Featherweight OCL

A Proposal for a Machine-Checked Formal Semantics for OCL 2.5

Achim D. Brucker†‡ Frédéric Tuong†‡ Burkhart Wolff†‡

June 11, 2019

*SAP SE
Vincenz-Priessnitz-Str. 1, 76131 Karlsruhe, Germany
achim.brucker@sap.com

†LRI, Univ. Paris-Sud, CNRS, CentraleSupélec, Université Paris-Saclay
bât. 650 Ada Lovelace, 91405 Orsay, France
fréderic.tuong@lri.fr burkhart.wolff@lri.fr

‡IRT SystemX
8 av. de la Vauve, 91120 Palaiseau, France
fréderic.tuong@irt-systemx.fr burkhart.wolff@irt-systemx.fr
Abstract

The Unified Modeling Language (UML) is one of the few modeling languages that is widely used in industry. While UML is mostly known as diagrammatic modeling language (e.g., visualizing class models), it is complemented by a textual language, called Object Constraint Language (OCL). OCL is a textual annotation language, originally based on a three-valued logic, that turns UML into a formal language. Unfortunately the semantics of this specification language, captured in the “Annex A” of the OCL standard, leads to different interpretations of corner cases. Many of these corner cases had been subject to formal analysis since more than ten years.

The situation complicated with the arrival of version 2.3 of the OCL standard. OCL was aligned with the latest version of UML; this led to the extension of the three-valued logic by a second exception element, called null. While the first exception element invalid has a strict semantics, null has a non strict interpretation. The combination of these semantic features lead to remarkable confusion for implementors of OCL compilers and interpreters.

In this paper, we provide a formalization of the core of OCL in HOL. It provides denotational definitions, a logical calculus and operational rules that allow for the execution of OCL expressions by a mixture of term rewriting and code compilation. Moreover, we describe a coding-scheme for UML class models that were annotated by code-invariants and code contracts. An implementation of this coding-scheme has been undertaken: it consists of a kind of compiler that takes a UML class model and translates it into a family of definitions and derived theorems over them capturing the properties of constructors and selectors, tests and casts resulting from the class model. However, this compiler is not included in this document.

Our formalization reveals several inconsistencies and contradictions in the current version of the OCL standard. They reflect a challenge to define and implement OCL tools in a uniform manner. Overall, this document is intended to provide the basis for a machine-checked text “Annex A” of the OCL standard targeting at tool implementors.
I. Formal Semantics of OCL

0.1. Introduction

0.2. Background

0.2.1. A Running Example for UML/OCL

0.2.2. Formal Foundation

0.2.3. How this Annex A was Generated from Isabelle/HOL Theories

0.3. The Essence of UML-OCL Semantics

1. Formalization I: OCL Types and Core Definitions

1.1. Preliminaries

1.1.1. Notations for the Option Type

1.1.2. Common Infrastructure for all OCL Types

1.1.3. Accommodation of Basic Types to the Abstract Interface

1.1.4. The Common Infrastructure of Object Types (Class Types) and States

1.1.5. Common Infrastructure for all OCL Types (II): Valuations as OCL Types

1.1.6. The fundamental constants ‘invalid’ and ‘null’ in all OCL Types

1.2. Basic OCL Value Types

1.3. Some OCL Collection Types

2. Formalization II: OCL Terms and Library Operations

2.1. The Operations of the Boolean Type and the OCL Logic

2.1.1. Basic Constants

2.1.2. Validity and Definedness

2.1.3. The Equalities of OCL Definition
Definition: First ................................................. 81
Definition: Second ........................................... 81
2.7.4. Logical Properties ........................................ 81
2.7.5. Algebraic Execution Properties ......................... 82
2.7.6. Test Statements ........................................... 82
2.8. Collection Type Bag: Operations ......................... 82
2.8.1. As a Motivation for the (infinite) Type Construction: Type-Extensions as Bags 83
2.8.2. Basic Properties of the Bag Type ....................... 84
2.8.3. Definition: Strict Equality .............................. 85
2.8.4. Constants: mtBag ......................................... 85
2.8.5. Definition: Including ...................................... 85
2.8.6. Definition: Excluding ...................................... 86
2.8.7. Definition: Includes ........................................ 86
2.8.8. Definition: Excludes ....................................... 86
2.8.9. Definition: Size ............................................ 86
2.8.10. Definition: IsEmpty ......................................... 87
2.8.11. Definition: NotEmpty ...................................... 87
2.8.12. Definition: Any ............................................ 87
2.8.13. Definition: Forall ......................................... 87
2.8.14. Definition: Exists ......................................... 87
2.8.15. Definition: Iterate ....................................... 88
2.8.16. Definition: Select ......................................... 88
2.8.17. Definition: Reject ......................................... 88
2.8.18. Definition: IncludesAll ................................... 88
2.8.19. Definition: ExcludesAll ................................. 88
2.8.20. Definition: Union .......................................... 89
2.8.21. Definition: Intersection ................................. 89
2.8.22. Definition: Count ......................................... 89
2.8.23. Definition (future operators) ......................... 89
2.8.24. Logical Properties ........................................ 89
2.8.25. Execution Laws with Invalid or Null or Infinite Set as Argument ..................... 91
Context Passing ................................................ 93
Const .......................................................... 94
2.8.26. Test Statements ........................................... 94
2.9. Collection Type Set: Operations ......................... 95
2.9.1. As a Motivation for the (infinite) Type Construction: Type-Extensions as Sets 95
2.9.2. Basic Properties of the Set Type ....................... 96
2.9.3. Definition: Strict Equality ................................ 97
2.9.4. Constants: mtSet ........................................... 97
2.9.5. Definition: Including ....................................... 98
2.9.6. Definition: Excluding ....................................... 98
2.9.7. Definition: Includes ........................................ 98
2.9.8. Definition: Excludes ....................................... 98
2.9.9. Definition: Size ............................................ 99
2.9.10. Definition: IsEmpty ......................................... 99
2.9.11. Definition: NotEmpty ...................................... 99
2.9.12. Definition: Any ............................................ 99
2.9.13. Definition: Forall ......................................... 99
2.9.14. Definition: Exists ......................................... 100
2.9.15. Definition: Iterate ....................................... 100
2.9.16. Definition: Select ......................................... 100
2.9.17. Definition: Reject ......................................... 100
2.9.18. Definition: IncludesAll ................................. 100
2.11. Miscellaneous Stuff

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.11.1.</td>
<td>Definition: asBoolean</td>
<td>121</td>
</tr>
<tr>
<td>2.11.2.</td>
<td>Definition: asInteger</td>
<td>122</td>
</tr>
<tr>
<td>2.11.3.</td>
<td>Definition: asReal</td>
<td>122</td>
</tr>
<tr>
<td>2.11.4.</td>
<td>Definition: asPair</td>
<td>122</td>
</tr>
<tr>
<td>2.11.5.</td>
<td>Definition: asSet</td>
<td>122</td>
</tr>
<tr>
<td>2.11.6.</td>
<td>Definition: asSequence</td>
<td>123</td>
</tr>
<tr>
<td>2.11.7.</td>
<td>Definition: asBag</td>
<td>123</td>
</tr>
<tr>
<td>2.11.8.</td>
<td>Collection Types</td>
<td>123</td>
</tr>
<tr>
<td>2.11.9.</td>
<td>Test Statements</td>
<td>123</td>
</tr>
</tbody>
</table>

3. Formalization III: UML/OCL constructs: State Operations and Objects

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.</td>
<td>Introduction: States over Typed Object Universes</td>
<td>125</td>
</tr>
<tr>
<td>3.1.1.</td>
<td>Fundamental Properties on Objects: Core Referential Equality</td>
<td>125</td>
</tr>
<tr>
<td></td>
<td>Definition</td>
<td>125</td>
</tr>
<tr>
<td></td>
<td>Strictness and context passing</td>
<td>125</td>
</tr>
<tr>
<td>3.1.2.</td>
<td>Logic and Algebraic Layer on Object</td>
<td>126</td>
</tr>
<tr>
<td></td>
<td>Validity and Definedness Properties</td>
<td>126</td>
</tr>
<tr>
<td></td>
<td>Symmetry</td>
<td>126</td>
</tr>
<tr>
<td></td>
<td>Behavior vs StrongEq</td>
<td>126</td>
</tr>
<tr>
<td>3.2.</td>
<td>Operations on Object</td>
<td>127</td>
</tr>
<tr>
<td>3.2.1.</td>
<td>Initial States (for testing and code generation)</td>
<td>127</td>
</tr>
<tr>
<td>3.2.2.</td>
<td>OclAllInstances</td>
<td>127</td>
</tr>
<tr>
<td></td>
<td>OclAllInstances (@post)</td>
<td>129</td>
</tr>
<tr>
<td></td>
<td>OclAllInstances (@pre)</td>
<td>131</td>
</tr>
<tr>
<td></td>
<td>@post or @pre</td>
<td>132</td>
</tr>
<tr>
<td>3.2.3.</td>
<td>OclIsNew, OclIsDeleted, OclIsMaintained, OclIsAbsent</td>
<td>132</td>
</tr>
<tr>
<td>3.2.4.</td>
<td>OclIsModifiedOnly</td>
<td>133</td>
</tr>
<tr>
<td></td>
<td>Definition</td>
<td>133</td>
</tr>
<tr>
<td></td>
<td>Execution with Invalid or Null as Argument</td>
<td>133</td>
</tr>
<tr>
<td></td>
<td>Context Passing</td>
<td>134</td>
</tr>
<tr>
<td>3.2.5.</td>
<td>OclSelf</td>
<td>134</td>
</tr>
<tr>
<td>3.2.6.</td>
<td>Framing Theorem</td>
<td>134</td>
</tr>
<tr>
<td>3.2.7.</td>
<td>Miscellaneous</td>
<td>135</td>
</tr>
<tr>
<td>3.3.</td>
<td>Accessors on Object</td>
<td>135</td>
</tr>
<tr>
<td>3.3.1.</td>
<td>Definition</td>
<td>135</td>
</tr>
<tr>
<td></td>
<td>Validity and Definedness Properties</td>
<td>135</td>
</tr>
</tbody>
</table>

4. Example: The Employee Analysis Model

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.</td>
<td>Introduction</td>
<td>145</td>
</tr>
<tr>
<td>4.1.1.</td>
<td>Outlining the Example</td>
<td>145</td>
</tr>
<tr>
<td>4.2.</td>
<td>Example Data-Universe and its Infrastructure</td>
<td>146</td>
</tr>
<tr>
<td>4.3.</td>
<td>Instantiation of the Generic Strict Equality</td>
<td>147</td>
</tr>
<tr>
<td>4.4.</td>
<td>OclAsType</td>
<td>147</td>
</tr>
<tr>
<td>4.4.1.</td>
<td>Definition</td>
<td>147</td>
</tr>
<tr>
<td>4.4.2.</td>
<td>Context Passing</td>
<td>148</td>
</tr>
<tr>
<td>4.4.3.</td>
<td>Execution with Invalid or Null as Argument</td>
<td>149</td>
</tr>
<tr>
<td>4.5.</td>
<td>OclIsTypeOf</td>
<td>149</td>
</tr>
<tr>
<td>4.5.1.</td>
<td>Definition</td>
<td>149</td>
</tr>
<tr>
<td>4.5.2.</td>
<td>Context Passing</td>
<td>150</td>
</tr>
<tr>
<td>4.5.3.</td>
<td>Execution with Invalid or Null as Argument</td>
<td>151</td>
</tr>
<tr>
<td>4.5.4.</td>
<td>Up Down Casting</td>
<td>151</td>
</tr>
</tbody>
</table>
4.6. **OclIsKindOf** 152

4.6.1. **Definition** 152
4.6.2. **Context Passing** 153
4.6.3. **Execution with Invalid or Null as Argument** 153
4.6.4. **Up Down Casting** 153

4.7. **OclAllInstances** 154

4.7.1. **OclIsTypeOf** 154
4.7.2. **OclIsKindOf** 155

4.8. **The Accessors (any, boss, salary)** 155

4.8.1. **Definition (of the association Employee-Boss)** 156
4.8.2. **Context Passing** 158
4.8.3. **Execution with Invalid or Null as Argument** 158
4.8.4. **Representation in States** 159

4.9. **A Little Infrastructure on Example States** 159

4.10. **OCL Part: Invariant** 163

4.11. **OCL Part: The Contract of a Recursive Query** 165


5. **Example: The Employee Design Model** 169

5.1. **Introduction** 169

5.1.1. **Outlining the Example** 169

5.2. **Example Data-Universe and its Infrastructure** 169

5.3. **Instantiation of the Generic Strict Equality** 170

5.4. **OclAsType** 171

5.4.1. **Definition** 171
5.4.2. **Context Passing** 172
5.4.3. **Execution with Invalid or Null as Argument** 173

5.5. **OclIsTypeOf** 173

5.5.1. **Definition** 173
5.5.2. **Context Passing** 174
5.5.3. **Execution with Invalid or Null as Argument** 175
5.5.4. **Up Down Casting** 175

5.6. **OclIsKindOf** 176

5.6.1. **Definition** 176
5.6.2. **Context Passing** 177
5.6.3. **Execution with Invalid or Null as Argument** 177
5.6.4. **Up Down Casting** 177

5.7. **OclAllInstances** 178

5.7.1. **OclIsTypeOf** 178
5.7.2. **OclIsKindOf** 179

5.8. **The Accessors (any, boss, salary)** 179

5.8.1. **Definition** 179
5.8.2. **Context Passing** 181
5.8.3. **Execution with Invalid or Null as Argument** 182
5.8.4. **Representation in States** 182

5.9. **A Little Infrastructure on Example States** 183

5.10. **OCL Part: Invariant** 187

5.11. **OCL Part: The Contract of a Recursive Query** 188
II. Conclusion

6. Conclusion

6.1. Lessons Learned and Contributions

6.2. Lessons Learned

6.3. Conclusion and Future Work

III. Appendix

A. The OCL And Featherweight OCL Syntax
Part I.

Formal Semantics of OCL
0.1. Introduction

The Unified Modeling Language (UML) \[30, 31\] is one of the few modeling languages that is widely used in industry. UML is defined in an open process by the Object Management Group (OMG), i.e., an industry consortium. While UML is mostly known as diagrammatic modeling language (e.g., visualizing class models), it also comprises a textual language, called Object Constraint Language (OCL) \[32\]. OCL is a textual annotation language, originally conceived as a three-valued logic, that turns substantial parts of UML into a formal language. Unfortunately the semantics of this specification language, captured in the “Annex A” (originally based on the work of Richters \[33\]) of the OCL standard leads to different interpretations of corner cases. Many of these corner cases had been subject to formal analysis since more than nearly fifteen years (see, e.g., \[5, 10, 18, 22, 26\]).

At its origins \[28, 33\], OCL was conceived as a strict semantics for undefinedness (e.g., denoted by the element invalid\(^1\)), with the exception of the logical connectives of type Boolean that constitute a three-valued propositional logic. At its core, OCL comprises four layers:

1. Operators (e.g., _ and _ , _ + _) on built-in data structures such as Boolean, Integer, or typed sets (Set(_)).
2. Operators on the user-defined data model (e.g., defined as part of a UML class model) such as accessors, type casts and tests.
3. Arbitrary, user-defined, side-effect-free methods called queries,
4. Specification for invariants on states and contracts for operations to be specified via pre- and post-conditions.

Motivated by the need for aligning OCL closer with UML, recent versions of the OCL standard \[29, 32\] added a second exception element. While the first exception element invalid has a strict semantics, null has a non strict semantic interpretation. Unfortunately, this extension results in several inconsistencies and contradictions. These problems are reflected in difficulties to define interpreters, code-generators, specification animators or theorem provers for OCL in a uniform manner and resulting incompatibilities of various tools.

For the OCL community, the semantics of invalid and null as well as many related issues resulted in the challenge to define a consistent version of the OCL standard that is well aligned with the recent developments of the UML. A syntactical and semantical consistent standard requires a major revision of both the informal and formal parts of the standard. To discuss the future directions of the standard, several OCL experts met in November 2013 in Aachen to discuss possible mid-term improvements of OCL, strategies of standardization of OCL within the OMG, and a vision for possible long-term developments of the language \[14\]. During this meeting, a Request for Proposals (RFP) for OCL 2.5 was finalized and meanwhile proposed. In particular, this RFP requires that the future OCL 2.5 standard document shall be generated from a machine-checked source. This will ensure

- the absence of syntax errors,
- the consistency of the formal semantics,
- a suite of corner-cases relevant for OCL tool implementors.

In this document, we present a formalization using Isabelle/HOL \[27\] of a core language of OCL. The semantic theory, based on a “shallow embedding”, is called Featherweight OCL, since it focuses on a formal treatment of the key-elements of the language (rather than a full treatment of all operators and thus, a “complete” implementation). In contrast to full OCL, it comprises just the logic captured in Boolean, the basic data types Integer, Real and String, the collection types Set, Sequence and Bag, as well as the generic construction principle of class models, which is instantiated and demonstrated for two examples (an automated construction support for this type-safe construction is out of the scope of Featherweight

\(^1\)In earlier versions of the OCL standard, this element was called OclUndefined.
OCL). This formal semantics definition is intended to be a proposal for the standardization process of OCL 2.5, which should ultimately replace parts of the mandatory part of the standard document [32] as well as replace completely its informative “Annex A.”

The semantic definitions are in large parts executable, in some parts only provable, namely the essence of Set-and Bag-constructions. The first goal of its construction is consistency, i.e., it should be possible to apply logical rules and/or evaluation rules for OCL in an arbitrary manner always yielding the same result. Moreover, except in pathological cases, this result should be unambiguously defined, i.e., represent a value.

To motivate the need for logical consistency and also the magnitude of the problem, we focus on one particular feature of the language as example: Tuples. Recall that tuples (in other languages known as records) are n-ary Cartesian products with named components, where the component names are used also as projection functions: the special case Pair{x:First, y:Second} stands for the usual binary pairing operator Pair{true,null} and the two projection functions x.First() and x.Second(). For a developer of a compiler or proof-tool (based on, say, a connection to an SMT solver designed to animate OCL contracts) it would be natural to add the rules Pair(X,Y).First() = X and Pair(X,Y).Second() = Y to give pairings the usual semantics. At some place, the OCL Standard requires the existence of a constant symbol invalid and requires all operators to be strict. To implement this, the developer might be tempted to add a generator for corresponding strictness axioms, producing among hundreds of other rules Pair{invalid,Y}=invalid, invalid.First()=invalid, invalid.Second()=invalid, etc. Unfortunately, this “natural” axiomatization of pairing and projection together with strictness is already inconsistent. One can derive:

\[
\text{Pair\{true,invalid\}.First()} = \text{invalid.}\text{First()} = \text{invalid}
\]

and:

\[
\text{Pair\{true,invalid\}.First()} = \text{true}
\]

which then results in the absurd logical consequence that invalid = true. Obviously, we need to be more careful on the side-conditions of our rules. And obviously, only a mechanized check of these definitions, following a rigorous methodology, can establish strong guarantees for logical consistency of the OCL language.

This leads us to our second goal of this document: it should not only be usable by logicians, but also by developers of compilers and proof-tools. For this end, we derived from the Isabelle definitions also logical rules allowing formal interactive and automated proofs on UML/OCL specifications, as well as execution rules and test-cases revealing corner-cases resulting from this semantics which give vital information for the implementor.

OCL is an annotation language for UML models, in particular class models allowing for specifying data and operations on them. As such, it is a typed object-oriented language. This means that it is—like Java or C++—based on the concept of a static type, that is the type that the type-checker infers from a UML class model and its OCL annotation, as well as a dynamic type, that is the type at which an object is dynamically created. Types are not only a means for efficient compilation and a support of separation of concerns in programming, there are of fundamental importance for our goal of logical consistency: it is impossible to have sets that contain themselves, i.e., to state Russel’s Paradox in OCL typed set-theory. Moreover, object-oriented typing means that types there can be in sub-typing relation; technically speaking, this means that they can be cast via oclIsTypeOf(T) one to the other, and under particular conditions to be described in detail later, these casts are semantically lossless, i.e.,

\[
(X.oclAsType(C_j).oclAsType(C_i) = X)
\]  

(0.1)

(where \(C_j\) and \(C_i\) are class types.) Furthermore, object-oriented means that operations and object-types can be grouped to classes on which an inheritance relation can be established; the latter induces a sub-type relation between the corresponding types.

---

2The solution to this little riddle can be found in Section 2.7.

3As side-effect free language, OCL has no object-constructors, but with OclIsNew(), the effect of object creation can be expressed in a declarative way.
Here is a feature-list of Featherweight OCL:

- it specifies key built-in types such as Boolean, Void, Integer, Real and String as well as generic types such as Pair(T,T'), Sequence(T) and Set(T).
- it defines the semantics of the operations of these types in denotational form—see explanation below—, and thus in an unambiguous (and in Isabelle/HOL executable or animatable) way.
- it develops the theory of these definitions, i.e., the collection of lemmas and theorems that can be proven from these definitions.
- all types in Featherweight OCL contain the elements null and invalid; since this extends to Boolean type, this results in a four-valued logic. Consequently, Featherweight OCL contains the derivation of the logic of OCL.
- collection types may contain null (so Set{null} is a defined set) but not invalid (Set{invalid} is just invalid).
- Wrt. to the static types, Featherweight OCL is a strongly typed language in the Hindley-Milner tradition. We assume that a pre-process for full OCL eliminates all implicit conversions due to subtyping by introducing explicit casts (e.g., oclAsType(Class)).
- Featherweight OCL types may be arbitrarily nested. For example, the expression Set{Set{1,2}} = Set{Set{2,1}} is legal and true.
- Featherweight OCL types may be higher-order nested. For example, the expression \( \lambda X. \text{Set}\{X\} = \text{Set}\{\text{Set}\{2,1\}\} \) is legal. Higher-order pattern-matching can be easily extended following the principles in the HOL library, which can be applied also to Featherweight OCL types.
- All objects types are represented in an object universe. The universe construction also gives semantics to type casts, dynamic type tests, as well as functions such as allInstances(), or oclIsNew(). The object universe construction is conceptually described and demonstrated at an example.
- As part of the OCL logic, Featherweight OCL develops the theory of equality in UML/OCL. This includes the standard equality, which is a computable strict equality using the object references for comparison, and the not necessarily computable logical equality, which expresses the Leibniz principle that ‘equals may be replaced by equals’ in OCL terms.
- Technically, Featherweight OCL is a semantic embedding into a powerful semantic meta-language and environment, namely Isabelle/HOL. It is a so-called shallow embedding in HOL; this means that types in OCL were mapped one-to-one to types in Isabelle/HOL. Ill-typed OCL specifications can therefore not be represented in Featherweight OCL and a type in Featherweight OCL contains exactly the values that are possible in OCL.

**Context.** This document stands in a more than fifteen years tradition of giving a formal semantics to the core of UML and its annotation language OCL, starting from Richters [33] and [18, 22, 26], leading to a number of formal, machine-checked versions, most notably HOL-OCL [1, 3, 7, 10] and more recent approaches [15]. All of them have in common the attempt to reconcile the conflicting demands of an industrially used specification language and its various stakeholders, the needs of OMG standardization process and the desire for sufficient logical precision for tool-implementors, in particular from the Formal Methods research community. To discuss the future directions of the standard, several OCL experts met in November 2013 in Aachen to discuss possible mid-term improvements of OCL, strategies of

---

4The details of such a pre-processing are described in [3].
5following the tradition of HOL-OCL [7]
standardization of OCL within the OMG, and a vision for possible long-term developments of the language [14]. The participants agreed that future proposals for a formal semantics should be machine-check, to ensure the absence of syntax errors, the consistency of the formal semantics, as well as provide a suite of corner-cases relevant for OCL tool implementors.

**Organization of this document.** This document is organized as follows. After a brief background section introducing a running example and basic knowledge on Isabelle/HOL and its formal notations, we present the formal semantics of Featherweight OCL introducing:

1. A conceptual description of the formal semantics, highlighting the essentials and avoiding the definitions in detail.
2. A detailed formal description. This covers:
   a) OCL Types and their presentation in Isabelle/HOL,
   b) OCL Terms, i.e., the semantics of library operators, together with definitions, lemmas, and test cases for the implementor,
   c) UML/OCL Constructs, i.e., a core of UML class models plus user-defined constructions on them such as class-invariants and operation contracts.
3. Since the latter, i.e., the construction of UML class models, has to be done on the meta-level (so not inside HOL, rather on the level of a pre-compiler), we will describe this process with two larger examples, namely formalizations of our running example.

### 0.2. Background

#### 0.2.1. A Running Example for UML/OCL

The Unified Modeling Language (UML) [30, 31] comprises a variety of model types for describing static (e.g., class models, object models) and dynamic (e.g., state-machines, activity graphs) system properties. One of the more prominent model types of the UML is the class model (visualized as class diagram) for modeling the underlying data model of a system in an object-oriented manner. As a running example, we model a part of a conference management system. Such a system usually supports the conference organizing process, e.g., creating a conference Website, reviewing submissions, registering attendees, organizing the different sessions and tracks, and indexing and producing the resulting proceedings. In this example, we constrain ourselves to the process of organizing conference sessions; Figure 0.1 shows the class model. We model the hierarchy of roles of our system as a hierarchy of classes (e.g., Hearer, Speaker, or Chair) using an inheritance relation (also called generalization).

![Figure 0.1: A simple UML class model representing a conference system for organizing conference sessions: persons can participate, in different roles, in a session.](image-url)
In particular, inheritance establishes a subtyping relationship, i.e., every Speaker (subclass) is also a Hearer (superclass).

A class does not only describe a set of instances (called objects), i.e., record-like data consisting of attributes such as name of class Session, but also operations defined over them. For example, for the class Session, representing a conference session, we model an operation findRole(p:Person):Role that should return the role of a Person in the context of a specific session; later, we will describe the behavior of this operation in more detail using UML. In the following, the term object describes a (run-time) instance of a class or one of its subclasses.

Relations between classes (called associations in UML) can be represented in a class diagram by connecting lines, e.g., Participant and Session or Person and Role. Associations may be labeled by a particular constraint called multiplicity, e.g., 0..* or 0..1, which means that in a relation between participants and sessions, each Participant object is associated to at most one Session object, while each Session object may be associated to arbitrarily many Participant objects. Furthermore, associations may be labeled by projection functions like person and role; these implicit function definitions allow for OCL-expressions like self.person, where self is a variable of the class Role. The expression self.person denotes persons being related to the specific object self of type role. A particular feature of the UML are association classes (Participant in our example) which represent a concrete tuple of the relation within a system state as an object; i.e., associations classes allow also for defining attributes and operations for such tuples. In a class diagram, association classes are represented by a dotted line connecting the class with the association. Associations classes can take part in other associations. Moreover, UML supports also n-ary associations (not shown in our example).

We refine this data model using the Object Constraint Language (OCL) for specifying additional invariants, preconditions and postconditions of operations. For example, we specify that objects of the class Person are uniquely determined by the value of the name attribute and that the attribute name is not equal to the empty string (denoted by ''):

```
context Person
  inv: name <> '' and
    Person::allInstances()->isUnique(p:Person | p.name)
```

Moreover, we specify that every session has exactly one chair by the following invariant (called onlyOneChair) of the class Session:

```
context Session
  inv onlyOneChair: self.participants->one( p:Participant | p.role.oclIsTypeOf(Chair))
```

where p.role.oclIsTypeOf(Chair) evaluates to true, if p.role is of dynamic type Chair. Besides the usual static types (i.e., the types inferred by a static type inference), objects in UML and other object-oriented languages have a second dynamic type concept. This is a consequence of a family of casting functions (written o[C] for an object o into another class type C) that allows for converting the static type of objects along the class hierarchy. The dynamic type of an object can be understood as its “initial static type” and is unchanged by casts. We complete our example by describing the behavior of the operation findRole as follows:

```
context Session::findRole(person:Person):Role
  pre: self.participates.person->includes(person)
  post: result=self.participants->one(p:Participant | p.person = person ).role
    and self.participants = self.participants@pre
    and self.name = self.name@pre
```

where in post-conditions, the operator @pre allows for accessing the previous state. Note that:

```
pre: self.participates.person->includes(person)
```

is actually a syntactic abbreviation for a constraint referring to the previous state:
Note, further, that conventions for full-OCL permit the suppression of the self-parameter, following similar syntactic conventions in other object-oriented languages such as Java:

context Session::findRole(person:Person):Role
pre: participates.person->includes(person)
post: result=participants->one(p:Participant |
p.person = person ).role
and participants = participants@pre
and name = name@pre

In UML, classes can contain attributes of the type of the defining class. Thus, UML can represent (mutually) recursive datatypes. Moreover, OCL introduces also recursively specified operations.

A key idea of defining the semantics of UML and extensions like SecureUML [11] is to translate the diagrammatic UML features into a combination of more elementary features of UML and OCL expressions [20]. For example, associations (i.e., relations on objects) can be implemented in specifications at the design level by aggregations, i.e., collection-valued class attributes together with OCL constraints expressing the multiplicity. Thus, having a semantics for a subset of UML and OCL is tantamount for the foundation of the entire method.

0.2.2. Formal Foundation

A Gentle Introduction to Isabelle

Isabelle [27] is a generic theorem prover. New object logics can be introduced by specifying their syntax and natural deduction inference rules. Among other logics, Isabelle supports first-order logic, Zermelo-Fraenkel set theory and the instance for Church’s higher-order logic (HOL).

The core language of Isabelle is a typed λ-calculus providing a uniform term language $T$ in which all logical entities where represented:

$$ T ::= C \mid V \mid \lambda V. T \mid T T $$

where:

- $C$ is the set of constant symbols like 'fst' or 'snd' as operators on pairs. Note that Isabelle's syntax engine supports mixfix-notation for terms: '(\_ \implies \_ ) A B$ or '(\_ + \_ ) A B$ can be parsed and printed as 'A \implies B'$ or 'A + B', respectively.

- $V$ is the set of variable symbols like 'x', 'y', 'z', ... Variables standing in the scope of a λ-operator were called bound variables, all others are free variables.

- '$\lambda V. T$' is called λ-abstraction. For example, consider the identity function $\lambda x.x$. A λ-abstraction forms a scope for the variable $V$.

- $T T'$ is called an application.

These concepts are not at all Isabelle specific and can be found in many modern programming languages ranging from Haskell over Python to Java.

Terms where associated to types by a set of type inference rules only terms for which a type can be inferred—i.e., for typed terms—were considered as legal input to the Isabelle system. The type-terms $\tau$ for λ-terms are defined as:

$$ \tau ::= TV \mid TV : \Xi \mid \tau \Rightarrow \tau \mid (\tau,\ldots,\tau)TC \quad (0.2) $$

6In the Isabelle implementation, there are actually two further variants which were irrelevant for this presentation and are therefore omitted.

7Similar to https://en.wikipedia.org/w/index.php?title=Hindley%E2%80%93Milner_type_system&oldid=668548458

8Again, the Isabelle implementation is actually slightly different; our presentation is an abstraction in order to improve readability.
• \(TV\) is the set of type variables like \(\alpha, \beta, \ldots\). The syntactic categories \(V\) and \(TV\) are disjoint; thus, \(\bar{x}\) is a perfectly possible type variable.

• \(\Xi\) is a set of type-classes like \(\text{ord, order, linorder,} \ldots\). This feature in the Isabelle type system is inspired by Haskell type classes. A type class constraint such as \(\alpha :: \text{order}\) expresses that the type variable \(\alpha\) may range over any type that has the algebraic structure of a partial ordering (as it is configured in the Isabelle/HOL library).

• The type \(\alpha \Rightarrow \beta\) denotes the total function space from \(\alpha\) to \(\beta\).

• \(TC\) is a set of type constructors like \((\alpha)\text{list}\) or \((\alpha)\text{tree}\). Again, Isabelle’s syntax engine supports mixfix-notation for type terms: cartesian products \(\alpha \times \beta\) or type sums \(\alpha + \beta\) are notations for \((\alpha, \beta)(\text{pair})\) or \((\alpha, \beta)(\text{sum})\), respectively. Also null-ary type-constructors like \((\text{bool})\) or \((\text{nat})\) are possible; note that the parentheses of null-ary type constructors are usually omitted.

Isabelle accepts also the notation \(t :: \tau\) as type assertion in the term-language; \(t :: \tau\) means \(t\) is required to have type \(\tau\). Note that typed terms can contain free variables; terms like \(x + y = y + x\) reflecting common mathematical notation (and the convention that free variables are implicitly universally quantified) are possible and common in Isabelle theories.

An environment providing \(\Xi, TC\) as well as a map from constant symbols \(C\) to types (built over these \(\Xi\) and \(TC\)) is called a global context; it provides a kind of signature, i.e., a mechanism to construct the syntactic material of a logical theory.

The most basic (built-in) global context of Isabelle provides just a language to construct logical rules. More concretely, it provides a constant declaration for the (built-in) meta-level implication \(\alpha \Rightarrow \beta\), allowing to form constructs like \(A_1 \Rightarrow \cdots \Rightarrow A_n \Rightarrow A_{n+1}\), which are viewed as a rule of the form “from assumptions \(A_1\) to \(A_n\), infer conclusion \(A_{n+1}\)” and which is written in Isabelle syntax as

\[
[A_1; \ldots; A_n] \Rightarrow A_{n+1}
\]

or, in mathematical notation,

\[
\frac{A_1 \cdots A_n}{A_{n+1}}
\]  

Moreover, the built-in meta-level quantification \(\forall x. E\) (pretty-printed and parsed as \(\bigwedge x. E\)) captures the usual side-constraints “\(x\) must not occur free in the assumptions” for quantifier rules; meta-quantified variables can be considered as “fresh” free variables. Meta-level quantification leads to a generalization of Horn-clauses of the form:

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

Isabelle supports forward- and backward reasoning on rules. For backward-reasoning, a proof state can be initialized in a given global context and further transformed into others. For example, a proof of \(\phi\), using the Isar language, will look as follows in Isabelle:

```
lemma label: \(\phi\)
apply(case_tac)
apply(simp_all)
done
```

This proof script instructs Isabelle to prove \(\phi\) by case distinction followed by a simplification of the resulting proof state. Such a proof state is an implicitly conjoint sequence of generalized Horn-clauses (called subgoals) \(\phi_1, \ldots, \phi_n\) and a goal \(\phi\). Proof states were usually denoted by:

\[
\text{label : } \phi
\]

1. \(\phi_1\)

\[
\vdots
\]

n. \(\phi_n\)


\(^{10}\)Here, we assume that \(\_ + \_\) and \(\_ = \_\) are declared constant symbols having type \(\Rightarrow \Rightarrow \Rightarrow \text{int} \Rightarrow \text{int} \Rightarrow \text{int} \Rightarrow \alpha \Rightarrow \text{bool}\), respectively.
Subgoals and goals may be extracted from the proof state into theorems of the form \([\phi_1; \ldots; \phi_n] \implies \phi\) at any time;

By extensions of global contexts with axioms and proofs of theorems, theories can be constructed step by step. Beyond the basic mechanisms to extend a global context by a type-constructor-, type-class-constant-definition or an axiom, Isabelle offers a number of commands that allow for more complex extensions of theories in a logically safe way (avoiding the use of axioms directly).

**Higher-order Logic (HOL)**

Higher-order logic (HOL) \[1, 16\] is a classical logic based on a simple type system. Isabelle/HOL is a theory extension of the basic Isabelle core-language with operators and the 7 axioms of HOL; together with large libraries this constitutes an implementation of HOL. Isabelle/HOL provides the usual logical connectives like \(_\land_\), \(_\rightarrow_\), \(_\neg_\) as well as the object-logical quantifiers \(\forall x. P x\) and \(\exists x. P x\); in contrast to first-order logic, quantifiers may range over arbitrary types, including total functions \(f :: \alpha \Rightarrow \beta\). HOL is centered around extensional equality \(_=\) :: \(\alpha \Rightarrow \alpha \Rightarrow \text{bool}\). Extensional equality means that two functions \(f\) and \(g\) are equal if and only if they are point-wise equal; this is captured by the rule: \((\forall x. f x = g x) \implies f = g\). HOL is more expressive than first-order logic, since, among many other things, induction schemes can be expressed inside the logic. For example, the standard induction rule on natural numbers in HOL:

\[ P \ 0 \implies (\forall x. P x \implies P (x + 1)) \implies P x \]

is just an ordinary rule in Isabelle which is in fact a proven theorem in the theory of natural numbers. This example exemplifies an important design principle of Isabelle: theorems and rules are technically the same, paving the way to derived rules and automated decision procedures based on them. This has the consequence that these procedures are consequently sound by construction with respect to their logical aspects (they may be incomplete or failing, though).

On the other hand, Isabelle/HOL can also be viewed as a functional programming language like SML or Haskell. Isabelle/HOL definitions can usually be read just as another functional programming language; if not interested in proofs and the possibilities of a specification language providing powerful logical quantifiers or equivalent free variables, the reader can just ignore these aspects in theories.

Isabelle/HOL offers support for a particular methodology to extend given theories in a logically safe way: A theory-extension is conservative if the extended theory is consistent provided that the original theory was consistent. Conservative extensions can be constant definitions, type definitions, datatype definitions, primitive recursive definitions and well founded recursive definitions.

For instance, the library includes the type constructor \(\tau_1 = \bot | \tau_\alpha : \alpha\) that assigns to each type \(\tau\) a type \(\tau_\bot\) disjointly extended by the exceptional element \(\bot\). The function \(\tau_\bot\) \(\alpha\) \(\Rightarrow\) \(\alpha\) is the inverse of \(\tau_\bot\) (unspecified for \(\bot\)). Partial functions \(\alpha \Rightarrow \beta\) are defined as functions \(\alpha \Rightarrow \beta\) supporting the usual concepts of domain (\(\text{dom}_{\tau}\)) and range (\(\text{ran}_{\tau}\)).

As another example of a conservative extension, typed sets were built in the Isabelle libraries conservatively on top of the kernel of HOL as functions to \(\text{bool}\); consequently, the constant definitions for membership is as follows\[11\]

\[
\begin{align*}
\text{types} & \quad \alpha \text{ set } = \alpha \Rightarrow \text{bool} \\
\text{definition} & \quad \text{Collect } ::(\alpha \Rightarrow \text{bool}) \Rightarrow \alpha \text{ set } - \text{ set comprehension} \\
\text{where} & \quad \text{Collect } S \equiv S \\
\text{definition} & \quad \text{member } ::\alpha \Rightarrow \alpha \Rightarrow \text{bool} - \text{ membership test} \\
\text{where} & \quad \text{member } s S \equiv \text{ran}_{\tau} 
\end{align*}
\]

Isabelle’s syntax engine is instructed to accept the notation \(\{ x \mid P\}\) for Collect \(\lambda x. P\) and the notation \(s \in S\) for member \(s S\). As can be inferred from the example, constant definitions are axioms that introduce a fresh constant symbol by some non-recursive expressions not containing free variables; this

\[11\]To increase readability, we use a slightly simplified presentation.
type of axiom is logically safe since it works like an abbreviation. The syntactic side conditions of this axiom are mechanically checked. It is straightforward to express the usual operations on sets like 
\[ \alpha \cup \alpha \cap \alpha \colon \alpha \text{ set } \Rightarrow \alpha \text{ set } \Rightarrow \alpha \text{ set}\] as conservative extensions, too, while the rules of typed set theory were derived by proofs from these definitions.

Similarly, a logical compiler is invoked for the following statements introducing the types option and list:

\[
\begin{align*}
\text{datatype} & \quad \text{option} \quad = \text{None} \mid \text{Some } \alpha \\
\text{datatype} & \quad \alpha \text{ list} \quad = \text{Nil} \mid \text{Cons } a \ l
\end{align*}
\]

Here, \([\ ]\) or \(a \# l\) are an alternative syntax for \(\text{Nil}\) or \(\text{Cons } a \ l\); moreover, \([a, b, c]\) is defined as alternative syntax for \(a \# b \# c \# [\ ]\). These (recursive) statements were internally represented in by internal type and constant definitions. Besides the constructors None, Some, \([\ ]\) and Cons, there is the match operation

\[
\text{case } x \text{ of } \text{None } \Rightarrow F \mid \text{Some } a \Rightarrow G a
\]

respectively

\[
\text{case } x \text{ of } [\ ] \Rightarrow F \mid \text{Cons } a \ r \Rightarrow G a \ r
\]

From the internal definitions (not shown here) several properties were automatically derived. We show only the case for lists:

\[
\begin{align*}
\text{(case } [\ ] \text{ of } [\ ] \Rightarrow F \mid (a \# r) \Rightarrow G a \ r) & = F \\
\text{(case } b \# t \text{ of } [\ ] \Rightarrow F \mid (a \# r) \Rightarrow G a \ r) & = G b \ t \\
[\ ] \neq a \# t & - \text{ distinctness} \\
[a = [\ ] \Rightarrow P; \exists x \ t. a = x \# t \Rightarrow P] & \Rightarrow P - \text{ exhaust} \\
[P [\ ]; \forall at. P \Rightarrow P(a \# t)] & \Rightarrow P \ x - \text{ induct}
\end{align*}
\]

Finally, there is a compiler for primitive and well founded recursive function definitions. For example, we may define the sort operation on linearly ordered lists by:

\[
\begin{align*}
\text{fun} & \quad \text{ins} \quad :: [\alpha :: \text{linorder}, \alpha \text{ list}] \Rightarrow \alpha \text{ list} \\
\text{where} & \quad \text{ins } x \ [\ ] \quad = [x] \\
& \quad \text{ins } x \ (y \# y s) \quad = \text{if } x < y \text{ then } x \# y \# y s \text{ else } y \# (\text{ins } x \ y s) \\
\text{fun} & \quad \text{sort} \quad :: (\alpha :: \text{linorder}) \text{ list } \Rightarrow \alpha \text{ list} \\
\text{where} & \quad \text{sort } [\ ] \quad = [\ ] \\
& \quad \text{sort}(x \# x s) \quad = \text{ins } x \ (\text{sort } x s)
\end{align*}
\]

The internal (non-recursive) constant definition for these operations is quite involved; however, the logical compiler will finally derive all the equations in the statements above from this definition and make them available for automated simplification.

Thus, Isabelle/HOL also provides a large collection of theories like sets, lists, orderings, and various arithmetic theories which only contain rules derived from conservative definitions. This library constitutes a comfortable basis for defining the OCL library and language constructs.

In particular, Isabelle manages a set of executable types and operators, i.e., types and operators for which a compilation to SML, OCaml or Haskell is possible. Setups for arithmetic types such as int have been done; moreover any datatype and any recursive function were included in this executable set (providing that they only consist of executable operators). This forms the basis that many OCL terms can be executed directly. Using the value command, it is possible to compile many OCL ground expressions (no free variables) to code and to execute them; for example value "3 + 7" just answers with 10 in Isabelle’s output window. This is even true for many expressions containing types which in themselves are not executable. For example, the Set type, which is defined in Featherweight OCL as the type of potentially infinite sets, is consequently not in itself executable; however, due to special setups of the code-generator, expressions like value "Set{1,2}" are, because the underlying constructors in this expression allow for automatically establishing that this set is finite and reducible to constructs that are in this special case executable.
0.2.3. How this Annex A was Generated from Isabelle/HOL Theories

Isabelle, as a framework for building formal tools \[35\], provides the means for generating formal documents. With formal documents (such as the one you are currently reading) we refer to documents that are machine-generated and ensure certain formal guarantees. In particular, all formal content (e.g., definitions, formulae, types) are checked for consistency during the document generation.

For writing documents, Isabelle supports the embedding of informal texts using a \texttt{LaTeX}-based markup language within the theory files. To ensure the consistency, Isabelle supports to use, within these informal texts, antiquotations that refer to the formal parts and that are checked while generating the actual document as PDF. For example, in an informal text, the antiquotation \texttt{@{thm ocl_not_not}} will instruct Isabelle to lock-up the (formally proven) theorem of name \texttt{ocl\_not\_not} and to replace the antiquotation with the actual theorem, i.e., \texttt{not (not x) = x}.

Figure 0.2 illustrates this approach: Figure 0.2a shows the \texttt{jEdit}-based development environment of Isabelle with an excerpt of one of the core theories of Featherweight OCL. Figure 0.2b shows the generated PDF document where all antiquotations are replaced. Moreover, the document generation tools allows for defining syntactic sugar as well as skipping technical details of the formalization.

Featherweight OCL is a formalization of the core of OCL aiming at formally investigating the relationship between the various concepts. At present, it does not attempt to define the complete OCL library. Instead, it concentrates on the core concepts of OCL as well as the types \texttt{Boolean}, \texttt{Integer}, and typed sets (\texttt{Set(T)}). Following the tradition of HOL-OCL \[6,8\], Featherweight OCL is based on the following principles:

1. It is an embedding into a powerful semantic meta-language and environment, namely Isabelle/HOL \[27\].

2. It is a shallow embedding in HOL; types in OCL were injectively mapped to types in Featherweight OCL. Ill-typed OCL specifications cannot be represented in Featherweight OCL and a type in Featherweight OCL contains exactly the values that are possible in OCL. Thus, sets may contain \texttt{null (Set{null}) is a defined set}) but not \texttt{invalid (Set{invalid}) is just invalid}.

3. Any Featherweight OCL type contains at least \texttt{invalid} and \texttt{null} (the type \texttt{Void} contains only these instances). The logic is consequently four-valued, and there is a \texttt{null}-element in the type \texttt{Set(A)}.

\[24\]
4. It is a strongly typed language in the Hindley-Milner tradition. We assume that a pre-process eliminates all implicit conversions due to sub-typing by introducing explicit casts (e.g., oclAsType()). The details of such a pre-processing are described in [4]. Casts are semantic functions, typically injections, that may convert data between the different Featherweight OCL types.

5. All objects are represented in an object universe in the HOL-OCL tradition [7]. The universe construction also gives semantics to type casts, dynamic type tests, as well as functions such as oclAllInstances(), or oclIsNew().

6. Featherweight OCL types may be arbitrarily nested. For example, the expression Set(Set{1,2}) = Set(Set{2,1}) is legal and true.

7. For demonstration purposes, the set type in Featherweight OCL may be infinite, allowing infinite quantification and a constant that contains the set of all Integers. Arithmetic laws like commutativity may therefore be expressed in OCL itself. The iterator is only defined on finite sets.

8. It supports equational reasoning and congruence reasoning, but this requires a differentiation of the different equalities like strict equality, strong equality, meta-equality (HOL). Strict equality and strong equality require a sub-calculus, “cp” (a detailed discussion of the different equalities as well as the sub-calculus “cp”—for three-valued OCL 2.0—is given in [9]), which is nasty but can be hidden from the user inside tools.

Overall, this would contribute to one of the main goals of the OCL 2.5 RFP, as discussed at the OCL meeting in Aachen [14].

0.3. The Essence of UML-OCL Semantics

0.3.1. The Theory Organization

The semantic theory is organized in a quite conventional manner in three layers. The first layer, called the denotational semantics comprises a set of definitions of the operators of the language. Presented as definitional axioms inside Isabelle/HOL, this part assures the logically consistency of the overall construction. The denotational definitions of types, constants and operations, and OCL contracts represent the “gold standard” of the semantics. The second layer, called logical layer, is derived from the former and centered around the notion of validity of an OCL formula $P$. For a state-transition from pre-state $\sigma$ to post-state $\sigma'$, a validity statement is written $(\sigma, \sigma') \models P$. Its major purpose is to logically establish facts (lemmas and theorems) about the denotational definitions. The third layer, called algebraic layer, also derived from the former layers, tries to establish algebraic laws of the form $P = P'$; such laws are amenable to equational reasoning and also help for automated reasoning and code-generation. For an implementor of an OCL compiler, these consequences are of most interest.

For space reasons, we will restrict ourselves in this document to a few operators and make a traversal through all three layers to give a high-level description of our formalization. Especially, the details of the semantic construction for sets and the handling of objects and object universes were excluded from a presentation here.

0.3.2. Denotational Semantics of Types

The syntactic material for type expressions, called TYPES($C$), is inductively defined as follows:

- $C \subseteq$ TYPES($C$)
- Boolean, Integer, Real, Void, ... are elements of TYPES($C$)
- Set($X$), Bag($X$), Sequence($X$), and Pair($X,Y$) (as example for a Tuple-type) are in TYPES($C$) (if $X,Y \in$ TYPES($C$)).
Types were directly represented in Featherweight OCL by types in HOL; consequently, any Featherweight OCL type must provide elements for a bottom element (also denoted \( \bot \)) and a null element; this is enforced in Isabelle by a type-class \( \text{null} \) that contains two distinguishable elements \( \bot \) and \( \text{null} \) (see Chapter 1 for the details of the construction).

Moreover, the representation mapping from OCL types to Featherweight OCL is one-to-one (i.e., injective), and the corresponding Featherweight OCL types were constructed to represent exactly the elements (“no junk, no confusion elements”) of their OCL counterparts. The corresponding Featherweight OCL types were constructed in two stages: First, a base type is constructed whose carrier set contains exactly the elements of the OCL type. Secondly, this base type is lifted to a valuation type that we use for type-checking Featherweight OCL constants, operations, and expressions. The valuation type takes into account that some UML-OCL functions of its OCL type (namely: accessors in path-expressions) depend on a pre- and a post-state.

For most base types like Boolean\(_\text{base} \) or Integer\(_\text{base} \), it suffices to double-lift a HOL library type:

\[
\text{type\_synonym } \text{Boolean}_\text{base} := \text{bool} \bot \bot (0.14)
\]

As a consequence of this definition of the type, we have the elements \( \bot, \bot, \bot, \bot, \text{true}, \text{false} \) in the carrier-set of Boolean\(_\text{base} \). We can therefore use the element \( \bot \) to define the generic type class element \( \bot \) and \( \bot \) for the generic type class null. For collection types and object types this definition is more evolved (see Chapter 1).

For object base types, we assume a typed universe \( \mathcal{A} \) of objects to be discussed later, for the moment we will refer it by its polymorphic variable.

With respect the valuation types for OCL expression in general and Boolean expressions in particular, they depend on the pair \((\sigma, \sigma')\) of pre- and post-state. Thus, we define valuation types by the synonym:

\[
\text{type\_synonym } V_{\mathcal{A}}(\alpha) := \text{state}(\mathcal{A}) \times \text{state}(\mathcal{A}) \rightarrow \alpha :: \text{null}. \quad (0.15)
\]

The valuation type for boolean, integer, etc. OCL terms is therefore defined as:

\[
\begin{align*}
\text{type\_synonym } V_{\mathcal{A}}(\text{Boolean}) := V_{\mathcal{A}}(\text{Boolean}_\text{base}) \\
\text{type\_synonym } V_{\mathcal{A}}(\text{Integer}) := V_{\mathcal{A}}(\text{Integer}_\text{base}) \\
\end{align*}
\]

...the other cases are analogous. In the subsequent subsections, we will drop the index \( \mathcal{A} \) since it is constant in all formulas and expressions except for operations related to the object universe construction in Section 3.1.

The rules of the logical layer (there are no algebraic rules related to the semantics of types), and more details can be found in Chapter 1.

### 0.3.3. Denotational Semantics of Constants and Operations

We use the notation \( I[E]r \) for the semantic interpretation function as commonly used in mathematical textbooks and the variable \( r \) standing for pairs of pre- and post state \((\sigma, \sigma')\). Note that we will also use \( r \) to denote the type of a state-pair; since both syntactic categories are independent, we can do so without arising confusion. OCL provides for all OCL types the constants invalid for the exceptional computation result and null for the non-existing value. Thus we define:

\[
I[\text{invalid} :: V(\alpha)]r := \text{bot} \quad I[\text{null} :: V(\alpha)]r := \text{null}
\]

For the concrete Boolean-type, we define similarly the boolean constants true and false as well as the fundamental tests for definedness and validity (generically defined for all types):

\[
I[\text{true} :: \text{Boolean}]r = \text{true} \quad I[\text{false} :: \text{Boolean}]r = \text{false} \quad I[X.\text{oclIsUndefined}()]r = (\text{if } I[X]r \in \{\text{bot}, \text{null}\} \text{ then } I[\text{true}]r \text{ else } I[\text{false}]r)
\]
For reasons of conciseness, we will write $\delta X$ for $\text{not}(X.\text{oclIsUndefined}())$ and $\nu X$ for $\text{not}(X.\text{oclIsValid}())$ throughout this document.

Due to the used style of semantic representation (a shallow embedding) $I$ is in fact superfluous and defined semantically as the identity $\lambda x. x$; instead of:

$$I X \tau = \begin{cases} \text{true} & \text{if } I J X K \tau = \text{bot} \\ \text{false} & \text{else} \end{cases}$$

we can therefore write:

$$I[\text{true}::\text{Boolean}]\tau = \nu_{\text{true}}$$

In Isabelle theories, this particular presentation of definitions paves the way for an automatic check that the underlying equation has the form of an axiomatic definition and is therefore logically safe.

On this basis, one can define the core logical operators $\text{not}$ and $\text{and}$ as follows:

$$I[\text{not} X]\tau = \begin{cases} \text{false} & \text{if } I J X K \tau = \text{bot} \\ \text{true} & \text{else} \end{cases}$$

These non-strict operations were used to define the other logical connectives in the usual classical way: $X \text{ or } Y \equiv (\text{not } X) \text{ and } (\text{not } Y)$ or $X \text{ implies } Y \equiv (\text{not } X) \text{ or } Y$.

The default semantics for an OCL library operator is strict semantics; this means that the result of an operation $f$ is invalid if one of its arguments is $+\text{invalid}+$ or $+\text{null}+$. The definition of the addition for integers as default variant reads as follows:

$$I[x + y]\tau = \begin{cases} \text{null} & \text{if } I[\delta x]\tau = \text{null} \land I[\delta y]\tau = \text{true} \\ \text{null} & \text{else} \end{cases}$$

where the operator “+” on the left-hand side of the equation denotes the OCL addition of type $\text{Integer} \Rightarrow \text{Integer} \Rightarrow \text{Integer}$ while the “+” on the right-hand side of the equation of type $\text{int}, \text{int} \Rightarrow \text{int}$ denotes the integer-addition from the HOL library.
0.3.4. Logical Layer

The topmost goal of the logic for OCL is to define the validity statement:

\[(\sigma, \sigma') \models P,\]

where \(\sigma\) is the pre-state and \(\sigma'\) the post-state of the underlying system and \(P\) is a formula, i.e., and OCL expression of type Boolean. Informally, a formula \(P\) is valid if and only if its evaluation in \((\sigma, \sigma')\) (i.e., \(\tau\) for short) yields true. Formally this means:

\[\tau \models P \equiv (I[P]_\tau = \text{true}_{\tau}).\]

On this basis, classical, two-valued inference rules can be established for reasoning over the logical connectives, the different notions of equality, definedness and validity. Generally speaking, rules over logical validity can relate bits and pieces in various OCL terms and allow—via strong logical equality discussed below—the replacement of semantically equivalent sub-expressions. The core inference rules are:

\[
\begin{align*}
\tau \models \text{true} & \quad \neg(\tau \models \text{false}) & \quad \neg(\tau \models \text{invalid}) & \quad \neg(\tau \models \text{null}) \\
\tau \models \text{not } P & \implies \neg(\tau \models P) \\
\tau \models P \land Q & \implies \tau \models P & \quad \tau \models P \land Q & \implies \tau \models Q \\
\tau \models P \implies \tau \models P \lor Q & \quad \tau \models Q \land \tau \implies \tau \models P \lor Q \\
\tau \models P & \implies (\text{if } P \text{ then } B_1 \text{ else } B_2 \text{ endif})\tau = B_1 \tau \\
\tau \models \text{not } P & \implies (\text{if } P \text{ then } B_1 \text{ else } B_2 \text{ endif})\tau = B_2 \tau \\
\tau \models P & \implies \delta P & \quad \tau \models \delta X & \implies \tau \models \upsilon X
\end{align*}
\]

By the latter two properties it can be inferred that any valid property \(P\) (so for example: a valid invariant) is defined, which allows to infer for terms composed by strict operations that their arguments and finally the variables occurring in it are valid or defined.

The mandatory part of the OCL standard refers to an equality (written \(x = y\) or \(x \neq y\) for its negation), which is intended to be a strict operation (thus: \(\text{invalid} = y\) evaluates to \(\text{invalid}\)) and which uses the references of objects in a state when comparing objects, similarly to C++ or Java. In order to avoid confusions, we will use the following notations for equality:

1. The symbol \(\_ = \_\) remains to be reserved to the HOL equality, i.e., the equality of our semantic meta-language,
2. The symbol \(\_ \triangleq \_\) will be used for the strong logical equality, which follows the general logical principle that “equals can be replaced by equals,” and is at the heart of the OCL logic,
3. The symbol \(\_ \doteq \_\) is used for the strict referential equality, i.e., the equality the mandatory part of the OCL standard refers to by the \(\_ = \_\) symbol.

The strong logical equality is a polymorphic concept which is defined using polymorphism for all OCL types by:

\[I[X \triangleq Y]_\tau \equiv \iota_{\upsilon[J[X]_\tau]} = I[Y]_\tau \upsilon_{\iota} \]

It enjoys nearly the laws of a congruence:

\[
\begin{align*}
\tau \models (x \triangleq x) \\
\tau \models (x \triangleq y) & \implies \tau \models (y \triangleq x) \\
\tau \models (x \triangleq y) & \implies \tau \models (y \triangleq z) & \implies \tau \models (x \triangleq z) \\
cp P & \implies \tau \models (x \triangleq y) & \implies \tau \models (P x) & \implies \tau \models (P y)
\end{align*}
\]

\[\text{[12]}\]

12 Strong logical equality is also referred as “Leibniz”-equality.
where the predicate $cp$ stands for context-passing, a property that is true for all pure OCL expressions (but not arbitrary mixtures of OCL and HOL) in Featherweight OCL. The necessary side-calculus for establishing $cp$ can be fully automated; the reader interested in the details is referred to Section 2.1.3.

The strong logical equality of Featherweight OCL give rise to a number of further rules and derived properties, that clarify the role of strong logical equality and the Boolean constants in OCL specifications:

$$
\tau \models \delta x \lor \tau \models x \triangleq \text{invalid} \lor \tau \models x \triangleq \text{null},
$$

$$(\tau \models A \triangleq \text{invalid}) = (\tau \models \neg(\nu A))$$

$$(\tau \models A \triangleq \text{true}) = (\tau \models A)$$

$$(\tau \models A \triangleq \text{false}) = (\tau \models \neg A)$$

$$(\tau \models \delta x) = (\neg \tau \models \delta x)$$

$$(\tau \models \neg(\nu x)) = (\neg \tau \models \nu x)$$

The logical layer of the Featherweight OCL rules gives also a means to convert an OCL formula living in its four-valued world into a representation that is classically two-valued and can be processed by standard SMT solvers such as CVC3 [2] or Z3 [19]. $\delta$-closure rules for all logical connectives have the following format, e.g.:

$$
\tau \models \delta x \implies (\tau \models \neg x) = (\neg(\tau \models x))
$$

$$
\tau \models \delta x \implies \tau \models \delta y \implies (\tau \models x \land y) = (\tau \models x \land \tau \models y)
$$

$$
\tau \models \delta x \implies \tau \models \delta y
$$

$$
\implies (\tau \models (x \implies y)) = ((\tau \models x) \implies (\tau \models y))
$$

Together with the already mentioned general case-distinction

$$
\tau \models \delta x \lor \tau \models x \triangleq \text{invalid} \lor \tau \models x \triangleq \text{null}
$$

which is possible for any OCL type, a case distinction on the variables in a formula can be performed; due to strictness rules, formulae containing somewhere a variable $x$ that is known to be invalid or null reduce usually quickly to contradictions. For example, we can infer from an invariant $\tau \models x = y - 3$ that we have $\tau \models x \triangleq y - 3 \land \tau \models \delta x \land \tau \models \delta y$. We call the latter formula the $\delta$-closure of the former. Now, we can convert a formula like $\tau \models x > 0 \lor 3 \cdot y > x \cdot x$ into the equivalent formula $\tau \models x > 0 \lor \tau \models 3 \cdot y > x \cdot x$ and thus internalize the OCL-logic into a classical (and more tool-conform) logic. This works—for the price of a potential, but due to the usually “rich” $\delta$-closures of invariants rare—exponential blow-up of the formula for all OCL formulas.

### 0.3.5. Algebraic Layer

Based on the logical layer, we build a system with simpler rules which are amenable to automated reasoning. We restrict ourselves to pure equations on OCL expressions.

Our denotational definitions on $\neg$ and $\land$ can be re-formulated in the following ground equations:

$$
\nu \text{invalid} = \text{false}
\nu \text{null} = \text{true}
\nu \text{true} = \text{true}
\nu \text{false} = \text{true}
\delta \text{invalid} = \text{false}
\delta \text{null} = \text{false}
\delta \text{true} = \text{true}
\delta \text{false} = \text{true}
\text{not invalid} = \text{invalid}
\text{not null} = \text{null}
\text{not true} = \text{false}
\text{not false} = \text{true}
(\text{null and true}) = \text{null}
(\text{null and false}) = \text{false}
(\text{null and null}) = \text{null}
(\text{null and invalid}) = \text{invalid}
(\text{false and true}) = \text{false}
(\text{false and false}) = \text{false}
(\text{false and null}) = \text{false}
(\text{false and invalid}) = \text{false}
$$
\begin{align*}
    (\text{true and true}) &= \text{true} & (\text{true and false}) &= \text{false} \\
    (\text{true and null}) &= \text{null} & (\text{true and invalid}) &= \text{invalid} \\
    (\text{invalid and true}) &= \text{invalid} & (\text{invalid and false}) &= \text{false} \\
    (\text{invalid and null}) &= \text{invalid} & (\text{invalid and invalid}) &= \text{invalid}
\end{align*}

On this core, the structure of a conventional lattice arises:

\[
\begin{align*}
    \text{X and X} &= \text{X} \\
    \text{X and Y} &= \text{Y and X} \\
    \text{false and X} &= \text{false} \\
    \text{true and X} &= \text{X} \\
    \text{X and (Y and Z)} &= \text{X and Y and Z}
\end{align*}
\]

as well as the dual equalities for \text{or} and \text{and} and the De Morgan rules. This wealth of algebraic properties makes the understanding of the logic easier as well as automated analysis possible: for example, it allows for computing a DNF of invariant systems (by term-rewriting techniques) which are a prerequisite for \(\delta\)-closures.

The above equations explain the behavior for the most-important non-strict operations. The clarification of the exceptional behaviors is of key-importance for a semantic definition of the standard and the major deviation point from HOL-OCL [6, 8] to Featherweight OCL as presented here. Expressed in algebraic equations, “strictness-principles” boil down to:

\[
\begin{align*}
    \text{invalid + X} &= \text{invalid} & \text{X + invalid} &= \text{invalid} \\
    \text{invalid->including(X)} &= \text{invalid} & \text{null->including(X)} &= \text{invalid} \\
    \text{X \# invalid} &= \text{invalid} & \text{invalid \# X} &= \text{invalid} \\
    \text{S->including(invalid)} &= \text{invalid} \\
    \text{X \# X} &= (\text{if } v x \text{ then true else invalid endif}) \\
    1 / 0 &= \text{invalid} & 1 / \text{null} &= \text{invalid} \\
    \text{invalid->isEmpty()} &= \text{invalid} & \text{null->isEmpty()} &= \text{null}
\end{align*}
\]

Algebraic rules are also the key for execution and compilation of Featherweight OCL expressions. We derived, e.g.:

\[
\begin{align*}
    \delta \text{ Set\{} &= \text{true} \\
    \delta (X->including(x)) &= \delta X \text{ and } v x \\
    \text{Set\{}->includes(x) &= (\text{if } v x \text{ then false}
    \quad \text{else invalid endif}) \\
    (X->including(x)->includes(y)) &=
    \quad \text{if } \delta X
    \quad \text{then if } x \# y
    \quad \text{then true}
    \quad \text{else } X->includes(y)
    \quad \text{endif}
    \quad \text{else invalid}
    \quad \text{endif})
\end{align*}
\]

As \text{Set\{}1\text{,2\}} is only syntactic sugar for

\[
\text{Set\{}->including(1)->including(2)}
\]

30
an expression like \( \text{Set\{1,2\}} \rightarrow \text{includes(null)} \) becomes decidable in Featherweight OCL by applying these algebraic laws (which can give rise to efficient compilations). The reader interested in the list of “test-statements” like:

\[ \tau |\rightarrow (\text{Set\{\text{Set\{2, null\}}\}} \rightarrow \text{Set\{\text{Set\{null, 2\}}\}}) \]

make consult Section 2.9; these test-statements have been machine-checked and proven consistent with the denotational and logic semantics of Featherweight OCL.

### 0.3.6. Object-oriented Datatype Theories

In the following, we will refine the concepts of a user-defined data-model implied by a class-model (visualized by a class-diagram) as well as the notion of state used in the previous section to much more detail. UML class models represent in a compact and visual manner quite complex, object-oriented data-types with a surprisingly rich theory. In this section, this theory is made explicit and corner cases were pointed out.

A UML class model underlying a given OCL invariant or operation contract produces several implicit operations which become accessible via appropriate OCL syntax. A class model is a four-tuple \((C, _, <, \text{Attrib}, \text{Assoc})\) where:

1. \( C \) is a set of class names (written as \( \{C_1, \ldots, C_n\} \)). To each class name a type of data in OCL is associated. Moreover, class names declare two projector functions to the set of all objects in a state: \( C_i\_\text{allInstances()} \) and \( C_i\_\text{allInstances@pre()} \),
2. \( _< \) is an inheritance relation on classes,
3. \( \text{Attrib}(C_i) \) is a collection of attributes associated to classes \( C_i \). It declares two families of accessors; for each attribute \( a \in \text{Attrib}(C_i) \) in a class definition \( C_i \) (denoted \( X.a : C_i \rightarrow A \) and \( X.a@pre : C_i \rightarrow A \) for \( A \in \text{TYPES}(C_i) \)),
4. \( \text{Assoc}(C_i, C_j) \) is a collection of associations\(^{13}\). An association \((n, rn_{from}, rn_{to}) \in \text{Assoc}(C_i, C_j)\) between to classes \( C_i \) and \( C_j \) is a triple consisting of a (unique) association name \( n \), and the role-names \( rn_{to} \) and \( rn_{from} \). To each role-name belong two families of accessors denoted \( X.a : C_i \rightarrow A \) and \( X.a@pre : C_i \rightarrow A \) for \( A \in \text{TYPES}(C_i) \),
5. for each pair \( C_i < C_j \) \((C_i, C_j < C)\), there is a cast operation of type \( C_j \rightarrow C_i \) that can change the static type of an object of type \( C_i \): \( \text{obj} : C_i \rightarrow \text{oclsAsType}(C_i) \),
6. for each class \( C_i \in C \), there are two dynamic type tests \((X\text{.oclIsTypeOf}(C_i) \) and \( X\text{.oclIsKindOf}(C_i) \)),
7. and last but not least, for each class name \( C_i \in C \) there is an instance of the overloaded referential equality (written \( _\text{=} \)).

Assuming a strong static type discipline in the sense of Hindley-Milner types, Featherweight OCL has no “syntactic subtyping.” In contrast, sub-typing can be expressed semantically in Featherweight OCL by adding suitable type-casts which do have a formal semantics. Thus, sub-typing becomes an issue of the front-end that can make implicit type-coercions explicit. Our perspective shifts the emphasis on the semantic properties of casting, and the necessary universe of object representations (induced by a class model) that allows to establish them.

As a pre-requisite of a denotational semantics for these operations induced by a class-model, we need an object-universe in which these operations can be defined in a denotational manner and from which the necessary properties for constructors, accessors, tests and casts can be derived. A concrete universe constructed from a class model will be used to instantiate the implicit type parameter \( \mathfrak{A} \) of all OCL operations discussed so far.

\(^{13}\)Given the fact that there is at present no consensus on the semantics of n-ary associations, Featherweight OCL restricts itself to binary associations.
A Denotational Space for Class-Models: Object Universes

It is natural to construct system states by a set of partial functions \( f \) that map object identifiers \( \text{oid} \) to some representations of objects:

\[
\text{typedef } \mathfrak{A} \text{ state} := \{ \sigma : \text{oid} \to \alpha | \text{inv}_\sigma(\sigma) \}
\]

where \( \text{inv}_\sigma \) is a to be discussed invariant on states.

The key point is that we need a common type \( \mathfrak{A} \) for the set of all possible object representations. Object representations model “a piece of typed memory,” i.e., a kind of record comprising administration information and the information for all attributes of an object; here, the primitive types as well as collections over them are stored directly in the object representations, class types and collections over them are represented by oid’s (respectively lifted collections over them).

In a shallow embedding which must represent UML types one-to-one by HOL types, there are two fundamentally different ways to construct such a set of object representations, which we call an object universe \( \mathfrak{A} \):

1. an object universe can be constructed from a given class model, leading to closed world semantics, and
2. an object universe can be constructed for a given class model and all its extensions by new classes added into the leaves of the class hierarchy, leading to an open world semantics.

For the sake of simplicity, the present semantics chose the first option for Featherweight OCL, while HOL-OCL \([7]\) used an involved construction allowing the latter.

A naïve attempt to construct \( \mathfrak{A} \) would look like this: the class type \( C_i \) induced by a class will be the type of such an object representation:

\[
C_i := (\text{oid} \times A_{i1} \times \cdots \times A_{in}) \text{ where the types } A_{i1}, \ldots, A_{in} \text{ are the attribute types (including inherited attributes) with class types substituted by oid. The function OidOf projects the first component, the oid, out of an object representation. Then the object universe will be constructed by the type definition:
\]

\[
\mathfrak{A} := C_1 + \cdots + C_n .
\]

It is possible to define constructors, accessors, and the referential equality on this object universe. However, the treatment of type casts and type tests cannot be faithful with common object-oriented semantics, be it in UML or Java: casting up along the class hierarchy can only be implemented by loosing information, such that casting up and casting down will not give the required identity, whenever \( C_k \prec C_i \) and \( X \) is valid:

\[
X.\text{oclIsTypeOf}(C_k) \text{ implies } X.\text{oclAsType}(C_i).\text{oclAsType}(C_k) \equiv X
\]

To overcome this limitation, we introduce an auxiliary type \( C_{\text{ext}} \) for class type extension; together, they were inductively defined for a given class diagram:

Let \( C_i \) be a class with a possibly empty set of subclasses \( \{C_{j1}, \ldots, C_{jm}\} \).

- Then the class type extension \( C_{\text{ext}} \) associated to \( C_i \) is \( A_{i1} \times \cdots \times A_{in} \times (C_{j1,\text{ext}} + \cdots + C_{jm,\text{ext}}) \) where \( A_{ik} \) ranges over the local attribute types of \( C_i \) and \( C_{j,\text{ext}} \) ranges over all class type extensions of the subclass \( C_j \) of \( C_i \).
- Then the class type for \( C_i \) is \( \text{oid} \times A_{i1} \times \cdots \times A_{in} \times (C_{j1,\text{ext}} + \cdots + C_{jm,\text{ext}}) \) where \( A_{ik} \) ranges over the inherited and local attribute types of \( C_i \) and \( C_{j,\text{ext}} \) ranges over all class type extensions of the subclass \( C_j \) of \( C_i \).

Example instances of this scheme—outlining a compiler—can be found in \([\text{Chapter 4}]\) and \([\text{Chapter 5}]\).

This construction can not be done in HOL itself since it involves quantifications and iterations over the “set of class-types”; rather, it is a meta-level construction. Technically, this means that we need a compiler to be done in SML on the syntactic “meta-model”-level of a class model.

With respect to our semantic construction here, which above all means is intended to be type-safe, this has the following consequences:
• there is a generic theory of states, which must be formulated independently from a concrete object universe,
• there is a principle of translation (captured by the inductive scheme for class type extensions and class types above) that converts a given class model into an concrete object universe,
• there are fixed principles that allow to derive the semantic theory of any concrete object universe, called the object-oriented datatype theory.

We will work out concrete examples for the construction of the object-universes in Chapter 4 and Chapter 5 and the derivation of the respective datatype theories. While an automatization is clearly possible and desirable for concrete applications of Featherweight OCL, we consider this out of the scope of this document which has a focus on the semantic construction and its presentation.

Denotational Semantics of Accessors on Objects and Associations

Our choice to use a shallow embedding of OCL in HOL and, thus having an injective mapping from OCL types to HOL types, results in type-safety of Featherweight OCL. Arguments and results of accessors are based on type-safe object representations and not oid’s. This implies the following scheme for an accessor:

• The evaluation and extraction phase. If the argument evaluation results in an object representation, the oid is extracted, if not, exceptional cases like invalid are reported.
• The de-referentiation phase. The oid is interpreted in the pre- or post-state, the resulting object is cast to the expected format. The exceptional case of non-existence in this state must be treated.
• The selection phase. The corresponding attribute is extracted from the object representation.
• The re-construction phase. The resulting value has to be embedded in the adequate HOL type. If an attribute has the type of an object (not value), it is represented by an optional (set of) oid, which must be converted via de-referentiation in one of the states to produce an object representation again. The exceptional case of non-existence in this state must be treated.

The first phase directly translates into the following formalization:

\[
\text{definition eval\_extract } X f = (\lambda \tau. \text{case } X \tau \text{ of } \bot \Rightarrow \text{invalid } \tau \quad \text{exception} \\
|_{\downarrow} \Rightarrow \text{invalid } \tau \\
|_{\uparrow_\text{obj}_\downarrow} \Rightarrow f (\text{oid\_of } \text{obj} \tau)
\] (0.19)

For each class \( C \), we introduce the de-referentiation phase of this form:

\[
\text{definition deref\_oid\_of } C \text{ fst\_snd } f \text{ oid } = (\lambda \tau. \text{case } (\text{heap (fst\_snd } \tau)) \text{ oid of } \\
|_{\text{in}_C \text{ obj}_\downarrow} \Rightarrow f \text{ obj } \tau \\
|_{\_} \Rightarrow \text{invalid } \tau
\] (0.20)

The operation yields undefined if the oid is uninterpretable in the state or referencing an object representation not conforming to the expected type.

We turn to the selection phase: for each class \( C \) in the class model with at least one attribute, and each attribute \( a \) in this class, we introduce the selection phase of this form:

\[
\text{definition select}_a \ f = (\lambda \text{ mk}_C \text{ oid } \cdots \bot \cdots C_{\text{ext}} \Rightarrow \text{null} \\
|_{\text{mk}_C \text{ oid } \cdots \_a_\downarrow \cdots C_{\text{ext}} \Rightarrow f (\lambda \_x_\downarrow \text{ ext}_x \downarrow a)}
\] (0.21)

33
This works for definitions of basic values as well as for object references in which the \( a \) is of type \( \text{oid} \). To increase readability, we introduce the functions:

\[
\begin{align*}
\text{definition} & \quad \text{in}_\text{pre}_\text{state} = \text{fst} & \text{first component} \\
\text{definition} & \quad \text{in}_\text{post}_\text{state} = \text{snd} & \text{second component} \\
\text{definition} & \quad \text{reconst}_\text{basetype} = \text{id} & \text{identity function}
\end{align*}
\]

Let \( \_ . \text{getBase} \) be an accessor of class \( C \) yielding a value of base-type \( A_{\text{base}} \). Then its definition is of the form:

\[
\begin{align*}
\text{definition} & \quad \_ . \text{getBase} :: C \Rightarrow A_{\text{base}} \\
\text{where} & \quad X . \text{getBase} = \text{eval}_\text{extract} X (\text{deref}_\text{oid}_C \text{ in } \text{post}_\text{state}) \\
& \quad (\text{select}_\text{getBase} \text{reconst}_\text{basetype})
\end{align*}
\]

Let \( \_ . \text{getObject} \) be an accessor of class \( C \) yielding a value of object-type \( A_{\text{object}} \). Then its definition is of the form:

\[
\begin{align*}
\text{definition} & \quad \_ . \text{getObject} :: C \Rightarrow A_{\text{object}} \\
\text{where} & \quad X . \text{getObject} = \text{eval}_\text{extract} X (\text{deref}_\text{oid}_C \text{ in } \text{post}_\text{state}) \\
& \quad (\text{select}_\text{getObject} (\text{deref}_\text{oid}_C \text{ in } \text{post}_\text{state}))
\end{align*}
\]

The variant for an accessor yielding a collection is omitted here; its construction follows by the application of the principles of the former two. The respective variants \( \_ . a @\text{pre} \) were produced when \( \text{in}_\text{post}_\text{state} \) is replaced by \( \text{in}_\text{pre}_\text{state} \).

Examples for the construction of accessors via associations can be found in Section 4.8, the construction of accessors via attributes in Section 5.8. The construction of casts and type tests \( \Rightarrow \text{oclIsTypeOf()} \) and \( \Rightarrow \text{oclIsKindOf()} \) is similarly.

In the following, we discuss the role of multiplicities on the types of the accessors. Depending on the specified multiplicity, the evaluation of an attribute can yield just a value (multiplicity \( 0..1 \) or \( 1 \)) or a collection type like \( \text{Set} \) or \( \text{Sequence} \) of values (otherwise). A multiplicity defines a lower bound as well as a possibly infinite upper bound on the cardinality of the attribute’s values.

**Single-Valued Attributes** If the upper bound specified by the attribute’s multiplicity is one, then an evaluation of the attribute yields a single value. Thus, the evaluation result is not a collection. If the lower bound specified by the multiplicity is zero, the evaluation is not required to yield a non-null value. In this case an evaluation of the attribute can return \( \text{null} \) to indicate an absence of value.

To facilitate accessing attributes with multiplicity \( 0..1 \), the OCL standard states that single values can be used as sets by calling collection operations on them. This implicit conversion of a value to a \( \text{Set} \) is not defined by the standard. We argue that the resulting set cannot be constructed the same way as when evaluating a \( \text{Set} \) literal. Otherwise, \( \text{null} \) would be mapped to the singleton set containing \( \text{null} \), but the standard demands that the resulting set is empty in this case. The conversion should instead be defined as follows:

\[
\text{context } \text{OclAny} :: \text{asSet}():T \\
\text{post: if self = null then result = Set{}} \\
\text{else result = Set{self} endif}
\]

**Collection-Valued Attributes** If the upper bound specified by the attribute’s multiplicity is larger than one, then an evaluation of the attribute yields a collection of values. This raises the question whether \( \text{null} \) can belong to this collection. The OCL standard states that \( \text{null} \) can be owned by collections. However, if an attribute can evaluate to a collection containing \( \text{null} \), it is not clear how multiplicity constraints should be interpreted for this attribute. The question arises whether the \( \text{null} \) element should be counted or not when determining the cardinality of the collection. Recall that \( \text{null} \) denotes the absence of value in the case of a cardinality upper bound of one, so we would assume that
null is not counted. On the other hand, the operation size defined for collections in OCL does count null.

We propose to resolve this dilemma by regarding multiplicities as optional. This point of view complies with the UML standard, that does not require lower and upper bounds to be defined for multiplicities. In case a multiplicity is specified for an attribute, i.e., a lower and an upper bound are provided, we require for any collection the attribute evaluates to a collection not containing null. This allows for a straightforward interpretation of the multiplicity constraint. If bounds are not provided for an attribute, we consider the attribute values to not be restricted in any way. Because in particular the cardinality of the attribute’s values is not bounded, the result of an evaluation of the attribute is of collection type. As the range of values that the attribute can assume is not restricted, the attribute can evaluate to a collection containing null. The attribute can also evaluate to invalid. Allowing multiplicities to be optional in this way gives the modeler the freedom to define attributes that can assume the full ranges of values provided by their types. However, we do not permit the omission of multiplicities for association ends, since the values of association ends are not only restricted by multiplicities, but also by other constraints enforcing the semantics of associations. Hence, the values of association ends cannot be completely unrestricted.

The Precise Meaning of Multiplicity Constraints

We are now ready to define the meaning of multiplicity constraints by giving equivalent invariants written in OCL. Let a be an attribute of a class C with a multiplicity specifying a lower bound m and an upper bound n. Then we can define the multiplicity constraint on the values of attribute a to be equivalent to the following invariants written in OCL:

\[
\begin{align*}
\text{context } C \text{ inv lowerBound: } a\rightarrow \text{ size() } &\geq m \\
\text{inv upperBound: } a\rightarrow \text{ size() } &\leq n \\
\text{inv notNull: not } a\rightarrow \text{ includes(null)}
\end{align*}
\]

If the upper bound n is infinite, the second invariant is omitted. For the definition of these invariants we are making use of the conversion of single values to sets described in Section 0.3.6. If \(n \leq 1\), the attribute a evaluates to a single value, which is then converted to a Set on which the size operation is called.

If a value of the attribute a includes a reference to a non-existent object, the attribute call evaluates to invalid. As a result, the entire expressions evaluate to invalid, and the invariants are not satisfied. Thus, references to non-existent objects are ruled out by these invariants. We believe that this result is appropriate, since we argue that the presence of such references in a system state is usually not intended and likely to be the result of an error. If the modeler wishes to allow references to non-existent objects, she can make use of the possibility described above to omit the multiplicity.

Logic Properties of Class-Models

In this section, we assume to be \(C_z, C_i, C_j \in C\) and \(C_i < C_j\). Let \(C_z\) be a smallest element with respect to the class hierarchy \(_<\). The operations induced from a class-model have the following properties:

\[
\begin{align*}
\tau \models X \cdot \text{oclAsType}(C_i) &\triangleq X \\
\tau \models \text{invalid} \cdot \text{oclAsType}(C_i) &\triangleq \text{invalid} \\
\tau \models \text{null} \cdot \text{oclAsType}(C_i) &\triangleq \text{null} \\
\tau \models ((X :: C_i) \cdot \text{oclAsType}(C_j) \cdot \text{oclAsType}(C_i)) &\triangleq X \\
\tau \models X \cdot \text{oclAsType}(C_j) \cdot \text{oclAsType}(C_i) &\triangleq X \\
\tau \models (X :: \text{OclAny}) \cdot \text{oclAsType}(\text{OclAny}) &\triangleq X \\
\tau \models v(X :: C_i) \implies \tau \models (X \cdot \text{oclIsTypeOf}(C_i)) \implies (X \cdot \text{oclAsType}(C_j) \cdot \text{oclAsType}(C_i)) \triangleq X
\end{align*}
\]

\(^{14}\)We are however aware that a well-formedness rule of the UML standard does define a default bound of one in case a lower or upper bound is not specified.
\[ \tau \models v(X :: C_i) \implies \tau \models X . oclIsTypeOf(C_i) \] implies \( (X . oclAsType(C_i) . oclAsType(C_i)) \models X \)

\[ \tau \models \delta X \implies \tau \models X . oclAsType(C_i) . oclAsType(C_i) \models X \]

\[ \tau \models vX \implies \tau \models X . oclIsTypeOf(C_i) \implies X . oclAsType(C_i) . oclAsType(C_i) \models X \]

\[ \tau \models X . oclIsTypeOf(C_i) \implies \tau \models \delta X \implies \tau \models \text{not}(vX . oclAsType(C_i)) \]

\[ \tau \models \text{invalid} . oclIsTypeOf(C_i) \models \text{invalid} \]

\[ \tau \models \text{null} . oclIsTypeOf(C_i) \models \text{true} \]

\[ \tau \models \text{Person} . allInstances() -> \text{forall}(X | X . oclIsTypeOf(C_i)) \]

\[ \tau \models \text{Person} . allInstances@pre() -> \text{forall}(X | X . oclIsTypeOf(C_i)) \]

\[ \tau \models \text{Person} . allInstances() -> \text{forall}(X | X . oclIsKindOf(C_i)) \]

\[ \tau \models (X :: C_i) . oclIsTypeOf(C_i) \implies \tau \models (X :: C_i) . oclIsKindOf(C_i) \]

\[ (\tau \models (X :: C_i) \models X) = (\tau \models \text{if} vX \text{then true else invalid endif}) \]

\[ \tau \models (X :: C_i) \models Y \implies \tau \models Y \models Z \implies \tau \models X \models Z \]

**Algebraic Properties of the Class-Models**

In this section, we assume to be \( C_i, C_j \in C \) and \( C_i < C_j \). The operations induced from a class-model have the following properties:

\[
\begin{align*}
\text{invalid} . oclIsTypeOf(C_i) & = \text{invalid} & \text{null} . oclIsTypeOf(C_i) & = \text{true} \\
\text{invalid} . oclIsKindOf(C_i) & = \text{invalid} & \text{null} . oclIsKindOf(C_i) & = \text{true} \\
(X :: C_i) . oclAsType(C_i) = X & \implies \text{invalid} . oclAsType(C_i) = \text{invalid} \\
\text{null} . oclAsType(C_i) = \text{null} & \implies (X :: C_i) . oclAsType(C_i) . oclAsType(C_i) = X \\
(X :: C_i) \models X & = \text{if} vX \text{then true else invalid endif}
\end{align*}
\]

With respect to attributes \_.a or \_.a@pre and role-ends \_.r or \_.r@pre we have

\[
\begin{align*}
\text{invalid} . a & = \text{invalid} & \text{null} . a & = \text{invalid} \\
\text{invalid} . a@pre & = \text{invalid} & \text{null} . a@pre & = \text{invalid} \\
\text{invalid} . r & = \text{invalid} & \text{null} . r & = \text{invalid} \\
\text{invalid} . r@pre & = \text{invalid} & \text{null} . r@pre & = \text{invalid}
\end{align*}
\]

**Other Operations on States**

Defining \_.allInstances() is straight-forward; the only difference is the property \( T . \text{allInstances}() -> \text{excludes} (\text{null}) \) which is a consequence of the fact that \text{null}'s are values and do not “live” in the state. OCL semantics admits states with “dangling references;”; it is the semantics of accessors or roles which maps these references to \text{invalid}, which makes it possible to rule out these situations in invariants.

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. This framing problem is well-known (one of the suggested solutions is [23]). We define

\[
(S : \text{Set(OclAny)}) -> \text{oclIsModifiedOnly}() : \text{Boolean}
\]

where \( S \) is a set of object representations, encoding a set of oid’s. The semantics of this operator is defined such that for any object whose oid is not represented in \( S \) and that is defined in pre and post
state, the corresponding object representation will not change in the state transition. A simplified presentation is as follows:

\[
I[X\rightarrow\text{oclIsModifiedOnly}()]\sigma,\sigma' = \begin{cases} \bot & \text{if } X' = \bot \lor \text{null} \in X' \\ \forall i \in M. \sigma_i = \sigma'_i & \text{otherwise.} \end{cases}
\]

where \(X' = I[X]\sigma,\sigma'\) and \(M = (\text{dom } \sigma \cap \text{dom } \sigma') \setminus \{\text{OidOf } x \mid x \in X'\}\). Thus, if we require in a postcondition \(\text{Set}{} \rightarrow \text{oclIsModifiedOnly}()\) and exclude via \(_.\text{oclIsNew}()\) and \(_.\text{oclIsDeleted}()\) the existence of new or deleted objects, the operation is a query in the sense of the OCL standard, i.e., the \text{isQuery} property is true. So, whenever we have \(\tau \models X\rightarrow\text{excluding}(s.a)\rightarrow\text{oclIsModifiedOnly}()\) and \(\tau \models X\rightarrow\text{forall}(x\not\equiv x.s.a))\), we can infer that \(\tau \models s.a \triangleq s.a@\text{pre}\).

0.3.7. Data Invariants

Since the present OCL semantics uses one interpretation function\(^{15}\) we express the effect of OCL terms occurring in preconditions and invariants by a syntactic transformation \_pre which replaces:

- all accessor functions \_a from the class model \(a \in \text{Attrib}(C)\) by their counterparts \_i@\text{pre}. For example, \((\text{self}.\text{salary} > 500)\)_pre is transformed to \((\text{self}.\text{salary}@\text{pre} > 500)\).

- all role accessor functions \_.rn from or \_.rn to within the class model (i.e., \((id, \text{rn}_\text{from}, \text{rn}_\text{to}) \in \text{Assoc}(C_i,C_j)\)) were replaced by their counterparts \_.rn@\text{pre}. For example, \((\text{self}.\text{boss} = \text{null})\)_pre is transformed to \(\text{self}.\text{boss}@\text{pre} = \text{null}\).

- The operation \_\_.allInstances() is also substituted by its \_\text{pre} counterpart.

Thus, we formulate the semantics of the invariant specification as follows:

\[
I[\text{context } c : C_i \text{ inv } n : \phi(c)]\tau \\
\tau \models (C_i.\text{allInstances}()\rightarrow\text{forall}(x|\phi(x))) \land (0.25) \\
\tau \models (C_i.\text{allInstances}()\rightarrow\text{forall}(x|\phi(x)))_\text{pre}
\]

Recall that expressions containing \_\text{pre} constructs in invariants or preconditions are syntactically forbidden; thus, mixed forms cannot arise.

0.3.8. Operation Contracts

Since operations have strict semantics in OCL, we have to distinguish for a specification of an operation \(op\) with the arguments \(a_1, \ldots, a_n\) the two cases where all arguments are valid and additionally, \text{self} is non-null (i.e., it must be defined), or not. In former case, a method call can be replaced by a \text{result} that satisfies the contract, in the latter case the result is invalid. This is reflected by the following definition of the contract semantics:

\[
I[\text{context } C :: \text{op}(a_1, \ldots, a_n) : T] \\
\text{pre } \phi(\text{self}, a_1, \ldots, a_n) \\
\text{post } \psi(\text{self}, a_1, \ldots, a_n, \text{result}) \equiv \lambda s, x_1, \ldots, x_n, \tau. \\
\text{if } \tau \models \partial s \land \tau \models \nu x_1 \land \ldots \land \tau \models \nu x_n \\
\text{then SOME result. } \tau \models \phi(s, x_1, \ldots, x_n)_\text{pre} \\
\text{else } \bot \ \\
(0.26)
\]

\(^{15}\)This has been handled differently in previous versions of the Annex A.
where SOME \( x \). \( P(x) \) is the Hilbert-Choice Operator that chooses an arbitrary element satisfying \( P \); if such an element does not exist, it chooses an arbitrary one\(^{16}\). Thus, using the Hilbert-Choice Operator, a contract can be associated to a function definition:

\[
\text{f}_\text{op} \equiv I[\text{context } C :: \text{op}(a_1, \ldots, a_n) : T \ldots]
\]

provided that neither \( \phi \) nor \( \psi \) contain recursive method calls of \( \text{op} \). In the case of a query operation (i.e., \( \tau \) must have the form: \((\sigma, \sigma)\), which means that query operations do not change the state; c.f. oclIsModifiedOnly() in Section 0.3.6), this constraint can be relaxed: the above equation is then stated as "axiom." Note however, that the consistency of the overall theory is for recursive query contracts left to the user (it can be shown, for example, by a proof of termination, i.e., by showing that all recursive calls were applied to argument vectors that are smaller wrt. a well-founded ordering). Under this condition, an \( \text{f}_\text{op} \) resulting from recursive query operations can be used safely inside pre- and post-conditions of other contracts.

For the general case of a user-defined contract, the following rule can be established that reduces the proof of a property \( E \) over a method call \( \text{f}_\text{op} \) to a proof of \( E(\text{res}) \) (where \( \text{res} \) must be one of the values that satisfy the post-condition \( \psi \)):

\[
\begin{align*}
\tau \models \psi \text{ self } a_1 \ldots a_n \ \text{res} \\
& \vdots \\
\tau \models E(\text{res}) \\
\tau \models E(f_{\text{op}} \text{ self } a_1 \ldots a_n)
\end{align*}
\]

under the conditions:

- \( E \) must be an OCL term and
- \( \text{self} \) must be defined, and the arguments valid in \( \tau \):
  \( \tau \models \partial \text{ self } \land \tau \models v \ a_1 \ldots \land \tau \models v \ a_n \)
- the post-condition must be satisfiable ("the operation must be implementable"): \( \exists \text{res}. \ \tau \models \psi \text{ self } a_1 \ldots a_n \ \text{res} \).

For the special case of a (recursive) query method, this rule can be specialized to the following executable "unfolding principle":

\[
\tau \models \phi \text{ self } a_1 \ldots a_n \\
(\tau \models E(f_{\text{op}} \text{ self } a_1 \ldots a_n)) = e(\tau \models E(BODY \text{ self } a_1 \ldots a_n))
\]

where

- \( E \) must be an OCL term.
- \( \text{self} \) must be defined, and the arguments valid in \( \tau \):
  \( \tau \models \partial \text{ self } \land \tau \models v \ a_1 \ldots \land \tau \models v \ a_n \)
- the postcondition \( \psi \text{ self } a_1 \ldots a_n \ \text{result} \) must be decomposable into:
  \( \psi' \text{ self } a_1 \ldots a_n \) and \( \text{result} \equiv BODY \text{ self } a_1 \ldots a_n \).

Currently, Featherweight OCL neither supports overloading nor overriding for user-defined operations: the Featherweight OCL compiler needs to be extended to generate pre-conditions that constrain the classes on which an overridden function can be called as well as the dispatch order. This construction, overall, is similar to the virtual function table that, e.g., is generated by C++ compilers. Moreover, to avoid logical contradictions (inconsistencies) between different instances of an overridden operation, the user has to prove Liskov’s principle for these situations: pre-conditions of the superclass must imply pre-conditions of the subclass, and post-conditions of a subclass must imply post-conditions of the superclass.

\(^{16}\)In HOL, the Hilbert-Choice operator is a first-class element of the logical language.
1. Formalization I: OCL Types and Core Definitions

theory UML-Types
imports HOL.Transcendental
keywords Assert :: thy-decl
and Assert-local :: thy-decl
begin

1.1. Preliminaries

1.1.1. Notations for the Option Type

First of all, we will use a more compact notation for the library option type which occur all over in our definitions and which will make the presentation more like a textbook:

no-notation ceiling (⌜-⌝)
no-notation floor (⌞-⌟)
type-notation option (⌜-⌟)
notation Some (⌜-⌟)
notation None (⊥)

These commands introduce an alternative, more compact notation for the type constructor ⟨′α⟩⊥, namely ⟨′α⟩⊥. Furthermore, the constructors ⌜X⌟ and ⊥ of the type ⟨′α⟩⊥, namely X and ⊥.

The following function (corresponding to the in the Isabelle/HOL library) is defined as the inverse of the injection Some.

fun drop :: ′a option ⇒ ′a (⌜-⌟)
where drop-lift[simp]: ⌜v⌟ = v

The definitions for the constants and operations based on functions will be geared towards a format that Isabelle can check to be a “conservative” (i.e., logically safe) axiomatic definition. By introducing an explicit interpretation function (which happens to be defined just as the identity since we are using a shallow embedding of OCL into HOL), all these definitions can be rewritten into the conventional semantic textbook format. To say it in other words: The interpretation function Sem as defined below is just a textual marker for presentation purposes, i.e. intended for readers used to conventional textbook notations on semantics. Since we use a “shallow embedding”, i.e. since we represent the syntax of OCL directly by HOL constants, the interpretation function is semantically not only superfluous, but from an Isabelle perspective strictly in the way for certain consistency checks performed by the definitional packages.

definition Sem :: ′a ⇒ ′a (I[]=)
where I[x] ≡ x

1.1.2. Common Infrastructure for all OCL Types

In order to have the possibility to nest collection types, such that we can give semantics to expressions like Set{Set{2},null}, it is necessary to introduce a uniform interface for types having the invalid (≡ bottom) element. The reason is that we impose a data-invariant on raw-collection types_code which assures that the invalid element is not allowed inside the collection; all raw-collections of this form
were identified with the invalid element itself. The construction requires that the new collection type
is not comparable with the raw-types (consisting of nested option type constructions), such that the
data-invariant must be expressed in terms of the interface. In a second step, our base-types will be
shown to be instances of this interface.

This uniform interface consists in a type class requiring the existence of a bot and a null element.
The construction proceeds by abstracting the null (defined by \( \bot \) on \( 'a \) option option) to a null
element, which may have an arbitrary semantic structure, and an undefinedness element \( \bot \) to an abstract
undefinedness element bot (also written \( \bot \) whenever no confusion arises). As a consequence, it is
necessary to redefine the notions of invalid, defined, valuation etc. on top of this interface.

This interface consists in two abstract type classes bot and null for the class of all types comprising
a bot and a distinct null element.

```plaintext
class bot =
  fixes bot :: 'a
  assumes nonEmpty : \( \exists \ x. \ x \neq \bot \)

class null = bot +
  fixes null :: 'a
  assumes null-is-valid : null \neq \bot
```

### 1.1.3. Accommodation of Basic Types to the Abstract Interface

In the following it is shown that the “option-option” type is in fact in the null class and that function
spaces over these classes again “live” in these classes. This motivates the default construction of the
semantic domain for the basic types (Boolean, Integer, Real, ...).

```plaintext
instantiation option :: (type)bot
begin
  definition bot-option-def: (bot::'a option) \equiv (None::'a option)
  instance ⟨proof⟩
end

instantiation option :: (bot)null
begin
  definition null-option-def: (null::'a::bot option) \equiv (\bot)
  instance ⟨proof⟩
end

instantiation fun :: (type,bot) bot
begin
  definition bot-fun-def: bot \equiv (\lambda x. bot)
  instance ⟨proof⟩
end

instantiation fun :: (type,null) null
begin
  definition null-fun-def: (null::'a \Rightarrow 'b::null) \equiv (\lambda x. null)
  instance ⟨proof⟩
end
```

A trivial consequence of this adaption of the interface is that abstract and concrete versions of null
are the same on base types (as could be expected).
1.1.4. The Common Infrastructure of Object Types (Class Types) and States.

Recall that OCL is a textual extension of the UML; in particular, we use OCL as means to annotate UML class models. Thus, OCL inherits a notion of *data* in the UML: UML class models provide classes, inheritance, types of objects, and subtypes connecting them along the inheritance hierarchy.

For the moment, we formalize the most common notions of objects, in particular the existance of object-identifiers (oid) for each object under which it can be referenced in a *state*.

*type-synonym* \( \text{oid} = \text{nat} \)

We refrained from the alternative:

*type-synonym* \( \text{oid} = \text{ind} \)

which is slightly more abstract but non-executable.

*States* in UML/OCL are a pair of

- a partial map from oid’s to elements of an *object universe*, i.e. the set of all possible object representations.
- and an oid-indexed family of *associations*, i.e. finite relations between objects living in a state.

These relations can be n-ary which we model by nested lists.

For the moment we do not have to describe the concrete structure of the object universe and denote it by the polymorphic variable \( \forall \).

*record* \( \langle \forall \rangle \text{state} =
\begin{align*}
\text{heap} & : \text{oid} \to \forall \\
\text{assocs} & : \text{oid} \to ((\text{oid list}) \text{ list}) \text{ list}
\end{align*}

In general, OCL operations are functions implicitly depending on a pair of pre- and post-state, i.e. *state transitions*. Since this will be reflected in our representation of OCL Types within HOL, we need to introduce the foundational concept of an object id (oid), which is just some infinite set, and some abstract notion of state.

*type-synonym* \( \langle \forall \rangle \text{st} = \forall \text{ state} \times \forall \text{ state} \)

We will require for all objects that there is a function that projects the oid of an object in the state (we will settle the question how to define this function later). We will use the Isabelle type class mechanism \[21\] to capture this:

*class* \( \text{object} = \text{fixes oid-of :: } \text{a ⇒ oid} \)

Thus, if needed, we can constrain the object universe to objects by adding the following type class constraint:

*typ* \( \forall \text{ :: object} \)

The major instance needed are instances constructed over options: once an object, options of objects are also objects.

*instantiation* \( \text{option :: (object)object} \)

begin
\begin{align*}
\text{definition oid-of-option-def: } \text{oid-of x} &= \text{oid-of (the x)} \\
\text{instance (proof)}
\end{align*}

end

1.1.5. Common Infrastructure for all OCL Types (II): Valuations as OCL Types

Since OCL operations in general depend on pre- and post-states, we will represent OCL types as *functions* from pre- and post-state to some HOL raw-type that contains exactly the data in the OCL type — see below. This gives rise to the idea that we represent OCL types by *Valuations*. 

41
Valuations are functions from a state pair (built upon data universe $\mathcal{A}$) to an arbitrary null-type (i.e., containing at least a distinguished null and invalid element).

**type-synonym** $(\mathcal{A},'\alpha) \text{ val} = \mathcal{A} \text{ st} \Rightarrow '\alpha :: \text{null}$

The definitions for the constants and operations based on valuations will be geared towards a format that Isabelle can check to be a “conservative” (i.e., logically safe) axiomatic definition. By introducing an explicit interpretation function (which happens to be defined just as the identity since we are using a shallow embedding of OCL into HOL), all these definitions can be rewritten into the conventional semantic textbook format as follows:

### 1.1.6. The fundamental constants 'invalid' and 'null' in all OCL Types

As a consequence of semantic domain definition, any OCL type will have the two semantic constants invalid (for exceptional, aborted computation) and null:

**definition** invalid :: $(\mathcal{A},'\alpha :: \text{bot}) \text{ val}$

**where**

invalid $\equiv \lambda \tau. \text{bot}$

This conservative Isabelle definition of the polymorphic constant invalid is equivalent with the textbook definition:

**lemma** textbook-invalid: $\mathcal{I}[[\text{invalid}]\tau = \text{bot}$

(proof)

Note that the definition:

**definition** null :: $'('\mathcal{A},'\alpha :: \text{null}) \text{ val'}$

**where**

null $\equiv \lambda \tau. \text{null}$

is not necessary since we defined the entire function space over null types again as null-types; the crucial definition is $\text{null} \equiv \lambda x. \text{null}$. Thus, the polymorphic constant null is simply the result of a general type class construction. Nevertheless, we can derive the semantic textbook definition for the OCL null constant based on the abstract null:

**lemma** textbook-null-fun: $\mathcal{I}[[\text{null}::(\mathcal{A},'\alpha :: \text{null}) \text{ val}]]\tau = (\text{null}::('\alpha :: \text{null}))$

(proof)

### 1.2. Basic OCL Value Types

The structure of this section roughly follows the structure of Chapter 11 of the OCL standard [32], which introduces the OCL Library.

The semantic domain of the (basic) boolean type is now defined as the Standard: the space of valuation to $\langle\langle\text{bool}\rangle\rangle_\bot$, i.e. the Boolean base type:

**type-synonym** Booleanbase = bool option option

**type-synonym** $(\mathcal{A})\text{ Boolean} = (\mathcal{A},\text{Booleanbase}) \text{ val}$

Because of the previous class definitions, Isabelle type-inference establishes that $\mathcal{A} \text{ Boolean}$ lives actually both in the type class UML-Types,bot-class,bot; this type is sufficiently rich to contain at least these two elements. Analogously we build:

**type-synonym** Integerbase = int option option

**type-synonym** $(\mathcal{A})\text{ Integer} = (\mathcal{A},\text{Integerbase}) \text{ val}$

**type-synonym** Stringbase = string option option

**type-synonym** $(\mathcal{A})\text{ String} = (\mathcal{A},\text{Stringbase}) \text{ val}$

**type-synonym** Realbase = real option option

**type-synonym** $(\mathcal{A})\text{ Real} = (\mathcal{A},\text{Realbase}) \text{ val}$
Since \textit{Real} is again a basic type, we define its semantic domain as the valuations over \textit{real option option} — i.e. the mathematical type of real numbers. The HOL-theory for \textit{real} “Real” transcendental numbers such as $\pi$ and $e$ as well as infrastructure to reason over infinite convergent Cauchy-sequences (it is thus possible, in principle, to reason in Featherweight OCL that the sum of inverted two-s exponentials is actually 2.

If needed, a code-generator to compile \textit{Real} to floating-point numbers can be added; this allows for mapping reals to an efficient machine representation; of course, this feature would be logically unsafe.

For technical reasons related to the Isabelle type inference for type-classes (we don’t get the properties in the right order that class instantiation provides them, if we would follow the previous scheme), we give a slightly atypic definition:

```isar
typedef Void_base = 
  \{X :: unit option option. X = \bot \lor X = null \} \langle\text{proof}\rangle
```

```isar
type-synonym (\forall) Void = (\forall, Void_base) val
```

### 1.3. Some OCL Collection Types

For the semantic construction of the collection types, we have two goals:

1. we want the types to be \textit{fully abstract}, i.e., the type should not contain junk-elements that are not representable by OCL expressions, and
2. we want a possibility to nest collection types (so, we want the potential of talking about \textit{Set(Set(Set(Pairs(X,Y))))}).

The former principle rules out the option to define 'α \textit{Set} just by (\forall, (\alpha \textit{ option option}) \textit{set}) \textit{val}. This would allow sets to contain junk elements such as \{⊥\} which we need to identify with undefinedness itself. Abandoning fully abstractness of rules would later on produce all sorts of problems when quantifying over the elements of a type. However, if we build an own type, then it must conform to our abstract interface in order to have nested types: arguments of type-constructors must conform to our abstract interface, and the result type too.

#### 1.3.1. The Construction of the Pair Type (Tuples)

The core of an own type construction is done via a type definition which provides the base-type (\langle α, β \rangle Pair\textsubscript{base}). It is shown that this type “fits” indeed into the abstract type interface discussed in the previous section.

```isar
typedef (overloaded) \langle α, β \rangle Pair\textsubscript{base} = \{X :: (\langle α::null \times β::null \rangle \textit{option option}. X = \bot \lor X = null \lor (\text{fst}(X) \neq \bot \land \text{snd}(X) \neq \bot))\} \langle\text{proof}\rangle
```

We “carve” out from the concrete type (\langle α × β \rangle)\bot the new fully abstract type, which will not contain representations like \langle⊥, a\rangle or \langle b, ⊥\rangle. The type constructor Pair\{x,y\} to be defined later will identify these with \textit{invalid}.

```isar
instantiation Pair\textsubscript{base} :: (null,null)bot
begin
  definition bot-Pair\textsubscript{base}-def: (bot-class.bot :: \langle α::null, β::null \rangle Pair\textsubscript{base}) \equiv Abs-Pair\textsubscript{base} None
  instance (\text{proof})
end

instantiation Pair\textsubscript{base} :: (null,null)null
begin
  definition null-Pair\textsubscript{base}-def: (null :: \langle α::null, β::null \rangle Pair\textsubscript{base}) \equiv Abs-Pair\textsubscript{base} None
```

43
... and lifting this type to the format of a valuation gives us:

\[
\text{type-synonym } \, (\forall \alpha, \beta \, \text{Pair} = (\forall \alpha, \beta \, \text{Pair_base}) \, \text{val}
\]

\[
\text{type-notation } \, \text{Pair_base} (\text{Pair}(\ldots))
\]

### 1.3.2. The Construction of the Set Type

The core of an own type construction is done via a type definition which provides the raw-type \(\alpha \, \text{Set_base} \). It is shown that this type “fits” indeed into the abstract type interface discussed in the previous section. Note that we make no restriction whatsoever to finite sets; while with the standards type-constructors only finite sets can be denoted, there is the possibility to define in fact infinite type constructors in Featherweight OCL (c.f. Section 2.9.1).

\[
\text{typedef (overloaded) } \, \alpha \, \text{Set_base} = \{X :: (\alpha :: \text{null}) \, \text{set} \, \text{option} \, \text{option}. \, X = \text{bot} \lor X = \text{null} \lor (\forall x \in X. \, x \neq \text{bot})\}
\]

\[
\langle \text{proof} \rangle
\]

\[
\text{instantiation } \, \text{Set_base} :: (\text{null} \text{bot} \begin{\text{definition} \text{bot-Set_base-def} \, (\text{bot} :: (\alpha :: \text{null}) \, \text{Set_base} \equiv \text{Abs-Set_base None \end{definition}}
\]

\[
\langle \text{proof} \rangle
\]

\[
\text{instantiation } \, \text{Set_base} :: (\text{null} \text{null} \begin{\text{definition} \text{null-Set_base-def} \, (\text{null} :: (\alpha :: \text{null}) \, \text{Set_base} \equiv \text{Abs-Set_base \text{None}} \text{None}) \end{definition}}
\]

\[
\langle \text{proof} \rangle
\]

... and lifting this type to the format of a valuation gives us:

\[
\text{type-synonym } \, (\forall \alpha \, \text{Set} = (\forall \alpha \, \text{Set_base}) \, \text{val}
\]

\[
\text{type-notation } \, \text{Set_base} (\text{Set}(\ldots))
\]

### 1.3.3. The Construction of the Bag Type

The core of an own type construction is done via a type definition which provides the raw-type \(\alpha \, \text{Bag_base} \) based on multi-sets from the HOL library. As in Sets, it is shown that this type “fits” indeed into the abstract type interface discussed in the previous section, and as in sets, we make no restriction whatsoever to finite multi-sets; while with the standards type-constructors only finite sets can be denoted, there is the possibility to define in fact infinite type constructors in Featherweight OCL (c.f. Section 2.9.1). However, while several null elements are possible in a Bag, there can’t be no bottom (invalid) element in them.

\[
\text{typedef (overloaded) } \, \alpha \, \text{Bag_base} = \{X :: (\alpha :: \text{null} \Rightarrow \text{nat}) \, \text{option} \, \text{option}. \, X = \text{bot} \lor X = \text{null} \lor \forall X. \, \text{bot} = 0\}
\]

\[
\langle \text{proof} \rangle
\]

\[
\text{instantiation } \, \text{Bag_base} :: (\text{null} \text{bot} \begin{\text{definition} \text{bot-Bag_base-def} \, (\text{bot} :: (\alpha :: \text{null}) \, \text{Bag_base} \equiv \text{Abs-Bag_base None}) \end{definition}}
\]

\[
\langle \text{proof} \rangle
\]
1.3.4. The Construction of the Sequence Type

The core of an own type construction is done via a type definition which provides the base-type \( \alpha \) \text{Sequence}_{\text{base}}. It is shown that this type “fits” indeed into the abstract type interface discussed in the previous section.

```
typedef (overloaded) \( \alpha \) \text{Sequence}_{\text{base}} = \{ X::(\alpha::null) list option option.
\quad X = \text{bot} \lor X = \text{null} \lor (\forall x\in \text{set} \neg X. x \neq \text{bot}) \}
```

```
instantiation \text{Sequence}_{\text{base}} :: (null)\text{bot}
begin
  definition \( \text{bot-Sequence}_{\text{base}}-\text{def} \): (\text{bot}::(\alpha::null) \text{Sequence}_{\text{base}}) \equiv \text{Abs-Sequence}_{\text{base}} \text{None}
  instance (proof)
end
```

```
instance \text{Sequence}_{\text{base}} :: (null)\text{null}
begin
  definition \( \text{null-Sequence}_{\text{base}}-\text{def} \): (\text{null}::(\alpha::null) \text{Sequence}_{\text{base}}) \equiv \text{Abs-Sequence}_{\text{base}} \_ \text{None}
  instance (proof)
end
```

... and lifting this type to the format of a valuation gives us:

```
type-synonym \( (\forall, \alpha) \text{Bag} = (\forall, \alpha \text{Bag}_{\text{base}}) \text{val} 

type-notation \text{Bag}_{\text{base}} (\text{Bag}'(-'))
```

1.3.5. Discussion: The Representation of UML/OCL Types in Featherweight OCL

In the introduction, we mentioned that there is an “injective representation mapping” between the types of OCL and the types of Featherweight OCL (and its meta-language: HOL). This injectivity is at the heart of our representation technique — a so-called shallow embedding — and means: OCL types were mapped one-to-one to types in HOL, ruling out a resentment where everything is mapped on some common HOL-type, say “OCL-expression”, in which we would have to sort out the typing of OCL and its impact on the semantic representation function in an own, quite heavy side-calculus.

After the previous sections, we are now able to exemplify this representation as follows:
<table>
<thead>
<tr>
<th>OCL Type</th>
<th>HOL Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boolean</td>
<td>$\forall \text{Boolean}$</td>
</tr>
<tr>
<td>Boolean $\rightarrow$ Boolean</td>
<td>$\forall \text{Boolean} \Rightarrow \forall \text{Boolean}$</td>
</tr>
<tr>
<td>(Integer,Integer) $\rightarrow$ Boolean</td>
<td>$\forall \text{Integer} \Rightarrow \forall \text{Integer} \Rightarrow \forall \text{Boolean}$</td>
</tr>
<tr>
<td>Set(Integer)</td>
<td>$\left(\forall \text{Integer}_{\text{base}}\right) \text{Set}$</td>
</tr>
<tr>
<td>Set(Integer)$\rightarrow$ Real</td>
<td>$\left(\forall , \text{Integer}_{\text{base}}\right) \text{Set} \Rightarrow \forall \text{Real}$</td>
</tr>
<tr>
<td>Set(Pair(Integer,Boolean))</td>
<td>$\left(\forall , \text{Pair(Integer}<em>{\text{base}},\text{Boolean}</em>{\text{base}})\right) \text{Set}$</td>
</tr>
<tr>
<td>Set($\langle T\rangle$)</td>
<td>$\left(\forall , \langle \alpha \rangle \right) \text{Set}$</td>
</tr>
</tbody>
</table>

Table 1.1.: Correspondance between OCL types and HOL types

We do not formalize the representation map here; however, its principles are quite straight-forward:

1. cartesian products of arguments were curried,
2. constants of type $T$ were mapped to valuations over the HOL-type for $T$,
3. functions $T \rightarrow T'$ were mapped to functions in HOL, where $T$ and $T'$ were mapped to the valuations for them, and
4. the arguments of type constructors Set($T$) remain corresponding HOL base-types.

Note, furthermore, that our construction of “fully abstract types” (no junk, no confusion) assures that the logical equality to be defined in the next section works correctly and comes as element of the “lingua franca”, i.e. HOL.

⟨ML⟩
end
2. Formalization II: OCL Terms and Library Operations

theory UML-Logic
imports UML-Types
begin

2.1. The Operations of the Boolean Type and the OCL Logic

2.1.1. Basic Constants

lemma bot-Boolean-def : (bot::(∀)Boolean) = (λ τ.⊥)
⟨proof⟩

lemma null-Boolean-def : (null::(∀)Boolean) = (λ τ.⊥)
⟨proof⟩

definition true :: (∀)Boolean
where true ≡ (λ τ.⌜True⌝)

definition false :: (∀)Boolean
where false ≡ (λ τ.⌜False⌝)

lemma bool-split-0: X τ = invalid τ ∨ X τ = null τ ∨
X τ = true τ ∨ X τ = false τ
⟨proof⟩

lemma [simp]: false (a, b) = ┐False
⟨proof⟩

lemma [simp]: true (a, b) = ┐True
⟨proof⟩

lemma textbook-true: I[true] τ = ┐True
⟨proof⟩

lemma textbook-false: I[false] τ = ┐False
⟨proof⟩

2.1.2. Validity and Definedness

However, this has also the consequence that core concepts like definedness, validity and even cp have

have to be redefined on this type class:

definition valid :: (∀'a::null)val ⇒ (∀)Boolean (v - [100]100)
where v X ≡ λ τ. if X τ = bot τ then false τ else true τ
<table>
<thead>
<tr>
<th>Name</th>
<th>Theorem</th>
</tr>
</thead>
<tbody>
<tr>
<td>textbook-invalid</td>
<td>$I[invalid] \tau = \text{UML-Types.bot-class.bot}$</td>
</tr>
<tr>
<td>textbook-null-fun</td>
<td>$I[null] \tau = \text{null}$</td>
</tr>
<tr>
<td>textbook-true</td>
<td>$I[true] \tau = <em>{\omega}\text{True}</em>{\omega}$</td>
</tr>
<tr>
<td>textbook-false</td>
<td>$I[false] \tau = <em>{\omega}\text{False}</em>{\omega}$</td>
</tr>
</tbody>
</table>

Table 2.1.: Basic semantic constant definitions of the logic

<table>
<thead>
<tr>
<th>Name</th>
<th>Lemma</th>
</tr>
</thead>
<tbody>
<tr>
<td>textbook-defined</td>
<td>$\delta\ (\lambda \ X. \tau) \ = \ (\text{if }\delta\ (\text{if }X\ \tau = \text{bot} \ \tau \ \text{then} \ false \ \tau \ \text{else} \ true \ \tau) \ \text{then} \ false \ \tau \ \text{else} \ true \ \tau)$</td>
</tr>
<tr>
<td>textbook-valid</td>
<td>$\upsilon\ (\lambda \ X. \tau) \ = \ (\text{if }\upsilon\ (\text{if }X\ \tau = \text{bot} \ \tau \ \text{then} \ false \ \tau \ \text{else} \ true \ \tau)$</td>
</tr>
</tbody>
</table>

The generalized definitions of invalid and definedness have the same properties as the old ones:

<table>
<thead>
<tr>
<th>Name</th>
<th>Lemma</th>
</tr>
</thead>
<tbody>
<tr>
<td>textbook-defined1</td>
<td>$\delta\ invalid = false$</td>
</tr>
<tr>
<td>textbook-defined2</td>
<td>$\delta\ null = false$</td>
</tr>
<tr>
<td>textbook-defined3</td>
<td>$\delta\ true = true$</td>
</tr>
<tr>
<td>textbook-defined4</td>
<td>$\delta\ false = true$</td>
</tr>
<tr>
<td>textbook-defined5</td>
<td>$\delta\ X = true$</td>
</tr>
<tr>
<td>textbook-defined6</td>
<td>$\delta\ \upsilon\ X = true$</td>
</tr>
<tr>
<td>textbook-valid5</td>
<td>$\upsilon\ X = true$</td>
</tr>
<tr>
<td>textbook-valid6</td>
<td>$\upsilon\ \delta\ X = true$</td>
</tr>
</tbody>
</table>

The definitions above for the constants defined and valid can be rewritten into the conventional semantic 'textbook' format as follows:

<table>
<thead>
<tr>
<th>Name</th>
<th>Lemma</th>
</tr>
</thead>
<tbody>
<tr>
<td>textbook-defined</td>
<td>$I[\delta(X)] \tau = (\text{if }I[X] \tau = I[\text{bot}] \ \tau \ \text{then} \ I[false] \ \tau \ \text{else} \ I[true] \ \tau)$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Lemma</th>
</tr>
</thead>
<tbody>
<tr>
<td>textbook-valid</td>
<td>$I[\upsilon(X)] \tau = (\text{if }I[X] \tau = I[\text{bot}] \ \tau \ \text{then} \ I[false] \ \tau \ \text{else} \ I[true] \ \tau)$</td>
</tr>
</tbody>
</table>

Table 2.2 and Table 2.3 summarize the results of this section.
2.1.3. The Equalities of OCL

The OCL contains a particular version of equality, written in Standard documents \( _= _\) and \( _\neq _\) for its negation, which is referred as weak referential equality hereafter and for which we use the symbol \( _\equiv _\) throughout the formal part of this document. Its semantics is motivated by the desire of fast execution, and similarity to languages like Java and C, but does not satisfy the needs of logical reasoning over OCL expressions and specifications. We therefore introduce a second equality, referred as strong equality or logical equality and written \( _\equiv _\) which is not present in the current standard but was discussed in prior texts on OCL like the Amsterdam Manifesto [18] and was identified as desirable extension of OCL in the Aachen Meeting [14] in the future 2.5 OCL Standard. The purpose of strong equality is to define and reason over OCL. It is therefore a natural task in Featherweight OCL to formally investigate the somewhat quite complex relationship between these two.

Strong equality has two motivations: a pragmatic one and a fundamental one.

1. The pragmatic reason is fairly simple: users of object-oriented languages want something like a “shallow object value equality”. You will want to say \( \text{a.boss} \equiv \text{b.boss@pre} \) instead of

\[
\text{a.boss} = \text{b.boss@pre and (} * \text{ just the pointers are equal! } *)
\]

\[
\text{a.boss.name} = \text{b.boss@pre.name@pre and}
\text{a.boss.age} \equiv \text{b.boss@pre.age@pre}
\]

Breaking a shallow-object equality down to referential equality of attributes is cumbersome, error-prone, and makes specifications difficult to extend (add for example an attribute sex to your class, and check in your OCL specification everywhere that you did it right with your simulation of strong equality). Therefore, languages like Java offer facilities to handle two different equalities, and it is problematic even in an execution oriented specification language to ignore shallow object equality because it is so common in the code.

2. The fundamental reason goes as follows: whatever you do to reason consistently over a language, you need the concept of equality: you need to know what expressions can be replaced by others because they mean the same thing. People call this also “Leibniz Equality” because this philosopher brought this principle first explicitly to paper and shed some light over it. It is the theoretic foundation of what you do in an optimizing compiler: you replace expressions by equal ones, which you hope are easier to evaluate. In a typed language, strong equality exists uniformly over all
types, it is “polymorphic” \( \cdot \) :: \( \alpha \ast \alpha \rightarrow bool \) —this is the way that equality is defined in HOL itself. We can express Leibniz principle as one logical rule of surprising simplicity and beauty:

\[ s = t \implies P(s) = P(t) \]  

(2.1)

“Whenever we know, that \( s \) is equal to \( t \), we can replace the sub-expression \( s \) in a term \( P \) by \( t \) and we have that the replacement is equal to the original.”

While weak referential equality is defined to be strict in the OCL standard, we will define strong equality as non-strict. It is quite nasty (but not impossible) to define the logical equality in a strict way (the substitutivity rule above would look more complex), however, whenever references were used, strong equality is needed since references refer to particular states (pre or post), and that they mean the same thing can therefore not be taken for granted.

**Definition**

The strict equality on basic types (actually on all types) must be exceptionally defined on \( null \) — otherwise the entire concept of null in the language does not make much sense. This is an important exception from the general rule that null arguments—especially if passed as “self”-argument—lead to invalid results.

We define strong equality extremely generic, even for types that contain a \( null \) or \( \perp \) element. Strong equality is simply polymorphic in Featherweight OCL, i.e., is defined identical for all types in OCL and HOL.

**Definition** \( \text{StrongEq} \) \( :: \langle \ast \alpha \ast \alpha \Rightarrow \ast \alpha, \ast \alpha \Rightarrow \ast \alpha \rangle \implies (\ast \alpha)\text{Boolean} \ (\text{infixl} \equiv 30) \)

where \( X \equiv Y \equiv \lambda \tau. \ u.X \tau = Y \tau \ast \downarrow \)

From this follow already elementary properties like:

**Lemma** \( \text{simp,code-unfold} \): \( \text{true} \equiv \text{false} = \text{false} \)

**Proof**

**Lemma** \( \text{simp,code-unfold} \): \( \text{false} \equiv \text{true} = \text{false} \)

**Proof**

**Fundamental Predicates on Strong Equality**

Equality reasoning in OCL is not humpty dumpty. While strong equality is clearly an equivalence:

**Lemma** \( \text{StrongEq-refl} \ [\text{simp}] \): \( X \equiv X = \text{true} \)

**Proof**

**Lemma** \( \text{StrongEq-sym} \): \( X \equiv Y = (Y \equiv X) \)

**Proof**

**Lemma** \( \text{StrongEq-trans-strong} \ [\text{simp}] \):

\begin{align*}
\text{assumes} & \ A: (X \equiv Y) = \text{true} \\
\text{and} & \ B: (Y \equiv Z) = \text{true} \\
\text{shows} & \ (X \equiv Z) = \text{true}
\end{align*}

**Proof**

it is only in a limited sense a congruence, at least from the point of view of this semantic theory. The point is that it is only a congruence on OCL expressions, not arbitrary HOL expressions (with which we can mix Featherweight OCL expressions). A semantic—not syntactic—characterization of OCL expressions is that they are context-passing or context-invariant, i.e., the context of an entire OCL expression, i.e. the pre and post state it refers to, is passed constantly and unmodified to the sub-expressions, i.e., all sub-expressions inside an OCL expression refer to the same context. Expressed formally, this boils down to:
lemma StrongEq-subst:
assumes cp: \( \forall X. P(X) \tau = P(\lambda - . X) \tau \)
and eq: \((X \trianglelefteq Y) \tau = true \ \tau \)
shows \((P X \trianglelefteq P Y) \tau = true \ \tau \)
{proof}

lemma defined7[simp]: \( \delta (X \trianglelefteq Y) = true \)
{proof}

lemma valid7[simp]: \( v (X \trianglelefteq Y) = true \)
{proof}

lemma cp-StrongEq: \((X \trianglelefteq Y) \ \tau = ((\lambda - . X) \trianglelefteq (\lambda - . Y) \ \tau) \ \tau \)
{proof}

2.1.4. Logical Connectives and their Universal Properties

It is a design goal to give OCL a semantics that is as closely as possible to a “logical system” in a known sense; a specification logic where the logical connectives can not be understood other than having the truth-table aside when reading fails its purpose in our view.

Practically, this means that we want to give a definition to the core operations to be as close as possible to the lattice laws; this makes also powerful symbolic normalization of OCL specifications possible as a pre-requisite for automated theorem provers. For example, it is still possible to compute without any definedness and validity reasoning the DNF of an OCL specification; be it for test-case generations or for a smooth transition to a two-valued representation of the specification amenable to fast standard SMT-solvers, for example.

Thus, our representation of the OCL is merely a 4-valued Kleene-Logics with invalid as least, null as middle and true resp. false as unrelated top-elements.

definition OclNot :: (\forall x. Boolean \Rightarrow (\forall x. Boolean) (not))
where not X \equiv \lambda \tau . case X \tau of
  | \bot \Rightarrow \bot
  | \bot \Rightarrow \bot
  | \bot \Rightarrow \bot

lemma cp-OclNot: \( (not X) \tau = (not (\lambda - . X) \ \tau) \ \tau \)
{proof}

lemma OclNot1[simp]: \( not invalid = invalid \)
{proof}

lemma OclNot2[simp]: \( not null = null \)
{proof}

lemma OclNot3[simp]: \( not true = false \)
{proof}

lemma OclNot4[simp]: \( not false = true \)
{proof}

lemma OclNot-not[simp]: \( not (not X) = X \)
{proof}

lemma OclNot-inject: \( \lambda x y. not x = not y \Rightarrow x = y \)
(proof)

definition OclAnd :: [(A)Boolean, (A)Boolean] ⇒ (A)Boolean (infixl and 30)
where  X and Y ≡ (λ τ. case X τ of
    False ⇒ False
    _ ⇒ (case Y τ of
        False ⇒ False
        _ ⇒ True
        ⊥ ⇒ Y τ)
)

Note that not is not defined as a strict function; proximity to lattice laws implies that we need a definition of not that satisfies not(not(x))=x.

In textbook notation, the logical core constructs not and (and) were represented as follows:

lemma textbook-OclNot:
  I[[not(X)]] τ = (case I[[X]] τ of
    ⊥ ⇒ ⊥
    _ ⇒ (case I[[Y]] τ of
      ⊥ ⇒ ⊥
      _ ⇒ (case I[[Y]] τ of
        ⊥ ⇒ ⊥
        _ ⇒ (case I[[Y]] τ of
          ⊥ ⇒ ⊥
          _ ⇒ (case I[[Y]] τ of
            ⊥ ⇒ ⊥
            _ ⇒ (case I[[Y]] τ of
              ⊥ ⇒ ⊥
              _ ⇒ (case I[[Y]] τ of
                ⊥ ⇒ ⊥
                _ ⇒ (case I[[Y]] τ of
                  ⊥ ⇒ ⊥
                  _ ⇒ (case I[[Y]] τ of
                    ⊥ ⇒ ⊥
                    _ ⇒ (case I[[Y]] τ of
                      ⊥ ⇒ ⊥
                      _ ⇒ (case I[[Y]] τ of
                        ⊥ ⇒ ⊥
                        _ ⇒ (case I[[Y]] τ of
                          ⊥ ⇒ ⊥
                          _ ⇒ (case I[[Y]] τ of
                            ⊥ ⇒ ⊥
                            _ ⇒ (case I[[Y]] τ of
                              ⊥ ⇒ ⊥
                              _ ⇒ (case I[[Y]] τ of
                                ⊥ ⇒ ⊥
                                _ ⇒ (case I[[Y]] τ of
                                  ⊥ ⇒ ⊥
                                  _ ⇒ (case I[[Y]] τ of
                                    ⊥ ⇒ ⊥
                                    _ ⇒ (case I[[Y]] τ of
                                      ⊥ ⇒ ⊥
                                      _ ⇒ (case I[[Y]] τ of
                                        ⊥ ⇒ ⊥
                                        _ ⇒ (case I[[Y]] τ of
                                          ⊥ ⇒ ⊥
                                          _ ⇒ (case I[[Y]] τ of
                                            ⊥ ⇒ ⊥
                                            _ ⇒ (case I[[Y]] τ of
                                              ⊥ ⇒ ⊥
                                              _ ⇒ (case I[[Y]] τ of
                                                ⊥ ⇒ ⊥
                                                _ ⇒ (case I[[Y]] τ of
                                                  ⊥ ⇒ ⊥
                                                  _ ⇒ (case I[[Y]] τ of
                                                    ⊥ ⇒ ⊥
                                                    _ ⇒ (case I[[Y]] τ of
                                                      ⊥ ⇒ ⊥
                                                      _ ⇒ (case I[[Y]] τ of
                                                        ⊥ ⇒ ⊥
                                                        _ ⇒ (case I[[Y]] τ of
                                                          ⊥ ⇒ ⊥
                                                          _ ⇒ (case I[[Y]] τ of
                                                            ⊥ ⇒ ⊥
                                                            _ ⇒ (case I[[Y]] τ of
                                                              ⊥ ⇒ ⊥
                                                              _ ⇒ (case I[[Y]] τ of
                                                                ⊥ ⇒ ⊥
                                                                _ ⇒ (case I[[Y]] τ of
                                                                  ⊥ ⇒ ⊥
                                                                  _ ⇒ (case I[[Y]] τ of
                                                                    ⊥ ⇒ ⊥
                                                                    _ ⇒ (case I[[Y]] τ of
                                                                      ⊥ ⇒ ⊥
                                                                      _ ⇒ (case I[[Y]] τ of
                                                                        ⊥ ⇒ ⊥
                                                                        _ ⇒ (case I[[Y]] τ of
                                                                          ⊥ ⇒ ⊥
                                                                          _ ⇒ (case I[[Y]] τ of
                                                                            ⊥ ⇒ ⊥
                                                                            _ ⇒ (case I[[Y]] τ of
                                                                              ⊥ ⇒ ⊥
                                                                              _ ⇒ (case I[[Y]] τ of
                                                                                ⊥ ⇒ ⊥
                                                                                _ ⇒ (case I[[Y]] τ of
                                                                                  ⊥ ⇒ ⊥
                                                                                  _ ⇒ (case I[[Y]] τ of
                                                                                    ⊥ ⇒ ⊥
                                                                                    _ ⇒ (case I[[Y]] τ of
                                                                                      ⊥ ⇒ ⊥
                                                                                      _ ⇒ (case I[[Y]] τ of
                                                                                        ⊥ ⇒ ⊥
                                                                                        _ ⇒ (case I[[Y]] τ of
                                                                                          ⊥ ⇒ ⊥
                                                                                          _ ⇒ (case I[[Y]] τ of
                                                                                             ⊥ ⇒ ⊥
                                                                                             _ ⇒ (case I[[Y]] τ of
                                                                                               ⊥ ⇒ ⊥
                                                                                               _ ⇒ (case I[[Y]] τ of
                                                                                                ⊥ ⇒ ⊥
                                                                                                _ ⇒ (case I[[Y]] τ of
                                                                                                  ⊥ ⇒ ⊥
                                                                                                  _ ⇒ (case I[[Y]] τ of
                                                                                                    ⊥ ⇒ ⊥
                                                                                                    _ ⇒ (case I[[Y]] τ of
                                                                                                      ⊥ ⇒ ⊥
                                                                                                      _ ⇒ (case I[[Y]] τ of
                                                                                                        ⊥ ⇒ ⊥
                                                                                                        _ ⇒ (case I[[Y]] τ of
                                                                                                          ⊥ ⇒ ⊥
                                                                                                          _ ⇒ (case I[[Y]] τ of
                                                                                                            ⊥ ⇒ ⊥
                                                                                                            _ ⇒ (case I[[Y]] τ of
                                                                                                              ⊥ ⇒ ⊥
                                                                                                              _ ⇒ (case I[[Y]] τ of
                                                                                                                ⊥ ⇒ ⊥
                                                                                                                _ ⇒ (case I[[Y]] τ of
                                                                                                                  ⊥ ⇒ ⊥
                                                                                                                  _ ⇒ (case I[[Y]] τ of
                                                                                                                    ⊥ ⇒ ⊥
                                                                                                                    _ ⇒ (case I[[Y]] τ of
                                                                                                                      ⊥ ⇒ ⊥
                                                                                                                      _ ⇒ (case I[[Y]] τ of
                                                                                                                        ⊥ ⇒ ⊥
                                                                                                                        _ ⇒ (case I[[Y]] τ of
                                                                                                                          ⊥ ⇒ ⊥
                                                                                                                          _ ⇒ (case I[[Y]] τ of
                                                                                                                            ⊥ ⇒ ⊥
                                                                                                                            _ ⇒ (case I[[Y]] τ of
                                                                                                                              ⊥ ⇒ ⊥
                                                                                                                              _ ⇒ (case I[[Y]] τ of
                                                                                                                                ⊥ ⇒ ⊥
                                                                                                                                _ ⇒ (case I[[Y]] τ of
                                                                                                                                  ⊥ ⇒ ⊥
                                                                                                                                  _ ⇒ (case I[[Y]] τ of
                                                                                                                                    ⊥ ⇒ ⊥
                                                                                                                                    _ ⇒ (case I[[Y]] τ of
                                                                                                                                      ⊥ ⇒ ⊥
                                                                                                                                      _ ⇒ (case I[[Y]] τ of
                                                                                                                                            ⊥ ⇒ ⊥
                                                                                                                                            _ ⇒ (case I[[Y]] τ of
                                                                                                                                                ⊥ ⇒ ⊥
                                                                                                                                                _ ⇒ (case I[[Y]] τ of
                                                                                                                                                    ⊥ ⇒ ⊥
                                                                                                                                                    _ ⇒ (case I[[Y]] τ of
                                                                                                                                                      ⊥ ⇒ ⊥
                                                                                                                                                      _ ⇒ (case I[[Y]] τ of
                                                                                                                                                         ⊥ ⇒ ⊥
                                                                                                                                                         _ ⇒ (case I[[Y]] τ of
                                                                                                                                                              ⊥ ⇒ ⊥
                                                                                                                                                              _ ⇒ (case I[[Y]] τ of
                                                                                                                                                                ⊥ ⇒ ⊥
                                                                                                                                                                _ ⇒ (case I[[Y]] τ of
                                                                                                                                                                      ⊥ ⇒ ⊥
                                                                                                                                                                      _ ⇒ (case I[[Y]] τ of
                                                                                                                                                                            ⊥ ⇒ ⊥
                                                                                                                                                                            _ ⇒ (case I[[Y]] τ of
                                                                                                                                                                                ⊥ ⇒ ⊥
                                                                                                                                                                                _ ⇒ (case I[[Y]] τ of
                                                                                                                                                                                    ⊥ ⇒ ⊥
                                                                                                                                                                                    _ ⇒ (case I[[Y]] τ of
                                                                                                                                                                                        ⊥ ⇒ ⊥
                                                                                                                                                                                        _ ⇒ (case I[[Y]] τ of
                                                                                                                                                                                            ⊥ ⇒ ⊥
                                                                                                                            ⟨proof⟩)

definition OclOr :: [(A)Boolean, (A)Boolean] ⇒ (A)Boolean (infixl or 25)
where  X or Y ≡ not(not X and not Y)

definition OclImplies :: [(A)Boolean, (A)Boolean] ⇒ (A)Boolean (infixl implies 25)
where  X implies Y ≡ not X or Y

lemma cp-OclAnd:(X and Y) τ = ((λ ·. X τ) and (λ ·. Y τ)) τ
⟨proof⟩

lemma cp-OclOr:(X or Y) τ = ((λ ·. X τ) or (λ ·. Y τ)) τ
⟨proof⟩

lemma cp-OclImplies:(X implies Y) τ = ((λ ·. X τ) implies (λ ·. Y τ)) τ
⟨proof⟩

52
lemma OclAnd1[simp]: (invalid and true) = invalid
⟨proof⟩
lemma OclAnd2[simp]: (invalid and false) = false
⟨proof⟩
lemma OclAnd3[simp]: (invalid and null) = invalid
⟨proof⟩
lemma OclAnd4[simp]: (invalid and invalid) = invalid
⟨proof⟩

lemma OclAnd5[simp]: (null and true) = null
⟨proof⟩
lemma OclAnd6[simp]: (null and false) = false
⟨proof⟩
lemma OclAnd7[simp]: (null and null) = null
⟨proof⟩
lemma OclAnd8[simp]: (null and invalid) = invalid
⟨proof⟩

lemma OclAnd9[simp]: (false and true) = false
⟨proof⟩
lemma OclAnd10[simp]: (false and false) = false
⟨proof⟩
lemma OclAnd11[simp]: (false and null) = false
⟨proof⟩
lemma OclAnd12[simp]: (false and invalid) = false
⟨proof⟩

lemma OclAnd-idem[simp]: (true and true) = true
⟨proof⟩
lemma OclAnd14[simp]: (true and false) = false
⟨proof⟩
lemma OclAnd15[simp]: (true and null) = null
⟨proof⟩
lemma OclAnd16[simp]: (true and invalid) = invalid
⟨proof⟩

lemma OclAnd-commute: (X and Y) = (Y and X)
⟨proof⟩

lemma OclAnd-true1[simp]: (false and X) = false
⟨proof⟩
lemma OclAnd-true2[simp]: (X and false) = false
⟨proof⟩

lemma OclAnd-true1[simp]: (true and X) = X
⟨proof⟩
lemma OclAnd-true2[simp]: (X and true) = X
⟨proof⟩
lemma OclAnd-bot1 [simp]: \( \forall \tau. X \tau \neq \text{false} \Rightarrow (\text{bot} \land X) \tau = \text{bot} \tau \)
(proof)

lemma OclAnd-bot2 [simp]: \( \forall \tau. X \tau \neq \text{false} \Rightarrow (X \land \text{bot}) \tau = \text{bot} \tau \)
(proof)

lemma OclAnd-null1 [simp]: \( \forall \tau. X \tau \neq \text{false} \Rightarrow X \tau \neq \text{false} \tau = \Rightarrow (\text{null} \land X) \tau = \text{null} \tau \)
(proof)

lemma OclAnd-null2 [simp]: \( \forall \tau. X \tau \neq \text{false} \Rightarrow X \tau \neq \text{false} \tau = \Rightarrow (X \land \text{null}) \tau = \text{null} \tau \)
(proof)

lemma OclAnd-assoc: \( (X \land (Y \land Z)) = (X \land Y \land Z) \)
(proof)

lemma OclOr1 [simp]: \( (\text{invalid} \lor \text{true}) = \text{true} \)
(proof)

lemma OclOr2 [simp]: \( (\text{invalid} \lor \text{false}) = \text{invalid} \)
(proof)

lemma OclOr3 [simp]: \( (\text{invalid} \lor \text{null}) = \text{invalid} \)
(proof)

lemma OclOr4 [simp]: \( (\text{invalid} \lor \text{invalid}) = \text{invalid} \)
(proof)

lemma OclOr5 [simp]: \( (\text{null} \lor \text{true}) = \text{true} \)
(proof)

lemma OclOr6 [simp]: \( (\text{null} \lor \text{false}) = \text{null} \)
(proof)

lemma OclOr7 [simp]: \( (\text{null} \lor \text{null}) = \text{null} \)
(proof)

lemma OclOr8 [simp]: \( (\text{null} \lor \text{invalid}) = \text{invalid} \)
(proof)

lemma OclOr-idem [simp]: \( (X \lor X) = X \)
(proof)

lemma OclOr-commute: \( (X \lor Y) = (Y \lor X) \)
(proof)

lemma OclOr-false1 [simp]: \( (\text{false} \lor Y) = Y \)
(proof)

lemma OclOr-false2 [simp]: \( (Y \lor \text{false}) = Y \)
(proof)

lemma OclOr-true1 [simp]: \( (\text{true} \lor Y) = \text{true} \)
(proof)

lemma OclOr-true2: \( (Y \lor \text{true}) = \text{true} \)
(proof)

lemma OclOr-bot1 [simp]: \( \forall \tau. X \tau \neq \text{true} \Rightarrow (\text{bot} \lor X) \tau = \text{bot} \tau \)
(proof)

lemma OclOr-bot2 [simp]: \( \forall \tau. X \tau \neq \text{true} \Rightarrow (X \lor \text{bot}) \tau = \text{bot} \tau \)
(proof)
lemma OclOr-null1[simp]: \( \forall \tau. \ X \neq true \tau \implies X \neq bot \tau \implies (null \ or \ X) \tau = null \tau \)
(proof)

lemma OclOr-null2[simp]: \( \forall \tau. \ X \neq true \tau \implies X \neq bot \tau \implies (X \ or \ null) \tau = null \tau \)
(proof)

lemma OclOr-assoc: \( (X \ or \ (Y \ or \ Z)) = (X \ or \ Y \ or \ Z) \)
(proof)

definition OclValid :: \( \langle \forall A st, \forall A Boolean \rangle \Rightarrow bool \)
where
\( \tau | \tau = P \equiv (\tau \ | \tau = P) \)

syntax OclNonValid :: \( \langle \forall A st, \forall A Boolean \rangle \Rightarrow bool \)
translations \( \tau \not\equiv P \equiv \neg (\tau \ | \tau = P) \)

Global vs. Local Judgements

lemma transform1: \( P = true \implies \tau \models P \)
(proof)

lemma transform1-rev: \( \forall \tau. \ \tau \models P \implies P = true \)
(proof)

lemma transform2: \( (P = Q) \implies (\tau \models P) = (\tau \models Q) \)
(proof)

lemma transform2-rev: \( \forall \tau. \ (\tau \models \delta P) \land (\tau \models \delta Q) \land (\tau \models P) = (\tau \models Q) \implies P = Q \)
(proof)

However, certain properties (like transitivity) cannot be transformed from the global level to the local one, they have to be re-proven on the local level.

lemma assumes H: \( P = true \implies Q = true \)
shows \( \tau \models P \implies \tau \models Q \)
(proof)
Local Validity and Meta-logic

**lemma foundation1**[simp]: $\tau \vDash true$
(proof)

**lemma foundation2**[simp]: $\neg(\tau \vDash false)$
(proof)

**lemma foundation3**[simp]: $\neg(\tau \vDash invalid)$
(proof)

**lemma foundation4**[simp]: $\neg(\tau \vDash null)$
(proof)

**lemma bool-split**[simp]:
$(\tau \vDash (x \triangleq invalid)) \vee (\tau \vDash (x \triangleq null)) \vee (\tau \vDash (x \triangleq true)) \vee (\tau \vDash (x \triangleq false))$
(proof)

**lemma defined-split**:
$(\tau \vDash \delta x) = (((\neg(\tau \vDash (x \triangleq invalid))) \wedge (\neg (\tau \vDash (x \triangleq null))))$
(proof)

**lemma valid-bool-split**: $(\tau \vDash \upsilon A) = ((\tau \vDash A \triangleq null) \vee (\tau \vDash A) \vee (\tau \vDash not A))$
(proof)

**lemma defined-bool-split**: $(\tau \vDash \delta A) = ((\tau \vDash A) \vee (\tau \vDash not A))$
(proof)

**lemma foundation5**:
$\tau \vDash (P and Q) \implies (\tau \vDash P) \wedge (\tau \vDash Q)$
(proof)

**lemma foundation6**:
$\tau \vDash P \implies \tau \vDash \delta P$
(proof)

**lemma foundation7**[simp]:
$(\tau \vDash not (\delta x)) = (\neg (\tau \vDash \delta x))$
(proof)

**lemma foundation7’**[simp]:
$(\tau \vDash not (\upsilon x)) = (\neg (\tau \vDash \upsilon x))$
(proof)

Key theorem for the $\delta$-closure: either an expression is defined, or it can be replaced (substituted via StrongEq-L-subst2; see below) by invalid or null. Strictness-reduction rules will usually reduce these substituted terms drastically.

**lemma foundation8**:
$(\tau \vDash \delta x) \vee (\tau \vDash (x \triangleq invalid)) \vee (\tau \vDash (x \triangleq null))$
(proof)

**lemma foundation9**:
$\tau \vDash \delta x \implies (\tau \vDash not x) = (\neg (\tau \vDash x))$

56
lemma foundation9:
\[ \tau \models \text{not } x \implies \neg (\tau \models x) \]

lemma foundation9':
\[ \tau \models \text{not } x \implies \tau \models \delta x \]

lemma foundation10:
\[ \tau \models \delta x \implies \tau \models \delta y \implies (\tau \models (x \text{ and } y)) = ( (\tau \models x) \land (\tau \models y)) \]

lemma foundation10':
\[ (\tau \models (A \text{ and } B)) = ((\tau \models A) \land (\tau \models B)) \]

lemma foundation11:
\[ \tau \models \delta x \implies \tau \models \delta y \implies (\tau \models (x \text{ or } y)) = ( (\tau \models x) \lor (\tau \models y)) \]

lemma foundation12:
\[ \tau \models \delta x \implies (\tau \models (x \implies y)) = ( (\tau \models x) \rightarrow (\tau \models y)) \]

lemma foundation13:
\[ (\tau \models A \triangleq \text{true}) = (\tau \models A) \]

lemma foundation14:
\[ (\tau \models A \triangleq \text{false}) = (\tau \models \text{not } A) \]

lemma foundation15:
\[ (\tau \models A \triangleq \text{invalid}) = (\tau \models \text{not}(v A)) \]

lemma foundation16:
\[ \tau \models (\delta X) = (X \tau \neq \text{bot} \land X \tau \neq \text{null}) \]

lemma foundation16':
\[ -(\tau \models (\delta X)) = ((\tau \models (X \triangleq \text{invalid})) \lor (\tau \models (X \triangleq \text{null}))) \]

lemma foundation16'':
\[ (\tau \models (\delta X)) = (X \tau \neq \text{invalid} \land X \tau \neq \text{null} \tau) \]

lemma foundation18:
\[ (\tau \models (v X)) = (X \tau \neq \text{invalid} \tau) \]

lemma foundation18':
\[ (\tau \models (v X)) = (X \tau \neq \text{bot}) \]
lemma foundation18': \( (\tau \models (\nu \, X)) = \neg (\neg (\tau \models (X \triangleleft invalid))) \)
Local Judgements and Strong Equality

lemma StrongEq-L-refl: \( \tau \models (x \triangleleft x) \)
<br/>(proof)

lemma StrongEq-L-sym: \( \tau \models (x \triangleleft y) \implies \tau \models (y \triangleleft x) \)
<br/>(proof)

lemma StrongEq-L-trans: \( \tau \models (x \triangleleft y) \implies \tau \models (y \triangleleft z) \implies \tau \models (x \triangleleft z) \)
<br/>(proof)

In order to establish substitutivity (which does not hold in general HOL formulas) we introduce the following predicate that allows for a calculus of the necessary side-conditions.

definition cp :: \((\mathcal{A}, \alpha) \val \Rightarrow (\mathcal{A}, \beta) \val \Rightarrow \text{bool}\)
where \( cp \ P \equiv (\exists f. \forall X \tau. P X \tau = f (X \tau) \tau) \)

The rule of substitutivity in Featherweight OCL holds only for context-passing expressions, i.e. those that pass the context \( \tau \) without changing it. Fortunately, all operators of the OCL language satisfy this property (but not all HOL operators).

lemma StrongEq-L-subst1: \( \forall \tau. cp P \implies \tau \models (x \triangleleft y) \implies \tau \models (P x \triangleleft P y) \)
<br/>(proof)

lemma StrongEq-L-subst2: \( \forall \tau. cp P \implies \tau \models (x \triangleleft y) \implies \tau \models (P x) \models (P y) \)
<br/>(proof)

lemma StrongEq-L-subst2-rev: \( \models y \triangleleft x \models cp P \models \tau \models (P x) \models \tau \models (P y) \)
<br/>(proof)

lemma StrongEq-L-subst3: assumes \( cp \): \( cp P \)
and \( eq \): \( \tau \models (x \triangleleft y) \)
shows \( (\tau \models P x) = (\tau \models P y) \)
<br/>(proof)

lemma StrongEq-L-subst3-rev: assumes \( eq \): \( \tau \models (x \triangleleft y) \)
and \( cp \): \( cp P \)
shows \( (\tau \models P x) = (\tau \models P y) \)
<br/>(proof)

lemma StrongEq-L-subst4-rev: assumes \( eq \): \( \tau \models (x \triangleleft y) \)
and \( cp \): \( cp P \)
shows \( (\neg (\tau \models P x)) = (\neg (\tau \models P y)) \)
<br/thm arg-cong[of - Not]
<br/>(proof)

lemma cpI1: \( (\forall X \tau. f X \tau = f(\lambda \cdot X \tau) \tau) \implies cp P \implies cp(\lambda X. f (P X)) \)
<br/>(proof)

lemma cpI2: \( (\forall X Y \tau. f X Y \tau = f(\lambda \cdot X \tau)(\lambda \cdot Y \tau) \tau) \implies cp P \implies cp Q \implies cp(\lambda X. f (P X) (Q X)) \)
<br/>(proof)
Lemma cpI3:
(∀ X Y Z τ. f X Y Z τ = f⟨λ· X τ⟩⟨λ· Y τ⟩⟨λ· Z τ⟩ τ) 𝛀

\[
\text{cp P} \implies \text{cp Q} \implies \text{cp R} \implies \text{cp}(\text{AX. } f\ (P \ X) \ (Q \ X) \ (R \ X))
\]
(proof)

Lemma cpI4:
(∀ W X Y Z τ. f W X Y Z τ = f⟨λ· W τ⟩⟨λ· X τ⟩⟨λ· Y τ⟩⟨λ· Z τ⟩ τ) 𝛀

\[
\text{cp N} \implies \text{cp P} \implies \text{cp Q} \implies \text{cp R} \implies \text{cp S} \implies \text{cp}(\text{AX. } f\ (N \ X) \ (P \ X) \ (Q \ X) \ (R \ X) \ (S X))
\]
(proof)

Lemma cp-const : cp⟨λ· c⟩
(proof)

Lemma cp-id : cp⟨λ· X. X⟩
(proof)

\[
\text{lemmas } \text{cp-intro[introl, simp, code-unfold]} =
\]
\[
\text{cp-const}
\text{cp-id}
\text{cp-defined[THEN allI[THEN allI[THEN cpI1], of defined]]}
\text{cp-valid[THEN allI[THEN allI[THEN cpI1], of valid]]}
\text{cp-OclNot[THEN allI[THEN allI[THEN cpI1], of not]]}
\text{cp-OclAnd[THEN allI[THEN allI[THEN cpI1], of (and)]}
\text{cp-OclOr[THEN allI[THEN allI[THEN cpI1], of (or)]}
\text{cp-OclImplies[THEN allI[THEN allI[THEN cpI1], of (implies)]}
\text{cp-StrongEq[THEN allI[THEN allI[THEN cpI1], of StrongEq]]}
\]

2.1.6. OCL’s if then else endif

Definition OclIf :: ([∀ Boolean, (∀ 'a::null) val, (∀ 'a) val ⇒ (∀ 'a, 'a) val]
\[
\text{if } (\text{- }) \text{ then } (\text{- }) \text{ else } (\text{- }) \text{ endif } \{10.10.10\}[50]
\]
Where (if C then B₁ else B₂ endif) = (λ τ. if (δ C) τ = true τ
\[
\text{then } (\text{if } (C \ τ) \tau = true \ τ
\]
\[
\text{then } B₁ \ τ
\]
\[
\text{else } B₂ \ τ
\]
\[
\text{else invalid } \tau
\]}

Lemma cp-OclIf:(if C then B₁ else B₂ endif) \tau =
\[
\text{(if } (\lambda · C \ τ) \text{ then } (\lambda · B₁ \ τ) \text{ else } (\lambda · B₂ \ τ) \text{ endif) } \tau
\]
(proof)

\[
\text{lemmas } \text{cp-intro[introl, simp, code-unfold]} =
\]
\[
\text{cp-OclIf[THEN allI[THEN allI[THEN allI[THEN cpI3]], of OclIf]]}
\text{OclIf-invalid [simp]: (if invalid then B₁ else B₂ endif) = invalid}
\]
(proof)

Lemma OclIf-null [simp]: (if null then B₁ else B₂ endif) = invalid
(proof)

Lemma OclIf-true [simp]: (if true then B₁ else B₂ endif) = B₁
(proof)

60
lemma OclIf-true' [simp]: $\tau \models P \implies (\text{if } P \text{ then } B_1 \text{ else } B_2 \text{ endif})\tau = B_1 \tau$
(proof)

lemma OclIf-true' [simp]: $\tau \models P \implies (\text{if } P \text{ then } B_1 \text{ else } B_2 \text{ endif}) \hat{=} B_1$
(proof)

lemma OclIf-false [simp]: $(\text{if } \text{false then } B_1 \text{ else } B_2 \text{ endif}) = B_2$
(proof)

lemma OclIf-false' [simp]: $\tau \models \text{not } P \implies (\text{if } P \text{ then } B_1 \text{ else } B_2 \text{ endif})\tau = B_2 \tau$
(proof)

lemma OclIf-idem1 [simp]: $(\text{if } \delta X \text{ then } A \text{ else } A \text{ endif}) = A$
(proof)

lemma OclIf-idem2 [simp]: $(\text{if } \upsilon X \text{ then } A \text{ else } A \text{ endif}) = A$
(proof)

lemma OclNot-if [simp]: \not((\text{if } P \text{ then } C \text{ else } E \text{ endif})) = (\text{if } P \text{ then } \not C \text{ else } \not E \text{ endif})
(proof)

2.1.7. Fundamental Predicates on Basic Types: Strict (Referential) Equality

In contrast to logical equality, the OCL standard defines an equality operation which we call “strict referential equality”. It behaves differently for all types—on value types, it is basically a strict version of strong equality, for defined values it behaves identical. But on object types it will compare their references within the store. We introduce strict referential equality as an overloaded concept and will handle it for each type instance individually.

casts StrictRefEq :: [(\a, val, (\a, val)] \Rightarrow (\a)Boolean (infixl \equiv 30)

with the term "\not" we can express the notation:

syntax
\not a = \not (\\a)\text{Boolean} \Rightarrow (\\a)\text{Boolean} (infix <> 40)

translations
a <> b == CONST OclNot(a \equiv b)

We will define instances of this equality in a case-by-case basis.

2.1.8. Laws to Establish Definedness ($\delta$-closure)

For the logical connectives, we have — beyond $\tau \models P \implies \tau \models \delta P$ — the following facts:

lemma OclNot-defargs:
$\tau \models (\text{not } P) \implies \tau \models \delta P$
(proof)

lemma OclNot-contrapos-nn:
assumes A: $\tau \models \delta A$
assumes B: $\tau \models \text{not } B$
assumes C: $\tau \models A \implies \tau \models B$
shows $\tau \models \text{not } A$
(proof)
2.1.9. A Side-calculus for Constant Terms

definition const X ≡ ∀ τ τ′. X τ = X τ′

lemma const-charn; const X ⇒ X τ = X τ′
(proof)

lemma const-subst:
assumes const-X: const X
and const-Y: const Y
and eq : X τ = Y τ
and cp-P: cp P
and pp : P Y τ = P Y τ′
shows P X τ = P X τ′
(proof)

lemma const-imply2:
assumes ⋀ τ τ′. P τ = P τ′ =⇒ Q τ = Q τ′
shows const P =⇒ const Q
(proof)

lemma const-imply3:
assumes ⋀ τ τ′. P τ = P τ′ =⇒ Q τ = Q τ′ =⇒ R τ = R τ′
shows const P =⇒ const Q =⇒ const R
(proof)

lemma const-imply4:
assumes ⋀ τ τ′. P τ = P τ′ =⇒ Q τ = Q τ′ =⇒ R τ = R τ′ =⇒ S τ = S τ′
shows const P =⇒ const Q =⇒ const R =⇒ const S
(proof)

lemma const-lam : const (λ-. e)
(proof)

lemma const-true[simp] : const true
(proof)

lemma const-false[simp] : const false
(proof)

lemma const-null[simp] : const null
(proof)

lemma const-invalid [simp]: const invalid
(proof)

lemma const-bot[simp] : const bot
(proof)

lemma const-defined :
assumes const X
shows const (δ X)
(proof)
lemma const-valid :
  assumes const X
  shows const (v X)
⟨proof⟩

lemma const-OclAnd :
  assumes const X
  assumes const X'
  shows const (X and X')
⟨proof⟩

lemma const-OclNot :
  assumes const X
  shows const (not X)
⟨proof⟩

lemma const-OclOr :
  assumes const X
  assumes const X'
  shows const (X or X')
⟨proof⟩

lemma const-OclImplies :
  assumes const X
  assumes const X'
  shows const (X implies X')
⟨proof⟩

lemma const-StrongEq:
  assumes const X
  assumes const X'
  shows const (X ≜ X')
⟨proof⟩

lemma const-OclIf :
  assumes const B
  and const C1
  and const C2
  shows const (if B then C1 else C2 endif)
⟨proof⟩

lemma const-OclValid1:
  assumes const x
  shows (τ |\models δ x) = (τ' |\models δ x)
⟨proof⟩

lemma const-OclValid2:
  assumes const x
  shows (τ |\models v x) = (τ' |\models v x)
⟨proof⟩

63
lemmas const-ss = const-bot const-null const-true const-undefined const-false const-lam const-defined const-valid const-StrongEq const-OclNot const-OclAnd const-OclOr const-OclImplies const-OclIf const-HOL-if const-HOL-and const-HOL-eq

Miscellaneous: Overloading the syntax of “bottom”

notation bot (\bot)

end

theory UML-PropertyProfiles
imports UML-Logic
begin

2.2. Property Profiles for OCL Operators via Isabelle Locales

We use the Isabelle mechanism of a Locale to generate the common lemmas for each type and operator; Locales can be seen as a functor that takes a local theory and generates a number of theorems. In our case, we will instantiate later these locales by the local theory of an operator definition and obtain the common rules for strictness, definedness propagation, context-passingness and constance in a systematic way.

2.2.1. Property Profiles for Monadic Operators

locale profile-mono-scheme-defined =
  fixes f :: (\A,\a::null)val \Rightarrow (\A,\b::null)val
  fixes g
  assumes def-scheme: (f x) \equiv \lambda \tau. if (\delta x) \tau = true \tau then g (x \tau) else invalid \tau
begin

lemma strict[simp,code-unfold]: f invalid = invalid
  (proof)

lemma null-strict[simp,code-unfold]: f null = invalid
  (proof)

lemma cp0 : f X \tau = f (\lambda \cdot. X \tau) \tau
  (proof)

lemma cp[simp,code-unfold] : cp P \Rightarrow cp (\lambda X. f (P X))
  (proof)

end

locale profile-mono-schemeV =
fixes $f : (\mathcal{A}, \alpha :: \text{null}) \Rightarrow (\mathcal{A}, \beta :: \text{null})$ val
fixes $g$
assumes def-scheme: $(f x) \equiv \lambda \tau. \text{if } (v x) \tau = \text{true } \tau \text{ then } g (x \tau) \text{ else invalid } \tau$

begin

lemma strict[simp, code-unfold]: $f \text{ invalid } \equiv \text{ invalid}$
(proof)

lemma $cp0 : f \text{ X } \tau = f (\lambda -. \text{ X } \tau) \tau$
(proof)

lemma $cp[simp, code-unfold] : cp \text{ P } \Rightarrow cp (\lambda \text{ X } . f (\text{ P } \text{ X } \) )$
(proof)

end

locale profile-mono = profile-mono-scheme-defined +
assumes def-body: \( x \neq \text{ bot } \Rightarrow x \neq \text{ null } \Rightarrow g x \neq \text{ bot } \)

begin

lemma const[simp, code-unfold] :
assumes $C1 : \text{const X}$
shows const($f \text{ X } \tau$)
(proof)

end

locale profile-mono = profile-mono-scheme-defined +
assumes def-body: \( x \neq \text{ bot } \Rightarrow x \neq \text{ null } \Rightarrow g x \neq \text{ bot } \) \& g x \neq \text{ null }$

sublocale profile-mono < profile-mono
(proof)

context profile-mono
begin

lemma def-homo[simp, code-unfold]: \( \delta (f x) = (\delta x) \)$
(proof)

lemma def-valid-then-def: \( \psi (f x) = (\delta (f x)) \)$
(proof)

end

2.2.2. Property Profiles for Single

locale profile-single =
fixes $d : (\mathcal{A}, \alpha :: \text{null}) \Rightarrow \mathcal{A}$ Boolean
assumes $d$-strict[simp, code-unfold]: $d \text{ invalid } \equiv \text{ false}$

assumes $d$-cp0: d $\text{ X } \tau = d (\lambda -. \text{ X } \tau)$
assumes $d$-const[simp, code-unfold]: const $\text{ X } \Rightarrow \text{ const } (d \text{ X })$

2.2.3. Property Profiles for Binary Operators

definition $\text{ bin’ } f g d_\alpha d_\beta : d_\alpha \text{ X Y }$
\( = f \text{ X Y } = \lambda \tau. \text{ if } (d_\alpha \text{ X } \tau = \text{true } \tau \& (d_\beta \text{ Y } \tau = \text{true } \tau \text{ then } g \text{ X Y } \tau \text{ else invalid } \tau )) \)$

definition $\text{ bin } f g = \text{ bin’ } f (\lambda \text{ X Y } . g (\text{ X } \tau) (\text{ Y } \tau))$

65
lemmas \[\text{simp, code-unfold} = \text{bin' - def bin - def}\]

locale profile-bin-scheme = 
  fixes \(d_x::('A', 'a::null)\) val \(\Rightarrow 'A\) Boolean 
  fixes \(d_y::('A', 'b::null)\) val \(\Rightarrow 'A\) Boolean 
  fixes \(f::('A', 'a::null)\) val \(\Rightarrow ('A', 'b::null)\) val \(\Rightarrow ('A', 'c::null)\) val 
  fixes \(g\)
  assumes \(d_x':\text{profile-single} d_x\)
  assumes \(d_y':\text{profile-single} d_y\)
  assumes \(d_x-d_y\)-homo[simp, code-unfold]: \(\text{cp} (f X) \iff\) 
    \(\text{cp} (\lambda x. f X Y) \iff\) 
    \(f X \text{ invalid} = \text{invalid} \iff\) 
    \(f \text{ invalid} Y = \text{invalid} \iff\) 
    \((\neg (\tau \models d_x X) \lor \neg (\tau \models d_y Y)) \iff\) 
    \(\tau \models (\delta f X Y \triangleq (d_x X \text{ and } d_y Y))\)
  assumes \(\text{def-scheme''}[\text{simplified}]: \text{bin} f g d_x d_y X Y\)
  assumes \(1: \tau \models d_x X \iff \tau \models d_y Y \iff \tau \models \delta f X Y\)
begin 
  interpretation \(d_x: \text{profile-single} d_x\) \(\langle\text{proof}\rangle\)
  interpretation \(d_y: \text{profile-single} d_y\) \(\langle\text{proof}\rangle\)

lemma strict1[simp, code-unfold]: \(f \text{ invalid} y = \text{invalid}\) \(\langle\text{proof}\rangle\)

lemma strict2[simp, code-unfold]: \(f x \text{ invalid} = \text{invalid}\) \(\langle\text{proof}\rangle\)

lemma cp0: \(f X Y \tau = f (\lambda -. X \tau) (\lambda -. Y \tau) \tau\) \(\langle\text{proof}\rangle\)

lemma cp[simp, code-unfold]: \(\text{cp} P \iff \text{cp} Q \iff \text{cp} (\lambda X. f (P X) (Q X))\) \(\langle\text{proof}\rangle\)

lemma def-homo[simp, code-unfold]: \(\delta(f x y) = (d_x x \text{ and } d_y y)\) \(\langle\text{proof}\rangle\)

lemma def-valid-then-def: \(v(f x y) = (\delta(f x y))\) \(\langle\text{proof}\rangle\)

lemma defined-args-valid: \((\tau \models \delta (f x y)) \iff ((\tau \models d_x x) \land (\tau \models d_y y))\) \(\langle\text{proof}\rangle\)

lemma const[simp, code-unfold]: 
  assumes \(C1: \text{const} X\) and \(C2: \text{const} Y\)
  shows \(\text{const}(f X Y)\) \(\langle\text{proof}\rangle\)
end

In our context, we will use Locales as “Property Profiles” for OCL operators; if an operator \(f\) is of profile \(\text{profile-bin-scheme defined} f g\) we know that it satisfies a number of properties like \text{strict1} or \text{strict2} i.e. \(f \text{ invalid} y = \text{invalid}\) and \(f \text{ null} y = \text{invalid}\). Since some of the more advanced Locales come with \(10 - 15\) theorems, property profiles represent a major structuring mechanism for the OCL library.

locale profile-bin-scheme-defined = 
  fixes \(d_y::('A', 'b::null)\) val \(\Rightarrow 'A\) Boolean 
  fixes \(f::('A', 'a::null)\) val \(\Rightarrow ('A', 'b::null)\) val \(\Rightarrow ('A', 'c::null)\) val 
  fixes \(g\)
  assumes \(d_y: \text{profile-single} d_y\)
assumes $d_y$-homo\[simp, code-unfold\]: \( cp(f X) \implies f X \text{ invalid} = \text{ invalid} \implies \)
\( \neg \tau \models d_y Y \implies \)
\( \tau \models \delta f X Y \equiv (\delta X \text{ and } d_y Y) \)
assumes def-scheme\[simplified\]: bin \( f \) \( g \) defined \( d_y X Y \)
assumes def-body': \( \bigwedge x y. \ x \neq \bot \implies x \neq \text{ null} \implies (d_y y) \tau = \text{ true} \implies g x (y \tau) \neq \bot \land g x (y \tau) \neq \text{ null} \)

begin

lemma strict3\[simp, code-unfold\]: \( f \text{ null } y = \text{ invalid} \)

end

sublocale profile-bin-scheme-defined defined \( < \) profile-bin-scheme defined

(\textit{proof})

locale profile-bin\(-d\):

fixes \( f \) :: \( \langle \alpha \cdot a::\text{null} \rangle \text{ val} \Rightarrow \langle \alpha \cdot b::\text{null} \rangle \text{ val} \)
fixes \( g \)
assumes def-scheme\[simplified\]: bin \( f \) \( g \) defined defined \( X Y \)
assumes def-body: \( \bigwedge x y. \ x \neq \bot \implies x \neq \text{ null} \implies y \neq \bot \implies y \neq \text{ null} \implies g x y \neq \bot \land g x y \neq \text{ null} \)

begin

lemma strict4\[simp, code-unfold\]: \( f x \text{ null } = \text{ invalid} \)

(\textit{proof})

end

sublocale profile-bin\(-d) \( < \) profile-bin-scheme-defined defined

(\textit{proof})

locale profile-bin\(-v) :

fixes \( f \) :: \( \langle \alpha \cdot a::\text{null} \rangle \text{ val} \Rightarrow \langle \alpha \cdot b::\text{null} \rangle \text{ val} \)
fixes \( g \)
assumes def-scheme\[simplified\]: bin \( f \) \( g \) defined valid \( X Y \)
assumes def-body: \( \bigwedge x y. \ x \neq \bot \implies x \neq \text{ null} \implies y \neq \bot \implies y \neq \text{ null} \implies g x y \neq \bot \land g x y \neq \text{ null} \)

sublocale profile-bin\(-v) \( < \) profile-bin-scheme valid valid \( f \)

λ \( x y. \langle x = y \rangle \)

(\textit{proof})

context profile-binStrongEq\(-v)

begin

lemma idem\[simp, code-unfold\]: \( f \text{ null } \text{ null } = \text{ true} \)

(\textit{proof})

lemma defargs: \( \tau \models f x y \implies (\tau \models v x) \land (\tau \models v y) \)

(\textit{proof})

lemma defined-args-valid': \( \delta f x y = (v x \text{ and } v y) \)

(\textit{proof})
lemma refl-ext[simp,code-unfold] : (f x x) = (if (v x) then true else invalid endif)
(proof)

lemma sym : τ |= (f x y) ⟹ τ |= (f y x)
(proof)

lemma symmetric : (f x y) = (f y x)
(proof)

lemma trans : τ |= (f x y) ⟹ τ |= (f y z) ⟹ τ |= (f x z)
(proof)

lemma StrictRefEq-vs-StrongEq: τ |= (v x) = τ |= (v y) ⟹ τ |= ((f x y) ≜ (x ≜ y)))
(proof)

locale profile-bin =
 fixes f :: ('A,α::null)val ⇒ ('A,β::null)val ⇒ ('A,γ::null)val
 fixes g
 assumes def-scheme[simplified]: bin f g valid valid X Y
 assumes def-body: \ x y. x\neq bot = y\neq bot = g x y ≠ bot ∧ g x y ≠ null
sublocale profile-bin < profile-bin-scheme valid valid
(proof)
end

theory UML-Boolean
imports ../UML-PropertyProfiles
begin

2.2.4. Fundamental Predicates on Basic Types: Strict (Referential) Equality

Here is a first instance of a definition of strict value equality—for the special case of the type 'A Boolean, it is just the strict extension of the logical equality:

overloading StrictRefEq ≡ StrictRefEq' : ([('A)Boolean,(A)Boolean] ⇒ ('A)Boolean
begin
  definition StrictRefEq_{boolean}[code-unfold] :
(x::('A)Boolean) ≜ y ≜ λ τ. if (v x) τ = true τ ∧ (v y) τ = true τ
  then (x ≜ y)τ
  else invalid τ
end

which implies elementary properties like:

lemma [simp,code-unfold] : (true ≜ false) = false
(proof)

lemma [simp,code-unfold] : (false ≜ true) = false
(proof)

lemma null-non-false [simp,code-unfold]:(null ≜ false) = false
(proof)

lemma null-non-true [simp,code-unfold]:(null ≜ true) = false
With respect to strictness properties and miscellaneous side-calculi, strict referential equality behaves on booleans as described in the profile-binStrongEq:

**interpretation** StrictRefEqBoolean : profile-binStrongEq-v-v λ x y. (x::(∀)Boolean) ≡ y

In particular, it is strict, cp-preserving and const-preserving. In particular, it generates the simplifier rules for terms like:

- **lemma** (invalid :: (∀)Boolean).= invalid (proof)
- **lemma** (true :: (∀)Boolean).= invalid (proof)
- **lemma** (false :: (∀)Boolean).= invalid (proof)
- **lemma** (true :: (∀)Boolean).= invalid (proof)

Thus, the weak equality is not reflexive.

### 2.2.5. Test Statements on Boolean Operations.

Here follows a list of code-examples, that explain the meanings of the above definitions by compilation to code and execution to True.

Elementary computations on Boolean

1. **Assert** τ |= v(true)
2. **Assert** τ |= δ(false)
3. **Assert** τ |≡ δ(null)
4. **Assert** τ |≡ δ(invalid)
5. **Assert** τ |= v((null::(∀)Boolean))
6. **Assert** τ |≡ v(invalid)
7. **Assert** τ |= (true and true) ≡ true
8. **Assert** τ |= (true or null) ≡ null
9. **Assert** τ |= (true or null) ≡ null
10. **Assert** τ |= (true ≡ false) ≡ false
11. **Assert** τ |= (invalid ≡ false) ≡ false
12. **Assert** τ |= (invalid ≡ false) ≡ invalid
13. **Assert** τ |= (true <>) false
14. **Assert** τ |= (false <>) true

end

**theory** UML-Void

**imports** ../UML-PropertyProfiles

**begin**

### 2.3. Basic Type Void: Operations

This minimal OCL type contains only two elements: invalid and null. Void could initially be defined as ⟨⟨unit⊥⟩⟩⊥, however the cardinal of this type is more than two, so it would have the cost to consider
Some None and Some (Some ()) seemingly everywhere.

### 2.3.1. Fundamental Properties on Voids: Strict Equality

**Definition**

**instantiation** \( \text{Void}_\text{base} :: \text{bot} \)

**begin**

**definition** \( \text{bot-Void-def}: (\text{bot-class}.\text{bot} :: \text{Void}_\text{base}) \equiv \text{Abs-Void}_\text{base} \text{None} \)

**instance** (proof)

**end**

**instantiation** \( \text{Void}_\text{base} :: \text{null} \)

**begin**

**definition** \( \text{null-Void-def}: (\text{null} :: \text{Void}_\text{base}) \equiv \text{Abs-Void}_\text{base} \upharpoonright \text{None}_\upharpoonright \)

**instance** (proof)

**end**

The last basic operation belonging to the fundamental infrastructure of a value-type in OCL is the weak equality, which is defined similar to the \( \lambda \) Void-case as strict extension of the strong equality:

**overloading** \( \text{StrictRefEq} \equiv \text{StrictRefEq} :: \lambda (\text{Void},(\text{Void}) \text{Void}) \Rightarrow (\text{Void})\text{Boolean} \)

**begin**

**definition** \( \text{StrictRefEq}_\text{Void}[\text{code-unfold}]: (x::(\text{Void}) \text{Void}) \equiv y \equiv \lambda \tau. \begin{align*} \text{if } (v \ x) \tau = \text{true } \& \ (v \ y) \tau = \text{true } \tau \\
\text{then } (x \equiv y) \tau \\
\text{else } \text{invalid } \tau \end{align*} \)

**end**

Property proof in terms of \( \text{profile-bin} \text{StrongEq}_\text{v}_\text{v} \text{-v} \)

**interpretation** \( \text{StrictRefEq}_\text{Void} : \text{profile-bin} \text{StrongEq}_\text{v}_\text{v} \lambda x y. (x::(\text{Void}) \text{Void}) \equiv y \)

### 2.3.2. Basic Void Constants

### 2.3.3. Validity and Definedness Properties

**lemma** \( \delta(\text{null}::(\text{Void}) \text{Void}) = \text{false} \text{ (proof)} \)

**lemma** \( \upsilon(\text{null}::(\text{Void}) \text{Void}) = \text{true} \text{ (proof)} \)

**lemma** [simp, code-unfold]: \( \delta (\lambda -. \text{Abs-Void}_\text{base} \upharpoonright \text{None}_\upharpoonright) = \text{false} \text{ (proof)} \)

**lemma** [simp, code-unfold]: \( \upsilon (\lambda -. \text{Abs-Void}_\text{base} \upharpoonright \text{None}_\upharpoonright) = \text{false} \text{ (proof)} \)

**lemma** [simp, code-unfold]: \( \delta (\lambda -. \text{Abs-Void}_\text{base} \downharpoonright \text{None}_\downharpoonright) = \text{false} \text{ (proof)} \)

**lemma** [simp, code-unfold]: \( \upsilon (\lambda -. \text{Abs-Void}_\text{base} \downharpoonright \text{None}_\downharpoonright) = \text{true} \text{ (proof)} \)

### 2.3.4. Test Statements

**Assert** \( \tau \models ((\text{null}::(\text{Void}) \text{Void}) \equiv \text{null}) \)
theory UML-Integer
imports ../UML-PropertyProfiles
begin

2.4. Basic Type Integer: Operations

2.4.1. Fundamental Predicates on Integers: Strict Equality

The last basic operation belonging to the fundamental infrastructure of a value-type in OCL is the weak
equality, which is defined similar to the \( A \) Boolean-case as strict extension of the strong equality:

overloading StrictRefEq \equiv \text{StrictRefEq} :: [\langle A \rangle \text{Integer},\langle A \rangle \text{Integer}] \Rightarrow \langle A \rangle \text{Boolean}

begin
  definition \text{StrictRefEq}_{\text{Integer}}[\text{code-unfold}] :
    \begin{align*}
      (x::\langle A \rangle \text{Integer}) \equiv y \equiv \lambda \tau. \text{if } (\upsilon x) \tau = \text{true} \tau \land (\upsilon y) \tau = \text{true} \tau \\
      \text{then } (x \triangleq y) \tau \\
      \text{else invalid } \tau
    \end{align*}
end

Property proof in terms of profile-bin\#\text{StrongEq}_v-v

interpretation \text{StrictRefEq}_{\text{Integer}} : profile-bin\#\text{StrongEq}_v-v \lambda x y. (x::\langle A \rangle \text{Integer}) \equiv y

(proof)

2.4.2. Basic Integer Constants

Although the remaining part of this library reasons about integers abstractly, we provide here as example
some convenient shortcuts.

definition \text{OclInt0} ::\langle A \rangle \text{Integer} \[(0)\] where \[0 = (\lambda \cdot \_0::\text{int}_\omega)\]
definition \text{OclInt1} ::\langle A \rangle \text{Integer} \[(1)\] where \[1 = (\lambda \cdot \_1::\text{int}_\omega)\]
definition \text{OclInt2} ::\langle A \rangle \text{Integer} \[(2)\] where \[2 = (\lambda \cdot \_2::\text{int}_\omega)\]
Etc.

definition \text{OclInt3} ::\langle A \rangle \text{Integer} \[(3)\] where \[3 = (\lambda \cdot \_3::\text{int}_\omega)\]
definition \text{OclInt4} ::\langle A \rangle \text{Integer} \[(4)\] where \[4 = (\lambda \cdot \_4::\text{int}_\omega)\]
definition \text{OclInt5} ::\langle A \rangle \text{Integer} \[(5)\] where \[5 = (\lambda \cdot \_5::\text{int}_\omega)\]
definition \text{OclInt6} ::\langle A \rangle \text{Integer} \[(6)\] where \[6 = (\lambda \cdot \_6::\text{int}_\omega)\]
definition \text{OclInt7} ::\langle A \rangle \text{Integer} \[(7)\] where \[7 = (\lambda \cdot \_7::\text{int}_\omega)\]
definition \text{OclInt8} ::\langle A \rangle \text{Integer} \[(8)\] where \[8 = (\lambda \cdot \_8::\text{int}_\omega)\]
definition \text{OclInt9} ::\langle A \rangle \text{Integer} \[(9)\] where \[9 = (\lambda \cdot \_9::\text{int}_\omega)\]
definition \text{OclInt10} ::\langle A \rangle \text{Integer} \[(10)\]where \[10 = (\lambda \cdot \_10::\text{int}_\omega)\]

2.4.3. Validity and Definedness Properties

lemma \( \delta(\text{null}::\langle A \rangle \text{Integer}) = \text{false} \) \(\langle\text{proof}\rangle\)
lemma \( \nu(\text{null}::\langle A \rangle \text{Integer}) = \text{true} \) \(\langle\text{proof}\rangle\)

lemma [simp,code-unfold]: \( \delta (\lambda\cdot \_n\omega) = \text{true} \) \(\langle\text{proof}\rangle\)

lemma [simp,code-unfold]: \( \nu (\lambda\cdot \_n\omega) = \text{true} \) \(\langle\text{proof}\rangle\)
2.4.4. Arithmetical Operations

Definition

Here is a common case of a built-in operation on built-in types. Note that the arguments must be both defined (non-null, non-bot).

Note that we can not follow the lexis of the OCL Standard for Isabelle technical reasons; these operators are heavily overloaded in the HOL library that a further overloading would lead to heavy technical buzz in this document.

definition OclAddInteger :: ('a)Integer ⇒ ('a)Integer ⇒ ('a)Integer (infix +int 40)
where x +int y ≡ λ τ. if (δ x) τ = true τ ∧ (δ y) τ = true τ
then x τ + τ y τ̃ else invalid τ

interpretation OclAddInteger : profile-bin_d' (+int) λ x y. (x τ + y τ̃)
(proof)

definition OclMinusInteger :: ('a)Integer ⇒ ('a)Integer ⇒ ('a)Integer (infix -int 41)
where x -int y ≡ λ τ. if (δ x) τ = true τ ∧ (δ y) τ = true τ
then x τ - τ y τ̃ else invalid τ

interpretation OclMinusInteger : profile-bin_d' (-int) λ x y. (x τ - y τ̃)
(proof)

definition OclMultInteger :: ('a)Integer ⇒ ('a)Integer ⇒ ('a)Integer (infix *int 45)
where x *int y ≡ λ τ. if (δ x) τ = true τ ∧ (δ y) τ = true τ
then x τ * τ y τ̃ else invalid τ

interpretation OclMultInteger : profile-bin_d' OclMultInteger λ x y. (x τ * y τ̃)
(proof)

Here is the special case of division, which is defined as invalid for division by zero.

definition OclDivisionInteger :: ('a)Integer ⇒ ('a)Integer ⇒ ('a)Integer (infix divint 45)
where x divint y ≡ λ τ. if (δ x) τ = true τ ∧ (δ y) τ = true τ
then if y τ ≠ OclInt0 τ then x τ div τ y τ̃ else invalid τ
else invalid τ

interpretation OclDivisionInteger : profile-bin_d' OclDivisionInteger λ x y. (x τ div y τ̃)
(proof)

definition OclModulusInteger :: ('a)Integer ⇒ ('a)Integer ⇒ ('a)Integer (infix modint 45)
where x modint y ≡ λ τ. if (δ x) τ = true τ ∧ (δ y) τ = true τ
then if y τ ≠ OclInt0 τ then x τ mod τ y τ̃ else invalid τ
else invalid τ
\[\text{definition } \text{OclLess}_{\text{Integer}} :: (\forall \text{Integer}) \Rightarrow (\forall \text{Integer}) \Rightarrow (\forall \text{Boolean}) \text{ (infix \(\leq_{\text{int}}\))} \]

\[\text{where } x \leq_{\text{int}} y \equiv \lambda \tau. \text{ if } (\delta x) \tau = \text{true } \tau \land (\delta y) \tau = \text{true } \tau \]
 \[\text{then } (\forall x, y) \tau \ni (\forall x^\tau < (\forall y^\tau \|)) \]
\[\text{else invalid } \tau\]

\[\text{interpretation } \text{OclLess}_{\text{Integer}} : \text{profile-bind-d} (\leq_{\text{int}}) \lambda x, y, (\forall x^\tau < (\forall y^\tau \|))\]
\[\text{proof}\]

\[\text{definition } \text{OclLe}_{\text{Integer}} :: (\forall \text{Integer}) \Rightarrow (\forall \text{Integer}) \Rightarrow (\forall \text{Boolean}) \text{ (infix \(\leq_{\text{int}}\))} \]

\[\text{where } x \leq_{\text{int}} y \equiv \lambda \tau. \text{ if } (\delta x) \tau = \text{true } \tau \land (\delta y) \tau = \text{true } \tau \]
\[\text{then } (\forall x, y) \tau \ni (\forall x^\tau \leq (\forall y^\tau \|)) \]
\[\text{else invalid } \tau\]

\[\text{interpretation } \text{OclLe}_{\text{Integer}} : \text{profile-bind-d} (\leq_{\text{int}}) \lambda x, y, (\forall x^\tau \leq (\forall y^\tau \|))\]
\[\text{proof}\]

Basic Properties

\[\text{lemma } \text{OclAdd}_{\text{Integer}}-\text{commute}: (X +_{\text{int}} Y) = (Y +_{\text{int}} X)\]
\[\text{proof}\]

Execution with Invalid or Null or Zero as Argument

\[\text{lemma } \text{OclAdd}_{\text{Integer}}-\text{zero1}[\text{simp,code-unfold}]: (x +_{\text{int}} 0) = (\text{if } v x \text{ and not } (\delta x) \text{ then invalid } x \text{ endif})\]
\[\text{proof}\]

\[\text{lemma } \text{OclAdd}_{\text{Integer}}-\text{zero2}[\text{simp,code-unfold}]: (0 +_{\text{int}} x) = (\text{if } v x \text{ and not } (\delta x) \text{ then invalid } x \text{ endif})\]
\[\text{proof}\]

2.4.5. Test Statements

Here follows a list of code-examples, that explain the meanings of the above definitions by compilation to code and execution to True.

\[\text{Assert } \tau \ni (9 \leq_{\text{int}} 10)\]
\[\text{Assert } \tau \ni ((4 +_{\text{int}} 4) \leq_{\text{int}} 10)\]
\[\text{Assert } \tau \ni \neg ((4 +_{\text{int}} (4 +_{\text{int}} 4)) <_{\text{int}} 10)\]
\[\text{Assert } \tau \ni \not\text{not } (v \text{ (null } +_{\text{int}} 1))\]
\[\text{Assert } \tau \ni (((0 *_{\text{int}} 4) \text{ div}_{\text{int}} 10) \leq_{\text{int}} 4)\]
\[\text{Assert } \tau \ni \not\text{not } (\delta (1 \text{ div}_{\text{int}} 0))\]
\[\text{Assert } \tau \ni \not\text{not } (v \text{ (1 } \text{ div}_{\text{int}} 0))\]

\[\text{lemma } \text{integer-non-null }[\text{simp}]: ((\lambda_. \_n_{\text{null}}) \ni (\text{null}: (\forall \text{Integer}))) = \text{false}\]
\[\text{proof}\]

\[\text{lemma } \text{null-non-integer }[\text{simp}]: ((\text{null}: (\forall \text{Integer})) \ni (\lambda_. \_n_{\text{null}})) = \text{false}\]
\[\text{proof}\]

\[\text{lemma } \text{OclInt0-non-null }[\text{simp,code-unfold}]: (0 \ni \text{null}) = \text{false}\]
\[\text{proof}\]

\[\text{lemma } \text{null-non-OclInt0 }[\text{simp,code-unfold}]: (\text{null} \ni 0) = \text{false}\]
\[\text{proof}\]

\[\text{lemma } \text{OclInt1-non-null }[\text{simp,code-unfold}]: (\text{null} \ni 1) = \text{false}\]
\[\text{proof}\]

\[\text{lemma } \text{null-non-OclInt1 }[\text{simp,code-unfold}]: (\text{null} \ni 1) = \text{false}\]
\[\text{proof}\]

73
lemma OclInt2-non-null [simp,code-unfold]: \(2 \neq \text{null} = \text{false}\) (proof)

lemma null-non-OclInt2 [simp,code-unfold]: \((\text{null} \neq 2) = \text{false}\) (proof)

lemma OclInt6-non-null [simp,code-unfold]: \(6 \neq \text{null} = \text{false}\) (proof)

lemma null-non-OclInt6 [simp,code-unfold]: \((\text{null} \neq 6) = \text{false}\) (proof)

lemma OclInt8-non-null [simp,code-unfold]: \(8 \neq \text{null} = \text{false}\) (proof)

lemma null-non-OclInt8 [simp,code-unfold]: \((\text{null} \neq 8) = \text{false}\) (proof)

lemma OclInt9-non-null [simp,code-unfold]: \(9 \neq \text{null} = \text{false}\) (proof)

lemma null-non-OclInt9 [simp,code-unfold]: \((\text{null} \neq 9) = \text{false}\) (proof)

Here follows a list of code-examples, that explain the meanings of the above definitions by compilation to code and execution to True.

Elementary computations on Integer

Assert \(\tau \models (0 <_{\text{int}} 2 \; \text{and} \; (0 <_{\text{int}} 1))\)

Assert \(\tau \models 1 <> 2\)

Assert \(\tau \models 2 <> 1\)

Assert \(\tau \models 2 \neq 2\)

begin

end

theory UML-Real
imports ../UML-PropertyProfiles
begin

2.5. Basic Type Real: Operations

2.5.1. Fundamental Predicates on Reals: Strict Equality

The last basic operation belonging to the fundamental infrastructure of a value-type in OCL is the weak equality, which is defined similar to the \(\mathbb{A}\) Boolean-case as strict extension of the strong equality:

overloading StrictRefEq \(\equiv\) StrictRefEq :: [(\(\mathbb{A}\)Real,(\(\mathbb{A}\)Real)] \(\Rightarrow\) (\(\mathbb{A}\))Boolean

begin

74
Although the remaining part of this library reasons about reals abstractly, we provide here as example some convenient shortcuts.

Note: For the sake of conciseness, we use 
\[ 0.0 = (\lambda \cdot \_0::real_{\tau}) \]
\[ 1.0 = (\lambda \cdot \_1::real_{\tau}) \]
\[ 2.0 = (\lambda \cdot \_2::real_{\tau}) \]
\[ 3.0 = (\lambda \cdot \_3::real_{\tau}) \]
\[ 4.0 = (\lambda \cdot \_4::real_{\tau}) \]
\[ 5.0 = (\lambda \cdot \_5::real_{\tau}) \]
\[ 6.0 = (\lambda \cdot \_6::real_{\tau}) \]
\[ 7.0 = (\lambda \cdot \_7::real_{\tau}) \]
\[ 8.0 = (\lambda \cdot \_8::real_{\tau}) \]
\[ 9.0 = (\lambda \cdot \_9::real_{\tau}) \]
\[ 10.0 = (\lambda \cdot \_10::real_{\tau}) \]
\[ \pi = (\lambda \cdot \_pi::real_{\tau}) \]

2.5.3. Validity and Definedness Properties

\[ \delta(null:(\forall \tau)Real) = false \] (proof)
\[ v(null:(\forall \tau)Real) = true \] (proof)

\[ simp.code-unfold: \delta (\lambda \cdot \_n::real_{\tau}) = true \] (proof)

\[ simp.code-unfold: v (\lambda \cdot \_n::real_{\tau}) = true \] (proof)

\[ simp.code-unfold: \delta 0.0 = true \] (proof)
\[ simp.code-unfold: v 0.0 = true \] (proof)
\[ simp.code-unfold: \delta 1.0 = true \] (proof)
\[ simp.code-unfold: v 1.0 = true \] (proof)
\[ simp.code-unfold: \delta 2.0 = true \] (proof)
\[ simp.code-unfold: v 2.0 = true \] (proof)
\[ simp.code-unfold: \delta 6.0 = true \] (proof)
\[ simp.code-unfold: v 6.0 = true \] (proof)
\[ simp.code-unfold: \delta 8.0 = true \] (proof)
\[ simp.code-unfold: v 8.0 = true \] (proof)
\[ simp.code-unfold: \delta 9.0 = true \] (proof)
\[ simp.code-unfold: v 9.0 = true \] (proof)
2.5.4. Arithmetical Operations

Definition

Here is a common case of a built-in operation on built-in types. Note that the arguments must be both defined (non-null, non-bot).

Note that we can not follow the lexis of the OCL Standard for Isabelle technical reasons; these operators are heavily overloaded in the HOL library that a further overloading would lead to heavy technical buzz in this document.

definition OclAddReal :: (\mathbb{R}) \Rightarrow (\mathbb{R}) \Rightarrow (\mathbb{R}) (infix +_real 40)
where x +_real y \equiv \lambda \tau. \text{if } (\delta x) \tau = \text{true} \ \land \ (\delta y) \tau = \text{true} \ \tau \ \text{then } \langle \langle x \tau \rangle + \langle y \tau \rangle \rangle \\
else \text{invalid } \tau

interpretation OclAddReal : profile-bind_d (+_real) \lambda x y. \langle \langle x \rangle + \langle y \rangle \rangle
(proof)

definition OclMultReal :: (\mathbb{R}) \Rightarrow (\mathbb{R}) \Rightarrow (\mathbb{R}) (infix *_real 45)
where x *_real y \equiv \lambda \tau. \text{if } (\delta x) \tau = \text{true} \ \land \ (\delta y) \tau = \text{true} \ \tau \ \text{then } \langle \langle x \tau \rangle \ast \langle y \tau \rangle \rangle \\
else \text{invalid } \tau

interpretation OclMultReal : profile-bind_d (*_real) OclMultReal \lambda x y. \langle \langle x \rangle \ast \langle y \rangle \rangle
(proof)

Here is the special case of division, which is defined as invalid for division by zero.

definition OclDivisionReal :: (\mathbb{R}) \Rightarrow (\mathbb{R}) \Rightarrow (\mathbb{R}) (infix \text{div}_real 45)
where x \text{div}_real y \equiv \lambda \tau. \text{if } (\delta x) \tau = \text{true} \ \land \ (\delta y) \tau = \text{true} \ \tau \ \text{then } \langle \langle x \tau \rangle / \langle y \tau \rangle \rangle \\
else \text{invalid } \tau

definition mod-float a b = a - \text{real-of-int} \ (\text{floor} \ (a / b)) \ast b

definition OclModulusReal :: (\mathbb{R}) \Rightarrow (\mathbb{R}) \Rightarrow (\mathbb{R}) (infix \text{mod}_real 45)
where x \text{mod}_real y \equiv \lambda \tau. \text{if } (\delta x) \tau = \text{true} \ \land \ (\delta y) \tau = \text{true} \ \tau \ \text{then } \langle \langle x \tau \rangle \mod \langle y \tau \rangle \rangle \\
else \text{invalid } \tau

definition OclLessReal :: (\mathbb{R}) \Rightarrow (\mathbb{R}) \Rightarrow (\mathbb{R}) (infix <_real 35)
where x <_real y \equiv \lambda \tau. \text{if } (\delta x) \tau = \text{true} \ \land \ (\delta y) \tau = \text{true} \ \tau \ \text{then } \langle \langle x \tau \rangle < \langle y \tau \rangle \rangle \\
else \text{invalid } \tau

interpretation OclLessReal : profile-bind_d (<_real) \lambda x y. \langle \langle x \rangle < \langle y \rangle \rangle
(proof)

definition OclLeReal :: (\mathbb{R}) \Rightarrow (\mathbb{R}) \Rightarrow (\mathbb{R}) (infix \leq_rea 35)
where x \leq_rea y \equiv \lambda \tau. \text{if } (\delta x) \tau = \text{true} \ \land \ (\delta y) \tau = \text{true} \ \tau \ \text{then } \langle \langle x \tau \rangle \leq \langle y \tau \rangle \rangle
interpretation $\text{OclAdd}$: \(\text{profile-bin}_{d\cdot a} (\leq_{\text{real}}) \lambda x, y. (\varpi x) \leq (\varpi y)\)

\langle proof \rangle

Basic Properties

lemma $\text{OclAdd}_\text{real-commute}$: \(X +_\text{real} Y = (Y +_\text{real} X)\)

\langle proof \rangle

Execution with Invalid or Null or Zero as Argument

lemma $\text{OclAdd}_\text{real-zero}1[\text{simp,code-unfold}]$:
\((x +_\text{real} 0.0) = (\text{if } v \text{ and not } (\delta x) \text{ then invalid else } x \text{ endif})\)

\langle proof \rangle

lemma $\text{OclAdd}_\text{real-zero}2[\text{simp,code-unfold}]$:
\((0.0 +_\text{real} x) = (\text{if } v \text{ and not } (\delta x) \text{ then invalid else } x \text{ endif})\)

\langle proof \rangle

2.5.5. Test Statements

Here follows a list of code-examples, that explain the meanings of the above definitions by compilation to code and execution to True.

Assert \(\tau \vdash (9.0 \leq_{\text{real}} 10.0)\)

Assert \(\tau \vdash (((4.0 +_\text{real} 4.0) \leq_{\text{real}} 10.0)\)

Assert \(\tau \vdash (\not(4.0 +_\text{real} (4.0 +_\text{real} 4.0)) <_{\text{real}} 10.0)\)

Assert \(\tau \vdash \not(\lambda \nu. ((\varpi \nu) = (null +_\text{real} 1.0))\)

Assert \(\tau \vdash (\not(\lambda \nu. ((\varpi \nu) \leq_{\text{real}} 4.0))\)

 Assert \(\tau \vdash \not(\lambda \nu. ((\varpi \nu) \leq_{\text{real}} 4.0))\)

lemma real-non-null [simp]: \((\lambda \nu. (\varpi \nu) \leq (null::(\forall \nu. \text{Real}))) = \text{false}\)

\langle proof \rangle

lemma null-non-real [simp]: \(((null::(\forall \nu. \text{Real}) \leq (\lambda \nu. (\varpi \nu))) = \text{false}\)

\langle proof \rangle

lemma $\text{OclReal0}_\text{null-non}$[simp,code-unfold]: \((0.0 \leq \text{null}) = \text{false}\)

\langle proof \rangle

lemma null-non-$\text{OclReal0}_\text{null}$[simp,code-unfold]: \((\text{null} \equiv 0.0) = \text{false}\)

\langle proof \rangle

lemma $\text{OclReal1}_\text{null-non}$[simp,code-unfold]: \((1.0 \equiv \text{null}) = \text{false}\)

\langle proof \rangle

lemma null-non-$\text{OclReal1}_\text{null}$[simp,code-unfold]: \((\text{null} \equiv 1.0) = \text{false}\)

\langle proof \rangle

lemma $\text{OclReal2}_\text{null-non}$[simp,code-unfold]: \((2.0 \equiv \text{null}) = \text{false}\)

\langle proof \rangle

lemma null-non-$\text{OclReal2}_\text{null}$[simp,code-unfold]: \((\text{null} \equiv 2.0) = \text{false}\)

\langle proof \rangle

lemma $\text{OclReal6}_\text{null-non}$[simp,code-unfold]: \((6.0 \equiv \text{null}) = \text{false}\)

\langle proof \rangle

lemma null-non-$\text{OclReal6}_\text{null}$[simp,code-unfold]: \((\text{null} \equiv 6.0) = \text{false}\)

\langle proof \rangle

lemma $\text{OclReal8}_\text{null-non}$[simp,code-unfold]: \((8.0 \equiv \text{null}) = \text{false}\)

\langle proof \rangle

lemma null-non-$\text{OclReal8}_\text{null}$[simp,code-unfold]: \((\text{null} \equiv 8.0) = \text{false}\)

\langle proof \rangle

lemma $\text{OclReal9}_\text{null-non}$[simp,code-unfold]: \((9.0 \equiv \text{null}) = \text{false}\)

\langle proof \rangle

lemma null-non-$\text{OclReal9}_\text{null}$[simp,code-unfold]: \((\text{null} \equiv 9.0) = \text{false}\)

\langle proof \rangle

Here follows a list of code-examples, that explain the meanings of the above definitions by compilation to code and execution to True.

Elementary computations on Real

assert \(\tau \vdash 1.0 \ll 2.0\)
2.6. Basic Type String: Operations

2.6.1. Fundamental Properties on Strings: Strict Equality

The last basic operation belonging to the fundamental infrastructure of a value-type in OCL is the weak equality, which is defined similar to the $\mathbf{A}$ Boolean-case as strict extension of the strong equality:

overloading $\text{StrictRefEq} \equiv \text{StrictRefEq} : (\mathbf{A})\text{String} \rightarrow (\mathbf{A})\text{Boolean}$

begin

definition $\text{StrictRefEq}_{\text{String}}$[code-unfold] :

$(x::(\mathbf{A})\text{String}) \doteq y \equiv \lambda \tau. \begin{cases} 
\text{true} & \text{if } \tau = \text{true} \land \tau = \text{true} \\
\text{invalid} & \text{else}
\end{cases}$

end

Property proof in terms of $\text{profile-bin}_{\text{StrongEq}-v-v}$

interpretation $\text{StrictRefEq}_{\text{String}} : \text{profile-bin}_{\text{StrongEq}-v-v} \lambda x y. (x::(\mathbf{A})\text{String}) \doteq y$

(proof)

2.6.2. Basic String Constants

Although the remaining part of this library reasons about integers abstractly, we provide here as example some convenient shortcuts.

definition $\text{OclString} : (\mathbf{A})\text{String} (a)$ where $a = (\lambda u. a^u) u$
2.6.3. Validity and Definedness Properties

lemma \( \delta (\text{null} :: (\mathcal{A}) \text{String}) = \text{false} \) \langle proof \rangle

lemma \( \nu (\text{null} :: (\mathcal{A}) \text{String}) = \text{true} \) \langle proof \rangle

lemma \[ \text{simp, code-unfold}: \delta (\lambda \cdot \_ n) = \text{true} \] \langle proof \rangle

lemma \[ \text{simp, code-unfold}: \nu (\lambda \cdot \_ n) = \text{true} \] \langle proof \rangle

2.6.4. String Operations

Definition

Here is a common case of a built-in operation on built-in types. Note that the arguments must be both defined (non-null, non-bot).

Note that we cannot follow the lexis of the OCL Standard for Isabelle technical reasons; these operators are heavily overloaded in the HOL library that a further overloading would lead to heavy technical buzz in this document.

definition \( \text{OclAdd} \) :: \( (\mathcal{A}) \text{String} \Rightarrow (\mathcal{A}) \text{String} \Rightarrow (\mathcal{A}) \text{String} \) \( \text{(infix } +\text{string } 40) \)
where \( x +\text{string } y \equiv \lambda \tau. \) if \( (\delta x) \tau = \text{true} \) \& \( (\delta y) \tau = \text{true} \) then \( \_ \text{concat } [\tau x, \tau y]_{\omega} \)
else invalid \( \tau \)
interpretation \( \text{OclAdd} : \text{profile-bin-d} \ ( +\text{string } ) \lambda x y. \_ \text{concat } [\tau x, \tau y]_{\omega} \)

Basic Properties

lemma \( \text{OclAdd-String-not-commute}: \exists X Y. (X +\text{string } Y) \neq (Y +\text{string } X) \)
\langle proof \rangle

2.6.5. Test Statements

Here follows a list of code-examples, that explain the meanings of the above definitions by compilation to code and execution to \textit{True}.

Here follows a list of code-examples, that explain the meanings of the above definitions by compilation to code and execution to \textit{True}.

Elementary computations on \textit{String}

Assert \( \tau \models a \leftrightarrow b \)
Assert \( \tau \models b \leftrightarrow a \)
Assert \( \tau \models b = b \)

Assert \( \tau \models v a \)
Assert \( \tau \models \delta a \)
Assert \( \tau \models v (\text{null} :: (\mathcal{A}) \text{String}) \)
2.7. Collection Type Pairs: Operations

The OCL standard provides the concept of Tuples, i.e. a family of record-types with projection functions. In FeatherWeight OCL, only the theory of a special case is developed, namely the type of Pairs, which is, however, sufficient for all applications since it can be used to mimic all tuples. In particular, it can be used to express operations with multiple arguments, roles of n-ary associations, ...

2.7.1. Semantic Properties of the Type Constructor

---

2.7.2. Fundamental Properties of Strict Equality

After the part of foundational operations on sets, we detail here equality on sets. Strong equality is inherited from the OCL core, but we have to consider the case of the strict equality. We decide to overload strict equality in the same way we do for other value's in OCL:

---
\[(x: (\mathcal{A},'\alpha::null,'\beta::null)\text{Pair}) \equiv y) \equiv (\lambda \tau. \text{if } (v \ x) \tau = \text{true } \land (v \ y) \tau = \text{true } \tau \text{then } (x \triangleq y)\tau \text{else invalid } \tau)
\]

end

Property proof in terms of \(\text{profile-bin}_{\text{StrongEq}} \cdot v \cdot v\)

interpretation \(\text{StrictRefEq}_\text{Pair} : \text{profile-bin}_{\text{StrongEq}} \cdot v \cdot v \lambda \ x \ y. \ (x:(\mathcal{A},'\alpha::null,'\beta::null)\text{Pair}) \equiv y\)

\[\langle \text{proof} \rangle\]

2.7.3. Standard Operations Definitions

This part provides a collection of operators for the Pair type.

Definition: Pair Constructor

definition \(\text{OclPair}: \forall \mathcal{A}, \forall \alpha::null, \forall \beta::null\) val \Rightarrow
\(\mathcal{A}, \beta\) val \Rightarrow
\(\mathcal{A},'\alpha::null,'\beta::null\) \text{Pair} \ (\text{Pair} \{-\},\{\})
where \(\text{Pair}\{X,Y\} \equiv \lambda \tau. \text{if } (\delta X) \tau = \text{true } \tau \text{then } \text{Abs-Pair}_{\text{base}}(X \tau, Y \tau)_{\|} \text{else invalid } \tau)

interpretation \(\text{OclPair} : \text{profile-bin}_{\text{v}} \cdot v\)
\(\text{OclPair} \lambda \ x \ y. \ \text{Abs-Pair}_{\text{base}}(x, y)_{\|}\)
\[\langle \text{proof} \rangle\]

Definition: First

definition \(\text{OclFirst}: \forall \mathcal{A},'\alpha::null,'\beta::null\) \text{Pair} \Rightarrow \forall \mathcal{A}, '\alpha\) val \ (\cdot .\text{First}('))
where \(X .\text{First}() \equiv \lambda \tau. \text{if } (\delta X) \tau = \text{true } \tau \text{then } \text{fst } \text{Rep-Pair}_{\text{base}}(X \tau)_{\|} \text{else invalid } \tau)

interpretation \(\text{OclFirst} : \text{profile-mono}_{\text{d}}\ \text{OclFirst} \lambda \ x. \ \text{fst } \text{Rep-Pair}_{\text{base}}(x)_{\|}\)
\[\langle \text{proof} \rangle\]

Definition: Second

definition \(\text{OclSecond}: \forall \mathcal{A},'\alpha::null,'\beta::null\) \text{Pair} \Rightarrow \forall \mathcal{A}, '\beta\) val \ (\cdot .\text{Second}('))
where \(X .\text{Second}() \equiv \lambda \tau. \text{if } (\delta X) \tau = \text{true } \tau \text{then } \text{snd } \text{Rep-Pair}_{\text{base}}(X \tau)_{\|} \text{else invalid } \tau)

interpretation \(\text{OclSecond} : \text{profile-mono}_{\text{d}}\ \text{OclSecond} \lambda \ x. \ \text{snd } \text{Rep-Pair}_{\text{base}}(x)_{\|}\)
\[\langle \text{proof} \rangle\]

2.7.4. Logical Properties

lemma 1 : \(\tau \vdash v \ Y \Rightarrow \tau \vdash \text{Pair}\{X,Y\}.\text{First}() \triangleq X\)
\[\langle \text{proof} \rangle\]

lemma 2 : \(\tau \vdash v \ X \Rightarrow \tau \vdash \text{Pair}\{X,Y\}.\text{Second}() \triangleq Y\)
\[\langle \text{proof} \rangle\]
2.7.5. Algebraic Execution Properties

lemma proj1-exec [simp, code-unfold]: Pair\{X,Y\}.First() = (if (υ Y) then X else invalid endif) (proof)

lemma proj2-exec [simp, code-unfold]: Pair\{X,Y\}.Second() = (if (υ X) then Y else invalid endif) (proof)

2.7.6. Test Statements

instantiation Pair\_base :: (equal,equal)equal
begin
definition HOL.equal k l ←→ (k::('a::equal,'b::equal)Pair\_base) = l
instance (proof)
end

lemma equal-Pair\_base-code [code]:
HOL.equal k (l::('a::{equal,null},'b::{equal,null})Pair\_base) ←→ Rep-Pair\_base k = Rep-Pair\_base l (proof)

Assert τ |≡ invalid .First() ≡ invalid
Assert τ |≡ null .First() ≡ invalid
Assert τ |≡ Pair{invalid, true} ≡ invalid
Assert τ |≡ v(Pair{null, true}).First())
Assert τ |≡ (Pair{null, true}).First() ≡ null
Assert τ |≡ (Pair{null, Pair{true,invalid}})).First() ≡ invalid

end

theory UML-Bag
imports ../basic-types/UML-Void
../basic-types/UML-Boolean
../basic-types/UML-Integer
../basic-types/UML-String
../basic-types/UML-Real
begin

no-notation None (⊥)

2.8. Collection Type Bag: Operations

definition Rep-Bag-base\' x = {\{x0, y\} . y < x\} x0 }
definition Rep-Bag-base x τ = {\{x0, y\} . y < x\} x\ τ x0 }
definition Rep-Set-base x τ = fst \{\{x0, y\} . y < x\} x\ τ x0 }
definition ApproxEq (infixl ≃ 30)
where X ≃ Y ≡ λ τ. \_Rep-Set-base X τ = Rep-Set-base Y τ \_
2.8.1. As a Motivation for the (infinite) Type Construction: Type-Extensions as Bags

Our notion of typed bag goes beyond the usual notion of a finite executable bag and is powerful enough to capture the extension of a type in UML and OCL. This means we can have in Featherweight OCL Bags containing all possible elements of a type, not only those (finite) ones representable in a state. This holds for base types as well as class types, although the notion for class-types — involving object id’s not occurring in a state — requires some care.

In a world with invalid and null, there are two notions extensions possible:

1. the bag of all defined values of a type \( T \) (for which we will introduce the constant \( T \))
2. the bag of all valid values of a type \( T \), so including null (for which we will introduce the constant \( T_{null} \)).

We define the bag extensions for the base type Integer as follows:

\[
\text{definition} \quad \text{Integer} :: (\forall A. \text{Integer}_{base}) \text{ Bag} \\
\text{where} \quad \text{Integer} \equiv (\lambda \tau. (\text{Abs-Bag}_{base} \circ \text{Some} \circ \text{Some}) (\lambda \text{None} \Rightarrow 0 \mid \text{Some} \text{None} \Rightarrow 0 \mid \text{-} \Rightarrow 1))
\]

\[
\text{definition} \quad \text{Integer}_{null} :: (\forall A. \text{Integer}_{base}) \text{ Bag} \\
\text{where} \quad \text{Integer}_{null} \equiv (\lambda \tau. (\text{Abs-Bag}_{base} \circ \text{Some} \circ \text{Some}) (\lambda \text{None} \Rightarrow 0 \mid \text{-} \Rightarrow 1))
\]

\[
\text{lemma} \quad \text{Integer-defined} : \delta \text{Integer} = \text{true} \\
\text{lemma} \quad \text{Integer}_{null}-defined : \delta \text{Integer}_{null} = \text{true}
\]

This allows the theorems:

\[
\tau \models \delta x \Rightarrow \tau \models (\text{Integer->includesBag}(x)) \quad \tau \models \delta x \Rightarrow \tau \models \text{Integer} \triangleq (\text{Integer->includingBag}(x))
\]

and

\[
\tau \models v x \Rightarrow \tau \models (\text{Integer}_{null}->\text{includesBag}(x)) \quad \tau \models v x \Rightarrow \tau \models \text{Integer}_{null} \triangleq (\text{Integer}_{null}->\text{includingBag}(x))
\]

which characterize the infiniteness of these bags by a recursive property on these bags.

In the same spirit, we proceed similarly for the remaining base types:

\[
\text{definition} \quad \text{Void}_{null} :: (\forall A. \text{Void}_{base}) \text{ Bag} \\
\text{where} \quad \text{Void}_{null} \equiv (\lambda \tau. (\text{Abs-Bag}_{base} \circ \text{Some} \circ \text{Some}) (\lambda x. \text{if } x = \text{Abs-Void}_{base} (\text{Some} \text{None}) \text{ then } 1 \text{ else } 0))
\]

\[
\text{definition} \quad \text{Void}_{empty} :: (\forall A. \text{Void}_{base}) \text{ Bag} \\
\text{where} \quad \text{Void}_{empty} \equiv (\lambda \tau. (\text{Abs-Bag}_{base} \circ \text{Some} \circ \text{Some}) (\lambda-. 0))
\]

\[
\text{lemma} \quad \text{Void}_{null}-defined : \delta \text{Void}_{null} = \text{true} \\
\text{lemma} \quad \text{Void}_{empty}-defined : \delta \text{Void}_{empty} = \text{true}
\]

\[
\text{lemma} \quad \text{assumes} \quad \tau \models \delta (V :: (\forall A. \text{Void}_{base}) \text{ Bag}) \\
\quad \text{shows} \quad \tau \models V \equiv \text{Void}_{null} \lor \tau \models V \equiv \text{Void}_{empty}
\]

\[
\text{definition} \quad \text{Boolean} :: (\forall A. \text{Boolean}_{base}) \text{ Bag} \\
\text{where} \quad \text{Boolean} \equiv (\lambda \tau. (\text{Abs-Bag}_{base} \circ \text{Some} \circ \text{Some}) (\lambda \text{None} \Rightarrow 0 \mid \text{Some} \text{None} \Rightarrow 0 \mid \text{-} \Rightarrow 1))
\]
definition Booleannull :: (\texttt{\textbackslash A}, Booleanbase) Bag
where \texttt{\textbackslash A} \equiv (\lambda \tau. (Abs-Bagbase o Some o Some) (\lambda None \Rightarrow 0 | - \Rightarrow 1))

lemma Boolean-defined : \delta Boolean = true (proof)
lemma Booleannull-defined : \delta Booleannull = true (proof)

definition String :: (\texttt{\textbackslash A}, Stringbase) Bag
where \texttt{\textbackslash A} \equiv (\lambda \tau. (Abs-Bagbase o Some o Some) (\lambda None \Rightarrow 0 | Some None \Rightarrow 0 | - \Rightarrow 1))

definition Stringnull :: (\texttt{\textbackslash A}, Stringbase) Bag
where \texttt{\textbackslash A} \equiv (\lambda \tau. (Abs-Bagbase o Some o Some) (\lambda None \Rightarrow 0 | - \Rightarrow 1))

lemma String-defined : \delta String = true (proof)
lemma Stringnull-defined : \delta Stringnull = true (proof)

definition Real :: (\texttt{\textbackslash A}, Realbase) Bag
where \texttt{\textbackslash A} \equiv (\lambda \tau. (Abs-Bagbase o Some o Some) (\lambda None \Rightarrow 0 | Some None \Rightarrow 0 | - \Rightarrow 1))

definition Realnull :: (\texttt{\textbackslash A}, Realbase) Bag
where \texttt{\textbackslash A} \equiv (\lambda \tau. (Abs-Bagbase o Some o Some) (\lambda None \Rightarrow 0 | - \Rightarrow 1))

lemma Real-defined : \delta Real = true (proof)
lemma Realnull-defined : \delta Realnull = true (proof)

2.8.2. Basic Properties of the Bag Type

Every element in a defined bag is valid.

lemma Bag-inv-lemma: \tau | (\delta X) \implies \top Rep-Bagbase (X \tau)\top bot = 0 (proof)

lemma Bag-inv-lemma':
assumes x-def : \tau | \delta X
and e-mem : \top Rep-Bagbase (X \tau)\top e \geq 1
shows \tau | \nu (\lambda-. e) (proof)

lemma abs-rep-simp':
assumes S-all-def : \tau | \delta S
shows Abs-Bagbase (\top Rep-Bagbase (S \tau)\top) = S \tau (proof)

lemma invalid-bag-OclNot-defined [simp, code-unfold]:\delta (invalid::(\texttt{\textbackslash A}, \alpha::null) Bag) = false (proof)
lemma null-bag-OclNot-defined [simp, code-unfold]:\delta (null::(\texttt{\textbackslash A}, \alpha::null) Bag) = false (proof)
lemma invalid-bag-valid [simp, code-unfold]:\nu (invalid::(\texttt{\textbackslash A}, \alpha::null) Bag) = false (proof)
lemma null-bag-valid [simp, code-unfold]:\nu (null::(\texttt{\textbackslash A}, \alpha::null) Bag) = true
2.8.3. Definition: Strict Equality

After the part of foundational operations on bags, we detail here equality on bags. Strong equality is inherited from the OCL core, but we have to consider the case of the strict equality. We decide to overload strict equality in the same way we do for other value’s in OCL:

overloading \( \text{StrictRefEq} \equiv \text{StrictRefEq} : [([\mathcal{A}, \alpha::\text{null}] \text{Bag}, ([\mathcal{A}, \alpha::\text{null}] \text{Bag}) \Rightarrow (\mathcal{A}) \text{Boolean} \]

begin
  definition \text{StrictRefEq}_\text{Bag} :
    (x::([\mathcal{A}, \alpha::\text{null}] \text{Bag})) = (y::([\mathcal{A}, \alpha::\text{null}] \text{Bag})) \equiv \lambda \tau. \text{if } (\delta x) \tau = \text{true} \land (\upsilon y) \tau = \text{true} \tau \text{ then } (x \not\cong y) \tau \text{ else invalid } \tau
  end

One might object here that for the case of objects, this is an empty definition. The answer is no, we will restrain later on states and objects such that any object has its oid stored inside the object (so the ref, under which an object can be referenced in the store will represented in the object itself). For such well-formed stores that satisfy this invariant (the WFF-invariant), the referential equality and the strong equality—and therefore the strict equality on bags in the sense above—coincides.

Property proof in terms of \text{profile-bin}_{\text{StrongEq}_{\text{v}_{\text{v}}}}

interpretation \( \text{StrictRefEq}_\text{Bag} : \text{profile-bin}_{\text{StrongEq}_{\text{v}_{\text{v}}}} \lambda x y. (x::([\mathcal{A}, \alpha::\text{null}] \text{Bag}) \not\cong y)

2.8.4. Constants: \text{mtBag}

definition \text{mtBag} : ([\mathcal{A}, \alpha::\text{null}] \text{Bag}) \Rightarrow (\mathcal{A}) \text{Bag}
where \text{Bag}\{} \equiv (\lambda \tau. \text{Abs-Bag base} \downarrow\downarrow (\lambda -\cdot 0 :: \text{nat}_\downarrow\downarrow))

lemma \text{mtBag-defined}[\text{simp, code-unfold}]: \delta (\text{Bag}\{\}) = \text{true}

lemma \text{mtBag-valid}[\text{simp, code-unfold}]: \upsilon (\text{Bag}\{\}) = \text{true}

lemma \text{mtBag-rep-bag} : \uparrow\text{Rep-Bag} \text{base} (\text{Bag}\{\}) = (\lambda -\cdot 0)

lemma [\text{simp, code-unfold}]: \text{const Bag}\{}

Note that the collection types in OCL allow for null to be included; however, there is the null-collection into which inclusion yields invalid.

2.8.5. Definition: \text{Including}

definition \text{OclIncluding} : ([\mathcal{A}, \alpha::\text{null}] \text{Bag}, ([\mathcal{A}, \alpha] \text{val}) \Rightarrow (\mathcal{A}) \text{Bag}
where \text{OclIncluding}\ x\ y = (\lambda \tau. \text{if } (\delta x) \tau = \text{true} \tau \land (\upsilon y) \tau = \text{true} \tau \text{ then Abs-Bag} \text{base}_{\downarrow\downarrow} \text{Rep-Bag} \text{base} (x\ \tau)_{\downarrow\downarrow} (y\ \tau + 1) \downarrow\downarrow (y\ \tau + 1))
2.8.6. Definition: Excluding

**Definition** \(\text{OclExcluding} \:: \ (\forall \alpha :: \text{null} \text{ Bag}, (\forall \alpha) \text{ Bag}) \Rightarrow (\forall \alpha) \text{ Bag} \)

where \(\text{OclExcluding\,} x\, y = (\lambda \tau. \text{ if } (\delta\, x)\, \tau = \text{true} \land (v\, y)\, \tau = \text{true} \tau \text{ then } A_{\text{Bag base}}\, (x\, \tau)_{\tau} \text{ then } (y\, \tau)_{\tau} = 0 :: \text{nat} \text{ else invalid } \tau) \)

**Notation** \(\text{OclExcluding\,} \rightarrow \text{excluding}_{B_{\text{ag}}} ('-') \)

**Interpretation** \(\text{OclExcluding\,} (\lambda\, x\, y. \text{Abs-Bag}_{\text{base}}(\text{Rep-Bag}_{\text{base}}(x)_{\tau})_{\tau}(y)_{\tau} = 0 :: \text{nat})_{\tau} \)

(proof)

2.8.7. Definition: Includes

**Definition** \(\text{OclIncludes} \:: \ (\forall \alpha :: \text{null} \text{ Bag}, (\forall \alpha) \text{ Bag}) \Rightarrow \forall \text{ Boolean} \)

where \(\text{OclIncludes}\, x\, y = (\lambda \tau. \text{ if } (\delta\, x)\, \tau = \text{true} \land (v\, y)\, \tau = \text{true} \tau \text{ then } A_{\text{Bag base}}\, (x\, \tau)_{\tau} \text{ then } (y\, \tau)_{\tau} > 0 \text{ else invalid } \tau) \)

**Notation** \(\text{OclIncludes\,} \rightarrow \text{including}_{B_{\text{ag}}} ('-') \)

**Interpretation** \(\text{OclIncludes\,} (\lambda\, x\, y. \text{Abs-Bag}_{\text{base}}(\text{Rep-Bag}_{\text{base}}(x)_{\tau})_{\tau}(y)_{\tau} > 0)_{\tau} \)

(proof)

2.8.8. Definition: Excludes

**Definition** \(\text{OclExcludes} \:: \ (\forall \alpha :: \text{null} \text{ Bag}, (\forall \alpha) \text{ Bag}) \Rightarrow \forall \text{ Boolean} \)

where \(\text{OclExcludes\,} x\, y = (\text{not}(\text{OclIncludes\,} x\, y)) \)

**Notation** \(\text{OclExcludes\,} \rightarrow \text{excluding}_{B_{\text{ag}}} ('-') \)

(proof)

The case of the size definition is somewhat special, we admit explicitly in Featherweight OCL the possibility of infinite bags. For the size definition, this requires an extra condition that assures that the cardinality of the bag is actually a defined integer.

**Interpretation** \(\text{OclExcludes\,} (\lambda\, x\, y. \text{Abs-Bag}_{\text{base}}(\text{Rep-Bag}_{\text{base}}(x)_{\tau})_{\tau}(y)_{\tau} \leq 0)_{\tau} \)

(proof)

2.8.9. Definition: Size

**Definition** \(\text{OclSize} \:: \ (\forall \alpha :: \text{null} \text{ Bag}) \Rightarrow \forall \text{ Integer} \)

where \(\text{OclSize\,} x = (\lambda \tau. \text{ if } (\delta\, x)\, \tau = \text{true} \land \text{finite } (\text{Rep-Bag-base}\, x\, \tau) \text{ then } \text{int}\, \text{(card}\, (\text{Rep-Bag-base}\, x\, \tau)) \text{ else invalid } \tau) \)

**Notation** \(\text{OclSize\,} \rightarrow \text{size}_{B_{\text{ag}}} ('-') \)
2.8.10. Definition: IsEmpty

definition OclIsEmpty :: (\text{'A}, \text{'a}::null) Bag => \text{'A} Boolean
where OclIsEmpty x = ((\nu x \text{ and } \text{not}(\delta x)) \text{ or } ((\text{OclSize} \ x) = 0))
notation OclIsEmpty \ (\lambda x \cdot (\text{not}(\text{OclEmpty} \ x)))

2.8.11. Definition: NotEmpty

definition OclNotEmpty :: (\text{'A}, \text{'a}::null) Bag => \text{'A} Boolean
where OclNotEmpty x = \text{not}(\text{OclIsEmpty} \ x)
notation OclNotEmpty \ (\lambda x \cdot (\text{not}(\text{OclEmpty} \ x)))

2.8.12. Definition: Any

definition OclANY :: [(\text{'A}, \text{'a}::null) Bag] => (\text{'A}, \text{'a}) val
where OclANY x = (\lambda \tau. \text{if } (\nu x) \tau = \text{true} \tau
then if (\delta x \text{ and } \text{OclNotEmpty} \ x) \tau = \text{true} \tau
then \text{SOME} \ \nu. \ y \in (\text{Rep-Set-base} \ x \tau)
else \text{null} \tau
else \bot)
notation OclANY \ (\lambda x \cdot (\text{any}_{\text{Bag}} \ \bot))

2.8.13. Definition: Forall

The definition of OclForall mimics the one of (and): OclForall is not a strict operation.

definition OclForall :: [(\text{'A}, \text{'a}::null) Bag, (\text{'A}, \text{'a}) val => (\text{'A}) Boolean] => (\text{'A}) Boolean
where OclForall S P = (\lambda \tau. \text{if } (\delta S) \tau = \text{true} \tau
then (\exists x \in \text{Rep-Set-base} S \tau. P (\lambda x) \tau = \text{false} \tau)
then false \tau
else if (\exists x \in \text{Rep-Set-base} S \tau. P (\lambda x) \tau = \text{invalid} \ \tau)
then invalid \ \tau
else if (\exists x \in \text{Rep-Set-base} S \tau. P (\lambda x) \tau = \text{null} \ \tau)
then null \ \tau
else true \ \tau
else \bot)
syntax -OclForallBag :: [(\text{'A}, \text{'a}::null) Bag, id, (\text{'A}) Boolean] => (\text{'A}) Boolean \ ((\cdot)\rightarrow \text{forAll}_{\text{Bag}} \ (\cdot | \cdot))
translations X\rightarrow \text{forAll}_{\text{Bag}}(x \mid P) \Rightarrow \text{CONST UML-Bag.OclForall} X (\%x. P)

2.8.14. Definition: Exists

Like OclForall, OclExists is also not strict.

definition OclExists :: [(\text{'A}, \text{'a}::null) Bag, (\text{'A}) val => (\text{'A}) Boolean] => (\text{'A}) Boolean
where OclExists S P = \text{not}(\text{UML-Bag.OclForall} S (\lambda X. \text{not} (P X)))
syntax -OclExistBag :: [(\text{'A}, \text{'a}::null) Bag, id, (\text{'A}) Boolean] => (\text{'A}) Boolean \ ((\cdot)\rightarrow \text{exists}_{\text{Bag}} \ (\cdot | \cdot))
translations X\rightarrow \text{exists}_{\text{Bag}}(x \mid P) \Rightarrow \text{CONST UML-Bag.OclExists} X (\%x. P)

The following definition follows the requirement of the standard to treat null as neutral element of bags. It is a well-documented exception from the general strictness rule and the rule that the distinguished argument self should be non-null.
2.8.15. Definition: Iterate

definition OclIterate :: [(\texttt{\textbackslash{}A},'\alpha::null) Bag, (\texttt{\textbackslash{}A},'\beta::null) val, (\texttt{\textbackslash{}A},'\alpha) val \Rightarrow (\texttt{\textbackslash{}A},'\beta) val] \Rightarrow (\texttt{\textbackslash{}A},'\beta) val
where OclIterate S A P = (\lambda \tau. \text{ if } (S \tau) = \text{ true } \tau \land (v A) \tau = \text{ true } \tau \land \text{ finite } (\text{Rep-Bag-base } S \tau) \text{ then } \text{Finite-Set.fold } (F o (\lambda a \tau. a) o fst) A (\text{Rep-Bag-base } S \tau) \tau)

syntax
- OclIterateBag :: [(\texttt{\textbackslash{}A},'\alpha::null) Bag, idt, idt, '\alpha, '\beta] \Rightarrow (\texttt{\textbackslash{}A},'\gamma) val
  (\cdot \rightarrow \text{iterate}_{\text{Bag}}(\cdot; \cdot; \cdot) )
translations
X \rightarrow \text{iterate}_{\text{Bag}}(a; x = A \mid P) \Rightarrow \text{CONST OclIterate } X A (\% a. (\% x. P))

2.8.16. Definition: Select

definition OclSelect :: [(\texttt{\textbackslash{}A},'\alpha::null) Bag, (\texttt{\textbackslash{}A},'\alpha) val \Rightarrow (\texttt{\textbackslash{}A},'\alpha) Bag
where OclSelect S P = (\lambda \tau. \text{ if } (S \tau) = \text{ true } \tau \text{ then } \text{null } \tau \text{ else Abs-Bag then invalid } \tau)

syntax
- OclSelectBag :: [(\texttt{\textbackslash{}A},'\alpha::null) Bag, idt, (\texttt{\textbackslash{}A},'\alpha) Boolean] \Rightarrow (\texttt{\textbackslash{}A},'\alpha) Bag
  (\cdot \rightarrow \text{select}_{\text{Bag}}(\cdot; \cdot)
translations
X \rightarrow \text{select}_{\text{Bag}}(x \mid P) \Rightarrow \text{CONST OclSelect } X (\% x. P)

2.8.17. Definition: Reject

definition OclReject :: [(\texttt{\textbackslash{}A},'\alpha::null) Bag, (\texttt{\textbackslash{}A},'\alpha) val \Rightarrow (\texttt{\textbackslash{}A},'\alpha) Bag
where OclReject S P = OclSelect S (not o P)

syntax
- OclRejectBag :: [(\texttt{\textbackslash{}A},'\alpha::null) Bag, idt, (\texttt{\textbackslash{}A},'\alpha) Boolean] \Rightarrow (\texttt{\textbackslash{}A},'\alpha) Bag
  (\cdot \rightarrow \text{reject}_{\text{Bag}}(\cdot; \cdot)
translations
X \rightarrow \text{reject}_{\text{Bag}}(x \mid P) \Rightarrow \text{CONST OclReject } X (\% x. P)

2.8.18. Definition: IncludesAll

definition OclIncludesAll :: [(\texttt{\textbackslash{}A},'\alpha::null) Bag, (\texttt{\textbackslash{}A},'\alpha) Bag \Rightarrow (\texttt{\textbackslash{}A},'\alpha) Bag
where OclIncludesAll x y = (\lambda \tau. \text{ if } (\delta x) \tau = \text{ true } \tau \land (\delta y) \tau = \text{ true } \tau \text{ then } \text{Rep-Bag-base } y \tau \subseteq \text{Rep-Bag-base } x \tau \text{ else } \bot)

notation OclIncludesAll (\dashrightarrow \text{includesAll}_{\text{Bag}}(\cdot))

interpretation OclIncludesAll : profile-bin^\dashrightarrow \dashrightarrow \text{OclIncludesAll } \lambda x. x \rightarrow \text{Rep-Bag-base}' y \subseteq \text{Rep-Bag-base}' x \downarrow
(proof)

2.8.19. Definition: ExcludesAll

definition OclExcludesAll :: [(\texttt{\textbackslash{}A},'\alpha::null) Bag, (\texttt{\textbackslash{}A},'\alpha) Bag \Rightarrow (\texttt{\textbackslash{}A},'\alpha) Bag
where OclExcludesAll x y = (\lambda \tau. \text{ if } (\delta x) \tau = \text{ true } \tau \land (\delta y) \tau = \text{ true } \tau \text{ then } \text{Rep-Bag-base } y \tau \cap \text{Rep-Bag-base } x \tau = \{ \}_\downarrow \text{ else } \bot)

notation OclExcludesAll (\dashrightarrow \text{excludesAll}_{\text{Bag}}(\cdot))
2.8.20. Definition: Union

**definition**

\[
\text{OclUnion} :: ([\langle\emptyset,\emptyset\rangle] \Rightarrow (\langle\emptyset,\emptyset\rangle) \Rightarrow (\langle\emptyset,\emptyset\rangle)
\]

**where**

\[
\text{OclUnion} x y = (\lambda \tau. \text{if } (x \tau) \text{ and } (y \tau) \text{ then } \text{true else invalid } \tau)
\]

**notation**

\[
\text{OclUnion} (-\rightarrow) (-)
\]

2.8.21. Definition: Intersection

**definition**

\[
\text{OclIntersection} :: ([\langle\emptyset,\emptyset\rangle] \Rightarrow (\langle\emptyset,\emptyset\rangle) \Rightarrow (\langle\emptyset,\emptyset\rangle)
\]

**where**

\[
\text{OclIntersection} x y = (\lambda \tau. \text{if } (x \tau) \text{ and } (y \tau) \text{ then } \text{true else invalid } \tau)
\]

**notation**

\[
\text{OclIntersection} (-\rightarrow) (-)
\]

2.8.22. Definition: Count

**definition**

\[
\text{OclCount} :: ([\langle\emptyset,\emptyset\rangle] \Rightarrow (\langle\emptyset,\emptyset\rangle) \Rightarrow (\langle\emptyset,\emptyset\rangle)
\]

**where**

\[
\text{OclCount} x y = (\lambda \tau. \text{if } (x \tau) \text{ and } (y \tau) \text{ then } \text{true else invalid } \tau)
\]

**notation**

\[
\text{OclCount} (-\rightarrow)
\]

2.8.23. Definition (future operators)

**consts**

\[
\text{OclSum} :: (\langle\emptyset,\emptyset\rangle) \Rightarrow (\langle\emptyset,\emptyset\rangle)
\]

**notation**

\[
\text{OclSum} (-\rightarrow)
\]

2.8.24. Logical Properties

**lemma**

\[
\text{OclIncluding-valid-args-valid:}
\]

\[
(\tau \vdash v \text{X-\rightarrow-including}_{\text{Bag}}(x)) = ((\tau \vdash (\delta X)) \land (\tau \vdash (v x)))
\]

**proof**

89
lemma OclIncluding-valid-args-valid:\[\text{simp, code-unfold}]:
\(\nu(X \rightarrow including_{Bag}(x)) = ((\delta X) \text{ and } (\nu x))\)
(proof)

e tc. etc.

OclExcluding

lemma OclExcluding-valid-args-valid:
\((\tau \models \nu(X \rightarrow excluding_{Bag}(x))) = ((\tau \models (\delta X)) \text{ and } (\tau \models (\nu x)))\)
(proof)

lemma OclExcluding-valid-args-valid\'[\text{simp, code-unfold}]:
\(\nu(X \rightarrow excluding_{Bag}(x)) = ((\delta X) \text{ and } (\nu x))\)
(proof)

OclIncludes

lemma OclIncludes-valid-args-valid:
\((\tau \models \nu(X \rightarrow includes_{Bag}(x))) = ((\tau \models (\delta X)) \text{ and } (\tau \models (\nu x)))\)
(proof)

lemma OclIncludes-valid-args-valid\'[\text{simp, code-unfold}]:
\(\nu(X \rightarrow includes_{Bag}(x)) = ((\delta X) \text{ and } (\nu x))\)
(proof)

OclExcludes

lemma OclExcludes-valid-args-valid:
\((\tau \models \nu(X \rightarrow excludes_{Bag}(x))) = ((\tau \models (\delta X)) \text{ and } (\tau \models (\nu x)))\)
(proof)

lemma OclExcludes-valid-args-valid\'[\text{simp, code-unfold}]:
\(\nu(X \rightarrow excludes_{Bag}(x)) = ((\delta X) \text{ and } (\nu x))\)
(proof)

OclSize

lemma OclSize-defined-args-valid: \(\tau \models \delta (X \rightarrow size_{Bag}()) \implies \tau \models \delta X\)
(proof)

lemma OclSize-infinite:
assumes non-finite: \(\tau \models \not(\delta(S \rightarrow size_{Bag}())\)
shows \((\tau \models \not(\delta(S))) \lor \text{ finite } (\text{Rep-Bag-base } S \tau)\)
(proof)

lemma \(\tau \models \delta X \implies \text{ finite } (\text{Rep-Bag-base } X \tau) \implies \neg \tau \models \delta (X \rightarrow size_{Bag}())\)
(proof)

lemma size-defined:
assumes X-finite: \(\bigwedge \tau. \text{ finite } (\text{Rep-Bag-base } X \tau)\)
shows \(\delta (X \rightarrow size_{Bag}()) = \delta X\)
(proof)

lemma size-defined':
assumes X-finite: finite (Rep-Bag-base X \tau)
shows \((\tau \models \delta (X \rightarrow size_{Bag}())) = (\tau \models \delta X)\)
(proof)

OclIsEmpty
lemma OclIsEmpty-defined-args-valid: \( \tau \models \delta (X \rightarrow \text{isEmpty}_{B_{ag}}()) \implies \tau \models \nu X \)
\{proof\}

lemma \( \tau \models \delta (\text{null} \rightarrow \text{isEmpty}_{B_{ag}}()) \)
\{proof\}

lemma OclIsEmpty-infinite: \( \tau \models \delta X \implies \neg \text{finite} (\text{Rep-Bag-base } X \ \tau) \implies \neg \tau \models \delta (X \rightarrow \text{isEmpty}_{B_{ag}}()) \)
\{proof\}

OclNotEmpty

lemma OclNotEmpty-defined-args-valid: \( \tau \models \delta (X \rightarrow \text{notEmpty}_{B_{ag}}()) \implies \tau \models \nu X \)
\{proof\}

lemma \( \tau \models \delta (\text{null} \rightarrow \text{notEmpty}_{B_{ag}}()) \)
\{proof\}

lemma OclNotEmpty-infinite: \( \tau \models \delta X \implies \neg \text{finite} (\text{Rep-Bag-base } X \ \tau) \implies \neg \tau \models \delta (X \rightarrow \text{notEmpty}_{B_{ag}}()) \)
\{proof\}

OclNotEmpty-has-elt

lemma OclNotEmpty-has-elt': \( \tau \models \delta X \implies \exists e. e \in (\text{Rep-Bag-base } X \ \tau) \)
\{proof\}

OclANY

lemma OclANY-defined-args-valid: \( \tau \models \delta (X \rightarrow \text{any}_{B_{ag}}()) \implies \tau \models \delta X \)
\{proof\}

lemma \( \tau \models \delta X \implies \tau \models X \rightarrow \text{isEmpty}_{B_{ag}}() \implies \neg \tau \models \delta (X \rightarrow \text{any}_{B_{ag}}()) \)
\{proof\}

lemma OclANY-valid-args-valid:
\( (\tau \models \nu(X \rightarrow \text{any}_{B_{ag}}())) = (\tau \models \nu X) \)
\{proof\}

lemma OclANY-valid-args-valid'\{simp, code-unfold\}:
\( \nu(X \rightarrow \text{any}_{B_{ag}}()) = (\nu X) \)
\{proof\}

2.8.25. Execution Laws with Invalid or Null or Infinite Set as Argument

OclIncluding

OclExcluding

OclIncludes

OclExcludes

OclSize

lemma OclSize-invalid\{simp, code-unfold\}: (invalid \rightarrow \text{size}_{B_{ag}}()) = invalid
\{proof\}
lemma OclSize-null [simp, code-unfold]: \( \text{null} \rightarrow \text{size}_{Bag}(()) = \text{invalid} \)  
(proof)

OclIsEmpty

lemma OclIsEmpty-invalid [simp, code-unfold]: \((\text{invalid} \rightarrow \text{isEmpty}_{Bag}(())) = \text{invalid} \)  
(proof)

lemma OclIsEmpty-null [simp, code-unfold]: \( \text{null} \rightarrow \text{isEmpty}_{Bag}(()) = \text{true} \)  
(proof)

OclNotEmpty

lemma OclNotEmpty-invalid [simp, code-unfold]: \((\text{invalid} \rightarrow \text{notEmpty}_{Bag}(()) = \text{invalid} \)  
(proof)

lemma OclNotEmpty-null [simp, code-unfold]: \( \text{null} \rightarrow \text{notEmpty}_{Bag}(()) = \text{false} \)  
(proof)

OclANY

lemma OclANY-invalid [simp, code-unfold]: \((\text{invalid} \rightarrow \text{any}_{Bag}(()) = \text{invalid} \)  
(proof)

lemma OclANY-null [simp, code-unfold]: \( \text{null} \rightarrow \text{any}_{Bag}(()) = \text{null} \)  
(proof)

OclForall

lemma OclForall-invalid [simp, code-unfold]: \((\text{invalid} \rightarrow \forall_{Bag}(a \mid P a) = \text{invalid} \)  
(proof)

lemma OclForall-null [simp, code-unfold]: \( \text{null} \rightarrow \forall_{Bag}(a \mid P a) = \text{invalid} \)  
(proof)

OclExists

lemma OclExists-invalid [simp, code-unfold]: \((\text{invalid} \rightarrow \exists_{Bag}(a \mid P a) = \text{invalid} \)  
(proof)

lemma OclExists-null [simp, code-unfold]: \( \text{null} \rightarrow \exists_{Bag}(a \mid P a) = \text{invalid} \)  
(proof)

OclIterate

lemma OclIterate-invalid [simp, code-unfold]: \((\text{invalid} \rightarrow \text{iterate}_{Bag}(a; x = A \mid P a x) = \text{invalid} \)  
(proof)

lemma OclIterate-null [simp, code-unfold]: \( \text{null} \rightarrow \text{iterate}_{Bag}(a; x = A \mid P a x) = \text{invalid} \)  
(proof)

lemma OclIterate-invalid-args [simp, code-unfold]: \( S \rightarrow \text{iterate}_{Bag}(a; x = \text{invalid} \mid P a x) = \text{invalid} \)  
(proof)

An open question is this ...

lemma \( S \rightarrow \text{iterate}_{Bag}(a; x = \text{null} \mid P a x) = \text{invalid} \)  
(proof)

lemma OclIterate-infinite:

assumes non-finite: \( \tau \models \text{not}(\delta(S \rightarrow \text{size}_{Bag}())) \)

shows \( (\text{OclIterate S A F}) \tau = \text{invalid} \)  
\( \tau \)
proof

lemma OclSelect-invalid [simp, code-unfold]: invalid ⇒ select \( B_a \) (\( P a \)) = invalid

proof

lemma OclSelect-null [simp, code-unfold]: null ⇒ select \( B_a \) (\( P a \)) = invalid

OclReject

lemma OclReject-invalid [simp, code-unfold]: invalid ⇒ reject \( B_a \) (\( P a \)) = invalid

lemma OclReject-null [simp, code-unfold]: null ⇒ reject \( B_a \) (\( P a \)) = invalid

Context Passing

lemma cp-OclIncludes1:
(\( X \) ⇒ includes \( B_a \) (\( x \))) \( \tau \) = (\( X \) ⇒ includes \( \lambda \cdot \ x \ \tau \)) \( \tau \)

proof

lemma cp-OclSize: \( X \) ⇒ size \( B_a \) () \( \tau \) = ((\( \lambda \cdot \ X \ \tau \)) ⇒ size \( B_a \)) \( \tau \)

proof

lemma cp-OclIsEmpty: \( X \) ⇒ isEmpty \( B_a \) () \( \tau \) = ((\( \lambda \cdot \ X \ \tau \)) ⇒ isEmpty \( B_a \)) \( \tau \)

proof

lemma cp-OclNotEmpty: \( X \) ⇒ notEmpty \( B_a \) () \( \tau \) = ((\( \lambda \cdot \ X \ \tau \)) ⇒ notEmpty \( B_a \)) \( \tau \)

proof

lemma cp-OclANY: \( X \) ⇒ any \( B_a \) () \( \tau \) = ((\( \lambda \cdot \ X \ \tau \)) ⇒ any \( B_a \)) \( \tau \)

proof

lemma cp-OclForall:
(\( S \) ⇒ forall \( B_a \) (\( x \) | \( P x \))) \( \tau \) = ((\( \lambda \cdot \ S \ \tau \)) ⇒ forall \( B_a \) (\( x \) | \( P \ ( \lambda \cdot \ x \ \tau ) \))) \( \tau \)

proof

lemma cp-OclForall1 [simp, intro]:
cp \( S \) \( \Rightarrow \) cp \( \lambda X. \ ((S X) ⇒ forall \( B_a \) (\( x \) | \( P x \))))

proof

lemma
cp \( \lambda X \ St \ x. \ P \ (\lambda \cdot \ x) \ X \ St \) \( \Rightarrow \) cp \( S \) \( \Rightarrow \) cp \( \lambda X. \ (S X) ⇒ forall \( B_a \) (\( x \) | \( P x X \)))

proof

lemma
cp \( S \) \( ⇒ \)
(\( \bigwedge \ x. \ CP \ (P x) \)) \( ⇒ \)
cp(\( \lambda X. \ ((S X) ⇒ forall \( B_a \) (\( x \) | \( P x X \))))

proof

lemma cp-OclExists:
(\( S \) ⇒ exists \( B_a \) (\( x \) | \( P x \))) \( \tau \) = ((\( \lambda \cdot \ S \ \tau \)) ⇒ exists \( B_a \) (\( x \) | \( P \ (\lambda \cdot \ x \ \tau ) \))) \( \tau \)

proof
lemma cp-OclExists1: simp, intro!
\[ cp \ S = \Rightarrow cp (\lambda X. ((S \ X) -\exists B a_g(x | P \ a x))) \]

(\langle proof \rangle)

lemma cp-OclIterate: simp, intro!
\[ (X -\Rightarrow iterate_{B a_g}(a; x = A | P \ a x)) \tau = \]
\[ ((\lambda -. X \tau) -\Rightarrow iterate_{B a_g}(a; x = A | P \ a x)) \tau \]

(\langle proof \rangle)

lemma cp-OclSelect: simp, intro!
\[ (X -\Rightarrow select_{B a_g}(a | P \ a)) \tau = \]
\[ ((\lambda -. X \tau) -\Rightarrow select_{B a_g}(a | P \ a)) \tau \]

(\langle proof \rangle)

lemma cp-OclReject: simp, intro!
\[ (X -\Rightarrow reject_{B a_g}(a | P \ a)) \tau = \]
\[ ((\lambda -. X \tau) -\Rightarrow reject_{B a_g}(a | P \ a)) \tau \]

(\langle proof \rangle)

lemmas cp-intro'_Bag = simp, intro!, simp, code-unfold
\[ cp-OclSize = \Rightarrow allI [\Rightarrow allI [\Rightarrow allI [\Rightarrow \Rightarrow cpI1, of OclSize]]] \]
\[ cp-OclIsEmpty = \Rightarrow allI [\Rightarrow allI [\Rightarrow allI [\Rightarrow \Rightarrow cpI1, of OclIsEmpty]]] \]
\[ cp-OclNotEmpty = \Rightarrow allI [\Rightarrow allI [\Rightarrow allI [\Rightarrow \Rightarrow cpI1, of OclNotEmpty]]] \]
\[ cp-OclANY = \Rightarrow allI [\Rightarrow allI [\Rightarrow allI [\Rightarrow \Rightarrow cpI1, of OclANY]]] \]

Const

lemma const-OclIncluding: simp, code-unfold
\[ \text{assumes const-x : const } x \quad \text{and } const-S : const S \]
\[ \text{shows } const (S -\Rightarrow including_{B a_g}(x)) \]

(\langle proof \rangle)

\section*{2.8.26. Test Statements}

instantiation Bag_base :: (equal)equal
begin
\[ \text{definition } \text{HOL.equal k l } \leftarrow (k:(a::equal)Bag_base) = l \]
\[ \text{instance } (\langle proof \rangle) \]
end

lemma equal-Bag_base-code [code]:
\[ \text{HOL.equal k (l:(a::{equal,null})Bag_base) } \leftarrow \text{Rep-Bag_base k = Rep-Bag_base l } \]

(\langle proof \rangle)

Assert \[ \tau \models (Bag\{\} \Rightarrow Bag\{\}) \]

end

theory UML-Set
imports ../basic-types/UML-Void
../basic-types/UML-Boolean
../basic-types/UML-Integer
../basic-types/UML-String
../basic-types/UML-Real
2.9. Collection Type Set: Operations

2.9.1. As a Motivation for the (infinite) Type Construction: Type-Extensions as Sets

Our notion of typed set goes beyond the usual notion of a finite executable set and is powerful enough to capture the extension of a type in UML and OCL. This means we can have in Featherweight OCL Sets containing all possible elements of a type, not only those (finite) ones representable in a state. This holds for base types as well as class types, although the notion for class-types — involving object id’s not occurring in a state — requires some care.

In a world with `invalid` and `null`, there are two notions extensions possible:

1. the set of all defined values of a type \( T \) (for which we will introduce the constant \( T \))
2. the set of all valid values of a type \( T \), so including `null` (for which we will introduce the constant \( T_{null} \)).

We define the set extensions for the base type `Integer` as follows:

**Definition** `Integer` :

\[
\text{Integer} :: (\lambda \tau. (\text{Abs-Set}_{base} \circ \text{Some} \circ \text{Some}) \ (\text{Some} \circ \text{Some} \ ' (\text{UNIV}::\text{int set})))
\]

**Definition** `Integer_{null}` :

\[
\text{Integer}_{null} :: (\lambda \tau. (\text{Abs-Set}_{base} \circ \text{Some} \circ \text{Some}) \ (\text{Some} \ ' (\text{UNIV}::\text{int option set})))
\]

**Lemma** `Integer-defined` :

\[\delta \text{Integer} = \text{true}\]

**Lemma** `Integer_{null}-defined` :

\[\delta \text{Integer}_{null} = \text{true}\]

This allows the theorems:

\[\tau \models \delta x \implies \tau \models (\text{Integer} \rightarrow \text{includes}_{\text{Set}}(x)) \quad \tau \models \delta \quad \tau \models (\text{Integer} \triangleq (\text{Integer} \rightarrow \text{includes}_{\text{Set}}(x)))
\]

which characterize the infiniteness of these sets by a recursive property on these sets.

In the same spirit, we proceed similarly for the remaining base types:

**Definition** `Void_{null}` :

\[
\text{Void}_{null} :: (\lambda \tau. (\text{Abs-Set}_{base} \circ \text{Some} \circ \text{Some}) \ (\text{Abs-Set}_{\text{base}} (\text{Some None}))
\]

**Definition** `Void_{empty}` :

\[
\text{Void}_{empty} :: (\lambda \tau. (\text{Abs-Set}_{base} \circ \text{Some} \circ \text{Some}) \ (\text{Abs-Set}_{\text{base}} (\text{Some None}))})
\]

**Lemma** `Void_{null}-defined` :

\[\delta \text{Void}_{null} = \text{true}\]

**Lemma** `Void_{empty}-defined` :

\[\delta \text{Void}_{empty} = \text{true}\]

**Lemma** assumes \( \tau \models \delta (V :: (\lambda \tau. \text{Void}_{base}) \text{Set}) \)
\[ \tau \models V \triangleq \text{Void} \lor \tau \models V \triangleq \text{Void}_\emptyset \]

**Definition**

**Boolean** :: (\'A, Boolean_base) Set

where

\[ \text{Boolean} \equiv (\lambda \tau. (\text{Abs-Set}_{\text{base}} \circ \text{Some} \circ \text{Some}) ((\text{Some} \circ \text{Some}) \cdot (\text{UNIV}::\text{bool set}))) \]

**Boolean_null** :: (\'A, Boolean_base) Set

where

\[ \text{Boolean_null} \equiv (\lambda \tau. (\text{Abs-Set}_{\text{base}} \circ \text{Some} \circ \text{Some}) ((\text{Some} \circ \text{Some}) \cdot (\text{UNIV}::\text{bool option set}))) \]

**Lemma**

**Boolean-defined** : \( \delta \text{Boolean} = \text{true} \)

(Proof)

**Lemma**

**Boolean_null-defined** : \( \delta \text{Boolean_null} = \text{true} \)

(Proof)

**Definition**

**String** :: (\'A, String_base) Set

where

\[ \text{String} \equiv (\lambda \tau. (\text{Abs-Set}_{\text{base}} \circ \text{Some} \circ \text{Some}) ((\text{Some} \circ \text{Some}) \cdot (\text{UNIV}::\text{string set}))) \]

**String_null** :: (\'A, String_base) Set

where

\[ \text{String_null} \equiv (\lambda \tau. (\text{Abs-Set}_{\text{base}} \circ \text{Some} \circ \text{Some}) ((\text{Some} \circ \text{Some}) \cdot (\text{UNIV}::\text{string option set}))) \]

**Lemma**

**String-defined** : \( \delta \text{String} = \text{true} \)

(Proof)

**Lemma**

**String_null-defined** : \( \delta \text{String_null} = \text{true} \)

(Proof)

**Definition**

**Real** :: (\'A, Real_base) Set

where

\[ \text{Real} \equiv (\lambda \tau. (\text{Abs-Set}_{\text{base}} \circ \text{Some} \circ \text{Some}) ((\text{Some} \circ \text{Some}) \cdot (\text{UNIV}::\text{real set}))) \]

**Real_null** :: (\'A, Real_base) Set

where

\[ \text{Real_null} \equiv (\lambda \tau. (\text{Abs-Set}_{\text{base}} \circ \text{Some} \circ \text{Some}) ((\text{Some} \circ \text{Some}) \cdot (\text{UNIV}::\text{real option set}))) \]

**Lemma**

**Real-defined** : \( \delta \text{Real} = \text{true} \)

(Proof)

**Lemma**

**Real_null-defined** : \( \delta \text{Real_null} = \text{true} \)

(Proof)

### 2.9.2. Basic Properties of the Set Type

Every element in a defined set is valid.

**Lemma**

**Set-inv-lemma** : \( \tau \models (\delta X) \implies \forall x \in (\text{Rep-Set}_{\text{base}} (X \tau))^\uparrow. x \neq \text{bot} \)

(Proof)

**Lemma**

\[ \text{Set-inv-lemma}' : \]

**Assume**

\[ x \cdot \text{def} : \tau \models \delta X \]

and

\[ e \cdot \text{mem} : e \in (\text{Rep-Set}_{\text{base}} (X \tau))^\uparrow \]

**Shows**

\[ \tau \models v (\lambda e. e) \]

(Proof)

**Lemma**

**abs-rep-simp’** :

**Assume**

\[ S \cdot \text{all-def} : \tau \models \delta S \]

**Shows**

\[ (\text{Abs-Set}_{\text{base}} (S \tau))_{\downarrow} = S \tau \]

(Proof)

**Lemma**

**S-lift’**:
assumes $S$-all-def : $\langle \tau :: \alpha \ a \rangle \models \delta S$

shows $\exists S'. \ (\lambda a :: \alpha \ a \rangle :: \tau) ^{\top} \text{Rep}_{base} \ (S \ \tau) = (\lambda a :: \alpha \ a \rangle :: \tau) ^{\top} \ ' S'$

\{proof\}

lemma invalid-set-OclNot-defined [simp,code-unfold];$\delta$(invalid::($\mathfrak{A}, \alpha :: \text{null}$) Set) = false \{proof\}

lemma null-set-OclNot-defined [simp,code-unfold];$\delta$(null::($\mathfrak{A}, \alpha :: \text{null}$) Set) = false \{proof\}

lemma invalid-set-valid [simp,code-unfold];$\nu$(invalid::($\mathfrak{A}, \alpha :: \text{null}$) Set) = false \{proof\}

lemma null-set-valid [simp,code-unfold];$\nu$(null::($\mathfrak{A}, \alpha :: \text{null}$) Set) = true \{proof\}

... which means that we can have a type ($\mathfrak{A}, ($\mathfrak{A}$), \alpha :: \text{Integer}) Set corresponding exactly to Set(Set(Integer)) in OCL notation. Note that the parameter $\mathfrak{A}$ still refers to the object universe; making the OCL semantics entirely parametric in the object universe makes it possible to study (and prove) its properties independently from a concrete class diagram.

2.9.3. Definition: Strict Equality

After the part of foundational operations on sets, we detail here equality on sets. Strong equality is inherited from the OCL core, but we have to consider the case of the strict equality. We decide to overload strict equality in the same way we do for other value’s in OCL:

overloading
StrictRefEq $\equiv$ StrictRefEq :: $\langle (\mathfrak{A}, \alpha :: \text{null})\text{Set}, (\mathfrak{A}, \alpha :: \text{null})\text{Set} \rangle \Rightarrow (\mathfrak{A})\text{Boolean}$

begin

definition StrictRefEq$_{set}$ :
(x::($\mathfrak{A}, \alpha :: \text{null})\text{Set}) \equiv \lambda \tau. \ if \ (v \ x) \ \tau = \text{true} \ \tau \land (v \ y) \ \tau = \text{true} \ \tau
then \ (x \ \delta = y) \ \tau
else invalid \ \tau
end

One might object here that for the case of objects, this is an empty definition. The answer is no, we will restrain later on states and objects such that any object has its oid stored inside the object (so the ref, under which an object can be referenced in the store will represented in the object itself). For such well-formed stores that satisfy this invariant (the WFF-invariant), the referential equality and the strong equality—and therefore the strict equality on sets in the sense above—coincides.

Property proof in terms of profile-bin\textit{StrongEq}_{\textit{v}=_{\nu=}}$

interpretation StrictRefEq$_{set}$ : profile-bin\textit{StrongEq}_{\textit{v}=_{\nu=}} \lambda \ x \ y. \ (x::($\mathfrak{A}, \alpha :: \text{null})\text{Set}) \ \delta = y$

\{proof\}

2.9.4. Constants: mtSet

definition mtSet::($\mathfrak{A}, \alpha :: \text{null})\text{Set} \ (\text{Set}\{\})$
where $\text{Set}\{\} \equiv (\lambda \ r. \ \text{Abs}_{base} \ r\{\}: \alpha \text{ set}_y )$

lemma mtSet-defined[simp,code-unfold];$\delta$(Set\{\}) = true \{proof\}

lemma mtSet-valid[simp,code-unfold];$\nu$(Set\{\}) = true \{proof\}

lemma mtSet-rep-set: ^{\top}\text{Rep}_{base} (Set\{\} \ \tau) = \{\}$ \{proof\}

97
lemma [simp,code-unfold]: const Set()
(proof)

Note that the collection types in OCL allow for null to be included; however, there is the null-collection into which inclusion yields invalid.

2.9.5. Definition: Including

definition OclIncluding :: [\(\mathfrak{A},'\alpha::null\)] Set,(\mathfrak{A},'\alpha) val \Rightarrow (\mathfrak{A},'\alpha) Set
where OclIncluding x y = (\lambda \tau. if (\delta x) \tau = true \tau \land (\nu y) \tau = true \tau
then Abs-Set_base \cup Rep-Set_base (x \tau) \cup \{ y \tau \} \cup\)
else invalid \tau )
notation OclIncluding (\dashrightarrow \text{including}_{\mathfrak{A}}\cdot('\cdot'))

interpretation OclIncluding : profile-bin_{\mathfrak{A}} OclIncluding \lambda x y. Abs-Set_base |\cup Rep-Set_base x \tau \cup \{ y \tau \}
(proof)

syntax
-OclFinset :: args => (\mathfrak{A},'a::null) Set (\{}\{\})
translations
Set\{ x, xs \} == const OclIncluding (Set\{ xs \}) x
Set\{ x \} == const OclIncluding (Set\{ \}) x

2.9.6. Definition: Excluding

definition OclExcluding :: [\(\mathfrak{A},'\alpha::null\)] Set,(\mathfrak{A},'\alpha) val \Rightarrow (\mathfrak{A},'\alpha) Set
where OclExcluding x y = (\lambda \tau. if (\delta x) \tau = true \tau \land (\nu y) \tau = true \tau
then Abs-Set_base \cup Rep-Set_base (x \tau) \cup \{ y \tau \} \cup\)
else invalid \tau )
notation OclExcluding (\dashrightarrow \text{excluding}_{\mathfrak{A}}\cdot('\cdot'))

lemma OclExcluding-inv: (x:: Set\{k::\{null\}\}) \neq \bot \Rightarrow x \neq null \Rightarrow y \neq \bot \Rightarrow
\cup Rep-Set_base x \tau \cup \{ y \tau \} \cup\{ X. X = bot \lor X = null \lor (\forall x\in|^\tau X^\tau. x \neq bot)\}
(proof)

interpretation OclExcluding : profile-bin_{\mathfrak{A}} OclExcluding \lambda x y. Abs-Set_base |\cup Rep-Set_base x \tau \cup \{ y \tau \}
(proof)

2.9.7. Definition: Includes

definition OclIncludes :: [\(\mathfrak{A},'\alpha::null\)] Set,(\mathfrak{A},'\alpha) val \Rightarrow \mathfrak{A} Boolean
where OclIncludes x y = (\lambda \tau. if (\delta x) \tau = true \tau \land (\nu y) \tau = true \tau
then Abs-Set_base \cup Rep-Set_base (x \tau) \cup \{ y \tau \} \cup\)
else invalid \tau )
notation OclIncludes (\dashrightarrow \text{includes}_{\mathfrak{A}}\cdot('\cdot'))

interpretation OclIncludes : profile-bin_{\mathfrak{A}} OclIncludes \lambda x y. \cup Rep-Set_base x \tau \cup \{ y \tau \}
(proof)

2.9.8. Definition: Excludes

definition OclExcludes :: [\(\mathfrak{A},'\alpha::null\)] Set,(\mathfrak{A},'\alpha) val \Rightarrow \mathfrak{A} Boolean
where OclExcludes x y = (not(OclIncludes x y))
notation OclExcludes (\dashrightarrow \text{excludes}_{\mathfrak{A}}\cdot('\cdot'))

The case of the size definition is somewhat special, we admit explicitly in Featherweight OCL the possibility of infinite sets. For the size definition, this requires an extra condition that assures that the
cardinality of the set is actually a defined integer.

interpretation \( \text{OclExcludes : profile-bin}_x \text{ OclExcludes } \lambda x. y. \_ y \notin \text{Rep-Set}_{base} x_\text{\{\}} \)

(proof)

2.9.9. Definition: Size

definition OclSize :: (\text{\{\} a::null})Set \Rightarrow \text{\{\} Integer}
where 
\( \text{OclSize } x = (\lambda \tau. \text{ if } (\delta x) \tau = \text{true } \tau \land \text{finite} (\text{\text{Rep-Set}}_{base} (x \tau)^\text{\{\}})) \text{ then int} (\text{card} (\text{\text{Rep-Set}}_{base} (x \tau)^\text{\{\}})). \)

notation 
\( \text{OclSize } (-\rightarrow \text{size}\_set (\{} ) \)

The following definition follows the requirement of the standard to treat null as neutral element of sets. It is a well-documented exception from the general strictness rule and the rule that the distinguished argument self should be non-null.

2.9.10. Definition: IsEmpty

definition OclIsEmpty :: (\text{\{\} a::null}) Set \Rightarrow \text{\{\} Boolean}
where 
\( \text{OclIsEmpty } x = ((v x \text{ and not } (\delta x)) \text{ or } ((\text{OclSize } x \equiv 0))) \)

notation \( \text{OclIsEmpty } (-\rightarrow \text{isEmpty}_{\text{set} (\{} ) \)

2.9.11. Definition: NotEmpty

definition OclNotEmpty :: (\text{\{\} a::null}) Set \Rightarrow \text{\{\} Boolean}
where 
\( \text{OclNotEmpty } x = \text{not} (\text{OclIsEmpty } x) \)

notation \( \text{OclNotEmpty } (-\rightarrow \text{notisEmpty}_{\text{set} (\{} ) \)

2.9.12. Definition: Any

definition OclANY :: [(\text{\{\} a::null}) Set] \Rightarrow (\text{\{} a \} val
where 
\( \text{OclANY } x = (\lambda \tau. \text{ if } (\upsilon x) \tau = \text{true } \tau \text{ then SOME } y. y \in \text{\text{Rep-Set}}_{base} (x \tau)^\text{\{\}} \text{ else null } \tau \)

notation \( \text{OclANY } (-\rightarrow \text{any}_{\text{set} (\{} ) \)

2.9.13. Definition: Forall

The definition of OclForall mimics the one of (and): OclForall is not a strict operation.

definition OclForall :: [(\text{\{\} a::null}) Set,(\text{\{} a \} val\Rightarrow (\text{\{} a \} Boolean)] \Rightarrow \text{\{\} Boolean}
where 
\( \text{OclForall } S P = (\lambda \tau. \text{ if } (\delta S) \tau = \text{true } \tau \text{ then false } \tau \text{ else if } (\exists x \in \text{\text{Rep-Set}}_{base} (S \tau)^\text{\{\}}. P(\lambda \_ . x) \tau = \text{false } \tau) \text{ then false } \tau \text{ else if } (\exists x \in \text{\text{Rep-Set}}_{base} (S \tau)^\text{\{\}}. P(\lambda \_ . x) \tau = \text{invalid } \tau) \text{ then invalid } \tau \text{ else if } (\exists x \in \text{\text{Rep-Set}}_{base} (S \tau)^\text{\{\}}. P(\lambda \_ . x) \tau = \text{null } \tau) \text{ then null } \tau \text{ else true } \tau \)

syntaxis

-OclForallSet :: [(\text{\{} a::null\} Set.id,(\text{\{} a\} Boolean)] \Rightarrow \text{\{} a\} Boolean \ ((\{}\rightarrow \text{forAll}_{\text{set} (\{} )\))

translations

\( \text{\{} \rightarrow \text{forall}_{\text{set} (\{} | P) \Rightarrow \text{CONST UML-Set} OclForall \text{ \{\}x. P) \}

99
2.9.14. Definition: Exists

Like OclForall, OclExists is also not strict.

**Definition** OclExists :: [\(A::\alpha::null\) Set,\(\alpha::\alpha\)val\(\Rightarrow\)\(\alpha\)Boolean] \(\Rightarrow\) \(\alpha\) Boolean

**where** OclExists S P = not(\(\alpha\)Set.OclForall S (\(\lambda\) X. not (P X)))

**Syntax**

- OclExistSet :: [\(\alpha::null\) Set,id,\(\alpha\)Boolean] \(\Rightarrow\) \(\alpha\) Boolean ((\(-\)\(\Rightarrow\)exists\(\alpha\)Set,\(\cdot\))

**Translations**

\(X\Rightarrow\)exists\(\alpha\)Set(x | P) == CONST UML-Set.OclExists X (%x. P)

2.9.15. Definition: Iterate

**Definition** OclIterate :: [\(\alpha::null\) Set,\(\beta::null\)val,\(\alpha::\alpha\)val\(\Rightarrow\)\(\alpha::\beta\)val] \(\Rightarrow\) \(\alpha::\beta\)val

**where** OclIterate S A F = (\(\lambda\) \(\tau\). if (\(\delta\) S) \(\tau\) = true \(\tau\) \& (\(\nu\) A) \(\tau\) = true \(\tau\) \& finite\(\Rightarrow\)Rep-Set\(\alpha\)base (S \(\tau\))^\(\tau\) then (Finite-Set.fold (F) (\(\lambda\)a. \(\alpha\) \(\tau\)) \(\Rightarrow\)Rep-Set\(\alpha\)base (S \(\tau\))^\(\tau\))\(\tau\)
else \(\perp\))

**Syntax**

- OclIterateSet :: [\(\alpha::null\) Set, idt, idt, \(\alpha::\beta\)] \(\Rightarrow\) \(\alpha::\gamma\)val

(-\(\Rightarrow\)iterate\(\alpha\)Set,\(\cdot::\cdot\)\(\Rightarrow\)\(\cdot::\cdot\))

**Translations**

\(X\Rightarrow\)iterate\(\alpha\)Set(a; x = A | P) == CONST OclIterate X A (%a. (% x. P))

2.9.16. Definition: Select

**Definition** OclSelect :: [\(\alpha::null\)Set,\(\alpha::\alpha\)val\(\Rightarrow\)\(\alpha\)Boolean] \(\Rightarrow\) \(\alpha::\alpha\)Set

**where** OclSelect S P = (\(\lambda\) \(\tau\). if (\(\delta\) S) \(\tau\) = true \(\tau\)
then if (\(\exists\alpha::\gamma::null\)Rep-Set\(\alpha\)base (S \(\tau\))^\(\tau\). P(\(\lambda\)\(\cdot\). \(\alpha\) \(\tau\)) \(\Rightarrow\) invalid \(\tau\))
else invalid \(\tau\)
else \(\Rightarrow\)Abs-Set\(\alpha\)base \(\Rightarrow\)Rep-Set\(\alpha\)base (S \(\tau\))^\(\tau\). P(\(\lambda\). \(\cdot\)) \(\tau\) \(\neq\) false \(\tau\))\(\tau\)
else invalid \(\tau\))

**Syntax**

- OclSelectSet :: [\(\alpha::null\) Set,idt,\(\alpha::\alpha\)Boolean] \(\Rightarrow\) \(\alpha::\alpha\)Set ((\(-\)\(\Rightarrow\)select\(\alpha\)Set,\(\cdot::\cdot\))

**Translations**

\(X\Rightarrow\)select\(\alpha\)Set(x | P) == CONST OclSelect X (% x. P)

2.9.17. Definition: Reject

**Definition** OclReject :: [\(\alpha::null\)Set,\(\alpha::\alpha\)val\(\Rightarrow\)\(\alpha\)Boolean] \(\Rightarrow\) \(\alpha::null\)Set

**where** OclReject S P = OclSelect S (not o P)

**Syntax**

- OclRejectSet :: [\(\alpha::null\) Set,idt,\(\alpha::\alpha\)Boolean] \(\Rightarrow\) \(\alpha::\alpha\)Set ((\(-\)\(\Rightarrow\)reject\(\alpha\)Set,\(\cdot::\cdot\))

**Translations**

\(X\Rightarrow\)reject\(\alpha\)Set(x | P) == CONST OclReject X (% x. P)

2.9.18. Definition: IncludesAll

**Definition** OclIncludesAll :: [\(\alpha::null\) Set,\(\alpha::\alpha\) Set] \(\Rightarrow\) \(\alpha::\alpha\) Boolean

**where** OclIncludesAll x y = (\(\lambda\) \(\tau\). if (\(\delta\) x) \(\tau\) = true \(\tau\) \& (\(\delta\) y) \(\tau\) = true \(\tau\)
then \(\Rightarrow\)Rep-Set\(\alpha\)base (y \(\tau\))^\(\tau\) \(\subseteq\) \(\Rightarrow\)Rep-Set\(\alpha\)base (x \(\tau\))^\(\tau\)
else \(\perp\))

**Notation** OclIncludesAll ((\-)\(\Rightarrow\)includes\(\alpha\)Set,\(\cdot::\cdot\))

**Interpretation** OclIncludesAll : profile-bind-a OclIncludesAll \(\lambda\) x y. \(\Rightarrow\)Rep-Set\(\alpha\)base y^\(\tau\) \(\subseteq\) \(\Rightarrow\)Rep-Set\(\alpha\)base x^\(\tau\)
(proof)
2.9.19. Definition: ExcludesAll

**definition** OclExcludesAll :: [(\x,\cdot::null) Set,(\x,\cdot) Set] \Rightarrow \forall Boolean

where
OclExcludesAll x y = (\lambda \tau. if (\delta x) \tau = true \tau \land (\delta y) \tau = true \tau then \margin{\text{\scriptsize Rep-Set}_{base} (y \tau)} \cap \margin{\text{\scriptsize Rep-Set}_{base} (x \tau)} = \{\lift \down\} else \bot)\margin{\scriptsize \textbf{(proof)}}

**notation** OclExcludesAll (\text{\ae\textnormal{-}excludesAll}_{\text{\scriptsize Set}}(\cdot \cdot))

**interpretation** OclExcludesAll : profile-bin_{\text{\scriptsize Set}} OclExcludesAll \lambda x y. \margin{\text{\scriptsize Rep-Set}_{base} y \tau} \cap \margin{\text{\scriptsize Rep-Set}_{base} x \tau} = \{\lift \down\}

2.9.20. Definition: Union

**definition** OclUnion :: [(\x,\cdot::null) Set,(\x,\cdot) Set] \Rightarrow (\x,\cdot) Set

where
OclUnion x y = (\lambda \tau. if (\delta x) \tau = true \tau \land (\delta y) \tau = true \tau then Abs-{\text{\scriptsize Set}_{base}}{(\margin{\text{\scriptsize Rep-Set}_{base} (y \tau)} \cup \margin{\text{\scriptsize Rep-Set}_{base} (x \tau)})} \margin{\scriptsize \textbf{(proof)}} else \bot)\margin{\scriptsize \textbf{(proof)}}

OclUnion-inv : x::Set((b::null)) \margin{\scriptsize \textbf{(proof)}}

**notation** OclUnion (\text{\ae\textnormal{-}union}_{\text{\scriptsize Set}}(\cdot \cdot))

**interpretation** OclUnion : profile-bin_{\text{\scriptsize Set}} OclUnion \lambda x y. Abs-{\text{\scriptsize Set}_{base}}{(\margin{\text{\scriptsize Rep-Set}_{base} y \tau} \cup \margin{\text{\scriptsize Rep-Set}_{base} x \tau})} \margin{\scriptsize \textbf{(proof)}}

2.9.21. Definition: Intersection

**definition** OclIntersection :: [(\x,\cdot::null) Set,(\x,\cdot) Set] \Rightarrow (\x,\cdot) Set

where
OclIntersection x y = (\lambda \tau. if (\delta x) \tau = true \tau \land (\delta y) \tau = true \tau then \margin{\text{\scriptsize Rep-Set}_{base} (y \tau)} \cap \margin{\text{\scriptsize Rep-Set}_{base} (x \tau)} \margin{\scriptsize \textbf{(proof)}} else \bot)\margin{\scriptsize \textbf{(proof)}}

OclIntersection-inv : x::Set((b::null)) \margin{\scriptsize \textbf{(proof)}}

**notation** OclIntersection (\text{\ae\textnormal{-}intersection}_{\text{\scriptsize Set}}(\cdot \cdot))

**interpretation** OclIntersection : profile-bin_{\text{\scriptsize Set}} OclIntersection \lambda x y. Abs-{\text{\scriptsize Set}_{base}}{(\margin{\text{\scriptsize Rep-Set}_{base} y \tau} \cap \margin{\text{\scriptsize Rep-Set}_{base} x \tau})} \margin{\scriptsize \textbf{(proof)}}

2.9.22. Definition (future operators)

**consts**

OclCount :: [(\x,\cdot::null) Set,(\x,\cdot) Set] \Rightarrow \forall Integer

OclSum :: (\x,\cdot::null) Set \Rightarrow \forall Integer

**notation** OclCount (\text{\ae\textnormal{-}count}_{\text{\scriptsize Set}}(\cdot \cdot))

OclSum (\text{\ae\textnormal{-}sum}_{\text{\scriptsize Set}}(\cdot \cdot))

2.9.23. Logical Properties

OclIncluding

**lemma** OclIncluding-valid-args-valid:
\[(\tau \models v(X \rightarrow including_{Set}(x))) = ((\tau \models (\delta X)) \land (\tau \models (\nu x)))\]

(proof)

**lemma OclIncluding-valid-args-valid'' [simp, code-unfold]:**
\[v(X \rightarrow including_{Set}(x)) = ((\delta X) \land (\nu x))\]
(proof)

etc. etc.

**OclExcluding**

**lemma OclExcluding-valid-args-valid:**
\[(\tau \models v(X \rightarrow excluding_{Set}(x))) = ((\tau \models (\delta X)) \land (\tau \models (\nu x)))\]
(proof)

**lemma OclExcludes-valid-args-valid'' [simp, code-unfold]:**
\[v(X \rightarrow excluding_{Set}(x)) = ((\delta X) \land (\nu x))\]
(proof)

**OclIncludes**

**lemma OclIncludes-valid-args-valid:**
\[(\tau \models v(X \rightarrow includes_{Set}(x))) = ((\tau \models (\delta X)) \land (\tau \models (\nu x)))\]
(proof)

**lemma OclExcludes-valid-args-valid':**
\[v(X \rightarrow excluding_{Set}(x)) = ((\delta X) \land (\nu x))\]
(proof)

**OclSize**

**lemma OclSize-defined-args-valid:**
\[\tau \models (\delta (X \rightarrow size_{Set}())) \implies \tau \models (\delta X)\]
(proof)

**lemma OclSize-infinite:**
\[\text{assumes } \text{non-finite: } \tau \models \neg (\delta (S \rightarrow size_{Set}()))\]
\[\text{shows } (\tau \models \neg (\delta(S))) \lor \text{ finite } [Rep-Set_{base}(S \tau)]\]
(proof)

**lemma \tau \models \delta X \implies \neg \text{ finite } [Rep-Set_{base}(X \tau)] \implies \neg \tau \models (\delta (X \rightarrow size_{Set}()))\]
(proof)

**lemma size-defined:**
\[\text{assumes } X\text{-finite: } \forall \tau. \text{ finite } [Rep-Set_{base}(X \tau)]\]
\[\text{shows } \delta (X \rightarrow size_{Set}()) = \delta X\]
(proof)

**lemma size-defined':**
\[\text{assumes } X\text{-finite: } \exists \tau. \text{ finite } [Rep-Set_{base}(X \tau)]\]
\[\text{shows } (\tau \models \delta (X \rightarrow size_{Set}()) = (\tau \models \delta X)\]
(proof)
OclIsEmpty

**Lemma OclIsEmpty-defined-args-valid:** \( \tau \models \delta (X \rightarrow \text{isEmptys}(\tau)) \Rightarrow \tau \models v X \)

**Proof**

\[ \text{proof} \]

**Lemma** \( \tau \models \delta (null \rightarrow \text{isEmptys}(\tau)) \)

**Proof**

\[ \text{proof} \]

**Lemma OclIsEmpty-infinite:** \( \tau \models \delta X \Rightarrow \neg \text{finite} \left( \text{Rep-Set}_{\text{base}} (X \tau) \right) \Rightarrow \neg \tau \models \delta (X \rightarrow \text{isEmptys}(\tau)) \)

**Proof**

OclNotEmpty

**Lemma OclNotEmpty-defined-args-valid:** \( \tau \models \delta (X \rightarrow \text{notEmptys}(\tau)) \Rightarrow \tau \models v X \)

**Proof**

\[ \text{proof} \]

**Lemma** \( \tau \models \delta (null \rightarrow \text{notEmptys}(\tau)) \)

**Proof**

\[ \text{proof} \]

**Lemma OclNotEmpty-infinite:** \( \tau \models \delta X \Rightarrow \neg \text{finite} \left( \text{Rep-Set}_{\text{base}} (X \tau) \right) \Rightarrow \neg \tau \models \delta (X \rightarrow \text{notEmptys}(\tau)) \)

**Proof**

**Lemma OclNotEmpty-has-elt:** \( \tau \models \delta X \Rightarrow \tau \models X \rightarrow \text{notEmpty}(\tau) \)

**Proof**

\[ \text{proof} \]

\[ \text{proof} \]

**Lemma OclANY-defined-args-valid:** \( \tau \models \delta (X \rightarrow \text{any}(\tau)) \Rightarrow \tau \models v X \)

**Proof**

\[ \text{proof} \]

**Lemma OclANY-valid-args-valid:**

\( (\tau \models v(X \rightarrow \text{any}(\tau))) \Rightarrow (\tau \models v X) \)

**Proof**

\[ \text{proof} \]

**Lemma OclANY-valid-args-valid′′:** \( (\tau \models v(X \rightarrow \text{any}(\tau))) = (\tau \models v X) \)

**Proof**

\[ \text{proof} \]

2.9.24. Execution Laws with Invalid or Null or Infinite Set as Argument

OclIncluding

OclExcluding

OclIncludes

OclExcludes

OclSize

**Lemma OclSize-invalid:** \( \text{invalid} \rightarrow \text{size}(\tau) \)

**Proof**

\[ \text{proof} \]

**Lemma OclSize-null:** \( \text{null} \rightarrow \text{size}(\tau) \)

**Proof**

\[ \text{proof} \]

OclIsEmpty
lemma OclIsEmpty-invalid[simp,code-unfold]:\(\text{invalid} \rightarrow \text{isEmpty}_{\text{Set}}()\) = invalid 
(proof)

lemma OclIsEmpty-null[simp,code-unfold]:\(\text{null} \rightarrow \text{isEmpty}_{\text{Set}}()\) = true 
(proof)

lemma OclNotEmpty-invalid[simp,code-unfold]:\(\text{invalid} \rightarrow \text{notEmpty}_{\text{Set}}()\) = invalid 
(proof)

lemma OclNotEmpty-null[simp,code-unfold]:\(\text{null} \rightarrow \text{notEmpty}_{\text{Set}}()\) = true 
(proof)

OclANY

lemma OclANY-invalid[simp,code-unfold]:\(\text{invalid} \rightarrow \text{any}_{\text{Set}}()\) = invalid 
(proof)

lemma OclANY-null[simp,code-unfold]:\(\text{null} \rightarrow \text{any}_{\text{Set}}()\) = null 
(proof)

OclForall

lemma OclForall-invalid[simp,code-unfold]:\(\text{invalid} \rightarrow \forall a \mid P a\) = invalid 
(proof)

lemma OclForall-null[simp,code-unfold]:\(\text{null} \rightarrow \forall a \mid P a\) = invalid 
(proof)

OclExists

lemma OclExists-invalid[simp,code-unfold]:\(\text{invalid} \rightarrow \exists a \mid P a\) = invalid 
(proof)

lemma OclExists-null[simp,code-unfold]:\(\text{null} \rightarrow \exists a \mid P a\) = invalid 
(proof)

OclIterate

lemma OclIterate-invalid[simp,code-unfold]:\(\text{invalid} \rightarrow \text{iterate}_{\text{Set}}(a; x = A \mid P a x)\) = invalid 
(proof)

lemma OclIterate-null[simp,code-unfold]:\(\text{null} \rightarrow \text{iterate}_{\text{Set}}(a; x = A \mid P a x)\) = invalid 
(proof)

lemma OclIterate-invalid-args[simp,code-unfold]:\(S \rightarrow \text{iterate}_{\text{Set}}(a; x = \text{invalid} \mid P a x)\) = invalid 
(proof)

An open question is this ...

lemma S \rightarrow \text{iterate}_{\text{Set}}(a; x = \text{null} \mid P a x) = \text{invalid} 
(proof)

lemma OclIterate-infinite:
assumes non-finite: \(\tau \models \text{not}(\delta(S \rightarrow \text{size}_{\text{Set}}()))\)
shows (OclIterate S A F) \(\tau = \text{invalid} \tau\) 
(proof)

OclSelect

lemma OclSelect-invalid[simp,code-unfold]:\(\text{invalid} \rightarrow \text{select}_{\text{Set}}(a \mid P a)\) = invalid
lemma OclSelect-null [simp, code-unfold]: null ⊢ select_{S \setminus (a \mid P a)} = invalid

OclReject

lemma OclReject-invalid [simp, code-unfold]: invalid ⊢ reject_{S \setminus (a \mid P a)} = invalid

lemma OclReject-null [simp, code-unfold]: null ⊢ reject_{S \setminus (a \mid P a)} = invalid

Context Passing

lemma cp-OclIncludes1:
(X ⊢ includes_{S \setminus (x \mid P x)}(\lambda \cdot. x \tau)) \tau

lemma cp-OclSize: X ⊢ size_{S \setminus (x \mid P x)}(\lambda \cdot. X \tau) \tau

lemma cp-OclIsEmpty: X ⊢ isEmpty_{S \setminus (x \mid P x)}(\lambda \cdot. X \tau) \tau

lemma cp-OclNotEmpty: X ⊢ notEmpty_{S \setminus (x \mid P x)}(\lambda \cdot. X \tau) \tau

lemma cp-OclANY: X ⊢ any_{S \setminus (x \mid P x)}(\lambda \cdot. X \tau) \tau

lemma cp-OclForall:
(S ⊢ forAll_{S \setminus (x \mid P x)}(\lambda \cdot. S \tau)) \tau

lemma cp-OclForall1 [simp, intro!]:
X \equiv cp S \Rightarrow cp (\lambda X. (S \tau) \Rightarrow forAll_{S \setminus (x \mid P x)}(\lambda \cdot. X \tau)) \tau

lemma cp-OclExists:
(S ⊢ exists_{S \setminus (x \mid P x)}(\lambda \cdot. x \tau)) \tau

lemma cp-OclExists1 [simp, intro!]:
X \equiv cp S \Rightarrow cp (\lambda X. (S \tau) \Rightarrow exists_{S \setminus (x \mid P x)}(\lambda \cdot. X \tau)) \tau

105
lemma cp-OclIterate: 
\((X \rightarrow \text{iterate}_{Set}(a; x = A \mid P a x)) \tau = 
((\lambda \cdot X \tau) \rightarrow \text{iterate}_{Set}(a; x = A \mid P a x)) \tau\) 
(proof)

lemma cp-OclSelect: 
\((X \rightarrow \text{select}_{Set}(a \mid P a)) \tau = 
((\lambda \cdot X \tau) \rightarrow \text{select}_{Set}(a \mid P a)) \tau\) 
(proof)

lemma cp-OclReject: 
\((X \rightarrow \text{reject}_{Set}(a \mid P a)) \tau = 
((\lambda \cdot X \tau) \rightarrow \text{reject}_{Set}(a \mid P a)) \tau\) 
(proof)

lemmas cp-intro''_{Set}[intro!, simp, code-unfold] = 
cp-OclSize \THEN \allI[\THEN \allI[\THEN \cpI1], \of \OclSize]\] 
cp-OclIsEmpty \THEN \allI[\THEN \allI[\THEN \cpI1], \of \OclIsEmpty]\] 
cp-OclNotEmpty \THEN \allI[\THEN \allI[\THEN \cpI1], \of \OclNotEmpty]\] 
cp-OclANY \THEN \allI[\THEN \allI[\THEN \cpI1], \of \OclANY]\]

Const

lemma const-OclIncluding[simp, code-unfold]: 
assumes const-x : const x 
and const-S : const S 
shows const (S \rightarrow \text{including}_{Set}(x)) 
(proof)

2.9.25. General Algebraic Execution Rules

Execution Rules on Including

lemma OclIncluding-finite-rep-set: 
assumes X-def : \tau \models \delta X 
and x-val : \tau \models \upsilon x 
shows finite \text{Rep-Set} base (X \rightarrow \text{including}_{Set}(x) \tau) = \text{finite} \text{Rep-Set} base (X \tau) 
(proof)

lemma OclIncluding-rep-set: 
assumes S-def : \tau \models \delta S 
shows \text{Rep-Set} base (S \rightarrow \text{including}_{Set}(\lambda \cdot \lb x \rb) \tau) = \text{insert} \lb x \rb \text{Rep-Set} base (S \tau) 
(proof)

lemma OclIncluding-notempty-rep-set: 
assumes X-def : \tau \models \delta X 
and a-val : \tau \models \upsilon a 
shows \text{Rep-Set} base (X \rightarrow \text{including}_{Set}(a) \tau) \neq \{\} 
(proof)

lemma OclIncluding-includes0: 
assumes \tau \models X \rightarrow \text{includes}_{Set}(x) 
shows X \rightarrow \text{including}_{Set}(x) \tau = X \tau 
(proof)

lemma OclIncluding-includes: 
assumes \tau \models X \rightarrow \text{includes}_{Set}(x) 
shows \tau \models X \rightarrow \text{including}_{Set}(x) \equiv X 
(proof)

lemma OclIncluding-commute0: 

106
assumes S-def : τ ⊨ δ S
  and i-val : τ ⊨ v i
  and j-val : τ ⊨ v j
shows τ ⊨ ((S :: ('A, 'a::null) Set)→excluding·Set(i)→excluding·Set(j)) Δ
(S→excluding·Set(j)→excluding·Set(i))
<proof>

lemma OclIncluding-commute[simp, code-unfold]:
((S :: ('A, 'a::null) Set)→including·Set(i)→including·Set(j) = (S→including·Set(j)→including·Set(i)))
<proof>

Execution Rules on Excluding

lemma OclExcluding-finite-rep-set :
  assumes X-def : τ ⊨ δ X
  and x-val : τ ⊨ v x
shows finite τ·Rep·Set·base (X→excluding·Set(x) τ) = finite τ·Rep·Set·base (X τ)
<proof>

lemma OclExcluding-rep-set:
  assumes S-def : τ ⊨ δ S
shows τ·Rep·Set·base (S→excluding·Set(λ·ω·x.ω) τ) = τ·Rep·Set·base (S τ) \{ω·x.ω\}
<proof>

lemma OclExcluding-excludes0:
  assumes τ ⊨ X→excluding·Set(x)
shows X→excluding·Set(x) τ = X τ
<proof>

lemma OclExcluding-excludes:
  assumes τ ⊨ X→excluding·Set(x)
shows τ ⊨ X→excluding·Set(x) Δ X
<proof>

lemma OclExcluding-charn0[simp]:
  assumes val·x·τ : τ ⊨ (v x)
shows τ ⊨ ((Set{}→excluding·Set(x)) Δ Set{})
<proof>

lemma OclExcluding-commute0 :
  assumes S-def : τ ⊨ δ S
  and i-val : τ ⊨ v i
  and j-val : τ ⊨ v j
shows τ ⊨ ((S :: ('A, 'a::null) Set)→excluding·Set(i)→excluding·Set(j) Δ
(S→excluding·Set(j)→excluding·Set(i)))
<proof>

lemma OclExcluding-commute[simp, code-unfold]:
((S :: ('A, 'a::null) Set)→excluding·Set(i)→excluding·Set(j) = (S→excluding·Set(j)→excluding·Set(i)))
<proof>

lemma OclExcluding-charn0-exec[simp, code-unfold]:
(Set{}→excluding·Set(x)) = (if (v x) then Set{} else invalid endif)
<proof>
Boolean, Integer, and Sets thereof... to be defined for each type individually. Consequently, it is only valid for concrete type instances for

Unfortunately, this does not hold in general, since referential equality is an overloaded concept and has

lemma OclExcluding-charn1:
assumes def-X:τ |= (δ X)
and val-x:τ |= (v x)
and val-y:τ |= (v y)
and neq :τ |= not(x ≠ y)
shows τ |= (X→including_{set}(x))→excluding_{set}(y)) ≜ ((X→excluding_{set}(y))→including_{set}(x))
(proof)

lemma OclExcluding-charn2:
assumes def-X:τ |= (δ X)
and val-x:τ |= (v x)
shows τ |= ((X→including_{set}(x))→excluding_{set}(x)) ≜ (X→excluding_{set}(x))
(proof)

theorem OclExcluding-charn3: ((X→including_{set}(x))→excluding_{set}(x)) = (X→excluding_{set}(x))
(proof)

One would like a generic theorem of the form:

lemma OclExcluding_charn_exec:
(X→including_{set}(x::'(A,a::null)val)→excluding_{set}(y)) =
( if δ X then if x ≈ y
  then X→excluding_{set}(y)
  else X→excluding_{set}(y)→including_{set}(x)
  endif
  else invalid endif)*

Unfortunately, this does not hold in general, since referential equality is an overloaded concept and has
to be defined for each type individually. Consequently, it is only valid for concrete type instances for
Boolean, Integer, and Sets thereof...
The computational law OclExcluding-charn-exec becomes generic since it uses strict equality which
in itself is generic. It is possible to prove the following generic theorem and instantiate it later (using
properties that link the polymorphic logical strong equality with the concrete instance of strict quality).

lemma OclExcluding-charn-exec:
assumes strict1: (invalid ≝ y) = invalid
and strict2: (x ≈ invalid) = invalid
and StrictRefEq-valid-args-valid: \( \exists (x::'(A,a::null)val) y τ. (τ |= δ (x ≈ y)) = (((τ |= (v x)) ∧ (τ |= v y)) \and
(τ |= v x → τ |= v y → (τ |= ((x ≈ y) ≝ (x ≈ y)))
and cp-StrictRefEq: \( ∃ (x::'(A,a::null)val) y τ. (X ≈ Y) τ = ((λ· X τ) ≝ (λ· Y τ)) τ
and StrictRefEq-vs-StrongEq: \( ∃ (x::'(A,a::null)val) y τ. τ |= v x → τ |= v y → (τ |= ((x ≈ y) ≝ (x ≈ y)))

shows (X→including_{set}(x::'(A,a::null)val)→excluding_{set}(y)) =
( if δ X then if x ≈ y
  then X→excluding_{set}(y)
  else X→excluding_{set}(y)→including_{set}(x)
  endif
  else invalid endif)
(proof)

schematic-goal OclExcluding-charn-exec_{integer[simp, code-unfold]}: ?X

108
 Execution Rules on Includes

**Lemma** \(\text{OclIncludes-charn0}[\text{simp}]:\)

- **Assumes** \(\text{val-x} \vdash (\nu \ x)\)
- **Shows** \(\tau \vdash \text{not}(\text{Set}{}\rightarrow \text{includes}_{\text{Set}}(x))\)

**Lemma** \(\text{OclIncludes-charn0}[\text{simp}, \text{code-unfold}]:\)

- \(\text{Set}{}\rightarrow \text{includes}_{\text{Set}}(x) = (\text{if } \nu \ z \text{ then false else invalid endif})\)

**Lemma** \(\text{OclIncludes-charn1}::\)

- **Assumes** \(\text{def-X} \vdash (\delta \ X)\)
- **Assumes** \(\text{val-x} \vdash (\nu \ x)\)
- **Shows** \(\tau \vdash (X \rightarrow \text{including}_{\text{Set}}(x)) \rightarrow \text{includes}_{\text{Set}}(x))\)

**Lemma** \(\text{OclIncludes-charn2}::\)

- **Assumes** \(\text{def-X} \vdash (\delta \ X)\)
- **And** \(\text{val-x} \vdash (\nu \ x)\)
- **And** \(\text{val-y} \vdash (\nu \ y)\)
- **And** \(\text{neq} \vdash \tau \vdash \text{not}(x \triangleq y)\)
- **Shows** \(\tau \vdash (X \rightarrow \text{including}_{\text{Set}}(x)) \rightarrow \text{includes}_{\text{Set}}(y)) \triangleq (X \rightarrow \text{includes}_{\text{Set}}(y))\)

Here is again a generic theorem similar as above.

**Lemma** \(\text{OclIncludes-execute-generic}::\)

- **Assumes** \(\text{strict1}: (\text{invalid} = y) = \text{invalid}\)
- **And** \(\text{strict2}: (x = \text{invalid}) = \text{invalid}\)
- **And** \(\text{cp-StrictRefEq}: \forall (a::(A,a::\text{null})\text{val}) Y. (X \equiv Y) \tau = ((\lambda. \ X \tau) \equiv (\lambda. \ Y \tau)) \tau\)
- **And** \(\text{StrictRefEq-\text{vs-StrongEq}}: \forall (x::(A,a::\text{null})\text{val}) y \tau. \tau \vdash \nu \ x \Rightarrow \tau \vdash \nu \ y \Rightarrow (\tau \vdash ((x \equiv y) \triangleq (x \triangleq y)))\)
- **Shows**

\[
(X \rightarrow \text{including}_{\text{Set}}(x); (A,a::\text{null})\text{val}) \rightarrow \text{includes}_{\text{Set}}(y)) =
\begin{cases}
\text{true} & \text{if } \delta \ X \text{ then } x \equiv y \text{ then true else } X \rightarrow \text{includes}_{\text{Set}}(y) \text{ endif else invalid endif}
\end{cases}
\]

**Proof**
schematic-goal OclIncludes-execute$_{\tau}$[simp, code-unfold] : ?$
abla X$

(proof)

lemma OclIncludes-including-generic :
assumes OclIncludes-execute-generic [simp] : \(X \rightarrow \text{including$_{\tau}$}(x::(\mathcal{A},'a::null)val) \rightarrow \text{includes$_{\tau}$}(y)) =
(if \(\delta \ X \text{ then } x = y \text{ then } \text{true else } X \rightarrow \text{includes$_{\tau}$}(y) \text{ endif else } \text{invalid} \text{ endif})
and StrictRefEq-strict'' : \(\forall x y. \ \text{if } \delta (x::(\mathcal{A},'a::null)val) = y \text{ then } (\nu(x) \text{ and } \nu(y)) \\text{ endif else } \text{invalid} \text{ endif})
and a-val : \(\tau \mid = \nu a\)
and x-val : \(\tau \mid = \nu x\)
shows \(\tau \mid = S \rightarrow \text{including$_{\tau}$(a::(\mathcal{A},'a::null)val)} \rightarrow \text{includes$_{\tau}$}(x)\)
(proof)

lemmas OclIncludes-including$_{\text{Integer}} =$
\ OclIncludes-including-generic[OF OclIncludes-execute$_{\text{Integer}}$ StrictRefEq-integer. def-homo]

Execution Rules on Excludes

lemma OclExcludes-charn1 :
assumes def-X : \(\tau \mid = (\delta \ X)\)
assumes val-x : \(\tau \mid = (\nu x)\)
shows \(\tau \mid = (X \rightarrow \text{excluding$_{\tau}$}(x) \rightarrow \text{excludes$_{\tau}$(x)})\)
(proof)

Execution Rules on Size

lemma [simp, code-unfold] : \(\text{Set}() \rightarrow \text{size$_{\tau}$}() = 0\)
(proof)

lemma OclSize-including-exec[simp, code-unfold] :
\(\nu (X \rightarrow \text{including$_{\tau}$(x)} \rightarrow \text{size$_{\tau}$(x)}) = (if \ \delta \ X \text{ and } x \text{ then } X \rightarrow \text{size$_{\tau}$(x)} +_{\nu \int} \text{if } X \rightarrow \text{includes$_{\tau}$(x)} \text{ then } 0 \text{ else } 1 \text{ endif }\text{ else } \text{invalid} \text{ endif})\)
(proof)

Execution Rules on IsEmpty

lemma [simp, code-unfold] : \(\text{Set}() \rightarrow \text{isEmpty$_{\tau}$}() = \text{true}\)
(proof)

lemma OclIsEmpty-including [simp]:
assumes X-def : \(\tau = \delta \ X\)
and X-finite: finite "Rep-Set$_{\text{base}}$ (X \tau)"
and a-val : \(\tau = \nu a\)
shows \(X \rightarrow \text{including$_{\tau}$(a)} \rightarrow \text{isEmpty$_{\tau}$(a)} \tau = \text{false } \tau\)
(proof)

Execution Rules on NotEmpty

lemma [simp, code-unfold] : \(\text{Set}() \rightarrow \text{notEmpty$_{\tau}$}() = \text{false}\)
(proof)

lemma OclNotEmpty-including [simp, code-unfold]:
assumes X-def : \(\tau = \delta \ X\)

and X-finite: finite \(\mathcal{R}_{\text{Rep-Set}_{base}}(X \tau)\)
and a-val: \(\tau \models v a\)
suppose \(X \rightarrow \text{including}_{Set}(a) \rightarrow \text{notEmpty}_{Set}(\tau) = \text{true} \tau\)

\(<\text{proof}>\)

**Execution Rules on Any**

**Lemma** \[\text{OclANY-singleton-exec}\] \([\text{simp}, \text{code-unfold}]\):
\(\{\}\rightarrow \text{any}_{Set}(\tau) = \text{null}\)
\(<\text{proof}>\)

**Execution Rules on Forall**

**Lemma** \[\text{OclForall-mtSet-exec}\] \([\text{simp}, \text{code-unfold}]\):
\(\{\}\rightarrow \text{forall}_{Set}(\tau) = \text{true}\)
\(<\text{proof}>\)

The following rule is a main theorem of our approach: From a denotational definition that assures consistency, but may be — as in the case of the \(\text{OclForall } X P\) — dauntingly complex, we derive operational rules that can serve as a gold-standard for operational execution, since they may be evaluated in whatever situation and according to whatever strategy. In the case of \(\text{OclForall } X P\), the operational rule gives immediately a way to evaluation in any finite (in terms of conventional OCL: denotable) set, although the rule also holds for the infinite case:

\(\text{Integer}_{null} \rightarrow \text{forall}_{Set}(\text{null} - x \rightarrow \text{forall}_{Set}(y \rightarrow P(x) \equiv y + \text{int} x))\)

or even:

\(\text{Integer} \rightarrow \text{forall}_{Set}(x) \rightarrow \text{forall}_{Set}(y \equiv y + \text{int} x)\)

are valid OCL statements in any context \(\tau\).

**Theorem** \[\text{OclForall-including-exec}\] \([\text{simp}, \text{code-unfold}]\):
\(\begin{array}{l}
\text{assumes } \text{cp0} : \text{cp } P \\
\text{shows } (\{\\} \rightarrow \text{forall}_{Set}(x) \rightarrow \text{forall}_{Set}(z \rightarrow P(z))) = (\text{if } \delta S \text{ and } v x \\
\text{then } P x \text{ and } (\{\\} \rightarrow \text{forall}_{Set}(z \rightarrow P(z))) \\
\text{else invalid } \text{endif})
\end{array}\)
\(<\text{proof}>\)

**Execution Rules on Exists**

**Lemma** \[\text{OclExists-mtSet-exec}\] \([\text{simp}, \text{code-unfold}]\):
\(\{\}\rightarrow \exists_{Set}(z \rightarrow P(z)) = \text{false}\)
\(<\text{proof}>\)

**Lemma** \[\text{OclExists-including-exec}\] \([\text{simp}, \text{code-unfold}]\):
\(\begin{array}{l}
\text{assumes } \text{cp} : \text{cp } P \\
\text{shows } (\{\\} \rightarrow \exists_{Set}(x) \rightarrow \exists_{Set}(z \rightarrow P(z))) = (\text{if } \delta S \text{ and } v x \\
\text{then } P x \text{ or } (\{\\} \rightarrow \exists_{Set}(z \rightarrow P(z))) \\
\text{else invalid } \text{endif})
\end{array}\)
\(<\text{proof}>\)

**Execution Rules on Iterate**

**Lemma** \[\text{OclIterate-empty}\] \([\text{simp}, \text{code-unfold}]\):
\(\{\}\rightarrow \text{iterate}_{Set}(a ; x = A | P a x) = A\)
\(<\text{proof}>\)

In particular, this does hold for \(A = \text{null}\).
lemma OclIterate-including:

assumes \( S \)-finite: \( \tau \models \delta(S \to \text{sizes} S t()) \)
and \( F \)-valid-arg: (\( v \ A \)) \( \tau \equiv (v (F \ a \ A)) \ \tau \)
and \( F \)-commute: \( \text{comp-fun-commute} F \)
and \( F \)-cp: \( \bigwedge \ x \ y \ \tau. \ F \ x \ y \ \tau = F (\lambda - x \ \tau) \ y \ \tau \)

shows \((S \to \text{including} S t(a)) \to \text{iterate} S t(a; x = A \ | \ F \ a \ x)) \ \tau = \)
\((S \to \text{excluding} S t(a)) \to \text{iterate} S t(a; x = F \ a \ A \ | \ F \ a \ x)) \ \tau \)

(proof)

Execution Rules on Select

lemma OclSelect-mtSet-exec[simp,code-unfold]: OclSelect mtSet \( P = \text{mtSet} \)
(proof)

definition OclSelect-body :: - \to - \to - \to (\forall \ 'a \ option \ option) \ Set
\equiv (\lambda P \ x \ acc. \ \text{if} P \ x = \text{false} \ \text{then} \ acc \ \text{else} \ acc \to \text{including} S t(x) \ \text{endif})

theorem OclSelect-including-exec[simp,code-unfold]:
assumes \( P \)-cp: \( \text{cp} \ P \)
shows OclSelect (\( X \to \text{including} S t(y) \)) \( P = \text{OclSelect-body} \ P \ y \ (\text{OclSelect} (\( X \to \text{excluding} S t(y) \)) \ P) \)
(is - = ?select)
(proof)

Execution Rules on Reject

lemma OclReject-mtSet-exec[simp,code-unfold]: OclReject mtSet \( P = \text{mtSet} \)
(proof)

lemma OclReject-including-exec[simp,code-unfold]:
assumes \( P \)-cp: \( \text{cp} \ P \)
shows OclReject (\( X \to \text{including} S t(y) \)) \( P = \text{OclSelect-body} \ (\text{not o} \ P) \ y \ (\text{OclReject} (\( X \to \text{excluding} S t(y) \)) \ P) \)
(proof)

Execution Rules Combining Previous Operators

OclIncluding

lemma OclIncluding-idem0 : 
assumes \( \tau \models \delta \ S \)
and \( \tau \models \nu \ i \)
shows \( \tau \models (S \to \text{including} S t(i)) \to \text{including} S t(i) \equiv (S \to \text{including} S t(i)) \)
(proof)

theorem OclIncluding-idem[simp,code-unfold]: ((\( S :: (\forall \ 'a::\text{null})\text{Set}) \to \text{including} S t(i)) \to \text{including} S t(i) =
(S \to \text{including} S t(i)))
(proof)

OclExcluding

lemma OclExcluding-idem0 : 
assumes \( \tau \models \delta \ S \)
and \( \tau \models \nu \ i \)
shows \( \tau \models (S \to \text{excluding} S t(i)) \to \text{excluding} S t(i) \equiv (S \to \text{excluding} S t(i)) \)
(proof)

theorem OclExcluding-idem[simp,code-unfold]: ((S \to \text{excluding} S t(i)) \to \text{excluding} S t(i)) =
(S \to \text{excluding} S t(i))
\[\text{proof}\]

OclIncludes

\textbf{lemma OclIncludes-any[simp, code-unfold]}:
\[
\begin{align*}
X \rightarrow \text{includes}\_\text{Set}(X \rightarrow \text{any}_\text{Set}) &= (\text{if } \delta X \text{ then} \\
& \quad \text{if } (X \rightarrow \text{size}_\text{Set}()) \text{ then not}(X \rightarrow \text{isEmpty}_\text{Set}()) \\
& \quad \text{else } X \rightarrow \text{includes}_\text{Set}(\text{null}) \text{ endif} \\
& \quad \text{else invalid endif})
\end{align*}
\]

\[\text{proof}\]

OclSize

\textbf{lemma [simp, code-unfold]}: \(\delta(\text{Set}\{} \rightarrow \text{size}_\text{Set}()) = \text{true}\)

\[\text{proof}\]

\textbf{lemma [simp]}:
\[
\begin{align*}
\delta(\text{Set}\{} \rightarrow \text{size}_\text{Set}()) &= \text{true}
\end{align*}
\]

\[\text{proof}\]

\textbf{lemma OclForall-rep-set-true}:
\[
\begin{align*}
\tau |\!\!\|= \text{OclForall}
\end{align*}
\]

\[\text{proof}\]

\textbf{lemma OclForall-rep-set-false}:
\[
\begin{align*}
\tau |\!\!\|= \text{OclForall}
\end{align*}
\]

\[\text{proof}\]

\textbf{lemma OclForall-includes}:
\[
\begin{align*}
\text{assumes } x\text{-def} : \tau |\!\!\|= \text{δ } x \\
\text{and } y\text{-def} : \tau |\!\!\|= \text{δ } y
\end{align*}
\]

\[\text{proof}\]

\textbf{lemma OclForall-not-includes}:
\[
\begin{align*}
\text{assumes } x\text{-def} : \tau |\!\!\|= \text{δ } x \\
\text{and } y\text{-def} : \tau |\!\!\|= \text{δ } y
\end{align*}
\]

\[\text{proof}\]

\textbf{lemma OclForall-iterate}:
\[
\begin{align*}
\text{assumes } S\text{-finite} : \text{finite } \forall \tau. \text{finite } \forall \tau. \text{finite } \text{Rep}_\text{base}(X \tau) \Rightarrow \\
\text{show } S \rightarrow \text{forall}_\text{Set}(x \mid P x) \tau &= (S \rightarrow \text{iterate}_\text{Set}(x; \text{acc} = \text{true} \mid \text{acc and } P x)) \tau
\end{align*}
\]

\[\text{proof}\]

\textbf{lemma OclForall-cong}:
\[
\begin{align*}
\forall x. x \in \forall \tau. \text{finite } \forall \tau. \text{finite } \text{Rep}_\text{base}(X \tau) \Rightarrow \\
\text{assumes } P: \tau |\!\!\|= \text{OclForall}
\end{align*}
\]

113
shows $\tau \models OclForall \pi X$  
(proof)

**Lemma OclForall-cong**:  
**assumes**  
\[ \forall x. x \in \text{Rep-Set}_{\text{ns}} \, (X \tau)^\tau \Rightarrow \tau \models P (\lambda \tau. \, x) \Rightarrow \tau \models Q (\lambda \tau. \, x) \Rightarrow \tau \models R (\lambda \tau. \, x) \]  
**assumes**  
\[ P; \tau \models OclForall X P \]  
**assumes**  
\[ Q; \tau \models OclForall X Q \]  
**shows**  
\[ \tau \models OclForall X R \]  
(proof)

**Strict Equality**  
**Lemma StrictRefEqsSet-defined**:  
**assumes**  
\[ x\text{-def}: \tau \models \delta x \]  
**assumes**  
\[ y\text{-def}: \tau \models \delta y \]  
**shows**  
\[ ((x:\langle \lambda', \alpha::\text{null}\rangle\text{Set}) \doteq y) = \]  
\[ (x \rightarrow \text{forAll}_{\text{set}}(z \rightarrow \text{includes}_{\text{set}}(z)) \text{ and } (y \rightarrow \text{forAll}_{\text{set}}(z \rightarrow \text{includes}_{\text{set}}(z)))) \tau \]  
(proof)

**Lemma StrictRefEqsSet-excsimp-code-anfold**:  
\[ ((x:\langle \lambda', \alpha::\text{null}\rangle\text{Set}) \doteq y) = \]  
\[ (\text{if } \delta x \text{ then (if } \delta y \text{ then } \]  
\[ (x \rightarrow \text{forAll}_{\text{set}}(z \rightarrow \text{includes}_{\text{set}}(z)) \text{ and } (y \rightarrow \text{forAll}_{\text{set}}(z \rightarrow \text{includes}_{\text{set}}(z)))) \) \text{ else if } \)  
\[ \]  
\[ \) \text{ else invalid endif) \text{ endif)}} \text{ endif) \]  
(proof)

**Lemma OclIncluding-cong'**:  
**shows**  
\[ \tau \models \delta s \Rightarrow \tau \models \delta t \Rightarrow \tau \models v x \Rightarrow \]  
\[ \tau \models ((s:\langle \lambda', \alpha::\text{null}\rangle\text{Set}) \doteq t) \Rightarrow \tau \models (s \rightarrow \text{includes}_{\text{set}}(x) \doteq (t \rightarrow \text{includes}_{\text{set}}(x))) \]  
(proof)

**Lemma OclIncluding-cong**:  
\[ (s:\langle \lambda', \alpha::\text{null}\rangle\text{Set}) t x y \tau. \tau \models \delta t \Rightarrow \tau \models v y \Rightarrow \]  
\[ \tau \models s \doteq t \Rightarrow x = y \Rightarrow \tau \models s \rightarrow \text{includes}_{\text{set}}(x) \doteq (t \rightarrow \text{includes}_{\text{set}}(y)) \]  
(proof)

**Lemma const-StrictRefEqsSet-empty**:  
\[ \text{const } X \Rightarrow \text{const } (X \doteq \text{Set}\{\}) \]  
(proof)

**Lemma const-StrictRefEqsSet-including**:  
\[ \text{const } a \Rightarrow \text{const } S \Rightarrow \text{const } X \Rightarrow \text{const } (X \doteq S \rightarrow \text{includes}_{\text{set}}(a)) \]  
(proof)

2.9.26. Test Statements  
**Assert**  
\[ (\tau \models (\text{Set}\{\lambda::\text{null}\}) \doteq \text{Set}\{\lambda::\text{null}\})) \]
2.10. Collection Type Sequence: Operations

2.10.1. Basic Properties of the Sequence Type

Every element in a defined sequence is valid.

Lemma **Sequence-inv-lemma**: \( \tau \models (\delta X) \implies \forall x \in \text{set } "\text{Rep-Sequence}_{\text{base}}(X \tau)". x \neq \bot \)  

\[\text{(proof)}\]

2.10.2. Definition: Strict Equality

After the part of foundational operations on sets, we detail here equality on sets. Strong equality is inherited from the OCL core, but we have to consider the case of the strict equality. We decide to overload strict equality in the same way we do for other value’s in OCL:

Overloading

\[\text{StrictRefEq} \equiv \text{StrictRefEq} : [\langle \text{null}, \alpha:::\text{null}\rangle\text{Sequence},\langle \text{null}, \alpha:::\text{null}\rangle\text{Sequence}] \rightarrow (\text{\$Boolean})\]

\[\text{(proof)}\]

One might object here that for the case of objects, this is an empty definition. The answer is no,
we will restrain later on states and objects such that any object has its oid stored inside the object (so the ref, under which an object can be referenced in the store will be represented in the object itself). For such well-formed stores that satisfy this invariant (the WFF-invariant), the referential equality and the strong equality—and therefore the strict equality on sequences in the sense above—coincides.

Property proof in terms of $\text{profile-bin}_{\text{StrongEq}}$

**interpretation** $\text{StrictRefEq}_{\text{seq}} : \text{profile-bin}_{\text{StrongEq}} \pi \lambda x. (x : (\text{null} : \text{Sequence})) \Rightarrow y$

(\text{proof})

## 2.10.3. Constants: $\text{mtSequence}$

**definition** $\text{mtSequence} :: (\forall \alpha . \text{null}) \text{Sequence} (\text{Sequence}())$

**where** $\text{Sequence}() \equiv (\lambda \tau. \text{\text{Abs-Sequence}}_{\text{base}} (\tau) :: (\forall \alpha. \text{\text{list}}_{\alpha}))$

**lemma** $\text{mtSequence-defined} [\text{simp, code-unfold}] : \delta (\text{Sequence}()) = \text{true}$

(\text{proof})

**lemma** $\text{mtSequence-valid} [\text{simp, code-unfold}] : \nu (\text{Sequence}()) = \text{true}$

(\text{proof})

**lemma** $\text{mtSequence-rep-set} : \text{Abs-Sequence}_{\text{base}} (\text{Sequence}()) \tau \equiv []$

(\text{proof})

**lemma** $\text{mtSequence-defined} [\text{simp, code-unfold}] : \text{const Sequence}()$

(\text{proof})

Note that the collection types in OCL allow for null to be included; however, there is the null-collection into which inclusion yields invalid.

## 2.10.4. Definition: Prepend

**definition** $\text{OclPrepend} :: (\forall \alpha. \text{null}) \text{Sequence}, (\forall \alpha. \text{val}) \Rightarrow (\forall \alpha) \text{Sequence}$

**where** $\text{OclPrepend} x y = (\lambda \tau. \text{if } (\delta x) \tau = \text{true } \tau \land (\nu y) \tau = \text{true } \tau$

then $\text{Abs-Sequence}_{\text{base}} (\tau) \equiv \text{Abs-Sequence}_{\text{base}} (x \tau) \tau$

else invalid $\tau$

)\text{)

**notation** $\text{OclPrepend} (\text{preprend}_{\text{Seq}} ' - ')$

**interpretation** $\text{OclPrepend} : \text{profile-bin}_{\text{d-v}} \text{OclPrepend} \lambda x y. \text{Abs-Sequence}_{\text{base}} (\tau) \equiv \text{\text{Abs-Sequence}_{\text{base}} (x \tau)}$

(\text{proof})

**syntax**

- $\text{OclFinsequence} :: \text{args} \Rightarrow (\forall \alpha. \text{null}) \text{Sequence} (\text{Sequence}())$

**translations**

$\text{Sequence} [[] \tau \Rightarrow \text{CONST OclPrepend (Sequence)x}]$

$\text{Sequence} (x) \Rightarrow \text{CONST OclPrepend (Sequence)x}$

## 2.10.5. Definition: Including

**definition** $\text{OclIncluding} :: (\forall \alpha. \text{null}) \text{Sequence}, (\forall \alpha. \text{val}) \Rightarrow (\forall \alpha) \text{Sequence}$

**where** $\text{OclIncluding} x y = (\lambda \tau. \text{if } (\delta x) \tau = \text{true } \tau \land (\nu y) \tau = \text{true } \tau$

then $\text{Abs-Sequence}_{\text{base}} (\tau) \equiv \text{Abs-Sequence}_{\text{base}} (x \tau) \tau$

else invalid $\tau$

)\text{)

**notation** $\text{OclIncluding} (\text{including} _{\text{Seq}} ' - ')$

**interpretation** $\text{OclIncluding} : \text{profile-bin}_{\text{d-v}} \text{OclIncluding} \lambda x. y. \text{Abs-Sequence}_{\text{base}} (\tau) \equiv \text{Abs-Sequence}_{\text{base}} (x \tau) \tau$

(\text{proof})
2.10.6. Definition: Excluding

**definition** OclExcluding :: \((\forall \alpha\cdot:\text{null})\ \text{Sequence},(\forall \alpha\cdot)\ \text{val} \Rightarrow (\forall \alpha\cdot)\ \text{Sequence}\)

where

\[
\text{OclExcluding } x \ y = (\lambda \tau. \text{if } (\delta \ x) \ \tau = \text{true } \tau \wedge (\nu \ y) \ \tau = \text{true } \tau \\
\text{then Abs-Sequence}_{\text{base}} \sqcup \text{filter} (\lambda x. x = y \ \tau) \\
\text{else invalid })
\]

**notation** OclExcluding \((-\rightarrow)\) \text{excluding}_{\text{Seq}}'(-'\))

**interpretation** OclExcluding-profile-bin\text{d}⇒ OclExcluding

\[
\lambda x \ y. \text{Abs-Sequence}_{\text{base}} \sqcup \text{filter} (\lambda x. x = y) \quad \text{Rep-Sequence}_{\text{base}} (x \ \tau)^\top_{\text{Seq}}
\]

(\text{proof})

2.10.7. Definition: Append

Identical to OclIncluding.

**definition** OclAppend :: \((\forall \alpha\cdot:\text{null})\ \text{Sequence},(\forall \alpha\cdot)\ \text{val} \Rightarrow (\forall \alpha\cdot)\ \text{Sequence}\)

where

\[
\text{OclAppend } = \text{OclIncluding}
\]

**notation** OclAppend \((-\rightarrow)\) \text{append}_{\text{Seq}}'(-'\))

**interpretation** OclAppend :

profile-bin\text{d}⇒ OclAppend \lambda x \ y. \text{Abs-Sequence}_{\text{base}} \sqcup \text{filter} (\lambda x. x = y) \quad \text{Rep-Sequence}_{\text{base}} (x \ \tau)^\top_{\text{Seq}}[y]_{\text{Seq}}

(\text{proof})

2.10.8. Definition: Union

**definition** OclUnion :: \((\forall \alpha\cdot:\text{null})\ \text{Sequence},(\forall \alpha\cdot)\ \text{Sequence} \Rightarrow (\forall \alpha\cdot)\ \text{Sequence}\)

where

\[
\text{OclUnion } x \ y = (\lambda \tau. \text{if } (\delta \ x) \ \tau = \text{true } \tau \wedge (\delta \ y) \ \tau = \text{true } \tau \\
\text{then Abs-Sequence}_{\text{base}} \sqcup \text{filter} (\lambda x. x \leq y \ y \ \tau) \\
\text{else invalid } \tau)
\]

**notation** OclUnion \((-\rightarrow)\) \text{union}_{\text{Seq}}'(-'\))

**interpretation** OclUnion :

profile-bin\text{d}⇒ OclUnion \lambda x \ y. \text{Abs-Sequence}_{\text{base}} \sqcup \text{filter} (\lambda x. x \leq y) \quad \text{Rep-Sequence}_{\text{base}} (x \ \tau)^\top_{\text{Seq}}[y]_{\text{Seq}}

(\text{proof})

2.10.9. Definition: At

**definition** OclAt :: \((\forall \alpha\cdot:\text{null})\ \text{Sequence},(\forall \alpha\cdot)\ \text{Integer} \Rightarrow (\forall \alpha\cdot)\ \text{val}\)

where

\[
\text{OclAt } x \ y = (\lambda \tau. \text{if } (\delta \ x) \ \tau = \text{true } \tau \wedge (\delta \ y) \ \tau = \text{true } \tau \\
\text{then Abs-Sequence}_{\text{base}} \sqcup \text{filter} (\lambda x. 1 \leq y \ \tau \wedge y \ \tau \leq \text{length}\text{Rep-Sequence}_{\text{base}} (x \ \tau)^\top_{\text{Seq}} \\
\text{then } \text{Rep-Sequence}_{\text{base}} (x \ \tau)^\top_{\text{Seq}}[\text{nat } y \ \tau - 1] \\
\text{else invalid } \tau)
\]

**notation** OclAt \((-\rightarrow)\) \text{at}_{\text{Seq}}'(-'\))

2.10.10. Definition: First

**definition** OclFirst :: \((\forall \alpha\cdot:\text{null})\ \text{Sequence} \Rightarrow (\forall \alpha\cdot)\ \text{val}\)
where \( \text{OclFirst} \ x = (\lambda \tau. \text{if } (\delta x) \tau = \text{true } \tau \text{ then } \text{case } \text{Rep-Sequence}_{\text{base}} (x \tau) \text{ of } \text{[] } \Rightarrow \text{invalid } \tau \ | \ x \# \Rightarrow x ) \)

\( \text{not} \not \text{ation} \text{OclFirst} \ (\text{-->first}_{\text{seq}}('\gamma')) \)

2.10.11. Definition: Last

\( \text{definition} \text{OclLast} \ :: \ [(\mathcal{A},'\alpha::\text{null}) \text{Sequence}] \Rightarrow (\mathcal{A},'\alpha) \text{val} \)

where \( \text{OclLast} \ x = (\lambda \tau. \text{if } (\delta x) \tau = \text{true } \tau \text{ then } \text{if } \text{Rep-Sequence}_{\text{base}} (x \tau) \text{=} \text{[]} \text{ then } \text{invalid } \tau \text{ else last } \text{Rep-Sequence}_{\text{base}} (x \tau) \text{=} \text{invalid } \tau \text{ else invalid } \tau \) \)

\( \text{not} \not \text{ation} \text{OclLast} \ (\text{-->last}_{\text{seq}}('\gamma')) \)

2.10.12. Definition: Iterate

\( \text{definition} \text{OclIterate} \ :: \ [(\mathcal{A},'\alpha::\text{null}) \text{Sequence},(\mathcal{A},'\beta::\text{null})\text{val}, \text{((\mathcal{A},'\alpha)\text{val})} \Rightarrow (\mathcal{A},'\beta)\text{val}] \Rightarrow (\mathcal{A},'\beta)\text{val} \)

where \( \text{OclIterate} \ A \ F = (\lambda \tau. \text{if } (\delta S) \tau = \text{true } \tau \& (v A) \tau = \text{true } \tau \text{ then } (\text{foldr } P (\text{map } (\lambda a. \tau. a) \text{Rep-Sequence}_{\text{base}} (S \tau))) (A) \tau \text{ else } \bot ) \)

\( \text{syntax} \ -\text{OclIterate}_{\text{Seq}} \ :: \ [(\mathcal{A},'\alpha::\text{null}) \text{Sequence}, \text{idt, idt, 'α, 'β}] \Rightarrow (\mathcal{A},'γ)\text{val} \)

\(-\text{-->iterate}_{\text{seq}}('\gamma:=-\cdot')\)

\( \text{translations} \ X\text{-}\rightarrow\text{iterate}_{\text{seq}}(a; x = A \mid P) == \text{CONST} \text{OclIterate } X \ A (\% a. (\% x. P)) \)

2.10.13. Definition: Forall

\( \text{definition} \text{OclForall} \ :: \ [(\mathcal{A},'\alpha::\text{null}) \text{Sequence},(\mathcal{A},'\alpha)\text{val}\Rightarrow(\mathcal{A})\text{Boolean}] \Rightarrow \mathcal{A} \text{ Boolean} \)

where \( \text{OclForall} \ S \ P = (S\text{-}\rightarrow\text{iterate}_{\text{seq}}(b; x = \text{true } \mid x \text{ and } (P b))) \)

\( \text{syntax} \ -\text{OclForall}_{\text{Seq}} \ :: \ [(\mathcal{A},'\alpha::\text{null}) \text{Sequence}, \text{id, '(\mathcal{A})\text{Boolean}] \Rightarrow \mathcal{A} \text{ Boolean } \text{-}\text{-->forAll}_{\text{seq}}('\cdot') \)

\( \text{translations} \ X\text{-}\rightarrow\text{forAll}_{\text{seq}}(x \mid P) == \text{CONST} \text{UML-Sequence.OclForall } X (\% x. P) \)

2.10.14. Definition: Exists

\( \text{definition} \text{OclExists} \ :: \ [(\mathcal{A},'\alpha::\text{null}) \text{Sequence},(\mathcal{A},'\alpha)\text{val}\Rightarrow(\mathcal{A})\text{Boolean}] \Rightarrow \mathcal{A} \text{ Boolean} \)

where \( \text{OclExists} \ S \ P = (S\text{-}\rightarrow\text{iterate}_{\text{seq}}(b; x = \text{false } \mid x \text{ or } (P b))) \)

\( \text{syntax} \ -\text{OclExists}_{\text{Seq}} \ :: \ [(\mathcal{A},'\alpha::\text{null}) \text{Sequence}, \text{id, '(\mathcal{A})\text{Boolean}] \Rightarrow \mathcal{A} \text{ Boolean } \text{-}\text{-->exists}_{\text{seq}}('\cdot') \)

\( \text{translations} \ X\text{-}\rightarrow\text{exists}_{\text{seq}}(x \mid P) == \text{CONST} \text{OclExists } X (\% x. P) \)

2.10.15. Definition: Collect

\( \text{definition} \text{OclCollect} \ :: \ [(\mathcal{A},'\alpha::\text{null}) \text{Sequence},(\mathcal{A},'\alpha)\text{val}\Rightarrow(\mathcal{A},'\beta)\text{val}]\Rightarrow(\mathcal{A},'\beta::\text{null})\text{Sequence} \)

where \( \text{OclCollect} \ S \ P = (S\text{-}\rightarrow\text{iterate}_{\text{seq}}(b; x = \text{Sequence} \{ \} \mid x\text{-}\rightarrow\text{prepend}_{\text{seq}}(P b))) \)

\( \text{syntax} \ -\text{OclCollect}_{\text{Seq}} \ :: \ [(\mathcal{A},'\alpha::\text{null}) \text{Sequence}, \text{id, '(\mathcal{A})\text{Boolean}] \Rightarrow \mathcal{A} \text{ Boolean } \text{-}\text{-->collect}_{\text{seq}}('\cdot') \)

\( \text{translations} \)

118
2.10.16. Definition: Select

\[ \text{OclSelect} :: \left[ (\mathcal{X}, \alpha::\text{null}) \text{Sequence} \rightarrow (\mathcal{X}) \text{Boolean} \right] \rightarrow (\mathcal{X}, \alpha::\text{null}) \text{Sequence} \]

where

\[ \text{OclSelect } S \ P = (S \rightarrow \text{iterate Seq } (b; \ x = \text{Sequence} \{} | \text{if } P \ b \ \text{then } x \rightarrow \text{prepend Seq } (b) \ \text{else } x \ \text{endif}) \]

syntax

\[ \text{OclSelectSeq} :: \left[ (\mathcal{X}, \alpha::\text{null}) \text{Sequence}, (\mathcal{X}, \alpha::\text{null}) \text{val} \rightarrow (\mathcal{X}, \alpha::\text{null}) \text{Sequence} \right] \]

translations

\[ X \rightarrow \text{select Seq } (x | P) = \text{CONST UML-Sequence} \text{. OclSelect } X (\% x. P) \]

2.10.17. Definition: Size

\[ \text{OclSize} :: \left[ (\mathcal{X}, \alpha::\text{null}) \text{Sequence} \right] \rightarrow (\mathcal{X}, \alpha::\text{null}) \text{Integer} \]

where

\[ \text{OclSize } S = (S \rightarrow \text{iterate Seq } (b; \ x = 0 | x + \text{int } 1 )) \]

2.10.18. Definition: IsEmpty

\[ \text{OclIsEmpty} :: (\mathcal{X}, \alpha::\text{null}) \text{Sequence} \rightarrow (\mathcal{X}, \alpha::\text{null}) \text{Boolean} \]

where

\[ \text{OclIsEmpty } x = (\nu x \ and \ not (\delta x)) \ or \ ((\text{OclSize } x) = 0) \]

notation

\[ \text{OclIsEmpty } (\rightarrow \text{isEmpty Seq } (\)) \]

2.10.19. Definition: NotEmpty

\[ \text{OclNotEmpty} :: (\mathcal{X}, \alpha::\text{null}) \text{Sequence} \rightarrow (\mathcal{X}, \alpha::\text{null}) \text{Boolean} \]

where

\[ \text{OclNotEmpty } x = \text{not}(\text{OclIsEmpty } x) \]

notation

\[ \text{OclNotEmpty } (\rightarrow \text{notEmpty Seq } (\)) \]

2.10.20. Definition: Any

\[ \text{OclANY } x = (\lambda \tau. \ \text{if } x \ \tau = \text{invalid } \tau \ \text{then } \perp \ \text{else } \text{case } \text{drop} \ (\text{drop } (\text{Rep-Sequence}_{\text{base}} (x \ \tau))) \ of \ [] \Rightarrow \perp \ | l \Rightarrow \text{hd } l) \]

notation

\[ \text{OclANY } (\rightarrow \text{any Seq } (\)) \]

2.10.21. Definition (future operators)

\[ \text{OclCount} :: \left[ (\mathcal{X}, \alpha::\text{null}) \text{Sequence}, (\mathcal{X}, \alpha) \text{Sequence} \right] \rightarrow (\mathcal{X}, \alpha) \text{Integer} \]

notation

\[ \text{OclCount } (\rightarrow \text{count Seq } (\)) \]

\[ \text{OclSum} :: (\mathcal{X}, \alpha::\text{null}) \text{Sequence} \rightarrow (\mathcal{X}, \alpha) \text{Integer} \]

notation

\[ \text{OclSum } (\rightarrow \text{sum Seq } (\)) \]
2.10.22. Logical Properties

2.10.23. Execution Laws with Invalid or Null as Argument

OclIterate

**lemma OclIterate-invalid**: \(\text{simp, code-unfold}: \text{invalid} \to \text{iterate}_{\text{Seq}}(a; x = A \mid P a x) = \text{invalid}\) (proof)

**lemma OclIterate-null**: \(\text{simp, code-unfold}: \text{null} \to \text{iterate}_{\text{Seq}}(a; x = A \mid P a x) = \text{invalid}\) (proof)

**lemma OclIterate-invalid-args**: \(\text{simp, code-unfold}: S \to \text{iterate}_{\text{Seq}}(a; x = \text{invalid} \mid P a x) = \text{invalid}\) (proof)

Context Passing

**lemma cp-OclIncluding**: \(\text{cp-OclIncluding:} (X \to \text{including}_{\text{Seq}}(x)) \tau = ((\lambda \cdot. X \tau) \to \text{including}_{\text{Seq}}(\lambda \cdot. x \tau)) \tau\) (proof)

**lemma cp-OclIterate**: \(\text{cp-OclIterate:} (X \to \text{iterate}_{\text{Seq}}(a; x = A \mid P a x)) \tau = ((\lambda \cdot. X \tau) \to \text{iterate}_{\text{Seq}}(a; x = A \mid P a x)) \tau\) (proof)

**lemmas cp-intro′′_{\text{Seq}}[intro!, simp, code-unfold] = cp-OclIncluding [THEN allI[THEN allI[THEN allI[THEN cpI2]], of OclIncluding]]**

Const

2.10.24. General Algebraic Execution Rules

Execution Rules on Iterate

**lemma OclIterate-empty**: \(\text{Sequence}{} \to \text{iterate}_{\text{Seq}}(a; x = A \mid P a x) = A\) (proof)

In particular, this does hold for A = null.

**lemma OclIterate-including**: \(\text{simp, code-unfold}:\)\(\text{Sequence}{} \to \text{iterate}_{\text{Seq}}(a; x = A \mid P a x) = A\) (proof)

**assumes strict1**: \(\land X. P \text{ invalid} X = \text{invalid}\)

and \(P\)-valid-arg: \(\land \tau. (v A) \tau = (v (P a A)) \tau\)

and \(P\)-cp: \(\land x y \tau. P x y \tau = P (\lambda \cdot. x \tau) y \tau\)

and \(P\)-cp′: \(\land x y \tau. P x y \tau = P x (\lambda \cdot. y \tau) \tau\)

**shows** \(S \to \text{iterate}_{\text{Seq}}(b; x = A \mid P b x) = S \to \text{iterate}_{\text{Seq}}(b; x = P a A \mid P b x)\) (proof)

**lemma OclIterate-prepend**: \(\text{simp, code-unfold}:\)\(\text{Sequence}{} \to \text{iterate}_{\text{Seq}}(a; x = A \mid P a x) = A\) (proof)

**assumes strict1**: \(\land X. P \text{ invalid} X = \text{invalid}\)

and \(P\)-valid-arg: \(\land \tau. (v A) \tau = (v (P a A)) \tau\)

and \(P\)-cp: \(\land x y \tau. P x y \tau = P (\lambda \cdot. x \tau) y \tau\)

and \(P\)-cp′: \(\land x y \tau. P x y \tau = P x (\lambda \cdot. y \tau) \tau\)

**shows** \(S \to \text{iterate}_{\text{Seq}}(b; x = A \mid P b x) = P a (S \to \text{iterate}_{\text{Seq}}(b; x = A \mid P b x))\) (proof)

2.10.25. Test Statements

**instantiation Sequence\_base := (equal)equal**

begin
\textbf{definition} \textit{HOL.equal} \( k \leftrightarrow (k::('a::equal)\text{Sequence} base) = l \)

\textbf{instance} \{\textit{proof}\}
end

\textbf{lemma} \textit{equal-Sequence\_base-code} [code]:
\textit{HOL.equal} \( k \leftrightarrow (Rep\text{-Sequence} base k = Rep\text{-Sequence} base l) \)
\{\textit{proof}\}

\textbf{end}

\textbf{theory} \textit{UML-Library}
\textbf{imports}
\begin{itemize}
  \item basic-types/\textit{UML-Boolean}
  \item basic-types/\textit{UML-Void}
  \item basic-types/\textit{UML-Integer}
  \item basic-types/\textit{UML-Real}
  \item basic-types/\textit{UML-String}
  \item collection-types/\textit{UML-Pair}
  \item collection-types/\textit{UML-Bag}
  \item collection-types/\textit{UML-Set}
  \item collection-types/\textit{UML-Sequence}
\end{itemize}
\textbf{begin}

\textbf{2.11. Miscellaneous Stuff}

\textbf{2.11.1. Definition: asBoolean}

\textbf{definition} \textit{OclAsBoolean\_Int} :: ('\textit{\_A} Integer ⇒ ('\textit{\_A}) Boolean)
where
\textit{OclAsBoolean\_Int} \( X = (\lambda\tau. \text{if } (\delta X) \tau = \text{true } \tau \text{ then } \downarrow\uparrow\uparrow X \tau \downarrow\downarrow \neq 0 \downarrow\downarrow \text{ else invalid } \tau) \)

\textbf{interpretation} \textit{OclAsBoolean\_Int} : \textit{profile-mono} \textit{OclAsBoolean\_Int} \( \lambda x. \downarrow\uparrow\uparrow x \tau \downarrow\downarrow \neq 0 \downarrow\downarrow \)
\{\textit{proof}\}

\textbf{definition} \textit{OclAsBoolean\_Real} :: ('\textit{\_A} Real ⇒ ('\textit{\_A}) Boolean)
where
\textit{OclAsBoolean\_Real} \( X = (\lambda\tau. \text{if } (\delta X) \tau = \text{true } \tau \text{ then } \downarrow\uparrow\uparrow X \tau \downarrow\downarrow \neq 0 \downarrow\downarrow \text{ else invalid } \tau) \)

\textbf{interpretation} \textit{OclAsBoolean\_Real} : \textit{profile-mono} \textit{OclAsBoolean\_Real} \( \lambda x. \downarrow\uparrow\uparrow x \tau \downarrow\downarrow \neq 0 \downarrow\downarrow \)
\{\textit{proof}\}
2.11.2. Definition: asInteger

definition OclAsInteger_{Real} :: (\mathcal{A}) Real \to (\mathcal{A}) Integer ((\cdot)\to\text{oclAsType}_{\text{Real}}(\text{Integer}'))

where OclAsInteger_{Real} X = (\lambda \tau. \text{if } (\delta X) \tau = \text{true } \tau
\text{ then } \lfloor X \rfloor \tau^n_{\downarrow} \text{ else invalid } \tau)

interpretation OclAsInteger_{Real} : profile-\text{mono}d OclAsInteger_{Real} \lambda x. \lfloor X \rfloor \tau^n_{\downarrow}

(proof)

2.11.3. Definition: asReal

definition OclAsReal_{Int} :: (\mathcal{A}) Integer \to (\mathcal{A}) Real ((\cdot)\to\text{oclAsType}_{\text{Int}}(\text{Real}'))

where OclAsReal_{Int} X = (\lambda \tau. \text{if } (\delta X) \tau = \text{true } \tau
\text{ then } \lfloor X \rfloor \tau^n_{\downarrow} \text{ else invalid } \tau)

interpretation OclAsReal_{Int} : profile-\text{mono}d OclAsReal_{Int} \lambda x. \lfloor X \rfloor \tau^n_{\downarrow}

(proof)

lemma Integer-subtype-of-Real:
assumes \tau \equiv \delta X
shows \tau \equiv X \to \text{oclAsType}_{\text{Int}}(\text{Real}) \to \text{oclAsType}_{\text{Real}}(\text{Integer}) \equiv X

(proof)

2.11.4. Definition: asPair

definition OclAsPair_{Seq} :: ((\mathcal{A},'a::null)\text{Sequence})\Rightarrow((\mathcal{A},'a::null,'a::null)\text{ Pair }) ((\cdot)\to\text{asPair}_{\text{seq}}(\cdot))

where OclAsPair_{Seq} S = (\text{if } S \to \text{size}_{\text{Seq}}() = 2
\text{ then } \text{Pair}(S \to \text{at}_{\text{Seq}}(0),S \to \text{at}_{\text{Seq}}(1))
\text{ else invalid endif})

definition OclAsPair_{Set} :: ((\mathcal{A},'a::null)\text{Set})\Rightarrow((\mathcal{A},'a::null,'a::null)\text{ Pair }) ((\cdot)\to\text{asPair}_{\text{set}}(\cdot))

where OclAsPair_{Set} S = (\text{if } S \to \text{size}_{\text{Set}}() = 2
\text{ then let } v = S \to \text{any}_{\text{Set}}() \text{ in }
\text{Pair}(v,S \to \text{excluding}_{\text{Set}}(v) \to \text{any}_{\text{Set}}())
\text{ else invalid endif})

definition OclAsPair_{Bag} :: ((\mathcal{A},'a::null)\text{Bag})\Rightarrow((\mathcal{A},'a::null,'a::null)\text{ Pair }) ((\cdot)\to\text{asPair}_{\text{bag}}(\cdot))

where OclAsPair_{Bag} S = (\text{if } S \to \text{size}_{\text{Bag}}() = 2
\text{ then let } v = S \to \text{any}_{\text{Bag}}() \text{ in }
\text{Pair}(v,S \to \text{excluding}_{\text{Bag}}(v) \to \text{any}_{\text{Bag}}())
\text{ else invalid endif})

2.11.5. Definition: asSet

definition OclAsSets_{Seq} :: ((\mathcal{A},'a::null)\text{Sequence})\Rightarrow((\mathcal{A},'a)\text{Set }) ((\cdot)\to\text{asSets}_{\text{seq}}(\cdot))

where OclAsSets_{Seq} S = (S \to \text{iterate}_{\text{Seq}}(b;x = \text{Set}(); x \to \text{including}_{\text{Set}}(b)))

definition OclAsSets_{Pair} :: ((\mathcal{A},'a::null,'a::null)\text{Pair})\Rightarrow((\mathcal{A},'a)\text{Set }) ((\cdot)\to\text{asSet}_{\text{pair}}(\cdot))

where OclAsSets_{Pair} S = \text{Set}(S . \text{First}(), S . \text{Second}())

definition OclAsSets_{Bag} :: ((\mathcal{A},'a::null)\text{Bag})\Rightarrow((\mathcal{A},'a)\text{Set }) ((\cdot)\to\text{asSet}_{\text{bag}}(\cdot))

where OclAsSets_{Bag} S = (\lambda \tau. \text{if } (\delta S) \tau = \text{true } \tau
\text{ then } \text{Abs-Set}_{\text{asSet}}\text{Rep-Set-base } S \tau_{\downarrow}
\text{ else invalid endif})
2.11.6. Definition: asSequence

**Definition** \(\text{OclAsSeq}_{\text{set}}::((\forall \alpha::\text{null})\text{Set})\Rightarrow((\forall \alpha)\text{Sequence})\)

**where** \(\text{OclAsSeq}_{\text{set}} S = (S \Rightarrow \text{iterate}_{\text{set}}(b; x = \text{Sequence}()) | x \Rightarrow \text{including}_{\text{seq}}(b))\)

**Definition** \(\text{OclAsSeq}_{\text{bag}}::((\forall \alpha::\text{null})\text{Bag})\Rightarrow((\forall \alpha)\text{Sequence})\)

**where** \(\text{OclAsSeq}_{\text{bag}} S = (S \Rightarrow \text{iterate}_{\text{bag}}(b; x = \text{Sequence}()) | x \Rightarrow \text{including}_{\text{seq}}(b))\)

**Definition** \(\text{OclAsSeq}_{\text{pair}}::((\forall \alpha::\text{null},\alpha::\text{null})\text{Pair})\Rightarrow((\forall \alpha)\text{Sequence})\)

**where** \(\text{OclAsSeq}_{\text{pair}} S = \text{Sequence}(S .\text{First}(), S .\text{Second}())\)

2.11.7. Definition: asBag

**Definition** \(\text{OclAsBag}_{\text{set}}::((\forall \alpha::\text{null})\text{Sequence})\Rightarrow((\forall \alpha)\text{Bag})\)

**where** \(\text{OclAsBag}_{\text{set}} S = (\lambda \tau. \text{Abs-Bag}_{\text{base}}(\lambda s. \text{if list-ex} ((\Rightarrow) s)^n \text{Rep-Sequence}_{\text{base}}(S \tau)^n \text{then} 1 \text{ else} 0 \_\_))\)

**Definition** \(\text{OclAsBag}_{\text{bag}}::((\forall \alpha::\text{null})\text{Set})\Rightarrow((\forall \alpha)\text{Bag})\)

**where** \(\text{OclAsBag}_{\text{bag}} S = (\lambda \tau. \text{Abs-Bag}_{\text{base}}(\lambda s. \text{if } s \in ((\Rightarrow) \text{Rep-Set}_{\text{base}}(S \tau)^n \text{then} 1 \text{ else} 0 \_\_))\)

**Lemma** assumes \(\tau \Rightarrow \delta (S \Rightarrow \text{size}_{\text{set}}())\)

**shows** \(\text{OclAsBag}_{\text{set}} S = (S \Rightarrow \text{iterate}_{\text{set}}(b; x = \text{Bag}()) | x \Rightarrow \text{including}_{\text{bag}}(b))\)

**proof**

**Definition** \(\text{OclAsBag}_{\text{pair}}::((\forall \alpha::\text{null},\alpha::\text{null})\text{Pair})\Rightarrow((\forall \alpha)\text{Bag})\)

**where** \(\text{OclAsBag}_{\text{pair}} S = \text{Bag}(S .\text{First}(), S .\text{Second}())\)

2.11.8. Collection Types

**Lemmas** \(cp\-intro''\ [\text{intro\_simp\_code\_unfold} = cp\-intro'\)

**cp\-intro''_{\text{set}}**

**cp\-intro''_{\text{seq}}**

2.11.9. Test Statements

**Lemma** \(\text{syntax-test}: \text{Set}(2) = (\text{Set}() \Rightarrow \text{including}_{\text{set}}(1) \Rightarrow \text{including}_{\text{set}}(2))\)

**proof**

Here is an example of a nested collection.

**Lemma** \(\text{semantic-test2}:\)

**assumes** \(H:\{\text{Set}(2) = \text{null}\} = (false::(\forall)\text{Boolean})\)

**shows** \(\tau::(\forall)\text{st} | (\text{Set}(\text{Set}(2),\text{null}) \Rightarrow \text{includes}_{\text{set}}(\text{null}))\)

**proof**

**Lemma** \(\text{short\-cut'}[\text{simp\_code\_unfold}]: (8 \Rightarrow 6) = false\)

**proof**

**Lemma** \(\text{short\-cut''}[\text{simp\_code\_unfold}]: (2 \Rightarrow 1) = false\)

**proof**

**Lemma** \(\text{short\-cut''}[\text{simp\_code\_unfold}]: (1 \Rightarrow 2) = false\)

**proof**

123
Assert $\tau \models (0 <_{\text{int}} 2)$ and $(0 <_{\text{int}} 1)$

Elementary computations on Sets.

declare OclSelect-body-def [simp]

Assert $\neg (\tau \models v(\text{invalid}:(\forall,\alpha::\text{null}) \text{Set}))$
Assert $\tau \models v(\text{null}:(\forall,\alpha::\text{null}) \text{Set})$
Assert $\neg (\tau \models \delta(\text{null}:(\forall,\alpha::\text{null}) \text{Set}))$
Assert $\tau \models v(\text{Set}())$
 Assert $\tau \models v(\text{Set}() \text{null})$
Assert $\tau \models \delta(\text{Set}() \text{null})$
Assert $\tau \models (\text{Set}() \text{null}) \rightarrow \text{includes}_{\text{sset}}(1)$
Assert $\neg (\tau \models (\text{Set}() \text{null}) \rightarrow \text{includes}_{\text{sset}}(\text{null}))$
Assert $\neg (\tau \models (\text{Set}() \text{null}) \rightarrow \text{includes}_{\text{sset}}(\text{null}))$
Assert $\tau \models (\text{Set}() \text{null}) \rightarrow \text{includes}_{\text{sset}}(\text{null})$
Assert $\tau \models (\text{Set}() \text{null}) \rightarrow \text{forAll}_{\text{sset}}(z \mid 0 <_{\text{int}} z)$

Assert $\tau \models ((\text{Set}() \text{null}) \rightarrow \text{forall}_{\text{sset}}(z \mid 0 <_{\text{int}} z))$
Assert $\neg (\tau \models ((\text{Set}() \text{null}) \rightarrow \text{exists}_{\text{sset}}(z \mid z <_{\text{int}} 0)))$
Assert $\neg (\tau \models ((\text{Set}() \text{null}) \rightarrow \text{forall}_{\text{sset}}(z \mid z <_{\text{int}} 0)))$
Assert $\neg (\tau \models ((\text{Set}() \text{null}) \rightarrow \text{exists}_{\text{sset}}(z \mid z <_{\text{int}} 0)))$
Assert $\tau \models ((\text{Set}() \text{null}) \rightarrow \text{forall}_{\text{sset}}(z \mid 0 <_{\text{int}} z))$
Assert $\tau \models ((\text{Set}() \text{null}) \rightarrow \text{exists}_{\text{sset}}(z \mid 0 <_{\text{int}} z))$

Assert $\neg (\tau \models (\text{Set}() \text{null}::a \text{ Boolean} \models \text{Set}()))$
Assert $\neg (\tau \models (\text{Set}() \text{null}::a \text{ Integer} \models \text{Set}()))$

Assert $\neg (\tau \models (\text{Set}() \text{true} \models \text{Set}() \text{false}))$
Assert $\neg (\tau \models (\text{Set}() \text{true} \text{true} \models \text{Set}() \text{false}))$
Assert $\neg (\tau \models (\text{Set}() \text{false} \models \text{Set}()))$
Assert $\tau \models (\text{Set}() \text{true} \models \text{Set}())$
Assert $\tau \models (\text{Set}() \text{false} \models \text{Set}())$
Assert $\tau \models (\text{Set}() \text{false} \models \text{Set}())$
Assert $\tau \models (\text{Set}() \text{false} \models \text{Set}())$
Assert $\tau \models (\text{Set}() \text{false} \models \text{Set}())$

lemma const (\text{Set}() \text{null}, \text{invalid}) (proof)

Elementary computations on Sequences.

Assert $\neg (\tau \models v(\text{invalid}:(\forall,\alpha::\text{null}) \text{Sequence}))$
Assert $\tau \models v(\text{null}:(\forall,\alpha::\text{null}) \text{Sequence})$
Assert $\neg (\tau \models \delta(\text{null}:(\forall,\alpha::\text{null}) \text{Sequence}))$
Assert $\tau \models v(\text{Sequence}())$

lemma const (\text{Sequence}() \text{null}, \text{invalid}) (proof)

end
3. Formalization III: UML/OCL constructs: State Operations and Objects

theory UML-State
imports UML-Library
begin

no-notation None (⊥)

3.1. Introduction: States over Typed Object Universes

In the following, we will refine the concepts of a user-defined data-model (implied by a class-diagram) as well as the notion of state used in the previous section to much more detail. Surprisingly, even without a concrete notion of objects and a universe of object representation, the generic infrastructure of state-related operations is fairly rich.

3.1.1. Fundamental Properties on Objects: Core Referential Equality

Definition

Generic referential equality - to be used for instantiations with concrete object types ...

definition StrictRefEqObject :: (∀.a::{object,null})val ⇒ (∀.a)val ⇒ (∀)Boolean
where StrictRefEqObject x y
  ≡ λ τ. if (υ x) τ = true τ ∧ (υ y) τ = true τ
      then if x τ = null ∨ y τ = null
          then (oid-of (x τ)) = (oid-of (y τ)) ⊥
          else invalid τ
      else invalid τ

Strictness and context passing

lemma StrictRefEqObject-strict1[simp,code-unfold] : (StrictRefEqObject x invalid) = invalid ⟨proof⟩
lemma StrictRefEqObject-strict2[simp,code-unfold] : (StrictRefEqObject invalid x) = invalid ⟨proof⟩

lemma cp-StrictRefEqObject:
  (StrictRefEqObject x y τ) = (StrictRefEqObject (λ- x τ) (λ- y τ)) τ
⟨proof⟩lemmas cp0-StrictRefEqObject = cp-StrictRefEqObject[THEN allI[THEN allI[THEN allI[THEN cpI2]],
  of StrictRefEqObject]
lemmas cp-intro"[intro!,simp,code-unfold] =
  cp-intro" cp-StrictRefEqObject[TTHEN allI[TTHEN allI[TTHEN allI[TTHEN cpI2]],
  of StrictRefEqObject]"
3.1.2. Logic and Algebraic Layer on Object

Validity and Definedness Properties

We derive the usual laws on definedness for (generic) object equality:

**lemma** StrictRefEqObject-defargs:
\[ \tau \models (\text{StrictRefEq}_\text{Object} \ x \ y) \iff (\tau \models (v \ x)) \land (\tau \models (v \ y)) \]

**lemma** defined-StrictRefEqObject-I:
Assumes \( v \models x \)
Assumes \( v \models y \)
Shows \( \tau \models \text{StrictRefEq}_\text{Object} \ x \ y \)

**lemma** StrictRefEqObject-def-homo:
\[ \delta(\text{StrictRefEq}_\text{Object} \ x \ y) = (v \ x) \land (v \ y) \]

**Symmetry**

**lemma** StrictRefEqObject-sym :
Assumes \( x \models v \)
Shows \( \tau \models \text{StrictRefEq}_\text{Object} \ x \ x \)

**Behavior vs StrongEq**

It remains to clarify the role of the state invariant \( \text{inv}_\sigma(\sigma) \) mentioned above that states the condition that there is a “one-to-one” correspondence between object representations and oid’s: \( \forall \text{oid} \in \text{dom} \sigma. \text{oid} = \text{OidOf} \lceil \sigma(\text{oid}) \rceil \). This condition is also mentioned in [32, Annex A] and goes back to Richters [33]; however, we state this condition as an invariant on states rather than a global axiom. It can, therefore, not be taken for granted that an oid makes sense both in pre- and post-states of OCL expressions.

We capture this invariant in the predicate WFF :

**definition** WFF :: \( \forall \text{object} \models \text{bool} \)
Where
\[ \text{WFF} \ \tau = (\forall x \in \text{ran} \text{heap}(\text{fst} \ \tau). \ \text{heap}(\text{fst} \ \tau) (\text{oid-of} x) = x) \land \]
\[ (\forall x \in \text{ran} \text{heap}(\text{snd} \ \tau). \ \text{heap}(\text{snd} \ \tau) (\text{oid-of} x) = x) \]

It turns out that WFF is a key-concept for linking strict referential equality to logical equality: in well-formed states (i.e. those states where the self (oid-of) field contains the pointer to which the object is associated to in the state), referential equality coincides with logical equality.

We turn now to the generic definition of referential equality on objects: Equality on objects in a state is reduced to equality on the references to these objects. As in HOL-OCL [6, 8], we will store the reference of an object inside the object in a (ghost) field. By establishing certain invariants (“consistent state”), it can be assured that there is a “one-to-one-correspondence” of objects to their references—and therefore the definition below behaves as we expect.

Generic Referential Equality enjoys the usual properties: (quasi) reflexivity, symmetry, transitivity, substitutivity for defined values. For type-technical reasons, for each concrete object type, the equality \( \models \) is defined by generic referential equality.

**theorem** StrictRefEqObject-vs-StrongEq:
Assumes WFF, WFF \( \tau \)
And \( v \models x \)
And \( v \models y \)
And \( x \text{-present-pre: } x \in \text{ran} \text{heap(fst} \ \tau) \)
And \( y \text{-present-pre: } y \in \text{ran} \text{heap(fst} \ \tau) \)
and \( x\text{-present-post} \): \( x \in \text{ran} \ (\text{heap} (\text{snd} \ \tau)) \)
and \( y\text{-present-post} \): \( y \in \text{ran} \ (\text{heap} (\text{snd} \ \tau)) \)

shows \( (\tau \models (\text{StrictRefEq}_{\text{Object}} \ x \ y)) \Rightarrow (\tau \models (x \approx y)) \)

(proof)

**theorem** StrictRefEq\_{Object}-vs-StrongEq:

assumes \( \text{WFF} : \text{WFF} \ \tau \)
and \( \text{valid-x} \): \( \tau \models (u \ (x : (A::\text{object},'a::\{\text{null},\text{object}\})\text{val})) \)
and \( \text{valid-y} \): \( \tau \models (v \ y) \)
and \( \text{oid-preserve} \): \( \forall x \in \text{ran} \ (\text{heap} (\text{fst} \ \tau)) \lor x \in \text{ran} \ (\text{heap} (\text{snd} \ \tau)) \Rightarrow \)
\( H \ x \neq \bot \Rightarrow \text{oid-of} \ (H \ x) = \text{oid-of} \ x \)
and \( \text{xy-together} \): \( x \ \tau \in H \ \tau \text{ ran} \ (\text{heap} (\text{fst} \ \tau)) \land y \ \tau \in H \ \tau \text{ ran} \ (\text{heap} (\text{fst} \ \tau)) \lor \)
\( x \ \tau \in H \ \tau \text{ ran} \ (\text{heap} (\text{snd} \ \tau)) \land y \ \tau \in H \ \tau \text{ ran} \ (\text{heap} (\text{snd} \ \tau)) \)

shows \( (\tau \models (\text{StrictRefEq}_{\text{Object}} \ x \ y)) \Rightarrow (\tau \models (x \approx y)) \)

(proof)

So, if two object descriptions live in the same state (both pre or post), the referential equality on objects implies in a WFF state the logical equality.

### 3.2. Operations on Object

#### 3.2.1. Initial States (for testing and code generation)

**definition** \( \tau_0 :: (A)\text{st} \)

where \( \tau_0 \equiv ([\text{heap}=\text{Map}.\text{empty}, \text{assocs} = \text{Map}.\text{empty}],\)
\( ([\text{heap}=\text{Map}.\text{empty}, \text{assocs} = \text{Map}.\text{empty}]) \)

#### 3.2.2. OclAllInstances

To denote OCL types occurring in OCL expressions syntactically—as, for example, as “argument” of \( \text{oclAllInstances}() \)—we use the inverses of the injection functions into the object universes; we show that this is a sufficient “characterization.”

**definition** \( \text{OclAllInstances-generic} :: ((A::\text{object}) \text{ st} \Rightarrow A \text{ state}) \Rightarrow (A::\text{object} \rightarrow 'a) \Rightarrow \)
\( (A, 'a \text{ option option}) \text{ Set} \)

where \( \text{OclAllInstances-generic fst-snd} \ H = \)
\( (\lambda \tau. \text{Abs}\_\text{Set}\_\text{base} \_\text{null} \_\text{Some} \_\text{H} \_\text{ran} \ (\text{heap} (\text{fst-snd} \ \tau))) - \{ \text{None} \} \_\text{\_\_} \)

**lemma** OclAllInstances-generic-defined: \( \tau \models \delta \ (\text{OclAllInstances-generic pre-post} \ H) \)

(proof)

**lemma** OclAllInstances-generic-init-empty:

assumes \( \text{[simp]}: \forall x. \text{ pre-post} (x, x) = x \)

shows \( \tau_0 \models \text{OclAllInstances-generic pre-post} H \equiv \text{Set} \{\} \)

(proof)

**lemma** represented-generic-objects-null:

assumes \( A: \tau \models (\text{OclAllInstances-generic pre-post} (H::(A::\text{object} \rightarrow 'a))) \rightarrow \text{includes}_{\text{st}}(x) \)

shows \( \tau \models \text{not}(x \approx \text{null}) \)

(proof)

**lemma** represented-generic-objects-defined:

assumes \( A: \tau \models (\text{OclAllInstances-generic pre-post} (H::(A::\text{object} \rightarrow 'a))) \rightarrow \text{includes}_{\text{st}}(x) \)

shows \( \tau \models \delta \ (\text{OclAllInstances-generic pre-post} H) \land \tau \models \delta \ x \)

127
One way to establish the actual presence of an object representation in a state is:

**definition** is-represented-in-state \( \text{fst-snd } x H \tau = (x \tau \in (\text{Some } o H) \setminus \text{ran} (\text{heap} (\text{fst-snd } \tau))) \)

**lemma** represented-generic-objects-in-state:
**assumes** \( A : \tau \models \text{(OclAllInstances-generic pre-post } H \setminus \text{includes}_{S,\tau}(x) \)  
**shows** is-represented-in-state \( \text{pre-post } x H \tau \)

**proof**

Here comes a couple of operational rules that allow to infer the value of \( \text{oclAllInstances} \) from the context \( \tau \). These rules are a special-case in the sense that they are the only rules that relate statements with different \( \tau \)'s. For that reason, new concepts like “constant contexts P” are necessary (for which we do not elaborate an own theory for reasons of space limitations; in examples, we will prove resulting constraints straight forward by hand).

**lemma** state-update-vs-allInstances-generic-empty:
**assumes** [simp]: \( \forall a. \text{pre-post} (mk a) = a \)
**shows** \( (mk (\llheap=\text{Map.empty}, \text{assocs}=A)) \models \text{OclAllInstances-generic pre-post } Type \models \text{Set}\{\} \)

**proof**

**lemma** state-update-vs-allInstances-generic-including:
**assumes** [simp]: \( \forall a. \text{pre-post} (mk a) = a \)
**assumes** \( \forall x. \sigma' \text{ oid} = \text{Some } x \Rightarrow x = \text{Object} \)  
**and** Type Object \( \neq \text{None} \)
**shows** \( (\text{OclAllInstances-generic pre-post } Type) \)  
\( (mk (\llheap=\sigma'(\text{oid}\rightarrow \text{Object}), \text{assocs}=A)) \)  
\( = \)  
\( ((\text{OclAllInstances-generic pre-post } Type) \setminus \text{includes}_{S,\tau}(\lambda \ldots. \text{drop } (\text{Type Object}) _\perp)) \)  
\( (mk (\llheap=\sigma', \text{assocs}=A)) \)

**proof**

**lemma** state-update-vs-allInstances-generic-including:
**assumes** [simp]: \( \forall a. \text{pre-post} (mk a) = a \)
**assumes** \( \forall x. \sigma' \text{ oid} = \text{Some } x \Rightarrow x = \text{Object} \)  
**and** Type Object \( \neq \text{None} \)
**shows** \( (\text{OclAllInstances-generic pre-post } Type) \)  
\( (mk (\llheap=\sigma'(\text{oid}\rightarrow \text{Object}), \text{assocs}=A)) \)  
\( = \)  
\( ((\lambda \ldots. (\text{OclAllInstances-generic pre-post } Type) \setminus \text{includes}_{S,\tau}(\lambda \ldots. \text{drop } (\text{Type Object}) _\perp)) \)  
\( (mk (\llheap=\sigma', \text{assocs}=A)) \)

**proof**

**lemma** state-update-vs-allInstances-generic-noincluding:
**assumes** [simp]: \( \forall a. \text{pre-post} (mk a) = a \)
**assumes** \( \forall x. \sigma' \text{ oid} = \text{Some } x \Rightarrow x = \text{Object} \)  
**and** Type Object \( = \text{None} \)
**shows** \( (\text{OclAllInstances-generic pre-post } Type) \)  
\( (mk (\llheap=\sigma'(\text{oid}\rightarrow \text{Object}), \text{assocs}=A)) \)  
\( = \)  
\( ((\text{OclAllInstances-generic pre-post } Type) \setminus \text{includes}_{S,\tau}(\lambda \ldots. \text{drop } (\text{Type Object}) _\perp)) \)  
\( (mk (\llheap=\sigma', \text{assocs}=A)) \)

**proof**

128
One way to establish the actual presence of an object representation in a state is:

lemma state-update-vs-allInstances-at-post-empty:
  assumes $A: \tau \models \text{H.allInstances}() \rightarrow \text{includes}_{\text{Set}}(x)$
  shows $\text{is-represented-in-state} (\text{snd} z \text{H})$  \(\tau\)
  \(\text{proof}\)

lemma state-update-vs-allInstances-at-post-defined:
  assumes $A: \tau \models ((\text{H}::(\forall x: \text{object} \rightarrow 'a).\text{allInstances()} \rightarrow \text{includes}_{\text{Set}}(x))$
  shows $\tau \models \delta (\text{H}.\text{allInstances()} \land \tau \models \delta x)$
  \(\text{proof}\)
(proof)

Here comes a couple of operational rules that allow to infer the value of oclAllInstances from the context τ. These rules are a special-case in the sense that they are the only rules that relate statements with different τ’s. For that reason, new concepts like “constant contexts P” are necessary (for which we do not elaborate an own theory for reasons of space limitations; in examples, we will prove resulting constraints straight forward by hand).

lemma state-update-vs-allInstances-at-post-including’:
assumes \( \forall x. \sigma’ \text{ oid} = \text{Some } x \implies x = \text{Object} \)
and Type Object \( \neq \) None
shows (Type .allInstances())
\( (\sigma, \{\text{heap}=\sigma’(\text{oid} \to \text{Object}), \text{assocs}=A\}) \)
\( = \)
\( ((\lambda-. (Type .allInstances())) \implies \text{including}_{S \setminus \{\lambda \}} \text{drop} (\text{Type Object}) \_\omega)) \)
\( (\sigma, \{\text{heap}=\sigma’, \text{assocs}=A\}) \)
(proof)

lemma state-update-vs-allInstances-at-post-noincluding’:
assumes \( \forall x. \sigma’ \text{ oid} = \text{Some } x \implies x = \text{Object} \)
and Type Object = None
shows (Type .allInstances())
\( (\sigma, \{\text{heap}=\sigma’(\text{oid} \to \text{Object}), \text{assocs}=A\}) \)
\( = \)
\( ( Type .allInstances()) \)
\( (\sigma, \{\text{heap}=\sigma’, \text{assocs}=A\}) \)
(proof)

theorem state-update-vs-allInstances-at-post-ntc:
assumes oid-def: \( \text{oid} \notin \text{dom} \sigma’ \)
and non-type-conform: Type Object = None
and cp-ctxt: \( cp \ P \)
and const-ctxt: \( \forall X. \text{const } X \implies \text{const } (P X) \)
shows (\( (\sigma, \{\text{heap}=\sigma’(\text{oid} \to \text{Object}), \text{assocs}=A\}) \models (P(\text{Type .allInstances()}))) \)
\( = \)
\( (\sigma, \{\text{heap}=\sigma’, \text{assocs}=A\}) \models (P(\text{Type .allInstances()}))) \)
(proof)

theorem state-update-vs-allInstances-at-post-tc:
assumes oid-def: \( \text{oid} \notin \text{dom} \sigma’ \)
and type-conform: Type Object \( \neq \) None
and cp-ctxt: \( cp \ P \)
and const-ctxt: \( \forall X. \text{const } X \implies \text{const } (P X) \)
shows (\( (\sigma, \{\text{heap}=\sigma’(\text{oid} \to \text{Object}), \text{assocs}=A\}) \models (P(\text{Type .allInstances()}))) \)
\( = \)
\( (\sigma, \{\text{heap}=\sigma’, \text{assocs}=A\}) \models (P(\text{Type .allInstances()})) \)

130
OclAllInstances (@pre)

**definition** OclAllInstances-at-pre :: ('α :: object -> 'a) => (forall _'a_. 'a option option) Set
(- .allInstances@pre'(_'))

**where** OclAllInstances-at-pre = OclAllInstances-generic fst

**lemma** OclAllInstances-at-pre-defined: \( \tau \models \delta \ (H .allInstances@pre()) \)

**lemma** \( \tau_0 \models H .allInstances@pre() \Rightarrow Set() \)

**lemma** represented-at-pre-objects-nonnull:
assumes \( A \): \( \tau \models H .allInstances@pre() \Rightarrow \text{includes}_{Set}(x) \)
shows \( \tau \models \not(x \equiv \text{null}) \)

**lemma** represented-at-pre-objects-defined:
assumes \( A \): \( \tau \models H .allInstances@pre() \Rightarrow \text{includes}_{Set}(x) \)
shows \( \tau \models \delta \ (H .allInstances@pre()) \wedge \tau \models \delta \ x \)

One way to establish the actual presence of an object representation in a state is:

**lemma**
assumes \( A \): \( \tau \models H .allInstances@pre() \Rightarrow \text{includes}_{Set}(x) \)
shows \( \text{is-represented-in-state} \ \text{fst} \ x \ \tau \)

**lemma** state-update-vs-allInstances-at-pre-empty:
shows \( ((| heap = \text{Map.empty}, \text{assocs} = A |), \sigma) \models Type .allInstances@pre() \Rightarrow Set() \)

Here comes a couple of operational rules that allow to infer the value of \( \text{oclAllInstances@pre} \) from the context \( \tau \). These rules are a special-case in the sense that they are the only rules that relate statements with different \( \tau \)'s. For that reason, new concepts like “constant contexts \( P \)” are necessary (for which we do not elaborate an own theory for reasons of space limitations; in examples, we will prove resulting constraints straight forward by hand).

**lemma** state-update-vs-allInstances-at-pre-including:
assumes \( A \): \( \forall x. \sigma ' \text{oid} = \text{Some} \ x \Rightarrow x = \text{Object} \)
and \( Type \text{ Object} \neq \text{None} \)
shows \( (\text{Type}.allInstances@pre()) \Rightarrow \text{includes}_{Set}(\lambda x. \Rightarrow (Type \text{ Object} \Rightarrow)) \)

**lemma** state-update-vs-allInstances-at-pre-including':
assumes \( A \): \( \forall x. \sigma ' \text{oid} = \text{Some} \ x \Rightarrow x = \text{Object} \)
and \( Type \text{ Object} \neq \text{None} \)
shows \( (\text{Type}.allInstances@pre()) \Rightarrow \text{includes}_{Set}(\lambda x. \Rightarrow (Type \text{ Object} \Rightarrow)) \)
\((\text{heap}=\sigma'(\text{oid} \to \text{Object}), \text{assocs}=A], \sigma)\)  
\(=\)  
\((\lambda x. (\text{Type}. \text{allInstances}@\text{pre}()))  
\((\text{heap}=\sigma', \text{assocs}=A], \sigma)) \overset{\text{includings}_{\text{set}}}{\Rightarrow} \lambda \text{oid} \cdot \text{drop}(\text{Type Object})\)\)  
\((\text{heap}=\sigma'(\text{oid} \to \text{Object}), \text{assocs}=A], \sigma)\)

\(\langle \text{proof} \rangle\)

**lemma** state-update-vs-allInstances-at-pre-noincluding':
**assumes** \(\forall x. \sigma' \text{ oid} = \text{Some } x \implies x = \text{ Object}\)  
and Type Object = None  
**shows** \((\text{Type}. \text{allInstances}@\text{pre}())\)  
\((\text{heap}=\sigma'(\text{oid} \to \text{Object}), \text{assocs}=A], \sigma)\)  
\(=\)  
\((\text{Type}. \text{allInstances}@\text{pre}())\)  
\((\text{heap}=\sigma', \text{assocs}=A], \sigma)\)

\(\langle \text{proof} \rangle\)

**theorem** state-update-vs-allInstances-at-pre-ntc:
**assumes** oid-def: \(\text{oid} \notin \text{dom } \sigma'\)  
and non-type-conform: Type Object = None  
and cp-ctxt: \(\text{cp P}\)  
and const-ctxt: \(\forall X. \text{const } X \implies \text{const } (P X)\)  
**shows** \((\text{heap}=\sigma'(\text{oid} \to \text{Object}), \text{assocs}=A], \sigma)\)  
\(\models (P(\text{Type}. \text{allInstances}@\text{pre}())))\)  
\((\text{heap}=\sigma', \text{assocs}=A], \sigma)\)  
\(\models (P(\text{Type}. \text{allInstances}@\text{pre}())))\)

\(\langle \text{proof} \rangle\)

**theorem** state-update-vs-allInstances-at-pre-tc:
**assumes** oid-def: \(\text{oid} \notin \text{dom } \sigma'\)  
and type-conform: Type Object \(\neq\) None  
and cp-ctxt: \(\text{cp P}\)  
and const-ctxt: \(\forall X. \text{const } X \implies \text{const } (P X)\)  
**shows** \((\text{heap}=\sigma'(\text{oid} \to \text{Object}), \text{assocs}=A], \sigma)\)  
\(\models (P(\text{Type}. \text{allInstances}@\text{pre}())))\)  
\((\text{heap}=\sigma', \text{assocs}=A], \sigma)\)  
\(\models (P(\text{Type}. \text{allInstances}@\text{pre}())))\)

\(\rightarrow\text{includings}_{\text{set}}(\lambda \cdot , (\text{Type Object})))\)

\(\langle \text{proof} \rangle\)

\(\@\text{post or @pre}\)

**theorem** StrictRefEqObject-vs-StrongEq'':
**assumes** WFF: WFF \(\tau\)  
and valid-x: \(\tau \models (\forall x : (\forall \alpha::\text{object}, \alpha::\text{object} \text{ option} \text{ option})\text{val}))\)  
and valid-y: \(\tau \models (\forall y)\)  
and oid-preserve: \(\forall x. x \in \text{ran}(\text{heap}(\text{fst } \tau)) \vee x \in \text{ran}(\text{heap}(\text{snd } \tau)) \implies \text{oid-of}(H x) = \text{oid-of } x\)  
and xy-together: \(\tau \models ((H \text{ allInstances}() \rightarrow \text{includes}_{\text{set}}(x)) \text{ and } H \text{ allInstances}() \rightarrow \text{includes}_{\text{set}}(y))\)  
\text{ or } \((H \text{ allInstances}@\text{pre}() \rightarrow \text{includes}_{\text{set}}(x)) \text{ and } H \text{ allInstances}@\text{pre}() \rightarrow \text{includes}_{\text{set}}(y))\)

**shows** \((\tau \models (\text{StrictRefEqObject } x y) = (\tau \models (x \triangleq y)))\)

\(\langle \text{proof} \rangle\)

### 3.2.3. OclIsNew, OclIsDeleted, OclIsMaintained, OclIsAbsent

**definition** OclIsNew:: \((\forall x::\text{null}, \text{object})\text{val} = (\forall x::\text{Boolean}) (\lambda x. \text{oclsNew'}(x))\)

**where** X .oclIsNew() \(\equiv (\lambda x. \text{if } (\delta X) \tau = \text{true } \tau\)  
then \(\text{oid-of } (X \tau) \notin \text{dom}(\text{heap}(\text{fst } \tau)) \land \text{oid-of } (X \tau) \in \text{dom}(\text{heap}(\text{snd } \tau))\)\)
The following predicates — which are not part of the OCL standard descriptions — complete the goal of oclIsNew by describing where an object belongs.

definition OclIsDeleted:: (A, 'a::null.object)val ⇒ A Boolean (¬.oclIsDeleted(′))
where X .oclIsDeleted() ≡ (X .oclIsNew()) \True \Rightarrow X
then oid-of (X τ) ∈ dom(heap(fst τ)) \land
oid-of (X τ) \notin dom(heap(snd τ))_∪
else invalid τ

definition OclIsMaintained:: (A, 'a::null.object)val ⇒ A Boolean (¬.oclIsMaintained(′))
where X .oclIsMaintained() ≡ (X .oclIsNew()) \True \Rightarrow X
then oid-of (X τ) ∈ dom(heap(fst τ)) \land
oid-of (X τ) \notin dom(heap(snd τ))_∪
else invalid τ

definition OclIsAbsent:: (A, 'a::null.object)val ⇒ A Boolean (¬.oclIsAbsent(′))
where X .oclIsAbsent() ≡ (X .oclIsNew()) \True \Rightarrow X
then oid-of (X τ) \notin dom(heap(fst τ)) \land
oid-of (X τ) \notin dom(heap(snd τ))_∪
else invalid τ

{lemma} state-split : τ \True \Rightarrow \delta X \True
τ \True \Rightarrow (X .oclIsNew()) \lor τ \True \Rightarrow (X .oclIsDeleted()) \lor
τ \True \Rightarrow (X .oclIsMaintained()) \lor τ \True \Rightarrow (X .oclIsAbsent())
{proof}

{lemma} notNew-vs-others : τ \True \Rightarrow \delta X \True
(¬ τ \True \Rightarrow (X .oclIsNew())) = (τ \True \Rightarrow (X .oclIsDeleted()) \lor
τ \True \Rightarrow (X .oclIsMaintained()) \lor τ \True \Rightarrow (X .oclIsAbsent())
{proof}

3.2.4. OclIsModifiedOnly

Definition

The following predicate—which is not part of the OCL standard—provides a simple, but powerful means to describe framing conditions. For any formal approach, be it animation of OCL contracts, test-case generation or die-hard theorem proving, the specification of the part of a system transition that does not change is of primordial importance. The following operator establishes the equality between old and new objects in the state (provided that they exist in both states), with the exception of those objects.

{definition} OclIsModifiedOnly::(A::object, 'a::null.object)Set ⇒ A Boolean (¬.oclIsModifiedOnly(′))
where X-->oclIsModifiedOnly() ≡ (λ(σ,σ′). let X′ = oid-of X Rep-Set_{base} X σ σ; S = (dom (heap σ) \cap dom (heap σ′)) \setminus X′
in if (δ X) (σ,σ′) = true (σ,σ′) \land (∀x∈Rep-Set_{base} X σ σ′, x \neq null)
then ∀x ∈ S, (heap σ) x = (heap σ′) x_∪
else invalid (σ,σ′))

{Execution with Invalid or Null or Null Element as Argument}

{lemma} invalid-->oclIsModifiedOnly() = invalid
{proof}

{lemma} null-->oclIsModifiedOnly() = invalid
{proof}
lemma
assumes $X$-null : $\tau \models X \rightarrow \text{includes}_{Sels}(\text{null})$
shows $\tau \models X \rightarrow \text{oclIsModifiedOnly}() \equiv \text{invalid}$
(proof)

Context Passing

lemma $cp$-$\text{oclIsModifiedOnly}$ : $X \rightarrow \text{oclIsModifiedOnly}() \tau = (\lambda X. X \tau) \rightarrow \text{oclIsModifiedOnly}() \tau$
(proof)

3.2.5. OclSelf

The following predicate—which is not part of the OCL standard—explicitly retrieves in the pre or post state the original OCL expression given as argument.

definition $\text{simp}$: $\text{OclSelf} x H \text{fst-snd} = (\lambda \tau. \text{if } \delta x \tau = \text{true } \tau \\
\text{then } H \{\text{heap}(\text{fst } \tau) \land \text{oid-of } (x \tau) \in \text{dom}(\text{heap } (\text{snd } \tau)) \\
\text{then } H \{\text{oid-of } (x \tau)\} \land \text{all-oid-diff} \}
\text{else } \text{invalid } \tau$ \\
\text{else } \text{invalid } \tau

definition $\text{OclSelf-at-pre}$ : $\{\forall a::\text{null-object}\} \models H x \Rightarrow (\{a::null\} \text{val } \Rightarrow (\{a::null\} \text{val } ((-\text{pre} (-))$

where $x \models \text{pre } H = \text{OclSelf } x H \text{ fst}$

definition $\text{OclSelf-at-post}$ : $\{\forall a::\text{null-object}\} \models H x \Rightarrow (\{a::null\} \text{val } \Rightarrow (\{a::null\} \text{val } ((-\text{post} (-))$

where $x \models \text{post } H = \text{OclSelf } x H \text{ snd}$

3.2.6. Framing Theorem

lemma all-oid-diff:
assumes def-x : $\tau \models \delta x$
assumes def-x' : $\forall x. x \in \text{Rep-Set}_{\text{base }} (X \tau) \Rightarrow x \neq \text{null}$

defines $P \equiv (\lambda a. \text{not } (\text{StrictRefEqObject } x a))$
shows $\models (X \rightarrow \forall x \in \text{Rep-Set}_{\text{base }} (X \tau)) (\{\text{oid-of } (x \tau) \notin \text{oid-of } ^{\text{Rep-Set}_{\text{base }} (X \tau)}\})$
(proof)

theorem framing:
assumes modifiesclause: $\tau \models (X \rightarrow \text{excluding}_{Sels}(x)) \rightarrow \text{oclIsModifiedOnly}()$
and oid-is-type-repr : $\tau \models X \rightarrow \text{forAll}_{Sels}(a) \text{ not } (\text{StrictRefEqObject } x a)$
shows $\tau \models (x \models \text{pre } P \Rightarrow (x \models \text{post } P))$
(proof)

As corollary, the framing property can be expressed with only the strong equality as comparison operator.

theorem framing':
assumes uff : $WFF \tau$
assumes modifiesclause: $\tau \models (X \rightarrow \text{excluding}_{Sels}(x)) \rightarrow \text{oclIsModifiedOnly}()$
and oid-is-type-repr : $\tau \models X \rightarrow \text{forAll}_{Sels}(a) \text{ not } (x \overset{\delta}{=} a)$
and oid-preserv: $\forall x. x \in \text{ran } (\text{heap}(\text{fst } \tau)) \lor x \in \text{ran } (\text{heap}(\text{snd } \tau)) \Rightarrow \text{oid-of } (H x) = \text{oid-of } x$
and xy-together:
\[ \tau \models X \rightarrow \text{forAll}_{\text{set}}(y \mid (H \cdot \text{allInstances}() \rightarrow \text{includes}_{\text{set}}(x) \text{ and } H \cdot \text{allInstances}() \rightarrow \text{includes}_{\text{set}}(y)) \text{ or } (H \cdot \text{allInstances}@\text{pre}() \rightarrow \text{includes}_{\text{set}}(x) \text{ and } H \cdot \text{allInstances}@\text{pre}() \rightarrow \text{includes}_{\text{set}}(y))) \]
\[ \text{shows } \tau \models (x \circ \text{pre } P \triangleq (x \circ \text{post } P)) \]

### 3.2.7. Miscellaneous

**Lemma 3.2.7.1.** `pre-post-new`: \[ \tau \models (x \cdot \text{oclIsNew}) \Rightarrow \neg (\tau \models v(x \circ \text{pre } H1)) \land \neg (\tau \models v(x \circ \text{post } H2)) \]

**Proof:**

\[ \tau \models (x \cdot \text{oclIsDeleted}) \Rightarrow \neg (\tau \models v(x \circ \text{pre } H1)) \land \neg (\tau \models v(x \circ \text{post } H2)) \]

**Lemma 3.2.7.2.** `pre-post-absent`: \[ \tau \models (x \cdot \text{oclIsAbsent}) \Rightarrow \neg (\tau \models v(x \circ \text{pre } H1)) \land \neg (\tau \models v(x \circ \text{post } H2)) \]

**Proof:**

\[ \tau \models (x \cdot \text{oclIsMaintained}) \Rightarrow \tau \models (x \cdot \text{oclIsMaintained})' \]

\[ \tau \models (x \cdot \text{oclIsMaintained}) \Rightarrow (\tau \models v(x \circ \text{pre } (\text{Some } o H1)) \land \tau \models v(x \circ \text{post } (\text{Some } o H2))) \]

**Proof:**

\[ \tau \models (x \cdot \text{oclIsMaintained})' \]

**Lemma 3.2.7.3.** `framing-same-state`: \[ (\sigma, \sigma) \models (x \circ \text{pre } H \triangleq (x \circ \text{post } H)) \]

**Proof:**

### 3.3. Accessors on Object

#### 3.3.1. Definition

**Definition** `select-object mt incl smash deref l = smash (foldl incl mt (map deref l))`

The continuation \( f \) is usually instantiated with a smashing function which is either the identity \( id \) or, for \( 0..1 \) cardinalities of associations, the \( \text{UML-Sequence.OclANY} \)-selector which also handles the \( null \)-cases appropriately. A standard use-case for this combinator is for example:

**Term** `(select-object mtSet \text{UML-Set.OclIncluding} \text{UML-Set.OclANY} f l oid):(\forall a \cdot \:'=\text{:null})val`

**Definition** `select-object_{\text{set}} = select-object mtSet \text{UML-Set.OclIncluding} id`

**Definition** `select-object_{\text{any0}} f s-set = \text{UML-Set.OclANY} (select-object_{\text{set}} f s-set)`

**Definition** `select-object_{\text{any}} f s-set = (let s = select-object_{\text{set}} f s-set in if s->\text{size}_{\text{set}}() \triangleq 1 then s->\text{any}_{\text{set}}() else )`

**Definition** `select-object_{\text{seq}} = select-object \text{UML-Sequence.OclIncluding} id`

**Definition** `select-object_{\text{anyseq}} f s-set = \text{UML-Sequence.OclANY} (select-object_{\text{seq}} f s-set)`

**Definition** `select-object_{\text{pair}} f1 f2 = (\lambda(a,b) OclPair (f1 a) (f2 b))`

### 3.3.2. Validity and Definedness Properties

**Lemma** `select-fold-excesq`:

**Assumes** `list-all (\lambda f. (\tau \models v f)) l`

**Shows** \( \tau \models (\text{Rep-Sequence}_{\text{ass}} \text{fold} \text{UML-Sequence.OclIncluding} \text{Sequence}()) \models \text{List.map} (\lambda f. \tau f) l \)

**Proof**
lemma select-fold-exec\textsubscript{Set}:
  assumes list-all \((\lambda f. (\tau \models v f))\) l
  shows \(\text{Rep-Set}_{\text{Set}}(\text{fold UML-Set.oclIncluding} \text{ Set}\{\} \ l \ \tau) = \text{set (List.map (}\lambda f. \tau)\ l)\)
  \(\langle\text{proof}\rangle\)

lemma fold-val-elm\textsubscript{Seq}:
  assumes \(\tau \models v (\text{foldl UML-Sequence.oclIncluding} \text{ Sequence}\{\} (\text{List.map (} f p\) \text{ s-set}))\)
  shows list-all \((\lambda x. (\tau \models v (f \ p x)))\) s-set
  \(\langle\text{proof}\rangle\)

lemma fold-val-elm\textsubscript{Set}:
  assumes \(\tau \models v (\text{foldl UML-Set.oclIncluding} \text{ Set}\{\} (\text{List.map (} f p\) \text{ s-set}))\)
  shows list-all \((\lambda x. (\tau \models v (f \ p x)))\) s-set
  \(\langle\text{proof}\rangle\)

lemma select-object-any-defined\textsubscript{Seq}:
  assumes def-sel: \(\tau \models \delta (\text{select-object-any}_{\text{Seq}} f\ \text{s-set})\)
  shows s-set \(\neq []\)
  \(\langle\text{proof}\rangle\)

lemma
  assumes def-sel: \(\tau \models \delta (\text{select-object-any}_{\text{Set}} f\ \text{s-set})\)
  shows s-set \(\neq []\)
  \(\langle\text{proof}\rangle\)

lemma select-object-any-defined\textsubscript{Set}:
  assumes def-sel: \(\tau \models \delta (\text{select-object-any}_{\text{Set}} f\ \text{s-set})\)
  shows s-set \(\neq []\)
  \(\langle\text{proof}\rangle\)

lemma select-object-any-exec\textsubscript{Seq}:
  assumes def-sel: \(\tau \models \delta (\text{select-object-any}_{\text{Seq}} f\ \text{s-set})\)
  shows \(\exists e. \text{List.member} \text{s-set} e \land (\tau \models (\text{select-object-any}_{\text{Seq}} f\ \text{s-set} \equiv f e))\)
  \(\langle\text{proof}\rangle\)

lemma
  assumes def-sel: \(\tau \models \delta (\text{select-object-any}_{\text{Set}} f\ \text{s-set})\)
  shows \(\exists e. \text{List.member} \text{s-set} e \land (\tau \models (\text{select-object-any}_{\text{Set}} f\ \text{s-set} \equiv f e))\)
  \(\langle\text{proof}\rangle\)

lemma select-object-any-exec\textsubscript{Set}:
  assumes def-sel: \(\tau \models \delta (\text{select-object-any}_{\text{Set}} f\ \text{s-set})\)
  shows \(\exists e. \text{List.member} \text{s-set} e \land (\tau \models (\text{select-object-any}_{\text{Set}} f\ \text{s-set} \equiv f e))\)
  \(\langle\text{proof}\rangle\)

end
Modeling of an operation contract for an operation with 2 arguments, (so depending on three parameters if one takes "self" into account).

locale contract-scheme =  
  fixes f-dollar  
  fixes f-lam  
  fixes f :: (′A ′α0::null)val ⇒  
  (′b ′res::null)val  
  fixes PRE  
  fixes POST  

assumes def-scheme′: f self x ≡ (λ τ. SOME res. let res = λ - res in  
  if (τ |= (δ self)) ∧ f-dollar x τ  
  then (τ |= PRE self x) ∧  
  (τ |= POST self x res)  
  else τ |= res ≈ invalid)  

assumes all-post′: ∀ σ σ’ σ”. ((σ,σ’) |= PRE self x) = ((σ,σ”) |= PRE self x)  

assumes cp-pre′: PRE (self) x τ = PRE (λ -. self τ) (f-lam x τ)  

assumes cp-post′: POST (self) x (res) τ = POST (λ -. self τ) (f-lam x τ) (λ -. res τ)  

assumes f-dollar-val: ⋀ a1. f-dollar (f-lam a1 τ) τ = f-dollar a1 τ  

begin  

lemma strict0 [simp]: f invalid X = invalid  
(proof)  

lemma nullstrict0[simp]: f null X = invalid  
(proof)  

lemma cp0 : f self a1 τ = f (λ -. self τ) (f-lam a1 τ) τ  
(proof)  

theorem unfold′:  
  assumes context-ok: cp E  
  and args-def-or-valid: (τ |= δ self) ∧ f-dollar a1 τ  
  and pre-satisfied: τ |= PRE self a1  
  and post-satisfiable: ∃ res. (τ |= POST self a1 (λ -. res))  
  and sat-for-sols-post: (⋀ res. τ |= POST self a1 (λ -. res) ⇒ τ |= E (λ -. res))  
  shows τ |= E(f self a1)  
(proof)  

lemma unfold2′:  
  assumes context-ok: cp E  
  and args-def-or-valid: (τ |= δ self) ∧ (f-dollar a1 τ)  
  and pre-satisfied: τ |= PRE self a1  
  and postsplit-satisfied: τ |= POST’ self a1  
  and post-decomposable: ⋀ res. (POST self a1 res) =  
  ((POST’ self a1) and (res ≈ (BODY self a1)))  
  shows (τ |= E(f self a1)) = (τ |= E(BODY self a1))  
(proof)  

end

locale contract0 =  
  fixes f :: (′A ′α0::null)val ⇒  
  (′b ′res::null)val  
  fixes PRE  
  fixes POST
assumes def-scheme: \( f \ self \equiv (\lambda \tau. \text{SOME res}. \text{let res} = \lambda -. \text{res in}) \)
if \((\tau \models (\delta \ self))\)
then \((\tau \models \text{PRE self}) \land \(\tau \models \text{POST self res}\)\)
else \(\tau \models \text{res} \not\equiv \text{invalid}\)
assumes all-post: \(\forall \sigma \sigma' \sigma''. (\sigma,\sigma') \models \text{PRE self} = ((\sigma,\sigma'') \models \text{PRE self})\)
assumes cpp PRE: \(\text{PRE (self)} \ (a1) \ \tau = \text{PRE (\lambda -. \ self \ \tau)} \ (\lambda -. \ a1 \ \tau) \ \tau\)
assumes cpp POST: \(\text{POST (self)} \ (a1) \ (\text{res}) \ \tau = \text{POST (\lambda -. \ self \ \tau)(\lambda -. \ a1 \ \tau)} \ (\lambda -. \ \text{res} \ \tau) \ \tau\)

context contract0
begin
lemma cp-pre: \(\text{cp self'} \implies \text{cp (\lambda X. \text{PRE (self'} X)}\)
(proof)
lemma cp-post: \(\text{cp self'} \implies \text{cp res'} \implies \text{cp (\lambda X. \text{POST (self'} X)(\text{res'} X)})\)
(proof)
lemma cp simp: \(\text{cp self'} \implies \text{cp res'} \implies \text{cp (\lambda X. f (self'} X)}\)
(proof)
lemmas unfold = unfold'[simplified]

lemma unfold2 :
assumes \(\text{cp } E\)
and \((\tau \models \delta \ self)\)
and \(\tau \models \text{PRE self}\)
and \(\tau \models \text{POST' self}\)
and \(\land \text{res. (POST self res)} = ((\text{POST' self)} \ (\text{and (res} \not\equiv (\text{BODY self}))})\)
shows \((\tau \models E(f \ self)) = (\tau \models E(\text{BODY self}))\)
(proof)
end

locale contract1 =
fixes \(f :: (\Lambda',\alpha0::null)\)
val \(\Rightarrow\)
\(\quad (\Lambda',\alpha1::null)\) \(\Rightarrow\)
\(\quad (\Lambda',\text{res::null})\)
fixes \(\text{PRE}\)
fixes \(\text{POST}\)
assumes def-scheme: \(\text{f self a1} \equiv (\lambda \tau. \text{SOME res}. \text{let res = \lambda -. \res in}) \)
if \((\tau \models (\delta \ self)) \land \(\tau \equiv v \ a1)\)
then \((\tau \models \text{PRE self a1}) \land \)
\((\tau \models \text{POST self a1 res})\)
else \(\tau \models \text{res} \not\equiv \text{invalid}\)
assumes all-post: \(\forall \sigma \sigma' \sigma''. (\sigma,\sigma') \models \text{PRE self a1} = ((\sigma,\sigma'') \models \text{PRE self a1})\)
assumes cpp PRE: \(\text{PRE (self)} \ (a1) \ \tau = \text{PRE (\lambda -. \ self \ \tau)} \ (\lambda -. \ a1 \ \tau) \ \tau\)
assumes cpp POST: \(\text{POST (self)} \ (a1) \ (\text{res}) \ \tau = \text{POST (\lambda -. \ self \ \tau)(\lambda -. \ a1 \ \tau)} \ (\lambda -. \ \text{res} \ \tau) \ \tau\)

138
sublocale contract1 < contract-scheme λa1 τ. (τ ≝ v aI) λa1 τ. (λ . aI τ)
⟨proof⟩

context contract1
begin

lemma strict1[simp]: f self invalid = invalid
⟨proof⟩

lemma defined-mono : τ ≝ v(f Y Z) ⇒ (τ ≝ v Y) ∧ (τ ≝ v Z)
⟨proof⟩

lemma cp-pre: cp self’ ⇒ cp aI’ ⇒ cp (λX. PRE (self’ X) (aI’ X))
⟨proof⟩

lemma cp-post: cp self’ ⇒ cp aI’ ⇒ cp res’
⇒ cp (λX. POST (self’ X) (aI’ X) (res’ X))
⟨proof⟩

lemma [simp]: cp self’ ⇒ cp aI’ ⇒ cp res’ ⇒ cp (λX. f (self’ X) (aI’ X))
⟨proof⟩

lemmas unfold = unfold’
lemmas unfold2 = unfold2’

end

locale contract2 =
fixes f :: (‘a, ‘a :: null) val ⇒ (‘a, ‘a1 :: null) val ⇒ (‘a, ‘res :: null) val
fixes PRE
fixes POST
assumes def-scheme: f self a1 a2 ≡
(λ τ. SOME res. let res = λ . res in
if (τ ≝ (δ self)) ∧ (τ ≝ v a1) ∧ (τ ≝ v a2)
then (τ ≝ PRE self a1 a2) ∧
(τ ≝ POST self a1 a2 res)
else τ ≝ res ≝ invalid)
assumes all-post: ∀ σ σ’ σ”. ((σ,σ’) ≝ PRE self a1 a2) = ((σ,σ”) ≝ PRE self a1 a2)
assumes cpPRE: PRE (self) (a1) (a2) τ = PRE (λ . self τ) (λ . a1 τ) (λ . a2 τ) τ
assumes cpPOST: ∀ res. POST (self) (a1) (a2) (res) τ =
POST (λ . self τ)(λ . a1 τ)(λ . a2 τ) (λ . res τ) τ

sublocale contract2 < contract-scheme λ(a1,a2) τ. (τ ≝ v aI) ∧ (τ ≝ v a2)
λ(a1,a2) τ. (λ . aI τ) (λ . a2 τ)
(λ x (a,b). f x a b)
(λ x (a,b). PRE x a b)
(λ x (a,b). POST x a b)
⟨proof⟩

context contract2
begin

lemma strict0 [simp] : f invalid X Y = invalid
⟨proof⟩
lemma nullstrict0[simp]: f null X Y = invalid
(proof)

lemma strict1[simp]: f self invalid Y = invalid
(proof)

lemma strict2[simp]: f self X invalid = invalid
(proof)

lemma defined-mono : τ |= v(f X Y Z) ⇒ (τ |= δ X) ∧ (τ |= v Y) ∧ (τ |= v Z)
(proof)

lemma cp-pre: cp self' ⇒ cp a1' ⇒ cp a2' ⇒ cp (λX. PRE (self' X) (a1' X) (a2' X))
(proof)

lemma cp-post: cp self' ⇒ cp a1' ⇒ cp a2' ⇒ cp res'
⇒ cp (λX. POST (self' X) (a1' X) (a2' X) (res' X))
(proof)

lemma cp0': f self a1 a2 τ = f (λf. self τ) (λf. a1 τ) (λf. a2 τ) τ
(proof)

lemma cp[simp]: cp self' ⇒ cp a1' ⇒ cp a2' ⇒ cp res'
⇒ cp (λX. f (self' X) (a1' X) (a2' X))
(proof)

theorem unfold :
  assumes cp E
  and (τ |= δ self) ∧ (τ |= v a1) ∧ (τ |= v a2)
  and τ |= PRE self a1 a2
  and (∃ res. τ |= POST self a1 a2 (λf. res))
  and (∀ res. τ |= POST self a1 a2 (λf. res) ⇒ τ |= E (λf. res))
  shows τ |= E(f self a1 a2)
(proof)

lemma unfold2 :
  assumes cp E
  and (τ |= δ self) ∧ (τ |= v a1) ∧ (τ |= v a2)
  and τ |= PRE self a1 a2
  and τ |= POST' self a1 a2
  and (∀ res. (POST' self a1 a2 res) = ((POST' self a1 a2) and (res ≠ (BODY self a1 a2))))
  shows (τ |= E(f self a1 a2)) = (τ |= E(BODY self a1 a2))
(proof)

end

locale contract3 =
  fixes f :: (nat,α0::null)val ⇒
    (nat,α1::null)val ⇒
    (nat,α2::null)val ⇒
    (nat,α3::null)val ⇒
    (nat,res::null)val
  fixes PRE
  fixes POST
  assumes def-scheme: f self a1 a2 a3 ≡
    (λτ. SOME res. let res = λf. res in
      if (τ |= (δ self)) ∧ (τ |= v a1) ∧ (τ |= v a2) ∧ (τ |= v a3)

140
\[ \text{then } (\tau \models \text{PRE self } a1 a2 a3) \land \\
\hspace{1cm} (\tau \models \text{POST self } a1 a2 a3 \text{ res}) \]

\[ \text{else } \tau \models \text{res } \Downarrow \text{ invalid} \]

**assumes all-post:** \( \forall \sigma \sigma' \sigma'' \cdot (\sigma, \sigma') \models \text{PRE self } a1 a2 a3 = ((\sigma, \sigma'') \models \text{PRE self } a1 a2 a3) \)

**assumes cp\_PRE:** \( \text{PRE (self) } (a1) (a2) (a3) \tau = \text{PRE (} \lambda - \cdot \text{ self } \tau) (\lambda - \cdot a1 \tau) (\lambda - \cdot a2 \tau) (\lambda - \cdot a3 \tau) \tau \)

**assumes cp\_POST:** \( \forall \text{res. POST (self) } (a1) (a2) (a3) \text{ (res) } \tau = \\
\hspace{1cm} \text{POST } (\lambda - \cdot \text{ self } \tau)(\lambda - \cdot a1 \tau)(\lambda - \cdot a2 \tau)(\lambda - \cdot a3 \tau)(\lambda - \cdot \text{ res } \tau) \tau \)

**sublocale contract3 < contract-scheme:** \( \lambda(a1,a2,a3) \tau. (\tau \models v a1) \land (\tau \models v a2) \land (\tau \models v a3) \)

\[ \lambda(a1,a2,a3) \tau. (\lambda - a1 \tau, \lambda - a2 \tau, \lambda - a3 \tau) \]

\[ (\lambda x (a,b,c). f x a b c) \]

\[ (\lambda x (a,b,c). \text{PRE } x a b c) \]

\[ (\lambda x (a,b,c). \text{POST } x a b c) \]

\[ \langle \text{proof} \rangle \]

**context contract3**

**begin**

**lemma strict0\_simp:** \( f \text{ invalid } X Y Z = \text{ invalid} \)

\[ \langle \text{proof} \rangle \]

**lemma nullstrict0\_simp:** \( f \text{ null } X Y Z = \text{ invalid} \)

\[ \langle \text{proof} \rangle \]

**lemma strict1\_simp:** \( f \text{ self } \text{ invalid } Y Z = \text{ invalid} \)

\[ \langle \text{proof} \rangle \]

**lemma strict2\_simp:** \( f \text{ self } \text{ invalid } Y Z = \text{ invalid} \)

\[ \langle \text{proof} \rangle \]

**lemma defined-mono:** \( \tau \models v(f W X Y Z) \implies (\tau \models \delta W) \land (\tau \models v X) \land (\tau \models v Y) \land (\tau \models v Z) \)

\[ \langle \text{proof} \rangle \]

**lemma cp\_pre:** \( \text{cp self} \implies \text{cp a1} \implies \text{cp a2} \implies \text{cp a3} \implies \text{cp a1'} \implies \text{cp a2'} \implies \text{cp a3'} \implies \text{cp (} \lambda X. \text{PRE (} \text{self'} X) (a1' X) (a2' X) (a3' X) \text{ )} \)

\[ \langle \text{proof} \rangle \]

**lemma cp\_post:** \( \text{cp self} \implies \text{cp a1} \implies \text{cp a2} \implies \text{cp a3} \implies \text{cp res} \implies \text{cp (} \lambda X. \text{POST (} \text{self'} X) (a1' X) (a2' X) (a3' X) (\text{res'} X) \text{)} \)

\[ \langle \text{proof} \rangle \]

**lemma cp\_0':** \( f \text{ self a1 a2 a3 } \tau = f (\lambda - \cdot \text{ self } \tau)(\lambda - \cdot a1 \tau)(\lambda - \cdot a2 \tau)(\lambda - \cdot a3 \tau) \tau \)

\[ \langle \text{proof} \rangle \]

**lemma cp\_simp:** \( \text{cp self} \implies \text{cp a1} \implies \text{cp a2} \implies \text{cp a3} \implies \text{cp res} \implies \text{cp (} \lambda X. f (\text{self'} X) (a1' X) (a2' X) (a3' X) \text{)} \)

\[ \langle \text{proof} \rangle \]

**theorem unfold:**

**assumes**

\[ (\tau \models \delta \text{ self}) \land (\tau \models v a1) \land (\tau \models v a2) \land (\tau \models v a3) \land \]

\[ \tau \models \text{PRE self a1 a2 a3} \]

\[ \exists \text{res. } \tau \models \text{POST self a1 a2 a3 (} \lambda - \cdot \text{ res)} \]

\[ (\text{f res. } \tau \models \text{POST self a1 a2 a3 (} \lambda - \cdot \text{ res)}) \implies \tau \models E (\lambda - \cdot \text{ res}) \]

**shows**

\[ \tau \models E (f \text{ self a1 a2 a3}) \]
proof

lemma unfold2 : assumes cp E and (τ |= δ self) ∧ (τ |= v a1) ∧ (τ |= v a2) ∧ (τ |= v a3) and τ |= PRE self a1 a2 a3 and τ |= POST' self a1 a2 a3 and \( \land \) res. (POST' self a1 a2 a3 res) = ((POST' self a1 a2 a3) and (res \( \triangleq \) (BODY self a1 a2 a3))) shows (τ |= E(f self a1 a2 a3)) = (τ |= E(BODY self a1 a2 a3))

(proof)

end

end

theory UML-Tools
imports UML-Logic
begin

lemmas substs1 = StrongEq-L-subst2-rev
  foundation15[THEN iffD2, THEN StrongEq-L-subst2-rev]
  foundation7[THEN iffD2, THEN foundation15[THEN iffD2, THEN StrongEq-L-subst2-rev]]
  foundation14[THEN iffD2, THEN StrongEq-L-subst2-rev]
  foundation13[THEN iffD2, THEN StrongEq-L-subst2-rev]

lemmas substs2 = StrongEq-L-subst3-rev
  foundation15[THEN iffD2, THEN StrongEq-L-subst3-rev]
  foundation7[THEN iffD2, THEN foundation15[THEN iffD2, THEN StrongEq-L-subst3-rev]]
  foundation14[THEN iffD2, THEN StrongEq-L-subst3-rev]
  foundation13[THEN iffD2, THEN StrongEq-L-subst3-rev]

lemmas substs4 = StrongEq-L-subst4-rev
  foundation15[THEN iffD2, THEN StrongEq-L-subst4-rev]
  foundation7[THEN iffD2, THEN foundation15[THEN iffD2, THEN StrongEq-L-subst4-rev]]
  foundation14[THEN iffD2, THEN StrongEq-L-subst4-rev]
  foundation13[THEN iffD2, THEN StrongEq-L-subst4-rev]

lemmas substs = substs1 substs2 substs4 [THEN iffD2] substs4

thm substs (ML)

lemma test1 : τ |= A \implies τ |= (A and B \triangleq B)
(proof)

lemma test2 : τ |= A \implies τ |= (A and B \triangleq B)
(proof)

lemma test3 : τ |= A \implies τ |= (A and A)
(proof)
lemma test4 : \( \tau \models \neg A \Rightarrow \tau \models (A \text{ and } B \triangleq \text{false}) \)

\langle proof \rangle

lemma test5 : \( \tau \models (A \triangleq \text{null}) \Rightarrow \tau \models (B \triangleq \text{null}) \Rightarrow \neg (\tau \models (A \text{ and } B)) \)

\langle proof \rangle

lemma test6 : \( \tau \models \neg A \Rightarrow \neg (\tau \models (A \text{ and } B)) \)

\langle proof \rangle

lemma test7 : \( \neg (\tau \models (\nu A)) \Rightarrow \tau \models (\neg B) \Rightarrow \neg (\tau \models (A \text{ and } B)) \)

\langle proof \rangle

lemma X : \( \neg (\tau \models (\text{invalid and } B)) \)

\langle proof \rangle

lemma X' : \( \neg (\tau \models (\text{invalid and } B)) \)

\langle proof \rangle

lemma Y : \( \neg (\tau \models (\text{null and } B)) \)

\langle proof \rangle

lemma Z : \( \neg (\tau \models (\text{false and } B)) \)

\langle proof \rangle

lemma Z' : \( (\tau \models (\text{true and } B)) = (\tau \models B) \)

\langle proof \rangle

end

theory UML-Main
imports UML-Contracts UML-Tools
begin
end
4. Example: The Employee Analysis Model

theory
  Analysis-UML
imports
  ../../../UML-Main
begin

4.1. Introduction

For certain concepts like classes and class-types, only a generic definition for its resulting semantics can be given. Generic means, there is a function outside HOL that “compiles” a concrete, closed-world class diagram into a “theory” of this data model, consisting of a bunch of definitions for classes, accessors, method, casts, and tests for actual types, as well as proofs for the fundamental properties of these operations in this concrete data model.

Such generic function or “compiler” can be implemented in Isabelle on the ML level. This has been done, for a semantics following the open-world assumption, for UML 2.0 in [4, 7]. In this paper, we follow another approach for UML 2.4: we define the concepts of the compilation informally, and present a concrete example which is verified in Isabelle/HOL.

4.1.1. Outlining the Example

We are presenting here an “analysis-model” of the (slightly modified) example Figure 7.3, page 20 of the OCL standard [32]. Here, analysis model means that associations were really represented as relation on objects on the state—as is intended by the standard—rather by pointers between objects as is done in our “design model” (see Chapter 5). To be precise, this theory contains the formalization of the data-part covered by the UML class model (see Figure 4.1):

This means that the association (attached to the association class EmployeeRanking) with the association ends boss and employees is implemented by the attribute boss and the operation employees (to be discussed in the OCL part captured by the subsequent theory).

Figure 4.1.: A simple UML class model drawn from Figure 7.3, page 20 of [32].
4.2. Example Data-Universe and its Infrastructure

Ideally, the following is generated automatically from a UML class model.

Our data universe consists in the concrete class diagram just of node’s, and implicitly of the class object. Each class implies the existence of a class type defined for the corresponding object representations as follows:

\[
\text{datatype } \text{typePerson} = \text{mkPerson oid} \\
\quad \text{int option}
\]

\[
\text{datatype } \text{typeOclAny} = \text{mkOclAny oid} \\
\quad \text{(int option) option}
\]

Now, we construct a concrete “universe of OclAny types” by injection into a sum type containing the class types. This type of OclAny will be used as instance for all respective type-variables.

\[
\text{datatype } \exists = \text{inPerson typePerson} \mid \text{inOclAny typeOclAny}
\]

Having fixed the object universe, we can introduce type synonyms that exactly correspond to OCL types. Again, we exploit that our representation of OCL is a “shallow embedding” with a one-to-one correspondence of OCL-types to types of the meta-language HOL.

\[
\begin{align*}
\text{type-synonym } \text{Boolean} &= \exists \text{ Boolean} \\
\text{type-synonym } \text{Integer} &= \exists \text{ Integer} \\
\text{type-synonym } \text{Void} &= \exists \text{ Void} \\
\text{type-synonym } \text{OclAny} &= (\exists, \text{typeOclAny option option}) \text{ val} \\
\text{type-synonym } \text{Person} &= (\exists, \text{typePerson option option}) \text{ val} \\
\text{type-synonym } \text{Set-Integer} &= (\exists, \text{int option option}) \text{ Set} \\
\text{type-synonym } \text{Set-Person} &= (\exists, \text{typePerson option option}) \text{ Set}
\end{align*}
\]

Just a little check:

\[
\text{typ } \text{Boolean}
\]

To reuse key-elements of the library like referential equality, we have to show that the object universe belongs to the type class “oclany,” i.e., each class type has to provide a function oid-of yielding the object id (oid) of the object.

\[
\begin{align*}
\text{instantiation } \text{typePerson} :: \text{object} \\
\text{begin} \\
\text{definition } \text{oid-of-typePerson-def}: \text{oid-of } x = (\text{case } x \text{ of } \text{mkPerson } \text{oid - } \Rightarrow \text{oid}) \\
\text{instance } \langle \text{proof} \rangle
\end{align*}
\]

\[
\begin{align*}
\text{instantiation } \text{typeOclAny} :: \text{object} \\
\text{begin} \\
\text{definition } \text{oid-of-typeOclAny-def}: \text{oid-of } x = (\text{case } x \text{ of } \text{mkOclAny } \text{oid - } \Rightarrow \text{oid}) \\
\text{instance } \langle \text{proof} \rangle
\end{align*}
\]

\[
\begin{align*}
\text{instantiation } \exists :: \text{object} \\
\text{begin} \\
\text{definition } \text{oid-of-}\exists\text{-def}: \text{oid-of } x = (\text{case } x \text{ of } \\
\quad \text{inPerson person } \Rightarrow \text{oid-of person} \\
\quad | \text{inOclAny oclany } \Rightarrow \text{oid-of oclany}) \\
\text{instance } \langle \text{proof} \rangle
\end{align*}
\]
4.3. Instantiation of the Generic Strict Equality

We instantiate the referential equality on \(\text{Person}\) and \(\text{OclAny}\)

\[
\text{overloading } \text{StrictRefEq} \equiv \text{StrictRefEq} :: [\text{Person}, \text{Person}] \Rightarrow \text{Boolean}
\]

\[
\text{begin}
\text{definition } \text{StrictRefEq}_{\text{Object-Person}} : (x :: \text{Person}).(y :: \text{Person}) \equiv \text{StrictRefEq}_{\text{Object}} x y \\
\text{end}
\]

\[
\text{overloading } \text{StrictRefEq} \equiv \text{StrictRefEq} :: [\text{OclAny}, \text{OclAny}] \Rightarrow \text{Boolean}
\]

\[
\text{begin}
\text{definition } \text{StrictRefEq}_{\text{Object-OclAny}} : (x :: \text{OclAny}).(y :: \text{OclAny}) \equiv \text{StrictRefEq}_{\text{Object}} x y \\
\text{end}
\]

\[
\text{lemmas } \text{cps23} = \\
\text{cp-StrictRefEq}_{\text{Object-Person}}[\text{of } x :: \text{Person}, y :: \text{Person} \Rightarrow \text{Person}, \text{symmetric}] \\
\text{cp-intro}(9) [\text{of } P :: \text{Person} \Rightarrow \text{Person}, \text{Q :: Person} \Rightarrow \text{Person}, \text{symmetric}] \\
\text{StrictRefEq}_{\text{Object-Person-def}} [\text{of } x :: \text{Person}, y :: \text{Person}, \text{symmetric}] \\
\text{StrictRefEq}_{\text{Object-Person-defargs}} [\text{of } x :: \text{Person}, y :: \text{Person}, \text{symmetric}] \\
\text{StrictRefEq}_{\text{Object-Person-strict1}} [\text{of } x :: \text{Person}, \text{symmetric}] \\
\text{StrictRefEq}_{\text{Object-Person-strict2}} [\text{of } x :: \text{Person}, \text{symmetric}] \\
\text{for } x \ y \ P Q
\]

For each Class \(C\), we will have a casting operation \(\text{oclAsType}(C)\), a test on the actual type \(\text{oclIsTypeOf}(C)\) as well as its relaxed form \(\text{oclIsKindOf}(C)\) (corresponding exactly to Java’s \(\text{instanceof}\)-operator.

Thus, since we have two class-types in our concrete class hierarchy, we have two operations to declare and to provide two overloading definitions for the two static types.

4.4. \texttt{OclAsType}

4.4.1. Definition

\[
\text{consts } \text{OclAsType}_{\text{OclAny}} :: \alpha \Rightarrow \text{OclAny} ((\cdot) \cdot \text{oclAsType'}('\text{OclAny}')) \\
\text{consts } \text{OclAsType}_{\text{Person}} :: \alpha \Rightarrow \text{Person} ((\cdot) \cdot \text{oclAsType'}('\text{Person}'))
\]

\[
\text{definition } \text{OclAsType}_{\text{OclAny}-\text{OclAny}} = (\lambda u. \text{case } u \text{ of } \text{inOclAny } a \Rightarrow a \\
| \text{inPerson } (\text{mkOclAny } \text{oid } a) \Rightarrow \text{mkOclAny } \text{oid } a_u)
\]

\[
\text{lemma } \text{OclAsType}_{\text{OclAny}-\text{OclAny}} \text{-some: } \text{OclAsType}_{\text{OclAny}-\text{OclAny}} x \neq \text{None} \\
\langle \text{proof} \rangle
\]

\[
\text{overloading } \text{OclAsType}_{\text{OclAny}} \equiv \text{OclAsType}_{\text{OclAny}} :: \text{OclAny} \Rightarrow \text{OclAny}
\]

\[
\text{begin}
\text{definition } \text{OclAsType}_{\text{OclAny-OclAny}} :: \text{OclAny} \Rightarrow \text{OclAny} : \\
(X :: \text{OclAny}).\text{oclAsType}(\text{OclAny}) \equiv X \\
\text{end}
\]

\[
\text{overloading } \text{OclAsType}_{\text{OclAny}} \equiv \text{OclAsType}_{\text{OclAny}} :: \text{Person} \Rightarrow \text{OclAny}
\]

147
begin

definition OclAsTypeOclAny-Person: (X::Person) . oclAsType(OclAny) \equiv

(\forall \tau. \ case X \tau \ of
  \ \bot \Rightarrow invalid \ \tau
  | \ \bot_\tau \Rightarrow null \ \tau
  | \ \_mkPerson oid a_j \Rightarrow \_mkOclAny oid (a_j)_\_\)
end

definition OclAsTypePerson-A \equiv

(\forall \tau. \ case u of
  \ \text{inOclAny} (\_mkOclAny oid (a_j)) \Rightarrow \_mkPerson oid a_j
  | \ - \Rightarrow None)

overloading OclAsType\_Person \equiv OclAsType\_Person :: OclAny \Rightarrow Person
begin

definition OclAsType\_Person::OclAny:

(X::OclAny) . oclAsType(Person) \equiv

(\forall \tau. \ case X \tau \ of
  \ \bot \Rightarrow invalid \ \tau
  | \ \bot_\tau \Rightarrow null \ \tau
  | \ \_mkOclAny oid \_ \Rightarrow invalid \ \tau \ — down-cast exception
  | \ \_mkOclAny oid (a_j)_\_ \Rightarrow \_mkPerson oid a_j)
end

overloading OclAsType\_Person \equiv OclAsType\_Person :: Person \Rightarrow Person
begin

definition OclAsType\_Person::Person:

(X::Person) . oclAsType(Person) \equiv X
end

lemmas [simp] =
  OclAsTypeOclAny-OclAny
  OclAsType\_Person::OclAny

4.4.2. Context Passing

lemma cp-OclAsType\_Person::OclAny-Person-Person::Person: cp P \Rightarrow cp(\lambda X. (P \ (X::Person)::Person) . oclAsType(OclAny))
(proof)

lemma cp-OclAsType\_OclAny\_OclAny::OclAny-OclAny::OclAny::OclAny:

(cp \ (P \ (X::OclAny)::OclAny)) . oclAsType(OclAny)
(proof)

lemma cp-OclAsType\_Person::Person::Person::OclAny::OclAny:

(cp \ (P \ (X::Person)::Person) . oclAsType(Person))
(proof)

lemma cp-OclAsType\_Person::OclAny::OclAny::Person::OclAny:

(cp \ (P \ (X::OclAny)::Person) . oclAsType(Person))
(proof)

lemma cp-OclAsType\_Person::Person::OclAny::OclAny::Person:

(cp \ (P \ (X::OclAny)::Person) . oclAsType(Person))
(proof)

lemma cp-OclAsType\_Person::OclAny::OclAny::Person:

(cp \ (P \ (X::OclAny)::Person))
(proof)

lemmas [simp] =
  cp-OclAsType\_OclAny::OclAny-Person-Person
  cp-OclAsType\_OclAny::OclAny-OclAny
  cp-OclAsType\_Person::Person-Person-Person

148
4.4.3. Execution with Invalid or Null as Argument

**Lemma:** \( \text{OclAsType} \) \( \text{OclAny} \rightarrow \text{OclAny} \)-strict : (invalid::OclAny) .oclAsType(OclAny) = invalid \( \langle \text{proof} \rangle \)

**Lemma:** \( \text{OclAsType} \) \( \text{OclAny} \rightarrow \text{OclAny} \)-nullstrict : (null::OclAny) .oclAsType(OclAny) = null \( \langle \text{proof} \rangle \)

**Lemma:** \( \text{OclAsType} \) \( \text{Person} \rightarrow \text{OclAny} \)-strict : (invalid::Person) .oclAsType(OclAny) = invalid \( \langle \text{proof} \rangle \)

**Lemma:** \( \text{OclAsType} \) \( \text{Person} \rightarrow \text{OclAny} \)-nullstrict : (null::Person) .oclAsType(OclAny) = null \( \langle \text{proof} \rangle \)

4.5. OclIsTypeOf

4.5.1. Definition

**Consts:** \( \text{OclIsTypeOf} \) \( \text{OclAny} \) :: '\( \alpha \) \Rightarrow \text{Boolean} \)

**Consts:** \( \text{OclIsTypeOf} \) \( \text{Person} \) :: '\( \alpha \) \Rightarrow \text{Boolean} \)

**Overloading:** \( \text{OclIsTypeOf} \) \( \text{OclAny} \) \( \equiv \) \( \text{OclIsTypeOf} \) \( \text{Person} \)

**Definition:** \( \text{OclIsTypeOf} \) \( \text{OclAny} \rightarrow \text{OclAny} \):

\[
(X::\text{OclAny}) .\text{oclIsTypeOf}(\text{OclAny}) \equiv \\
(\lambda \tau . \text{case } X \tau \text{ of} \\
\text{⊥} \\ \text{true } \tau \text{ — invalid ??} \\
\text{ mkOclAny oid } \text{⊥} \\ \text{true } \tau \\
\text{ mkOclAny oid } \text{⊥} \\ \text{false } \tau)
\]

**Lemma:** \( \text{OclIsTypeOf} \) \( \text{OclAny} \rightarrow \text{OclAny} \):

\[
(X::\text{OclAny}) .\text{oclIsTypeOf}(\text{OclAny}) = \\
(\lambda \tau . \text{if } \tau = v \text{ then } (\text{case } X \tau \text{ of} \\
\text{⊥} \\ \text{true } \tau \text{ — invalid ??} \\
\text{ mkOclAny oid } \text{⊥} \\ \text{true } \tau \\
\text{ mkOclAny oid } \text{⊥} \\ \text{false } \tau)
\]

**Proof**

**Interpretation:** \( \text{OclIsTypeOf} \) \( \text{OclAny} \rightarrow \text{OclAny} \):

\[
\text{projde-mono-schemeV} \\
\text{OclIsTypeOf} : \text{OclAny} \Rightarrow \text{Boolean} \\
\lambda X . \text{case } X \text{ of} \\
\text{None} \Rightarrow \text{True} \\ \text{mkOclAny oid None} \Rightarrow \text{True} \\
\text{mkOclAny oid} \Rightarrow \text{False})
\]

\( \langle \text{proof} \rangle \)

149
overloading $\text{OclIsTypeOf}\ Ocl\text{Any} \equiv \text{OclIsTypeOf}\ Ocl\text{Any} :: \text{Person} \Rightarrow \text{Boolean}$

begin
definition $\text{OclIsTypeOf}\ Ocl\text{Any} :: \text{Person}$:
$(X :: \text{Person}) . \text{oclIsTypeOf}(\text{OclAny}) \equiv$
$(\lambda \tau. \text{case } X \tau \text{ of }$
$\bot \Rightarrow \text{invalid } \tau$
$| \bot_\tau \Rightarrow \text{true } \tau \quad \text{— invalid } ??$
$| \_ \_ \Rightarrow\text{false } \tau$
$— \text{must have actual type } \text{Person} \text{ otherwise}$
end

overloading $\text{OclIsTypeOf}\ Person \equiv \text{OclIsTypeOf}\ Person :: \text{OclAny} \Rightarrow \text{Boolean}$

begin
definition $\text{OclIsTypeOf}\ Person :: \text{OclAny}$:
$(X :: \text{OclAny}) . \text{oclIsTypeOf}(\text{Person}) \equiv$
$(\lambda \tau. \text{case } X \tau \text{ of }$
$\bot \Rightarrow \text{invalid } \tau$
$| \bot_\tau \Rightarrow \text{true } \tau$
$| \_ \_ \Rightarrow \text{false } \tau$
$\text{— must have actual type } \text{Person} \text{ otherwise}$
end

4.5.2. Context Passing

lemma $\text{cp-}\text{OclIsTypeOf}\ Ocl\text{Any} :: \text{Person} \Rightarrow \text{OclIsTypeOf}\ Person :: \text{OclAny}$:
$\text{cp} P \Rightarrow \text{cp}(\lambda X. (X :: \text{Person}) :: \text{Person}). \text{oclIsTypeOf}(\text{OclAny})$
(proof)

lemma $\text{cp-}\text{OclIsTypeOf}\ Ocl\text{Any} :: \text{OclAny} :: \text{OclAny} \Rightarrow \text{OclIsTypeOf}\ Ocl\text{Any}$:
$\text{cp} P \Rightarrow \text{cp}(\lambda X. (X :: \text{OclAny}) :: \text{OclAny}). \text{oclIsTypeOf}(\text{OclAny})$
(proof)

lemma $\text{cp-}\text{OclIsTypeOf}\ Person :: \text{Person} :: \text{Person} \Rightarrow \text{OclIsTypeOf}\ Person :: \text{OclAny}$:
$\text{cp} P \Rightarrow \text{cp}(\lambda X. (X :: \text{Person}) :: \text{Person}). \text{oclIsTypeOf}(\text{Person})$
(proof)

lemma $\text{cp-}\text{OclIsTypeOf}\ Person :: \text{OclAny} :: \text{OclAny} \Rightarrow \text{OclIsTypeOf}\ Person :: \text{OclAny}$:
$\text{cp} P \Rightarrow \text{cp}(\lambda X. (X :: \text{OclAny}) :: \text{OclAny}). \text{oclIsTypeOf}(\text{Person})$
(proof)

lemma $\text{cp-}\text{OclIsTypeOf}\ Person :: \text{OclAny} :: \text{Person} :: \text{Person} \Rightarrow \text{OclIsTypeOf}\ Person :: \text{OclAny}$:
$\text{cp} P \Rightarrow \text{cp}(\lambda X. (X :: \text{OclAny}) :: \text{Person} :: \text{Person}). \text{oclIsTypeOf}(\text{Person})$
(proof)

lemmas $[\text{simp}] =$
$\text{cp-}\text{OclIsTypeOf}\ Ocl\text{Any} :: \text{Person} :: \text{Person}$
$\text{cp-}\text{OclIsTypeOf}\ Ocl\text{Any} :: \text{OclAny} :: \text{OclAny}$
$\text{cp-}\text{OclIsTypeOf}\ Person :: \text{Person} :: \text{Person}$
$\text{cp-}\text{OclIsTypeOf}\ Person :: \text{OclAny} :: \text{OclAny}$
$\text{cp-}\text{OclIsTypeOf}\ Person :: \text{OclAny} :: \text{Person} :: \text{Person}$

4.5.3. Execution with Invalid or Null as Argument

Lemma OclIsTypeOf_OclAny-OclAny-strict1 [simp]:

\( \text{invalid}::\text{OclAny} \).oclIsTypeOf(\text{OclAny}) = \text{invalid}  

(proof)

Lemma OclIsTypeOf_OclAny-OclAny-strict2 [simp]:

\( \text{null}::\text{OclAny} \).oclIsTypeOf(\text{OclAny}) = \text{true}  

(proof)

Lemma OclIsTypeOf_Person-OclAny-strict1 [simp]:

\( \text{invalid}::\text{Person} \).oclIsTypeOf(\text{OclAny}) = \text{invalid}  

(proof)

Lemma OclIsTypeOf_Person-OclAny-strict2 [simp]:

\( \text{null}::\text{Person} \).oclIsTypeOf(\text{OclAny}) = \text{true}  

(proof)

Lemma OclIsTypeOf_Person-OclAny-strict1 [simp]:

\( \text{invalid}::\text{OclAny} \).oclIsTypeOf(\text{Person}) = \text{invalid}  

(proof)

Lemma OclIsTypeOf_Person-OclAny-strict2 [simp]:

\( \text{null}::\text{OclAny} \).oclIsTypeOf(\text{Person}) = \text{true}  

(proof)

Lemma OclIsTypeOf_Person-Person-strict1 [simp]:

\( \text{invalid}::\text{Person} \).oclIsTypeOf(\text{Person}) = \text{invalid}  

(proof)

Lemma OclIsTypeOf_Person-Person-strict2 [simp]:

\( \text{null}::\text{Person} \).oclIsTypeOf(\text{Person}) = \text{true}  

(proof)

4.5.4. Up Down Casting

Lemma actualType-larger-staticType:

assumes isdef: \( \tau \models (\delta \ X) \)

shows \( \tau \models (\text{X}::\text{Person}) \).oclIsTypeOf(\text{OclAny}) = \text{false}  

(proof)

Lemma down-cast-type:

assumes isOclAny: \( \tau \models (\text{X}::\text{OclAny}) \).oclIsTypeOf(\text{OclAny})

and non-null: \( \tau \models (\delta \ X) \)

shows \( \tau \models (\text{X} \ . \text{oclAsType} (\text{Person})) \models \text{invalid}  

(proof)

Lemma down-cast-type':

assumes isOclAny: \( \tau \models (\text{X}::\text{OclAny}) \).oclIsTypeOf(\text{OclAny})

and non-null: \( \tau \models (\delta \ X) \)

shows \( \tau \models \neg \nu (\text{X} . \text{oclAsType}(\text{Person})) \)  

(proof)

Lemma up-down-cast :

assumes isdef: \( \tau \models (\delta \ X) \)

shows \( \tau \models (\text{X}::\text{Person}) \ . \text{oclAsType}(\text{OclAny}) \ . \text{oclAsType} (\text{Person}) \models X \)  

(proof)
lemma up-down-cast-Person-OclAny-Person [simp]:
shows \((X :: \text{Person}) \cdot \text{oclAsType}(\text{OclAny}) \cdot \text{oclAsType}(\text{Person}) = X)\)
(proof)

lemma up-down-cast-Person-OclAny-Person':
assumes \(\tau \models v \ X\)
shows \(\tau \models ((X :: \text{Person}) \cdot \text{oclAsType}(\text{OclAny}) \cdot \text{oclAsType}(\text{Person}) ) \equiv X)\)
(proof)

lemma up-down-cast-Person-OclAny-Person'':
assumes \(\tau \models v (X :: \text{Person})\)
shows \(\tau \models (X \cdot \text{oclIsTypeOf}(\text{Person}) \implies (X \cdot \text{oclAsType}(\text{OclAny}) \cdot \text{oclAsType}(\text{Person})) \equiv X)\)
(proof)

4.6. OclIsKindOf

4.6.1. Definition

consts \(\text{OclIsKindOf}_{\text{OclAny}} :: \alpha \Rightarrow \text{Boolean}\)
\(\text{OclIsKindOf}_{\text{Person}} :: \alpha \Rightarrow \text{Boolean}\)

overloading \(\text{OclIsKindOf}_{\text{OclAny}} \equiv \text{OclIsKindOf}_{\text{OclAny}} :: \text{OclAny} \Rightarrow \text{Boolean}\)
begin
definition \(\text{OclIsKindOf}_{\text{OclAny}}\):
\((X :: \text{OclAny}) \cdot \text{oclIsKindOf}(\text{OclAny})) \equiv
(\lambda \tau. \text{case } X \tau \text{ of}
\quad \bot \Rightarrow \text{invalid } \tau
\quad \_ \Rightarrow \text{true } \tau)
end

overloading \(\text{OclIsKindOf}_{\text{OclAny}} \equiv \text{OclIsKindOf}_{\text{OclAny}} :: \text{Person} \Rightarrow \text{Boolean}\)
begin
definition \(\text{OclIsKindOf}_{\text{OclAny}}\):
\((X :: \text{Person}) \cdot \text{oclIsKindOf}(\text{OclAny})) \equiv
(\lambda \tau. \text{case } X \tau \text{ of}
\quad \bot \Rightarrow \text{invalid } \tau
\quad \_ \Rightarrow \text{true } \tau)
end

overloading \(\text{OclIsKindOf}_{\text{Person}} \equiv \text{OclIsKindOf}_{\text{Person}} :: \text{OclAny} \Rightarrow \text{Boolean}\)
begin
definition \(\text{OclIsKindOf}_{\text{Person}}\):
\((X :: \text{OclAny}) \cdot \text{oclIsKindOf}(\text{Person})) \equiv
(\lambda \tau. \text{case } X \tau \text{ of}
\quad \bot \Rightarrow \text{invalid } \tau
\quad \downarrow \Rightarrow \text{true } \tau
\quad \text{mk}\_\text{OclAny} \_ \_ \Rightarrow \text{false } \tau
\quad \text{mk}\_\text{OclAny} \_ \_ \Rightarrow \text{true } \tau)
end

overloading \(\text{OclIsKindOf}_{\text{Person}} \equiv \text{OclIsKindOf}_{\text{Person}} :: \text{Person} \Rightarrow \text{Boolean}\)
begin
definition \(\text{OclIsKindOf}_{\text{Person}}\):
\((X :: \text{Person}) \cdot \text{oclIsKindOf}(\text{Person})) \equiv
(\lambda \tau. \text{case } X \tau \text{ of}
\quad \bot \Rightarrow \text{invalid } \tau
\quad \_ \Rightarrow \text{true } \tau
\quad \_ \Rightarrow \text{true } \tau
\quad \_ \Rightarrow \text{true } \tau)
end

4.6. OclIsKindOf

4.6.1. Definition

consts \(\text{OclIsKindOf}_{\text{OclAny}} :: \alpha \Rightarrow \text{Boolean}\)
\(\text{OclIsKindOf}_{\text{Person}} :: \alpha \Rightarrow \text{Boolean}\)

overloading \(\text{OclIsKindOf}_{\text{OclAny}} \equiv \text{OclIsKindOf}_{\text{OclAny}} :: \text{OclAny} \Rightarrow \text{Boolean}\)
begin
definition \(\text{OclIsKindOf}_{\text{OclAny}}\):
\((X :: \text{OclAny}) \cdot \text{oclIsKindOf}(\text{OclAny})) \equiv
(\lambda \tau. \text{case } X \tau \text{ of}
\quad \bot \Rightarrow \text{invalid } \tau
\quad \_ \Rightarrow \text{true } \tau)
end

overloading \(\text{OclIsKindOf}_{\text{OclAny}} \equiv \text{OclIsKindOf}_{\text{OclAny}} :: \text{Person} \Rightarrow \text{Boolean}\)
begin
definition \(\text{OclIsKindOf}_{\text{OclAny}}\):
\((X :: \text{Person}) \cdot \text{oclIsKindOf}(\text{OclAny})) \equiv
(\lambda \tau. \text{case } X \tau \text{ of}
\quad \bot \Rightarrow \text{invalid } \tau
\quad \_ \Rightarrow \text{true } \tau
\quad \_ \Rightarrow \text{true } \tau)
end

overloading \(\text{OclIsKindOf}_{\text{Person}} \equiv \text{OclIsKindOf}_{\text{Person}} :: \text{OclAny} \Rightarrow \text{Boolean}\)
begin
definition \(\text{OclIsKindOf}_{\text{Person}}\):
\((X :: \text{OclAny}) \cdot \text{oclIsKindOf}(\text{Person})) \equiv
(\lambda \tau. \text{case } X \tau \text{ of}
\quad \bot \Rightarrow \text{invalid } \tau
\quad \_ \Rightarrow \text{true } \tau
\quad \_ \Rightarrow \text{true } \tau
\quad \_ \Rightarrow \text{true } \tau)
end

overloading \(\text{OclIsKindOf}_{\text{Person}} \equiv \text{OclIsKindOf}_{\text{Person}} :: \text{Person} \Rightarrow \text{Boolean}\)
begin
definition \(\text{OclIsKindOf}_{\text{Person}}\):
\((X :: \text{Person}) \cdot \text{oclIsKindOf}(\text{Person})) \equiv
(\lambda \tau. \text{case } X \tau \text{ of}
\quad \bot \Rightarrow \text{invalid } \tau
\quad \_ \Rightarrow \text{true } \tau
\quad \_ \Rightarrow \text{true } \tau
\quad \_ \Rightarrow \text{true } \tau)
end

152
\[ \bot \Rightarrow \text{invalid } \tau \]
\[ \cdot \Rightarrow \text{true } \tau) \]

4.6.2. Context Passing

**lemma** \( cp-\text{OclIsKindOfOclAny-Person-Person} \): \( cp \implies cp(\lambda X. (P(X::\text{Person})::\text{Person}).\text{oclIsKindOf}(\text{OclAny})) \)

**proof**

**lemma** \( cp-\text{OclIsKindOfOclAny-OclAny-OclAny} \): \( cp \implies cp(\lambda X. (P(X::\text{OclAny})::\text{OclAny}).\text{oclIsKindOf}(\text{OclAny})) \)

**proof**

**lemma** \( cp-\text{OclIsKindOfPerson-Person-Person} \): \( cp \implies cp(\lambda X. (P(X::\text{Person})::\text{Person}).\text{oclIsKindOf}(\text{Person})) \)

**proof**

**lemma** \( cp-\text{OclIsKindOfPerson-OclAny-OclAny} \): \( cp \implies cp(\lambda X. (P(X::\text{OclAny})::\text{OclAny}).\text{oclIsKindOf}(\text{Person})) \)

**proof**

**lemmas** [\text{simp}]
\[
\begin{align*}
& \text{cp-\text{OclIsKindOfOclAny-Person-Person}} \\
& \text{cp-\text{OclIsKindOfOclAny-OclAny-OclAny}} \\
& \text{cp-\text{OclIsKindOfPerson-Person-Person}} \\
& \text{cp-\text{OclIsKindOfPerson-OclAny-OclAny}} \\
& \text{cp-\text{OclIsKindOfPerson-OclAny-Person}} \\
& \text{cp-\text{OclIsKindOfPerson-OclAny-OclAny-Person}}
\end{align*}
\]

4.6.3. Execution with Invalid or Null as Argument

**lemma** \( \text{OclIsKindOfOclAny-OclAny-strict1}[\text{simp}] \): \( (\text{invalid}::\text{OclAny} \cdot \text{oclIsKindOf}(\text{OclAny}) = \text{invalid} \)

**proof**

**lemma** \( \text{OclIsKindOfOclAny-OclAny-strict2}[\text{simp}] \): \( (\text{null}::\text{OclAny} \cdot \text{oclIsKindOf}(\text{OclAny}) = \text{true} \)

**proof**

**lemma** \( \text{OclIsKindOfOclAny-Person-strict1}[\text{simp}] \): \( (\text{invalid}::\text{Person} \cdot \text{oclIsKindOf}(\text{OclAny}) = \text{invalid} \)

**proof**

**lemma** \( \text{OclIsKindOfOclAny-Person-strict2}[\text{simp}] \): \( (\text{null}::\text{Person} \cdot \text{oclIsKindOf}(\text{OclAny}) = \text{true} \)

**proof**

**lemma** \( \text{OclIsKindOfPerson-OclAny-strict1}[\text{simp}] \): \( (\text{invalid}::\text{Person} \cdot \text{oclIsKindOf}(\text{Person}) = \text{invalid} \)

**proof**

**lemma** \( \text{OclIsKindOfPerson-OclAny-strict2}[\text{simp}] \): \( (\text{null}::\text{Person} \cdot \text{oclIsKindOf}(\text{Person}) = \text{true} \)

**proof**

4.6.4. Up Down Casting

**lemma** \( \text{actualKind-larger-staticKind} \):

**assumes** \( \text{isdef}: \tau |\rightarrow (\delta \ X) \)

153
\[ \tau \models (\langle X::\text{Person} \rangle .\ oclIsKindOf(\text{OclAny}) \equiv \text{true}) \]

(\text{proof})

\text{lemma} \downcast-kind:
\text{assumes} \ isOclAny: \neg (\tau \models ((X::\text{OclAny}).\ oclIsKindOf(\text{Person})))
\text{and} \ non-null: \tau \models (\delta X)
\text{shows} \tau \models ((X .\ oclAsType(\text{Person})) \equiv \text{invalid})
(\text{proof})

4.7. OclAllInstances

To denote OCL-types occurring in OCL expressions syntactically—as, for example, as “argument” of oclAllInstances()—we use the inverses of the injection functions into the object universes; we show that this is sufficient “characterization.”

\text{definition} \ Person \equiv \text{OclAsType}_\text{Person} - A
\text{definition} \ OclAny \equiv \text{OclAsType}_\text{OclAny} - A

\text{lemmas} \ [\text{simp}] = \text{Person-def OclAny-def}

\text{lemma} OclAllInstances-generic\_OclAny\_exec: OclAllInstances-generic \_pre-post OclAny =
(\lambda \tau. \ Abs-Set\_base \_\_ Some ' OclAny ' ran (heap (pre-post \tau)) \_\_)
(\text{proof})

\text{lemma} OclAllInstances-at-post\_\text{OclAny}\_exec: OclAny .\ allInstances() =
(\lambda \tau. \ Abs-Set\_base \_\_ Some ' OclAny ' ran (heap (snd \tau)) \_\_)
(\text{proof})

\text{lemma} OclAllInstances-at-pre\_\text{OclAny}\_exec: OclAny .\ allInstances@pre() =
(\lambda \tau. \ Abs-Set\_base \_\_ Some ' OclAny ' ran (heap (fst \tau)) \_\_)
(\text{proof})

4.7.1. OclIsTypeOf

\text{lemma} OclAny-allInstances-generic-oclIsTypeOf\_\text{OclAny}1:
\text{assumes} [\text{simp}]: \forall x. \ pre-post (x, x) = x
\text{shows} \exists \tau. (\tau \models ((\text{OclAllInstances-generic \_pre-post OclAny}) \Rightarrow \text{forAll}_{Set}(X|X .\ oclIsTypeOf(\text{OclAny}))))
(\text{proof})

\text{lemma} OclAny-allInstances-at-post-oclIsTypeOf\_\text{OclAny}1:
\exists \tau. (\tau \models (\text{OclAny .\ allInstances()} \Rightarrow \text{forAll}_{Set}(X|X .\ oclIsTypeOf(\text{OclAny}))))
(\text{proof})

\text{lemma} OclAny-allInstances-at-pre-oclIsTypeOf\_\text{OclAny}1:
\exists \tau. (\tau \models (\text{OclAny .\ allInstances@pre()} \Rightarrow \text{forAll}_{Set}(X|X .\ oclIsTypeOf(\text{OclAny}))))
(\text{proof})

\text{lemma} OclAny-allInstances-generic-oclIsTypeOf\_\text{OclAny}2:
\text{assumes} [\text{simp}]: \forall x. \ pre-post (x, x) = x
\text{shows} \exists \tau. (\tau \models \neg ((\text{OclAllInstances-generic \_pre-post OclAny}) \Rightarrow \text{forAll}_{Set}(X|X .\ oclIsTypeOf(\text{OclAny}))))
(\text{proof})

\text{lemma} OclAny-allInstances-at-post-oclIsTypeOf\_\text{OclAny}2:
\exists \tau. (\tau \models \neg (\text{OclAny .\ allInstances()} \Rightarrow \text{forAll}_{Set}(X|X .\ oclIsTypeOf(\text{OclAny}))))
(\text{proof})

\text{lemma} OclAny-allInstances-at-pre-oclIsTypeOf\_\text{OclAny}2:
\exists \tau. (\tau \models \neg (\text{OclAny .\ allInstances@pre()} \Rightarrow \text{forAll}_{Set}(X|X .\ oclIsTypeOf(\text{OclAny}))))
⟨proof⟩

lemma Person-allInstances-generic-oclIsTypeOf Person:
\[ \tau \models ((\text{OclAllInstances-generic pre-post Person}) \rightarrow \text{forAll}_{\mathcal{S}et}(X | X . \text{oclIsTypeOf}(\text{Person}))) \]
⟨proof⟩

lemma Person-allInstances-at-post-oclIsTypeOf Person:
\[ \tau \models (\text{Person}. \text{allInstances()} \rightarrow \text{forAll}_{\mathcal{S}et}(X | X . \text{oclIsTypeOf}(\text{Person}))) \]
⟨proof⟩

lemma Person-allInstances-at-pre-oclIsTypeOf Person:
\[ \tau \models (\text{Person}. \text{allInstances}()@\pre \rightarrow \text{forAll}_{\mathcal{S}et}(X | X . \text{oclIsTypeOf}(\text{Person}))) \]
⟨proof⟩

4.7.2. OclIsKindOf

lemma OclAny-allInstances-generic-oclIsKindOf OclAny:
\[ \tau \models ((\text{OclAllInstances-generic pre-post OclAny}) \rightarrow \text{forAll}_{\mathcal{S}et}(X | X . \text{oclIsKindOf}(\text{OclAny}))) \]
⟨proof⟩

lemma OclAny-allInstances-at-post-oclIsKindOf OclAny:
\[ \tau \models (\text{OclAny}. \text{allInstances()} \rightarrow \text{forAll}_{\mathcal{S}et}(X | X . \text{oclIsKindOf}(\text{OclAny}))) \]
⟨proof⟩

lemma OclAny-allInstances-at-pre-oclIsKindOf OclAny:
\[ \tau \models (\text{OclAny}. \text{allInstances}@\pre \rightarrow \text{forAll}_{\mathcal{S}et}(X | X . \text{oclIsKindOf}(\text{OclAny}))) \]
⟨proof⟩

lemma Person-allInstances-generic-oclIsKindOf OclAny:
\[ \tau \models ((\text{OclAllInstances-generic pre-post Person}) \rightarrow \text{forAll}_{\mathcal{S}et}(X | X . \text{oclIsKindOf}(\text{OclAny}))) \]
⟨proof⟩

lemma Person-allInstances-at-post-oclIsKindOf OclAny:
\[ \tau \models (\text{Person}. \text{allInstances()} \rightarrow \text{forAll}_{\mathcal{S}et}(X | X . \text{oclIsKindOf}(\text{OclAny}))) \]
⟨proof⟩

lemma Person-allInstances-at-pre-oclIsKindOf OclAny:
\[ \tau \models (\text{Person}. \text{allInstances}()@\pre \rightarrow \text{forAll}_{\mathcal{S}et}(X | X . \text{oclIsKindOf}(\text{OclAny}))) \]
⟨proof⟩

4.7.2. OclIsKindOf

lemma OclAny-allInstances-generic-oclIsKindOf Person:
\[ \tau \models ((\text{OclAllInstances-generic pre-post Person}) \rightarrow \text{forAll}_{\mathcal{S}et}(X | X . \text{oclIsKindOf}(\text{Person}))) \]
⟨proof⟩

lemma Person-allInstances-at-post-oclIsKindOf Person:
\[ \tau \models (\text{Person}. \text{allInstances()} \rightarrow \text{forAll}_{\mathcal{S}et}(X | X . \text{oclIsKindOf}(\text{Person}))) \]
⟨proof⟩

lemma Person-allInstances-at-pre-oclIsKindOf Person:
\[ \tau \models (\text{Person}. \text{allInstances}()@\pre \rightarrow \text{forAll}_{\mathcal{S}et}(X | X . \text{oclIsKindOf}(\text{Person}))) \]
⟨proof⟩

4.8. The Accessors (any, boss, salary)

Should be generated entirely from a class-diagram.
4.8.1. Definition (of the association Employee-Boss)

We start with a oid for the association; this oid can be used in presence of association classes to represent
the association inside an object, pretty much similar to the Design_UML, where we stored an oid inside
the class as “pointer.”

definition oid_{Person}BOSS :: oid where oid_{Person}BOSS = 10

From there on, we can already define an empty state which must contain for oid_{Person}BOSS the
empty relation (encoded as association list, since there are associations with a Sequence-like structure).

definition eval-extract :: ((\A('a::object) option option) val
⇒ (oid ⇒ (\A,'c::null) val)
⇒ (\A,'c::null) val

where eval-extract X f = (\A τ. case X τ of
  | \_ \_ ⇒ invalid τ — exception propagation
  | \_, \_ ⇒ invalid τ — dereferencing null pointer
  | \_, obj \_ ⇒ f (oid-of obj) τ)

definition choose2-1 = fst
definition choose2-2 = snd

definition List-flatten = (\A (foldl ((\A acc. (\A l. (foldl ((\A acc. (\A l. (Cons l) (acc)))) (acc) ((rev l)))))) (Nil) ((rev (l))))))

definition deref-assocs2 :: (\A state × \A state ⇒ \A state)
⇒ (oid list list ⇒ oid list × oid list)
⇒ oid
⇒ (oid list ⇒ (\A,'f)'val)
⇒ oid
⇒ (\A,'f::null)'val

where deref-assocs2 pre-post from assoc-oid f oid =
(\A τ. case (assoc (pre-post τ)) assoc-oid of
  | \_ \_ ⇒ invalid τ
  | - ⇒ invalid τ)

  S \_ ⇒ f (List-flatten (map (choose2-2 o to-from)
    (filter (\A p. List.member (choose2-1 (to-from p)) oid) S)))

The pre-post-parameter is configured with fst or snd, the to-from-parameter either with the identity
id or the following combinator switch:

definition switch2-1 = (\A[x,y]⇒ (x,y))
definition switch2-2 = (\A[x,y]⇒ (y,x))
definition switch3-1 = (\A[x,y,z]⇒ (x,y))
definition switch3-2 = (\A[x,y,z]⇒ (x,z))
definition switch3-3 = (\A[x,y,z]⇒ (y,x))
definition switch3-4 = (\A[x,y,z]⇒ (y,z))
definition switch3-5 = (\A[x,y,z]⇒ (z,x))
definition switch3-6 = (\A[x,y,z]⇒ (z,y))

definition deref-oid_{Person} :: (\A state × \A state ⇒ \A state)
⇒ (type_{Person} ⇒ (\A,'c::null)'val)
⇒ oid
⇒ (\A,'c::null)'val

where deref-oid_{Person} fst-snd f oid = (\A τ. case (heap (fst-snd τ)) oid of
  | \_ in_Person obj \_ ⇒ f obj τ
  | - ⇒ invalid τ)

definition deref-oid_{Ocl.Any} :: (\A state × \A state ⇒ \A state)
\[
\Rightarrow \text{type}_{\text{OclAny}} \Rightarrow (\lambda x. 'c::null)val
\Rightarrow \text{oid} \Rightarrow (\lambda x. 'c::null)val
\]

**where** deref-oid\(_{\text{OclAny}}\) fst-snd f oid = \((\lambda \tau. \text{case heap(fst-snd \(\tau\)) oid of }
\begin{array}{l}
\text{i}_{\text{OclAny}} \text{obj} \Rightarrow f \text{ obj} \\tau \\
\text{-} \Rightarrow \text{invalid} \\tau
\end{array})
\]

pointer undefined in state or not referencing a type conform object representation

**definition** select\(_{\text{OclAny}}\)ANY f = \((\lambda X. \text{case } X \text{ of }
\begin{array}{l}
(\text{mk}_{\text{OclAny}} - \bot) \Rightarrow \text{null} \\
(\text{mk}_{\text{OclAny}} - \text{any}) \Rightarrow f (\lambda x. \text{-}_{\text{u}x_{\text{any}}}) \text{any}
\end{array})
\]

**definition** select\(_{\text{Person}}\)BOSS f = select-object mtSet UML-Set.OclIncluding UML-Set.OclANY \((f (\lambda x. \text{-}_{\text{u}x_{\text{any}}}))\)

**definition** select\(_{\text{Person}}\)SALARY f = \((\lambda X. \text{case } X \text{ of }
\begin{array}{l}
(\text{mk}_{\text{Person}} - \bot) \Rightarrow \text{null} \\
(\text{mk}_{\text{Person}} - \text{salary}) \Rightarrow f (\lambda x. \text{-}_{\text{u}x_{\text{salary}}}) \text{salary}
\end{array})
\]

**definition** deref-assocs\(_{2}\)BOSS fst-snd f oid = \((\lambda \text{mk}_{\text{Person}} \text{oid} - \Rightarrow \text{deref-assocs}\(_{2}\)fst-snd switch\(_{2}\)-1 oid_{\text{Person}}BOSS f oid)
\]

**definition** in-pre-state = fst
**definition** in-post-state = snd
**definition** reconst-basetype = \((\lambda \text{convert} \ x. \text{convert} \ x)\)

**definition** dot\(_{\text{OclAny}}\)ANY :: OclAny \Rightarrow - \((1(-).\text{any}) 50\) where \(X).\text{any} = \text{eval-extract} X \text{ (deref-oid}_{\text{OclAny}}\text{ in-post-state})\text{ (select}_{\text{OclAny}}\text{ANY reconst-basetype)})\)

**definition** dot\(_{\text{Person}}\)BOSS :: Person \Rightarrow Person \((1(-).\text{boss}) 50\) where \(X).\text{boss} = \text{eval-extract} X \text{ (deref-oid}_{\text{Person}}\text{ in-post-state})\text{ (deref-assocs}_{2}\text{BOSS in-post-state})\text{ (select}_{\text{Person}}\text{BOSS (deref-oid}_{\text{Person}}\text{ in-post-state))))\)

**definition** dot\(_{\text{Person}}\)SALARY :: Person \Rightarrow Integer \((1(-).\text{salary}) 50\) where \(X).\text{salary} = \text{eval-extract} X \text{ (deref-oid}_{\text{Person}}\text{ in-post-state})\text{ (select}_{\text{Person}}\text{SALARY reconst-basetype)})\)

**definition** dot\(_{\text{OclAny}}\)ANY-at-pre :: OclAny \Rightarrow - \((1(-).\text{any}@pre) 50\) where \(X).\text{any}@pre = \text{eval-extract} X \text{ (deref-oid}_{\text{OclAny}}\text{ in-pre-state})\text{ (select}_{\text{OclAny}}\text{ANY reconst-basetype)})\)

**definition** dot\(_{\text{Person}}\)BOSS-at-pre :: Person \Rightarrow Person \((1(-).\text{boss}@pre) 50\) where \(X).\text{boss}@pre = \text{eval-extract} X \text{ (deref-oid}_{\text{Person}}\text{ in-pre-state})
4.8.2. Context Passing

lemmas \[ \text{cp-dot-accessor} = \]
- \[ \text{cp-dot}\_\text{OclAny}\_\text{ANY-def} \]
- \[ \text{dot}\_\text{Person}\_\text{BOSS-def} \]
- \[ \text{dot}\_\text{Person}\_\text{SALARY-def} \]
- \[ \text{cp-dot}\_\text{OclAny}\_\text{ANY-at-pre-def} \]
- \[ \text{dot}\_\text{Person}\_\text{BOSS-at-pre-def} \]
- \[ \text{dot}\_\text{Person}\_\text{SALARY-at-pre-def} \]

4.8.3. Execution with Invalid or Null as Argument

lemma \[ \text{dot}\_\text{OclAny}\_\text{ANY-nullstrict} \text{ simp: } \text{null} \_\text{any} = \text{invalid} \]

lemma \[ \text{dot}\_\text{OclAny}\_\text{ANY-at-pre-nullstrict} \text{ simp: } \text{null} \_\text{any@pre} = \text{invalid} \]
lemma dot\textsubscript{Ocl\textsubscript{Any}}\textsubscript{ANY}-strict [simp] : (invalid).any = invalid
  ⟨proof⟩
lemma dot\textsubscript{Ocl\textsubscript{Any}}\textsubscript{ANY}-at-pre-strict [simp] : (invalid).any\@pre = invalid
  ⟨proof⟩

lemma dot\textsubscript{person}\textsubscript{BOSS-nullstrict} [simp]: (null).boss = invalid
  ⟨proof⟩
lemma dot\textsubscript{person}\textsubscript{BOSS-at-pre-nullstrict} [simp] : (null).boss\@pre = invalid
  ⟨proof⟩
lemma dot\textsubscript{person}\textsubscript{BOSS-strict} [simp] : (invalid).boss = invalid
  ⟨proof⟩
lemma dot\textsubscript{person}\textsubscript{BOSS-at-pre-strict} [simp] : (invalid).boss\@pre = invalid
  ⟨proof⟩

lemma dot\textsubscript{person}\textsubscript{SALARY-nullstrict} [simp]: (null).salary = invalid
  ⟨proof⟩
lemma dot\textsubscript{person}\textsubscript{SALARY-at-pre-nullstrict} [simp] : (null).salary\@pre = invalid
  ⟨proof⟩
lemma dot\textsubscript{person}\textsubscript{SALARY-strict} [simp] : (invalid).salary = invalid
  ⟨proof⟩
lemma dot\textsubscript{person}\textsubscript{SALARY-at-pre-strict} [simp] : (invalid).salary\@pre = invalid
  ⟨proof⟩

4.8.4. Representation in States

lemma dot\textsubscript{person}\textsubscript{BOSS-def-mono}: τ \models δ(X . boss) ⇒ τ \models δ(X)
  ⟨proof⟩
lemma repr-boss:
  assumes A : τ \models δ(x . boss)
  shows is-represented-in-state in-post-state (x . boss) Person τ
  ⟨proof⟩
lemma repr-bossX :
  assumes A: τ \models δ(x . boss)
  shows τ = ((Person . allInstances()) \rightarrow includes\textsubscript{Set}(x . boss))
  ⟨proof⟩

4.9. A Little Infra-structure on Example States

The example we are defining in this section comes from the figure 4.2.
definition OclInt1000 (1000) where OclInt1000 = (λ \cdot _\textsubscript{1000})
definition OclInt1200 (1200) where OclInt1200 = (λ \cdot _\textsubscript{1200})
definition OclInt1300 (1300) where OclInt1300 = (λ \cdot _\textsubscript{1300})
definition OclInt1800 (1800) where OclInt1800 = (λ \cdot _\textsubscript{1800})
definition OclInt2600 (2600) where OclInt2600 = (λ \cdot _\textsubscript{2600})
definition OclInt2900 (2900) where OclInt2900 = (λ \cdot _\textsubscript{2900})
definition OclInt3200 (3200) where OclInt3200 = (λ \cdot _\textsubscript{3200})
definition OclInt3500 (3500) where OclInt3500 = (λ \cdot _\textsubscript{3500})
definition oid0 ≡ 0
definition oid1 ≡ 1
definition oid2 ≡ 2
definition oid3 ≡ 3
\[ \sigma_1 \equiv \{ \text{heap} = \text{Map.empty}(\text{oid0} \mapsto \text{inPerson}(\text{mkPerson} \text{ oid0}, 1300)) \] 
\[ (\text{oid1} \mapsto \text{inPerson}(\text{mkPerson} \text{ oid1}, 1200)) \] 
\[ (\text{oid2} \mapsto \text{inPerson}(\text{mkPerson} \text{ oid2}, \text{None})) \] 
\[ (\text{oid3} \mapsto \text{inPerson}(\text{mkPerson} \text{ oid3}, 2600)) \] 
\[ (\text{oid4} \mapsto \text{inPerson}(\text{mkPerson} \text{ oid4}, 2500)) \] 
\[ (\text{oid5} \mapsto \text{inPerson}(\text{mkPerson} \text{ oid5}, 3500)) \] 
\[ (\text{oid6} \mapsto \text{inPerson}(\text{mkPerson} \text{ oid6}, 2300)) \] 
\[ (\text{oid7} \mapsto \text{inPerson}(\text{mkPerson} \text{ oid7}, \text{None})) \] 
\[ (\text{oid8} \mapsto \text{inPerson}(\text{mkPerson} \text{ oid8}, 0)) \] 
\[ \text{assocs} = \text{Map.empty}(\text{oidPersonBOSS} \mapsto \text{Map.empty}) \] 

\[ \sigma_1' \equiv \{ \text{heap} = \text{Map.empty}(\text{oid0} \mapsto \text{inPerson}(\text{person1})) \] 
\[ (\text{oid1} \mapsto \text{inPerson}(\text{person2})) \] 
\[ (\text{oid2} \mapsto \text{inPerson}(\text{person3})) \] 
\[ (\text{oid3} \mapsto \text{inPerson}(\text{person4})) \] 
\[ (\text{oid4} \mapsto \text{inPerson}(\text{person5})) \] 
\[ (\text{oid5} \mapsto \text{inPerson}(\text{person6})) \] 
\[ (\text{oid6} \mapsto \text{inPerson}(\text{person7})) \] 
\[ (\text{oid7} \mapsto \text{inPerson}(\text{person8})) \] 
\[ (\text{oid8} \mapsto \text{inPerson}(\text{person9})) \] 
\[ \text{assocs} = \text{Map.empty}(\text{oidPersonBOSS} \mapsto \text{Map.empty}) \] 

\[ \sigma_0 \equiv \{ \text{heap} = \text{Map.empty}, \text{assocs} = \text{Map.empty} \} \] 

**Lemma** basic-\(\tau\)-wff: \(WFF(\sigma_1, \sigma_1')\)
lemma [simp,code-unfold]: dom (heap σ₁) = {oid0,oid1,oid2,oid3,oid4,oid5,oid6,oid7,oid8}
(proof)

lemma [simp,code-unfold]: dom (heap σ₁') = {oid0,oid1,oid2,oid3,oid4,oid5,oid6,oid7,oid8}
(proof)
definition XPerson₁ :: Person ≡ person1.
definition XPerson₂ :: Person ≡ person2.
definition XPerson₃ :: Person ≡ person3.
definition XPerson₄ :: Person ≡ person4.
definition XPerson₅ :: Person ≡ person5.
definition XPerson₆ :: Person ≡ person6.
definition XPerson₇ :: OclAny ≡ person7.
definition XPerson₈ :: OclAny ≡ person8.
definition XPerson₉ :: Person ≡ person9.

lemma [code-unfold]: ((x::Person) = y) = StrictRefEq x y (proof)
lemma [code-unfold]: ((x::OclAny) = y) = StrictRefEq x y (proof)

lemmas [simp,code-unfold] =
OclAsTypeOclAny-OclAny
OclAsTypeOclAny-Person
OclAsTypePerson-OclAny
OclAsTypePerson-Person
OclIsTypeOfOclAny-OclAny
OclIsTypeOfOclAny-Person
OclIsTypeOfPerson-OclAny
OclIsTypeOfPerson-Person

OclIsKindOfOclAny-OclAny
OclIsKindOfOclAny-Person
OclIsKindOfPerson-OclAny
OclIsKindOfPerson-Person

OclIsKindOfPerson-Person Assert \( \forall \sigma_{pre} . \ (\sigma_{pre},\sigma_{1}) \models (X_{Person\_1} . \text{salary} \leftrightarrow 1000) \)
OclAsTypeOclAny-Person
OclAsTypePerson-OclAny
OclIsTypeOfPerson-OclAny
OclIsKindOfPerson-Person
OclIsKindOfPerson-Person

\( \forall \sigma_{pre} \ . \ \sigma_{pre},\sigma_{1} \models (X_{Person\_1} . \text{salary} \leftrightarrow 1300) \)
\( \forall \sigma_{post} . \ (\sigma_{1},\sigma_{post}) \models (X_{Person\_1} . \text{salary} @pre \leftrightarrow 1000) \)
\( \forall \sigma_{post} . \ (\sigma_{1},\sigma_{post}) \models (X_{Person\_1} . \text{salary} @pre \leftrightarrow 1300) \)

lemma \( \ (\sigma_{1},\sigma_{1}') \models (X_{Person\_1} . \text{oclIsMaintained}) \) (proof)

lemma \( \forall \sigma_{pre} \ . \ (\sigma_{pre},\sigma_{post}) \models ((X_{Person\_1} . \text{oclAsType}(OclAny) . \text{oclAsType}(Person)) \hat{=} X_{Person\_1}) \) (proof)

OclIsKindOfPerson-Person
OclIsKindOfPerson-Person

\( \forall \sigma_{pre} \ . \ (\sigma_{pre},\sigma_{1}') \models (X_{Person\_2} . \text{salary} \hat{=} 1800) \)
\( \forall \sigma_{post} . \ (\sigma_{1},\sigma_{post}) \models (X_{Person\_2} . \text{salary} @pre \hat{=} 1200) \)

lemma \( \ (\sigma_{1},\sigma_{1}') \models (X_{Person\_2} . \text{oclIsMaintained}) \) (proof)

\( \forall \sigma_{pre} . \ (\sigma_{pre},\sigma_{1}') \models (X_{Person\_3} . \text{salary} \hat{=} \text{null}) \)
Assert \( s_{\text{post}} \) \( \sigma, \sigma' \models \text{not}(v(X_{\text{Person}}. \text{salary} @ \text{pre})) \)

lemma \( \sigma, \sigma' \models (X_{\text{Person}}. \text{oclIsNew}()) \)

(proof)

lemma \( \sigma, \sigma' \models (X_{\text{Person}}. \text{oclIsMaintained}()) \)

(proof)

Assert \( s_{\text{pre}} \land s_{\text{post}} \) \( \sigma, \sigma', \sigma'' \models \text{not}(v(X_{\text{Person}}. \text{salary})) \)

Assert \( s_{\text{pre}} \land s_{\text{post}} \) \( \sigma, \sigma', \sigma'' \models (X_{\text{Person}}. \text{salary} @ \text{pre} \geq 3500) \)

lemma \( \sigma, \sigma' \models (X_{\text{Person}}. \text{oclIsDeleted}()) \)

(proof)

lemma \( \sigma, \sigma' \models (X_{\text{Person}}. \text{oclIsMaintained}()) \)

(proof)

Assert \( s_{\text{pre}} \land s_{\text{post}} \) \( \sigma, \sigma', \sigma'' \models v(X_{\text{Person}}. \text{oclAsType}()) \)

lemma \( s_{\text{pre}} \land s_{\text{post}} \) \( \sigma, \sigma', \sigma'' \models ((X_{\text{Person}}. \text{oclAsType}(\text{Person}). \text{oclAsType}(\text{OclAny}). \text{oclAsType}(\text{Person})) \equiv (X_{\text{Person}}. \text{oclAsType}(\text{Person}))) \)

lemma \( \sigma, \sigma' \models (X_{\text{Person}}. \text{oclIsNew}()) \)

(proof)

(proof)

(proof)

(proof)

(proof)

(proof)

(proof)

(proof)

lemma \( \sigma, \sigma' \models \text{oclIsModifiedOnly}() \)

(proof)

lemma \( \sigma, \sigma' \models (\text{Set} \{ X_{\text{Person}}. \text{oclAsType}(\text{OclAny}) \}) \)

(proof)

lemma \( \sigma, \sigma' \models ((X_{\text{Person}}. \text{oclAsType}(\text{OclAny}) \triangleq X_{\text{Person}}) @ \text{pre}) \)

(proof)

lemma \( \sigma, \sigma' \models ((X_{\text{Person}}. \text{oclAsType}(\text{OclAny}) @ \text{post}) \)

(proof)

lemma \( \sigma, \sigma' \models (X_{\text{Person}}. \text{oclAsType}(\text{OclAny}) @ \text{pre}) \)

(proof)

lemma \( \sigma, \sigma' \models ((X_{\text{Person}}. \text{oclAsType}(\text{OclAny}) @ \text{post}) \)

(proof)

lemma 162
\[((\text{Person}9 \cdot \text{oclAsType}(\text{OclAny})) @ \text{post} (\lambda x. \_\cdot \text{OclAsType} \text{OclAny} \cdot \exists x))\]

\langle proof \rangle

\text{lemma perm-} \sigma_1' : \sigma_1' = (\assoc \equiv \text{Map.empty} \\
(\text{oid}8 \mapsto \text{inPerson} \text{person}9) \\
(\text{oid}7 \mapsto \text{inOclAny} \text{person}8) \\
(\text{oid}6 \mapsto \text{inOclAny} \text{person}7) \\
(\text{oid}5 \mapsto \text{inPerson} \text{person}6) \\
\text{\ldots} \\
(\text{oid}3 \mapsto \text{inPerson} \text{person}4) \\
(\text{oid}2 \mapsto \text{inPerson} \text{person}3) \\
(\text{oid}1 \mapsto \text{inPerson} \text{person}2) \\
(\text{oid}0 \mapsto \text{inPerson} \text{person}1) \\
, \text{assocs = assocs } \sigma_1' \rangle

\langle proof \rangle

\text{declare const-s} [\text{simp}]

\text{lemma } \bigwedge \sigma_1. \\
(\sigma_1, \sigma_1') \models (\text{Person}.\text{allInstances}) \equiv \text{Set}\{ \text{Person}1, \text{Person}2, \text{Person}3, \text{Person}4, \text{Person}5, \text{Person}6, \text{Person}7, \text{Person}8, \text{Person}9\}

\langle proof \rangle

\text{lemma } \bigwedge \sigma_1. \\
(\sigma_1, \sigma_1') \models (\text{OclAny}.\text{allInstances}) \equiv \text{Set}\{ \text{Person}1 \cdot \text{oclAsType}(\text{OclAny}), \text{Person}2 \cdot \text{oclAsType}(\text{OclAny}), \text{Person}3 \cdot \text{oclAsType}(\text{OclAny}), \text{Person}4 \cdot \text{oclAsType}(\text{OclAny}), \text{Person}5, \text{Person}6 \cdot \text{oclAsType}(\text{OclAny}), \text{Person}7, \text{Person}8, \text{Person}9 \cdot \text{oclAsType}(\text{OclAny})\}

\langle proof \rangle

\text{end}

\text{theory} \ 
\text{Analysis-OCL}

\text{imports} \ 
\text{Analysis-UML}

\text{begin}

\textbf{4.10. OCL Part: Invariant}

These recursive predicates can be defined conservatively by greatest fix-point constructions—automatically. See [4, 6] for details. For the purpose of this example, we state them as axioms here.

\begin{verbatim}
context Person
  inv label : self . boss <> null implies (self . salary \<le> ((self . boss) . salary))

definition Person-label_{inv} :: Person \Rightarrow Boolean
where  Person-label_{inv} (self) \equiv 
  (self . boss <> null implies (self . salary \leq \text{int} ((self . boss) . salary)))

definition Person-label_{invATpre} :: Person \Rightarrow Boolean
where  Person-label_{invATpre} (self) \equiv 
  (self . boss@pre <> null implies (self . salary@pre \leq \text{int} ((self . boss@pre) . salary@pre)))
\end{verbatim}

163
\textbf{definition} \ Person-label_{globalInv} :: Boolean \\
\textbf{where} \hspace{1em} \ Person-label_{globalInv} \equiv (\text{Person} \ \text{allInstances}() \rightarrow \text{forAllSet}(x \mid \text{Person-label}_{inv}(x)) \text{ and} \text{ (Person} \ \text{allInstances}_{pre}() \rightarrow \text{forAllSet}(x \mid \text{Person-label}_{invATprech}(x))) \\

\textbf{lemma} \ \tau \models \delta \ (X \ . \text{boss}) \Rightarrow \tau \models \text{Person} \ . \text{allInstances}() \rightarrow \text{includesSet}(X \ . \text{boss}) \text{ and} \tau \models \text{Person} \ . \text{allInstances}() \rightarrow \text{includesSet}(X) \\
\textbf{(proof)} \\

\textbf{lemma} \ \text{REC-pre} : \ \tau \models \text{Person-label}_{globalInv} \\
\Rightarrow \tau \models \text{Person} \ . \text{allInstances}() \rightarrow \text{includesSet}(X) \Leftarrow X \text{ represented object in state} \\
\Rightarrow \exists \text{REC}. \ \tau \models \text{REC}(X) \equiv (\text{Person-label}_{inv}(X) \text{ and} (X \ . \text{boss} <> \text{null} \text{ implies} \text{REC}(X \ . \text{boss}))) \\
\textbf{(proof)} \\

This allows to state a predicate: \\
\textbf{axiomatization} \ \text{invPerson-label} :: \text{Person} \Rightarrow \text{Boolean} \\
\textbf{where} \ \text{invPerson-label}_{def} : \\
(\tau \models \text{Person} \ . \text{allInstances}() \rightarrow \text{includesSet}(self)) \Rightarrow \\
(\tau \models \text{invPerson-label}(self)) \equiv (self \ . \text{boss} <> \text{null} \text{ implies} \\
\text{(self} \ . \text{salary} \leq_{\text{int}} ((\text{self} \ . \text{boss}) \ . \text{salary}) \text{ and} \text{invPerson-label}(self \ . \text{boss})))) \\

\textbf{axiomatization} \ \text{invPerson-label}_{ATprech} :: \text{Person} \Rightarrow \text{Boolean} \\
\textbf{where} \ \text{invPerson-label}_{ATprech}_{def} : \\
(\tau \models \text{Person} \ . \text{allInstances}_{pre}() \rightarrow \text{includesSet}(self)) \Rightarrow \\
(\tau \models \text{invPerson-label}_{ATprech}(self)) \equiv (self \ . \text{boss}_{pre} <> \text{null} \text{ implies} \\
\text{(self} \ . \text{salary}_{pre} \leq_{\text{int}} ((\text{self} \ . \text{boss}_{pre}) \ . \text{salary}_{pre}) \text{ and} \text{invPerson-label}_{ATprech}(self \ . \text{boss}_{pre})))) \\

\textbf{lemma} \ \text{inv-1} : \\
(\tau \models \text{Person} \ . \text{allInstances}() \rightarrow \text{includesSet}(self)) \Rightarrow \\
(\tau \models \text{invPerson-label}(self)) = ((\tau \models (self \ . \text{boss} \equiv \text{null})) \lor \\
(\tau \models (self \ . \text{boss} <> \text{null}) \land \\
\tau \models ((self \ . \text{salary} \leq_{\text{int}} (self \ . \text{boss} \ . \text{salary})) \land \\
\tau \models \text{invPerson-label}(self \ . \text{boss})))) \\
\textbf{(proof)} \\

\textbf{lemma} \ \text{inv-2} : \\
(\tau \models \text{Person} \ . \text{allInstances}_{pre}() \rightarrow \text{includesSet}(self)) \Rightarrow \\
(\tau \models \text{invPerson-label}_{ATprech}(self)) = ((\tau \models (self \ . \text{boss}_{prech} \equiv \text{null})) \lor \\
(\tau \models (self \ . \text{boss}_{prech} <> \text{null}) \land \\
(\tau \models (self \ . \text{boss}_{prech} \ . \text{salary}_{prech} \leq_{\text{int}} \text{self} \ . \text{salary}_{prech})) \land \\
(\tau \models \text{invPerson-label}_{ATprech}(self \ . \text{boss}_{prech})))) \\
\textbf{(proof)} \\

A very first attempt to characterize the axiomatization by an inductive definition - this can not be 
the last word since too weak (should be equality!) \\
\textbf{coinductive} \ \text{inv} :: \text{Person} \Rightarrow (\exists \delta) \text{st} \Rightarrow \text{bool} \text{ where} \\
(\tau \models \delta \ \text{self}) \Rightarrow (\tau \models (self \ . \text{boss} \equiv \text{null}) \lor \\
(\tau \models (self \ . \text{boss} <> \text{null}) \land (\tau \models (self \ . \text{boss} \ . \text{salary} \leq_{\text{int}} \text{self} \ . \text{salary})))) \land \\
(\text{inv}(self \ . \text{boss}) \tau )) \\
\Rightarrow (\text{inv self} \ \tau )
4.11. OCL Part: The Contract of a Recursive Query

The original specification of a recursive query:

\[
\text{context } \text{Person}::\text{contents}() : \text{Set}() \text{Integer)
\]
\[
\text{pre: } \text{true}
\]
\[
\text{post: } \text{result } = \text{if } \text{self.boss } = \text{null}
\]
\[
\text{then } \text{Set(i)}
\]
\[
\text{else } \text{self.boss.contents()} \rightarrow \text{including(i)}
\]
\[
\text{endif}
\]

For the case of recursive queries, we use at present just axiomatizations:

axiomatization \text{contents} : \text{Person } \Rightarrow \text{Set}-\text{Integer } ((\lambda(\text{-} -\text{contents}()) 50)

\text{where contents-def:}
\[
(\text{self} .\text{contents}()) = (\lambda \text{. res} . \text{let res } = \lambda \text{- res in}
\]
\[
\text{if } \tau \vdash (\delta \text{ self})
\]
\[
\text{then } ((\tau \vdash \text{true}) \land
\]
\[
(\tau \vdash \text{res } \triangleq \text{if } (\text{self} .\text{boss } \hat{=} \text{null})
\]
\[
\text{then } (\text{Set}(\text{self}.\text{salary}))
\]
\[
\text{else } (\text{self} .\text{boss}.\text{contents}())
\]
\[
\rightarrow \text{includingSet}(\text{self}.\text{salary})
\]
\[
\text{endif})
\]
\[
\text{else } \tau \vdash \text{res } \triangleq \text{invalid}
\]
\[
\text{and } \text{cp0-contents}(X .\text{contents}()) \tau = ((\lambda X \tau .\text{contents}()) \tau
\]

interpretation \text{contents} : \text{contract}\text{0 contents } \lambda \text{ self}. \text{true}
\[
\lambda \text{ self}. \text{ res } \triangleq \text{if } (\text{self} .\text{boss } \hat{=} \text{null})
\]
\[
\text{then } (\text{Set}(\text{self}.\text{salary}))
\]
\[
\text{else } (\text{self} .\text{boss}.\text{contents}())
\]
\[
\rightarrow \text{includingSet}(\text{self}.\text{salary})
\]
\[
\text{endif}
\]

\text{proof}

Specializing \boxed{cp E; \tau \vdash \delta \text{ self}; \tau \vdash \text{true}; \tau \vdash \text{POST'} \text{ self}; \Lambda \text{res. (res } \triangleq \text{if } \text{self.boss } \hat{=} \text{null then Set}(\text{self}.\text{salary}) \text{ else self.boss.contents}() \rightarrow \text{includingSet}(\text{self}.\text{salary}) \text{ endif}) = (\text{POST'} \text{ self and (res } \triangleq \text{BODY self)})} \quad \Rightarrow \quad \tau \vdash \text{E} (\text{self}.\text{contents}()) = (\tau \vdash \text{E} (\text{BODY self}))

\text{one gets the following more practical rewrite rule that is amenable to symbolic evaluation:}

\text{theorem unfold-contents :}
\[
\text{assumes cp E}
\]
\[
\text{and } \tau \vdash \delta \text{ self}
\]
\[
\text{shows } (\tau \vdash \text{E} (\text{self}.\text{contents}()) =
\]
\[
(\tau \vdash \text{E} (\text{if } \text{self} .\text{boss } \hat{=} \text{null}
\]
\[
\text{then Set}(\text{self}.\text{salary})
\]
\[
\text{else self.boss.contents()} \rightarrow \text{includingSet}(\text{self}.\text{salary}) \text{ endif}))
\]

\text{proof}

Since we have only one interpretation function, we need the corresponding operation on the pre-state:

\text{consts contentsATpre :: Person } \Rightarrow \text{Set-Integer } ((1(-).\text{contents}@\text{pre'}()) 50)

axiomatization \text{where contentsATpre-def:}
\[
(\text{self}.\text{contents}@\text{pre}()) = (\lambda . \tau.
\]
\[
\text{SOME res. let res } = \lambda -. \text{res in}
\]
\[
\text{if } \tau \vdash (\delta \text{ self})
\]
\[
\text{then } ((\tau \vdash \text{true}) \land
\]
\[
(\tau \vdash \text{res } \triangleq \text{if } (\text{self}.\text{boss}@\text{pre } \hat{=} \text{null})
\]
\[
\text{-- pre}
\]
\[
\text{then Set}(\text{self}.\text{salary}@\text{pre})
\]
\[
\text{else } (\text{self}.\text{boss}@\text{pre}.\text{contents}@\text{pre}())
\]

\text{165}
\[
\text{\texttt{contents@pre} : contract0 contents@pre \chi self. true}
\]
\[
\lambda \text{self res. res} \triangleq \text{if (self .boss@pre} = \text{null)}
\]
\[
\text{then (Set\{self .salary@pre\})}
\]
\[
\text{else (self .boss@pre .contents@pre(} \rightarrow \text{including}_{S_{ext}}(\text{self .salary@pre})\text{))}
\]
\[
\text{endif}
\]

⟨proof⟩

Again, we derive via \texttt{contents.unfold2} a Knaster-Tarski like Fixpoint rule that is amenable to symbolic evaluation:

\textbf{theorem unfold-contents@pre} :

\textbf{assumes} \texttt{cp E}

\textbf{and} \( \tau \models \delta \text{ self} \)

\textbf{shows} \( (\tau \models E (\text{self .contents@pre}())) = \)
\[
(\tau \models E (\text{if self .boss@pre} = \text{null)} \text{ then Set\{self .salary@pre\}}
\]
\[
\text{else self .boss@pre .contents@pre(} \rightarrow \text{including}_{S_{ext}}(\text{self .salary@pre})\text{))}
\]

⟨proof⟩

Note that these \texttt{@pre} variants on methods are only available on queries, i.e., operations without side-effect.

\section{4.12. OCL Part: The Contract of a User-defined Method}

The example specification in high-level OCL input syntax reads as follows:

\textbf{context} \texttt{Person::insert(x: Integer)}

\textbf{pre:} true

\textbf{post:} \texttt{contents(): Set(Integer) contents() = contents@pre() \rightarrow including(x)}

This boils down to:

\textbf{definition} \texttt{insert ::= Person => Integer => Void)((1(-).insert(-') 50)}

\textbf{where} \texttt{self .insert(x) \equiv}
\[
(\lambda \tau. \text{SOME res. let res} = \chi \tau. \text{ res in}
\]
\[
\text{if } (\tau \models (\delta \text{ self})) \land (\tau \models v x)
\]
\[
\text{then } (\tau \models \text{true} \land
\]
\[
(\tau \models (((\text{self.contents()} \triangleq (\text{self.contents@pre()} \rightarrow \text{including}_{S_{ext}}(x)))))
\]
\[
\text{else } \tau \models \text{res} \triangleq \text{invalid})
\]

The semantic consequences of this definition were computed inside this locale interpretation:

\textbf{interpretation} \texttt{insert : contract1 insert \chi self x. true}
\[
\lambda \text{self x res. ((self .contents())} \triangleq \)
\[
(\text{self .contents@pre()} \rightarrow \text{including}_{S_{ext}}(x)))
\]

⟨proof⟩

The result of this locale interpretation for our \texttt{Analysis-OCL.insert} contract is the following set of properties, which serves as basis for automated deduction on them:

\textbf{end}
<table>
<thead>
<tr>
<th>Name</th>
<th>Theorem</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>insert.strict0</code></td>
<td>((\text{invalid}. \text{insert}(X)) = \text{invalid})</td>
</tr>
<tr>
<td><code>insert.nullstrict0</code></td>
<td>((\text{null}. \text{insert}(X)) = \text{invalid})</td>
</tr>
<tr>
<td><code>insert.strict1</code></td>
<td>((\text{self}. \text{insert}(\text{invalid})) = \text{invalid})</td>
</tr>
<tr>
<td><code>insert.cppRE</code></td>
<td>(\text{true} \tau = \text{true} \tau)</td>
</tr>
<tr>
<td><code>insert.cppPOST</code></td>
<td>((\text{self}. \text{contents}() \triangleq \text{self}. \text{contents}@\text{pre}() \rightarrow \text{including}@\text{Set}(a1.0)) \tau = (\lambda.\ \text{self}. \text{contents}() \triangleq \lambda.\ \text{self}. \text{contents}@\text{pre}() \rightarrow \text{including}@\text{Set}(\lambda.\ a1.0 \ \tau)) \tau)</td>
</tr>
<tr>
<td><code>insert.cp-pre</code></td>
<td>([\text{cp} \ \text{self}'; \ \text{cp a1'}; \ \text{cp res}] \rightarrow \text{cp} (\lambda X. \ \text{self}' X. \text{contents}() \triangleq \text{self}' X. \text{contents}@\text{pre}() \rightarrow \text{including}@\text{Set}(a1'. X)))</td>
</tr>
<tr>
<td><code>insert.cp-post</code></td>
<td>([\text{cp} \ \text{self}'; \ \text{cp a1'}; \ \text{cp res}] \rightarrow \text{cp} (\lambda X. \ \text{self}' X. \text{insert}(a1' X)))</td>
</tr>
<tr>
<td><code>insert.cp0</code></td>
<td>((\text{self}.\text{insert}(a1.0)) \tau = (\lambda.\ \text{self}. \text{insert}(\lambda.\ a1.0 \ \tau)) \tau)</td>
</tr>
<tr>
<td><code>insert.def-scheme</code></td>
<td>(\text{self}.\text{insert}(a1.0) \equiv \lambda \tau. \ \text{SOME} \ \text{res}. \ \text{let} \ \text{res} = \lambda.\ \text{res} \ \text{in} \ \text{if} \ \tau \triangleright \delta \ \text{self} \ \land \ \tau \triangleright \nu \ \text{a1.0} \ \text{then} \ \tau \triangleright \ \text{true} \ \land \ \tau \triangleright \ \text{self}. \text{contents}() \triangleq \text{self}. \text{contents}@\text{pre}() \rightarrow \text{including}@\text{Set}(a1.0) \ \text{else} \ \tau \triangleright \ \text{res} \triangleq \text{invalid} )</td>
</tr>
<tr>
<td><code>insert.unfold</code></td>
<td>([\text{cp} \ \text{E}; \ \tau \triangleright \delta \ \text{self} \ \land \ \tau \triangleright \nu \ a1.0; \ \tau \triangleright \ \text{true}; \ \exists \ \text{res}. \ \tau \triangleright \ \text{self}. \text{contents}() \triangleq \text{self}. \text{contents}@\text{pre}() \rightarrow \text{including}@\text{Set}(a1.0); \ \land \ \text{res}. \ \tau \triangleright \ \text{self}. \text{contents}() \triangleq \text{self}. \text{contents}@\text{pre}() \rightarrow \text{including}@\text{Set}(a1.0) \rightarrow \tau \triangleright \ E (\lambda.\ \text{res})] \rightarrow \tau \triangleright \ E (\text{self}.\text{insert}(a1.0)))</td>
</tr>
<tr>
<td><code>insert.unfold2</code></td>
<td>([\text{cp} \ \text{E}; \ \tau \triangleright \delta \ \text{self} \ \land \ \tau \triangleright \nu \ a1.0; \ \tau \triangleright \ \text{true}; \ \tau \triangleright \ \text{POST}' \ \text{self} a1.0; \ \land \ \text{res}. \ \left(\text{self}. \text{contents}() \triangleq \text{self}. \text{contents}@\text{pre}() \rightarrow \text{including}@\text{Set}(a1.0)\right) = \left(\text{POST}' \ \text{self} a1.0 \ \text{and} \ \left(\text{res} \triangleq \text{BODY} \ \text{self} a1.0\right)\right) \rightarrow (\tau \triangleright \ E (\text{self}.\text{insert}(a1.0))) = (\tau \triangleright \ E (\text{BODY} \ \text{self} a1.0)))</td>
</tr>
</tbody>
</table>

Table 4.1.: Semantic properties resulting from a user-defined operation contract.
5. Example: The Employee Design Model

theory
  Design-UML
imports
  ../../../UML-Main
begin

5.1. Introduction

For certain concepts like classes and class-types, only a generic definition for its resulting semantics can be given. Generic means, there is a function outside HOL that “compiles” a concrete, closed-world class diagram into a “theory” of this data model, consisting of a bunch of definitions for classes, accessors, method, casts, and tests for actual types, as well as proofs for the fundamental properties of these operations in this concrete data model.

Such generic function or “compiler” can be implemented in Isabelle on the ML level. This has been done, for a semantics following the open-world assumption, for UML 2.0 in [4, 7]. In this paper, we follow another approach for UML 2.4: we define the concepts of the compilation informally, and present a concrete example which is verified in Isabelle/HOL.

5.1.1. Outlining the Example

We are presenting here a “design-model” of the (slightly modified) example Figure 7.3, page 20 of the OCL standard [32]. To be precise, this theory contains the formalization of the data-part covered by the UML class model (see Figure 5.1):

This means that the association (attached to the association class EmployeeRanking) with the association ends boss and employees is implemented by the attribute boss and the operation employees (to be discussed in the OCL part captured by the subsequent theory).

5.2. Example Data-Universe and its Infrastructure

Ideally, the following is generated automatically from a UML class model.

---

Figure 5.1.: A simple UML class model drawn from Figure 7.3, page 20 of [32].
Our data universe consists in the concrete class diagram just of node’s, and implicitly of the class object. Each class implies the existence of a class type defined for the corresponding object representations as follows:

```haskell
datatype typePerson = mkPerson oid
                int option
                oid option

datatype typeOclAny = mkOclAny oid
                (int option × oid option) option
```

Now, we construct a concrete “universe of OclAny types” by injection into a sum type containing the class types. This type of OclAny will be used as instance for all respective type-variables.

```haskell
datatype Ξ = inPerson typePerson | inOclAny typeOclAny
```

Having fixed the object universe, we can introduce type synonyms that exactly correspond to OCL types. Again, we exploit that our representation of OCL is a “shallow embedding” with a one-to-one correspondance of OCL-types to types of the meta-language HOL.

```haskell
type-synonym Boolean = Ξ Boolean

type-synonym Integer = Ξ Integer

type-synonym Void = Ξ Void

type-synonym OclAny = (Ξ, typeOclAny option option) val

type-synonym Person = (Ξ, typePerson option option) val

type-synonym Set-Integer = (Ξ, int option option) Set

type-synonym Set-Person = (Ξ, typePerson option option) Set
```

Just a little check:

```haskell
typ Boolean
```

To reuse key-elements of the library like referential equality, we have to show that the object universe belongs to the type class “oclany,” i.e., each class type has to provide a function oid-of yielding the object id (oid) of the object.

```haskell
instantiation typePerson :: object
begin
    definition oid-of-typePerson-def: oid-of x = (case x of mkPerson oid - - ⇒ oid)
    instance ⟨proof⟩
end

instantiation typeOclAny :: object
begin
    definition oid-of-typeOclAny-def: oid-of x = (case x of mkOclAny oid option option - ⇒ oid)
    instance ⟨proof⟩
end

instantiation Ξ :: object
begin
    definition oid-of-Ξ-def: oid-of x = (case x of
                      inPerson person ⇒ oid-of person
                      | inOclAny oclany ⇒ oid-of oclany)
    instance ⟨proof⟩
end
```

### 5.3. Instantiation of the Generic Strict Equality

We instantiate the referential equality on `Person` and `OclAny`
overloading \textit{StrictRefEq} \equiv \textit{StrictRefEq} : [\textit{Person,Person}] \Rightarrow \text{Boolean}

\textbf{definition} \textit{StrictRefEq}_{\textit{Object-Person}} : (x::\textit{Person}) \preceq y \equiv \textit{StrictRefEq}_{\textit{Object}} x y

overloading \textit{StrictRefEq} \equiv \textit{StrictRefEq} : [\textit{OclAny,OclAny}] \Rightarrow \text{Boolean}

\textbf{definition} \textit{StrictRefEq}_{\textit{Object-OclAny}} : (x::\textit{OclAny}) \preceq y \equiv \textit{StrictRefEq}_{\textit{Object}} x y

\textbf{lemmas} \textit{cps23} =
- \textit{cp-StrictRefEq}_{\textit{Object-}\textit{Person}} [\textit{of x::}\textit{Person} y::\textit{Person} \tau, simplified \textit{StrictRefEq}_{\textit{Object-Person}} [\textit{symmetric}]]
- \textit{cp-intro} (9) [\textit{of} \textit{P::Person} \Rightarrow \textit{PersonQ::Person} \Rightarrow \textit{Person}, simplified \textit{StrictRefEq}_{\textit{Object-Person}} [\textit{symmetric}]]
- \textit{StrictRefEq}_{\textit{Object-def}} [\textit{of x::}\textit{Person} y::\textit{Person}, simplified \textit{StrictRefEq}_{\textit{Object-Person}} [\textit{symmetric}]]
- \textit{StrictRefEq}_{\textit{Object-defargs}} [\textit{of} \textit{- x::}\textit{Person} y::\textit{Person}, simplified \textit{StrictRefEq}_{\textit{Object-Person}} [\textit{symmetric}]]
- \textit{StrictRefEq}_{\textit{Object-strict1}} [\textit{of} \textit{x::}\textit{Person}, simplified \textit{StrictRefEq}_{\textit{Object-Person}} [\textit{symmetric}]]
- \textit{StrictRefEq}_{\textit{Object-strict2}} [\textit{of} \textit{x::}\textit{Person}, simplified \textit{StrictRefEq}_{\textit{Object-Person}} [\textit{symmetric}]]

\textbf{for} \textit{x y \tau P Q}

For each Class \textit{C}, we will have a casting operation \texttt{.oclAsType\textit{(C)}}, a test on the actual type \texttt{.oclIsTypeOf\textit{(C)}} as well as its relaxed form \texttt{.oclIsKindOf\textit{(C)}} (corresponding exactly to Java’s \texttt{instanceof}-operator.

Thus, since we have two class-types in our concrete class hierarchy, we have two operations to declare and to provide two overloading definitions for the two static types.

\section{5.4. \texttt{OclAsType}}

\subsection{5.4.1. \textbf{Definition}}

\textbf{consts} \texttt{OclAsType\texttt{\_OclAny}} :: 'a \Rightarrow \texttt{OclAny} ((\textlangle \cdot \rangle .\texttt{oclAsType'}\texttt{(OclAny'))})

\textbf{consts} \texttt{OclAsType\texttt{\_Person}} :: 'a \Rightarrow \texttt{Person} ((\textlangle \cdot \rangle .\texttt{oclAsType'}\texttt{(Person'))})

\textbf{definition} \texttt{OclAsType\texttt{\_OclAny\texttt{-}\_A}} = (\lambda u . \texttt{case u of in\texttt{OclAny} a \Rightarrow a} | \texttt{in\texttt{Person} (mk\texttt{\_Person oid a b}) \Rightarrow mk\texttt{\_OclAny} oid (\langle a, b \rangle)>)

\textbf{lemma} \texttt{OclAsType\texttt{\_OclAny\texttt{-}\_A\_some}}: \texttt{OclAsType\texttt{\_OclAny\texttt{-}\_A}} \texttt{x \neq None}

\textbf{overloading} \texttt{OclAsType\texttt{\_OclAny}} \equiv \texttt{OclAsType\texttt{\_OclAny}} :: \texttt{OclAny} \Rightarrow \texttt{OclAny}

\textbf{definition} \texttt{OclAsType\texttt{\_OclAny\texttt{-}\_OclAny}}: \texttt{(X::OclAny) .\texttt{oclAsType\texttt{(OclAny)}}} \equiv X

\textbf{end}

\textbf{overloading} \texttt{OclAsType\texttt{\_OclAny}} \equiv \texttt{OclAsType\texttt{\_OclAny}} :: \texttt{Person} \Rightarrow \texttt{OclAny}

\textbf{definition} \texttt{OclAsType\texttt{\_OclAny\texttt{-}\_Person}}: \texttt{(X::Person) .\texttt{oclAsType\texttt{(OclAny)}}} \equiv
\(\lambda \tau. \text{case } X \tau \text{ of}
\)
\[
\begin{align*}
& \bot \Rightarrow \text{invalid } \tau \\
& \underline{\bot} \Rightarrow \text{null } \tau \\
& \underline{\mu} \text{mkPerson oid a b} \Rightarrow \underline{\mu} \text{ (mkOclAny oid ((a,b)_\bot))}
\end{align*}
\]

end

definition \(\text{OclAsTypePerson-\AA} = \)
\(\lambda u. \text{case } u \text{ of inPerson } p \Rightarrow \) \(\mu p_j
\)
\[
\begin{align*}
& \text{inOclAny (mkOclAny oid ((a,b)_\bot)) } \Rightarrow \mu \text{mkPerson oid a b}_j \\
& - \Rightarrow \text{None}
\end{align*}
\]
overloading \(\text{OclAsTypePerson} \equiv \text{OclAsTypePerson} :: \text{OclAny } \Rightarrow \text{Person}
\]
begin

definition \(\text{OclAsTypePerson-OclAny} : (X::\text{OclAny}) . \text{oclAsType}(\text{Person}) \equiv \)
\[
\begin{align*}
& \lambda \tau. \text{case } X \tau \text{ of}
& \bot \Rightarrow \text{invalid } \tau \\
& \underline{\bot} \Rightarrow \text{null } \tau \\
& \underline{\mu} \text{mkOclAny oid } \underline{\bot} \Rightarrow \text{invalid } \tau \quad \text{— down-cast exception}
& \underline{\mu} \text{mkOclAny oid ((a,b)_\bot)} \Rightarrow \underline{\mu} \text{mkPerson oid a b}_j
\end{align*}
\]
end

overloading \(\text{OclAsTypePerson} \equiv \text{OclAsTypePerson} :: \text{Person } \Rightarrow \text{Person}
\]
begin

definition \(\text{OclAsTypePerson-Person} : (X::\text{Person}) . \text{oclAsType}(\text{Person}) \equiv X
\]
endlemmas \([\text{simpl} = \)
\(\text{OclAsTypeOclAny-OclAny}
\)
\(\text{OclAsTypePerson-Person}
\]

5.4.2. Context Passing

lemma \(\text{cp-OclAsTypeOclAny-Person-Person} : \text{cp } P \Rightarrow \text{cp}(\lambda X. (P (X::\text{Person})::\text{Person}) . \text{oclAsType}(\text{OclAny}))
\)
(proof)

lemma \(\text{cp-OclAsTypeOclAny-OclAny-OclAny} : \text{cp } P \Rightarrow \text{cp}(\lambda X. (P (X::\text{OclAny})::\text{OclAny}) . \text{oclAsType}(\text{OclAny}))
\)
(proof)

lemma \(\text{cp-OclAsTypePerson-Person-Person} : \text{cp } P \Rightarrow \text{cp}(\lambda X. (P (X::\text{Person})::\text{Person}) . \text{oclAsType}(\text{Person}))
\)
(proof)

lemma \(\text{cp-OclAsTypeOclAny-OclAny-OclAny} : \text{cp } P \Rightarrow \text{cp}(\lambda X. (P (X::\text{OclAny})::\text{OclAny}) . \text{oclAsType}(\text{OclAny}))
\)
(proof)

lemma \(\text{cp-OclAsTypePerson-Person-OclAny} : \text{cp } P \Rightarrow \text{cp}(\lambda X. (P (X::\text{Person})::\text{OclAny}) . \text{oclAsType}(\text{OclAny}))
\)
(proof)

lemma \(\text{cp-OclAsTypePerson-Person-OclAny} : \text{cp } P \Rightarrow \text{cp}(\lambda X. (P (X::\text{Person})::\text{OclAny}) . \text{oclAsType}(\text{OclAny}))
\)
(proof)

lemma \(\text{cp-OclAsTypePerson-Person-OclAny} : \text{cp } P \Rightarrow \text{cp}(\lambda X. (P (X::\text{Person})::\text{OclAny}) . \text{oclAsType}(\text{Person}))
\)
(proof)

lemma \(\text{cp-OclAsTypePerson-OclAny-Person} : \text{cp } P \Rightarrow \text{cp}(\lambda X. (P (X::\text{OclAny})::\text{Person}) . \text{oclAsType}(\text{Person}))
\)
(proof)

lemmas \([\text{simpl} = \)
\(\text{cp-OclAsTypeOclAny-Person-Person}
\)
\(\text{cp-OclAsTypeOclAny-OclAny-OclAny}
\)
\(\text{cp-OclAsTypePerson-Person-Person}
\)
\(\text{cp-OclAsTypeOclAny-OclAny-OclAny}
\)
\(\text{cp-OclAsTypePerson-OclAny-OclAny}
\)

172
5.4.3. Execution with Invalid or Null as Argument

Lemma \textit{OclAsTypeOclAny-OclAny-strict} (\textit{invalid::OclAny}). \textit{oclAsType(OclAny)} = \textit{invalid} (\textit{proof})

Lemma \textit{OclAsTypeOclAny-OclAny-nullstrict} (\textit{null::OclAny}). \textit{oclAsType(OclAny)} = \textit{null} (\textit{proof})

Lemma \textit{OclAsTypePerson-Person-strict} (\textit{invalid::Person}). \textit{oclAsType(Person)} = \textit{invalid} (\textit{proof})

Lemma \textit{OclAsTypePerson-Person-nullstrict} (\textit{null::Person}). \textit{oclAsType(Person)} = \textit{null} (\textit{proof})

5.5. \textit{OclIsTypeOf}

5.5.1. Definition

\textit{consts} \textit{OclIsTypeOfOclAny} :: \textit{α} ⇒ Boolean ((\textit{-}).\textit{oclIsTypeOf('OclAny')})

\textit{consts} \textit{OclIsTypeOfPerson} :: \textit{α} ⇒ Boolean ((\textit{-}).\textit{oclIsTypeOf('Person')})

\textit{overloading} \textit{OclIsTypeOfOclAny} ≡ \textit{OclIsTypeOfOclAny} :: \textit{OclAny} ⇒ Boolean begin

definition \textit{OclIsTypeOfOclAny-OclAny}:
(X::OclAny).\textit{oclIsTypeOf}(OclAny) ≡
(\lambda \tau. case X \tau of
   \bot ⇒ invalid \tau
   | \bot ⇒ true \tau − invalid ?
   | \textit{mkOclAny oid \bot} ⇒ true \tau
   | \textit{mkOclAny oid \bot} ⇒ false \tau)

end

Lemma \textit{OclIsTypeOfOclAny-OclAny'}:
(X::OclAny).\textit{oclIsTypeOf}(OclAny) =
(\lambda \tau. if \tau \models X then case X \tau of
   \bot ⇒ true \tau − invalid ?
   | \textit{mkOclAny oid \bot} ⇒ true \tau
   | \textit{mkOclAny oid \bot} ⇒ false \tau
   else invalid \tau)

\textit{⟨proof⟩}

\textit{interpretation} \textit{OclIsTypeOfOclAny-OclAny}:
\textit{profile-mono-schemeV}
\textit{OclIsTypeOfOclAny::OclAny ⇒ Boolean}
\lambda X. (case X of
   \textit{None} ⇒ \textit{True}
   | \textit{mkOclAny oid None} ⇒ \textit{True}
   | \textit{mkOclAny oid \bot} ⇒ \textit{False})

\textit{⟨proof⟩}

\textit{overloading} \textit{OclIsTypeOfOclAny} ≡ \textit{OclIsTypeOfOclAny} :: \textit{Person} ⇒ Boolean begin
overloading OclIsTypeOfPerson ≡ OclIsTypeOfPerson :: OclAny ⇒ Boolean
begin
  definition OclIsTypeOfPerson(OclAny)

  begin
    definition OclIsTypeOfPerson(OclAny):  

begin

  end

end

5.5.2. Context Passing

lemma cp-OclIsTypeOfOclAny-Person-Person: cp P =⇒ cp(X.(P(X::Person)::Person).oclIsTypeOf(OclAny)) (proof)

lemma cp-OclIsTypeOfOclAny-OclAny-OclAny: cp P =⇒ cp(X.(P(X::OclAny)::OclAny).oclIsTypeOf(OclAny)) (proof)

lemma cp-OclIsTypeOfOclAny-Person-Person: cp P =⇒ cp(X.(P(X::Person)::Person).oclIsTypeOf(OclAny)) (proof)

lemma cp-OclIsTypeOfPerson-OclAny: cp P =⇒ cp(X.(P(X::OclAny)::Person).oclIsTypeOf(Person)) (proof)

lemma cp-OclIsTypeOfPerson-Person-OclAny: cp P =⇒ cp(X.(P(X::Person)::Person).oclIsTypeOf(Person)) (proof)

lemma cp-OclIsTypeOfPerson-Person-Person: cp P =⇒ cp(X.(P(X::Person)::Person).oclIsTypeOf(Person)) (proof)

lemmas [simp] = 
  cp-OclIsTypeOfOclAny-Person-Person 
  cp-OclIsTypeOfOclAny-OclAny-OclAny 
  cp-OclIsTypeOfPerson-Person-Person 
  cp-OclIsTypeOfPerson-OclAny-OclAny

174
5.5.3. Execution with Invalid or Null as Argument

lemma OclIsTypeOfOclAny-OclAny-strict1[simp]:
  (invalid::OclAny) .oclIsTypeOf(OclAny) = invalid
⟨proof⟩

lemma OclIsTypeOfOclAny-OclAny-strict2[simp]:
  (null::OclAny) .oclIsTypeOf(OclAny) = true
⟨proof⟩

lemma OclIsTypeOfPerson-OclAny-strict1[simp]:
  (invalid::Person) .oclIsTypeOf(Person) = invalid
⟨proof⟩

lemma OclIsTypeOfPerson-OclAny-strict2[simp]:
  (null::Person) .oclIsTypeOf(Person) = true
⟨proof⟩

lemma OclIsTypeOfPerson-Person-strict1[simp]:
  (invalid::Person) .oclIsTypeOf(Person) = invalid
⟨proof⟩

lemma OclIsTypeOfPerson-Person-strict2[simp]:
  (null::Person) .oclIsTypeOf(Person) = true
⟨proof⟩

5.5.4. Up Down Casting

lemma actualType-larger-staticType:
assumes isdef: τ ⊨ (δ X)
shows τ ⊨ (X::Person) .oclIsTypeOf(OclAny) ≜ false
⟨proof⟩

lemma down-cast-type:
assumes isOclAny: τ ⊨ (X::OclAny) .oclIsTypeOf(OclAny)
and non-null: τ ⊨ (δ X)
shows τ ⊨ (X .oclAsType(Person)) ≜ invalid
⟨proof⟩

lemma down-cast-type':
assumes isOclAny: τ ⊨ (X::OclAny) .oclIsTypeOf(OclAny)
and non-null: τ ⊨ (δ X)
shows τ ⊨ not (v (X .oclAsType(Person)))
⟨proof⟩

lemma up-down-cast :
assumes isdef: τ ⊨ (δ X)
shows τ ⊨ (((X::Person) .oclAsType(OclAny) .oclAsType(Person) ≜ X)
⟨proof⟩

lemma up-down-cast-Person-OclAny-Person [simp]:
shows ((X::Person) .oclAsType(OclAny) .oclAsType(Person) = X)
proof

lemma up-down-cast-Person-OclAny-Person':
assumes τ
shows τ \vdash (X::Person).oclAsType(OclAny).oclAsType(Person) \equiv X
(proof)

lemma up-down-cast-Person-OclAny-Person'':
assumes τ
shows τ \vdash (X::Person).oclIsTypeOf(Person) \Rightarrow (X.oclAsType(OclAny).oclAsType(Person) \equiv X)
(proof)

5.6. OclIsKindOf

5.6.1. Definition

consts OclIsKindOf_OclAny :: 'α \Rightarrow Boolean ((-).oclIsKindOf'(OclAny'))
consts OclIsKindOf_Person :: 'α \Rightarrow Boolean ((-).oclIsKindOf'(Person'))

overloading OclIsKindOf_OclAny \equiv OclIsKindOf_OclAny :: OclAny \Rightarrow Boolean
begin
  definition OclIsKindOf_OclAny-OclAny:
(X::OclAny).oclIsKindOf(OclAny) \equiv
(\lambda \tau. \text{case } X \tau \text{ of}
  \bot \Rightarrow \text{invalid } \tau
  \mid \_ \Rightarrow \text{true } \tau)
end

overloading OclIsKindOf_OclAny \equiv OclIsKindOf_OclAny :: Person \Rightarrow Boolean
begin
  definition OclIsKindOf_OclAny-Person:
(X::Person).oclIsKindOf(OclAny) \equiv
(\lambda \tau. \text{case } X \tau \text{ of}
  \bot \Rightarrow \text{invalid } \tau
  \mid \_ \Rightarrow \text{true } \tau)
end

overloading OclIsKindOf_Person \equiv OclIsKindOf_Person :: OclAny \Rightarrow Boolean
begin
  definition OclIsKindOf_Person-OclAny:
(X::OclAny).oclIsKindOf(Person) \equiv
(\lambda \tau. \text{case } X \tau \text{ of}
  \bot \Rightarrow \text{invalid } \tau
  \mid \bot \Rightarrow \text{true } \tau
  \mid \_
    \mid \bot \Rightarrow false \tau
  \mid \_
    \mid \bot \Rightarrow true \tau)
end

overloading OclIsKindOf_Person \equiv OclIsKindOf_Person :: Person \Rightarrow Boolean
begin
  definition OclIsKindOf_Person-Person:
(X::Person).oclIsKindOf(Person) \equiv
(\lambda \tau. \text{case } X \tau \text{ of}
  \bot \Rightarrow \text{invalid } \tau
  \mid \_ \Rightarrow \text{true } \tau)
end
5.6.2. Context Passing

**lemma** \( cp-\text{OclIsKindOf}_{\text{OclAny}-\text{Person}-\text{Person}} : cp P \implies \lambda X . (P(X::\text{Person})::\text{Person}) . \text{oclIsKindOf}(\text{OclAny}) \)  
(proof)

**lemma** \( cp-\text{OclIsKindOf}_{\text{OclAny}-\text{OclAny}-\text{OclAny}} : cp P \implies \lambda X . (P(X::\text{OclAny})::\text{OclAny}) . \text{oclIsKindOf}(\text{OclAny}) \)  
(proof)

**lemma** \( cp-\text{OclIsKindOf}_{\text{Person}-\text{Person}-\text{Person}} : cp P \implies \lambda X . (P(X::\text{Person})::\text{Person}) . \text{oclIsKindOf}(\text{Person}) \)  
(proof)

**lemma** \( cp-\text{OclIsKindOf}_{\text{Person}-\text{OclAny}-\text{OclAny}} : cp P \implies \lambda X . (P(X::\text{OclAny})::\text{OclAny}) . \text{oclIsKindOf}(\text{Person}) \)  
(proof)

**lemma** \( cp-\text{OclIsKindOf}_{\text{OclAny}-\text{Person}-\text{OclAny}} : cp P \implies \lambda X . (P(X::\text{OclAny})::\text{OclAny}) . \text{oclIsKindOf}(\text{OclAny}) \)  
(proof)

**lemma** \( cp-\text{OclIsKindOf}_{\text{OclAny}-\text{OclAny}-\text{OclAny}} : cp P \implies \lambda X . (P(X::\text{OclAny})::\text{OclAny}) . \text{oclIsKindOf}(\text{OclAny}) \)  
(proof)

**lemma** \( cp-\text{OclIsKindOf}_{\text{Person}-\text{OclAny}-\text{OclAny}} : cp P \implies \lambda X . (P(X::\text{OclAny})::\text{OclAny}) . \text{oclIsKindOf}(\text{Person}) \)  
(proof)

**lemma** \( cp-\text{OclIsKindOf}_{\text{Person}-\text{OclAny}-\text{Person}} : cp P \implies \lambda X . (P(X::\text{OclAny})::\text{Person}) . \text{oclIsKindOf}(\text{Person}) \)  
(proof)

**lemmas** [simp] =  
\( cp-\text{OclIsKindOf}_{\text{OclAny}-\text{Person}-\text{Person}} \)
\( cp-\text{OclIsKindOf}_{\text{OclAny}-\text{OclAny}-\text{OclAny}} \)
\( cp-\text{OclIsKindOf}_{\text{Person}-\text{Person}-\text{Person}} \)
\( cp-\text{OclIsKindOf}_{\text{Person}-\text{OclAny}-\text{OclAny}} \)
\( cp-\text{OclIsKindOf}_{\text{OclAny}-\text{Person}-\text{OclAny}} \)
\( cp-\text{OclIsKindOf}_{\text{OclAny}-\text{OclAny}-\text{OclAny}} \)
\( cp-\text{OclIsKindOf}_{\text{Person}-\text{OclAny}-\text{OclAny}} \)
\( cp-\text{OclIsKindOf}_{\text{Person}-\text{OclAny}-\text{Person}} \)
\( cp-\text{OclIsKindOf}_{\text{Person}-\text{Person}-\text{OclAny}} \)
\( cp-\text{OclIsKindOf}_{\text{Person}-\text{Person}-\text{Person}} \)

5.6.3. Execution with Invalid or Null as Argument

**lemma** \( \text{OclIsKindOf}_{\text{OclAny}-\text{OclAny}-\text{strict1}[simp]} : (\text{invalid}::\text{OclAny}) . \text{oclIsKindOf}(\text{OclAny}) = \text{invalid} \)  
(proof)

**lemma** \( \text{OclIsKindOf}_{\text{OclAny}-\text{OclAny}-\text{strict2}[simp]} : (\text{null}::\text{OclAny}) . \text{oclIsKindOf}(\text{OclAny}) = \text{true} \)  
(proof)

**lemma** \( \text{OclIsKindOf}_{\text{OclAny}-\text{Person}-\text{strict1}[simp]} : (\text{invalid}::\text{Person}) . \text{oclIsKindOf}(\text{OclAny}) = \text{invalid} \)  
(proof)

**lemma** \( \text{OclIsKindOf}_{\text{OclAny}-\text{Person}-\text{strict2}[simp]} : (\text{null}::\text{Person}) . \text{oclIsKindOf}(\text{OclAny}) = \text{true} \)  
(proof)

**lemma** \( \text{OclIsKindOf}_{\text{Person}-\text{OclAny}-\text{strict1}[simp]} : (\text{invalid}::\text{OclAny}) . \text{oclIsKindOf}(\text{Person}) = \text{invalid} \)  
(proof)

**lemma** \( \text{OclIsKindOf}_{\text{Person}-\text{OclAny}-\text{strict2}[simp]} : (\text{null}::\text{OclAny}) . \text{oclIsKindOf}(\text{Person}) = \text{true} \)  
(proof)

**lemma** \( \text{OclIsKindOf}_{\text{Person}-\text{Person}-\text{strict1}[simp]} : (\text{invalid}::\text{OclAny}) . \text{oclIsKindOf}(\text{Person}) = \text{invalid} \)  
(proof)

**lemma** \( \text{OclIsKindOf}_{\text{Person}-\text{Person}-\text{strict2}[simp]} : (\text{null}::\text{OclAny}) . \text{oclIsKindOf}(\text{Person}) = \text{true} \)  
(proof)

5.6.4. Up Down Casting

**lemma** \( \text{actualKind-larger-staticKind}: \)

assumes isdef: \( \tau \models (\delta . X) \)

shows \( \tau \models (X::\text{Person}) . \text{oclIsKindOf}(\text{OclAny}) \supseteq \text{true} \)  
(proof)

**lemma** \( \text{down-cast-kind}: \)
assumes \( \text{isOclAny} \): \( \neg (\tau \mid \{(X::\text{OclAny}).\text{oclIsKindOf(Person)}\}) \)
and \( \text{non-null} \): \( \tau \mid \{\delta X\} \)
shows \( \tau \mid \{(X.\text{oclAsType(Person)}) \equiv \text{invalid}\)  

\[
\text{5.7. } \text{OclAllInstances}
\]

To denote OCL-types occurring in OCL expressions syntactically—as, for example, as “argument” of oclAllInstances()—we use the inverses of the injection functions into the object universes; we show that this is sufficient “characterization.”

definition \( \text{Person} \equiv \text{OclAsType}_{\text{Person}} \cdot \Xi \)
definition \( \text{OclAny} \equiv \text{OclAsType}_{\text{OclAny}} \cdot \Xi \)
lemmas [\( \text{simp} \) = \( \text{Person-def} \cdot \text{OclAny-def} \)]

\[
\text{lemma } \text{OclAllInstances-generic}_{\text{OclAny}}\cdot\text{exec}: \text{OclAllInstances-generic pre-post } \text{OclAny} = \\
(\lambda \tau. \text{Abs-Set}_{\text{base}} \uplus \text{Some } ' \text{OclAny } ' \text{ ran (heap (pre-post } \tau )) \downset) \\
\text{⟨proof⟩}
\]

\[
\text{lemma } \text{OclAllInstances-at-post}_{\text{OclAny}}\cdot\text{exec}: \text{OclAny } .\text{allInstances}() = \\
(\lambda \tau. \text{Abs-Set}_{\text{base}} \uplus \text{Some } ' \text{OclAny } ' \text{ ran (heap (snd } \tau )) \downset) \\
\text{⟨proof⟩}
\]

\[
\text{lemma } \text{OclAllInstances-at-pre}_{\text{OclAny}}\cdot\text{exec}: \text{OclAny } .\text{allInstances}@\text{pre}() = \\
(\lambda \tau. \text{Abs-Set}_{\text{base}} \uplus \text{Some } ' \text{OclAny } ' \text{ ran (heap (fst } \tau )) \downset) \\
\text{⟨proof⟩}
\]

\[
\text{5.7.1. } \text{OclIsTypeOf}
\]

\[
\text{lemma } \text{OclAny-allInstances-generic-oclIsTypeOf}_{\text{OclAny}}1: \\
\text{assumes } [\( \text{simp} \)]: \forall x. \text{pre-post } (x, x) = x \\
\text{shows } \exists \tau. (\tau \mid \text{not } ((\text{OclAllInstances-generic pre-post } \text{OclAny}) \rightarrow \forall \text{Set}_X (X | X .\text{oclIsTypeOf}(\text{OclAny})))) \\
\text{⟨proof⟩}
\]

\[
\text{lemma } \text{OclAny-allInstances-at-post-oclIsTypeOf}_{\text{OclAny}}1: \\
\exists \tau. (\tau \mid \text{not } ((\text{OclAny } .\text{allInstances}() \rightarrow \forall \text{Set}_X (X | X .\text{oclIsTypeOf}(\text{OclAny})))) \\
\text{⟨proof⟩}
\]

\[
\text{lemma } \text{OclAny-allInstances-at-pre-oclIsTypeOf}_{\text{OclAny}}1: \\
\exists \tau. (\tau \mid \text{not } ((\text{OclAny } .\text{allInstances}@\text{pre}() \rightarrow \forall \text{Set}_X (X | X .\text{oclIsTypeOf}(\text{OclAny})))) \\
\text{⟨proof⟩}
\]

\[
\text{lemma } \text{OclAny-allInstances-generic-oclIsTypeOf}_{\text{OclAny}}2: \\
\text{assumes } [\( \text{simp} \)]: \forall x. \text{pre-post } (x, x) = x \\
\text{shows } \exists \tau. (\tau \mid \text{not } ((\text{OclAllInstances-generic pre-post } \text{OclAny}) \rightarrow \forall \text{Set}_X (X | X .\text{oclIsTypeOf}(\text{OclAny})))) \\
\text{⟨proof⟩}
\]

\[
\text{lemma } \text{OclAny-allInstances-at-post-oclIsTypeOf}_{\text{OclAny}}2: \\
\exists \tau. (\tau \mid \text{not } ((\text{OclAny } .\text{allInstances}() \rightarrow \forall \text{Set}_X (X | X .\text{oclIsTypeOf}(\text{OclAny})))) \\
\text{⟨proof⟩}
\]

\[
\text{lemma } \text{OclAny-allInstances-at-pre-oclIsTypeOf}_{\text{OclAny}}2: \\
\exists \tau. (\tau \mid \text{not } ((\text{OclAny } .\text{allInstances}@\text{pre}() \rightarrow \forall \text{Set}_X (X | X .\text{oclIsTypeOf}(\text{OclAny})))) \\
\text{⟨proof⟩}
\]

\[
\text{lemma } \text{Person-allInstances-generic-oclIsTypeOf}_{\text{Person}}: \\
\tau \mid ((\text{OclAllInstances-generic pre-post } \text{Person}) \rightarrow \forall \text{Set}_X (X | X .\text{oclIsTypeOf}(\text{Person})))
\]

178
5.7.2. OclIsKindOf

lemma Person-allInstances-generic-oclIsKindOfPerson:
\[ \forall \sigma. (\sigma . allInstances\sigma \rightarrow \text{forAll}\_\text{set}\_\text{set}\_\text{X}(X . \text{oclIsKindOf}\_\text{Person})) \]

proof

lemma Person-allInstances-at-post-oclIsKindOfPerson:
\[ \forall \sigma. (\sigma . allInstances\@\text{post}\sigma \rightarrow \text{forAll}\_\text{set}\_\text{set}\_\text{X}(X . \text{oclIsKindOf}\_\text{Person})) \]

proof

lemma Person-allInstances-generic-oclIsKindOfOclAny:
\[ \forall \sigma. ((\sigma . allInstances\sigma \rightarrow \text{forAll}\_\text{set}\_\text{set}\_\text{X}(X . \text{oclIsKindOf}\_\text{OclAny}))) \]

proof

lemma Person-allInstances-at-post-oclIsKindOfOclAny:
\[ \forall \sigma. (\sigma . allInstances\@\text{post}\sigma \rightarrow \text{forAll}\_\text{set}\_\text{set}\_\text{X}(X . \text{oclIsKindOf}\_\text{OclAny}))) \]

proof

lemma Person-allInstances-generic-oclIsKindOfOclAny:
\[ \forall \sigma. ((\sigma . allInstances\sigma \rightarrow \text{forAll}\_\text{set}\_\text{set}\_\text{X}(X . \text{oclIsKindOf}\_\text{OclAny}))) \]

proof

lemma Person-allInstances-at-post-oclIsKindOfOclAny:
\[ \forall \sigma. (\sigma . allInstances\@\text{post}\sigma \rightarrow \text{forAll}\_\text{set}\_\text{set}\_\text{X}(X . \text{oclIsKindOf}\_\text{OclAny}))) \]

proof

lemma Person-allInstances-generic-oclIsKindOfPerson:
\[ \forall \sigma. ((\sigma . allInstances\sigma \rightarrow \text{forAll}\_\text{set}\_\text{set}\_\text{X}(X . \text{oclIsKindOf}\_\text{Person}))) \]

proof

lemma Person-allInstances-at-post-oclIsKindOfPerson:
\[ \forall \sigma. (\sigma . allInstances\@\text{post}\sigma \rightarrow \text{forAll}\_\text{set}\_\text{set}\_\text{X}(X . \text{oclIsKindOf}\_\text{Person}))) \]

proof

lemma Person-allInstances-at-pre-oclIsKindOfPerson:
\[ \forall \sigma. (\sigma . allInstances\@\text{pre}\sigma \rightarrow \text{forAll}\_\text{set}\_\text{set}\_\text{X}(X . \text{oclIsKindOf}\_\text{Person}))) \]

proof

lemma Person-allInstances-generic-oclIsKindOfPerson:
\[ \forall \sigma. ((\sigma . allInstances\sigma \rightarrow \text{forAll}\_\text{set}\_\text{set}\_\text{X}(X . \text{oclIsKindOf}\_\text{Person}))) \]

proof

lemma Person-allInstances-at-pre-oclIsKindOfPerson:
\[ \forall \sigma. (\sigma . allInstances\@\text{pre}\sigma \rightarrow \text{forAll}\_\text{set}\_\text{set}\_\text{X}(X . \text{oclIsKindOf}\_\text{Person}))) \]

proof

5.8. The Accessors (any, boss, salary)

Should be generated entirely from a class-diagram.

5.8.1. Definition

definition eval-extract :: (\forall \sigma . (\forall a . object option option) val
\Rightarrow (\forall oid . (\forall \sigma . (\forall a . ::\text{null}) val)
$$\Rightarrow (\forall \cdot c::\text{null}) \text{ val}$$

**where** eval-extract \(X \ f = (\lambda \ \tau. \ \text{case } X \ \tau \ of\)

\[\perp \Rightarrow \text{invalid } \tau \quad \text{— exception propagation}\]
\[\downarrow \ \perp \Rightarrow \text{invalid } \tau \quad \text{— dereferencing null pointer}\]
\[\downarrow \ \text{obj}_j \Rightarrow f \ (\text{oid-of } \text{obj}) \ \tau\]

**definition** deref-oid\(\text{Person} :: (\forall \ \text{state} \times \forall \ \text{state} \Rightarrow \forall \ \text{state})

\Rightarrow (\text{type } \text{Person} \Rightarrow (\forall, \cdot c::\text{null}) \text{ val})

\Rightarrow \text{oid}

\Rightarrow (\forall, \cdot c::\text{null}) \text{ val}

**where** deref-oid\(\text{Person} \ \text{fst-snd} \ f \ \text{oid} = (\lambda \ \tau. \ \text{case } \text{heap} \ (\text{fst-snd} \ \tau) \ \text{oid} \ of\)

\[\downarrow \ \text{in}_{\text{Person}} \ \text{obj}_j \Rightarrow f \ \text{obj} \ \tau\]
\[\downarrow \ - \Rightarrow \text{invalid } \tau\]

pointer undefined in state or not referencing a type conform object representation

**definition** select\(\text{OclAny} \ ANY \ f = (\lambda \ X. \ \text{case } X \ of \)

\[(\text{mk-}\text{OclAny} - \perp) \Rightarrow \text{null} \quad \text{— object contains null pointer}\]
\[(\text{mk-}\text{OclAny} - \text{any}_j) \Rightarrow f \ (\lambda x - \downarrow x \downarrow) \ \text{any}\]

**definition** select\(\text{Person} \ BOSS \ f = (\lambda \ X. \ \text{case } X \ of \)

\[(\text{mk-}\text{Person} - \perp) \Rightarrow \text{null} \quad \text{— object contains null pointer}\]
\[(\text{mk-}\text{Person} - \text{boss}) \Rightarrow f \ (\lambda x - \downarrow x \downarrow) \ \text{boss}\]

**definition** select\(\text{Person} \ SALARY \ f = (\lambda \ X. \ \text{case } X \ of \)

\[(\text{mk-}\text{Person} - \perp - \perp) \Rightarrow \text{null} \quad \text{— object contains null pointer}\]
\[(\text{mk-}\text{Person} - \text{salary}_j - \perp) \Rightarrow f \ (\lambda x - \downarrow x \downarrow) \ \text{salary}\]

**definition** in-pre-state = fst

**definition** in-post-state = snd

**definition** reconstr-basetype = (\lambda \ \text{convert } x. \ \text{convert } x)

**definition** dot\(\text{OclAny} \ ANY :: \text{OclAny} \Rightarrow - ((1\cdot\text{any}) \ 50)

where \((X).\text{any} = \text{eval-extract } X \quad \text{where } \text{(deref-oid}_{\text{OclAny}} \text{ in-post-state (select}_{\text{OclAny} \text{ANY}) \ reconstr-basetype)})

**definition** dot\(\text{Person} \ BOSS :: \text{Person} \Rightarrow \text{Person} ((1\cdot\text{boss}) \ 50)

where \((X).\text{boss} = \text{eval-extract } X \quad \text{where } \text{(deref-oid}_{\text{Person}} \text{ in-post-state (select}_{\text{Person} \text{BOSS}) \ (deref-oid}_{\text{Person}} \text{ in-post-state)})\)
definition dot_person\texttt{SALARY} :: Person \implies \text{Integer} \ ((1\cdot\text{salary}) 50)
  where (X).salary = \text{eval-extract} X
    (\text{deref-oid}_\text{Person} \ \text{in-post-state}
    (\text{select}_\text{Person}\texttt{SALARY}
    \ \text{reconst-basetype}))

definition dot_{OclAny}\texttt{ANY-at-pre} :: OclAny \Rightarrow \ ((1\cdot\text{any@pre}) 50)
  where (X).any@pre = \text{eval-extract} X
    (\text{deref-oid}_{OclAny} \ \text{in-pre-state}
    (\text{select}_{OclAny}\texttt{ANY}
    \ \text{reconst-basetype}))

definition dot_{Person}\texttt{BOSS-at-pre} :: Person \Rightarrow Person \ ((1\cdot\text{boss@pre}) 50)
  where (X).boss@pre = \text{eval-extract} X
    (\text{deref-oid}_{Person} \ \text{in-pre-state}
    (\text{select}_{Person}\texttt{BOSS}
    (\text{deref-oid}_{Person} \ \text{in-pre-state})))

definition dot_{Person}\texttt{SALARY-at-pre} :: Person \Rightarrow \text{Integer} \ ((1\cdot\text{salary@pre}) 50)
  where (X).salary@pre = \text{eval-extract} X
    (\text{deref-oid}_{Person} \ \text{in-pre-state}
    (\text{select}_{Person}\texttt{SALARY}
    \ \text{reconst-basetype})))

lemmas dot-accessor =
  dot_{OclAny}\texttt{ANY-def}
  dot_{Person}\texttt{BOSS-def}
  dot_{Person}\texttt{SALARY-def}
  dot_{OclAny}\texttt{ANY-at-pre-def}
  dot_{Person}\texttt{BOSS-at-pre-def}
  dot_{Person}\texttt{SALARY-at-pre-def}

5.8.2. Context Passing

lemmas [simp] = \text{eval-extract-def}

lemma cp-dot_{OclAny}\texttt{ANY} :: ((X).any) \ \tau = ((\lambda \cdot X \ \tau).\text{any}) \ \tau \ \langle \text{proof} \rangle
lemma cp-dot_{Person}\texttt{BOSS} :: ((X).boss) \ \tau = ((\lambda \cdot X \ \tau).\text{boss}) \ \tau \ \langle \text{proof} \rangle
lemma cp-dot_{Person}\texttt{SALARY} :: ((X).salary) \ \tau = ((\lambda \cdot X \ \tau).\text{salary}) \ \tau \ \langle \text{proof} \rangle

lemma cp-dot_{OclAny}\texttt{ANY-at-pre} :: ((X).any@pre) \ \tau = ((\lambda \cdot X \ \tau).\text{any@pre}) \ \tau \ \langle \text{proof} \rangle
lemma cp-dot_{Person}\texttt{BOSS-at-pre} :: ((X).boss@pre) \ \tau = ((\lambda \cdot X \ \tau).\text{boss@pre}) \ \tau \ \langle \text{proof} \rangle
lemma cp-dot_{Person}\texttt{SALARY-at-pre} :: ((X).salary@pre) \ \tau = ((\lambda \cdot X \ \tau).\text{salary@pre}) \ \tau \ \langle \text{proof} \rangle

lemmas cp-dot_{OclAny}\texttt{ANY}-I [simp, intro]=
  cp-dot_{OclAny}\texttt{ANY}[\text{THEN allI}]\ [\text{THEN allI}],
  of \ \lambda \ X \cdot X \ \lambda \cdot \tau. \ \tau, \ \text{THEN cpI}]
lemma cp-dot_{OclAny}\texttt{ANY-at-pre-I} [simp, intro]=
  cp-dot_{OclAny}\texttt{ANY-at-pre}[\text{THEN allI}]\ [\text{THEN allI}],
  of \ \lambda \ X \cdot X \ \lambda \cdot \tau. \ \tau, \ \text{THEN cpI}]
lemma cp-dot_{Person}\texttt{BOSS-I} [simp, intro]=
  cp-dot_{Person}\texttt{BOSS}[\text{THEN allI}]\ [\text{THEN allI}],
  of \ \lambda \ X \cdot X \ \lambda \cdot \tau. \ \tau, \ \text{THEN cpI}]
lemma cp-dot_{Person}\texttt{BOSS-at-pre-I} [simp, intro]=
  cp-dot_{Person}\texttt{BOSS-at-pre}[\text{THEN allI}]\ [\text{THEN allI}],

181
of \( \lambda X \cdot X \lambda \tau \cdot \tau \), THEN cpI1]

lemmas cp-dot{Person}SALARY-I [simp, intro]=
    cp-dot{Person}SALARY[THEN allI[THEN allI],
of \( \lambda X \cdot X \lambda \tau \cdot \tau \), THEN cpI1]

lemmas cp-dot{Person}SALARY-at-pre-I [simp, intro]=
    cp-dot{Person}SALARY-at-pre[THEN allI[THEN allI],
of \( \lambda X \cdot X \lambda \tau \cdot \tau \), THEN cpI1]

5.8.3. Execution with Invalid or Null as Argument

lemma dot{OCL}AnyANY-nullstrict [simp]: (null).any = invalid (proof)
lemma dot{OCL}AnyANY-at-pre-nullstrict [simp] : (null).any@pre = invalid (proof)
lemma dot{OCL}AnyANY-strict [simp] : (invalid).any = invalid (proof)
lemma dot{OCL}AnyANY-at-pre-strict [simp] : (invalid).any@pre = invalid (proof)

lemma dot{Person}BOSS-nullstrict [simp]: (null).boss = invalid (proof)
lemma dot{Person}BOSS-at-pre-nullstrict [simp] : (null).boss@pre = invalid (proof)
lemma dot{Person}BOSS-strict [simp] : (invalid).boss = invalid (proof)
lemma dot{Person}BOSS-at-pre-strict [simp] : (invalid).boss@pre = invalid (proof)

lemma dot{Person}SALARY-nullstrict [simp]: (null).salary = invalid (proof)
lemma dot{Person}SALARY-at-pre-nullstrict [simp] : (null).salary@pre = invalid (proof)
lemma dot{Person}SALARY-strict [simp] : (invalid).salary = invalid (proof)
lemma dot{Person}SALARY-at-pre-strict [simp] : (invalid).salary@pre = invalid (proof)

5.8.4. Representation in States

lemma dot{Person}BOSS-def-mono: \( \delta(X . \text{boss}) \Rightarrow \tau \models \delta(X) \) (proof)

lemma repr-boss:
assumes A : \( \tau \models \delta(X . \text{boss}) \)
shows is-represented-in-state in-post-state (x .\text{boss}) Person \( \tau \) (proof)

lemma repr-bossX:
assumes A : \( \tau \models \delta(X . \text{boss}) \)
shows \( \tau \models ((\text{Person .allInstances}(\)) \Rightarrow \text{includesSet}(x .\text{boss})) \) (proof)
Figure 5.2.: (a) pre-state $\sigma_1$ and (b) post-state $\sigma'_1$.

5.9. A Little Infra-structure on Example States

The example we are defining in this section comes from the figure 5.2.

definition OclInt1000 (1000) where OclInt1000 = ($\lambda$ - $\uparrow$1000 $\uparrow$)
definition OclInt1200 (1200) where OclInt1200 = ($\lambda$ - $\uparrow$1200 $\uparrow$)
definition OclInt1300 (1300) where OclInt1300 = ($\lambda$ - $\uparrow$1300 $\uparrow$)
definition OclInt1800 (1800) where OclInt1800 = ($\lambda$ - $\uparrow$1800 $\uparrow$)
definition OclInt2600 (2600) where OclInt2600 = ($\lambda$ - $\uparrow$2600 $\uparrow$)
definition OclInt2900 (2900) where OclInt2900 = ($\lambda$ - $\uparrow$2900 $\uparrow$)
definition OclInt3200 (3200) where OclInt3200 = ($\lambda$ - $\uparrow$3200 $\uparrow$)
definition OclInt3500 (3500) where OclInt3500 = ($\lambda$ - $\uparrow$3500 $\uparrow$)
definition oid0 $\equiv$ 0
definition oid1 $\equiv$ 1
definition oid2 $\equiv$ 2
definition oid3 $\equiv$ 3
definition oid4 $\equiv$ 4
definition oid5 $\equiv$ 5
definition oid6 $\equiv$ 6
definition oid7 $\equiv$ 7
definition oid8 $\equiv$ 8
definition person1 $\equiv$ mkPerson oid0 $\uparrow$1300$\downarrow$oid1$\downarrow$
definition person2 $\equiv$ mkPerson oid1 $\uparrow$1800$\downarrow$oid1$\downarrow$
definition person3 $\equiv$ mkPerson oid2 None None
definition person4 $\equiv$ mkPerson oid3 $\uparrow$2600$\downarrow$oid4$\downarrow$
definition person5 $\equiv$ mkPerson oid4 $\uparrow$2900$\downarrow$None
definition person6 $\equiv$ mkPerson oid5 $\uparrow$2300$\downarrow$oid3$\downarrow$
definition person7 $\equiv$ mkOclAny oid6 $\langle$3200 $\uparrow$oid6$\downarrow$,$\rangle$
definition person8 $\equiv$ mkOclAny oid7 None
definition person9 $\equiv$ mkPerson oid8 None

definition $\sigma_1 \equiv$ (heap $\rightarrow::$ (Map.empty(oid0 $\mapsto$ inPerson (mkPerson oid0 $\uparrow$1000$\downarrow$oid1$\downarrow$)))
(oid1 $\mapsto$ inPerson (mkPerson oid1 $\uparrow$1200$\downarrow$None))
(oid3 $\mapsto$ inPerson (mkPerson oid3 $\uparrow$2600$\downarrow$oid4$\downarrow$))
(oid4 $\mapsto$ inPerson person5)
(oid5 $\mapsto$ inPerson (mkPerson oid5 $\uparrow$2300$\downarrow$oid3$\downarrow$))
(oid8 $\mapsto$ inPerson person9),
assocs = Map.empty())
definition

\[ \sigma_1 \equiv \{ \text{heap} = \text{Map.empty}(\text{oid0} \mapsto \text{inPerson}\ person1) \]
\[ (\text{oid1} \mapsto \text{inPerson}\ person2) \]
\[ (\text{oid2} \mapsto \text{inPerson}\ person3) \]
\[ (\text{oid3} \mapsto \text{inPerson}\ person4) \]
\[ \cdots \]
\[ (\text{oid5} \mapsto \text{inPerson}\ person6) \]
\[ (\text{oid6} \mapsto \text{inOclAny}\ person7) \]
\[ (\text{oid7} \mapsto \text{inOclAny}\ person8) \]
\[ (\text{oid8} \mapsto \text{inPerson}\ person9) \],
\]
\[ \text{assocs} = \text{Map.empty} () \]

definition

\[ \sigma_0 \equiv \{ \text{heap} = \text{Map.empty}, \text{assocs} = \text{Map.empty} () \]
lemma \langle s_1, s_2 \rangle \models (X_{Person1} . oclIsMaintained())

lemma \langle s_1, s_2 \rangle \models (X_{Person1} . oclAsType(OclAny) . oclAsType(Person)) \models X_{Person1}

lemma \langle s_1, s_2 \rangle \models (X_{Person2} . salary \models 1800)
lemma \langle s_1, s_2 \rangle \models (X_{Person2} . salary@pre \models 1200)
lemma \langle s_1, s_2 \rangle \models (X_{Person2} . salary@pre \models X_{Person2})
lemma \langle s_1, s_2 \rangle \models (X_{Person2} . salary@pre \models null)
lemma \langle s_1, s_2 \rangle \models (X_{Person2} . salary@pre \models X_{Person2})
lemma \langle s_1, s_2 \rangle \models (X_{Person2} . salary@pre \models null)
lemma \langle s_1, s_2 \rangle \models (X_{Person2} . salary@pre \models X_{Person2})
lemma \langle s_1, s_2 \rangle \models (X_{Person2} . salary@pre \models null)
lemma \langle s_1, s_2 \rangle \models (X_{Person2} . salary@pre \models X_{Person2})
lemma \langle s_1, s_2 \rangle \models (X_{Person3} . salary \models null)
lemma \langle s_1, s_2 \rangle \models (X_{Person3} . salary \models X_{Person3})
lemma \langle s_1, s_2 \rangle \models (X_{Person3} . salary \models null)
lemma \langle s_1, s_2 \rangle \models (X_{Person3} . salary \models X_{Person3})
lemma \langle s_1, s_2 \rangle \models (X_{Person3} . salary \models null)
lemma \langle s_1, s_2 \rangle \models (X_{Person3} . salary \models X_{Person3})
lemma \langle s_1, s_2 \rangle \models (X_{Person4} . salary@pre \models X_{Person4})
lemma \langle s_1, s_2 \rangle \models (X_{Person4} . salary@pre \models X_{Person4})
lemma \langle s_1, s_2 \rangle \models (X_{Person4} . salary@pre \models X_{Person4})
lemma \langle s_1, s_2 \rangle \models (X_{Person5} . salary@pre \models X_{Person5})
lemma \langle s_1, s_2 \rangle \models (X_{Person5} . salary@pre \models X_{Person5})
lemma \langle s_1, s_2 \rangle \models (X_{Person5} . salary@pre \models X_{Person5})
lemma \langle s_1, s_2 \rangle \models (X_{Person5} . salary@pre \models X_{Person5})
lemma \langle s_1, s_2 \rangle \models (X_{Person5} . salary@pre \models X_{Person5})
lemma \langle s_1, s_2 \rangle \models (X_{Person5} . salary@pre \models X_{Person5})
Assert \( s_{post}. \ (\sigma_1, s_{post}) \models (X_{Person6}. \text{boss@pre} \models X_{Person4}) \)

Assert \( (\sigma_1, \sigma_1') \models (X_{Person6}. \text{boss@pre}. \text{salary} \models 2000) \)

Assert \( s_{post}. \ (\sigma_1, s_{post}) \models (X_{Person6}. \text{boss@pre}. \text{salary@pre} \models 2600) \)

Assert \( s_{post}. \ (\sigma_1, s_{post}) \models (X_{Person6}. \text{boss@pre}. \text{boss@pre} \models X_{Person5}) \)

lemma \( (\sigma_1, \sigma_1') \models (X_{Person6}. \text{oclIsMaintained}) \)

(proof)

lemma \( (\sigma_1, \sigma_1') \models (X_{Person7}. \text{oclIsNew}) \)

(proof)

lemma \( \sigma\text{-modifiedOnly:} \ (\sigma_1, \sigma_1') \models (\text{Set}(X_{Person1}. \text{oclAsType(OclAny)}) \)

(proof)

lemma \( (\sigma_1, \sigma_1') \models (\text{((X_{Person9} \circ \text{pre}) (\lambda x. \text{OclAsType}_\text{Person} \circ \text{x}) \models X_{Person9})}) \)

(proof)

lemma \( (\sigma_1, \sigma_1') \models (\text{((X_{Person9} \circ \text{post}) (\lambda x. \text{OclAsType}_\text{Person} \circ \text{x}) \models X_{Person9})}) \)

(proof)

lemma \( (\sigma_1, \sigma_1') \models (\text{((X_{Person9} \circ \text{oclAsType(OclAny)}) \circ \text{pre}) (\lambda x. \text{OclAsType}_\text{OclAny} \circ \text{x}) \models X_{Person9}) \circ \text{oclIsMaintained}) \)

(proof)

lemma \( \text{perm-\sigma_1'} : \sigma_1' = \emptyset \text{ heap = Map.empty} \)

\[
\begin{aligned}
\text{oid8} & \rightarrow \text{inPerson person9} \\
\text{oid7} & \rightarrow \text{inOclAny person8} \\
\text{oid6} & \rightarrow \text{inOclAny person7} \\
\text{oid5} & \rightarrow \text{inPerson person6} \\
\text{oid4} & \rightarrow \text{inPerson person4} \\
\text{oid2} & \rightarrow \text{inPerson person3} \\
\text{oid1} & \rightarrow \text{inPerson person2} \\
\text{oid0} & \rightarrow \text{inPerson person1}
\end{aligned}
\]
\[ \text{assocs} = \text{assocs} \sigma_1' \]

\[ \text{lemma } \land \sigma_1. \]
\( (\sigma_1, \sigma_1') \models (\text{Person} \ . \text{allInstances}) \models \text{Set} \{ X_{\text{Person}1}, X_{\text{Person}2}, X_{\text{Person}3}, X_{\text{Person}4}, X_{\text{Person}6}, X_{\text{Person}7} . \text{oclAsType}(\text{Person}), X_{\text{Person}8}, X_{\text{Person}9} \} \)

\[ \text{lemma } \land \sigma_1. \]
\( (\sigma_1, \sigma_1') \models (\text{OclAny} \ . \text{allInstances}) \models \text{Set} \{ X_{\text{Person}1} . \text{oclAsType}(\text{OclAny}), X_{\text{Person}2} . \text{oclAsType}(\text{OclAny}), X_{\text{Person}3} . \text{oclAsType}(\text{OclAny}), X_{\text{Person}4} . \text{oclAsType}(\text{OclAny}), X_{\text{Person}6} . \text{oclAsType}(\text{OclAny}), X_{\text{Person}7}, X_{\text{Person}8}, X_{\text{Person}9} . \text{oclAsType}(\text{OclAny}) \} \)

\[ \text{end} \]

```
theory Design-OCL
imports Design-UML
begin

5.10. OCL Part: Invariant

These recursive predicates can be defined conservatively by greatest fix-point constructions—automatically. See [4, 6] for details. For the purpose of this example, we state them as axioms here.

context Person
inv label : self . boss <> null implies (self . salary <= int((self . boss) . salary))

definition Person-label_{inv} :: Person \Rightarrow Boolean
where Person-label_{inv} (self) \equiv (self . boss <> null implies (self . salary <= int((self . boss) . salary)))

definition Person-label_{invATpre} :: Person \Rightarrow Boolean
where Person-label_{invATpre} (self) \equiv (self . boss@pre <> null implies (self . salary@pre <= int((self . boss@pre) . salary@pre)))

definition Person-label_{globalinv} :: Boolean
where Person-label_{globalinv} \equiv (Person . allInstances() \Rightarrow \text{forAllSet}(x \mid \text{Person-label}_{inv}(x)) \& \text{Person} . allInstances@pre() \Rightarrow \text{forAllSet}(x \mid \text{Person-label}_{invATpre}(x)))

lemma \( \tau \models \delta (X . boss) \Rightarrow \tau \models \text{Person} . \text{allInstances()} \Rightarrow \text{includesSet}(X . boss) \& \tau \models \text{Person} . \text{allInstances()} \Rightarrow \text{includesSet}(X) \)

lemma REC-pre : \( \tau \models \text{Person-label}_{globalinv} \Rightarrow \tau \models \text{Person} . \text{allInstances()} \Rightarrow \text{includesSet}(X) \) — X represented object in state
```

187
⇒ ∃ REC. τ |= REC(X) ≜ (Person-label\textsubscript{av}(X) and (X . boss <> null implies REC(X . boss)))
(proof)

This allows to state a predicate:

**axiomatization** `invPerson-label :: Person ⇒ Boolean`

**where** `invPerson-label\textsubscript{def}`:
(τ |= Person . allInstances() → includes\textsubscript{set}(self)) ⇒
(τ |= (invPerson-label(self)) ≜ (self . boss <> null implies
  (self . salary ≤\textsubscript{int} ((self . boss) . salary)) and
  invPerson-label(self . boss))))

**axiomatization** `invPerson-label\textsubscript{ATpre} :: Person ⇒ Boolean`

**where** `invPerson-label\textsubscript{ATpre-def}`:
(τ |= Person . allInstances@pre() → includes\textsubscript{set}(self)) ⇒
(τ |= (invPerson-label\textsubscript{ATpre}(self)) ≜ (self . boss@pre <> null implies
  (self . salary@pre ≤\textsubscript{int} ((self . boss@pre) . salary@pre)) and
  invPerson-label\textsubscript{ATpre}(self . boss@pre))))

**lemma** `inv-1` :
(τ |= Person . allInstances() → includes\textsubscript{set}(self)) ⇒
(τ |= invPerson-label(self) = (((τ |= (self . boss = null)) ∨
  (τ |= (self . boss <> null)) ∧
  τ |= (self . salary) ≤\textsubscript{int} (self . boss . salary)) ∧
  τ |= (invPerson-label(self . boss))))
(proof)

**lemma** `inv-2` :
(τ |= Person . allInstances@pre() → includes\textsubscript{set}(self)) ⇒
(τ |= invPerson-label\textsubscript{ATpre}(self) = (((τ |= (self . boss@pre = null)) ∨
  (τ |= (self . boss@pre <> null)) ∧
  (τ |= (self . boss@pre . salary@pre ≤\textsubscript{int} self . salary@pre)) ∧
  τ |= (invPerson-label\textsubscript{ATpre}(self . boss@pre)))))
(proof)

A very first attempt to characterize the axiomatization by an inductive definition - this can not be the last word since too weak (should be equality!)

**coinductive** `inv :: Person ⇒ \(\exists st ⇒ bool\)`

**where**
(τ |= (\(δ\) self)) ⇒ ((τ |= (self . boss = null)) ∨
(τ |= (self . boss <> null)) ∧
(τ |= (self . boss . salary ≤\textsubscript{int} self . salary)) ∧
( (inv(self . boss)) τ ))
⇒ ( inv self τ )

### 5.11. OCL Part: The Contract of a Recursive Query

This part is analogous to the Analysis Model and skipped here.

end
Part II.

Conclusion
6. Conclusion

6.1. Lessons Learned and Contributions

We provided a typed and type-safe shallow embedding of the core of UML [30, 31] and OCL [32]. Shallow embedding means that types of OCL were mapped by the embedding one-to-one to types in Isabelle/HOL [27]. We followed the usual methodology to build up the theory uniquely by conservative extensions of all operators in a denotational style and to derive logical and algebraic (execution) rules from them; thus, we can guarantee the logical consistency of the library and instances of the class model construction. The class models were given a closed-world interpretation as object-oriented datatype theories, as long as it follows the described methodology. Moreover, all derived execution rules are by construction type-safe (which would be an issue, if we had chosen to use an object universe construction in Zermelo-Fraenkel set theory as an alternative approach to subtyping.). In more detail, our theory gives answers and concrete solutions to a number of open major issues for the UML/OCL standardization:

1. the role of the two exception elements invalid and null, the former usually assuming strict evaluation while the latter ruled by non-strict evaluation.

2. the functioning of the resulting four-valued logic, together with safe rules (for example foundation9 – foundation12 in Section 2.1.5) that allow a reduction to two-valued reasoning as required for many automated provers. The resulting logic still enjoys the rules of a strong Kleene Logic in the spirit of the Amsterdam Manifesto [18].

3. the complicated life resulting from the two necessary equalities: the standard’s “strict weak referential equality” as default (written \_\_\_\_\_\_\_ throughout this document) and the strong equality (written \_\_\_\_\_\_\_\_\_), which follows the logical Leibniz principle that “equals can be replaced by equals.” Which is not necessarily the case if invalid or objects of different states are involved.

4. a type-safe representation of objects and a clarification of the old idea of a one-to-one correspondence between object representations and object-id’s, which became a state invariant.

5. a simple concept of state-framing via the novel operator \_\_\_\_\_\_\_oclIsModifiedOnly() and its consequences for strong and weak equality.

6. a semantic view on subtyping clarifying the role of static and dynamic type (aka apparent and actual type in Java terminology), and its consequences for casts, dynamic type-tests, and static types.

7. a semantic view on path expressions, that clarify the role of invalid and null as well as the tricky issues related to de-referentiation in pre- and post state.

8. an optional extension of the OCL semantics by infinite sets that provide means to represent “the set of potential objects or values” to state properties over them (this will be an important feature if OCL is intended to become a full-blown code annotation language in the spirit of JML [25] for semi-automated code verification, and has been considered desirable in the Aachen Meeting [14]).

Our two examples of Employee_AnalysisModel and Employee_DesignModel (see Chapter 4 and Figure 0.3.8 as well as Chapter 5 and Figure 0.3.8) sketch how this construction can be captured by an automated process; its implementation is described elsewhere.
Moreover, we managed to make our theory in large parts executable, which allowed us to include mechanically checked value-statements that capture numerous corner-cases relevant for OCL implementors. Among many minor issues, we thus pin-pointed the behavior of null in collections as well as in casts and the desired isKindOf-semantics of allInstances()

6.2. Lessons Learned

While our paper and pencil arguments, given in [12], turned out to be essentially correct, there had also been a lesson to be learned: If the logic is not defined as a Kleene-Logic, having a structure similar to a complete partial order (CPO), reasoning becomes complicated: several important algebraic laws break down which makes reasoning in OCL inherent messy and a semantically clean compilation of OCL formulae to a two-valued presentation, that is amenable to animators like KodKod [34] or SMT-solvers like Z3 [19] completely impractical. Concretely, if the expression not(null) is defined invalid (as was the case in prior versions of the standard [32]), then standard involution does not hold, i.e., not(not(A)) = A does not hold universally. Similarly, if null and null is invalid, then not even idempotence X and X = X holds. We strongly argue in favor of a lattice-like organization, where null represents “more information” than invalid and the logical operators are monotone with respect to this semantical “information ordering.”

A similar experience with prior paper and pencil arguments was our investigation of the object-oriented data-models, in particular path-expressions [15]. The final presentation is again essentially correct, but the technical details concerning exception handling lead finally to a continuation-passing style of the (in future generated) definitions for accessors, casts and tests. Apparently, OCL semantics (as many other “real” programming and specification languages) is meanwhile too complex to be treated by informal arguments solely.

Featherweight OCL makes several minor deviations from the standard and showed how the previous constructions can be made correct and consistent, and the DNF-normalization as well as δ-closure laws (necessary for a transition into a two-valued presentation of OCL specifications ready for interpretation in SMT solvers (see [13] for details)) are valid in Featherweight OCL.

6.3. Conclusion and Future Work

Featherweight OCL concentrates on formalizing the semantics of a core subset of OCL in general and in particular on formalizing the consequences of a four-valued logic (i.e., OCL versions that support, besides the truth values true and false also the two exception values invalid and null). In the following, we outline the following future extensions to use Featherweight OCL for a concrete fully fledged tool for OCL. There are essentially five extensions necessary:

- development of a compiler that compiles a textual or CASE tool representation (e.g., using XMI or the textual syntax of the USE tool [33]) of class models into an object-oriented data type theory automatically.

- Full support of OCL standard syntax in a front-end parser; Such a parser could also generate the necessary casts as well as converting standard OCL to Featherweight OCL as well as providing “normalizations” such as converting multiplicities of class attributes to into OCL class invariants.

- a setup for translating Featherweight OCL into a two-valued representation as described in [13]. As, in real-world scenarios, large parts of UML/OCL specifications are defined (e.g., from the default multiplicity 1 of an attributes x, we can directly infer that for all valid states x is neither invalid nor null), such a translation enables both an integration of fast constraint solvers such as Z3 as well as test-case generation scenarios as described in [13].

- a setup in Featherweight OCL of the Nitpick animator [8]. It remains to be shown that the standard, Kodkod [34] based animator in Isabelle can give a similar quality of animation as the OCLexec Tool [24].
• a code-generator setup for Featherweight OCL for Isabelle’s code generator. For example, the Isabelle code generator supports the generation of F#, which would allow to use OCL specifications for testing arbitrary .net-based applications.

The first two extensions are sufficient to provide a formal proof environment for OCL 2.5 similar to HOL-OCL while the remaining extensions are geared towards increasing the degree of proof automation and usability as well as providing a tool-supported test methodology for UML/OCL.

Our work shows that developing a machine-checked formal semantics of recent OCL standards still reveals significant inconsistencies—even though this type of research is not new. In fact, we started our work already with the 1.x series of OCL. The reasons for this ongoing consistency problems of OCL standard are manifold. For example, the consequences of adding an additional exception value to OCL 2.2 are widespread across the whole language and many of them are also quite subtle. Here, a machine-checked formal semantics is of great value, as one is forced to formalize all details and subtleties. Moreover, the standardization process of the OMG, in which standards (e.g., the UML infrastructure and the OCL standard) that need to be aligned closely are developed quite independently, are prone to ad-hoc changes that attempt to align these standards. And, even worse, updating a standard document by voting on the acceptance (or rejection) of isolated text changes does not help either. Here, a tool for the editor of the standard that helps to check the consistency of the whole standard after each and every modifications can be of great value as well.
Bibliography


Part III.

Appendix
A. The OCL And Featherweight OCL Syntax

<table>
<thead>
<tr>
<th>OCL</th>
<th>Featherweight OCL</th>
<th>Logical Constant</th>
</tr>
</thead>
<tbody>
<tr>
<td>_ * _</td>
<td>( \text{op} \triangleq ) (_ \text{oclAsSet}<em>{}(</em>_) )</td>
<td>\text{UML-Logic.StrongEq}</td>
</tr>
<tr>
<td>(&lt;) _</td>
<td>( \text{op} \triangleq ) (_ \text{not}_{}() )</td>
<td>\text{notequal}</td>
</tr>
<tr>
<td>_ -&gt;oclAsSet( _ ) _ -&gt;oclIsUndefined()</td>
<td>_ -&gt;oclIsNew() _</td>
<td>\text{UML-State.OclIsNew}</td>
</tr>
<tr>
<td>_ -&gt;oclAsType( _ ) _ -&gt;oclIsTypeOf( _ ) _ -&gt;oclIsKindOf( _ ) _ -&gt;oclIsInState( _ ) _ -&gt;oclType() _ -&gt;oclLocale()</td>
<td>_ -&gt;oclType() _</td>
<td>\text{UML-Logic.valid}</td>
</tr>
</tbody>
</table>

| OclAny | \_ ->oclAsSet( _ ) \_ ->oclIsUndefined() \_ ->oclIsInvalid() \_ ->oclAsType( _ ) \_ ->oclIsTypeOf( _ ) \_ ->oclIsKindOf( _ ) \_ ->oclIsInState( _ ) \_ ->oclType() \_ ->oclLocale() | \_ ->oclType() \_ | \text{UML-Logic.valid} |

| OclVoid | \_ ->oclAsSet( _ ) \_ ->oclIsUndefined() \_ ->oclIsInvalid() \_ ->oclAsType( _ ) \_ ->oclIsTypeOf( _ ) \_ ->oclIsKindOf( _ ) \_ ->oclIsInState( _ ) \_ ->oclType() \_ ->oclLocale() | \_ ->oclType() \_ | \text{UML-Logic.valid} |

| OclInvalid | \_ ->oclAsSet( _ ) \_ ->oclIsUndefined() \_ ->oclIsInvalid() \_ ->oclAsType( _ ) \_ ->oclIsTypeOf( _ ) \_ ->oclIsKindOf( _ ) \_ ->oclIsInState( _ ) \_ ->oclType() \_ ->oclLocale() | \_ ->oclType() \_ | \text{UML-Logic.valid} |

| Real | \_ + _ | \( \text{op} \triangleq \) \(_ \text{rea}_{}l \) \_ | \text{UML-Real.OclAddReal} |
| \_ - _ | \( \text{op} \triangleq \) \(_ \text{rea}_{}l \) \_ | \text{UML-Real.OclMinusReal} |
| \_ * _ | \( \text{op} \triangleq \) \(_ \text{rea}_{}l \) \_ | \text{UML-Real.OclMulReal} |

Continued on next page
<table>
<thead>
<tr>
<th>OCL</th>
<th>Featherweight OCL</th>
<th>Logical Constant</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>_</td>
<td>UML-Real.OclLessReal</td>
</tr>
<tr>
<td>-</td>
<td>_ / _</td>
<td>UML-Real.OclDivReal</td>
</tr>
<tr>
<td>_</td>
<td>.abs()</td>
<td>UML-Real.OclDivReal</td>
</tr>
<tr>
<td>_</td>
<td>.floor()</td>
<td>UML-Real.OclDivReal</td>
</tr>
<tr>
<td>_</td>
<td>.round()</td>
<td>UML-Real.OclDivReal</td>
</tr>
<tr>
<td>_</td>
<td>.max()</td>
<td>UML-Real.OclDivReal</td>
</tr>
<tr>
<td>_</td>
<td>.min()</td>
<td>UML-Real.OclDivReal</td>
</tr>
<tr>
<td>_</td>
<td>&lt; _</td>
<td>UML-Real.OclLessReal</td>
</tr>
<tr>
<td>_</td>
<td>_ &gt; _</td>
<td>UML-Real.OclLeReal</td>
</tr>
<tr>
<td>_</td>
<td>&lt;= _</td>
<td>UML-Real.OclLeReal</td>
</tr>
<tr>
<td>_</td>
<td>.toString()</td>
<td>UML-Real.OclLeReal</td>
</tr>
<tr>
<td>_</td>
<td>.div(_)</td>
<td>UML-Real.OclLeReal</td>
</tr>
<tr>
<td>_</td>
<td>.mod(_)</td>
<td>UML-Real.OclLeReal</td>
</tr>
<tr>
<td>_</td>
<td>_ -&gt;oclAsType(Integer)</td>
<td>UML-Library.OclAsIntegerReal</td>
</tr>
<tr>
<td>_</td>
<td>_ -&gt;oclAsType(Boolean)</td>
<td>UML-Library.OclAsBooleanReal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Real Literals</th>
<th>0.0</th>
<th>0.0</th>
<th>UML-Real.OclReal0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1.0</td>
<td>1.0</td>
<td>UML-Real.OclReal1</td>
</tr>
<tr>
<td></td>
<td>2.0</td>
<td>2.0</td>
<td>UML-Real.OclReal2</td>
</tr>
<tr>
<td></td>
<td>3.0</td>
<td>3.0</td>
<td>UML-Real.OclReal3</td>
</tr>
<tr>
<td></td>
<td>4.0</td>
<td>4.0</td>
<td>UML-Real.OclReal4</td>
</tr>
<tr>
<td></td>
<td>5.0</td>
<td>5.0</td>
<td>UML-Real.OclReal5</td>
</tr>
<tr>
<td></td>
<td>6.0</td>
<td>6.0</td>
<td>UML-Real.OclReal6</td>
</tr>
<tr>
<td></td>
<td>7.0</td>
<td>7.0</td>
<td>UML-Real.OclReal7</td>
</tr>
<tr>
<td></td>
<td>8.0</td>
<td>8.0</td>
<td>UML-Real.OclReal8</td>
</tr>
<tr>
<td></td>
<td>9.0</td>
<td>9.0</td>
<td>UML-Real.OclReal9</td>
</tr>
<tr>
<td></td>
<td>10.0</td>
<td>10.0</td>
<td>UML-Real.OclReal10</td>
</tr>
<tr>
<td></td>
<td>π</td>
<td></td>
<td>UML-Real.OclRealpi</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Integer Literals</th>
<th>0</th>
<th>0</th>
<th>UML-Integer.OclInt0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>UML-Integer.OclInt1</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>2</td>
<td>UML-Integer.OclInt2</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>3</td>
<td>UML-Integer.OclInt3</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>4</td>
<td>UML-Integer.OclInt4</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>5</td>
<td>UML-Integer.OclInt5</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>OCL</th>
<th>Featherweight OCL</th>
<th>Logical Constant</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>6</td>
<td>UML-Integer.OclInt6</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>UML-Integer.OclInt7</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>UML-Integer.OclInt8</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>UML-Integer.OclInt9</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>UML-Integer.OclInt10</td>
</tr>
</tbody>
</table>

- * 
- .size() 
- .concat( _ ) 
- .substring( _ , _ ) 
- .toInteger() 
- .toReal() 
- .toUpperCase() 
- .toLowerCase() 
- .indexOf() 
- .equalsIgnoreCase( _ ) 
- .at( _ ) 
- .characters() 
- .toBoolean() 
- < _ 
- > _ 
- <= _ 
- >= _ 

- + _ 
- op +string 
- UML-String.OclAddString 

- or _ 
- xor _ 
- and _ 
- not _ 
- op implies _ 
- op toString() 
- if _ then _ else _ endif 
- op = 
- op <> 
- op ≠ 
- op |≠ _ 
- op |= _ 
- UML-String.OclStrings 
- UML-String.OclStringsb 
- UML-String.OclStringc 

- or _ 
- xor _ 
- and _ 
- not _ 
- op implies _ 
- op toString() 
- if _ then _ else _ endif 
- op = 
- op <> 
- op ≠ 

- Set ( _ ) 
- Set( type ) 
- UML-Types.Set base type 
- UML-Set.setSet 
- Set( _ ) 
- Set{ args } 
- UML-Set.setSet 
- UML-Set.mSet 
- _ ->union( _ ) 
- _ ->unionSet( _ ) 
- UML-Set.OclUnion 
- _ ->intersection( _ ) 
- _ ->intersectionSet( _ ) 
- UML-Set.OclIntersection 
- _ ->including( _ ) 
- _ ->includingSet( _ ) 
- UML-Set.OclIncluding 
- _ ->excluding( _ ) 
- _ ->excludingSet( _ ) 
- UML-Set.OclExcluding 
- _ ->count( _ ) 
- _ ->countSet( _ ) 
- UML-Set.OclCount 
- _ ->flatten() 

Continued on next page
Continued on next page
<table>
<thead>
<tr>
<th>OCL</th>
<th>Featherweight OCL</th>
<th>Logical Constant</th>
</tr>
</thead>
<tbody>
<tr>
<td>_ -&gt;excludesAll( _ )</td>
<td>_ -&gt;excludesAllBag( _ )</td>
<td>UML-Bag.OclExcludesAll</td>
</tr>
<tr>
<td>_ -&gt;includesAll( _ )</td>
<td>_ -&gt;includesAllBag( _ )</td>
<td>UML-Bag.OclIncludesAll</td>
</tr>
<tr>
<td>_ -&gt;reject( _</td>
<td>_ )</td>
<td>_ -&gt;rejectBag( id</td>
</tr>
<tr>
<td>_ -&gt;select( _</td>
<td>_ )</td>
<td>_ -&gt;selectBag( id</td>
</tr>
<tr>
<td>_ -&gt;iterate( _ ; _ = _</td>
<td>_ )</td>
<td>_ -&gt;iterateBag( idt ; idt = any</td>
</tr>
<tr>
<td>_ -&gt;exists( _</td>
<td>_ )</td>
<td>_ -&gt;existsBag( id</td>
</tr>
<tr>
<td>_ -&gt;forall( _</td>
<td>_ )</td>
<td>_ -&gt;forallBag( id</td>
</tr>
<tr>
<td>_ -&gt;any()</td>
<td>_ -&gt;anyBag()</td>
<td>UML-Bag.OclANY</td>
</tr>
<tr>
<td>_ -&gt;notEmpty()</td>
<td>_ -&gt;notEmptyBag()</td>
<td>UML-Bag.OclNotEmpty</td>
</tr>
<tr>
<td>_ -&gt;size()</td>
<td>_ -&gt;sizeBag()</td>
<td>UML-Bag.OclSize</td>
</tr>
<tr>
<td>_ -&gt;excludes( _ )</td>
<td>_ -&gt;excludesBag( _ )</td>
<td>UML-Bag.OclExcludes</td>
</tr>
<tr>
<td>_ -&gt;excluding( _ )</td>
<td>_ -&gt;excludingBag( _ )</td>
<td>UML-Bag.OclExcluding</td>
</tr>
<tr>
<td>_ -&gt;including( _ )</td>
<td>_ -&gt;includingBag( _ )</td>
<td>UML-Bag.OclIncluding</td>
</tr>
<tr>
<td>_ -&gt;asSet()</td>
<td>_ -&gt;asSetBag()</td>
<td>UML-Library.OclAsSetBag</td>
</tr>
<tr>
<td>_ -&gt;asSeq()</td>
<td>_ -&gt;asSeqBag()</td>
<td>UML-Library.OclAsSeqBag</td>
</tr>
<tr>
<td>_ -&gt;asPair()</td>
<td>_ -&gt;asPairBag()</td>
<td>UML-Library.OclAsPairBag</td>
</tr>
<tr>
<td>Pair( type , type )</td>
<td>Pair( _ , _ )</td>
<td>UML-Types.Pair t a s e type</td>
</tr>
<tr>
<td>_ . Second()</td>
<td>_ . First()</td>
<td>UML-Pair.OclSecond</td>
</tr>
<tr>
<td>_ . Second()</td>
<td>_ . First()</td>
<td>UML-Pair.OclFirst</td>
</tr>
<tr>
<td>_ -&gt;asSequence()</td>
<td>_ -&gt;asSequencePair()</td>
<td>UML-Library.OclAsSeqPair</td>
</tr>
<tr>
<td>_ . allInstances()</td>
<td>_ . allInstances()</td>
<td>UML-State.OclAllInstances-at-post</td>
</tr>
<tr>
<td>_ . allInstances@pre()</td>
<td>_ . allInstances@pre()</td>
<td>UML-State.OclAllInstances-at-pre</td>
</tr>
<tr>
<td>_ . oclIsDeleted()</td>
<td>_ . oclIsDeleted()</td>
<td>UML-State.OclIsDeleted</td>
</tr>
<tr>
<td>_ . oclIsMaintained()</td>
<td>_ . oclIsMaintained()</td>
<td>UML-State.OclIsMaintained</td>
</tr>
<tr>
<td>_ . oclIsAbsent()</td>
<td>_ . oclIsAbsent()</td>
<td>UML-State.OclIsAbsent</td>
</tr>
<tr>
<td>_ . oclIsModifiedOnly()</td>
<td>_ . oclIsModifiedOnly()</td>
<td>UML-State.OclIsModifiedOnly</td>
</tr>
<tr>
<td>_ . @pre _</td>
<td>_ . @pre _</td>
<td>UML-State.OclSelf-at-pre</td>
</tr>
<tr>
<td>_ . @post _</td>
<td>_ . @post _</td>
<td>UML-State.OclSelf-at-post</td>
</tr>
</tbody>
</table>