy:

\[UML\_ocl.level1.encoding.A\_2\_OclAny ::\]
\[(state\ U\ ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a\ up + \ b)\ up + \ 'c)\times state\ U\ ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a\ up + \ b)\ up + \ 'c)\Rightarrow OclAny\_0\ ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a\ up + \ b)\ up)\Rightarrow state\ U\ ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a\ up + \ b)\ up + \ 'c)\times state\ U\ ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a\ up + \ b)\ up + \ 'c)\Rightarrow OclAny\_0\ ((A\_key \times Integer\_0) \times (B\_key \times oid) \times 'a\ up + \ b)\ up + \ 'c)\]

\[level1.encoding.A\_2\_OclAny \equiv lift\_1\ level0.encoding.A\_2\_OclAny\]
C.3. Importing UML/OCaml models

\[ UML_{-}OCL_{.}level_{1}\.encoding\.OclAny_{-}2_{-}A :: \]
\[
\text{(state } U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up } + 'b) up + 'c) \times \]
\[
\text{state } U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up } + 'b) up + 'c) \Rightarrow \text{OclAny}_0 \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up } + 'b) up + 'c) \]
\[
\text{state } U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up } + 'b) up + 'c) \Rightarrow \text{OclAny}_0 \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up } + 'b) up + 'c) \]
\[
\text{level}_1\.encoding\.OclAny_{-}2_{-}A \equiv \text{lift}_1 \text{ level}_0\.encoding\.OclAny_{-}2_{-}A \]

Analogous we define for the inherited class B:

\[ UML_{-}OCL_{.}level_{1}\.encoding\.B_{-}2_{-}A :: \]
\[
\text{(state } U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up } + 'b) up + 'c) \times \]
\[
\text{state } U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up } + 'b) up + 'c) \Rightarrow \text{OclAny}_0 \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up } + 'b) up + 'c) \]
\[
\text{state } U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up } + 'b) up + 'c) \Rightarrow \text{OclAny}_0 \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up } + 'b) up + 'c) \]
\[
\text{level}_1\.encoding\.B_{-}2_{-}A \equiv \text{lift}_1 \text{ level}_0\.encoding\.B_{-}2_{-}A \]

\[ UML_{-}OCL_{.}level_{1}\.encoding\.A_{-}2_{-}B :: \]
\[
\text{(state } U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up } + 'b) up + 'c) \times \]
\[
\text{state } U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up } + 'b) up + 'c) \Rightarrow \text{OclAny}_0 \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up } + 'b) up + 'c) \]
\[
\text{state } U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up } + 'b) up + 'c) \Rightarrow \text{OclAny}_0 \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up } + 'b) up + 'c) \]
\[
\text{level}_1\.encoding\.A_{-}2_{-}B \equiv \text{lift}_1 \text{ level}_0\.encoding\.A_{-}2_{-}B \]
Appendix C. Encoding UML/ocl by Example

Finally, we provide accessor functions for the class attributes:

\[
\text{UML\_OCL.level1.encoding.A.i ::} \\
(\text{state } U \ (A\text{\textunderscore key} \times \text{Integer}_0) \times (B\text{\textunderscore key} \times \text{oid}) \times \text{’a up + b up + c}) \times \\
\text{state } U \ (A\text{\textunderscore key} \times \text{Integer}_0) \times (B\text{\textunderscore key} \times \text{oid}) \times \text{’a up + b up + c) } \\
\Rightarrow \text{OclAny}_0 ((A\text{\textunderscore key} \times \text{Integer}_0) \times (B\text{\textunderscore key} \times \text{oid}) \times \text{’a up + b up})) \\
\Rightarrow \text{state } U \ (A\text{\textunderscore key} \times \text{Integer}_0) \times (B\text{\textunderscore key} \times \text{oid}) \times \text{’a up + b up + c}) \\
\Rightarrow \text{OclAny}_0 ((A\text{\textunderscore key} \times \text{Integer}_0) \times (B\text{\textunderscore key} \times \text{oid}) \times \text{’a up}) \\
\Rightarrow \text{Integer}_0 \\
\text{level1.encoding.A.i} \equiv \text{lift1 (strictify level0.encoding.A.i)}
\]

\[
\text{UML\_OCL.level1.encoding.B.j ::} \\
(\text{state } U \ (A\text{\textunderscore key} \times \text{Integer}_0) \times (B\text{\textunderscore key} \times \text{oid}) \times \text{’a up + b up + c}) \times \\
\text{state } U \ (A\text{\textunderscore key} \times \text{Integer}_0) \times (B\text{\textunderscore key} \times \text{oid}) \times \text{’a up + b up + c) } \\
\Rightarrow \text{OclAny}_0 ((A\text{\textunderscore key} \times \text{Integer}_0) \times (B\text{\textunderscore key} \times \text{oid}) \times \text{’a up})) \\
\Rightarrow \text{state } U \ (A\text{\textunderscore key} \times \text{Integer}_0) \times (B\text{\textunderscore key} \times \text{oid}) \times \text{’a up + b up + c}) \\
\Rightarrow \text{OclAny}_0 ((A\text{\textunderscore key} \times \text{Integer}_0) \times (B\text{\textunderscore key} \times \text{oid}) \times \text{’a up}) \\
\Rightarrow \text{Integer}_0 \\
\text{level1.encoding.B.j} \equiv \\
\lambda X. \text{case fst St (level0.encoding.B.j (X St)) of } \text{None} \Rightarrow \bot \\
| \text{Some x} \Rightarrow \text{level0.encoding.get_B x}
\]

Proving Properties

Already on this level, we can prove important properties of our encoding. For example, the following theorem “UML\_OCL.level1.encoding.is\_A\_univ\_implies\_OclAny\_univ” shows, that on the universe types, every object of class A is also an object of class OclAny:

\[?St \models \text{level1.encoding.is\_A\_univ?obj} \implies ?St \models \text{level1.is\_OclAny\_univ?obj} \]
C.3. Importing UML/OCL models

Using get_mk_A_id and get_mk_A_id we can convert “lossless” between our class type representation and universe representation, this is shown by “UML/OCL.level1.encoding.get_mk_A_id”:

\[ \text{level1.encoding.get}_A (\text{level1.encoding.mk}_A \ ? \text{obj}) \ ? \text{St} = \ ? \text{obj} \ ? \text{St} \]

and “UML/OCL.level1.encoding.mk_get_A_id”:

\[ \text{level1.encoding.mk}_A (\text{level1.encoding.get}_A \ ? \text{univ}) \ ? \text{St} = \ ? \text{univ} \ ? \text{St} \]

and “UML/OCL.level1.encoding.is_A_univ_implies_is_get” shows that a successful type test on the universe types also implies a successful type test on the class types:

\[ \text{DEF} (\text{level1.encoding.get}_A \ ? \text{univ} \ ? \text{St}); \ ? \text{St} = \ ? \text{level1.encoding.is}_A \ ? \text{univ} \ ? \text{univ} \]

\[ \implies \ ? \text{St} = \ ? \text{level1.encoding.is}_A (\text{level1.encoding.get}_A \ ? \text{univ}) \]

The theorem “UML/OCL.level1.encoding.is_mk_A” shows that the constructor creates an object that is of type A:

\[ \text{level1.encoding.is}_A \ ? \text{obj} \implies \ ? \text{St} = \ ? \text{level1.encoding.is}_A \ ? \text{obj} \]

and also satisfies the test of its super-type, e.g., OclAny. This is shown by the following theorem “UML/OCL.level1.encoding.is_OclAny_mk_A”:

\[ \text{level1.encoding.is}_A \ ? \text{obj} \implies \ ? \text{St} = \ ? \text{level1.is}_A \ ? \text{univ} (\text{level1.encoding.mk}_A \ ? \text{obj}) \]

“UML/OCL.level1.encoding.cast_A_id” shows that we can successfully downcast objects:

\[ \text{level1.encoding.OclAny}_2 \ ? \text{A} (\text{level1.encoding.A}_2 \ ? \text{OclAny} \ ? \text{obj}) \ ? \text{St} = \ ? \text{obj} \ ? \text{St} \]
Appendix C. Encoding UML/OCL by Example

Analogous, these properties are also shown for class B:

UML_OCL.level1.encoding.is_B_univ_implies_A_univ:

?St ⊨ level1.encoding.is_B_univ ?obj → ?St ⊨ level1.encoding.is_A_univ ?obj

UML_OCL.level1.encoding.is_B_univ_implies_is_get:

[DEF (level1.encoding.get_B ?univ ?St); ?St ⊨ level1.encoding.is_B_univ ?univ] → ?St ⊨ level1.encoding.is_B (level1.encoding.get_B ?univ)

UML_OCL.level1.encoding.get_mk_B_id:

?St ⊨ level1.encoding.is_B ?obj → level1.encoding.get_B (level1.encoding.mk_B ?obj) ?St = ?obj ?St

UML_OCL.level1.encoding.is_mk_B:

?St ⊨ level1.encoding.is_B ?obj → ?St ⊨ level1.encoding.is_B_univ (level1.encoding.mk_B ?obj)

UML_OCL.level1.encoding.is_A_mk_B:

?St ⊨ level1.encoding.is_B ?obj → ?St ⊨ level1.encoding.is_A_univ (level1.encoding.mk_B ?obj)

UML_OCL.level1.encoding.mk_get_B_id:

?St ⊨ level1.encoding.is_B_univ ?univ → level1.encoding.mk_B (level1.encoding.get_B ?univ) ?St = ?univ ?St

UML_OCL.level1.encoding.cast_B_id:

?St ⊨ level1.encoding.is_B ?obj → level1.encoding.A_2_B (level1.encoding.B_2_A ?obj) ?St = ?obj ?St
C.3. Importing UML/OCL models

Further we show that our definitions are context passing:

UML_OCL.level1.encoding.cp_get_A:

cp level1.encoding.get_A

UML_OCL.level1.encoding.cp_mk_A:

cp level1.encoding.mk_A

UML_OCL.level1.encoding.cp_is_A:

cp level1.encoding.is_A

UML_OCL.level1.encoding.cp_is_univ_A:

cp level1.encoding.is_A_univ

UML_OCL.level1.encoding.cp_get_B:

cp level1.encoding.get_B

UML_OCL.level1.encoding.cp_mk_B:

cp level1.encoding.mk_B

UML_OCL.level1.encoding.cp_is_B:

cp level1.encoding.is_B

UML_OCL.level1.encoding.cp_is_univ_B:

cp level1.encoding.is_B_univ
Appendix C. Encoding UML/\text{OCL} by Example

C.3.3. Encoding Level 2:

Encoding of [\text{OCL}] Invariants: Part One

Here we bring the data part (i.e., UML) together with the \text{OCL} specification. The encoding of \text{OCL} formulae is two-staged. First, the formulae are encoding without requiring the definedness of the occurring path expressions, we extend these formulae later with the required definedness constraints. This two-staged process allows us to break cyclic dependencies and thus encode \text{OCL} conservatively.

Thus, for class A we generate two invariants; The first one describes the initial value of the attribute i:

\textit{UML\textunderscore OCL.\textunderscore level1.\textunderscore encoding.\textunderscore A.\textunderscore model.hol\_invariant.init\_i ::}
\begin{align*}
\text{state } U ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times (a \uparrow \downarrow + (b \uparrow \downarrow) + (c \uparrow \downarrow) \times \\
\text{state } U ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times (a \uparrow \downarrow) + (b \uparrow \downarrow) + (c \uparrow \downarrow) \times \\
\Rightarrow (\text{state } U ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times (a \uparrow \downarrow) + (b \uparrow \downarrow) + (c \uparrow \downarrow) \times \\
\text{state } U ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times (a \uparrow \downarrow) + (b \uparrow \downarrow) + (c \uparrow \downarrow) \times \\
\Rightarrow \text{OclAny}_0 ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times (a \uparrow \downarrow) + (b \uparrow \downarrow) + (c \uparrow \downarrow)) \downarrow \text{set} \\
\Rightarrow (\text{state } U ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times (a \uparrow \downarrow) + (b \uparrow \downarrow) + (c \uparrow \downarrow) \times \\
\text{state } U ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times (a \uparrow \downarrow) + (b \uparrow \downarrow) + (c \uparrow \downarrow) \times \\
\Rightarrow \text{OclAny}_0 ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times (a \uparrow \downarrow) + (b \uparrow \downarrow) + (c \uparrow \downarrow)) \downarrow \text{up}) \\
\Rightarrow \text{bool}\downarrow
\end{align*}

\begin{align*}
\text{model.hol\_invariant.init\_i} & \equiv \\
\lambda \text{C self}. \downarrow \text{OclIsNew self} \dashrightarrow \text{level1.\textunderscore encoding.\textunderscore A.i self} \Downarrow 42
\end{align*}

and the second one describes the user defined invariant:

\textit{UML\textunderscore OCL.\textunderscore level1.\textunderscore encoding.\textunderscore A.\textunderscore model.hol\_invariant.inv\_1 ::}
\begin{align*}
\text{state } U ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times (a \uparrow \downarrow + (b \uparrow \downarrow) + (c \uparrow \downarrow) \times \\
\text{state } U ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times (a \uparrow \downarrow) + (b \uparrow \downarrow) + (c \uparrow \downarrow) \times \\
\Rightarrow (\text{state } U ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times (a \uparrow \downarrow) + (b \uparrow \downarrow) + (c \uparrow \downarrow) \times \\
\text{state } U ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times (a \uparrow \downarrow) + (b \uparrow \downarrow) + (c \uparrow \downarrow) \times \\
\Rightarrow \text{OclAny}_0 ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times (a \uparrow \downarrow) + (b \uparrow \downarrow) + (c \uparrow \downarrow)) \downarrow \text{set} \\
\Rightarrow (\text{state } U ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times (a \uparrow \downarrow) + (b \uparrow \downarrow) + (c \uparrow \downarrow) \times \\
\text{state } U ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times (a \uparrow \downarrow) + (b \uparrow \downarrow) + (c \uparrow \downarrow) \times \\
\Rightarrow \text{OclAny}_0 ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times (a \uparrow \downarrow) + (b \uparrow \downarrow) + (c \uparrow \downarrow)) \downarrow \text{up}) \\
\Rightarrow \text{bool}\downarrow
\end{align*}

\begin{align*}
\text{model.hol\_invariant.inv\_1} & \equiv \lambda \text{C self}. \downarrow \text{level1.\textunderscore encoding.\textunderscore A.i self} \geq 0
\end{align*}
The overall invariant for class $A$ is constructed by conjoining these invariants.

\[ UML\_OCL.level1.encoding.A.model.hol\_invariant :: \]
\[
\text{state } U \ ( (A\_key \times \text{Integer}\_0) \times ((B\_key \times \text{oid}) \times 'a \ \text{up} + 'b) \ \text{up} + 'c) \times \\
\text{state } U \ ( (A\_key \times \text{Integer}\_0) \times ((B\_key \times \text{oid}) \times 'a \ \text{up} + 'b) \ \text{up} + 'c) \\
\Rightarrow (\text{state } U \ ( (A\_key \times \text{Integer}\_0) \times ((B\_key \times \text{oid}) \times 'a \ \text{up} + 'b) \ \text{up} + 'c) \times \\
\text{state } U \ ( (A\_key \times \text{Integer}\_0) \times ((B\_key \times \text{oid}) \times 'a \ \text{up} + 'b) \ \text{up} + 'c) \\
\Rightarrow \text{OclAny\_0} \ ( (A\_key \times \text{Integer}\_0) \times ((B\_key \times \text{oid}) \times 'a \ \text{up} + 'b) \ \text{up}) \text{ set} \\
\Rightarrow (\text{state } U \ ( (A\_key \times \text{Integer}\_0) \times ((B\_key \times \text{oid}) \times 'a \ \text{up} + 'b) \ \text{up} + 'c) \times \\
\text{state } U \ ( (A\_key \times \text{Integer}\_0) \times ((B\_key \times \text{oid}) \times 'a \ \text{up} + 'b) \ \text{up} + 'c) \\
\Rightarrow \text{OclAny\_0} \ ( (A\_key \times \text{Integer}\_0) \times ((B\_key \times \text{oid}) \times 'a \ \text{up} + 'b) \ \text{up})) \\
\Rightarrow \text{bool} \\
\]

\[ A.model.hol\_invariant \equiv \]
\[ \lambda \tau \text{ C obj,} \\
\text{model.hol\_invariant.init\_i } \tau \text{ C obj } \land \\
\text{model.hol\_invariant.inv\_1 } \tau \text{ C obj } \land \\
\text{A.model.hol\_invariant.check\_parent\_inv } \tau \text{ C obj} \]

Analogous we are encoding the pre-condition and post-condition of the operation $f$:

\[ encoding.A.f\_Integer\_Integer.pre1.pre\_0 :: \]
\[
\text{state } U \ ( (A\_key \times \text{Integer}\_0) \times ((B\_key \times \text{oid}) \times 'a \ \text{up} + 'b) \ \text{up} + 'c) \times \\
\text{state } U \ ( (A\_key \times \text{Integer}\_0) \times ((B\_key \times \text{oid}) \times 'a \ \text{up} + 'b) \ \text{up} + 'c) \\
\Rightarrow \text{OclAny\_0} \ ( (A\_key \times \text{Integer}\_0) \times ((B\_key \times \text{oid}) \times 'a \ \text{up} + 'b) \ \text{up})) \\
\Rightarrow (\text{state } U \ ( (A\_key \times \text{Integer}\_0) \times ((B\_key \times \text{oid}) \times 'a \ \text{up} + 'b) \ \text{up} + 'c) \times \\
\text{state } U \ ( (A\_key \times \text{Integer}\_0) \times ((B\_key \times \text{oid}) \times 'a \ \text{up} + 'b) \ \text{up} + 'c) \\
\Rightarrow \text{Integer\_0} \\
\Rightarrow \text{state } U \ ( (A\_key \times \text{Integer}\_0) \times ((B\_key \times \text{oid}) \times 'a \ \text{up} + 'b) \ \text{up} + 'c) \times \\
\text{state } U \ ( (A\_key \times \text{Integer}\_0) \times ((B\_key \times \text{oid}) \times 'a \ \text{up} + 'b) \ \text{up} + 'c) \\
\Rightarrow \text{Boolean\_0} \\
\]

\[ \text{pre\_0 } \equiv \lambda \text{self } x. \ x > 0 \]
Appendix C. Encoding UML/\textit{OCL} by Example

\hspace{1cm} encoding.A.f \_Integer\_Integer.post1.post_0 ::
\hspace{1cm} (state U ((A\_key \times Integer\_0) \times (B\_key \times oid)) \times \text{'a up + 'b up + 'c}) \times
\hspace{1cm} state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \text{'a up + 'b up + 'c})
\hspace{1cm} \Rightarrow \text{OclAny}_0 ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \text{'a up + 'b up}))
\hspace{1cm} \Rightarrow (state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \text{'a up + 'b up + 'c}) \times
\hspace{1cm} state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \text{'a up + 'b up + 'c})
\hspace{1cm} \Rightarrow Integer\_0)
\hspace{1cm} \Rightarrow (state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \text{'a up + 'b up + 'c}) \times
\hspace{1cm} state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \text{'a up + 'b up + 'c})
\hspace{1cm} \Rightarrow Integer\_0)
\hspace{1cm} \Rightarrow state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \text{'a up + 'b up + 'c}) \times
\hspace{1cm} state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \text{'a up + 'b up + 'c})
\hspace{1cm} \Rightarrow Boolean\_0)
\hspace{1cm} post_0 \equiv \lambda\text{self x result. result} \triangleq \text{x ->div( level1.encoding.A.i self )}

\hspace{1cm} encoding.A.f \_Integer\_Integer.pre1 ::
\hspace{1cm} (state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \text{'a up + 'b up + 'c}) \times
\hspace{1cm} state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \text{'a up + 'b up + 'c})
\hspace{1cm} \Rightarrow \text{OclAny}_0 ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \text{'a up + 'b up}))
\hspace{1cm} \Rightarrow (state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \text{'a up + 'b up + 'c}) \times
\hspace{1cm} state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \text{'a up + 'b up + 'c})
\hspace{1cm} \Rightarrow Integer\_0)
\hspace{1cm} \Rightarrow (state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \text{'a up + 'b up + 'c}) \times
\hspace{1cm} state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \text{'a up + 'b up + 'c})
\hspace{1cm} \Rightarrow Boolean\_0)
\hspace{1cm} pre1 \equiv pre_0
C.3. Importing UML/OCaml models

encoding.A.f_Integer_Integer.post1 ::
(state U ((\text{A\_key} \times \text{Integer\_0}) \times ((\text{B\_key} \times \text{oid}) \times 'a\ up\ +\ 'b)\ up\ +\ 'c) \times
\text{state U} ((\text{A\_key} \times \text{Integer\_0}) \times ((\text{B\_key} \times \text{oid}) \times 'a\ up\ +\ 'b)\ up\ +\ 'c)
\Rightarrow \text{OclAny\_0} ((\text{A\_key} \times \text{Integer\_0}) \times ((\text{B\_key} \times \text{oid}) \times 'a\ up\ +\ 'b)\ up))
\Rightarrow (\text{state U} ((\text{A\_key} \times \text{Integer\_0}) \times ((\text{B\_key} \times \text{oid}) \times 'a\ up\ +\ 'b)\ up\ +\ 'c) \times
\text{state U} ((\text{A\_key} \times \text{Integer\_0}) \times ((\text{B\_key} \times \text{oid}) \times 'a\ up\ +\ 'b)\ up\ +\ 'c)
\Rightarrow \text{Integer\_0})
\Rightarrow (\text{state U} ((\text{A\_key} \times \text{Integer\_0}) \times ((\text{B\_key} \times \text{oid}) \times 'a\ up\ +\ 'b)\ up\ +\ 'c) \times
\text{state U} ((\text{A\_key} \times \text{Integer\_0}) \times ((\text{B\_key} \times \text{oid}) \times 'a\ up\ +\ 'b)\ up\ +\ 'c)
\Rightarrow \text{Integer\_0})
\Rightarrow (\text{state U} ((\text{A\_key} \times \text{Integer\_0}) \times ((\text{B\_key} \times \text{oid}) \times 'a\ up\ +\ 'b)\ up\ +\ 'c) \times
\text{state U} ((\text{A\_key} \times \text{Integer\_0}) \times ((\text{B\_key} \times \text{oid}) \times 'a\ up\ +\ 'b)\ up\ +\ 'c)
\Rightarrow Boolean\_0)
\text{post1} \equiv \text{post\_0}

For class B no initial values or invariants are given, thus we generate invariants that are just true:

encoding.B.inv.init\_j ::
(state U ((\text{A\_key} \times \text{Integer\_0}) \times ((\text{B\_key} \times \text{oid}) \times 'a\ up\ +\ 'b)\ up\ +\ 'c) \times
\text{state U} ((\text{A\_key} \times \text{Integer\_0}) \times ((\text{B\_key} \times \text{oid}) \times 'a\ up\ +\ 'b)\ up\ +\ 'c)
\Rightarrow \text{OclAny\_0} ((\text{A\_key} \times \text{Integer\_0}) \times ((\text{B\_key} \times \text{oid}) \times 'a\ up\) up))
\Rightarrow (\text{state U} ((\text{A\_key} \times \text{Integer\_0}) \times ((\text{B\_key} \times \text{oid}) \times 'a\ up\ +\ 'b)\ up\ +\ 'c) \times
\text{state U} ((\text{A\_key} \times \text{Integer\_0}) \times ((\text{B\_key} \times \text{oid}) \times 'a\ up\ +\ 'b)\ up\ +\ 'c)
\Rightarrow \text{Boolean\_0})
\text{inv.init\_j} \equiv \lambda\text{self. T}

encoding.B.inv.init\_j ::
(state U ((\text{A\_key} \times \text{Integer\_0}) \times ((\text{B\_key} \times \text{oid}) \times 'a\ up\ +\ 'b)\ up\ +\ 'c) \times
\text{state U} ((\text{A\_key} \times \text{Integer\_0}) \times ((\text{B\_key} \times \text{oid}) \times 'a\ up\ +\ 'b)\ up\ +\ 'c)
\Rightarrow \text{OclAny\_0} ((\text{A\_key} \times \text{Integer\_0}) \times ((\text{B\_key} \times \text{oid}) \times 'a\ up\) up))
\Rightarrow (\text{state U} ((\text{A\_key} \times \text{Integer\_0}) \times ((\text{B\_key} \times \text{oid}) \times 'a\ up\ +\ 'b)\ up\ +\ 'c) \times
\text{state U} ((\text{A\_key} \times \text{Integer\_0}) \times ((\text{B\_key} \times \text{oid}) \times 'a\ up\ +\ 'b)\ up\ +\ 'c)
\Rightarrow \text{Boolean\_0})
\text{inv.init\_j} \equiv \lambda\text{self. T}
Appendix C. Encoding UML/OCL by Example

The overall invariant for class B is constructed by conjoining these invariants.

\[
\text{encoding.B.inv.inv} ::
\text{state } U \left( (A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a up + 'b) up + 'c) \times \\
\text{state } U \left( (A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a up + 'b) up + 'c) \\
\Rightarrow \text{OclAny}_0 ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a up) up) \\
\Rightarrow \text{state } U \left( (A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a up + 'b) up + 'c) \times \\
\text{state } U \left( (A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a up + 'b) up + 'c) \\
\Rightarrow \text{Boolean}_0
\]

\[
B.inv.inv \equiv \text{inv.init}_j
\]

Encoding Of Operations

First we define a constant for the operation \(f\) describing its core semantics specified by the pre-condition and post-condition:

\[
\text{encoding.A.f} ::
\text{state } U \left( (A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a up + 'b) up + 'c) \times \\
\text{state } U \left( (A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a up + 'b) up + 'c) \\
\Rightarrow \text{OclAny}_0 'd) \\
\Rightarrow \text{state } U \left( (A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a up + 'b) up + 'c) \times \\
\text{state } U \left( (A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a up + 'b) up + 'c) \\
\Rightarrow \text{Integer}_0 \\
\Rightarrow \text{state } U \left( (A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a up + 'b) up + 'c) \times \\
\text{state } U \left( (A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times 'a up + 'b) up + 'c) \\
\Rightarrow \text{Boolean}_0
\]

\[
f \equiv \lambda self \ x \ result. \ \text{pre1 self x} \ \land \ \text{post1 self x result}
\]
For each method, we create a table storing all variants, i.e., overloading.

\[
\text{UML\textunderscore OCL.\textit{ops.f\_Integer\_Integer.tab}} \defeq \\
\begin{array}{l}
\text{\textit{\textquote{a} set} }\mapsto \\
\text{(state U ((A\_key \times \text{\textit{Integer\_0}}) \times ((B\_key \times \text{\textit{oid}}) \times \text{\textquote{b up \textquote{c} up \textquote{d}}) \times \\
state U ((A\_key \times \text{\textit{Integer\_0}}) \times ((\text{\textit{b up \textquote{c} up \textquote{d}}}) \times \\
\Rightarrow \text{{\textit{OclAny\_0 \textquote{a}}} (state U ((A\_key \times \text{\textit{Integer\_0}}) \times ((B\_key \times \text{\textit{oid}}) \times \text{\textquote{b up \textquote{c} up \textquote{d}}) \\
\Rightarrow \text{{\textit{Integer\_0}}} (state U ((A\_key \times \text{\textit{Integer\_0}}) \times ((B\_key \times \text{\textit{oid}}) \times \text{\textquote{b up \textquote{c} up \textquote{d}}) \\
\Rightarrow \text{Boolean\_0}})
\end{array}
\]

The entry for \textit{f} in this operation table is defined as follows:

\[
\text{UML\textunderscore OCL.\textit{ops.f\_Integer\_Integer.Op}} \defeq \\
\begin{array}{l}
\text{(state U ((A\_key \times \text{\textit{Integer\_0}}) \times ((B\_key \times \text{\textit{oid}}) \times \text{\textquote{a up \textquote{b} up \textquote{c}}}))) \times \\
\text{(state U ((A\_key \times \text{\textit{Integer\_0}}) \times ((\text{\textit{a up \textquote{b} up \textquote{c}}}))) \times \\
\Rightarrow \text{{\textit{OclAny\_0 \textquote{d}}} (state U ((A\_key \times \text{\textit{Integer\_0}}) \times ((\text{\textit{a up \textquote{b} up \textquote{c}}}))) \\
\Rightarrow \text{{\textit{Integer\_0}}} (state U ((A\_key \times \text{\textit{Integer\_0}}) \times ((\text{\textit{a up \textquote{b} up \textquote{c}}}))) \\
\Rightarrow \text{Integer\_0}) \\
\Rightarrow \text{\textit{OCL\_choose}} (\text{\textit{OCL\_invokeS arbitrary tab self x}})
\end{array}
\]

\[
\text{Op \equiv \lambda self \ x. OCL\_choose (OCL\_invokeS arbitrary tab self x)}
\]

and as UML\textunderscore OCL.\textit{ops.f\_Integer\_Integer.overwrite\_A}:

\[
\text{tab (range encoding.mk\_A) }\equiv \text{Some f}
\]

\[
(C.1)
\]
Appendix C. Encoding \textit{UML}/OCL by Example

\textbf{Encoding the Basic UML part}

The encoding of the data model on level 2 follows strictly the known schema from level 0 and 1, i.e., we also start two type tests for objects, one for testing if an object is of a specific type or subtype (i.e., this test is true, if the object is of the given kind):

\begin{verbatim}
encoding.is_A ::
    (state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c) ×
    state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c)
⇒ OclAny_0 ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up))
⇒ state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c) ×
    state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c)
⇒ Boolean_0

encoding.is_A ≡ λx. if A.model.inv x then level1.encoding.is_A x else Fendif
\end{verbatim}

and one for testing if an object is exactly the requested type

\begin{verbatim}
encoding.isType_A ::
    (state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c) ×
    state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c)
⇒ OclAny_0 ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up))
⇒ state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c) ×
    state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c)
⇒ Boolean_0

encoding.isType_A ≡ λx. if A.model.inv x then level1.encoding.isType_A x else Fendif
\end{verbatim}

Further, we define a type for universe instances:

\begin{verbatim}
encoding.is_A_univ ::
    (state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c) ×
    state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c)
⇒ U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c))
⇒ state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c) ×
    state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c)
⇒ Boolean_0

encoding.is_A_univ ≡ λx. if (A.model.inv o level1.encoding.get_A) x then level1.encoding.is_A_univ x else Fendif
\end{verbatim}

462
C.3. Importing UML/OCL models

Analogous we define for the inherited class B:

\[\text{encoding.is}_B ::\]
\[
\text{(state } U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up + 'b) up + 'c) \times
\]
\[
\text{state } U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up + 'b) up + 'c)
\]
\[
\Rightarrow \text{OclAny}_0 \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up) up))
\]
\[
\Rightarrow \text{state } U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up + 'b) up + 'c) \times
\]
\[
\text{state } U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up + 'b) up + 'c)
\]
\[
\Rightarrow \text{Boolean}_0
\]
\[\text{encoding.is}_B \equiv \lambda x. \text{ if } B\text{.model.inv } x \text{ then level1.encoding.is}_B x \text{ else Fendif}\]

\[\text{encoding.isType}_B ::\]
\[
\text{(state } U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up + 'b) up + 'c) \times
\]
\[
\text{state } U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up + 'b) up + 'c)
\]
\[
\Rightarrow \text{OclAny}_0 \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up) up))
\]
\[
\Rightarrow \text{state } U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up + 'b) up + 'c) \times
\]
\[
\text{state } U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up + 'b) up + 'c)
\]
\[
\Rightarrow \text{Boolean}_0
\]
\[\text{encoding.isType}_B \equiv \lambda x. \text{ if } B\text{.model.inv } x \text{ then level1.encoding.isType}_B x \text{ else Fendif}\]

\[\text{encoding.is}_B\text{.univ} ::\]
\[
\text{(state } U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up + 'b) up + 'c) \times
\]
\[
\text{state } U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up + 'b) up + 'c)
\]
\[
\Rightarrow U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up + 'b) up + 'c))
\]
\[
\Rightarrow \text{state } U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up + 'b) up + 'c) \times
\]
\[
\text{state } U \text{ ((A_key } \times \text{ Integer}_0) \times ((B_key } \times \text{ oid}) \times 'a up + 'b) up + 'c)
\]
\[
\Rightarrow \text{Boolean}_0
\]
\[\text{encoding.is}_B\text{.univ} \equiv \lambda x. \text{ if } (B\text{.model.inv o level1.encoding.get}_B) x \text{ then level1.encoding.is}_B\text{.univ } x \text{ else Fendif}\]
Appendix C. Encoding UML/OCL by Example

We define a functions for embedding a class into the corresponding universe

\[
\text{encoding.mk}_A ::
\begin{align*}
\text{state } U & \Rightarrow (\text{state } U \Rightarrow \text{state } U) \\
& \Rightarrow \text{OclAny}_0 \Rightarrow \text{state } U \\
& \Rightarrow U \Rightarrow \text{OclAny}_0 \\
\end{align*}
\]

\[
\text{encoding.mk}_B ::
\begin{align*}
\text{state } U & \Rightarrow (\text{state } U \Rightarrow \text{state } U) \\
& \Rightarrow \text{OclAny}_0 \Rightarrow \text{state } U \\
& \Rightarrow U \Rightarrow \text{OclAny}_0 \\
\end{align*}
\]

\[
\text{encoding.mk}_A \equiv \lambda x. \text{if } A.\text{model.inv} \ x \ \text{then level1.encoding.mk}_A \ x \ \text{else level1.encoding.mk}_A \ \text{endif}
\]

and one for extracting an object out of a given universe:

\[
\text{encoding.get}_A ::
\begin{align*}
\text{state } U & \Rightarrow (\text{state } U \Rightarrow \text{state } U) \\
& \Rightarrow \text{OclAny}_0 \Rightarrow \text{state } U \\
& \Rightarrow U \Rightarrow \text{OclAny}_0 \\
\end{align*}
\]

\[
\text{encoding.get}_B ::
\begin{align*}
\text{state } U & \Rightarrow (\text{state } U \Rightarrow \text{state } U) \\
& \Rightarrow \text{OclAny}_0 \Rightarrow \text{state } U \\
& \Rightarrow U \Rightarrow \text{OclAny}_0 \\
\end{align*}
\]

\[
\text{encoding.get}_A \equiv \lambda x. \text{if } (A.\text{model.inv} \circ \text{level1.encoding.get}_A) \ x \ \text{then level1.encoding.get}_A \ x \ \text{else } \text{level1.encoding.get}_A \ \text{endif}
\]

These two functions can also be understood as conversion between object types and universe types.

Analogous we define for the inherited class B:

\[
\text{encoding.mk}_B \equiv \lambda x. \text{if } B.\text{model.inv} \ x \ \text{then level1.encoding.mk}_B \ x \ \text{else level1.encoding.mk}_B \ \text{endif}
\]
encoding.get_B ::
(state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c) × 
state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c)
⇒ U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c)
⇒ state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c) × 
state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c)
⇒ OclAny_0 ((A_key × Integer_0) × ((B_key × oid) × 'a up) up)
encoding.get_B ≡
λx. if (B.model.inv o level1.encoding.get_B) x then level1.encoding.get_B x else ⊥endif

For converting along type hierarchies (i.e. down-casting and up-casting) we provide for each class two functions for the conversion to the direct predecessor and direct successor in the class hierarchy:

encoding.A_2_OclAny ::
(state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c) × 
state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c)
⇒ OclAny_0 ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up))
⇒ state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c) × 
state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c)
⇒ OclAny_0 ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c)
encoding.A_2_OclAny ≡ λx. if A.model.inv x then level1.encoding.A_2_OclAny x else ⊥endif

encoding.OclAny_2_A ::
(state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c) × 
state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c)
⇒ OclAny_0 ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c))
⇒ state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c) × 
state U ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up + 'c)
⇒ OclAny_0 ((A_key × Integer_0) × ((B_key × oid) × 'a up + 'b) up)
encoding.OclAny_2_A ≡ λx. if T then level1.encoding.OclAny_2_A x else ⊥endif
Appendix C. Encoding UML/ocl by Example

Analogous we define for the inherited class B:

\[
\text{encoding.B} = \lambda x. \begin{cases} \\
\text{if } \oplus \text{ then } \text{level.1} \text{encoding.B } \text{else } \text{endif} \\
\end{cases}
\]

Finally, we provide accessor functions for the class attributes:

\[
\text{encoding.A} = \lambda x. \begin{cases} \\
\text{if } \oplus \text{ then } \text{level.1} \text{encoding.A } \text{else } \text{endif} \\
\end{cases}
\]


**Defining oclAsType and allInstances**

The constants for `oclAsType` and `allInstances` must be defined for each class separately (using overloading). We provide for each class two definitions for `oclAsType`: one for the actual state (“UML_OCL.univ.encoding.A.OclAllInstancesencoding_A”)

\[ OclAllInstances ?self \equiv \lambda{s, s\prime}. \text{Abs}_0.\text{level}.\text{encoding}.\text{get} _A \cdot \text{ran} \; s\prime \]

and one for the previous state (“UML_OCL.univ.encoding.A.OclAllInstancesencoding_AAtpre”):

\[ OclAllInstancesAtpre ?self \equiv \lambda{s, s\prime}. \text{Abs}_0.\text{level}.\text{encoding}.\text{get} _A \cdot \text{ran} \; s_j \]

Analogous for class B we define “UML_OCL.univ.encoding.B.OclAllInstancesencoding_B”:

\[ OclAllInstances ?self \equiv \lambda{s, s\prime}. \text{Abs}_0.\text{level}.\text{encoding}.\text{get} _B \cdot \text{ran} \; s\prime \]

and “UML_OCL.univ.encoding.B.OclAllInstancesencoding_BAtpre”:

\[ OclAllInstancesAtpre ?self \equiv \lambda{s, s\prime}. \text{Abs}_0.\text{level}.\text{encoding}.\text{get} _B \cdot \text{ran} \; s_j \]

In a similar way, we have to overload the definition of `oclAsType`, based on the already defined conversion for adjacent classes. For class A the following cases must be considered along the inheritance hierarchy: The downcast from `OclAny` “UML_OCL.univ.encoding.A.from_OclAny”:

\[ OclAsType \equiv \lambda{self \cdot \text{cSet}}. \text{level}.\text{encoding}.\text{OclAny} _2 \cdot A \; \text{self} \]

the upcast to `OclAny` “UML_OCL.univ.encoding.A.to_OclAny”:

\[ OclAsType \equiv \lambda{self \cdot \text{cSet}}. \text{level}.\text{encoding}.\text{A} _2 \cdot \text{OclAny} \; \text{self} \]

467
Appendix C. Encoding UML/ocl by Example

and the identity “UML_OCL.univ.encoding.A to_A”:

\[ \text{OclAsType} \equiv \lambda self \; cSet. \; self \]

For class B more cases have to be considered, i.e., the downcast from A “UML_OCL.univ.encoding.B from_A”:

\[ \text{OclAsType} \equiv \lambda self \; cSet. \; \text{level1.encoding.A}_2 \_B \circ \text{level1.encoding.OclAny}_2 \_A \; self \]

the downcast from OclAny “UML_OCL.univ.encoding.B from_OclAny”:

\[ \text{OclAsType} \equiv \lambda self \; cSet. \; \text{level1.encoding.A}_2 \_\text{B} \; self \]

the upcast to OclAny “UML_OCL.univ.encoding.B to_OclAny”:

\[ \text{OclAsType} \equiv \lambda self \; cSet. \; \text{level1.encoding.B}_2 \_A \; self \]

and the identity “UML_OCL.univ.encoding.B to_B”:

\[ \text{OclAsType} \equiv \lambda self \; cSet. \; self \]

Optional, the encoder generates all definitions that are orthogonal to the class hierarchy. On the one hand, they are defined to be OclUndefined according to the OCL standard, on the other hand, they violate a well-formed constraint.

Encoding of OCL Invariants: Part Two

Finally, we generate the the final invariant, e.g., for class A we generate:

\[ \text{encoding.A.inv.init} _i ::
  \text{(state} \; U \; ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times (a \; \text{up} + b) \; \text{up} + c)) \times \text{state} \; U \; ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times (a \; \text{up} + b) \; \text{up} + c) \Rightarrow \text{OclAny}_0 \; ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times (a \; \text{up} + b) \; \text{up})) \Rightarrow \text{state} \; U \; ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times (a \; \text{up} + b) \; \text{up} + c)) \times \text{state} \; U \; ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times (a \; \text{up} + b) \; \text{up} + c) \Rightarrow \text{Boolean}_0 \]

\[ \text{inv.init}_i \equiv \lambda self. \; \text{OclIsNew self} \longrightarrow \text{encoding.A.i self} \triangleq 42 \]
and the second one describes the user defined invariant:

\[ encoding.A.inv \_1 :: \]
\[
(state \_U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times 'a up + 'b) up + 'c) \times
state \_U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times 'a up + 'b) up + 'c)
\Rightarrow OclAny\_0 ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times 'a up + 'b) up))
\Rightarrow state \_U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times 'a up + 'b) up + 'c) \times
state \_U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times 'a up + 'b) up + 'c)
\Rightarrow Boolean\_0
\]

\[ inv.inv \_1 \equiv \lambda self. encoding.A.i \ self > 0 \]

The overall invariant for class A is constructed by conjoining these invariants.

\[ encoding.A.inv :: \]
\[
(state \_U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times 'a up + 'b) up + 'c) \times
state \_U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times 'a up + 'b) up + 'c)
\Rightarrow OclAny\_0 ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times 'a up + 'b) up))
\Rightarrow state \_U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times 'a up + 'b) up + 'c) \times
state \_U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times 'a up + 'b) up + 'c)
\Rightarrow Boolean\_0
\]

\[ A.inv.inv \equiv \lambda obj. inv.init_i \ obj \land inv.inv \_1 \ obj \]

Analogous we are encoding the pre-condition and post-condition of the operation f:

\[ encoding.A.f \_Integer\_Integer.pre1.pre \_0 :: \]
\[
(state \_U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times 'a up + 'b) up + 'c) \times
state \_U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times 'a up + 'b) up + 'c)
\Rightarrow OclAny\_0 ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times 'a up + 'b) up))
\Rightarrow (state \_U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times 'a up + 'b) up + 'c) \times
state \_U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times 'a up + 'b) up + 'c)
\Rightarrow Integer\_0)
\Rightarrow state \_U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times 'a up + 'b) up + 'c) \times
state \_U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times 'a up + 'b) up + 'c)
\Rightarrow Boolean\_0
\]

\[ pre \_0 \equiv \lambda self \ x. x > 0 \]
Appendix C. Encoding UML/OCL by Example

encoding.A.f_Integer_Integer.post1.post_0 ::
  (state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \ ('a up + 'b) up + 'c)) \times
  state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \ ('a up + 'b) up + 'c)
  \Rightarrow OclAny_0 ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \ ('a up + 'b) up)))
  \Rightarrow (state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \ ('a up + 'b) up + 'c)) \times
  state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \ ('a up + 'b) up + 'c)
  \Rightarrow Integer_0)
  \Rightarrow (state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \ ('a up + 'b) up + 'c)) \times
  state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \ ('a up + 'b) up + 'c)
  \Rightarrow Integer_0)
  \Rightarrow state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \ ('a up + 'b) up + 'c)) \times
  state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \ ('a up + 'b) up + 'c)
  \Rightarrow Boolean_0)

post_0 \equiv \lambda self x. result. result \triangleq x \rightarrow div( level1.encoding.A.i self )\)

encoding.A.f_Integer_Integer.pre1 ::
  (state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \ ('a up + 'b) up + 'c)) \times
  state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \ ('a up + 'b) up + 'c)
  \Rightarrow OclAny_0 ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \ ('a up + 'b) up))
  \Rightarrow (state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \ ('a up + 'b) up + 'c)) \times
  state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \ ('a up + 'b) up + 'c)
  \Rightarrow Integer_0)
  \Rightarrow (state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \ ('a up + 'b) up + 'c)) \times
  state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \ ('a up + 'b) up + 'c)
  \Rightarrow Integer_0)
  \Rightarrow state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \ ('a up + 'b) up + 'c)) \times
  state U ((A\_key \times Integer\_0) \times ((B\_key \times oid) \times \ ('a up + 'b) up + 'c)
  \Rightarrow Boolean_0)

pre1 \equiv pre_0

470
C.3. Importing UML/OC
cmodels

encoding.A.f_IntegerInteger.post1 ::
  (state U ((A_key x Integer_0) x (B_key x oid) x 'a up + 'b) up + 'c) x
  state U ((A_key x Integer_0) x (B_key x oid) x 'a up + 'b) up + 'c)
⇒ OclAny_0 ((A_key x Integer_0) x ((B_key x oid) x 'a up + 'b) up))
⇒ (state U ((A_key x Integer_0) x (B_key x oid) x 'a up + 'b) up + 'c) x
  state U ((A_key x Integer_0) x ((B_key x oid) x 'a up + 'b) up + 'c)
⇒ Integer_0
⇒ (state U ((A_key x Integer_0) x ((B_key x oid) x 'a up + 'b) up + 'c) x
  state U ((A_key x Integer_0) x ((B_key x oid) x 'a up + 'b) up + 'c)
⇒ Integer_0)
⇒ state U ((A_key x Integer_0) x ((B_key x oid) x 'a up + 'b) up + 'c) x
  state U ((A_key x Integer_0) x ((B_key x oid) x 'a up + 'b) up + 'c)
⇒ Boolean_0

post1 ≡ post_0

For class B no initial values or invariants are given, thus we generate invariants that are just true:

encoding.B.inv.init_j ::
  (state U ((A_key x Integer_0) x (B_key x oid) x 'a up + 'b) up + 'c) x
  state U ((A_key x Integer_0) x (B_key x oid) x 'a up + 'b) up + 'c)
⇒ OclAny_0 ((A_key x Integer_0) x ((B_key x oid) x 'a up) up))
⇒ state U ((A_key x Integer_0) x ((B_key x oid) x 'a up + 'b) up + 'c) x
  state U ((A_key x Integer_0) x ((B_key x oid) x 'a up + 'b) up + 'c)
⇒ Boolean_0

inv.init_j ≡ λself. T

encoding.B.inv.init_j ::
  (state U ((A_key x Integer_0) x (B_key x oid) x 'a up + 'b) up + 'c) x
  state U ((A_key x Integer_0) x (B_key x oid) x 'a up + 'b) up + 'c)
⇒ OclAny_0 ((A_key x Integer_0) x ((B_key x oid) x 'a up) up))
⇒ state U ((A_key x Integer_0) x ((B_key x oid) x 'a up + 'b) up + 'c) x
  state U ((A_key x Integer_0) x ((B_key x oid) x 'a up + 'b) up + 'c)
⇒ Boolean_0

inv.init_j ≡ λself. T
Appendix C. Encoding UML/ocl by Example

The overall invariant for class B is constructed by conjoining these invariants.

\[
\text{encoding.} \ B.\text{inv.inv} ::
\]
\[
\text{state } U \ ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times \text{'}a \text{ up } \text{'}b \text{ up } \text{'}c) \times \\
\text{state } U \ ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times \text{'}a \text{ up } \text{'}b \text{ up } \text{'}c) \\
\Rightarrow \text{OclAny}_0 \ ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times \text{'}a \text{ up} \text{'}b) \text{ up} + \text{'}c) \\
\Rightarrow \text{state } U \ ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times \text{'}a \text{ up } \text{'}b \text{ up } \text{'}c) \times \\
\text{state } U \ ((A\_key \times \text{Integer}_0) \times ((B\_key \times \text{oid}) \times \text{'}a \text{ up } \text{'}b \text{ up } \text{'}c) \\
\Rightarrow \text{Boolean}_0
\]

\[B.\text{inv.inv} \equiv \text{inv.init}_j\]
Appendix D.

The GNU General Public Licence

The following is the text of the GNU General Public Licence, under the terms of which this software is distributed.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
675 Mass Ave, Cambridge, MA 02139, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

D.1. Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation’s software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.
Appendix D. The GNU General Public Licence

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author’s protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors’ reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone’s free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

D.2. Terms and conditions for copying, distribution and modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program”, below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you”.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program’s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

474
D.2. Terms and conditions for copying, distribution and modification

(a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

(b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

(c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

(a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

(b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding
Appendix D. The GNU General Public Licence

source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

(c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients’ exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you
D.2. Terms and conditions for copying, distribution and modification

(whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision
Appendix D. The GNU General Public Licence

will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. Because the Program is licensed free of charge, there is no warranty for the Program, to the extent permitted by applicable law. except when otherwise stated in writing the copyright holders and/or other parties provide the program “as is” without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the quality and performance of the Program is with you. Should the Program prove defective, you assume the cost of all necessary servicing, repair or correction.

12. In no event unless required by applicable law or agreed to in writing will any copyright holder, or any other party who may modify and/or redistribute the program as permitted above, be liable to you for damages, including any general, special, incidental or consequential damages arising out of the use or inability to use the program (including but not limited to loss of data or data being rendered inaccurate or losses sustained by you or third parties or a failure of the Program to operate with any other programs), even if such holder or other party has been advised of the possibility of such damages.

END OF TERMS AND CONDITIONS

D.3. Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program’s name and a brief idea of what it does.>
Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or...
D.3. Appendix: How to Apply These Terms to Your New Programs

(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Also add information on how to contact you by electronic and paper mail.
If the program is interactive, make it output a short notice like this when it starts
in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate
parts of the General Public License. Of course, the commands you use may be called
something other than 'show w' and 'show c'; they could even be mouse-clicks or menu
items—whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if
any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample;
alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into pro-
netary programs. If your program is a subroutine library, you may consider it more
useful to permit linking proprietary applications with the library. If this is what you
want to do, use the GNU Library General Public License instead of this License.
Appendix D. The GNU General Public Licence
Part V.

Bibliography and Index
Bibliography


[3] Isabelle. URL http://isabelle.in.tum.de (Cited on pages 12 and 91.)


Bibliography


Bibliography


486
Bibliography


Bibliography
List of Acronyms

ACI  Associativity, commutativity, and idempotency
CASE  Computer Aided Software Engineering
CCS  A Calculus of Communicating Systems
CTL  Computational Tree Logic
CSP  Communicating Sequential Processes
DNF  disjunctive normal form
ETH  Swiss Federal Institute of Technology
EBNF  Extended Backus-Naur Form
FXP  Functional XML Parser
GNU  GNU is not Unix
GUI  Graphical User Interface
HOAS  higher-order abstract syntax
HOL  higher-order logic
Isar  Intelligible semi-automated reasoning
LCF  Logic for Computable Functions
LE  Local (Formula) Equivalence
LJE  Local Judgement Equivalence
LTL  Linear Temporal Logic
LTC  Local Judgement Tableaux Calculus
OCL  Object Constraint Language
OMG  Object Management Group
SKL  Strong Kleene Logic
SML  Standard Meta Language
### Bibliography

- **sml/NJ**: SML of New Jersey
- **su4sml**: SecureUML for SML
- **UC**: Universal (Formula) Congruence
- **UJE**: Universal Judgement Equivalence
- **UML**: Unified Modelling Language
- **VDM**: Vienna Definition Method
- **XMI**: XML Metadata Interchange
- **XML**: Extensible Markup Language
- **ZF**: Zermelo-Fränkel
- **ZFC**: Zermelo-Fränkel set theory with the axiom of choice.
List of Glitches

The formal semantics of \texttt{implies} does not satisfy its requirements. \footnote{42}
Underspecification of Overload-Resolution \footnote{47}
referential vs. non-referential universe construction \footnote{52}
Underspecification of Recursion \footnote{68}
\texttt{self.OclsNew()} ill-defined \footnote{74}
The truth for \texttt{implies} does not fulfill the normative requirement. \footnote{177}
Definition for \texttt{implies} inappropriate \footnote{192}
Typo in requirement 11.7.5.10, \footnote{291}
No specification of the returned index of \texttt{indexOf}, \footnote{291}
\texttt{sum} \footnote{367}
Wrong definition of the correspondence of includesAll and iterate \footnote{413}
Wrong definition of the correspondence of excludesAll and iterate \footnote{414}
no preconditions about range of index. But they are surely needed because of the correspondence to \texttt{at()}, \footnote{426}
the valid range must be from \texttt{index} to \texttt{self->size()} \footnote{426}
Bibliography
List of Extensions

late-binding invocation, 47
Characteristic Type Sets, 64
infinite set, 64
typeSetOf(), 64
kindSetOf(), 64
late-binding invocation, 65
strong (≜) and strict (=) referential equality, 74
strong (≃) and strict (˙≃) shallow value equality, 74
->modifiedOnly(), 75
## List of Figures

2.1. Modeling a simple banking scenario with UML ........................................... 21  
4.1. An High-Level Overview of the HOL-OCL Embedding Architecture ............ 37  
4.2. Derivation of the OCL-library ............................................................ 44  
4.3. Extending Class Hierarchies and Universes with Holes ......................... 50  
4.4. Modelling Directed Graphs: Data Model ................................................. 53  
4.5. The Relation Between Type Casts and Injections and Projections ............ 59  
6.1. Overview of the HOL-OCL architecture ................................................ 98  
7.1. Overview of the High-level System Architecture of HOL-OCL ................. 107  
7.2. A HOL-OCL session Using the Isar Interface of Isabelle .......................... 111  
9.1. The HOL-OCL Workflow ........................................................................ 118  
9.2. Using ArgoUML for Data Modelling ........................................................ 118  
9.3. Using the Dresden OCL Parser and Type-checker ..................................... 120  
10.1. Modelling a Stack: Data Model ............................................................. 125  
B.1. Session Graph ......................................................................................... 136  
C.1. A simple Encoding Example: Data Model .............................................. 440
List of Figures
List of Tables

3.1. Comparing Logical Embeddings .............................................. 32
4.1. Equalities in an Object-oriented Setting ............................ 74
4.2. Comparing Equalities (non-referential universe) .............. 74
4.3. Comparing Equalities (referential universe) ..................... 75
5.1. The Context Passing Side-Calculus (Excerpt) .................... 81
5.2. The Definedness Calculi ..................................................... 83
5.3. The \texttt{UC} Core-Calculus (“Propositional Calculus”) ....... 86
5.4. The OCL to HOL Conversion Rules .................................... 91
5.5. The Core of LEC ............................................................. 92
A.1. Formal Grammar of OCL (fragment) ................................. 130
A.2. Comparison of different concrete syntax variants for OCL .... 131
B.1. Comparison of the formal syntax and the Isabelle syntax .... 138
List of Definitions

4.1. Attribute Types ................................................. 54
4.2. Tag Types ..................................................... 54
4.3. Base Class Types .............................................. 54
4.4. OclAny ......................................................... 55
4.5. Universe Types ............................................... 55
4.6. Referential Universe Types .................................. 55
4.7. Non-Referential Universe Types .............................. 56
4.8. Class Type ...................................................... 56
4.9. Finite Constant Definition Family ............................ 67
4.10. Value Types .................................................. 71
4.11. Values ......................................................... 71
4.12. Equivalence Relation ........................................ 71
4.13. Reference Equality .......................................... 71
4.14. Shallow Value Equality ...................................... 71
4.15. Deep Value Equality ........................................ 72
4.16. Equivalence Operators ...................................... 72
4.17. Strong Equality .............................................. 73
4.18. Strict Equality ................................................ 73
List of Tables
## Listings

<table>
<thead>
<tr>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1. su4sml: Representing OCL types</td>
</tr>
<tr>
<td>6.2. su4sml: Representing OCL expressions</td>
</tr>
<tr>
<td>6.3. su4sml: Representing the UML core</td>
</tr>
<tr>
<td>6.4. The Top-level Interface of the Repository Encoder</td>
</tr>
<tr>
<td>6.5. Proving Cast and Re-Cast (simplified)</td>
</tr>
<tr>
<td>9.1. A OCL Specification (Excerpt of the Royals and Loyals Model)</td>
</tr>
<tr>
<td>9.2. A simple HOL-OCL Theory File</td>
</tr>
<tr>
<td>10.1. Modelling a Stack: OCL specification</td>
</tr>
<tr>
<td>C.1. A simple Encoding Example: OCL specification</td>
</tr>
</tbody>
</table>
Index

symbols
V_r(α), 38
sml/NJ, 107

A
abstraction, 17
activity charts, 12
activity diagram, 20
application, 17
association, 20
attribute, 20
attribute type, 54

B
base class type, 54

C
catch-all rule, 67
characteristic set, 87
⟨clasimpmod⟩, 123
class, 20
class diagram, 20, 39, 43, 49, 51
class diagram extension, 50
class diagrams, 12
class type, 51, 56, 168
compliance, 39, 40, 45
comprehensions, 85
computational rules, 40
conformance, 49
congruence, 78
conservative theory extension, 18
conservative type definition, 46
consistent OCL specification, 48
constant definition, 18, 39, 40, 44–46
constant specification, 18
context, 30, 35, 42
context lifting, 30, 38
context passing, 38, 173
core-logic, 85

D
datatype adaption, 36, 45
definedness, 78
derivation tree, 19

equality
  referential, 71
  strict, 79
  strong, 73
  value
    deep, 72
    shallow, 71
equality operators, 73
equivalence, 78
  equivalence operator, 72
  equivalence relation, 71

F
finalized, 67
formal methods, 11, 13
formality, 11
functional adaption, 36, 46

G
global validity judgement, 77
goal, 19

H
Haskell, 17
higher-order logic, see HOL
HOL, 17
INDEX

I
implication introduction, 19
inheritance, 20, 35, 49, 50
invariant, 36
Isabelle, 19, 107

K
Kleene Logic, 42
Kleene-Logic, 173

L
late-binding invocation, 46
layer, 36, 43
level, 36
lifting, 138
lifting over contexts, 38, 39, 48
Local (Formula) Equivalence, 79
Local Judgement Equivalence, 79
local judgement tableaux calculus, 80
local validity judgements, 77
logical judgement, 61, 73

M
Main (theory), 121
meta-implication, 19
meta-models, 12
meta-quantifier, 19
meta-variable, 19
method invocation, 47
methods, 35
model-based testing, 11
model-checking, 11
modularity, 30

N
natural deduction rules, 19
non-referential, 135
notation τ⊥, 38
notation Vτ(α), 30

O
object, 51
instance, 51
object diagram, 20
object id, 49
object instances, 20
object structure, 35
object-orientation, 65
object-oriented, 20, 30
object-type system, 30
OCL (theory), 121
OclAny, 55
operation, 20, 29, 35, 36
operation invocation, 47
operation specification, 30, 35, 47, 64
overriding, 20

P
partial map, 66
Poly/ML, 107
postcondition, 29, 36, 65
precondition, 29, 36, 65
Proof General, 107
proof state, 19
proof-object, 19
propositional fragment, 85

R
reference types, 52
referential, 135

S
semantic combinator, 44–50
semantic combinators, 44
sequence charts, 12
set constructors, 87
side-calculus, 30, 38
smashed, 95, 137
smashing, 138
SML, 17
specialization, 20
splintering, 95
splinters, 95
Standard ML, see SML
state, 29, 49
state chart, 20
state charts, 12
state diagram, 30
state transition, 29, 49
static types, 30
strict, 39

503
INDEX

strictification, 46
strictness, 37, 40, 139
subgoal, 19
subtyping, 20, 49

T
tactics, 19
tag type, 54
theorem proving, 11
theory, 135
theory file, 17
theory morphism, 43
totalized operation specification, 66
type class, 17
type constructor, 17, 31
type definition, 18
type specification, 18
type variables, 17
type-checking, 11
types, 46

U
UML_OCL (theory), 121
undefined, 36, 37, 39, 138
undefinedness, 78, 138
undefinedness lifting, 38, 39
Universal (Formula) Congruence, 79
Universal Judgement Equivalence, 79
universal validity judgement, 77
universe
    non-referential, 52
    referential, 52
universe type, 55
    non-referential, 56
    referential type, 55
universe types, 168
unsmashed, 137

V
validation, 11
value, 71
value type, 51, 71
value types, 168

504