

# Featherweight OCL

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

Achim D. Brucker\*    Frédéric Tuong<sup>‡</sup>    Burkhart Wolff<sup>†</sup>

August 28, 2014

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

<sup>‡</sup>Univ. Paris-Sud, IRT SystemX, 8 av. de la Vauve,  
91120 Palaiseau, France  
frederic.tuong@{u-psud, irt-systemx}.fr

<sup>†</sup>Univ. Paris-Sud, Laboratoire LRI, UMR8623, 91405 Orsay, France  
CNRS, 91405 Orsay, France  
burkhart.wolff@lri.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, 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 when with version 2.3 the 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 semantic interpretation. These semantic difficulties 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. 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.



# Contents

|   |           |
|---|-----------|
| <b>I. Introduction</b>  | <b>9</b>  |
| <b>1. Motivation</b>  | <b>11</b> |
| <b>2. Background</b>  | <b>13</b> |
| 2.1. A Guided Tour Through UML/OCL . . . . .                            | 13        |
| 2.2. Formal Foundation . . . . .  | 15        |
| 2.2.1. Isabelle . . . . .   | 15        |
| 2.2.2. Higher-order Logic (HOL) . . . . .                               | 16        |
| 2.3. Featherweight OCL: Design Goals . . . . .                          | 18        |
| 2.4. The Theory Organization . . . . .                                  | 19        |
| 2.4.1. Denotational Semantics . . . . .                                 | 19        |
| 2.4.2. Logical Layer . . . . .  | 21        |
| 2.4.3. Algebraic Layer . . . . .  | 23        |
| 2.5. Object-oriented Datatype Theories . . . . .                        | 26        |
| 2.5.1. Object Universes . . . . .                                       | 26        |
| 2.5.2. Accessors on Objects and Associations . . . . .                  | 28        |
| 2.5.3. Other Operations on States . . . . .                             | 31        |
| 2.6. A Machine-checked Annex A . . . . .                                | 32        |
| <br>  |           |
| <b>II. A Proposal for Formal Semantics of OCL 2.5</b>                   | <b>35</b> |
| <b>3. Formalization I: Core Definitions</b>                             | <b>37</b> |
| 3.1. Preliminaries . . . . .  | 37        |
| 3.1.1. Notations for the Option Type . . . . .                          | 37        |
| 3.1.2. Minimal Notions of State and State Transitions . . . . .         | 37        |
| 3.1.3. Prerequisite: An Abstract Interface for OCL Types . . . . .      | 38        |
| 3.1.4. Accommodation of Basic Types to the Abstract Interface . . . . . | 38        |
| 3.1.5. The Semantic Space of OCL Types: Valuations . . . . .            | 39        |
| 3.2. Definition of the Boolean Type . . . . .                           | 40        |
| 3.2.1. Basic Constants . . . . .  | 40        |
| 3.2.2. Validity and Definedness . . . . .                               | 41        |
| 3.3. The Equalities of OCL . . . . .                                    | 43        |
| 3.3.1. Definition . . . . .   | 44        |
| 3.3.2. Fundamental Predicates on Strong Equality . . . . .              | 45        |

|           |   |           |
|-----------|---|-----------|
| 3.4.      | Logical Connectives and their Universal Properties . . . . .              | 46        |
| 3.5.      | A Standard Logical Calculus for OCL . . . . .                             | 51        |
| 3.5.1.    | Global vs. Local Judgements . . . . .                                     | 51        |
| 3.5.2.    | Local Validity and Meta-logic . . . . .                                   | 52        |
| 3.5.3.    | Local Judgements and Strong Equality . . . . .                            | 54        |
| 3.5.4.    | Laws to Establish Definedness ( $\delta$ -closure) . . . . .              | 56        |
| 3.6.      | Miscellaneous . . . . .   | 56        |
| 3.6.1.    | OCL's if then else endif . . . . .  | 56        |
| 3.6.2.    | A Side-calculus for (Boolean) Constant Terms . . . . .                    | 57        |
| <b>4.</b> | <b>Formalization II: Library Definitions</b>                              | <b>61</b> |
| 4.1.      | Basic Types: Void and Integer . . . . .                                   | 61        |
| 4.1.1.    | The Construction of the Void Type . . . . .                               | 61        |
| 4.1.2.    | The Construction of the Integer Type . . . . .                            | 61        |
| 4.1.3.    | Validity and Definedness Properties . . . . .                             | 62        |
| 4.1.4.    | Arithmetical Operations on Integer . . . . .                              | 62        |
| 4.2.      | Fundamental Predicates on Basic Types: Strict Equality . . . . .          | 64        |
| 4.2.1.    | Definition . . . . .  | 64        |
| 4.2.2.    | Logic and Algebraic Layer on Basic Types . . . . .                        | 64        |
| 4.2.3.    | Test Statements on Basic Types. . . . .                                   | 67        |
| 4.3.      | Complex Types: The Set-Collection Type (I) Core . . . . .                 | 68        |
| 4.3.1.    | The Construction of the Set Type . . . . .                                | 68        |
| 4.3.2.    | Validity and Definedness Properties . . . . .                             | 69        |
| 4.3.3.    | Constants on Sets . . . . .   | 69        |
| 4.4.      | Complex Types: The Set-Collection Type (II) Library . . . . .             | 70        |
| 4.4.1.    | Computational Operations on Set . . . . .                                 | 70        |
| 4.4.2.    | Validity and Definedness Properties . . . . .                             | 73        |
| 4.4.3.    | Execution with Invalid or Null or Infinite Set as Argument . . . . .      | 76        |
| 4.4.4.    | Context Passing . . . . .   | 78        |
| 4.4.5.    | Const . . . . .   | 80        |
| 4.5.      | Fundamental Predicates on Set: Strict Equality . . . . .                  | 80        |
| 4.5.1.    | Definition . . . . .  | 80        |
| 4.5.2.    | Logic and Algebraic Layer on Set . . . . .                                | 81        |
| 4.6.      | Execution on Set's Operators (with mtSet and recursive case as arguments) | 82        |
| 4.6.1.    | OclIncluding . . . . .  | 82        |
| 4.6.2.    | OclExcluding . . . . .  | 82        |
| 4.6.3.    | OclIncludes . . . . .   | 84        |
| 4.6.4.    | OclExcludes . . . . .   | 85        |
| 4.6.5.    | OclSize . . . . .   | 85        |
| 4.6.6.    | OclIsEmpty . . . . .  | 86        |
| 4.6.7.    | OclNotEmpty . . . . .   | 86        |
| 4.6.8.    | OclANY . . . . .  | 86        |
| 4.6.9.    | OclForall . . . . .   | 86        |
| 4.6.10.   | OclExists . . . . .   | 87        |

|             |  |            |
|-------------|--|------------|
| 4.6.11.     | OclIterate . . . . .   | 87         |
| 4.6.12.     | OclSelect . . . . .  | 87         |
| 4.6.13.     | OclReject . . . . .  | 87         |
| 4.7.        | Execution on Set's Operators (higher composition) . . . . .    | 88         |
| 4.7.1.      | OclIncludes . . . . .  | 88         |
| 4.7.2.      | OclSize . . . . .  | 88         |
| 4.7.3.      | OclForall . . . . .  | 88         |
| 4.7.4.      | Strict Equality . . . . .                                      | 89         |
| 4.8.        | Test Statements . . . . .                                      | 90         |
| <b>5.</b>   | <b>Formalization III: State Operations and Objects</b>         | <b>93</b>  |
| 5.1.        | Introduction: States over Typed Object Universes . . . . .     | 93         |
| 5.1.1.      | Recall: The Generic Structure of States . . . . .              | 93         |
| 5.2.        | Fundamental Predicates on Object: Strict Equality . . . . .    | 94         |
| 5.2.1.      | Logic and Algebraic Layer on Object . . . . .                  | 94         |
| 5.3.        | Operations on Object . . . . .                                 | 96         |
| 5.3.1.      | Initial States (for testing and code generation) . . . . .     | 96         |
| 5.3.2.      | OclAllInstances . . . . .                                      | 96         |
| 5.3.3.      | OclIsNew, OclIsDeleted, OclIsMaintained, OclIsAbsent . . . . . | 103        |
| 5.3.4.      | OclIsModifiedOnly . . . . .                                    | 104        |
| 5.3.5.      | OclSelf . . . . .  | 104        |
| 5.3.6.      | Framing Theorem . . . . .                                      | 105        |
| 5.3.7.      | Miscellaneous . . . . .  | 105        |
| <b>III.</b> | <b>Examples</b>  | <b>107</b> |
| <b>6.</b>   | <b>The Employee Analysis Model</b>                             | <b>109</b> |
| 6.1.        | The Employee Analysis Model (UML) . . . . .                    | 109        |
| 6.1.1.      | Introduction . . . . .   | 109        |
| 6.1.2.      | Example Data-Universe and its Infrastructure . . . . .         | 110        |
| 6.1.3.      | Instantiation of the Generic Strict Equality . . . . .         | 111        |
| 6.1.4.      | OclAsType . . . . .  | 112        |
| 6.1.5.      | OclIsTypeOf . . . . .  | 114        |
| 6.1.6.      | OclIsKindOf . . . . .  | 117        |
| 6.1.7.      | OclAllInstances . . . . .                                      | 119        |
| 6.1.8.      | The Accessors (any, boss, salary) . . . . .                    | 121        |
| 6.1.9.      | A Little Infra-structure on Example States . . . . .           | 126        |
| 6.2.        | The Employee Analysis Model (OCL) . . . . .                    | 130        |
| 6.2.1.      | Standard State Infrastructure . . . . .                        | 131        |
| 6.2.2.      | Invariant . . . . .  | 131        |
| 6.2.3.      | The Contract of a Recursive Query . . . . .                    | 131        |
| 6.2.4.      | The Contract of a Method . . . . .                             | 132        |

|   |                |
|---|----------------|
| <b>7. The Employee Design Model</b>                 | <b>133</b>     |
| 7.1. The Employee Design Model (UML)                | 133            |
| 7.1.1. Introduction                                 | 133            |
| 7.1.2. Example Data-Universe and its Infrastructure | 133            |
| 7.1.3. Instantiation of the Generic Strict Equality | 135            |
| 7.1.4. OclAsType                                    | 136            |
| 7.1.5. OclIsTypeOf                                  | 138            |
| 7.1.6. OclIsKindOf                                  | 141            |
| 7.1.7. OclAllInstances                              | 143            |
| 7.1.8. The Accessors (any, boss, salary)            | 145            |
| 7.1.9. A Little Infra-structure on Example States   | 148            |
| 7.2. The Employee Design Model (OCL)                | 154            |
| 7.2.1. Standard State Infrastructure                | 154            |
| 7.2.2. Invariant                                    | 154            |
| 7.2.3. The Contract of a Recursive Query            | 155            |
| 7.2.4. The Contract of a Method                     | 155            |
| <br><b>IV. Conclusion</b>                           | <br><b>157</b> |
| <br><b>8. Conclusion</b>                            | <br><b>159</b> |
| 8.1. Lessons Learned and Contributions              | 159            |
| 8.2. Lessons Learned                                | 160            |
| 8.3. Conclusion and Future Work                     | 161            |



**Part I.**

**Introduction**



# 1. Motivation

The Unified Modeling Language (UML) [31, 32] 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) [33]. 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 [35]) 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, 11, 19, 22, 26]).

At its origins [28, 35], OCL was conceived as a strict semantics for undefinedness (e. g., denoted by the element `invalid`<sup>1</sup>), 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,
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 [30, 33] 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

---

<sup>1</sup>In earlier versions of the OCL standard, this element was called `OclUndefined`.

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 [15]. 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 type `Integer`, the collection type `Set`, as well as the generic construction principle of class models, which is instantiated and demonstrated for two examples (an automated support for this type-safe construction is again out of the scope of Featherweight 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 [33] as well as replace completely its informative “Annex A.”

## 2. Background

### 2.1. A Guided Tour Through UML/OCL

The Unified Modeling Language (UML) [31, 32] 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 2.1 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*). 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.

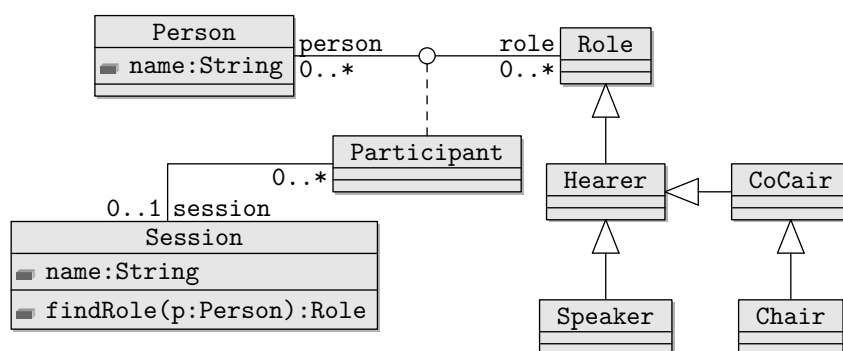


Figure 2.1.: A simple UML class model representing a conference system for organizing conference sessions: persons can participate, in different roles, in a session.

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., association 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. Association 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.

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 [12] is to translate the diagrammatic UML features into a combination of more elementary features of UML and OCL expressions [21]. For example, associations are usually represented by 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.

## 2.2. Formal Foundation

### 2.2.1. 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).

Isabelle’s inference rules are based on the built-in meta-level implication  $\Longrightarrow$  allowing to form constructs like  $A_1 \Longrightarrow \dots \Longrightarrow A_n \Longrightarrow A_{n+1}$ , 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 as

$$\llbracket A_1; \dots; A_n \rrbracket \Longrightarrow A_{n+1} \quad \text{or, in mathematical notation,} \quad \frac{A_1 \quad \dots \quad A_n}{A_{n+1}}. \quad (2.1)$$

The built-in meta-level quantification  $\bigwedge x. x$  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:

$$\bigwedge x_1, \dots, x_m. \llbracket A_1; \dots; A_n \rrbracket \Longrightarrow A_{n+1}. \quad (2.2)$$

Isabelle supports forward- and backward reasoning on rules. For backward-reasoning, a *proof-state* can be initialized and further transformed into others. For example, a proof of  $\phi$ , using the Isar [38] language, will look as follows in Isabelle:

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

(2.3)

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 conjointed sequence

of generalized Horn-clauses (called *subgoals*)  $\phi_1, \dots, \phi_n$  and a *goal*  $\phi$ . Proof states were usually denoted by:

$$\begin{array}{l} \text{label : } \phi \\ 1. \phi_1 \\ \vdots \\ n. \phi_n \end{array} \tag{2.4}$$

Subgoals and goals may be extracted from the proof state into theorems of the form  $\llbracket \phi_1; \dots; \phi_n \rrbracket \implies \phi$  at any time; this mechanism helps to generate test theorems. Further, Isabelle supports meta-variables (written  $?x, ?y, \dots$ ), which can be seen as “holes in a term” that can still be substituted. Meta-variables are instantiated by Isabelle’s built-in higher-order unification.

## 2.2.2. Higher-order Logic (HOL)

*Higher-order logic* (HOL) [1, 17] is a classical logic based on a simple type system. It provides the usual logical connectives like  $\_ \wedge \_$ ,  $\_ \rightarrow \_$ ,  $\_ \neg$  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  $\_ = \_ :: \alpha \Rightarrow \alpha \Rightarrow \text{bool}$ . HOL is more expressive than first-order logic, since, e.g., induction schemes can be expressed inside the logic. Being based on some polymorphically typed  $\lambda$ -calculus, HOL can be viewed as a combination of a programming language like SML or Haskell and a specification language providing powerful logical quantifiers ranging over elementary and function types.

Isabelle/HOL is a logical embedding of HOL into Isabelle. The (original) simple-type system underlying HOL has been extended by Hindley-Milner style polymorphism with type-classes similar to Haskell. While Isabelle/HOL is usually seen as proof assistant, we use it as symbolic computation environment. Implementations on top of Isabelle/HOL can re-use existing powerful deduction mechanisms such as higher-order resolution, tableaux-based reasoners, rewriting procedures, Presburger arithmetic, and via various integration mechanisms, also external provers such as Vampire [34] and the SMT-solver Z3 [20].

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 *wellfounded recursive definitions*.

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

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 `bool`; consequently,



the constant definitions for membership is as follows:<sup>1</sup>

$$\begin{array}{lll}
\text{types} & \alpha \text{ set} & = \alpha \Rightarrow \text{bool} \\
\text{definition} & \text{Collect} & :: (\alpha \Rightarrow \text{bool}) \Rightarrow \alpha \text{ set} \quad \text{--- set comprehension} \\
\text{where} & \text{Collect } S & \equiv S \quad (2.5) \\
\text{definition} & \text{member} & :: \alpha \Rightarrow \alpha \Rightarrow \text{bool} \quad \text{--- membership test} \\
\text{where} & \text{member } s S & \equiv S s
\end{array}$$

Isabelle's syntax engine is instructed to accept the notation  $\{x \mid P\}$  for  $\text{Collect } \lambda x. P$  and the notation  $s \in S$  for  $\text{member } s S$ . As can be inferred from the example, constant definitions are axioms that introduce a fresh constant symbol by some closed, non-recursive expressions; this type of axiom is logically safe since it works like an abbreviation. The syntactic side conditions of this axiom are mechanically checked, of course. It is straightforward to express the usual operations on sets like  $\_ \cup \_ , \_ \cap \_ :: \alpha \text{ set} \Rightarrow \alpha \text{ set} \Rightarrow \alpha \text{ set}$  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:

$$\begin{array}{ll}
\text{datatype} & \text{option} = \text{None} \mid \text{Some } \alpha \\
\text{datatype} & \alpha \text{ list} = \text{Nil} \mid \text{Cons } a l
\end{array} \quad (2.6)$$

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*  $\text{None}$ ,  $\text{Some}$ ,  $[]$  and  $\text{Cons}$ , there is the match operation

$$\text{case } x \text{ of } \text{None} \Rightarrow F \mid \text{Some } a \Rightarrow G a \quad (2.7)$$

respectively

$$\text{case } x \text{ of } [] \Rightarrow F \mid \text{Cons } a r \Rightarrow G a r. \quad (2.8)$$

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

$$\begin{array}{ll}
(\text{case } [] \text{ of } [] \Rightarrow F \mid (a\#r) \Rightarrow G a r) = F & \\
(\text{case } b\#t \text{ of } [] \Rightarrow F \mid (a\#r) \Rightarrow G a r) = G b t & \\
[] \neq a\#t & \text{--- distinctness} \\
[[a = [] \rightarrow P; \exists x t. a = x\#t \rightarrow P]] \Longrightarrow P & \text{--- exhaust} \\
[[P[]; \forall at. Pt \rightarrow P(a\#t)]] \Longrightarrow Px & \text{--- induct}
\end{array} \quad (2.9)$$

Finally, there is a compiler for primitive and wellfounded recursive function definitions. For example, we may define the sort operation of our running test example by:

$$\begin{array}{lll}
\text{fun} & \text{ins} & :: [\alpha :: \text{linorder}, \alpha \text{ list}] \Rightarrow \alpha \text{ list} \\
\text{where} & \text{ins } x [] & = [x] \\
& \text{ins } x (y\#ys) & = \text{if } x < y \text{ then } x\#y\#ys \text{ else } y\#(\text{ins } x ys)
\end{array} \quad (2.10)$$

<sup>1</sup>To increase readability, we use a slightly simplified presentation.

```

fun      sort      ::( $\alpha$  :: linorder) list  $\Rightarrow$   $\alpha$  list
where   sort []    = []
        sort( $x\#xs$ ) = ins  $x$  (sort  $xs$ )

```

(2.11)

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, multisets, orderings, and various arithmetic theories which only contain rules derived from conservative definitions. 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). Similarly, Isabelle manages a large set of (higher-order) rewrite rules into which recursive function definitions were included. Provided that this rule set represents a terminating and confluent rewrite system, the Isabelle simplifier provides also a highly potent decision procedure for many fragments of theories underlying the constraints to be processed when constructing test theorems.

### 2.3. Featherweight OCL: Design Goals

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 `Boolean`, `Integer`, and typed sets (`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 `null` (`Set{null}` is a defined set) but not `invalid` (`Set{invalid}` is just `invalid`).
3. Any Featherweight OCL type contains at least `invalid` and `null` (the type `Void` contains only these instances). The logic is consequently four-valued, and there is a `null`-element in the type `Set(A)`.
4. It is a strongly typed language in the Hindley-Milner tradition. We assume that a pre-process eliminates all implicit conversions due to subtyping 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 subcalculus, “cp” (a detailed discussion of the different equalities as well as the subcalculus “cp”—for three-valued OCL 2.0—is given in [10]), which is nasty but can be hidden from the user inside tools.

## 2.4. 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 logical consistency of the overall construction. 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  $\sigma'$ , validity statements were written  $(\sigma, \sigma') \models P$ . 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 space reasons, we will restrict ourselves in this paper 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.

### 2.4.1. Denotational Semantics

OCL is composed of

1. operators on built-in data structures such as `Boolean`, `Integer`, or `Set(A)`,
2. operators of the user-defined data-model such as accessors, type-casts and tests, and
3. user-defined, side-effect-free methods.

Conceptually, an OCL expression in general and Boolean expressions in particular (i. e., *formulae*) depends on the pair  $(\sigma, \sigma')$  of pre- and post-state. The precise form of states is irrelevant for this paper (compare [13]) and will be left abstract in this presentation. We construct in Isabelle a type-class `null` that contains two distinguishable elements `bot` and `null`. Any type of the form  $(\alpha_{\perp})_{\perp}$  is an instance of this type-class with  $\text{bot} \equiv \perp$  and  $\text{null} \equiv \lfloor \perp \rfloor$ . Now, any OCL type can be represented by an HOL type of the form:

$$V(\alpha) := \text{state} \times \text{state} \rightarrow \alpha :: \text{null} .$$

On this basis, we define  $V((\text{bool}_{\perp})_{\perp})$  as the HOL type for the OCL type `Boolean` and define:

$$\begin{aligned} I[\text{invalid} :: V(\alpha)]\tau &\equiv \text{bot} & I[\text{null} :: V(\alpha)]\tau &\equiv \text{null} \\ I[\text{true} :: \text{Boolean}]\tau &= \lfloor \text{true} \rfloor & I[\text{false}]\tau &= \lfloor \text{false} \rfloor \\ I[X.\text{oclIsUndefined}()]\tau &= (\text{if } I[X]\tau \in \{\text{bot}, \text{null}\} \text{ then } I[\text{true}]\tau \text{ else } I[\text{false}]\tau) \\ I[X.\text{oclIsValid}()]\tau &= (\text{if } I[X]\tau = \text{bot} \text{ then } I[\text{true}]\tau \text{ else } I[\text{false}]\tau) \end{aligned}$$

where  $I[E]$  is the semantic interpretation function commonly used in mathematical textbooks and  $\tau$  stands for pairs of pre- and post state  $(\sigma, \sigma')$ . For reasons of conciseness, we will write  $\delta X$  for `not X.oclIsUndefined()` and  $v X$  for `not X.oclIsValid()` throughout this paper.

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

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

we can therefore write:

$$\text{true} :: \text{Boolean} = \lambda \tau. \lfloor \text{true} \rfloor$$

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. Since all operators of the assertion language depend on the context  $\tau = (\sigma, \sigma')$  and result in values that can be  $\perp$ , all expressions can be viewed as *evaluations* from  $(\sigma, \sigma')$  to a type  $\alpha$  which must possess a  $\perp$  and a null-element. Given that such constraints can be expressed in Isabelle/HOL via *type classes* (written:  $\alpha :: \kappa$ ), all types for OCL-expressions are of a form captured by

$$V(\alpha) := \text{state} \times \text{state} \rightarrow \alpha :: \{\text{bot}, \text{null}\},$$

where `state` stands for the system state and `state × state` describes the pair of pre-state and post-state and  $\_ := \_$  denotes the type abbreviation.

The current OCL semantics [29, Annex A] uses different interpretation functions for invariants and pre-conditions; we achieve their semantic effect by a syntactic transformation  $\_ \text{-pre}$  which replaces, for example, all accessor functions  $\_.a$  by their counterparts  $\_.a @ \text{pre}$ . For example,  $(\text{self}.a > 5)_{\text{pre}}$  is just  $(\text{self}.a @ \text{pre} > 5)$ . This way, also invariants

and pre-conditions can be interpreted by the same interpretation function and have the same type of an evaluation  $V(\alpha)$ .

On this basis, one can define the core logical operators **not** and **and** as follows:

$$\begin{aligned}
I[\mathbf{not} X]\tau &= (\text{case } I[X]\tau \text{ of} \\
&\quad \perp \quad \Rightarrow \perp \\
&\quad |[ \perp ] \quad \Rightarrow [ \perp ] \\
&\quad |[ [x] ] \quad \Rightarrow [ [ \neg x ] ]) \\
\\
I[X \mathbf{and} Y]\tau &= (\text{case } I[X]\tau \text{ of} \\
&\quad \perp \quad \Rightarrow (\text{case } I[Y]\tau \text{ of} \\
&\quad \quad \perp \quad \Rightarrow \perp \\
&\quad \quad |[ \perp ] \quad \Rightarrow \perp \\
&\quad \quad |[ [ \mathbf{true} ] ] \quad \Rightarrow \perp \\
&\quad \quad |[ [ \mathbf{false} ] ] \quad \Rightarrow [ [ \mathbf{false} ] ]) \\
&\quad |[ \perp ] \quad \Rightarrow (\text{case } I[Y]\tau \text{ of} \\
&\quad \quad \perp \quad \Rightarrow \perp \\
&\quad \quad |[ \perp ] \quad \Rightarrow [ \perp ] \\
&\quad \quad |[ [ \mathbf{true} ] ] \quad \Rightarrow [ \perp ] \\
&\quad \quad |[ [ \mathbf{false} ] ] \quad \Rightarrow [ [ \mathbf{false} ] ]) \\
&\quad |[ [ \mathbf{true} ] ] \quad \Rightarrow (\text{case } I[Y]\tau \text{ of} \\
&\quad \quad \perp \quad \Rightarrow \perp \\
&\quad \quad |[ \perp ] \quad \Rightarrow [ \perp ] \\
&\quad \quad |[ [y] ] \quad \Rightarrow [ [y] ]) \\
&\quad |[ [ \mathbf{false} ] ] \quad \Rightarrow [ [ \mathbf{false} ] ])
\end{aligned}$$

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

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 invalid. For a semantics comprising null, we suggest to stay conform to the standard and define the addition for integers as follows:

$$\begin{aligned}
I[x + y]\tau &= \text{if } I[\delta x]\tau = [ [ \mathbf{true} ] ] \wedge I[\delta y]\tau = [ [ \mathbf{true} ] ] \\
&\quad \text{then } [ [ [ I[x]\tau ] ] + [ [ I[y]\tau ] ] ] \\
&\quad \text{else } \perp
\end{aligned}$$

where the operator “+” on the left-hand side of the equation denotes the OCL addition of type  $[V((\text{int}_{\perp})_{\perp}), V((\text{int}_{\perp})_{\perp})] \Rightarrow V((\text{int}_{\perp})_{\perp})$  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.

### 2.4.2. 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. 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:

$$\tau \models P \equiv (I\llbracket P \rrbracket \tau = \llbracket \text{true} \rrbracket).$$

On this basis, classical, two-valued inference rules can be established for reasoning over the logical connective, 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:

$$\begin{aligned} \tau \models \text{true} \quad \neg(\tau \models \text{false}) \quad \neg(\tau \models \text{invalid}) \quad \neg(\tau \models \text{null}) \\ \tau \models \text{not } P \implies \neg(\tau \models P) \\ \tau \models P \text{ and } Q \implies \tau \models P \quad \tau \models P \text{ and } Q \implies \tau \models Q \\ \tau \models P \implies (\text{if } P \text{ then } B_1 \text{ else } B_2 \text{ endif})\tau = B_1 \tau \\ \tau \models \text{not } P \implies (\text{if } P \text{ then } B_1 \text{ else } B_2 \text{ endif})\tau = B_2 \tau \\ \tau \models P \implies \tau \models \delta P \quad \tau \models \delta X \implies \tau \models v X \end{aligned}$$

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.

We propose to distinguish the *strong logical equality* (written  $_ \triangleq _$ ), which follows the general principle that “equals can be replaced by equals,” from the *strict referential equality* (written  $_ \doteq _$ ), which is an object-oriented concept that attempts to approximate and to implement the former. Strict referential equality, which is the default in the OCL language and is written  $_ = _$  in the standard, is an overloaded concept and has to be defined for each OCL type individually; for objects resulting from class definitions, it is implemented by comparing the references to the objects. In contrast, strong logical equality is a polymorphic concept which is defined once and for all by:

$$I\llbracket X \triangleq Y \rrbracket \tau \equiv \llbracket I\llbracket X \rrbracket \tau = I\llbracket Y \rrbracket \tau \rrbracket$$

It enjoys nearly the laws of a congruence:

$$\begin{aligned} \tau \models (x \triangleq x) \\ \tau \models (x \triangleq y) \implies \tau \models (y \triangleq x) \\ \tau \models (x \triangleq y) \implies \tau \models (y \triangleq z) \implies \tau \models (x \triangleq z) \\ \text{cp } P \implies \tau \models (x \triangleq y) \implies \tau \models (P x) \implies \tau \models (P y) \end{aligned}$$

where the predicate  $\text{cp}$  stands for *context-passing*, a property that is characterized by  $P(X)$  equals  $\lambda \tau. P(\lambda -. X\tau)\tau$ . It means that the state tuple  $\tau = (\sigma, \sigma')$  is passed unchanged from surrounding expressions to sub-expressions. it is true for all pure OCL expressions (but not arbitrary mixtures of OCL and HOL) in Featherweight OCL. The necessary side-calculus for establishing  $\text{cp}$  can be fully automated.

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 [20].  $\delta$ -closure rules for all logical connectives have the following format, e. g.:

$$\begin{aligned} \tau \models \delta x &\implies (\tau \models \mathbf{not} x) = (\neg(\tau \models x)) \\ \tau \models \delta x &\implies \tau \models \delta y \implies (\tau \models x \mathbf{and} y) = (\tau \models x \wedge \tau \models y) \\ \tau \models \delta x &\implies \tau \models \delta y \\ &\implies (\tau \models (x \mathbf{implies} y)) = ((\tau \models x) \longrightarrow (\tau \models y)) \end{aligned}$$

Together with the general case-distinction

$$\tau \models \delta x \vee \tau \models x \triangleq \mathbf{invalid} \vee \tau \models x \triangleq \mathbf{null},$$

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  $\tau \models x \doteq y - 3$  that we have  $\tau \models x \doteq y - 3 \wedge \tau \models \delta x \wedge \tau \models \delta y$ . We call the latter formula the  $\delta$ -closure of the former. Now, we can convert a formula like  $\tau \models x > 0$  or  $3 * y > x * x$  into the equivalent formula  $\tau \models x > 0 \vee \tau \models 3 * y > x * x$  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.

### 2.4.3. 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, where the used equality is the meta-(HOL-)equality.

Our denotational definitions on **not** and **and** can be re-formulated in the following ground equations:

$$\begin{array}{ll} v \mathbf{invalid} = \mathbf{false} & v \mathbf{null} = \mathbf{true} \\ v \mathbf{true} = \mathbf{true} & v \mathbf{false} = \mathbf{true} \\ \delta \mathbf{invalid} = \mathbf{false} & \delta \mathbf{null} = \mathbf{false} \\ \delta \mathbf{true} = \mathbf{true} & \delta \mathbf{false} = \mathbf{true} \\ \mathbf{not} \mathbf{invalid} = \mathbf{invalid} & \mathbf{not} \mathbf{null} = \mathbf{null} \\ \mathbf{not} \mathbf{true} = \mathbf{false} & \mathbf{not} \mathbf{false} = \mathbf{true} \\ (\mathbf{null} \mathbf{and} \mathbf{true}) = \mathbf{null} & (\mathbf{null} \mathbf{and} \mathbf{false}) = \mathbf{false} \\ (\mathbf{null} \mathbf{and} \mathbf{null}) = \mathbf{null} & (\mathbf{null} \mathbf{and} \mathbf{invalid}) = \mathbf{invalid} \\ (\mathbf{false} \mathbf{and} \mathbf{true}) = \mathbf{false} & (\mathbf{false} \mathbf{and} \mathbf{false}) = \mathbf{false} \\ (\mathbf{false} \mathbf{and} \mathbf{null}) = \mathbf{false} & (\mathbf{false} \mathbf{and} \mathbf{invalid}) = \mathbf{false} \end{array}$$

```

(true and true) = true      (true and false) = false
(true and null) = null     (true and invalid) = invalid
      (invalid and true) = invalid
      (invalid and false) = false
      (invalid and null) = invalid
      (invalid and invalid) = invalid

```

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

```

X and X = X      X and Y = Y and X
false and X = false      X and false = false
true and X = X      X and true = X
X and (Y and Z) = X and Y and Z

```

as well as the dual equalities for `_ or _` and the De Morgan rules. This wealth of algebraic properties makes the understanding of the logic easier as well as automated analysis possible: it allows for, for example, computing a DNF of invariant systems (by clever 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 the standard and the major deviation point from HOL-OCL [6, 8], to Featherweight OCL as presented here. The standard expresses at many places that most operations are strict, i. e., enjoy the properties (exemplary for `_ + _`):

```

invalid + X = invalid      X + invalid = invalid
X + null = invalid        null + X = invalid
null.oclAsType(X) = invalid

```

besides “classical” exceptional behavior:

```

1 / 0 = invalid      1 / null = invalid
null->isEmpty() = true

```

Moreover, there is also the proposal to use `null` as a kind of “don’t know” value for all strict operations, not only in the semantics of the logical connectives. Expressed in algebraic equations, this semantic alternative (this is *not* Featherweight OCL at present) would boil down to:

```

invalid + X = invalid      X + invalid = invalid
X + null = null           null + X = null
null.oclAsType(X) = null
1 / 0 = invalid      1 / null = null
null->isEmpty() = null

```

While this is logically perfectly possible, while it can be argued that this semantics is “intuitive”, and although we do not expect a too heavy cost in deduction when computing



$\delta$ -closures, we object that there are other, also “intuitive” interpretations that are even more wide-spread: In classical spreadsheet programs, for example, the semantics tends to interpret `null` (representing empty cells in a sheet) as the neutral element of the type, so 0 or the empty string, for example.<sup>2</sup> This semantic alternative (this is *not* Featherweight OCL at present) would yield:

```

invalid + X = invalid      X + invalid = invalid
X + null = X              null + X = X
      null.oclAsType(X) = invalid
1 / 0 = invalid          1 / null = invalid
      null->isEmpty() = true

```

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

```

       $\delta$  Set{} = true
       $\delta$  (X->including(x)) =  $\delta$  X and  $\delta$  x
Set{}->includes(x) = (if v x then false
                    else invalid endif)
(X->including(x)->includes(y)) =
  (if  $\delta$  X
   then if x  $\doteq$  y
        then true
        else X->includes(y)
        endif
   else invalid
   endif)

```

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

---

```
Set{}->including(1)->including(2)
```

---

an expression like `Set{1,2}->includes(null)` becomes decidable in Featherweight OCL by a combination of rewriting and code-generation and execution. The generated documentation from the theory files can thus be enriched by numerous “test-statements” like:

```
value "  $\tau \models (\text{Set}\{\text{Set}\{2, \text{null}\}\} \doteq \text{Set}\{\text{Set}\{\text{null}, 2\}\})$ "
```

which have been machine-checked and which present a high-level and in our opinion fairly readable information for OCL tool manufacturers and users.

---

<sup>2</sup>In spreadsheet programs the interpretation of `null` varies from operation to operation; e. g., the `average` function treats `null` as non-existing value and not as 0.

## 2.5. Object-oriented Datatype Theories

As mentioned earlier, the OCL is composed of

1. operators on built-in data structures such as Boolean, Integer or Set(-), and
2. operators of the user-defined data model such as accessors, type casts and tests.

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. In contrast to wide-spread opinions, UML class diagrams represent in a compact and visual manner quite complex, object-oriented data-types with a surprisingly rich theory. It is part of our endeavor here to make this theory explicit and to point out corner cases. A UML class diagram—underlying a given OCL formula—produces several implicit operations which become accessible via appropriate OCL syntax:

1. Classes and class names (written as  $C_1, \dots, C_n$ ), which become types of data in OCL. Class names declare two projector functions to the set of all objects in a state:  $C_i.allInstances()$  and  $C_i.allInstances@pre()$ ,
2. an inheritance relation  $- < -$  on classes and a collection of attributes  $A$  associated to classes,
3. two families of accessors; for each attribute  $a$  in a class definition (denoted  $X.a :: C_i \rightarrow A$  and  $X.a@pre :: C_i \rightarrow A$  for  $A \in \{V(\dots), C_1, \dots, C_n\}$ ),
4. type casts that can change the static type of an object of a class ( $X.oclAsType(C_i)$  of type  $C_j \rightarrow C_i$ )
5. two dynamic type tests ( $X.oclIsTypeOf(C_i)$  and  $X.oclIsKindOf(C_i)$  ),
6. and last but not least, for each class name  $C_i$  there is an instance of the overloaded referential equality (written  $- \doteq -$ ).

Assuming a strong static type discipline in the sense of Hindley-Milner types, Featherweight OCL has no “syntactic subtyping.” This does not mean that subtyping cannot be expressed *semantically* in Featherweight OCL; by giving a formal semantics to type-casts, subtyping becomes an issue of the front-end that can make implicit type-coersions explicit by introducing explicit type-casts. 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.

### 2.5.1. Object Universes

It is natural to construct system states by a set of partial functions  $f$  that map object identifiers oid to some representations of objects:

$$\text{typedef } \alpha \text{ state} := \{\sigma :: \text{oid} \rightarrow \alpha \mid \text{inv}_\sigma(\sigma)\} \quad (2.12)$$

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

The key point is that we need a common type  $\alpha$  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 injectively 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 for 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, we 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:  $C_i := (\text{oid} \times A_{i_1} \times \cdots \times A_{i_k})$  where the types  $A_{i_1}, \dots, A_{i_k}$  are the attribute types (including inherited attributes) with class types substituted by oid. The function  $\text{OidOf}$  projects the first component, the oid, out of an object representation. Then the object universe will be constructed by the type definition:

$$\mathfrak{A} := C_1 + \cdots + C_n. \quad (2.13)$$

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 losing information, such that casting up and casting down will *not* give the required identity:

$$X.\text{oclIsTypeOf}(C_k) \text{ implies } X.\text{oclAsType}(C_i).\text{oclAsType}(C_k) \doteq X \quad (2.14)$$

$$\text{whenever } C_k < C_i \text{ and } X \text{ is valid.} \quad (2.15)$$

To overcome this limitation, we introduce an auxiliary type  $C_{i\text{ext}}$  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  $\{C_{j_1}, \dots, C_{j_m}\}$ .

- Then the *class type extension*  $C_{i\text{ext}}$  associated to  $C_i$  is  $A_{i_1} \times \cdots \times A_{i_n} \times (C_{j_1\text{ext}} + \cdots + C_{j_m\text{ext}})_\perp$  where  $A_{i_k}$  ranges over the local attribute types of  $C_i$  and  $C_{j_l\text{ext}}$  ranges over all class type extensions of the subclass  $C_j$  of  $C_i$ .

- Then the *class type* for  $C_i$  is  $oid \times A_{i_1} \times \cdots \times A_{i_n} \times (C_{j_1\text{ext}} + \cdots + C_{j_m\text{ext}})_{\perp}$  where  $A_{i_k}$  ranges over the inherited *and* local attribute types of  $C_i$  and  $C_{j_l\text{ext}}$  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 Section 6.1 and Section 7.1.

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 a 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 Section 6.1 and Section 7.1 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 paper which has a focus on the semantic construction and its presentation.

### 2.5.2. 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 *dereferentiation* phase. The oid is interpreted in the pre- or post-state, the resulting object is casted to the expected format. The exceptional case of nonexistence 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 dereferentiation in one of the states to produce an object representation again. The exceptional case of nonexistence in this state must be treated.

The first phase directly translates into the following formalization:

**definition**

$$\text{eval\_extract } X \ f = (\lambda \tau. \text{ case } X \ \tau \text{ of } \begin{array}{ll} \perp & \Rightarrow \text{invalid } \tau \quad \text{exception} \\ | \ \lfloor \perp \rfloor & \Rightarrow \text{invalid } \tau \quad \text{deref. null} \\ | \ \lfloor \text{obj} \rfloor & \Rightarrow f (\text{oid\_of } \text{obj}) \ \tau \end{array}) \quad (2.16)$$

For each class  $C$ , we introduce the dereferentiation phase of this form:

$$\text{definition } \text{deref\_oid}_C \ f \ \text{oid} = (\lambda \tau. \text{ case } (\text{heap } (\text{fst\_snd } \tau)) \ \text{oid} \ \text{of } \begin{array}{ll} \lfloor \text{in}_C \ \text{obj} \rfloor & \Rightarrow f \ \text{obj} \ \tau \\ | \ \_ & \Rightarrow \text{invalid } \tau \end{array}) \quad (2.17)$$

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:

$$\text{definition } \text{select}_a \ f = (\lambda \ \text{mk}_C \ \text{oid} \ \dots \ \perp \ \dots \ C_{X_{\text{ext}}} \Rightarrow \text{null} \quad (2.18) \\ | \ \text{mk}_C \ \text{oid} \ \dots \ \lfloor a \rfloor \ \dots \ C_{X_{\text{ext}}} \Rightarrow f (\lambda \ x \ \_ \ \lfloor x \rfloor) \ a)$$

This works for definitions of basic values as well as for object references in which the  $a$  is of type oid. To increase readability, we introduce the functions:

$$\begin{array}{lll} \text{definition} & \text{in\_pre\_state} & = \text{fst} & \text{first component} \\ \text{definition} & \text{in\_post\_state} & = \text{snd} & \text{second component} \\ \text{definition} & \text{reconst\_basetype} & = \text{id} & \text{identity function} \end{array} \quad (2.19)$$

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:

$$\begin{array}{ll} \text{definition} & \_.\text{getBase} \quad :: C \Rightarrow A_{\text{base}} \\ \text{where} & X.\text{getBase} = \text{eval\_extract } X \ (\text{deref\_oid}_C \ \text{in\_post\_state} \\ & \quad (\text{select}_{\text{getBase}} \ \text{reconst\_basetype})) \end{array} \quad (2.20)$$

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:

$$\begin{array}{ll} \text{definition} & \_.\text{getObject} \quad :: C \Rightarrow A_{\text{object}} \\ \text{where} & X.\text{getObject} = \text{eval\_extract } X \ (\text{deref\_oid}_C \ \text{in\_post\_state} \\ & \quad (\text{select}_{\text{getObject}} (\text{deref\_oid}_C \ \text{in\_post\_state}))) \end{array} \quad (2.21)$$

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@pre` were produced when `in_post_state` is replaced by `in_pre_state`.

Examples for the construction of accessors via associations can be found in Section 6.1.8, the construction of accessors via attributes in Section 7.1.8. The construction of casts and type tests `->oclIsTypeOf()` and `->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 `Set` or `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 `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 `Set` is not defined by the standard. We argue that the resulting set cannot be constructed the same way as when evaluating a `Set` literal. Otherwise, `null` would be mapped to the singleton set containing `null`, but the standard demands that the resulting set is empty in this case. The conversion should instead be defined as follows:

```
context OclAny::asSet():T
  post: if self = null then result = Set{}
        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 `null` can belong to this collection. The OCL standard states that `null` can be owned by collections. However, if an attribute can evaluate to a collection containing `null`, it is not clear how multiplicity constraints should be interpreted for this attribute. The question arises whether the `null` element should be counted or not when determining the cardinality of the collection. Recall that `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.<sup>3</sup> In case a multiplicity is specified for an attribute, i. e., a lower and an upper bound are provided, we require any collection the attribute evaluates to not contain `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:

---

```
context C inv lowerBound: a->size() >= m
           inv upperBound: a->size() <= n
           inv notNull: not a->includes(null)
```

---

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 2.5.2. 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.

### 2.5.3. Other Operations on States

Defining `_.allInstances()` is straight-forward; the only difference is the property `T.allInstances()->excludes(null)` which is a consequence of the fact that `null`'s are values and do not “live” in the state. In our semantics which admits states with

---

<sup>3</sup>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.

“dangling references,” it is possible to define a counterpart to `_.oclIsNew()` called `_.oclIsDeleted()` which asks if an object id (represented by an object representation) is contained in the pre-state, but not the post-state.

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 : Set (OclAny)) -> oclIsModifiedOnly () : 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:

$$I\llbracket X \rightarrow \text{oclIsModifiedOnly}() \rrbracket(\sigma, \sigma') \equiv \begin{cases} \perp & \text{if } X' = \perp \vee \text{null} \in X' \\ \bigwedge_{i \in M} \sigma \ i = \sigma' \ i & \text{otherwise.} \end{cases}$$

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

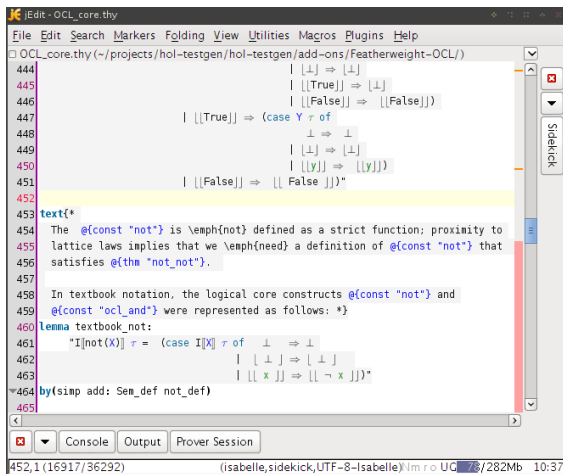
## 2.6. A Machine-checked Annex A

Isabelle, as a framework for building formal tools [37], 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.

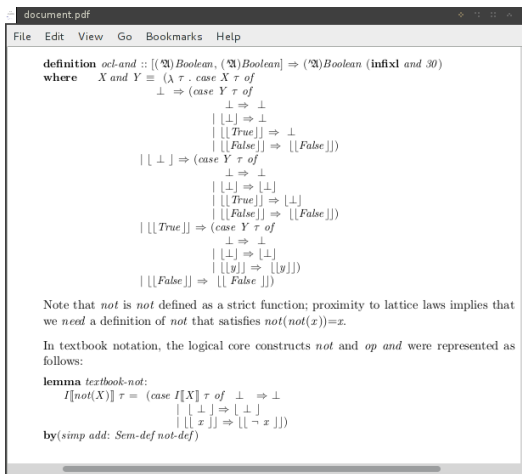
For writing documents, Isabelle supports the embedding of informal texts using a  $\text{\LaTeX}$ -based markup language within the theory files. To ensure the consistency, Isabelle supports to use, within these informal texts, *antiquotations* that refer to the formal parts and that are checked while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

Figure 2.2 illustrates this approach: Figure 2.2a shows the jEdit-based development environment of Isabelle with an excerpt of one of the core theories of Featherweight OCL. Figure 2.2b 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.





(a) The Isabelle jEdit environment.



(b) The generated formal document.

Figure 2.2.: Generating documents with guaranteed syntactical and semantical consistency.

Thus, applying the Featherweight OCL approach to writing an updated Annex A that provides a formal semantics of the most fundamental concepts of OCL would ensure

1. that all formal context is syntactically correct and well-typed, and
2. all formal definitions and the derived logical rules are semantically consistent.

Overall, this would contribute to one of the main goals of the OCL 2.5 RFP, as discussed at the OCL meeting in Aachen [15].



**Part II.**

**A Proposal for Formal Semantics of  
OCL 2.5**



## 3. Formalization I: Core Definitions

```
theory
  OCL-core
imports
  Main
begin
```

### 3.1. Preliminaries

#### 3.1.1. 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:

```
notation Some ( $\llbracket(-)\rrbracket$ )
notation None ( $\perp$ )
```

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

```
fun drop :: 'α option ⇒ 'α ( $\llbracket(-)\rrbracket$ )
where drop-lift[simp]:  $\llbracket\llbracket v \rrbracket\rrbracket = v$ 
```

#### 3.1.2. Minimal Notions of State and State Transitions

Next we will introduce the foundational concept of an object id (oid), which is just some infinite set.

In order to assure executability of as much as possible formulas, we fixed the type of object id's to just natural numbers.

```
type-synonym oid = nat
```

We refrained from the alternative:

```
type-synonym oid = ind
```

which is slightly more abstract but non-executable.

States are just a partial map from oid's to elements of an object universe  $\mathfrak{A}$ , and state transitions pairs of states ...

```
record ('A)state =
  heap :: oid → 'A
  assocs2 :: oid → (oid × oid) list
  assocs3 :: oid → (oid × oid × oid) list
```

**type-synonym** ( $'\mathcal{A}$ )*st* =  $'\mathcal{A}$  *state* ×  $'\mathcal{A}$  *state*

### 3.1.3. Prerequisite: An Abstract Interface for OCL Types

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  $\lfloor \perp \rfloor$  on  $'a$  *option option*) to a *null* element, which may have an arbitrary semantic structure, and an undefinedness element  $\perp$  to an abstract undefinedness element *bot* (also written  $\perp$  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.

```
class  bot =
  fixes bot :: 'a
  assumes nonEmpty :  $\exists x. x \neq bot$ 
```

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

### 3.1.4. 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**, ...).

```
instantiation  option :: (type)bot
begin
  definition bot-option-def: (bot::'a option)  $\equiv$  (None::'a option)
  instance  $\langle proof \rangle$ 
end
```

```
instantiation  option :: (bot)null
```

```

begin
  definition null-option-def: (null::'a::bot option)  $\equiv$  [ bot ]
  instance  $\langle$ proof $\rangle$ 
end

```

```

instantiation fun :: (type,bot) bot
begin
  definition bot-fun-def: bot  $\equiv$  ( $\lambda$  x. bot)

  instance  $\langle$ proof $\rangle$ 
end

```

```

instantiation fun :: (type,null) null
begin
  definition null-fun-def: (null::'a  $\Rightarrow$  'b::null)  $\equiv$  ( $\lambda$  x. null)

  instance  $\langle$ proof $\rangle$ 
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).

### 3.1.5. The Semantic Space of OCL Types: Valuations

Valuations are now 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** ( $\mathcal{A}, \alpha$ ) *val* =  $\mathcal{A}$  *st*  $\Rightarrow$   $\alpha$ ::*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:

**definition** *Sem* :: 'a  $\Rightarrow$  'a (*I*[-])  
**where** *I*[[*x*]]  $\equiv$  *x*

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* :: ( $\mathcal{A}, \alpha$ ::*bot*) *val*  
**where** *invalid*  $\equiv$   $\lambda$   $\tau$ . *bot*

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

**lemma** *textbook-invalid*: *I*[[*invalid*]] $\tau$  = *bot*

*<proof>*

Note that the definition :

**definition**  $\text{null} :: \text{"('}\mathfrak{A}, \text{'}\alpha :: \text{null)} \text{ val"}$   
**where**  $\text{"null} \equiv \lambda \tau. \text{null"}$

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  $\text{null}$  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*:  $I[\text{null}::(\mathfrak{A}, \alpha::\text{null}) \text{ val}] \tau = (\text{null}::\alpha::\text{null})$   
*<proof>*

## 3.2. Definition of the Boolean Type

The semantic domain of the (basic) boolean type is now defined as the Standard: the space of valuation to *bool option option*:

**type-synonym**  $(\mathfrak{A})\text{Boolean} = (\mathfrak{A}, \text{bool option option}) \text{ val}$

### 3.2.1. Basic Constants

**lemma** *bot-Boolean-def* :  $(\text{bot}::(\mathfrak{A})\text{Boolean}) = (\lambda \tau. \perp)$   
*<proof>*

**lemma** *null-Boolean-def* :  $(\text{null}::(\mathfrak{A})\text{Boolean}) = (\lambda \tau. \lfloor \perp \rfloor)$   
*<proof>*

**definition**  $\text{true} :: (\mathfrak{A})\text{Boolean}$   
**where**  $\text{true} \equiv \lambda \tau. \lfloor \text{True} \rfloor$

**definition**  $\text{false} :: (\mathfrak{A})\text{Boolean}$   
**where**  $\text{false} \equiv \lambda \tau. \lfloor \text{False} \rfloor$

**lemma** *bool-split*:  $X \tau = \text{invalid } \tau \vee X \tau = \text{null } \tau \vee$   
 $X \tau = \text{true } \tau \quad \vee X \tau = \text{false } \tau$   
*<proof>*

**lemma** [*simp*]:  $\text{false } (a, b) = \lfloor \text{False} \rfloor$   
*<proof>*

**lemma** [*simp*]:  $\text{true } (a, b) = \lfloor \text{True} \rfloor$   
*<proof>*

**lemma** *textbook-true*:  $I[\text{true}] \tau = \lfloor \text{True} \rfloor$   
*<proof>*



**lemma** *textbook-false*:  $I[\text{false}] \tau = \llbracket \text{False} \rrbracket$   
 ⟨proof⟩

| Name                     | Theorem   |
|--------------------------|---|
| <i>textbook-invalid</i>  | $I[\text{invalid}] \tau = \text{OCL-core.bot-class.bot}$    |
| <i>textbook-null-fun</i> | $I[\text{null}] \tau = \text{null}$                         |
| <i>textbook-true</i>     | $I[\text{true}] \tau = \llbracket \text{True} \rrbracket$   |
| <i>textbook-false</i>    | $I[\text{false}] \tau = \llbracket \text{False} \rrbracket$ |

Table 3.1.: Basic semantic constant definitions of the logic (except *null*)

### 3.2.2. Validity and Definedness

However, this has also the consequence that core concepts like definedness, validness and even *cp* have to be redefined on this type class:

**definition** *valid* ::  $(\mathfrak{A}, 'a::\text{null})\text{val} \Rightarrow (\mathfrak{A})\text{Boolean} (v - [100]100)$   
**where**  $v X \equiv \lambda \tau . \text{if } X \tau = \text{bot } \tau \text{ then false } \tau \text{ else true } \tau$

**lemma** *valid1[simp]*:  $v \text{ invalid} = \text{false}$   
 ⟨proof⟩

**lemma** *valid2[simp]*:  $v \text{ null} = \text{true}$   
 ⟨proof⟩

**lemma** *valid3[simp]*:  $v \text{ true} = \text{true}$   
 ⟨proof⟩

**lemma** *valid4[simp]*:  $v \text{ false} = \text{true}$   
 ⟨proof⟩

**lemma** *cp-valid*:  $(v X) \tau = (v (\lambda \tau . X \tau)) \tau$   
 ⟨proof⟩

**definition** *defined* ::  $(\mathfrak{A}, 'a::\text{null})\text{val} \Rightarrow (\mathfrak{A})\text{Boolean} (\delta - [100]100)$   
**where**  $\delta X \equiv \lambda \tau . \text{if } X \tau = \text{bot } \tau \vee X \tau = \text{null } \tau \text{ then false } \tau \text{ else true } \tau$

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

**lemma** *defined1[simp]*:  $\delta \text{ invalid} = \text{false}$   
 ⟨proof⟩

**lemma** *defined2[simp]*:  $\delta \text{ null} = \text{false}$   
 $\langle \text{proof} \rangle$

**lemma** *defined3[simp]*:  $\delta \text{ true} = \text{true}$   
 $\langle \text{proof} \rangle$

**lemma** *defined4[simp]*:  $\delta \text{ false} = \text{true}$   
 $\langle \text{proof} \rangle$

**lemma** *defined5[simp]*:  $\delta \delta X = \text{true}$   
 $\langle \text{proof} \rangle$

**lemma** *defined6[simp]*:  $\delta v X = \text{true}$   
 $\langle \text{proof} \rangle$

**lemma** *valid5[simp]*:  $v v X = \text{true}$   
 $\langle \text{proof} \rangle$

**lemma** *valid6[simp]*:  $v \delta X = \text{true}$   
 $\langle \text{proof} \rangle$

**lemma** *cp-defined*:  $(\delta X) \tau = (\delta (\lambda -. X \tau)) \tau$   
 $\langle \text{proof} \rangle$

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

**lemma** *textbook-defined*:  $I[\delta(X)] \tau = (\text{if } I[X] \tau = I[\text{bot}] \tau \vee I[X] \tau = I[\text{null}] \tau$   
 $\text{then } I[\text{false}] \tau$   
 $\text{else } I[\text{true}] \tau)$

$\langle \text{proof} \rangle$

**lemma** *textbook-valid*:  $I[v(X)] \tau = (\text{if } I[X] \tau = I[\text{bot}] \tau$   
 $\text{then } I[\text{false}] \tau$   
 $\text{else } I[\text{true}] \tau)$

$\langle \text{proof} \rangle$

Table 3.2 and Table 3.3 summarize the results of this section.

| Name                    | Theorem   |
|-------------------------|---|
| <i>textbook-defined</i> | $I[\delta X] \tau = (\text{if } I[X] \tau = I[\text{OCL-core.bot-class.bot}] \tau \vee I[X] \tau = I[\text{null}] \tau \text{ then } I[\text{false}] \tau \text{ else } I[\text{true}] \tau)$ |
| <i>textbook-valid</i>   | $I[v X] \tau = (\text{if } I[X] \tau = I[\text{OCL-core.bot-class.bot}] \tau \text{ then } I[\text{false}] \tau \text{ else } I[\text{true}] \tau)$   |

Table 3.2.: Basic predicate definitions of the logic.

| Name            | Theorem                                 |
|-----------------|---|
| <i>defined1</i> | $\delta \text{ invalid} = \text{false}$ |
| <i>defined2</i> | $\delta \text{ null} = \text{false}$    |
| <i>defined3</i> | $\delta \text{ true} = \text{true}$     |
| <i>defined4</i> | $\delta \text{ false} = \text{true}$    |
| <i>defined5</i> | $\delta \delta ?X = \text{true}$        |
| <i>defined6</i> | $\delta v ?X = \text{true}$             |

Table 3.3.: Laws of the basic predicates of the logic.

### 3.3. The Equalities of OCL

The OCL contains a particular version of equality, written in Standard documents  $_ = _$  and  $_ \langle \rangle _$  for its negation, which is referred as *weak referential equality* hereafter and for which we use the symbol  $_ \doteq _$  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  $_ \triangleq _$  which is not present in the current standard but was discussed in prior texts on OCL like the Amsterdam Manifesto [19] and was identified as desirable extension of OCL in the Aachen Meeting [15] 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  $a.\text{boss} \triangleq b.\text{boss@pre}$  instead of

$a.\text{boss} \doteq b.\text{boss@pre}$  **and** *(\* just the pointers are equal! \*)*  
 $a.\text{boss.name} \doteq b.\text{boss@pre.name@pre}$  **and**  
 $a.\text{boss.age} \doteq b.\text{boss@pre.age@pre}$

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”  $_ = _ :: \alpha * \alpha \rightarrow bool$ —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:

$$s = t \implies P(s) = P(t) \tag{3.1}$$

“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.

### 3.3.1. 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** *StrongEq*:: $['\mathfrak{A} \ st \Rightarrow '\alpha, '\mathfrak{A} \ st \Rightarrow '\alpha] \Rightarrow (''\mathfrak{A})Boolean \ (\mathbf{infixl} \triangleq 30)$   
**where**  $X \triangleq Y \equiv \lambda \tau. \llbracket X \ \tau = Y \ \tau \rrbracket$

From this follow already elementary properties like:

**lemma** [*simp,code-unfold*]:  $(true \triangleq false) = false$   
*<proof>*

**lemma** [*simp,code-unfold*]:  $(false \triangleq true) = false$   
*<proof>*

In contrast, referential equality behaves differently for all types—on value types, it is basically strong equality for defined values, but on object types it will compare references—we introduce it as an *overloaded* concept and will handle it for each type instance individually.

**consts** *StrictRefEq* ::  $[(('\mathfrak{A}, 'a)val, (''\mathfrak{A}, 'a)val)] \Rightarrow (''\mathfrak{A})Boolean \ (\mathbf{infixl} \doteq 30)$

Here is a first instance of a definition of weak equality—for the special case of the type  $\mathcal{A}$  *Boolean*, it is just the strict extension of the logical equality:

```
defs (overloaded) StrictRefEqBoolean[code-unfold] :
  (x::( $\mathcal{A}$ )Boolean)  $\doteq$  y  $\equiv$   $\lambda$   $\tau$ . if (v x)  $\tau$  = true  $\tau$   $\wedge$  (v y)  $\tau$  = true  $\tau$ 
    then (x  $\triangleq$  y) $\tau$ 
    else invalid  $\tau$ 
```

which implies elementary properties like:

```
lemma [simp,code-unfold] : (true  $\doteq$  false) = false
<proof>
```

```
lemma [simp,code-unfold] : (false  $\doteq$  true) = false
<proof>
```

```
lemma [simp,code-unfold] : (invalid  $\doteq$  false) = invalid
<proof>
```

```
lemma [simp,code-unfold] : (invalid  $\doteq$  true) = invalid
<proof>
```

```
lemma [simp,code-unfold] : (false  $\doteq$  invalid) = invalid
<proof>
```

```
lemma [simp,code-unfold] : (true  $\doteq$  invalid) = invalid
<proof>
```

```
lemma [simp,code-unfold] : ((invalid::( $\mathcal{A}$ )Boolean)  $\doteq$  invalid) = invalid
<proof>
```

Thus, the weak equality is *not* reflexive.

```
lemma null-non-false [simp,code-unfold]:(null  $\doteq$  false) = false
<proof>
```

```
lemma null-non-true [simp,code-unfold]:(null  $\doteq$  true) = false
<proof>
```

```
lemma false-non-null [simp,code-unfold]:(false  $\doteq$  null) = false
<proof>
```

```
lemma true-non-null [simp,code-unfold]:(true  $\doteq$  null) = false
<proof>
```

### 3.3.2. Fundamental Predicates on Strong Equality

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

```
lemma StrongEq-refl [simp]: (X  $\triangleq$  X) = true
<proof>
```

```
lemma StrongEq-sym: (X  $\triangleq$  Y) = (Y  $\triangleq$  X)
<proof>
```

**lemma** *StrongEq-trans-strong* [simp]:

**assumes**  $A: (X \triangleq Y) = true$

**and**  $B: (Y \triangleq Z) = true$

**shows**  $(X \triangleq Z) = true$

*<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**  $cp: \bigwedge X. P(X)\tau = P(\lambda -. X \tau)\tau$

**and**  $eq: (X \triangleq Y)\tau = true \tau$

**shows**  $(P X \triangleq P Y)\tau = true \tau$

*<proof>*

**lemma** *defined7*[simp]:  $\delta (X \triangleq Y) = true$

*<proof>*

**lemma** *valid7*[simp]:  $v (X \triangleq Y) = true$

*<proof>*

**lemma** *cp-StrongEq*:  $(X \triangleq Y) \tau = ((\lambda -. X \tau) \triangleq (\lambda -. Y \tau)) \tau$

*<proof>*

### 3.4. 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* ::  $(\mathfrak{A})Boolean \Rightarrow (\mathfrak{A})Boolean (not)$

**where**  $not\ X \equiv \lambda\ \tau .\ case\ X\ \tau\ of$   
 $\quad \perp \quad \Rightarrow \perp$   
 $\quad | \ [\perp] \quad \Rightarrow \ [\perp]$   
 $\quad | \ [x] \quad \Rightarrow \ [ \neg\ x ]$

with term "not" we can express the notation:

**syntax**

$notequal \quad ::\ ('A)Boolean \Rightarrow ('A)Boolean \Rightarrow ('A)Boolean \quad (\mathbf{infix}\ <>\ 40)$

**translations**

$a\ <>\ b ==\ CONST\ OclNot\ (a \doteq b)$

**lemma**  $cp\ OclNot$ :  $(not\ X)\tau = (not\ (\lambda\ -. X\ \tau))\ \tau$   
 $\langle proof \rangle$

**lemma**  $OclNot1[simp]$ :  $not\ invalid = invalid$   
 $\langle proof \rangle$

**lemma**  $OclNot2[simp]$ :  $not\ null = null$   
 $\langle proof \rangle$

**lemma**  $OclNot3[simp]$ :  $not\ true = false$   
 $\langle proof \rangle$

**lemma**  $OclNot4[simp]$ :  $not\ false = true$   
 $\langle proof \rangle$

**lemma**  $OclNot\ not[simp]$ :  $not\ (not\ X) = X$   
 $\langle proof \rangle$

**lemma**  $OclNot\ inject$ :  $\bigwedge\ x\ y.\ not\ x = not\ y \implies x = y$   
 $\langle proof \rangle$

**definition**  $OclAnd$  ::  $[('A)Boolean, ('A)Boolean] \Rightarrow ('A)Boolean \quad (\mathbf{infix1}\ and\ 30)$

**where**  $X\ and\ Y \equiv (\lambda\ \tau .\ case\ X\ \tau\ of$

$$\begin{aligned} & \quad | \ [False] \quad \Rightarrow \quad [False] \\ & \quad | \ \perp \quad \Rightarrow \ (case\ Y\ \tau\ of \\ & \quad \quad | \ [False] \quad \Rightarrow \ [False] \\ & \quad \quad | \ - \quad \Rightarrow \ \perp) \\ & \quad | \ [\perp] \quad \Rightarrow \ (case\ Y\ \tau\ of \\ & \quad \quad | \ [False] \quad \Rightarrow \ [False] \\ & \quad \quad | \ \perp \quad \Rightarrow \ \perp \\ & \quad \quad | \ - \quad \Rightarrow \ [\perp]) \\ & \quad | \ [True] \quad \Rightarrow \quad Y\ \tau) \end{aligned}$$

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 *op and* were represented as follows:

**lemma** *textbook-OclNot*:

$$I[\text{not}(X)] \tau = (\text{case } I[X] \tau \text{ of } \perp \Rightarrow \perp \\ | [\perp] \Rightarrow [\perp] \\ | [[x]] \Rightarrow [[\neg x]])$$

*<proof>*

**lemma** *textbook-OclAnd*:

$$I[X \text{ and } Y] \tau = (\text{case } I[X] \tau \text{ of } \perp \Rightarrow (\text{case } I[Y] \tau \text{ of } \perp \Rightarrow \perp \\ | [\perp] \Rightarrow \perp \\ | [[True]] \Rightarrow \perp \\ | [[False]] \Rightarrow [[False]]) \\ | [\perp] \Rightarrow (\text{case } I[Y] \tau \text{ of } \perp \Rightarrow \perp \\ | [\perp] \Rightarrow [\perp] \\ | [[True]] \Rightarrow [\perp] \\ | [[False]] \Rightarrow [[False]]) \\ | [[True]] \Rightarrow (\text{case } I[Y] \tau \text{ of } \perp \Rightarrow \perp \\ | [\perp] \Rightarrow [\perp] \\ | [[y]] \Rightarrow [[y]]) \\ | [[False]] \Rightarrow [[False]])$$

*<proof>*

**definition** *OclOr* ::  $(\mathfrak{A})\text{Boolean}, (\mathfrak{A})\text{Boolean} \Rightarrow (\mathfrak{A})\text{Boolean}$  (infixl or 25)  
**where**  $X \text{ or } Y \equiv \text{not}(\text{not } X \text{ and } \text{not } Y)$

**definition** *OclImplies* ::  $(\mathfrak{A})\text{Boolean}, (\mathfrak{A})\text{Boolean} \Rightarrow (\mathfrak{A})\text{Boolean}$  (infixl implies 25)  
**where**  $X \text{ implies } Y \equiv \text{not } X \text{ or } Y$

**lemma** *cp-OclAnd*:  $(X \text{ and } Y) \tau = ((\lambda -. X \tau) \text{ and } (\lambda -. Y \tau)) \tau$   
*<proof>*

**lemma** *cp-OclOr*:  $((X :: (\mathfrak{A})\text{Boolean}) \text{ or } Y) \tau = ((\lambda -. X \tau) \text{ or } (\lambda -. Y \tau)) \tau$   
*<proof>*

**lemma** *cp-OclImplies*:  $(X \text{ implies } Y) \tau = ((\lambda -. X \tau) \text{ implies } (\lambda -. Y \tau)) \tau$   
*<proof>*

**lemma** *OclAnd1[simp]*:  $(\text{invalid and true}) = \text{invalid}$   
*<proof>*

**lemma** *OclAnd2[simp]*:  $(\text{invalid and false}) = \text{false}$   
*<proof>*

**lemma** *OclAnd3[simp]*:  $(\text{invalid and null}) = \text{invalid}$   
*<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** *OclAnd13[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-idem[simp]: (X and X) = X*  
*<proof>*

**lemma** *OclAnd-commute: (X and Y) = (Y and X)*  
*<proof>*

**lemma** *OclAnd-false1[simp]: (false and X) = false*  
*<proof>*

**lemma** *OclAnd-false2[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]*:  $\bigwedge \tau. X \tau \neq \text{false } \tau \implies (\text{bot and } X) \tau = \text{bot } \tau$   
*<proof>*

**lemma** *OclAnd-bot2[simp]*:  $\bigwedge \tau. X \tau \neq \text{false } \tau \implies (X \text{ and bot}) \tau = \text{bot } \tau$   
*<proof>*

**lemma** *OclAnd-null1[simp]*:  $\bigwedge \tau. X \tau \neq \text{false } \tau \implies X \tau \neq \text{bot } \tau \implies (\text{null and } X) \tau = \text{null } \tau$   
*<proof>*

**lemma** *OclAnd-null2[simp]*:  $\bigwedge \tau. X \tau \neq \text{false } \tau \implies X \tau \neq \text{bot } \tau \implies (X \text{ and null}) \tau = \text{null } \tau$   
*<proof>*

**lemma** *OclAnd-assoc*:  $(X \text{ and } (Y \text{ and } Z)) = (X \text{ and } Y \text{ and } Z)$   
*<proof>*

**lemma** *OclOr1[simp]*:  $(\text{invalid or true}) = \text{true}$   
*<proof>*

**lemma** *OclOr2[simp]*:  $(\text{invalid or false}) = \text{invalid}$   
*<proof>*

**lemma** *OclOr3[simp]*:  $(\text{invalid or null}) = \text{invalid}$   
*<proof>*

**lemma** *OclOr4[simp]*:  $(\text{invalid or invalid}) = \text{invalid}$   
*<proof>*

**lemma** *OclOr5[simp]*:  $(\text{null or true}) = \text{true}$   
*<proof>*

**lemma** *OclOr6[simp]*:  $(\text{null or false}) = \text{null}$   
*<proof>*

**lemma** *OclOr7[simp]*:  $(\text{null or null}) = \text{null}$   
*<proof>*

**lemma** *OclOr8[simp]*:  $(\text{null or invalid}) = \text{invalid}$   
*<proof>*

**lemma** *OclOr-idem[simp]*:  $(X \text{ or } X) = X$   
*<proof>*

**lemma** *OclOr-commute*:  $(X \text{ or } Y) = (Y \text{ or } X)$   
*<proof>*

**lemma** *OclOr-false1[simp]*:  $(\text{false or } Y) = Y$   
*<proof>*

**lemma** *OclOr-false2[simp]*:  $(Y \text{ or false}) = Y$   
*<proof>*

**lemma** *OclOr-true1[simp]*:  $(\text{true or } Y) = \text{true}$   
*<proof>*

**lemma** *OclOr-true2*:  $(Y \text{ or } true) = true$   
*<proof>*

**lemma** *OclOr-bot1[simp]*:  $\bigwedge \tau. X \ \tau \neq true \ \tau \implies (bot \text{ or } X) \ \tau = bot \ \tau$   
*<proof>*

**lemma** *OclOr-bot2[simp]*:  $\bigwedge \tau. X \ \tau \neq true \ \tau \implies (X \text{ or } bot) \ \tau = bot \ \tau$   
*<proof>*

**lemma** *OclOr-null1[simp]*:  $\bigwedge \tau. X \ \tau \neq true \ \tau \implies X \ \tau \neq bot \ \tau \implies (null \text{ or } X) \ \tau = null \ \tau$   
*<proof>*

**lemma** *OclOr-null2[simp]*:  $\bigwedge \tau. X \ \tau \neq true \ \tau \implies X \ \tau \neq bot \ \tau \implies (X \text{ or } null) \ \tau = null \ \tau$   
*<proof>*

**lemma** *OclOr-assoc*:  $(X \text{ or } (Y \text{ or } Z)) = (X \text{ or } Y \text{ or } Z)$   
*<proof>*

**lemma** *OclImplies-true*:  $(X \text{ implies } true) = true$   
*<proof>*

**lemma** *deMorgan1*:  $not(X \text{ and } Y) = ((not \ X) \text{ or } (not \ Y))$   
*<proof>*

**lemma** *deMorgan2*:  $not(X \text{ or } Y) = ((not \ X) \text{ and } (not \ Y))$   
*<proof>*

### 3.5. A Standard Logical Calculus for OCL

**definition** *OclValid* ::  $[(\mathfrak{A})st, (\mathfrak{A})Boolean] \Rightarrow bool \ ((1(-)/ \models (-)) \ 50)$   
**where**  $\tau \models P \equiv ((P \ \tau) = true \ \tau)$

**value**  $\tau \models true \ \langle \rangle \ false$

**value**  $\tau \models false \ \langle \rangle \ true$

#### 3.5.1. 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*:  $\forall \tau. (\tau \models \delta \ P) \wedge (\tau \models \delta \ Q) \wedge (\tau \models P) = (\tau \models Q) \implies P = Q$

*<proof>*

However, certain properties (like transitivity) can not 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>*

### 3.5.2. Local Validity and Meta-logic

**lemma** *foundation1[simp]*:  $\tau \models true$

*<proof>*

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

*<proof>*

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

*<proof>*

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

*<proof>*

**lemma** *bool-split-local[simp]*:

$(\tau \models (x \triangleq invalid)) \vee (\tau \models (x \triangleq null)) \vee (\tau \models (x \triangleq true)) \vee (\tau \models (x \triangleq false))$

*<proof>*

**lemma** *def-split-local*:

$(\tau \models \delta x) = ((\neg(\tau \models (x \triangleq invalid))) \wedge (\neg(\tau \models (x \triangleq null))))$

*<proof>*

**lemma** *foundation5*:

$\tau \models (P \text{ and } Q) \implies (\tau \models P) \wedge (\tau \models Q)$

*<proof>*

**lemma** *foundation6*:

$\tau \models P \implies \tau \models \delta P$

*<proof>*

**lemma** *foundation7[simp]*:

$(\tau \models not (\delta x)) = (\neg(\tau \models \delta x))$

*<proof>*

**lemma** *foundation7'[simp]*:

$(\tau \models not (v x)) = (\neg(\tau \models v x))$

*<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:**

$$(\tau \models \delta x) \vee (\tau \models (x \triangleq \text{invalid})) \vee (\tau \models (x \triangleq \text{null}))$$

*<proof>*

**lemma foundation9:**

$$\tau \models \delta x \implies (\tau \models \text{not } x) = (\neg (\tau \models x))$$

*<proof>*

**lemma foundation10:**

$$\tau \models \delta x \implies \tau \models \delta y \implies (\tau \models (x \text{ and } y)) = ((\tau \models x) \wedge (\tau \models y))$$

*<proof>*

**lemma foundation11:**

$$\tau \models \delta x \implies \tau \models \delta y \implies (\tau \models (x \text{ or } y)) = ((\tau \models x) \vee (\tau \models y))$$

*<proof>*

**lemma foundation12:**

$$\tau \models \delta x \implies \tau \models \delta y \implies (\tau \models (x \text{ implies } y)) = ((\tau \models x) \implies (\tau \models y))$$

*<proof>*

**lemma foundation13:**  $(\tau \models A \triangleq \text{true}) = (\tau \models A)$

*<proof>*

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

*<proof>*

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

*<proof>*

**lemma foundation16:**  $\tau \models (\delta X) = (X \tau \neq \text{bot} \wedge X \tau \neq \text{null})$

*<proof>*

**lemma foundation16':**  $(\tau \models (\delta X)) = (X \tau \neq \text{invalid } \tau \wedge X \tau \neq \text{null } \tau)$

*<proof>*

**lemmas foundation17** = *foundation16*[*THEN iffD1*]

**lemmas foundation17'** = *foundation16'*[*THEN iffD1*]

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

*<proof>*

**lemma** *foundation18'*:  $\tau \models (v X) = (X \tau \neq \text{bot})$   
*<proof>*

**lemmas** *foundation19* = *foundation18*[*THEN iffD1*]

**lemma** *foundation20* :  $\tau \models (\delta X) \implies \tau \models v X$   
*<proof>*

**lemma** *foundation21*:  $(\text{not } A \triangleq \text{not } B) = (A \triangleq B)$   
*<proof>*

**lemma** *foundation22*:  $(\tau \models (X \triangleq Y)) = (X \tau = Y \tau)$   
*<proof>*

**lemma** *foundation23*:  $(\tau \models P) = (\tau \models (\lambda \cdot . P \tau))$   
*<proof>*

**lemmas** *cp-validity=foundation23*

**lemma** *foundation24*:  $(\tau \models \text{not}(X \triangleq Y)) = (X \tau \neq Y \tau)$   
*<proof>*

**lemma** *defined-not-I* :  $\tau \models \delta (x) \implies \tau \models \delta (\text{not } x)$   
*<proof>*

**lemma** *valid-not-I* :  $\tau \models v (x) \implies \tau \models v (\text{not } x)$   
*<proof>*

**lemma** *defined-and-I* :  $\tau \models \delta (x) \implies \tau \models \delta (y) \implies \tau \models \delta (x \text{ and } y)$   
*<proof>*

**lemma** *valid-and-I* :  $\tau \models v (x) \implies \tau \models v (y) \implies \tau \models v (x \text{ and } y)$   
*<proof>*

### 3.5.3. Local Judgements and Strong Equality

**lemma** *StrongEq-L-refl*:  $\tau \models (x \triangleq x)$   
*<proof>*

**lemma** *StrongEq-L-sym*:  $\tau \models (x \triangleq y) \implies \tau \models (y \triangleq x)$   
*<proof>*

**lemma** *StrongEq-L-trans*:  $\tau \models (x \triangleq y) \implies \tau \models (y \triangleq z) \implies \tau \models (x \triangleq z)$

*<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**  $cp :: (('A, 'α) val \Rightarrow ('A, 'β) val) \Rightarrow bool$   
**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*:  $\bigwedge \tau. cp P \Longrightarrow \tau \models (x \triangleq y) \Longrightarrow \tau \models (P x \triangleq P y)$   
*<proof>*

**lemma** *StrongEq-L-subst2*:  
 $\bigwedge \tau. cp P \Longrightarrow \tau \models (x \triangleq y) \Longrightarrow \tau \models (P x) \Longrightarrow \tau \models (P y)$   
*<proof>*

**lemma** *StrongEq-L-subst2-rev*:  $\tau \models y \triangleq x \Longrightarrow cp P \Longrightarrow \tau \models P x \Longrightarrow \tau \models P y$   
*<proof>*

**lemma** *StrongEq-L-subst3*:  
**assumes**  $cp: cp P$   
**and**  $eq: \tau \models x \triangleq y$   
**shows**  $(\tau \models P x) = (\tau \models P y)$   
*<proof>*

**lemma** *cpI1*:  
 $(\forall X \tau. f X \tau = f(\lambda-. X \tau) \tau) \Longrightarrow cp P \Longrightarrow cp(\lambda X. f (P X))$   
*<proof>*

**lemma** *cpI2*:  
 $(\forall X Y \tau. f X Y \tau = f(\lambda-. X \tau)(\lambda-. Y \tau) \tau) \Longrightarrow$   
 $cp P \Longrightarrow cp Q \Longrightarrow cp(\lambda X. f (P X) (Q X))$   
*<proof>*

**lemma** *cpI3*:  
 $(\forall X Y Z \tau. f X Y Z \tau = f(\lambda-. X \tau)(\lambda-. Y \tau)(\lambda-. Z \tau) \tau) \Longrightarrow$   
 $cp P \Longrightarrow cp Q \Longrightarrow cp R \Longrightarrow cp(\lambda X. f (P X) (Q X) (R X))$   
*<proof>*

**lemma** *cpI4*:  
 $(\forall W X Y Z \tau. f W X Y Z \tau = f(\lambda-. W \tau)(\lambda-. X \tau)(\lambda-. Y \tau)(\lambda-. Z \tau) \tau) \Longrightarrow$   
 $cp P \Longrightarrow cp Q \Longrightarrow cp R \Longrightarrow cp S \Longrightarrow cp(\lambda X. f (P X) (Q X) (R X) (S X))$   
*<proof>*

**lemma** *cp-const* :  $cp(\lambda-. c)$   
*<proof>*

**lemma** *cp-id* :  $cp(\lambda X. X)$   
 ⟨*proof*⟩

**lemmas** *cp-intro*[*intro!*,*simp*,*code-unfold*] =  
*cp-const*  
*cp-id*  
*cp-defined*[*THEN* *allI*[*THEN* *allI*[*THEN* *cpI1*], *of defined*]]  
*cp-valid*[*THEN* *allI*[*THEN* *allI*[*THEN* *cpI1*], *of valid*]]  
*cp-OclNot*[*THEN* *allI*[*THEN* *allI*[*THEN* *cpI1*], *of not*]]  
*cp-OclAnd*[*THEN* *allI*[*THEN* *allI*[*THEN* *allI*[*THEN* *cpI2*]], *of op and*]]  
*cp-OclOr*[*THEN* *allI*[*THEN* *allI*[*THEN* *allI*[*THEN* *cpI2*]], *of op or*]]  
*cp-OclImplies*[*THEN* *allI*[*THEN* *allI*[*THEN* *allI*[*THEN* *cpI2*]], *of op implies*]]  
*cp-StrongEq*[*THEN* *allI*[*THEN* *allI*[*THEN* *allI*[*THEN* *cpI2*]],  
*of StrongEq*]]

### 3.5.4. 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**  $\tau \models \delta A$   
**assumes**  $\tau \models \text{not } B$   
**assumes**  $\tau \models A \implies \tau \models B$   
**shows**  $\tau \models \text{not } A$   
 ⟨*proof*⟩

So far, we have only one strict Boolean predicate (-family): the strict equality.

## 3.6. Miscellaneous

### 3.6.1. OCL's if then else endif

**definition** *OclIf* ::  $[(\mathfrak{A})\text{Boolean}, (\mathfrak{A}, \alpha::\text{null}) \text{val}, (\mathfrak{A}, \alpha) \text{val}] \Rightarrow (\mathfrak{A}, \alpha) \text{val}$   
 (*if* (-) *then* (-) *else* (-) *endif* [*10,10,10*]50)

**where** (*if* *C* *then* *B*<sub>1</sub> *else* *B*<sub>2</sub> *endif*) =  $(\lambda \tau. \text{if } (\delta C) \tau = \text{true } \tau$   
     *then* (*if* (*C*  $\tau$ ) = *true*  $\tau$   
     *then* *B*<sub>1</sub>  $\tau$   
     *else* *B*<sub>2</sub>  $\tau$ )  
     *else* *invalid*  $\tau$ )

**lemma** *cp-OclIf*:((*if* *C* *then* *B*<sub>1</sub> *else* *B*<sub>2</sub> *endif*)  $\tau$  =  
 (*if* ( $\lambda -. C \tau$ ) *then* ( $\lambda -. B$ <sub>1</sub>  $\tau$ ) *else* ( $\lambda -. B$ <sub>2</sub>  $\tau$ ) *endif*)  $\tau$ )



*<proof>*

**lemmas** *cp-intro'*[*intro!,simp,code-unfold*] =  
    *cp-intro*  
    *cp-OclIf*[*THEN allI[THEN allI[THEN allI[THEN allI[THEN cpI3]]], of OclIf*]]

**lemma** *OclIf-invalid* [*simp*]: (*if invalid then B<sub>1</sub> else B<sub>2</sub> endif*) = *invalid*  
*<proof>*

**lemma** *OclIf-null* [*simp*]: (*if null then B<sub>1</sub> else B<sub>2</sub> endif*) = *invalid*  
*<proof>*

**lemma** *OclIf-true* [*simp*]: (*if true then B<sub>1</sub> else B<sub>2</sub> endif*) = *B<sub>1</sub>*  
*<proof>*

**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-false* [*simp*]: (*if false then B<sub>1</sub> else B<sub>2</sub> endif*) = *B<sub>2</sub>*  
*<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*]:(*if  $\delta$  X then A else A endif*) = *A*  
*<proof>*

**lemma** *OclIf-idem2*[*simp*]:(*if  $v$  X then A else A endif*) = *A*  
*<proof>*

**lemma** *OclNot-if*[*simp*]:  
*not*(*if P then C else E endif*) = (*if P then not C else not E endif*)

*<proof>*

### 3.6.2. A Side-calculus for (Boolean) Constant Terms

**definition** *const X*  $\equiv \forall \tau \tau'. X \tau = X \tau'$

**lemma** *const-charn*: *const X*  $\implies X \tau = X \tau'$   
*<proof>*

**lemma** *const-subst*:

**assumes** *const-X*: *const X*  
    **and** *const-Y*: *const Y*  
    **and** *eq* :  $X \tau = Y \tau$   
    **and** *cp-P*: *cp P*  
    **and** *pp* :  $P Y \tau = P Y \tau'$

**shows**  $P X \tau = P X \tau'$   
*<proof>*

**lemma** *const-imp1y2* :

**assumes**  $\bigwedge \tau 1 \tau 2. P \tau 1 = P \tau 2 \implies Q \tau 1 = Q \tau 2$   
**shows**  $\text{const } P \implies \text{const } Q$   
*<proof>*

**lemma** *const-imp1y3* :

**assumes**  $\bigwedge \tau 1 \tau 2. P \tau 1 = P \tau 2 \implies Q \tau 1 = Q \tau 2 \implies R \tau 1 = R \tau 2$   
**shows**  $\text{const } P \implies \text{const } Q \implies \text{const } R$   
*<proof>*

**lemma** *const-imp1y4* :

**assumes**  $\bigwedge \tau 1 \tau 2. P \tau 1 = P \tau 2 \implies Q \tau 1 = Q \tau 2 \implies R \tau 1 = R \tau 2 \implies S \tau 1 = S \tau 2$   
**shows**  $\text{const } P \implies \text{const } Q \implies \text{const } R \implies \text{const } S$   
*<proof>*

**lemma** *const-lam* :  $\text{const } (\lambda \cdot e)$   
*<proof>*

**lemma** *const-true* :  $\text{const true}$   
*<proof>*

**lemma** *const-false* :  $\text{const false}$   
*<proof>*

**lemma** *const-null* :  $\text{const null}$   
*<proof>*

**lemma** *const-invalid* :  $\text{const invalid}$   
*<proof>*

**lemma** *const-bot* :  $\text{const bot}$   
*<proof>*

**lemma** *const-defined* :

**assumes**  $\text{const } X$   
**shows**  $\text{const } (\delta X)$   
*<proof>*

**lemma** *const-valid* :

**assumes**  $\text{const } X$   
**shows**  $\text{const } (v X)$   
*<proof>*

**lemma** *const-OclValid1*:

**assumes** *const x*

**shows**  $(\tau \models \delta x) = (\tau' \models \delta x)$

*<proof>*

**lemma** *const-OclValid2*:

**assumes** *const x*

**shows**  $(\tau \models v x) = (\tau' \models v x)$

*<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  $\triangleq$  X')*

*<proof>*

**lemma** *const-OclIf* :

**assumes** *const B*

**and** *const C1*

**and** *const C2*

**shows** *const (if B then C1 else C2 endif)*

*<proof>*

**lemmas** *const-ss = const-bot const-null const-invalid const-false const-true const-lam*  
*const-defined const-valid const-StrongEq const-OclNot const-OclAnd*  
*const-OclOr const-OclImplies const-OclIf*  
**end**

## 4. Formalization II: Library Definitions

```
theory OCL-lib
imports OCL-core
begin
```

The structure of this chapter roughly follows the structure of Chapter 10 of the OCL standard [33], which introduces the OCL Library.

### 4.1. Basic Types: Void and Integer

#### 4.1.1. The Construction of the Void Type

```
type-synonym ('A) Void = ('A, unit option) val
```

This *minimal* OCL type contains only two elements: *invalid* and *null*. *Void* could initially be defined as *unit option option*, 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.

#### 4.1.2. The Construction of the Integer Type

Since *Integer* is again a basic type, we define its semantic domain as the valuations over *int option option*.

```
type-synonym ('A) Integer = ('A, int option option) val
```

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

```
definition OclInt0 :: ('A) Integer (0)
where 0 = ( $\lambda$  . . [[0::int]])
```

```
definition OclInt1 :: ('A) Integer (1)
where 1 = ( $\lambda$  . . [[1::int]])
```

```
definition OclInt2 :: ('A) Integer (2)
where 2 = ( $\lambda$  . . [[2::int]])
```

```
definition OclInt3 :: ('A) Integer (3)
where 3 = ( $\lambda$  . . [[3::int]])
```

```
definition OclInt4 :: ('A) Integer (4)
where 4 = ( $\lambda$  . . [[4::int]])
```

**definition** *OclInt5* :: (' $\mathcal{A}$ )Integer (5)  
**where** **5** = ( $\lambda$  - . [[5::int]])

**definition** *OclInt6* :: (' $\mathcal{A}$ )Integer (6)  
**where** **6** = ( $\lambda$  - . [[6::int]])

**definition** *OclInt7* :: (' $\mathcal{A}$ )Integer (7)  
**where** **7** = ( $\lambda$  - . [[7::int]])

**definition** *OclInt8* :: (' $\mathcal{A}$ )Integer (8)  
**where** **8** = ( $\lambda$  - . [[8::int]])

**definition** *OclInt9* :: (' $\mathcal{A}$ )Integer (9)  
**where** **9** = ( $\lambda$  - . [[9::int]])

**definition** *OclInt10* :: (' $\mathcal{A}$ )Integer (10)  
**where** **10** = ( $\lambda$  - . [[10::int]])

### 4.1.3. Validity and Definedness Properties

**lemma**  $\delta(\text{null}::('A)\text{Integer}) = \text{false}$  *<proof>*

**lemma**  $v(\text{null}::('A)\text{Integer}) = \text{true}$  *<proof>*

**lemma** [*simp,code-unfold*]:  $\delta(\lambda - . [[n]]) = \text{true}$   
*<proof>*

**lemma** [*simp,code-unfold*]:  $v(\lambda - . [[n]]) = \text{true}$   
*<proof>*

**lemma** [*simp,code-unfold*]:  $\delta \mathbf{0} = \text{true}$  *<proof>*

**lemma** [*simp,code-unfold*]:  $v \mathbf{0} = \text{true}$  *<proof>*

**lemma** [*simp,code-unfold*]:  $\delta \mathbf{1} = \text{true}$  *<proof>*

**lemma** [*simp,code-unfold*]:  $v \mathbf{1} = \text{true}$  *<proof>*

**lemma** [*simp,code-unfold*]:  $\delta \mathbf{2} = \text{true}$  *<proof>*

**lemma** [*simp,code-unfold*]:  $v \mathbf{2} = \text{true}$  *<proof>*

**lemma** [*simp,code-unfold*]:  $\delta \mathbf{6} = \text{true}$  *<proof>*

**lemma** [*simp,code-unfold*]:  $v \mathbf{6} = \text{true}$  *<proof>*

**lemma** [*simp,code-unfold*]:  $\delta \mathbf{8} = \text{true}$  *<proof>*

**lemma** [*simp,code-unfold*]:  $v \mathbf{8} = \text{true}$  *<proof>*

**lemma** [*simp,code-unfold*]:  $\delta \mathbf{9} = \text{true}$  *<proof>*

**lemma** [*simp,code-unfold*]:  $v \mathbf{9} = \text{true}$  *<proof>*

### 4.1.4. Arithmetical Operations on Integer

#### 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**  $OclAdd_{Integer} :: ('A)Integer \Rightarrow ('A)Integer \Rightarrow ('A)Integer$  (**infix**  $' + 40$ )  
**where**  $x ' + y \equiv \lambda \tau. \text{if } (\delta x) \tau = \text{true} \tau \wedge (\delta y) \tau = \text{true} \tau$   
*then*  $[[[x \tau]] + [[y \tau]]]$   
*else*  $\text{invalid } \tau$

**definition**  $OclLess_{Integer} :: ('A)Integer \Rightarrow ('A)Integer \Rightarrow ('A)Boolean$  (**infix**  $' < 40$ )  
**where**  $x ' < y \equiv \lambda \tau. \text{if } (\delta x) \tau = \text{true} \tau \wedge (\delta y) \tau = \text{true} \tau$   
*then*  $[[[x \tau]] < [[y \tau]]]$   
*else*  $\text{invalid } \tau$

**definition**  $OclLe_{Integer} :: ('A)Integer \Rightarrow ('A)Integer \Rightarrow ('A)Boolean$  (**infix**  $' \leq 40$ )  
**where**  $x ' \leq y \equiv \lambda \tau. \text{if } (\delta x) \tau = \text{true} \tau \wedge (\delta y) \tau = \text{true} \tau$   
*then*  $[[[x \tau]] \leq [[y \tau]]]$   
*else*  $\text{invalid } \tau$

## Basic Properties

**lemma**  $OclAdd_{Integer}\text{-commute}: (X ' + Y) = (Y ' + X)$   
 $\langle \text{proof} \rangle$

## Execution with Invalid or Null or Zero as Argument

**lemma**  $OclAdd_{Integer}\text{-strict1}[simp,code-unfold] : (x ' + \text{invalid}) = \text{invalid}$   
 $\langle \text{proof} \rangle$

**lemma**  $OclAdd_{Integer}\text{-strict2}[simp,code-unfold] : (\text{invalid} ' + x) = \text{invalid}$   
 $\langle \text{proof} \rangle$

**lemma**  $[simp,code-unfold] : (x ' + \text{null}) = \text{invalid}$   
 $\langle \text{proof} \rangle$

**lemma**  $[simp,code-unfold] : (\text{null} ' + x) = \text{invalid}$   
 $\langle \text{proof} \rangle$

**lemma**  $OclAdd_{Integer}\text{-zero1}[simp,code-unfold] :$   
 $(x ' + \mathbf{0}) = (\text{if } v \ x \ \text{and not } (\delta x) \ \text{then } \text{invalid} \ \text{else } x \ \text{endif})$   
 $\langle \text{proof} \rangle$

**lemma**  $OclAdd_{Integer}\text{-zero2}[simp,code-unfold] :$   
 $(\mathbf{0} ' + x) = (\text{if } v \ x \ \text{and not } (\delta x) \ \text{then } \text{invalid} \ \text{else } x \ \text{endif})$   
 $\langle \text{proof} \rangle$

## Context Passing

**lemma**  $cp\text{-}OclAdd_{Integer}: (X ' + Y) \tau = ((\lambda -. X \tau) ' + (\lambda -. Y \tau)) \tau$   
 $\langle \text{proof} \rangle$

**lemma** *cp-OclLessInteger*: $(X \text{ '<' } Y) \tau = ((\lambda \cdot. X \tau) \text{ '<' } (\lambda \cdot. Y \tau)) \tau$   
*<proof>*

**lemma** *cp-OclLeInteger*: $(X \text{ '<=' } Y) \tau = ((\lambda \cdot. X \tau) \text{ '<=' } (\lambda \cdot. Y \tau)) \tau$   
*<proof>*

## 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*.

```
value  $\tau \models (9 \text{ '<=' } 10)$ 
value  $\tau \models ((4 \text{ '+ } 4) \text{ '<=' } 10)$ 
value  $\neg(\tau \models ((4 \text{ '+ } (4 \text{ '+ } 4)) \text{ '<' } 10))$ 
value  $\tau \models \text{not } (v \text{ (null '+ 1)})$ 
```

## 4.2. Fundamental Predicates on Basic Types: Strict Equality

### 4.2.1. Definition

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  $\mathfrak{A}$  *Boolean*-case as strict extension of the strong equality:

**defs** (overloaded) *StrictRefEqInteger*<sup>[code-unfold]</sup> :  
 $(x::(\mathfrak{A})Integer) \doteq y \equiv \lambda \tau. \text{if } (v \ x) \tau = \text{true} \ \tau \wedge (v \ y) \tau = \text{true} \ \tau$   
     *then*  $(x \hat{=} y) \tau$   
     *else* *invalid*  $\tau$

```
value  $\tau \models 1 \text{ '<>' } 2$ 
value  $\tau \models 2 \text{ '<>' } 1$ 
value  $\tau \models 2 \doteq 2$ 
```

### 4.2.2. Logic and Algebraic Layer on Basic Types

#### Validity and Definedness Properties (I)

**lemma** *StrictRefEqBoolean-defined-args-valid*:  
 $(\tau \models \delta((x::(\mathfrak{A})Boolean) \doteq y)) = ((\tau \models (v \ x)) \wedge (\tau \models (v \ y)))$   
*<proof>*

**lemma** *StrictRefEqInteger-defined-args-valid*:  
 $(\tau \models \delta((x::(\mathfrak{A})Integer) \doteq y)) = ((\tau \models (v \ x)) \wedge (\tau \models (v \ y)))$   
*<proof>*

#### Validity and Definedness Properties (II)

**lemma** *StrictRefEqBoolean-defargs*:  
 $\tau \models ((x::(\mathfrak{A})Boolean) \doteq y) \implies (\tau \models (v \ x)) \wedge (\tau \models (v \ y))$



*<proof>*

**lemma** *StrictRefEqInteger-defargs*:

$\tau \models ((x::(\mathfrak{A})Integer) \doteq y) \implies (\tau \models (v\ x)) \wedge (\tau \models (v\ y))$

*<proof>*

### Validity and Definedness Properties (III) Miscellaneous

**lemma** *StrictRefEqBoolean-strict''* :  $\delta ((x::(\mathfrak{A})Boolean) \doteq y) = (v(x) \text{ and } v(y))$

*<proof>*

**lemma** *StrictRefEqInteger-strict''* :  $\delta ((x::(\mathfrak{A})Integer) \doteq y) = (v(x) \text{ and } v(y))$

*<proof>*

**lemma** *StrictRefEqInteger-strict* :

**assumes** *A*:  $v (x::(\mathfrak{A})Integer) = true$

**and** *B*:  $v\ y = true$

**shows**  $v (x \doteq y) = true$

*<proof>*

**lemma** *StrictRefEqInteger-strict'* :

**assumes** *A*:  $v ((x::(\mathfrak{A})Integer)) \doteq y) = true$

**shows**  $v\ x = true \wedge v\ y = true$

*<proof>*

### Reflexivity

**lemma** *StrictRefEqBoolean-refl[simp,code-unfold]* :

$((x::(\mathfrak{A})Boolean) \doteq x) = (if\ (v\ x) \text{ then } true \text{ else } invalid \text{ endif})$

*<proof>*

**lemma** *StrictRefEqInteger-refl[simp,code-unfold]* :

$((x::(\mathfrak{A})Integer) \doteq x) = (if\ (v\ x) \text{ then } true \text{ else } invalid \text{ endif})$

*<proof>*

### Execution with Invalid or Null as Argument

**lemma** *StrictRefEqBoolean-strict1[simp,code-unfold]* :  $((x::(\mathfrak{A})Boolean) \doteq invalid) = invalid$

*<proof>*

**lemma** *StrictRefEqBoolean-strict2[simp,code-unfold]* :  $(invalid \doteq (x::(\mathfrak{A})Boolean)) = invalid$

*<proof>*

**lemma** *StrictRefEqInteger-strict1[simp,code-unfold]* :  $((x::(\mathfrak{A})Integer) \doteq invalid) = invalid$

*<proof>*

**lemma** *StrictRefEqInteger-strict2[simp,code-unfold]* :  $(invalid \doteq (x::(\mathfrak{A})Integer)) = invalid$

$\langle \text{proof} \rangle$

**lemma** *integer-non-null* [simp]:  $((\lambda-. [|n|]) \doteq (\text{null}::('a)\text{Integer})) = \text{false}$   
 $\langle \text{proof} \rangle$

**lemma** *null-non-integer* [simp]:  $((\text{null}::('a)\text{Integer}) \doteq (\lambda-. [|n|])) = \text{false}$   
 $\langle \text{proof} \rangle$

**lemma** *OclInt0-non-null* [simp,code-unfold]:  $(\mathbf{0} \doteq \text{null}) = \text{false} \langle \text{proof} \rangle$

**lemma** *null-non-OclInt0* [simp,code-unfold]:  $(\text{null} \doteq \mathbf{0}) = \text{false} \langle \text{proof} \rangle$

**lemma** *OclInt1-non-null* [simp,code-unfold]:  $(\mathbf{1} \doteq \text{null}) = \text{false} \langle \text{proof} \rangle$

**lemma** *null-non-OclInt1* [simp,code-unfold]:  $(\text{null} \doteq \mathbf{1}) = \text{false} \langle \text{proof} \rangle$

**lemma** *OclInt2-non-null* [simp,code-unfold]:  $(\mathbf{2} \doteq \text{null}) = \text{false} \langle \text{proof} \rangle$

**lemma** *null-non-OclInt2* [simp,code-unfold]:  $(\text{null} \doteq \mathbf{2}) = \text{false} \langle \text{proof} \rangle$

**lemma** *OclInt6-non-null* [simp,code-unfold]:  $(\mathbf{6} \doteq \text{null}) = \text{false} \langle \text{proof} \rangle$

**lemma** *null-non-OclInt6* [simp,code-unfold]:  $(\text{null} \doteq \mathbf{6}) = \text{false} \langle \text{proof} \rangle$

**lemma** *OclInt8-non-null* [simp,code-unfold]:  $(\mathbf{8} \doteq \text{null}) = \text{false} \langle \text{proof} \rangle$

**lemma** *null-non-OclInt8* [simp,code-unfold]:  $(\text{null} \doteq \mathbf{8}) = \text{false} \langle \text{proof} \rangle$

**lemma** *OclInt9-non-null* [simp,code-unfold]:  $(\mathbf{9} \doteq \text{null}) = \text{false} \langle \text{proof} \rangle$

**lemma** *null-non-OclInt9* [simp,code-unfold]:  $(\text{null} \doteq \mathbf{9}) = \text{false} \langle \text{proof} \rangle$

## Const

**lemma** [simp,code-unfold]:  $\text{const}(\mathbf{0}) \langle \text{proof} \rangle$

**lemma** [simp,code-unfold]:  $\text{const}(\mathbf{1}) \langle \text{proof} \rangle$

**lemma** [simp,code-unfold]:  $\text{const}(\mathbf{2}) \langle \text{proof} \rangle$

**lemma** [simp,code-unfold]:  $\text{const}(\mathbf{6}) \langle \text{proof} \rangle$

**lemma** [simp,code-unfold]:  $\text{const}(\mathbf{8}) \langle \text{proof} \rangle$

**lemma** [simp,code-unfold]:  $\text{const}(\mathbf{9}) \langle \text{proof} \rangle$

## Behavior vs StrongEq

**lemma** *StrictRefEqBoolean-vs-StrongEq*:

$\tau \models (v\ x) \implies \tau \models (v\ y) \implies (\tau \models (((x::('a)\text{Boolean}) \doteq y) \triangleq (x \triangleq y)))$   
 $\langle \text{proof} \rangle$

**lemma** *StrictRefEqInteger-vs-StrongEq*:

$\tau \models (v\ x) \implies \tau \models (v\ y) \implies (\tau \models (((x::('a)\text{Integer}) \doteq y) \triangleq (x \triangleq y)))$   
 $\langle \text{proof} \rangle$

## Context Passing

**lemma** *cp-StrictRefEqBoolean*:

$((X::('a)\text{Boolean}) \doteq Y) \tau = ((\lambda -. X\ \tau) \doteq (\lambda -. Y\ \tau)) \tau$   
 $\langle \text{proof} \rangle$

**lemma** *cp-StrictRefEqInteger*:

$((X::('a)\text{Integer}) \doteq Y) \tau = ((\lambda -. X\ \tau) \doteq (\lambda -. Y\ \tau)) \tau$   
 $\langle \text{proof} \rangle$

```

lemmas cp-intro'[intro!,simp,code-unfold] =
  cp-intro'
  cp-StrictRefEqBoolean[THEN allI[THEN allI[THEN allI[THEN cpI2]], of StrictRefEq]]
  cp-StrictRefEqInteger[THEN allI[THEN allI[THEN allI[THEN cpI2]], of StrictRefEq]]
  cp-OclAddInteger[THEN allI[THEN allI[THEN allI[THEN cpI2]], of OclAddInteger]]
  cp-OclLessInteger[THEN allI[THEN allI[THEN allI[THEN cpI2]], of OclLessInteger]]
  cp-OclLeInteger[THEN allI[THEN allI[THEN allI[THEN cpI2]], of OclLeInteger]]

```

### 4.2.3. Test Statements on Basic Types.

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 Booleans

```

value  $\tau \models v(\text{true})$ 
value  $\tau \models \delta(\text{false})$ 
value  $\neg(\tau \models \delta(\text{null}))$ 
value  $\neg(\tau \models \delta(\text{invalid}))$ 
value  $\tau \models v(\text{null}::(\mathfrak{A})\text{Boolean})$ 
value  $\neg(\tau \models v(\text{invalid}))$ 
value  $\tau \models (\text{true and true})$ 
value  $\tau \models (\text{true and true} \triangleq \text{true})$ 
value  $\tau \models ((\text{null or null}) \triangleq \text{null})$ 
value  $\tau \models ((\text{null or null}) \doteq \text{null})$ 
value  $\tau \models ((\text{true} \triangleq \text{false}) \triangleq \text{false})$ 
value  $\tau \models ((\text{invalid} \triangleq \text{false}) \triangleq \text{false})$ 
value  $\tau \models ((\text{invalid} \doteq \text{false}) \triangleq \text{invalid})$ 

```

Elementary computations on Integer

```

value  $\tau \models v\ 4$ 
value  $\tau \models \delta\ 4$ 
value  $\tau \models v(\text{null}::(\mathfrak{A})\text{Integer})$ 
value  $\tau \models (\text{invalid} \triangleq \text{invalid})$ 
value  $\tau \models (\text{null} \triangleq \text{null})$ 
value  $\tau \models (4 \triangleq 4)$ 
value  $\neg(\tau \models (9 \triangleq 10))$ 
value  $\neg(\tau \models (\text{invalid} \triangleq 10))$ 
value  $\neg(\tau \models (\text{null} \triangleq 10))$ 
value  $\neg(\tau \models (\text{invalid} \doteq (\text{invalid}::(\mathfrak{A})\text{Integer})))$ 
value  $\neg(\tau \models v(\text{invalid} \doteq (\text{invalid}::(\mathfrak{A})\text{Integer})))$ 
value  $\neg(\tau \models (\text{invalid} <> (\text{invalid}::(\mathfrak{A})\text{Integer})))$ 
value  $\neg(\tau \models v(\text{invalid} <> (\text{invalid}::(\mathfrak{A})\text{Integer})))$ 
value  $\tau \models (\text{null} \doteq (\text{null}::(\mathfrak{A})\text{Integer}))$ 
value  $\tau \models (\text{null} \doteq (\text{null}::(\mathfrak{A})\text{Integer}))$ 
value  $\tau \models (4 \doteq 4)$ 
value  $\neg(\tau \models (4 <> 4))$ 
value  $\neg(\tau \models (4 \doteq 10))$ 

```

```

value  $\tau \models (4 <> 10)$ 
value  $\neg(\tau \models (0 ' < null))$ 
value  $\neg(\tau \models (\delta (0 ' < null)))$ 

```

## 4.3. Complex Types: The Set-Collection Type (I) Core

### 4.3.1. The Construction of the Set Type

**no-notation** *None* ( $\perp$ )

**notation** *bot* ( $\perp$ )

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

1. we want the types to be *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 to talking about *Set(Set(Sequences(Pairs(X, Y)))*)).

The former principle rules out the option to define *' $\alpha$  Set* just by ( $\mathfrak{A}$ , (*' $\alpha$  option option set*) *val*). This would allow sets to contain junk elements such as  $\{\perp\}$  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.

The core of an own type construction is done via a type definition which provides the raw-type *' $\alpha$  Set-0*. It is shown that this type “fits” indeed into the abstract type interface discussed in the previous section.

```

typedef ' $\alpha$  Set-0 = {X::(' $\alpha$ ::null) set option option.
                    X = bot  $\vee$  X = null  $\vee$  ( $\forall x \in [[X]]$ . x  $\neq$  bot)}
                    <proof>

```

```

instantiation Set-0 :: (null)bot
begin

```

```

    definition bot-Set-0-def: (bot::('a::null) Set-0)  $\equiv$  Abs-Set-0 None

```

```

    instance <proof>
end

```

```

instantiation Set-0 :: (null)null
begin

```

```

    definition null-Set-0-def: (null::('a::null) Set-0)  $\equiv$  Abs-Set-0 [ None ]

```

```

    instance <proof>

```

end

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

**type-synonym**  $(\mathfrak{A}, 'α) \text{Set} = (\mathfrak{A}, 'α \text{Set-0}) \text{val}$

### 4.3.2. Validity and Definedness Properties

Every element in a defined set is valid.

**lemma** *Set-inv-lemma*:  $\tau \models (\delta X) \implies \forall x \in [[\text{Rep-Set-0} (X \tau)]] . x \neq \text{bot}$   
*<proof>*

**lemma** *Set-inv-lemma'* :  
**assumes**  $x\text{-def} : \tau \models \delta X$   
**and**  $e\text{-mem} : e \in [[\text{Rep-Set-0} (X \tau)]]$   
**shows**  $\tau \models v(\lambda \cdot e)$   
*<proof>*

**lemma** *abs-rep-simp'* :  
**assumes**  $S\text{-all-def} : \tau \models \delta S$   
**shows**  $\text{Abs-Set-0} [[[\text{Rep-Set-0} (S \tau)]]] = S \tau$   
*<proof>*

**lemma** *S-lift'* :  
**assumes**  $S\text{-all-def} : (\tau :: \mathfrak{A} \text{st}) \models \delta S$   
**shows**  $\exists S'. (\lambda a (-::\mathfrak{A} \text{st}). a) ' [[\text{Rep-Set-0} (S \tau)]] = (\lambda a (-::\mathfrak{A} \text{st}). [a]) ' S'$   
*<proof>*

**lemma** *invalid-set-OclNot-defined* [*simp,code-unfold*]:  $\delta(\text{invalid}::(\mathfrak{A}, 'α::\text{null}) \text{Set}) = \text{false}$   
*<proof>*

**lemma** *null-set-OclNot-defined* [*simp,code-unfold*]:  $\delta(\text{null}::(\mathfrak{A}, 'α::\text{null}) \text{Set}) = \text{false}$   
*<proof>*

**lemma** *invalid-set-valid* [*simp,code-unfold*]:  $v(\text{invalid}::(\mathfrak{A}, 'α::\text{null}) \text{Set}) = \text{false}$   
*<proof>*

**lemma** *null-set-valid* [*simp,code-unfold*]:  $v(\text{null}::(\mathfrak{A}, 'α::\text{null}) \text{Set}) = \text{true}$   
*<proof>*

... which means that we can have a type  $(\mathfrak{A}, (\mathfrak{A}, (\mathfrak{A}) \text{Integer}) \text{Set}) \text{Set}$  corresponding exactly to  $\text{Set}(\text{Set}(\text{Integer}))$  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.

### 4.3.3. Constants on Sets

**definition**  $\text{mtSet}::(\mathfrak{A}, 'α::\text{null}) \text{Set} (\text{Set}\{\})$   
**where**  $\text{Set}\{\} \equiv (\lambda \tau. \text{Abs-Set-0} [[\{\}::'\alpha \text{set}]])$

**lemma** *mtSet-defined*[simp,code-unfold]: $\delta(\text{Set}\{\}) = \text{true}$   
 ⟨proof⟩

**lemma** *mtSet-valid*[simp,code-unfold]: $v(\text{Set}\{\}) = \text{true}$   
 ⟨proof⟩

**lemma** *mtSet-rep-set*:  $\llbracket \llbracket \text{Rep-Set-0 } (\text{Set}\{\}) \tau \rrbracket \rrbracket = \{\}$   
 ⟨proof⟩

**lemma** [simp,code-unfold]: *const*  $\text{Set}\{\}$   
 ⟨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.

## 4.4. Complex Types: The Set-Collection Type (II) Library

This part provides a collection of operators for the Set type.

### 4.4.1. Computational Operations on Set

#### Definition

**definition** *OclIncluding*  $:: [(\mathfrak{A}, 'a::\text{null}) \text{Set}, (\mathfrak{A}, 'a) \text{val}] \Rightarrow (\mathfrak{A}, 'a) \text{Set}$   
**where**  $\text{OclIncluding } x \ y = (\lambda \tau. \text{if } (\delta \ x) \ \tau = \text{true} \ \tau \wedge (v \ y) \ \tau = \text{true} \ \tau$   
 $\text{then Abs-Set-0 } \llbracket \llbracket \text{Rep-Set-0 } (x \ \tau) \rrbracket \rrbracket \cup \{y \ \tau\} \rrbracket$   
 $\text{else } \perp)$

**notation** *OclIncluding*  $(-->\text{including}'(-))$

#### syntax

*-OclFinset*  $:: \text{args} \Rightarrow (\mathfrak{A}, 'a::\text{null}) \text{Set} \quad (\text{Set}\{-\})$

#### translations

$\text{Set}\{x, xs\} == \text{CONST } \text{OclIncluding } (\text{Set}\{xs\}) \ x$

$\text{Set}\{x\} == \text{CONST } \text{OclIncluding } (\text{Set}\{\}) \ x$

**definition** *OclExcluding*  $:: [(\mathfrak{A}, 'a::\text{null}) \text{Set}, (\mathfrak{A}, 'a) \text{val}] \Rightarrow (\mathfrak{A}, 'a) \text{Set}$   
**where**  $\text{OclExcluding } x \ y = (\lambda \tau. \text{if } (\delta \ x) \ \tau = \text{true} \ \tau \wedge (v \ y) \ \tau = \text{true} \ \tau$   
 $\text{then Abs-Set-0 } \llbracket \llbracket \text{Rep-Set-0 } (x \ \tau) \rrbracket \rrbracket - \{y \ \tau\} \rrbracket$   
 $\text{else } \perp)$

**notation** *OclExcluding*  $(-->\text{excluding}'(-))$

**definition** *OclIncludes*  $:: [(\mathfrak{A}, 'a::\text{null}) \text{Set}, (\mathfrak{A}, 'a) \text{val}] \Rightarrow \mathfrak{A} \text{ Boolean}$   
**where**  $\text{OclIncludes } x \ y = (\lambda \tau. \text{if } (\delta \ x) \ \tau = \text{true} \ \tau \wedge (v \ y) \ \tau = \text{true} \ \tau$   
 $\text{then } \llbracket \llbracket (y \ \tau) \in \llbracket \llbracket \text{Rep-Set-0 } (x \ \tau) \rrbracket \rrbracket \rrbracket$   
 $\text{else } \perp)$

**notation** *OclIncludes*  $(-->\text{includes}'(-))$

**definition** *OclExcludes*  $:: [(\mathfrak{A}, 'a::\text{null}) \text{Set}, (\mathfrak{A}, 'a) \text{val}] \Rightarrow \mathfrak{A} \text{ Boolean}$   
**where**  $\text{OclExcludes } x \ y = (\text{not}(\text{OclIncludes } x \ y))$

**notation** *OclExcludes*  $(-->excludes'(-))$

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.

**definition** *OclSize*  $:: ('A, 'A::null) Set \Rightarrow 'A Integer$   
**where**  $OclSize\ x = (\lambda\ \tau.\ \text{if } (\delta\ x)\ \tau = \text{true } \tau \wedge \text{finite}([\text{Rep-Set-0 } (x\ \tau)]])$   
 $\text{then } [[\ \text{int}(\text{card } [\text{Rep-Set-0 } (x\ \tau)])\ ]]$   
 $\text{else } \perp)$

**notation**  
*OclSize*  $(-->size'())$

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.

**definition** *OclIsEmpty*  $:: ('A, 'A::null) Set \Rightarrow 'A Boolean$   
**where**  $OclIsEmpty\ x = ((v\ x\ \text{and}\ \text{not } (\delta\ x))\ \text{or } ((OclSize\ x) \doteq \mathbf{0}))$   
**notation** *OclIsEmpty*  $(-->isEmpty'())$

**definition** *OclNotEmpty*  $:: ('A, 'A::null) Set \Rightarrow 'A Boolean$   
**where**  $OclNotEmpty\ x = \text{not}(OclIsEmpty\ x)$   
**notation** *OclNotEmpty*  $(-->notEmpty'())$

**definition** *OclANY*  $:: [ ('A, 'A::null) Set ] \Rightarrow ('A, 'A) val$   
**where**  $OclANY\ x = (\lambda\ \tau.\ \text{if } (v\ x)\ \tau = \text{true } \tau$   
 $\text{then if } (\delta\ x\ \text{and } OclNotEmpty\ x)\ \tau = \text{true } \tau$   
 $\text{then SOME } y.\ y \in [\text{Rep-Set-0 } (x\ \tau)]$   
 $\text{else null } \tau$   
 $\text{else } \perp)$

**notation** *OclANY*  $(-->any'())$

The definition of *OclForall* mimics the one of *op and*: *OclForall* is not a strict operation.

**definition** *OclForall*  $:: [ ('A, 'A::null) Set, ('A, 'A) val \Rightarrow ('A) Boolean ] \Rightarrow 'A Boolean$   
**where**  $OclForall\ S\ P = (\lambda\ \tau.\ \text{if } (\delta\ S)\ \tau = \text{true } \tau$   
 $\text{then if } (\exists x \in [\text{Rep-Set-0 } (S\ \tau)].\ P(\lambda\ -. x)\ \tau = \text{false } \tau$   
 $\text{then false } \tau$   
 $\text{else if } (\exists x \in [\text{Rep-Set-0 } (S\ \tau)].\ P(\lambda\ -. x)\ \tau = \perp\ \tau)$   
 $\text{then } \perp\ \tau$   
 $\text{else if } (\exists x \in [\text{Rep-Set-0 } (S\ \tau)].\ P(\lambda\ -. x)\ \tau = \text{null } \tau)$   
 $\text{then null } \tau$   
 $\text{else true } \tau$   
 $\text{else } \perp)$

**syntax**  
 $-OclForall :: [ ('A, 'A::null) Set, id, ('A) Boolean ] \Rightarrow 'A Boolean \quad ((-)-->forall'(-))$

**translations**  
 $X-->forall(x | P) == CONST\ OclForall\ X\ (\%x.\ P)$

Like *OclForall*, *OclExists* is also not strict.

**definition**  $OclExists$  ::  $[('A, 'α::null) Set, ('A, 'α) val ⇒ ('A) Boolean] ⇒ 'A Boolean$   
**where**  $OclExists S P = not(OclForall S (λ X. not (P X)))$

**syntax**

$-OclExist$  ::  $[('A, 'α::null) Set, id, ('A) Boolean] ⇒ 'A Boolean$   $((-) → exists'(-|-'))$

**translations**

$X → exists(x | P) == CONST OclExists X (%x. P)$

**definition**  $OclIterate$  ::  $[('A, 'α::null) Set, ('A, 'β::null) val,$   
 $(('A, 'α) val ⇒ ('A, 'β) val ⇒ ('A, 'β) val)] ⇒ ('A, 'β) val$   
**where**  $OclIterate S A F = (λ τ. if (δ S) τ = true τ ∧ (v A) τ = true τ ∧ finite[[Rep-Set-0$   
 $(S τ)])$

$then (Finite-Set.fold (F) (A) ((λ a τ. a) ' [[Rep-Set-0 (S τ)]])τ$   
 $else ⊥)$

**syntax**

$-OclIterate$  ::  $[('A, 'α::null) Set, idt, idt, 'α, 'β] ⇒ ('A, 'γ) val$   
 $(- → iterate'(-;=- | -'))$

**translations**

$X → iterate(a; x = A | P) == CONST OclIterate X A (%a. (% x. P))$

**definition**  $OclSelect$  ::  $[('A, 'α::null) Set, ('A, 'α) val ⇒ ('A) Boolean] ⇒ ('A, 'α) Set$   
**where**  $OclSelect S P = (λ τ. if (δ S) τ = true τ$   
 $then if (∃ x ∈ [[Rep-Set-0 (S τ)]]. P(λ -. x) τ = ⊥ τ)$   
 $then ⊥$   
 $else Abs-Set-0 [[{x ∈ [[Rep-Set-0 (S τ)]]. P(λ -. x) τ ≠ false τ}]]$   
 $else ⊥)$

**syntax**

$-OclSelect$  ::  $[('A, 'α::null) Set, id, ('A) Boolean] ⇒ 'A Boolean$   $((-) → select'(-|-'))$

**translations**

$X → select(x | P) == CONST OclSelect X (% x. P)$

**definition**  $OclReject$  ::  $[('A, 'α::null) Set, ('A, 'α) val ⇒ ('A) Boolean] ⇒ ('A, 'α::null) Set$   
**where**  $OclReject S P = OclSelect S (not o P)$

**syntax**

$-OclReject$  ::  $[('A, 'α::null) Set, id, ('A) Boolean] ⇒ 'A Boolean$   $((-) → reject'(-|-'))$

**translations**

$X → reject(x | P) == CONST OclReject X (% x. P)$

## Definition (futur operators)

**consts**

$OclCount$  ::  $[('A, 'α::null) Set, ('A, 'α) Set] ⇒ 'A Integer$

$OclSum$  ::  $(('A, 'α::null) Set) ⇒ 'A Integer$

$OclIncludesAll$  ::  $[('A, 'α::null) Set, ('A, 'α) Set] ⇒ 'A Boolean$

$OclExcludesAll$  ::  $[('A, 'α::null) Set, ('A, 'α) Set] ⇒ 'A Boolean$

$OclComplement$  ::  $(('A, 'α::null) Set) ⇒ ('A, 'α) Set$

$OclUnion$  ::  $[('A, 'α::null) Set, ('A, 'α) Set] ⇒ ('A, 'α) Set$

$OclIntersection$ ::  $[('A, 'α::null) Set, ('A, 'α) Set] ⇒ ('A, 'α) Set$



**notation** $OclCount \quad ( \dashrightarrow count'(-') )$ **notation** $OclSum \quad ( \dashrightarrow sum'(-') )$ **notation** $OclIncludesAll \quad ( \dashrightarrow includesAll'(-') )$ **notation** $OclExcludesAll \quad ( \dashrightarrow excludesAll'(-') )$ **notation** $OclComplement \quad ( \dashrightarrow complement'(-') )$ **notation** $OclUnion \quad ( \dashrightarrow union'(-') )$ **notation** $OclIntersection \quad ( \dashrightarrow intersection'(-') )$ 

## 4.4.2. Validity and Definedness Properties

### OclIncluding

**lemma** *OclIncluding-defined-args-valid*: $(\tau \models \delta(X \dashrightarrow including(x))) = ((\tau \models (\delta X)) \wedge (\tau \models (v x)))$   
*<proof>***lemma** *OclIncluding-valid-args-valid*: $(\tau \models v(X \dashrightarrow including(x))) = ((\tau \models (\delta X)) \wedge (\tau \models (v x)))$   
*<proof>***lemma** *OclIncluding-defined-args-valid'[simp,code-unfold]*: $\delta(X \dashrightarrow including(x)) = ((\delta X) \text{ and } (v x))$   
*<proof>***lemma** *OclIncluding-valid-args-valid''[simp,code-unfold]*: $v(X \dashrightarrow including(x)) = ((\delta X) \text{ and } (v x))$   
*<proof>*

### OclExcluding

**lemma** *OclExcluding-defined-args-valid*: $(\tau \models \delta(X \dashrightarrow excluding(x))) = ((\tau \models (\delta X)) \wedge (\tau \models (v x)))$   
*<proof>***lemma** *OclExcluding-valid-args-valid*: $(\tau \models v(X \dashrightarrow excluding(x))) = ((\tau \models (\delta X)) \wedge (\tau \models (v x)))$   
*<proof>***lemma** *OclExcluding-valid-args-valid'[simp,code-unfold]*:

$\delta(X \rightarrow \text{excluding}(x)) = ((\delta X) \text{ and } (v x))$   
*<proof>*

**lemma** *OclExcluding-valid-args-valid*'[simp,code-unfold]:  
 $v(X \rightarrow \text{excluding}(x)) = ((\delta X) \text{ and } (v x))$   
*<proof>*

## OclIncludes

**lemma** *OclIncludes-defined-args-valid*:  
 $(\tau \models \delta(X \rightarrow \text{includes}(x))) = ((\tau \models (\delta X)) \wedge (\tau \models (v x)))$   
*<proof>*

**lemma** *OclIncludes-valid-args-valid*:  
 $(\tau \models v(X \rightarrow \text{includes}(x))) = ((\tau \models (\delta X)) \wedge (\tau \models (v x)))$   
*<proof>*

**lemma** *OclIncludes-valid-args-valid*'[simp,code-unfold]:  
 $\delta(X \rightarrow \text{includes}(x)) = ((\delta X) \text{ and } (v x))$   
*<proof>*

**lemma** *OclIncludes-valid-args-valid*''[simp,code-unfold]:  
 $v(X \rightarrow \text{includes}(x)) = ((\delta X) \text{ and } (v x))$   
*<proof>*

## OclExcludes

**lemma** *OclExcludes-defined-args-valid*:  
 $(\tau \models \delta(X \rightarrow \text{excludes}(x))) = ((\tau \models (\delta X)) \wedge (\tau \models (v x)))$   
*<proof>*

**lemma** *OclExcludes-valid-args-valid*:  
 $(\tau \models v(X \rightarrow \text{excludes}(x))) = ((\tau \models (\delta X)) \wedge (\tau \models (v x)))$   
*<proof>*

**lemma** *OclExcludes-valid-args-valid*'[simp,code-unfold]:  
 $\delta(X \rightarrow \text{excludes}(x)) = ((\delta X) \text{ and } (v x))$   
*<proof>*

**lemma** *OclExcludes-valid-args-valid*''[simp,code-unfold]:  
 $v(X \rightarrow \text{excludes}(x)) = ((\delta X) \text{ and } (v x))$   
*<proof>*

## OclSize

**lemma** *OclSize-defined-args-valid*:  $\tau \models \delta(X \rightarrow \text{size}()) \implies \tau \models \delta X$   
*<proof>*

**lemma** *OclSize-infinite*:

**assumes** *non-finite*:  $\tau \models \text{not}(\delta(S \rightarrow \text{size}()))$   
**shows**  $(\tau \models \text{not}(\delta(S))) \vee \neg \text{finite} \llbracket \text{Rep-Set-0 } (S \ \tau) \rrbracket$   
 $\langle \text{proof} \rangle$

**lemma**  $\tau \models \delta X \implies \neg \text{finite} \llbracket \text{Rep-Set-0 } (X \ \tau) \rrbracket \implies \neg \tau \models \delta (X \rightarrow \text{size}())$   
 $\langle \text{proof} \rangle$

**lemma** *size-defined*:  
**assumes** *X-finite*:  $\bigwedge \tau. \text{finite} \llbracket \text{Rep-Set-0 } (X \ \tau) \rrbracket$   
**shows**  $\delta (X \rightarrow \text{size}()) = \delta X$   
 $\langle \text{proof} \rangle$

**lemma** *size-defined'*:  
**assumes** *X-finite*:  $\text{finite} \llbracket \text{Rep-Set-0 } (X \ \tau) \rrbracket$   
**shows**  $(\tau \models \delta (X \rightarrow \text{size}())) = (\tau \models \delta X)$   
 $\langle \text{proof} \rangle$

## OclIsEmpty

**lemma** *OclIsEmpty-defined-args-valid*:  $\tau \models \delta (X \rightarrow \text{isEmpty}()) \implies \tau \models v X$   
 $\langle \text{proof} \rangle$

**lemma**  $\tau \models \delta (\text{null} \rightarrow \text{isEmpty}())$   
 $\langle \text{proof} \rangle$

**lemma** *OclIsEmpty-infinite*:  $\tau \models \delta X \implies \neg \text{finite} \llbracket \text{Rep-Set-0 } (X \ \tau) \rrbracket \implies \neg \tau \models \delta (X \rightarrow \text{isEmpty}())$   
 $\langle \text{proof} \rangle$

## OclNotEmpty

**lemma** *OclNotEmpty-defined-args-valid*:  $\tau \models \delta (X \rightarrow \text{notEmpty}()) \implies \tau \models v X$   
 $\langle \text{proof} \rangle$

**lemma**  $\tau \models \delta (\text{null} \rightarrow \text{notEmpty}())$   
 $\langle \text{proof} \rangle$

**lemma** *OclNotEmpty-infinite*:  $\tau \models \delta X \implies \neg \text{finite} \llbracket \text{Rep-Set-0 } (X \ \tau) \rrbracket \implies \neg \tau \models \delta (X \rightarrow \text{notEmpty}())$   
 $\langle \text{proof} \rangle$

**lemma** *OclNotEmpty-has-elt* :  $\tau \models \delta X \implies$   
 $\tau \models X \rightarrow \text{notEmpty}() \implies$   
 $\exists e. e \in \llbracket \text{Rep-Set-0 } (X \ \tau) \rrbracket$   
 $\langle \text{proof} \rangle$

## OclANY

**lemma** *OclANY-defined-args-valid*:  $\tau \models \delta (X \rightarrow \text{any}()) \implies \tau \models \delta X$   
 $\langle \text{proof} \rangle$

**lemma**  $\tau \models \delta X \implies \tau \models X \rightarrow isEmpty() \implies \neg \tau \models \delta (X \rightarrow any())$   
{proof}

**lemma** *OclANY-valid-args-valid*:  
 $(\tau \models v(X \rightarrow any())) = (\tau \models v X)$   
{proof}

**lemma** *OclANY-valid-args-valid''[simp,code-unfold]*:  
 $v(X \rightarrow any()) = (v X)$   
{proof}

### 4.4.3. Execution with Invalid or Null or Infinite Set as Argument

#### OclIncluding

**lemma** *OclIncluding-invalid[simp,code-unfold]*: $(invalid \rightarrow including(x)) = invalid$   
{proof}

**lemma** *OclIncluding-invalid-args[simp,code-unfold]*: $(X \rightarrow including(invalid)) = invalid$   
{proof}

**lemma** *OclIncluding-null[simp,code-unfold]*: $(null \rightarrow including(x)) = invalid$   
{proof}

#### OclExcluding

**lemma** *OclExcluding-invalid[simp,code-unfold]*: $(invalid \rightarrow excluding(x)) = invalid$   
{proof}

**lemma** *OclExcluding-invalid-args[simp,code-unfold]*: $(X \rightarrow excluding(invalid)) = invalid$   
{proof}

**lemma** *OclExcluding-null[simp,code-unfold]*: $(null \rightarrow excluding(x)) = invalid$   
{proof}

#### OclIncludes

**lemma** *OclIncludes-invalid[simp,code-unfold]*: $(invalid \rightarrow includes(x)) = invalid$   
{proof}

**lemma** *OclIncludes-invalid-args[simp,code-unfold]*: $(X \rightarrow includes(invalid)) = invalid$   
{proof}

**lemma** *OclIncludes-null[simp,code-unfold]*: $(null \rightarrow includes(x)) = invalid$   
{proof}

#### OclExcludes

**lemma** *OclExcludes-invalid[simp,code-unfold]*: $(invalid \rightarrow excludes(x)) = invalid$

*<proof>*

**lemma** *OclExcludes-invalid-args*[simp,code-unfold]:( $X \rightarrow \text{excludes}(\text{invalid})$ ) = *invalid*  
*<proof>*

**lemma** *OclExcludes-null*[simp,code-unfold]:( $\text{null} \rightarrow \text{excludes}(x)$ ) = *invalid*  
*<proof>*

### **OclSize**

**lemma** *OclSize-invalid*[simp,code-unfold]:( $\text{invalid} \rightarrow \text{size}()$ ) = *invalid*  
*<proof>*

**lemma** *OclSize-null*[simp,code-unfold]:( $\text{null} \rightarrow \text{size}()$ ) = *invalid*  
*<proof>*

### **OclIsEmpty**

**lemma** *OclIsEmpty-invalid*[simp,code-unfold]:( $\text{invalid} \rightarrow \text{isEmpty}()$ ) = *invalid*  
*<proof>*

**lemma** *OclIsEmpty-null*[simp,code-unfold]:( $\text{null} \rightarrow \text{isEmpty}()$ ) = *true*  
*<proof>*

### **OclNotEmpty**

**lemma** *OclNotEmpty-invalid*[simp,code-unfold]:( $\text{invalid} \rightarrow \text{notEmpty}()$ ) = *invalid*  
*<proof>*

**lemma** *OclNotEmpty-null*[simp,code-unfold]:( $\text{null} \rightarrow \text{notEmpty}()$ ) = *false*  
*<proof>*

### **OclANY**

**lemma** *OclANY-invalid*[simp,code-unfold]:( $\text{invalid} \rightarrow \text{any}()$ ) = *invalid*  
*<proof>*

**lemma** *OclANY-null*[simp,code-unfold]:( $\text{null} \rightarrow \text{any}()$ ) = *null*  
*<proof>*

### **OclForall**

**lemma** *OclForall-invalid*[simp,code-unfold]:( $\text{invalid} \rightarrow \text{forAll}(a \mid P a)$ ) = *invalid*  
*<proof>*

**lemma** *OclForall-null*[simp,code-unfold]:( $\text{null} \rightarrow \text{forAll}(a \mid P a)$ ) = *invalid*  
*<proof>*

### **OclExists**

**lemma** *OclExists-invalid*[simp,code-unfold]:( $\text{invalid} \rightarrow \text{exists}(a \mid P a)$ ) = *invalid*

*<proof>*

**lemma** *OclExists-null[simp,code-unfold]:null- $\rightarrow$ exists(a | P a) = invalid*

*<proof>*

### **OclIterate**

**lemma** *OclIterate-invalid[simp,code-unfold]:invalid- $\rightarrow$ iterate(a; x = A | P a x) = invalid*

*<proof>*

**lemma** *OclIterate-null[simp,code-unfold]:null- $\rightarrow$ iterate(a; x = A | P a x) = invalid*

*<proof>*

**lemma** *OclIterate-invalid-args[simp,code-unfold]:S- $\rightarrow$ iterate(a; x = invalid | P a x) = invalid*

*<proof>*

An open question is this ...

**lemma** *S- $\rightarrow$ iterate(a; x = null | P a x) = invalid*

*<proof>*

**lemma** *OclIterate-infinite:*

**assumes** *non-finite:  $\tau \models \text{not}(\delta(S \rightarrow \text{size}()))$*

**shows** *(OclIterate S A F)  $\tau = \text{invalid } \tau$*

*<proof>*

### **OclSelect**

**lemma** *OclSelect-invalid[simp,code-unfold]:invalid- $\rightarrow$ select(a | P a) = invalid*

*<proof>*

**lemma** *OclSelect-null[simp,code-unfold]:null- $\rightarrow$ select(a | P a) = invalid*

*<proof>*

### **OclReject**

**lemma** *OclReject-invalid[simp,code-unfold]:invalid- $\rightarrow$ reject(a | P a) = invalid*

*<proof>*

**lemma** *OclReject-null[simp,code-unfold]:null- $\rightarrow$ reject(a | P a) = invalid*

*<proof>*

#### **4.4.4. Context Passing**

**lemma** *cp-OclIncluding:*

*(X- $\rightarrow$ including(x))  $\tau = ((\lambda -. X \tau)-\mathbf{\rightarrow}$ including( $\lambda -. x \tau)) \tau$*

*<proof>*

**lemma** *cp-OclExcluding:*

$(X \rightarrow \text{excluding}(x)) \tau = ((\lambda -. X \tau) \rightarrow \text{excluding}(\lambda -. x \tau)) \tau$   
 $\langle \text{proof} \rangle$

**lemma** *cp-OclIncludes*:

$(X \rightarrow \text{includes}(x)) \tau = ((\lambda -. X \tau) \rightarrow \text{includes}(\lambda -. x \tau)) \tau$   
 $\langle \text{proof} \rangle$

**lemma** *cp-OclIncludes1*:

$(X \rightarrow \text{includes}(x)) \tau = (X \rightarrow \text{includes}(\lambda -. x \tau)) \tau$   
 $\langle \text{proof} \rangle$

**lemma** *cp-OclExcludes*:

$(X \rightarrow \text{excludes}(x)) \tau = ((\lambda -. X \tau) \rightarrow \text{excludes}(\lambda -. x \tau)) \tau$   
 $\langle \text{proof} \rangle$

**lemma** *cp-OclSize*:  $X \rightarrow \text{size}()$   $\tau = ((\lambda -. X \tau) \rightarrow \text{size}()) \tau$   
 $\langle \text{proof} \rangle$

**lemma** *cp-OclIsEmpty*:  $X \rightarrow \text{isEmpty}()$   $\tau = ((\lambda -. X \tau) \rightarrow \text{isEmpty}()) \tau$   
 $\langle \text{proof} \rangle$

**lemma** *cp-OclNotEmpty*:  $X \rightarrow \text{notEmpty}()$   $\tau = ((\lambda -. X \tau) \rightarrow \text{notEmpty}()) \tau$   
 $\langle \text{proof} \rangle$

**lemma** *cp-OclANY*:  $X \rightarrow \text{any}()$   $\tau = ((\lambda -. X \tau) \rightarrow \text{any}()) \tau$   
 $\langle \text{proof} \rangle$

**lemma** *cp-OclForall*:

$(S \rightarrow \text{forAll}(x \mid P x)) \tau = ((\lambda -. S \tau) \rightarrow \text{forAll}(x \mid P (\lambda -. x \tau))) \tau$   
 $\langle \text{proof} \rangle$

**lemma** *cp-OclForall1* [*simp,intro!*]:

$cp S \implies cp (\lambda X. ((S X) \rightarrow \text{forAll}(x \mid P x)))$   
 $\langle \text{proof} \rangle$

**lemma**

$cp (\lambda X St x. P (\lambda \tau. x) X St) \implies cp S \implies cp (\lambda X. (S X) \rightarrow \text{forAll}(x \mid P x X))$   
 $\langle \text{proof} \rangle$

**lemma**

$cp S \implies$   
 $(\bigwedge x. cp(P x)) \implies$   
 $cp(\lambda X. ((S X) \rightarrow \text{forAll}(x \mid P x X)))$   
 $\langle \text{proof} \rangle$

**lemma** *cp-OclExists*:

$(S \rightarrow \text{exists}(x \mid P x)) \tau = ((\lambda -. S \tau) \rightarrow \text{exists}(x \mid P (\lambda -. x \tau))) \tau$   
 ⟨proof⟩

**lemma** *cp-OclExists1* [*simp,intro!*]:  
 $cp\ S \implies cp\ (\lambda X. ((S\ X) \rightarrow \text{exists}(x \mid P\ x)))$   
 ⟨proof⟩

**lemma** *cp-OclIterate*:  $(X \rightarrow \text{iterate}(a; x = A \mid P\ a\ x)) \tau =$   
 $((\lambda -. X\ \tau) \rightarrow \text{iterate}(a; x = A \mid P\ a\ x)) \tau$   
 ⟨proof⟩

**lemma** *cp-OclSelect*:  $(X \rightarrow \text{select}(a \mid P\ a)) \tau =$   
 $((\lambda -. X\ \tau) \rightarrow \text{select}(a \mid P\ a)) \tau$   
 ⟨proof⟩

**lemma** *cp-OclReject*:  $(X \rightarrow \text{reject}(a \mid P\ a)) \tau =$   
 $((\lambda -. X\ \tau) \rightarrow \text{reject}(a \mid P\ a)) \tau$   
 ⟨proof⟩

**lemmas** *cp-intro''* [*intro!,simp,code-unfold*] =  
*cp-intro'*  
*cp-OclIncluding* [*THEN allI[THEN allI[THEN allI[THEN cpI2]], of OclIncluding*]]  
*cp-OclExcluding* [*THEN allI[THEN allI[THEN allI[THEN cpI2]], of OclExcluding*]]  
*cp-OclIncludes* [*THEN allI[THEN allI[THEN allI[THEN cpI2]], of OclIncludes*]]  
*cp-OclExcludes* [*THEN allI[THEN allI[THEN allI[THEN cpI2]], of OclExcludes*]]  
*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*]]

#### 4.4.5. Const

**lemma** *const-OclIncluding* [*simp,code-unfold*] :  
**assumes** *const-x* : *const x*  
**and** *const-S* : *const S*  
**shows** *const* ( $S \rightarrow \text{including}(x)$ )  
 ⟨proof⟩

## 4.5. Fundamental Predicates on Set: Strict Equality

### 4.5.1. Definition

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:

**defs** (overloaded) *StrictRefEqSet* :



$$(x::('A, 'a::null)Set) \doteq y \equiv \lambda \tau. \text{if } (v x) \tau = \text{true } \tau \wedge (v y) \tau = \text{true } \tau \\ \text{then } (x \triangleq y) \tau \\ \text{else } \text{invalid } \tau$$

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 sets in the sense above—coincides.

## 4.5.2. Logic and Algebraic Layer on Set

### Reflexivity

To become operational, we derive:

**lemma** *StrictRefEqSet-refl[simp,code-unfold]*:  
 $((x::('A, 'a::null)Set) \doteq x) = (\text{if } (v x) \text{ then true else invalid endif})$   
*<proof>*

### Symmetry

**lemma** *StrictRefEqSet-sym*:  
 $((x::('A, 'a::null)Set) \doteq y) = (y \doteq x)$   
*<proof>*

### Execution with Invalid or Null as Argument

**lemma** *StrictRefEqSet-strict1[simp,code-unfold]*:  $((x::('A, 'a::null)Set) \doteq \text{invalid}) = \text{invalid}$   
*<proof>*

**lemma** *StrictRefEqSet-strict2[simp,code-unfold]*:  $(\text{invalid} \doteq (y::('A, 'a::null)Set)) = \text{invalid}$   
*<proof>*

**lemma** *StrictRefEqSet-strictEq-valid-args-valid*:  
 $(\tau \models \delta ((x::('A, 'a::null)Set) \doteq y)) = ((\tau \models (v x)) \wedge (\tau \models (v y)))$   
*<proof>*

### Behavior vs StrongEq

**lemma** *StrictRefEqSet-vs-StrongEq*:  
 $\tau \models v x \implies \tau \models v y \implies (\tau \models (((x::('A, 'a::null)Set) \doteq y) \triangleq (x \triangleq y)))$   
*<proof>*

### Context Passing

**lemma** *cp-StrictRefEqSet*:  $((X::('A, 'a::null)Set) \doteq Y) \tau = ((\lambda \cdot. X \tau) \doteq (\lambda \cdot. Y \tau)) \tau$   
*<proof>*

## Const

**lemma** *const-StrictRefEqSet* :  
 **assumes** *const* ( $X :: (-, :: \text{null}) \text{Set}$ )  
 **assumes** *const*  $X'$   
 **shows** *const* ( $X \doteq X'$ )  
  $\langle \text{proof} \rangle$

## 4.6. Execution on Set's Operators (with mtSet and recursive case as arguments)

### 4.6.1. OclIncluding

**lemma** *OclIncluding-finite-rep-set* :  
 **assumes**  $X\text{-def} : \tau \models \delta X$   
 **and**  $x\text{-val} : \tau \models v x$   
 **shows** *finite*  $\llbracket \text{Rep-Set-0 } (X \text{-> including}(x) \tau) \rrbracket = \text{finite } \llbracket \text{Rep-Set-0 } (X \tau) \rrbracket$   
  $\langle \text{proof} \rangle$

**lemma** *OclIncluding-rep-set*:  
 **assumes**  $S\text{-def} : \tau \models \delta S$   
 **shows**  $\llbracket \text{Rep-Set-0 } (S \text{-> including}(\lambda \cdot \llbracket x \rrbracket) \tau) \rrbracket = \text{insert } \llbracket x \rrbracket \llbracket \text{Rep-Set-0 } (S \tau) \rrbracket$   
  $\langle \text{proof} \rangle$

**lemma** *OclIncluding-notempty-rep-set*:  
 **assumes**  $X\text{-def} : \tau \models \delta X$   
 **and**  $a\text{-val} : \tau \models v a$   
 **shows**  $\llbracket \text{Rep-Set-0 } (X \text{-> including}(a) \tau) \rrbracket \neq \{\}$   
  $\langle \text{proof} \rangle$

**lemma** *OclIncluding-includes*:  
 **assumes**  $\tau \models X \text{-> includes}(x)$   
 **shows**  $X \text{-> including}(x) \tau = X \tau$   
  $\langle \text{proof} \rangle$

### 4.6.2. OclExcluding

**lemma** *OclExcluding-charn0[simp]*:  
 **assumes**  $\text{val-}x : \tau \models (v x)$   
 **shows**  $\tau \models ((\text{Set}\{\}) \text{-> excluding}(x)) \triangleq \text{Set}\{\}$   
  $\langle \text{proof} \rangle$

**lemma** *OclExcluding-charn0-exec[simp,code-unfold]*:  
  $(\text{Set}\{\}) \text{-> excluding}(x) = (\text{if } (v x) \text{ then } \text{Set}\{\} \text{ else } \text{invalid endif})$   
  $\langle \text{proof} \rangle$

**lemma** *OclExcluding-charn1*:  
 **assumes**  $\text{def-}X : \tau \models (\delta X)$

**and**  $val\text{-}x:\tau \models (v\ x)$   
**and**  $val\text{-}y:\tau \models (v\ y)$   
**and**  $neg\ \tau \models not(x \triangleq y)$   
**shows**  $\tau \models ((X \text{->} including(x)) \text{->} excluding(y)) \triangleq ((X \text{->} excluding(y)) \text{->} including(x))$   
 <proof>

**lemma** *OclExcluding-charn2*:

**assumes**  $def\text{-}X:\tau \models (\delta\ X)$   
**and**  $val\text{-}x:\tau \models (v\ x)$   
**shows**  $\tau \models (((X \text{->} including(x)) \text{->} excluding(x)) \triangleq (X \text{->} excluding(x)))$   
 <proof>

One would like a generic theorem of the form:

**lemma** *OclExcluding\_charn\_exec*:

” $(X \text{->} including(x::('A, 'a::null)val)) \text{->} excluding(y)) =$   
 (if  $\delta\ X$  then if  $x \doteq y$   
     then  $X \text{->} excluding(y)$   
     else  $X \text{->} excluding(y) \text{->} including(x)$   
     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**  $strict1: (x \doteq invalid) = invalid$   
**and**  $strict2: (invalid \doteq y) = invalid$   
**and**  $StrictRefEq\text{-}valid\text{-}args\text{-}valid: \bigwedge (x::('A, 'a::null)val)\ y\ \tau.$   
      $(\tau \models \delta\ (x \doteq y)) = ((\tau \models (v\ x)) \wedge (\tau \models v\ y))$   
**and**  $cp\text{-}StrictRefEq: \bigwedge (X::('A, 'a::null)val)\ Y\ \tau. (X \doteq Y)\ \tau = ((\lambda\cdot. X\ \tau) \doteq (\lambda\cdot. Y\ \tau))\ \tau$   
**and**  $StrictRefEq\text{-}vs\text{-}StrongEq: \bigwedge (x::('A, 'a::null)val)\ y\ \tau.$   
      $\tau \models v\ x \implies \tau \models v\ y \implies (\tau \models ((x \doteq y) \triangleq (x \triangleq y)))$   
**shows**  $(X \text{->} including(x::('A, 'a::null)val)) \text{->} excluding(y)) =$   
 (if  $\delta\ X$  then if  $x \doteq y$   
     then  $X \text{->} excluding(y)$   
     else  $X \text{->} excluding(y) \text{->} including(x)$   
     endif  
 else invalid endif)

<proof>

**schematic-lemma** *OclExcluding-charn-execInteger[simp,code-unfold]*: ?X

<proof>

**schematic-lemma** *OclExcluding-charn-exec<sub>Boolean</sub>*[*simp,code-unfold*]: ?*X*  
 ⟨*proof*⟩

**schematic-lemma** *OclExcluding-charn-exec<sub>Set</sub>*[*simp,code-unfold*]: ?*X*  
 ⟨*proof*⟩

**lemma** *OclExcluding-finite-rep-set* :  
**assumes** *X-def* :  $\tau \models \delta X$   
**and** *x-val* :  $\tau \models v x$   
**shows** *finite* [[*Rep-Set-0* (*X*  $\rightarrow$  *excluding*(*x*)  $\tau$ )] = *finite* [[*Rep-Set-0* (*X*  $\tau$ )]]  
 ⟨*proof*⟩

**lemma** *OclExcluding-rep-set*:  
**assumes** *S-def*:  $\tau \models \delta S$   
**shows** [[*Rep-Set-0* (*S*  $\rightarrow$  *excluding*( $\lambda$ -. [[*x*]])  $\tau$ )] = [[*Rep-Set-0* (*S*  $\tau$ )] - {[[*x*]]}]  
 ⟨*proof*⟩

### 4.6.3. OclIncludes

**lemma** *OclIncludes-charn0*[*simp*]:  
**assumes** *val-x*: $\tau \models (v x)$   
**shows**  $\tau \models \text{not}(\text{Set}\{\} \rightarrow \text{includes}(x))$   
 ⟨*proof*⟩

**lemma** *OclIncludes-charn0'*[*simp,code-unfold*]:  
*Set*{ $\}$   $\rightarrow$  *includes*(*x*) = (if *v x* then false else invalid endif)  
 ⟨*proof*⟩

**lemma** *OclIncludes-charn1*:  
**assumes** *def-X*: $\tau \models (\delta X)$   
**assumes** *val-x*: $\tau \models (v x)$   
**shows**  $\tau \models (X \rightarrow \text{including}(x) \rightarrow \text{includes}(x))$   
 ⟨*proof*⟩

**lemma** *OclIncludes-charn2*:  
**assumes** *def-X*: $\tau \models (\delta X)$   
**and** *val-x*: $\tau \models (v x)$   
**and** *val-y*: $\tau \models (v y)$   
**and** *neq* : $\tau \models \text{not}(x \triangleq y)$   
**shows**  $\tau \models (X \rightarrow \text{including}(x) \rightarrow \text{includes}(y)) \triangleq (X \rightarrow \text{includes}(y))$   
 ⟨*proof*⟩

Here is again a generic theorem similar as above.

**lemma** *OclIncludes-execute-generic*:

**assumes** *strict1*:  $(x \doteq \text{invalid}) = \text{invalid}$   
**and** *strict2*:  $(\text{invalid} \doteq y) = \text{invalid}$   
**and** *cp-StrictRefEq*:  $\bigwedge (X :: ('A, 'a :: \text{null}) \text{val}) Y \tau. (X \doteq Y) \tau = ((\lambda \cdot. X \tau) \doteq (\lambda \cdot. Y \tau)) \tau$   
**and** *StrictRefEq-vs-StrongEq*:  $\bigwedge (x :: ('A, 'a :: \text{null}) \text{val}) y \tau.$   
 $\tau \models v x \implies \tau \models v y \implies (\tau \models ((x \doteq y) \triangleq (x \triangleq y)))$

**shows**

$(X \text{-->including}(x :: ('A, 'a :: \text{null}) \text{val}) \text{-->includes}(y)) =$   
 $(\text{if } \delta X \text{ then if } x \doteq y \text{ then true else } X \text{-->includes}(y) \text{ endif else invalid endif})$   
 $\langle \text{proof} \rangle$

**schematic-lemma** *OclIncludes-execute<sub>Integer</sub>[simp,code-unfold]*:  $?X$   
 $\langle \text{proof} \rangle$

**schematic-lemma** *OclIncludes-execute<sub>Boolean</sub>[simp,code-unfold]*:  $?X$   
 $\langle \text{proof} \rangle$

**schematic-lemma** *OclIncludes-execute<sub>Set</sub>[simp,code-unfold]*:  $?X$   
 $\langle \text{proof} \rangle$

**lemma** *OclIncludes-including-generic* :

**assumes** *OclIncludes-execute-generic [simp]* :  $\bigwedge X x y.$   
 $(X \text{-->including}(x :: ('A, 'a :: \text{null}) \text{val}) \text{-->includes}(y)) =$   
 $(\text{if } \delta X \text{ then if } x \doteq y \text{ then true else } X \text{-->includes}(y) \text{ endif else invalid endif})$   
**and** *StrictRefEq-strict''* :  $\bigwedge x y. \delta ((x :: ('A, 'a :: \text{null}) \text{val}) \doteq y) = (v(x) \text{ and } v(y))$   
**and** *a-val* :  $\tau \models v a$   
**and** *x-val* :  $\tau \models v x$   
**and** *S-incl* :  $\tau \models (S) \text{-->includes}((x :: ('A, 'a :: \text{null}) \text{val}))$   
**shows**  $\tau \models S \text{-->including}((a :: ('A, 'a :: \text{null}) \text{val})) \text{-->includes}(x)$   
 $\langle \text{proof} \rangle$

**lemmas** *OclIncludes-including<sub>Integer</sub> =*  
 $OclIncludes-including-generic[OF OclIncludes-execute<sub>Integer</sub> StrictRefEq<sub>Integer</sub>-strict'']$

#### 4.6.4. OclExcludes

#### 4.6.5. OclSize

**lemma** *[simp,code-unfold]*:  $\text{Set}\{\} \text{-->size}() = \mathbf{0}$   
 $\langle \text{proof} \rangle$

**lemma** *OclSize-including-exec[simp,code-unfold]*:

$((X \text{-->including}(x)) \text{-->size}()) = (\text{if } \delta X \text{ and } v x \text{ then}$   
 $X \text{-->size}() \text{ ' + if } X \text{-->includes}(x) \text{ then } \mathbf{0} \text{ else } \mathbf{1} \text{ endif}$   
 $\text{else}$   
 $\text{invalid}$   
 $\text{endif})$

*<proof>*

#### 4.6.6. OclIsEmpty

**lemma** *[simp,code-unfold]: Set{} -> isEmpty() = true*  
*<proof>*

**lemma** *OclIsEmpty-including [simp]:*  
**assumes** *X-def:  $\tau \models \delta X$*   
    **and** *X-finite: finite [[Rep-Set-0 (X  $\tau$ )]]*  
    **and** *a-val:  $\tau \models v a$*   
**shows** *X -> including(a) -> isEmpty()  $\tau = false \tau$*   
*<proof>*

#### 4.6.7. OclNotEmpty

**lemma** *[simp,code-unfold]: Set{} -> notEmpty() = false*  
*<proof>*

**lemma** *OclNotEmpty-including [simp,code-unfold]:*  
**assumes** *X-def:  $\tau \models \delta X$*   
    **and** *X-finite: finite [[Rep-Set-0 (X  $\tau$ )]]*  
    **and** *a-val:  $\tau \models v a$*   
**shows** *X -> including(a) -> notEmpty()  $\tau = true \tau$*   
*<proof>*

#### 4.6.8. OclANY

**lemma** *[simp,code-unfold]: Set{} -> any() = null*  
*<proof>*

**lemma** *OclANY-singleton-exec[simp,code-unfold]:*  
    *(Set{} -> including(a) -> any() = a*  
    *<proof>*

#### 4.6.9. OclForall

**lemma** *OclForall-mtSet-exec[simp,code-unfold] :*  
*((Set{} -> forAll(z | P(z))) = true*  
*<proof>*

**lemma** *OclForall-including-exec[simp,code-unfold] :*  
**assumes** *cp0 : cp P*  
**shows** *((S -> including(x) -> forAll(z | P(z))) = (if  $\delta S$  and  $v x$*   
    *then  $P x$  and  $(S -> forAll(z | P(z)))$*   
    *else invalid*  
    *endif)*

*<proof>*

#### 4.6.10. OclExists

**lemma** *OclExists-mtSet-exec*[simp,code-unfold] :  
((Set{ })->exists(z | P(z))) = false  
<proof>

**lemma** *OclExists-including-exec*[simp,code-unfold] :  
**assumes** cp: cp P  
**shows** ((S->including(x))->exists(z | P(z))) = (if  $\delta$  S and  $v$  x  
then P x or (S->exists(z | P(z)))  
else invalid  
endif)  
<proof>

#### 4.6.11. OclIterate

**lemma** *OclIterate-empty*[simp,code-unfold]: ((Set{ })->iterate(a; x = A | P a x)) = A  
<proof>

In particular, this does hold for A = null.

**lemma** *OclIterate-including*:  
**assumes** S-finite:  $\tau \models \delta(S->size())$   
**and** F-valid-arg:  $(v A) \tau = (v (F a A)) \tau$   
**and** F-commute: comp-fun-commute F  
**and** F-cp:  $\bigwedge x y \tau. F x y \tau = F (\lambda -. x \tau) y \tau$   
**shows** ((S->including(a))->iterate(a; x = A | F a x))  $\tau =$   
((S->excluding(a))->iterate(a; x = F a A | F a x))  $\tau$   
<proof>

#### 4.6.12. OclSelect

**lemma** *OclSelect-mtSet-exec*[simp,code-unfold]: OclSelect mtSet P = mtSet  
<proof>

**definition** *OclSelect-body* ::  $- \Rightarrow - \Rightarrow - \Rightarrow ('a, 'a \text{ option option}) \text{ Set}$   
 $\equiv (\lambda P x \text{ acc. if } P x \doteq \text{false then acc else acc->including(x) endif)$

**lemma** *OclSelect-including-exec*[simp,code-unfold]:  
**assumes** P-cp : cp P  
**shows** OclSelect (X->including(y)) P = OclSelect-body P y (OclSelect (X->excluding(y))  
P)  
(is - = ?select)  
<proof>

#### 4.6.13. OclReject

**lemma** *OclReject-mtSet-exec*[simp,code-unfold]: OclReject mtSet P = mtSet  
<proof>

**lemma** *OclReject-including-exec*[simp,code-unfold]:

**assumes**  $P\text{-cp} : \text{cp } P$   
**shows**  $\text{OclReject } (X \rightarrow \text{including}(y)) P = \text{OclSelect-body } (\text{not } o P) y (\text{OclReject } (X \rightarrow \text{excluding}(y)) P)$   
 <proof>

## 4.7. Execution on Set's Operators (higher composition)

### 4.7.1. OclIncludes

**lemma**  $\text{OclIncludes-any}[\text{simp,code-unfold}]$ :  
 $X \rightarrow \text{includes}(X \rightarrow \text{any}()) = (\text{if } \delta X \text{ then}$   
      $\text{if } \delta (X \rightarrow \text{size}()) \text{ then } \text{not}(X \rightarrow \text{isEmpty}())$   
      $\text{else } X \rightarrow \text{includes}(\text{null}) \text{ endif}$   
      $\text{else invalid endif})$   
 <proof>

### 4.7.2. OclSize

**lemma**  $[\text{simp,code-unfold}]$ :  $\delta (\text{Set}\{\} \rightarrow \text{size}()) = \text{true}$   
 <proof>

**lemma**  $[\text{simp,code-unfold}]$ :  $\delta ((X \rightarrow \text{including}(x)) \rightarrow \text{size}()) = (\delta(X \rightarrow \text{size}()) \text{ and } v(x))$   
 <proof>

**lemma**  $[\text{simp,code-unfold}]$ :  $\delta ((X \rightarrow \text{excluding}(x)) \rightarrow \text{size}()) = (\delta(X \rightarrow \text{size}()) \text{ and } v(x))$   
 <proof>

**lemma**  $[\text{simp}]$ :  
**assumes**  $X\text{-finite} : \bigwedge \tau. \text{finite } [[\text{Rep-Set-0 } (X \ \tau)]]$   
**shows**  $\delta ((X \rightarrow \text{including}(x)) \rightarrow \text{size}()) = (\delta(X) \text{ and } v(x))$   
 <proof>

### 4.7.3. OclForall

**lemma**  $\text{OclForall-rep-set-false}$ :  
**assumes**  $\tau \models \delta X$   
**shows**  $(\text{OclForall } X P \ \tau = \text{false } \tau) = (\exists x \in [[\text{Rep-Set-0 } (X \ \tau)]] . P (\lambda \tau. x) \ \tau = \text{false } \tau)$   
 <proof>

**lemma**  $\text{OclForall-rep-set-true}$ :  
**assumes**  $\tau \models \delta X$   
**shows**  $(\tau \models \text{OclForall } X P) = (\forall x \in [[\text{Rep-Set-0 } (X \ \tau)]] . \tau \models P (\lambda \tau. x))$   
 <proof>

**lemma**  $\text{OclForall-includes}$  :  
**assumes**  $x\text{-def} : \tau \models \delta x$   
     **and**  $y\text{-def} : \tau \models \delta y$   
**shows**  $(\tau \models \text{OclForall } x (\text{OclIncludes } y)) = ([[ \text{Rep-Set-0 } (x \ \tau) ]] \subseteq [[ \text{Rep-Set-0 } (y \ \tau) ]])$



*<proof>*

**lemma** *OclForall-not-includes* :

**assumes**  $x\text{-def} : \tau \models \delta x$

**and**  $y\text{-def} : \tau \models \delta y$

**shows**  $(\text{OclForall } x (\text{OclIncludes } y) \tau = \text{false } \tau) = (\neg \llbracket \text{Rep-Set-0 } (x \ \tau) \rrbracket \subseteq \llbracket \text{Rep-Set-0 } (y \ \tau) \rrbracket)$

*<proof>*

**lemma** *OclForall-iterate*:

**assumes**  $S\text{-finite: finite } \llbracket \text{Rep-Set-0 } (S \ \tau) \rrbracket$

**shows**  $S\text{->forAll}(x \mid P \ x) \ \tau = (S\text{->iterate}(x; \text{acc} = \text{true} \mid \text{acc and } P \ x)) \ \tau$

*<proof>*

**lemma** *OclForall-cong*:

**assumes**  $\bigwedge x. x \in \llbracket \text{Rep-Set-0 } (X \ \tau) \rrbracket \implies \tau \models P (\lambda\tau. x) \implies \tau \models Q (\lambda\tau. x)$

**assumes**  $P: \tau \models \text{OclForall } X \ P$

**shows**  $\tau \models \text{OclForall } X \ Q$

*<proof>*

**lemma** *OclForall-cong'*:

**assumes**  $\bigwedge x. x \in \llbracket \text{Rep-Set-0 } (X \ \tau) \rrbracket \implies \tau \models P (\lambda\tau. x) \implies \tau \models Q (\lambda\tau. x) \implies \tau \models R (\lambda\tau. x)$

**assumes**  $P: \tau \models \text{OclForall } X \ P$

**assumes**  $Q: \tau \models \text{OclForall } X \ Q$

**shows**  $\tau \models \text{OclForall } X \ R$

*<proof>*

#### 4.7.4. Strict Equality

**lemma** *StrictRefEqSet-defined* :

**assumes**  $x\text{-def}: \tau \models \delta x$

**assumes**  $y\text{-def}: \tau \models \delta y$

**shows**  $((x::(\mathfrak{A}, \alpha::\text{null})\text{Set}) \doteq y) \ \tau =$

$(x\text{->forAll}(z \mid y\text{->includes}(z)) \text{ and } (y\text{->forAll}(z \mid x\text{->includes}(z)))) \ \tau$

*<proof>*

**lemma** *StrictRefEqSet-exec[simp,code-unfold]* :

$((x::(\mathfrak{A}, \alpha::\text{null})\text{Set}) \doteq y) =$

$(\text{if } \delta x \text{ then } (\text{if } \delta y$

$\text{then } ((x\text{->forAll}(z \mid y\text{->includes}(z)) \text{ and } (y\text{->forAll}(z \mid x\text{->includes}(z))))$

$\text{else if } v \ y$

$\text{then false } (* \ x'\text{->includes} = \text{null} *)$

$\text{else invalid}$

$\text{endif}$

$\text{endif})$

$\text{else if } v \ x \ (* \ \text{null} = ??? *)$

$\text{then if } v \ y \ \text{then not}(\delta y) \ \text{else invalid endif}$

$\text{else invalid}$

endif  
endif)

⟨proof⟩

**lemma** *StrictRefEqSet-L-subst1* :  $cp\ P \implies \tau \models v\ x \implies \tau \models v\ y \implies \tau \models v\ P\ x \implies \tau \models v\ P\ y \implies$   
 $\tau \models (x :: ('A, 'a :: null)\ Set) \doteq y \implies \tau \models (P\ x :: ('A, 'a :: null)\ Set) \doteq P\ y$   
 ⟨proof⟩

**lemma** *OclIncluding-cong'* :  
**shows**  $\tau \models \delta\ s \implies \tau \models \delta\ t \implies \tau \models v\ x \implies$   
 $\tau \models ((s :: ('A, 'a :: null)\ Set) \doteq t) \implies \tau \models (s \rightarrow including(x) \doteq (t \rightarrow including(x)))$   
 ⟨proof⟩

**lemma** *OclIncluding-cong* :  $\bigwedge (s :: ('A, 'a :: null)\ Set)\ t\ x\ y\ \tau. \tau \models \delta\ t \implies \tau \models v\ y \implies$   
 $\tau \models s \doteq t \implies x = y \implies \tau \models s \rightarrow including(x) \doteq (t \rightarrow including(y))$   
 ⟨proof⟩

**lemma** *const-StrictRefEqSet-including* :  $const\ a \implies const\ S \implies const\ X \implies$   
 $const\ (X \doteq S \rightarrow including(a))$   
 ⟨proof⟩

## 4.8. Test Statements

**lemma** *syntax-test*:  $Set\{2,1\} = (Set\{\}\rightarrow including(1)\rightarrow including(2))$   
 ⟨proof⟩

Here is an example of a nested collection. Note that we have to use the abstract null (since we did not (yet) define a concrete constant *null* for the non-existing Sets) :

**lemma** *semantic-test2*:  
**assumes**  $H : (Set\{2\} \doteq null) = (false :: ('A)\ Boolean)$   
**shows**  $(\tau :: ('A)\ st) \models (Set\{Set\{2\}, null\} \rightarrow includes(null))$   
 ⟨proof⟩

**lemma** *short-cut'[simp,code-unfold]*:  $(8 \doteq 6) = false$   
 ⟨proof⟩

**lemma** *short-cut''[simp,code-unfold]*:  $(2 \doteq 1) = false$   
 ⟨proof⟩

**lemma** *short-cut'''[simp,code-unfold]*:  $(1 \doteq 2) = false$   
 ⟨proof⟩

Elementary computations on Sets.

**declare** *OclSelect-body-def* [simp]

**value**  $\neg (\tau \models v(invalid :: ('A, 'a :: null)\ Set))$   
**value**  $\tau \models v(null :: ('A, 'a :: null)\ Set)$

```

value  $\neg$  ( $\tau \models \delta(\text{null}::('A, 'a::\text{null}) \text{Set})$ )
value  $\tau \models v(\text{Set}\{\})$ 
value  $\tau \models v(\text{Set}\{\text{Set}\{\mathbf{2}\}, \text{null}\})$ 
value  $\tau \models \delta(\text{Set}\{\text{Set}\{\mathbf{2}\}, \text{null}\})$ 
value  $\tau \models (\text{Set}\{\mathbf{2}, \mathbf{1}\} \rightarrow \text{includes}(\mathbf{1}))$ 
value  $\neg$  ( $\tau \models (\text{Set}\{\mathbf{2}\} \rightarrow \text{includes}(\mathbf{1}))$ )
value  $\neg$  ( $\tau \models (\text{Set}\{\mathbf{2}, \mathbf{1}\} \rightarrow \text{includes}(\text{null}))$ )
value  $\tau \models (\text{Set}\{\mathbf{2}, \text{null}\} \rightarrow \text{includes}(\text{null}))$ 
value  $\tau \models (\text{Set}\{\text{null}, \mathbf{2}\} \rightarrow \text{includes}(\text{null}))$ 

value  $\tau \models ((\text{Set}\{\}) \rightarrow \text{forAll}(z \mid \mathbf{0} < z))$ 

value  $\tau \models ((\text{Set}\{\mathbf{2}, \mathbf{1}\}) \rightarrow \text{forAll}(z \mid \mathbf{0} < z))$ 
value  $\neg$  ( $\tau \models ((\text{Set}\{\mathbf{2}, \mathbf{1}\}) \rightarrow \text{exists}(z \mid z < \mathbf{0}))$ )
value  $\neg$  ( $\tau \models \delta(\text{Set}\{\mathbf{2}, \text{null}\}) \rightarrow \text{forAll}(z \mid \mathbf{0} < z)$ )
value  $\neg$  ( $\tau \models ((\text{Set}\{\mathbf{2}, \text{null}\}) \rightarrow \text{forAll}(z \mid \mathbf{0} < z))$ )
value  $\tau \models ((\text{Set}\{\mathbf{2}, \text{null}\}) \rightarrow \text{exists}(z \mid \mathbf{0} < z))$ 

value  $\neg$  ( $\tau \models (\text{Set}\{\text{null}::'a \text{ Boolean}\} \doteq \text{Set}\{\})$ )
value  $\neg$  ( $\tau \models (\text{Set}\{\text{null}::'a \text{ Integer}\} \doteq \text{Set}\{\})$ )

value ( $\tau \models (\text{Set}\{\lambda-. [|x|]\} \doteq \text{Set}\{\lambda-. [|x|]\})$ )
value ( $\tau \models (\text{Set}\{\lambda-. [x]\} \doteq \text{Set}\{\lambda-. [x]\})$ )

lemma  $\neg$  ( $\tau \models (\text{Set}\{\text{true}\} \doteq \text{Set}\{\text{false}\})$ ) <proof>
lemma  $\neg$  ( $\tau \models (\text{Set}\{\text{true}, \text{true}\} \doteq \text{Set}\{\text{false}\})$ ) <proof>
lemma  $\neg$  ( $\tau \models (\text{Set}\{\mathbf{2}\} \doteq \text{Set}\{\mathbf{1}\})$ ) <proof>
lemma  $\tau \models (\text{Set}\{\mathbf{2}, \text{null}, \mathbf{2}\} \doteq \text{Set}\{\text{null}, \mathbf{2}\})$  <proof>
lemma  $\tau \models (\text{Set}\{\mathbf{1}, \text{null}, \mathbf{2}\} <> \text{Set}\{\text{null}, \mathbf{2}\})$  <proof>
lemma  $\tau \models (\text{Set}\{\text{Set}\{\mathbf{2}, \text{null}\}\} \doteq \text{Set}\{\text{Set}\{\text{null}, \mathbf{2}\}\})$  <proof>
lemma  $\tau \models (\text{Set}\{\text{Set}\{\mathbf{2}, \text{null}\}\} <> \text{Set}\{\text{Set}\{\text{null}, \mathbf{2}\}, \text{null}\})$  <proof>
lemma  $\tau \models (\text{Set}\{\text{null}\} \rightarrow \text{select}(x \mid \text{not } x) \doteq \text{Set}\{\text{null}\})$  <proof>
lemma  $\tau \models (\text{Set}\{\text{null}\} \rightarrow \text{reject}(x \mid \text{not } x) \doteq \text{Set}\{\text{null}\})$  <proof>

lemma const ( $\text{Set}\{\text{Set}\{\mathbf{2}, \text{null}\}, \text{invalid}\}$ ) <proof>

```

**end**



## 5. Formalization III: State Operations and Objects

```
theory OCL-state
imports OCL-lib
begin
```

### 5.1. 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 an objects and a universe of object representation, the generic infrastructure of state-related operations is fairly rich.

#### 5.1.1. Recall: The Generic Structure of States

Recall the foundational concept of an object id (oid), which is just some infinite set.

```
type-synonym oid = nat
```

Further, recall that states are pair of a partial map from oid's to elements of an object universe  $\mathcal{A}$ —the heap—and a map to relations of objects. The relations were encoded as lists of pairs to leave the possibility to have Bags, OrderedSets or Sequences as association ends.

This leads to the definitions:

```
record ('A)state =
  heap    :: "oid  $\rightarrow$  'A "
  assocs2 :: "oid  $\rightarrow$  (oid  $\times$  oid) list "
  assocs3 :: "oid  $\rightarrow$  (oid  $\times$  oid  $\times$  oid) list "
```

```
type-synonym ('A)st = "'A state  $\times$  'A state"
```

Now we refine our state-interface. In certain contexts, we will require that the elements of the object universe have a particular structure; more precisely, we will require that there is a function that reconstructs the oid of an object in the state (we will settle the question how to define this function later).

```
class object = fixes oid-of :: 'a  $\Rightarrow$  oid
```

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

```
typ 'A :: object
```

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

```
instantiation option :: (object)object
begin
  definition oid-of-option-def: oid-of x = oid-of (the x)
  instance <proof>
end
```

## 5.2. Fundamental Predicates on Object: Strict Equality

### Definition

Generic referential equality - to be used for instantiations with concrete object types ...

```
definition StrictRefEqObject :: ('A,'a::{object,null})val => ('A,'a)val => ('A)Boolean
where
  StrictRefEqObject x y
    ≡ λ τ. if (v x) τ = true τ ∧ (v y) τ = true τ
            then if x τ = null ∨ y τ = null
                  then [[x τ = null ∧ y τ = null]]
                  else [[(oid-of (x τ)) = (oid-of (y τ)) ]]
            else invalid τ
```

### 5.2.1. Logic and Algebraic Layer on Object

#### Validity and Definedness Properties

We derive the usual laws on definedness for (generic) object equality:

```
lemma StrictRefEqObject-defargs:
τ ⊨ (StrictRefEqObject x (y::('A,'a::{null,object})val))=> (τ ⊨(v x)) ∧ (τ ⊨(v y))
<proof>
```

#### Symmetry

```
lemma StrictRefEqObject-sym :
assumes x-val : τ ⊨ v x
shows τ ⊨ StrictRefEqObject x x
<proof>
```

#### Execution with Invalid or Null as Argument

```
lemma StrictRefEqObject-strict1[simp,code-unfold] :
(StrictRefEqObject x invalid) = invalid
<proof>
```

```
lemma StrictRefEqObject-strict2[simp,code-unfold] :
```

$(\text{StrictRefEq}_{\text{Object}} \text{ invalid } x) = \text{invalid}$   
 ⟨proof⟩

## Context Passing

**lemma**  $\text{cp-StrictRefEq}_{\text{Object}}$ :

$(\text{StrictRefEq}_{\text{Object}} x y \tau) = (\text{StrictRefEq}_{\text{Object}} (\lambda\cdot. x \tau) (\lambda\cdot. y \tau)) \tau$   
 ⟨proof⟩

**lemmas**  $\text{cp-intro''}[\text{intro!}, \text{simp}, \text{code-unfold}] =$   
 $\text{cp-intro''}$

$\text{cp-StrictRefEq}_{\text{Object}}[\text{THEN allI}[\text{THEN allI}[\text{THEN allI}[\text{THEN cpI2}]],$   
 $\text{of StrictRefEq}_{\text{Object}}]]$

## 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 [33, Annex A] and goes back to Richters [35]; 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**  $\text{WFF} :: (\mathfrak{A}::\text{object})st \Rightarrow \text{bool}$

**where**  $\text{WFF } \tau = ((\forall x \in \text{ran}(\text{heap}(\text{fst } \tau)). \lceil \text{heap}(\text{fst } \tau) (\text{oid-of } x) \rceil = x) \wedge$   
 $(\forall x \in \text{ran}(\text{heap}(\text{snd } \tau)). \lceil \text{heap}(\text{snd } \tau) (\text{oid-of } x) \rceil = x))$

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  $\doteq$  is defined by generic referential equality.

**theorem**  $\text{StrictRefEq}_{\text{Object-}vs\text{-StrongEq}}$ :

**assumes**  $\text{WFF}$ :  $\text{WFF } \tau$

**and**  $\text{valid-x}$ :  $\tau \models (v x)$

**and**  $\text{valid-y}$ :  $\tau \models (v y)$

**and**  $\text{x-present-pre}$ :  $x \tau \in \text{ran}(\text{heap}(\text{fst } \tau))$

**and** *y-present-pre*:  $y \tau \in \text{ran} (\text{heap}(\text{fst } \tau))$   
**and** *x-present-post*:  $x \tau \in \text{ran} (\text{heap}(\text{snd } \tau))$   
**and** *y-present-post*:  $y \tau \in \text{ran} (\text{heap}(\text{snd } \tau))$

**shows**  $(\tau \models (\text{StrictRefEqObject } x \ y)) = (\tau \models (x \triangleq y))$   
*<proof>*

**theorem** *StrictRefEqObject-vs-StrongEq'*:

**assumes** *WFF*:  $WFF \ \tau$

**and** *valid-x*:  $\tau \models (v \ (x :: ('A::\text{object}, 'a::\{\text{null}, \text{object}\}) \text{val}))$

**and** *valid-y*:  $\tau \models (v \ y)$

**and** *oid-preserve*:  $\bigwedge x. x \in \text{ran} (\text{heap}(\text{fst } \tau)) \vee x \in \text{ran} (\text{heap}(\text{snd } \tau)) \implies$   
 $H \ x \neq \perp \implies \text{oid-of } (H \ x) = \text{oid-of } x$

**and** *xy-together*:  $x \tau \in H \text{ ' ran } (\text{heap}(\text{fst } \tau)) \wedge y \tau \in H \text{ ' ran } (\text{heap}(\text{fst } \tau)) \vee$   
 $x \tau \in H \text{ ' ran } (\text{heap}(\text{snd } \tau)) \wedge y \tau \in H \text{ ' ran } (\text{heap}(\text{snd } \tau))$

**shows**  $(\tau \models (\text{StrictRefEqObject } x \ y)) = (\tau \models (x \triangleq y))$   
*<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.

## 5.3. Operations on Object

### 5.3.1. Initial States (for testing and code generation)

**definition**  $\tau_0 :: ('A) \text{st}$

**where**  $\tau_0 \equiv ((\text{heap} = \text{Map.empty}, \text{assocs}_2 = \text{Map.empty}, \text{assocs}_3 = \text{Map.empty}),$   
 $(\text{heap} = \text{Map.empty}, \text{assocs}_2 = \text{Map.empty}, \text{assocs}_3 = \text{Map.empty}))$

### 5.3.2. 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 a sufficient “characterization.”

**definition** *OclAllInstances-generic* ::  $((('A::\text{object}) \text{st} \Rightarrow 'A \ \text{state}) \Rightarrow ('A::\text{object} \rightarrow 'a) \Rightarrow$   
 $('A, 'a \ \text{option}) \ \text{Set}$

**where** *OclAllInstances-generic* *fst-snd*  $H =$

$(\lambda \tau. \text{Abs-Set-0 } [ [ \text{Some } \text{ ' } ((H \text{ ' ran } (\text{heap} (\text{fst-snd } \tau))) - \{ \text{None } \} ) ] ])$

**lemma** *OclAllInstances-generic-defined*:  $\tau \models \delta \ (OclAllInstances-generic \ \text{pre-post } H)$   
*<proof>*

**lemma** *OclAllInstances-generic-init-empty*:

**assumes** [*simp*]:  $\bigwedge x. \text{pre-post } (x, x) = x$

**shows**  $\tau_0 \models OclAllInstances-generic \ \text{pre-post } H \triangleq \text{Set}\{\}$

*<proof>*



**lemma** *represented-generic-objects-nonnul*:

**assumes**  $A: \tau \models ((\text{OclAllInstances-generic pre-post } (H::('A::\text{object} \rightarrow 'a))) \rightarrow \text{includes}(x))$

**shows**  $\tau \models \text{not}(x \hat{=} \text{null})$

*<proof>*

**lemma** *represented-generic-objects-defined*:

**assumes**  $A: \tau \models ((\text{OclAllInstances-generic pre-post } (H::('A::\text{object} \rightarrow 'a))) \rightarrow \text{includes}(x))$

**shows**  $\tau \models \delta (\text{OclAllInstances-generic pre-post } H) \wedge \tau \models \delta x$

*<proof>*

One way to establish the actual presence of an object representation in a state is:

**lemma** *represented-generic-objects-in-state*:

**assumes**  $A: \tau \models (\text{OclAllInstances-generic pre-post } H) \rightarrow \text{includes}(x)$

**shows**  $x \tau \in (\text{Some } o \ H) \text{ 'ran } (\text{heap}(\text{pre-post } \tau))$

*<proof>*

**lemma** *state-update-vs-allInstances-generic-empty*:

**assumes**  $[\text{simp}]: \bigwedge a. \text{pre-post } (\text{mk } a) = a$

**shows**  $(\text{mk } (\text{heap}=\text{empty}, \text{assocs}_2=A, \text{assocs}_3=B)) \models \text{OclAllInstances-generic pre-post Type} \doteq \text{Set}\{\}$

*<proof>*

Here comes a couple of operational rules that allow to infer the value of `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-including'*:

**assumes**  $[\text{simp}]: \bigwedge a. \text{pre-post } (\text{mk } a) = a$

**assumes**  $\bigwedge x. \sigma' \text{ oid} = \text{Some } x \implies x = \text{Object}$

**and**  $\text{Type Object} \neq \text{None}$

**shows**  $(\text{OclAllInstances-generic pre-post Type})$

$(\text{mk } (\text{heap}=\sigma'(\text{oid} \mapsto \text{Object}), \text{assocs}_2=A, \text{assocs}_3=B))$

$=$

$((\text{OclAllInstances-generic pre-post Type}) \rightarrow \text{including}(\lambda -. \llbracket \text{drop } (\text{Type Object}) \rrbracket))$

$(\text{mk } (\text{heap}=\sigma', \text{assocs}_2=A, \text{assocs}_3=B))$

*<proof>*

**lemma** *state-update-vs-allInstances-generic-including*:

**assumes**  $[\text{simp}]: \bigwedge a. \text{pre-post } (\text{mk } a) = a$

**assumes**  $\bigwedge x. \sigma' \text{ oid} = \text{Some } x \implies x = \text{Object}$

**and**  $\text{Type Object} \neq \text{None}$

**shows**  $(\text{OclAllInstances-generic pre-post Type})$

$(\text{mk } (\text{heap}=\sigma'(\text{oid} \mapsto \text{Object}), \text{assocs}_2=A, \text{assocs}_3=B))$

$=$

$((\lambda -. (OclAllInstances-generic\ pre-post\ Type)$   
 $(mk\ (\!heap=\sigma',\ assoc_2=A,\ assoc_3=B))) \rightarrow including(\lambda -. \llbracket drop\ (Type\ Object)$   
 $\rrbracket))$   
 $(mk\ (\!heap=\sigma'(oid \mapsto Object),\ assoc_2=A,\ assoc_3=B))$   
 $\langle proof \rangle$

**lemma** *state-update-vs-allInstances-generic-noincluding'*:  
**assumes**  $[simp]: \bigwedge a. pre-post\ (mk\ a) = a$   
**assumes**  $\bigwedge x. \sigma'\ oid = Some\ x \implies x = Object$   
**and**  $Type\ Object = None$   
**shows**  $(OclAllInstances-generic\ pre-post\ Type)$   
 $(mk\ (\!heap=\sigma'(oid \mapsto Object),\ assoc_2=A,\ assoc_3=B))$   
 $=$   
 $(OclAllInstances-generic\ pre-post\ Type)$   
 $(mk\ (\!heap=\sigma',\ assoc_2=A,\ assoc_3=B))$   
 $\langle proof \rangle$

**theorem** *state-update-vs-allInstances-generic-ntc*:  
**assumes**  $[simp]: \bigwedge a. pre-post\ (mk\ a) = a$   
**assumes** *oid-def*:  $oid \notin dom\ \sigma'$   
**and** *non-type-conform*:  $Type\ Object = None$   
**and** *cp-ctxt*:  $cp\ P$   
**and** *const-ctxt*:  $\bigwedge X. const\ X \implies const\ (P\ X)$   
**shows**  $(mk\ (\!heap=\sigma'(oid \mapsto Object),\ assoc_2=A,\ assoc_3=B)) \models P\ (OclAllInstances-generic$   
 $pre-post\ Type)) =$   
 $(mk\ (\!heap=\sigma',\ assoc_2=A,\ assoc_3=B)) \models P\ (OclAllInstances-generic\ pre-post$   
 $Type))$   
 $(is\ (? \tau \models P\ ? \varphi) = (? \tau' \models P\ ? \varphi))$   
 $\langle proof \rangle$

**theorem** *state-update-vs-allInstances-generic-tc*:  
**assumes**  $[simp]: \bigwedge a. pre-post\ (mk\ a) = a$   
**assumes** *oid-def*:  $oid \notin dom\ \sigma'$   
**and** *type-conform*:  $Type\ Object \neq None$   
**and** *cp-ctxt*:  $cp\ P$   
**and** *const-ctxt*:  $\bigwedge X. const\ X \implies const\ (P\ X)$   
**shows**  $(mk\ (\!heap=\sigma'(oid \mapsto Object),\ assoc_2=A,\ assoc_3=B)) \models P\ (OclAllInstances-generic$   
 $pre-post\ Type)) =$   
 $(mk\ (\!heap=\sigma',\ assoc_2=A,\ assoc_3=B)) \models P\ ((OclAllInstances-generic\ pre-post$   
 $Type)$   
 $\rightarrow including(\lambda -. \llbracket (Type\ Object) \rrbracket))$   
 $(is\ (? \tau \models P\ ? \varphi) = (? \tau' \models P\ ? \varphi'))$   
 $\langle proof \rangle$

**declare** *OclAllInstances-generic-def*  $[simp]$

## OclAllInstances (@post)

**definition**  $OclAllInstances\text{-}at\text{-}post :: ('\mathfrak{A} :: object \rightarrow '\alpha) \Rightarrow ('\mathfrak{A}, '\alpha\ option\ option)\ Set$   
 $(- .allInstances'(\cdot))$

**where**  $OclAllInstances\text{-}at\text{-}post = OclAllInstances\text{-}generic\ snd$

**lemma**  $OclAllInstances\text{-}at\text{-}post\text{-}defined: \tau \models \delta (H .allInstances())$   
 $\langle proof \rangle$

**lemma**  $\tau_0 \models H .allInstances() \triangleq Set\{\}$   
 $\langle proof \rangle$

**lemma**  $represented\text{-}at\text{-}post\text{-}objects\text{-}nonnull:$   
**assumes**  $A: \tau \models (((H::(''\mathfrak{A}::object \rightarrow '\alpha)).allInstances()) \rightarrow includes(x))$   
**shows**  $\tau \models not(x \triangleq null)$   
 $\langle proof \rangle$

**lemma**  $represented\text{-}at\text{-}post\text{-}objects\text{-}defined:$   
**assumes**  $A: \tau \models (((H::(''\mathfrak{A}::object \rightarrow '\alpha)).allInstances()) \rightarrow includes(x))$   
**shows**  $\tau \models \delta (H .allInstances()) \wedge \tau \models \delta x$   
 $\langle proof \rangle$

One way to establish the actual presence of an object representation in a state is:

**lemma**  
**assumes**  $A: \tau \models H .allInstances() \rightarrow includes(x)$   
**shows**  $x \tau \in (Some\ o\ H) \text{ 'ran } (heap(snd\ \tau))$   
 $\langle proof \rangle$

**lemma**  $state\text{-}update\text{-}vs\text{-}allInstances\text{-}at\text{-}post\text{-}empty:$   
**shows**  $(\sigma, (\heaps=empty, assoc_2=A, assoc_3=B)) \models Type .allInstances() \doteq Set\{\}$   
 $\langle proof \rangle$

Here comes a couple of operational rules that allow to infer the value of `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**  $state\text{-}update\text{-}vs\text{-}allInstances\text{-}at\text{-}post\text{-}including':$   
**assumes**  $\bigwedge x. \sigma' oid = Some\ x \implies x = Object$   
**and**  $Type\ Object \neq None$   
**shows**  $(Type .allInstances())$   
 $(\sigma, (\heaps=\sigma'(oid \mapsto Object), assoc_2=A, assoc_3=B))$   
 $=$   
 $((Type .allInstances()) \rightarrow including(\lambda -. \llbracket drop (Type\ Object) \rrbracket))$   
 $(\sigma, (\heaps=\sigma', assoc_2=A, assoc_3=B))$   
 $\langle proof \rangle$

**lemma** *state-update-vs-allInstances-at-post-including*:  
**assumes**  $\bigwedge x. \sigma' \text{ oid} = \text{Some } x \implies x = \text{Object}$   
**and** *Type Object*  $\neq \text{None}$   
**shows**  $(\text{Type} . \text{allInstances}())$   
 $(\sigma, (\text{heap}=\sigma'(\text{oid} \mapsto \text{Object}), \text{assocs}_2=A, \text{assocs}_3=B))$   
 $=$   
 $(\lambda \cdot (\text{Type} . \text{allInstances}())$   
 $(\sigma, (\text{heap}=\sigma', \text{assocs}_2=A, \text{assocs}_3=B))) \rightarrow \text{including}(\lambda \cdot \llbracket \text{drop } (\text{Type } \text{Object})$   
 $\rrbracket))$   
 $(\sigma, (\text{heap}=\sigma'(\text{oid} \mapsto \text{Object}), \text{assocs}_2=A, \text{assocs}_3=B))$   
 $\langle \text{proof} \rangle$

**lemma** *state-update-vs-allInstances-at-post-noincluding'*:  
**assumes**  $\bigwedge x. \sigma' \text{ oid} = \text{Some } x \implies x = \text{Object}$   
**and** *Type Object*  $= \text{None}$   
**shows**  $(\text{Type} . \text{allInstances}())$   
 $(\sigma, (\text{heap}=\sigma'(\text{oid} \mapsto \text{Object}), \text{assocs}_2=A, \text{assocs}_3=B))$   
 $=$   
 $(\text{Type} . \text{allInstances}())$   
 $(\sigma, (\text{heap}=\sigma', \text{assocs}_2=A, \text{assocs}_3=B))$   
 $\langle \text{proof} \rangle$

**theorem** *state-update-vs-allInstances-at-post-ntc*:  
**assumes** *oid-def*:  $\text{oid} \notin \text{dom } \sigma'$   
**and** *non-type-conform*: *Type Object*  $= \text{None}$   
**and** *cp-ctxt*:  $\text{cp } P$   
**and** *const-ctxt*:  $\bigwedge X. \text{const } X \implies \text{const } (P X)$   
**shows**  $((\sigma, (\text{heap}=\sigma'(\text{oid} \mapsto \text{Object}), \text{assocs}_2=A, \text{assocs}_3=B)) \models (P(\text{Type} . \text{allInstances}()))) =$   
 $((\sigma, (\text{heap}=\sigma', \text{assocs}_2=A, \text{assocs}_3=B)) \models (P(\text{Type} . \text{allInstances}())))$   
 $\langle \text{proof} \rangle$

**theorem** *state-update-vs-allInstances-at-post-tc*:  
**assumes** *oid-def*:  $\text{oid} \notin \text{dom } \sigma'$   
**and** *type-conform*: *Type Object*  $\neq \text{None}$   
**and** *cp-ctxt*:  $\text{cp } P$   
**and** *const-ctxt*:  $\bigwedge X. \text{const } X \implies \text{const } (P X)$   
**shows**  $((\sigma, (\text{heap}=\sigma'(\text{oid} \mapsto \text{Object}), \text{assocs}_2=A, \text{assocs}_3=B)) \models (P(\text{Type} . \text{allInstances}()))) =$   
 $((\sigma, (\text{heap}=\sigma', \text{assocs}_2=A, \text{assocs}_3=B)) \models (P((\text{Type} . \text{allInstances}())$   
 $\rightarrow \text{including}(\lambda \cdot \llbracket (\text{Type } \text{Object}) \rrbracket))))$   
 $\langle \text{proof} \rangle$

## OclAllInstances (@pre)

**definition** *OclAllInstances-at-pre* ::  $(\mathfrak{A} :: \text{object} \rightarrow \alpha) \Rightarrow (\mathfrak{A}, \alpha \text{ option option}) \text{ Set}$   
 $(\cdot . \text{allInstances}@pre'(\cdot))$

**where**  $OclAllInstances\text{-}at\text{-}pre = OclAllInstances\text{-}generic\ fst$

**lemma**  $OclAllInstances\text{-}at\text{-}pre\text{-}defined: \tau \models \delta (H .allInstances@pre())$   
 $\langle proof \rangle$

**lemma**  $\tau_0 \models H .allInstances@pre() \triangleq Set\{\}$   
 $\langle proof \rangle$

**lemma**  $represented\text{-}at\text{-}pre\text{-}objects\text{-}nonnull:$   
**assumes**  $A: \tau \models (((H::('Q::object \rightarrow 'a)).allInstances@pre()) \rightarrow includes(x))$   
**shows**  $\tau \models not(x \triangleq null)$   
 $\langle proof \rangle$

**lemma**  $represented\text{-}at\text{-}pre\text{-}objects\text{-}defined:$   
**assumes**  $A: \tau \models (((H::('Q::object \rightarrow 'a)).allInstances@pre()) \rightarrow includes(x))$   
**shows**  $\tau \models \delta (H .allInstances@pre()) \wedge \tau \models \delta x$   
 $\langle proof \rangle$

One way to establish the actual presence of an object representation in a state is:

**lemma**  
**assumes**  $A: \tau \models H .allInstances@pre() \rightarrow includes(x)$   
**shows**  $x \tau \in (Some\ o\ H) \text{ ' } ran\ (heap\ fst\ \tau)$   
 $\langle proof \rangle$

**lemma**  $state\text{-}update\text{-}vs\text{-}allInstances\text{-}at\text{-}pre\text{-}empty:$   
**shows**  $((heap=empty, assoc_2=A, assoc_3=B), \sigma) \models Type .allInstances@pre() \doteq Set\{\}$   
 $\langle proof \rangle$

Here comes a couple of operational rules that allow to infer the value of  $oclAllInstances@pre$  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**  $state\text{-}update\text{-}vs\text{-}allInstances\text{-}at\text{-}pre\text{-}including':$   
**assumes**  $\bigwedge x. \sigma' oid = Some\ x \implies x = Object$   
**and**  $Type\ Object \neq None$   
**shows**  $(Type .allInstances@pre())$   
 $((heap=\sigma'(oid \mapsto Object), assoc_2=A, assoc_3=B), \sigma)$   
 $=$   
 $((Type .allInstances@pre()) \rightarrow including(\lambda \cdot. [| drop (Type\ Object) ]))$   
 $((heap=\sigma', assoc_2=A, assoc_3=B), \sigma)$   
 $\langle proof \rangle$

**lemma**  $state\text{-}update\text{-}vs\text{-}allInstances\text{-}at\text{-}pre\text{-}including:$   
**assumes**  $\bigwedge x. \sigma' oid = Some\ x \implies x = Object$

**and** *Type Object*  $\neq$  *None*  
**shows** (*Type .allInstances@pre*())  
 ((*heap*= $\sigma'$ (*oid* $\mapsto$ *Object*), *assoc*<sub>2</sub>=*A*, *assoc*<sub>3</sub>=*B*),  $\sigma$ )  
 =  
 (( $\lambda$ -. (*Type .allInstances@pre*()))  
 ((*heap*= $\sigma'$ , *assoc*<sub>2</sub>=*A*, *assoc*<sub>3</sub>=*B*),  $\sigma$ )) $\rightarrow$ *including*( $\lambda$  -. [*drop* (*Type Object*)])  
 ]])  
 ((*heap*= $\sigma'$ (*oid* $\mapsto$ *Object*), *assoc*<sub>2</sub>=*A*, *assoc*<sub>3</sub>=*B*),  $\sigma$ )  
 <*proof*>

**lemma** *state-update-vs-allInstances-at-pre-noincluding'*:

**assumes**  $\bigwedge x. \sigma' \text{ oid} = \text{Some } x \implies x = \text{Object}$   
**and** *Type Object* = *None*  
**shows** (*Type .allInstances@pre*())  
 ((*heap*= $\sigma'$ (*oid* $\mapsto$ *Object*), *assoc*<sub>2</sub>=*A*, *assoc*<sub>3</sub>=*B*),  $\sigma$ )  
 =  
 (*Type .allInstances@pre*()))  
 ((*heap*= $\sigma'$ , *assoc*<sub>2</sub>=*A*, *assoc*<sub>3</sub>=*B*),  $\sigma$ )  
 <*proof*>

**theorem** *state-update-vs-allInstances-at-pre-ntc*:

**assumes** *oid-def*: *oid*  $\notin$  *dom*  $\sigma'$   
**and** *non-type-conform*: *Type Object* = *None*  
**and** *cp-ctxt*: *cp* *P*  
**and** *const-ctxt*:  $\bigwedge X. \text{const } X \implies \text{const } (P X)$   
**shows** (((*heap*= $\sigma'$ (*oid* $\mapsto$ *Object*), *assoc*<sub>2</sub>=*A*, *assoc*<sub>3</sub>=*B*),  $\sigma$ )  $\models$  (*P*(*Type .allInstances@pre*()))  
 =  
 (((*heap*= $\sigma'$ , *assoc*<sub>2</sub>=*A*, *assoc*<sub>3</sub>=*B*),  $\sigma$ )  $\models$  (*P*(*Type .allInstances@pre*()))  
 <*proof*>

**theorem** *state-update-vs-allInstances-at-pre-tc*:

**assumes** *oid-def*: *oid*  $\notin$  *dom*  $\sigma'$   
**and** *type-conform*: *Type Object*  $\neq$  *None*  
**and** *cp-ctxt*: *cp* *P*  
**and** *const-ctxt*:  $\bigwedge X. \text{const } X \implies \text{const } (P X)$   
**shows** (((*heap*= $\sigma'$ (*oid* $\mapsto$ *Object*), *assoc*<sub>2</sub>=*A*, *assoc*<sub>3</sub>=*B*),  $\sigma$ )  $\models$  (*P*(*Type .allInstances@pre*()))  
 =  
 (((*heap*= $\sigma'$ , *assoc*<sub>2</sub>=*A*, *assoc*<sub>3</sub>=*B*),  $\sigma$ )  $\models$  (*P*((*Type .allInstances@pre*))  
 $\rightarrow$ *including*( $\lambda$  -. [*Type Object*])))  
 <*proof*>

## @post or @pre

**theorem** *StrictRefEqObject-vs-StrongEq''*:

**assumes** *WFF*: *WFF*  $\tau$   
**and** *valid-x*:  $\tau \models (v (x :: (\mathfrak{A}::\text{object}, \alpha::\text{object option option}) \text{val}))$   
**and** *valid-y*:  $\tau \models (v y)$

**and** *oid-preserve*:  $\bigwedge x. x \in \text{ran}(\text{heap}(\text{fst } \tau)) \vee x \in \text{ran}(\text{heap}(\text{snd } \tau)) \implies$   
 $\text{oid-of}(H x) = \text{oid-of } x$   
**and** *xy-together*:  $\tau \models ((H .\text{allInstances}() \text{-->includes}(x) \text{ and } H .\text{allInstances}() \text{-->includes}(y))$   
*or*  
 $(H .\text{allInstances}@pre() \text{-->includes}(x) \text{ and } H .\text{allInstances}@pre() \text{-->includes}(y))$   
**shows**  $(\tau \models (\text{StrictRefEqObject } x y)) = (\tau \models (x \hat{=} y))$   
*<proof>*

### 5.3.3. OclIsNew, OclIsDeleted, OclIsMaintained, OclIsAbsent

**definition** *OclIsNew*::  $(\mathfrak{A}, ' \alpha :: \{ \text{null}, \text{object} \}) \text{val} \Rightarrow (\mathfrak{A}) \text{Boolean } ((-).\text{oclIsNew}'('))$   
**where**  $X .\text{oclIsNew}() \equiv (\lambda \tau . \text{if } (\delta X) \tau = \text{true } \tau$   
 $\text{then } [[\text{oid-of}(X \tau) \notin \text{dom}(\text{heap}(\text{fst } \tau)) \wedge$   
 $\text{oid-of}(X \tau) \in \text{dom}(\text{heap}(\text{snd } \tau))]]$   
 $\text{else } \text{invalid } \tau)$

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*::  $(\mathfrak{A}, ' \alpha :: \{ \text{null}, \text{object} \}) \text{val} \Rightarrow (\mathfrak{A}) \text{Boolean } ((-).\text{oclIsDeleted}'('))$   
**where**  $X .\text{oclIsDeleted}() \equiv (\lambda \tau . \text{if } (\delta X) \tau = \text{true } \tau$   
 $\text{then } [[\text{oid-of}(X \tau) \in \text{dom}(\text{heap}(\text{fst } \tau)) \wedge$   
 $\text{oid-of}(X \tau) \notin \text{dom}(\text{heap}(\text{snd } \tau))]]$   
 $\text{else } \text{invalid } \tau)$

**definition** *OclIsMaintained*::  $(\mathfrak{A}, ' \alpha :: \{ \text{null}, \text{object} \}) \text{val} \Rightarrow (\mathfrak{A}) \text{Boolean}((-).\text{oclIsMaintained}'('))$   
**where**  $X .\text{oclIsMaintained}() \equiv (\lambda \tau . \text{if } (\delta X) \tau = \text{true } \tau$   
 $\text{then } [[\text{oid-of}(X \tau) \in \text{dom}(\text{heap}(\text{fst } \tau)) \wedge$   
 $\text{oid-of}(X \tau) \in \text{dom}(\text{heap}(\text{snd } \tau))]]$   
 $\text{else } \text{invalid } \tau)$

**definition** *OclIsAbsent*::  $(\mathfrak{A}, ' \alpha :: \{ \text{null}, \text{object} \}) \text{val} \Rightarrow (\mathfrak{A}) \text{Boolean } ((-).\text{oclIsAbsent}'('))$   
**where**  $X .\text{oclIsAbsent}() \equiv (\lambda \tau . \text{if } (\delta X) \tau = \text{true } \tau$   
 $\text{then } [[\text{oid-of}(X \tau) \notin \text{dom}(\text{heap}(\text{fst } \tau)) \wedge$   
 $\text{oid-of}(X \tau) \notin \text{dom}(\text{heap}(\text{snd } \tau))]]$   
 $\text{else } \text{invalid } \tau)$

**lemma** *state-split* :  $\tau \models \delta X \implies$   
 $\tau \models (X .\text{oclIsNew}()) \vee \tau \models (X .\text{oclIsDeleted}()) \vee$   
 $\tau \models (X .\text{oclIsMaintained}()) \vee \tau \models (X .\text{oclIsAbsent}())$   
*<proof>*

**lemma** *notNew-vs-others* :  $\tau \models \delta X \implies$   
 $(\neg \tau \models (X .\text{oclIsNew}())) = (\tau \models (X .\text{oclIsDeleted}()) \vee$   
 $\tau \models (X .\text{oclIsMaintained}()) \vee \tau \models (X .\text{oclIsAbsent}())$   
*<proof>*

### 5.3.4. 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**  $OclIsModifiedOnly :: (\mathcal{A}::object, \alpha::\{null, object\})Set \Rightarrow \mathcal{A} Boolean$   
 $(-->oclIsModifiedOnly'(\prime))$

**where**  $X-->oclIsModifiedOnly() \equiv (\lambda(\sigma, \sigma')).$

$let X' = (oid-of \prime \llbracket Rep-Set-0(X(\sigma, \sigma')) \rrbracket \rrbracket);$

$S = ((dom(heap \sigma) \cap dom(heap \sigma')) - X')$

$in \text{ if } (\delta X) (\sigma, \sigma') = true (\sigma, \sigma') \wedge (\forall x \in \llbracket Rep-Set-0(X(\sigma, \sigma')) \rrbracket. x \neq null)$

$then \llbracket \forall x \in S. (heap \sigma) x = (heap \sigma') x \rrbracket$

$else invalid (\sigma, \sigma')$

#### Execution with Invalid or Null or Null Element as Argument

**lemma**  $invalid-->oclIsModifiedOnly() = invalid$   
 $\langle proof \rangle$

**lemma**  $null-->oclIsModifiedOnly() = invalid$   
 $\langle proof \rangle$

#### lemma

**assumes**  $X-null : \tau \models X-->includes(null)$

**shows**  $\tau \models X-->oclIsModifiedOnly() \triangleq invalid$

$\langle proof \rangle$

#### Context Passing

**lemma**  $cp-OclIsModifiedOnly : X-->oclIsModifiedOnly() \tau = (\lambda-. X \tau)-->oclIsModifiedOnly()$   
 $\tau$   
 $\langle proof \rangle$

### 5.3.5. 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**  $[simp]: OclSelf x H fst-snd = (\lambda\tau . \text{ if } (\delta x) \tau = true \tau$   
 $then \text{ if } oid-of (x \tau) \in dom(heap(fst \tau)) \wedge oid-of (x \tau) \in dom(heap(snd \tau))$   
 $then H \llbracket (heap(fst-snd \tau))(oid-of (x \tau)) \rrbracket$   
 $else invalid \tau$   
 $else invalid \tau)$

**definition**  $OclSelf-at-pre :: (\mathcal{A}::object, \alpha::\{null, object\})val \Rightarrow$



$(\mathcal{A} \Rightarrow \alpha) \Rightarrow$   
 $(\mathcal{A}::\text{object}, \alpha::\{\text{null}, \text{object}\}) \text{val } ((-)\text{@pre}(-))$   
**where**  $x \text{@pre } H = \text{OclSelf } x \text{ } H \text{ } \text{fst}$

**definition**  $\text{OclSelf-at-post} :: (\mathcal{A}::\text{object}, \alpha::\{\text{null}, \text{object}\}) \text{val } \Rightarrow$   
 $(\mathcal{A} \Rightarrow \alpha) \Rightarrow$   
 $(\mathcal{A}::\text{object}, \alpha::\{\text{null}, \text{object}\}) \text{val } ((-)\text{@post}(-))$   
**where**  $x \text{@post } H = \text{OclSelf } x \text{ } H \text{ } \text{snd}$

### 5.3.6. Framing Theorem

**lemma** *all-oid-diff*:

**assumes**  $\text{def-}x : \tau \models \delta \ x$

**assumes**  $\text{def-}X : \tau \models \delta \ X$

**assumes**  $\text{def-}X' : \bigwedge x. x \in [[\text{Rep-Set-0 } (X \ \tau)]] \Rightarrow x \neq \text{null}$

**defines**  $P \equiv (\lambda a. \text{not } (\text{StrictRefEqObject } x \ a))$

**shows**  $(\tau \models X \text{->forAll}(a \mid P \ a)) = (\text{oid-of } (x \ \tau) \notin \text{oid-of } ' [[\text{Rep-Set-0 } (X \ \tau)]])$

*<proof>*

**theorem** *framing*:

**assumes**  $\text{modifiesclause} : \tau \models (X \text{->excluding}(x)) \text{->oclIsModifiedOnly}()$

**and**  $\text{oid-is-typerepr} : \tau \models X \text{->forAll}(a \mid \text{not } (\text{StrictRefEqObject } x \ a))$

**shows**  $\tau \models (x \text{@pre } P \stackrel{\Delta}{=} (x \text{@post } P))$

*<proof>*

As corollary, the framing property can be expressed with only the strong equality as comparison operator.

**theorem** *framing'*:

**assumes**  $\text{wff} : \text{WFF } \tau$

**assumes**  $\text{modifiesclause} : \tau \models (X \text{->excluding}(x)) \text{->oclIsModifiedOnly}()$

**and**  $\text{oid-is-typerepr} : \tau \models X \text{->forAll}(a \mid \text{not } (x \stackrel{\Delta}{=} a))$

**and**  $\text{oid-preserve} : \bigwedge x. x \in \text{ran } (\text{heap}(\text{fst } \tau)) \vee x \in \text{ran } (\text{heap}(\text{snd } \tau)) \Rightarrow$   
 $\text{oid-of } (H \ x) = \text{oid-of } x$

**and** *xy-together*:

$\tau \models X \text{->forAll}(y \mid (H \ .\text{allInstances}() \text{->includes}(x) \ \text{and } H \ .\text{allInstances}() \text{->includes}(y)) \ \text{or}$   
 $(H \ .\text{allInstances}@pre() \text{->includes}(x) \ \text{and } H \ .\text{allInstances}@pre() \text{->includes}(y)))$

**shows**  $\tau \models (x \text{@pre } P \stackrel{\Delta}{=} (x \text{@post } P))$

*<proof>*

### 5.3.7. Miscellaneous

**lemma** *pre-post-new*:  $\tau \models (x \ .\text{oclIsNew}()) \Rightarrow \neg (\tau \models v(x \text{@pre } H1)) \wedge \neg (\tau \models v(x \text{@post } H2))$

*<proof>*

**lemma** *pre-post-old*:  $\tau \models (x \ .\text{oclIsDeleted}()) \Rightarrow \neg (\tau \models v(x \text{@pre } H1)) \wedge \neg (\tau \models v(x \text{@post } H2))$

*<proof>*

**lemma** *pre-post-absent*:  $\tau \models (x .oclIsAbsent()) \implies \neg (\tau \models v(x @pre H1)) \wedge \neg (\tau \models v(x @post H2))$   
*<proof>*

**lemma** *pre-post-maintained*:  $(\tau \models v(x @pre H1) \vee \tau \models v(x @post H2)) \implies \tau \models (x .oclIsMaintained())$   
*<proof>*

**lemma** *pre-post-maintained'*:  
 $\tau \models (x .oclIsMaintained()) \implies (\tau \models v(x @pre (Some o H1)) \wedge \tau \models v(x @post (Some o H2)))$   
*<proof>*

**lemma** *framing-same-state*:  $(\sigma, \sigma) \models (x @pre H \triangleq (x @post H))$   
*<proof>*

**end**

**theory** *OCL-tools*  
**imports** *OCL-core*  
**begin**

**end**

**theory** *OCL-main*  
**imports** *OCL-lib OCL-state OCL-tools*  
**begin**

**end**

**Part III.**  
**Examples**



## 6. The Employee Analysis Model

### 6.1. The Employee Analysis Model (UML)

```
theory
  Employee-AnalysisModel-UMLPart
imports
  ../OCL-main
begin
```

#### 6.1.1. 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.

#### Outlining the Example

We are presenting here an “analysis-model” of the (slightly modified) example Figure 7.3, page 20 of the OCL standard [33]. 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 Section 7.1). To be precise, this theory contains the formalization of the data-part covered by the UML class model (see Figure 6.1):

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).

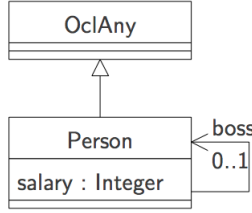


Figure 6.1.: A simple UML class model drawn from Figure 7.3, page 20 of [33].

### 6.1.2. 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:

```
datatype typePerson = mkPerson oid
                    int option
```

```
datatype typeOclAny = mkOclAny oid
                    (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.

```
datatype  $\mathfrak{A}$  = 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.

```
type-synonym Boolean    =  $\mathfrak{A}$  Boolean
type-synonym Integer   =  $\mathfrak{A}$  Integer
type-synonym Void     =  $\mathfrak{A}$  Void
type-synonym OclAny    = ( $\mathfrak{A}$ , typeOclAny option option) val
type-synonym Person    = ( $\mathfrak{A}$ , typePerson option option) val
type-synonym Set-Integer = ( $\mathfrak{A}$ , int option option) Set
type-synonym Set-Person = ( $\mathfrak{A}$ , typePerson option option) Set
```

Just a little check:

```
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.

**instantiation** *typePerson* :: *object*

**begin**

**definition** *oid-of-typePerson-def*: *oid-of* *x* = (*case* *x* of *mkPerson* *oid* -  $\Rightarrow$  *oid*)

**instance**  $\langle$ *proof* $\rangle$

**end**

**instantiation** *typeOclAny* :: *object*

**begin**

**definition** *oid-of-typeOclAny-def*: *oid-of* *x* = (*case* *x* of *mkOclAny* *oid* -  $\Rightarrow$  *oid*)

**instance**  $\langle$ *proof* $\rangle$

**end**

**instantiation**  $\mathfrak{A}$  :: *object*

**begin**

**definition** *oid-of- $\mathfrak{A}$ -def*: *oid-of* *x* = (*case* *x* of

*inPerson* *person*  $\Rightarrow$  *oid-of* *person*  
| *inOclAny* *oclany*  $\Rightarrow$  *oid-of* *oclany*)

**instance**  $\langle$ *proof* $\rangle$

**end**

### 6.1.3. Instantiation of the Generic Strict Equality

We instantiate the referential equality on *Person* and *OclAny*

**defs(overloaded)** *StrictRefEqObjectPerson* : (*x*::*Person*)  $\doteq$  *y*  $\equiv$  *StrictRefEqObject* *x* *y*

**defs(overloaded)** *StrictRefEqObjectOclAny* : (*x*::*OclAny*)  $\doteq$  *y*  $\equiv$  *StrictRefEqObject* *x* *y*

**lemmas**

*cp-StrictRefEqObject*[*of* *x*::*Person* *y*::*Person*  $\tau$ ,

*simplified* *StrictRefEqObjectPerson*[*symmetric*]]

*cp-intro*(9) [of *P*::*Person*  $\Rightarrow$  *Person* *Q*::*Person*  $\Rightarrow$  *Person*,

*simplified* *StrictRefEqObjectPerson*[*symmetric*]]

*StrictRefEqObject-def* [of *x*::*Person* *y*::*Person*,

*simplified* *StrictRefEqObjectPerson*[*symmetric*]]

*StrictRefEqObject-defargs* [of - *x*::*Person* *y*::*Person*,

*simplified* *StrictRefEqObjectPerson*[*symmetric*]]

*StrictRefEqObject-strict1*

[of *x*::*Person*,

*simplified* *StrictRefEqObjectPerson*[*symmetric*]]

*StrictRefEqObject-strict2*

[of *x*::*Person*,

*simplified* *StrictRefEqObjectPerson*[*symmetric*]]

For each Class *C*, we will have a casting operation *.oclAsType*(*C*), a test on the actual type *.oclIsTypeOf*(*C*) as well as its relaxed form *.oclIsKindOf*(*C*) (corresponding exactly to Java’s *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.

#### 6.1.4. OclAsType

##### Definition

**consts**  $OclAsType_{OclAny} :: 'α \Rightarrow OclAny \ ((-) .oclAsType' (OclAny'))$

**consts**  $OclAsType_{Person} :: 'α \Rightarrow Person \ ((-) .oclAsType' (Person'))$

**definition**  $OclAsType_{OclAny}\text{-}\mathfrak{A} = (\lambda u. \_case\ u\ of\ in_{OclAny}\ a \Rightarrow a$   
 $\quad | in_{Person}\ (mk_{Person}\ oid\ a) \Rightarrow mk_{OclAny}\ oid\ [a])$

**lemma**  $OclAsType_{OclAny}\text{-}\mathfrak{A}\text{-}some$ :  $OclAsType_{OclAny}\text{-}\mathfrak{A}\ x \neq None$   
 $\langle proof \rangle$

**defs (overloaded)**  $OclAsType_{OclAny}\text{-}OclAny$ :  
 $(X::OclAny) .oclAsType(OclAny) \equiv X$

**defs (overloaded)**  $OclAsType_{OclAny}\text{-}Person$ :  
 $(X::Person) .oclAsType(OclAny) \equiv$   
 $(\lambda \tau. case\ X\ \tau\ of$   
 $\quad \perp \Rightarrow invalid\ \tau$   
 $\quad | [\perp] \Rightarrow null\ \tau$   
 $\quad | [[mk_{Person}\ oid\ a]] \Rightarrow [[(mk_{OclAny}\ oid\ [a])]])$

**definition**  $OclAsType_{Person}\text{-}\mathfrak{A} = (\lambda u. case\ u\ of\ in_{Person}\ p \Rightarrow [p]$   
 $\quad | in_{OclAny}\ (mk_{OclAny}\ oid\ [a]) \Rightarrow [mk_{Person}\ oid\ a]$   
 $\quad | - \Rightarrow None)$

**defs (overloaded)**  $OclAsType_{Person}\text{-}OclAny$ :  
 $(X::OclAny) .oclAsType(Person) \equiv$   
 $(\lambda \tau. case\ X\ \tau\ of$   
 $\quad \perp \Rightarrow invalid\ \tau$   
 $\quad | [\perp] \Rightarrow null\ \tau$   
 $\quad | [[mk_{OclAny}\ oid\ \perp]] \Rightarrow invalid\ \tau\ (*\ down\text{-}cast\ exception\ *)$   
 $\quad | [[mk_{OclAny}\ oid\ [a]]] \Rightarrow [[mk_{Person}\ oid\ a]])$

**defs (overloaded)**  $OclAsType_{Person}\text{-}Person$ :  
 $(X::Person) .oclAsType(Person) \equiv X$

**lemmas**  $[simp] =$   
 $OclAsType_{OclAny}\text{-}OclAny$   
 $OclAsType_{Person}\text{-}Person$

##### Context Passing

**lemma**  $cp\text{-}OclAsType_{OclAny}\text{-}Person\text{-}Person$ :  $cp\ P \Longrightarrow cp(\lambda X. (P\ (X::Person)::Person)$   
 $.oclAsType(OclAny))$   
 $\langle proof \rangle$



**lemma** *cp-OclAsTypeOclAny-OclAny-OclAny*:  $cp\ P \implies cp(\lambda X. (P\ (X::OclAny)::OclAny))$   
*.oclAsType(OclAny)*

*<proof>*

**lemma** *cp-OclAsTypePerson-Person-Person*:  $cp\ P \implies cp(\lambda X. (P\ (X::Person)::Person))$   
*.oclAsType(Person)*

*<proof>*

**lemma** *cp-OclAsTypePerson-OclAny-OclAny*:  $cp\ P \implies cp(\lambda X. (P\ (X::OclAny)::OclAny))$   
*.oclAsType(Person)*

*<proof>*

**lemma** *cp-OclAsTypeOclAny-Person-OclAny*:  $cp\ P \implies cp(\lambda X. (P\ (X::Person)::OclAny))$   
*.oclAsType(OclAny)*

*<proof>*

**lemma** *cp-OclAsTypeOclAny-OclAny-Person*:  $cp\ P \implies cp(\lambda X. (P\ (X::OclAny)::Person))$   
*.oclAsType(OclAny)*

*<proof>*

**lemma** *cp-OclAsTypePerson-Person-OclAny*:  $cp\ P \implies cp(\lambda X. (P\ (X::Person)::OclAny))$   
*.oclAsType(Person)*

*<proof>*

**lemma** *cp-OclAsTypePerson-OclAny-Person*:  $cp\ P \implies cp(\lambda X. (P\ (X::OclAny)::Person))$   
*.oclAsType(Person)*

*<proof>*

**lemmas** *[simp]* =

*cp-OclAsTypeOclAny-Person-Person*  
*cp-OclAsTypeOclAny-OclAny-OclAny*  
*cp-OclAsTypePerson-Person-Person*  
*cp-OclAsTypePerson-OclAny-OclAny*

*cp-OclAsTypeOclAny-Person-OclAny*  
*cp-OclAsTypeOclAny-OclAny-Person*  
*cp-OclAsTypePerson-Person-OclAny*  
*cp-OclAsTypePerson-OclAny-Person*

## Execution with Invalid or Null as Argument

**lemma** *OclAsTypeOclAny-OclAny-strict* :  $(invalid::OclAny) .oclAsType(OclAny) = invalid$   
*<proof>*

**lemma** *OclAsTypeOclAny-OclAny-nullstrict* :  $(null::OclAny) .oclAsType(OclAny) = null$   
*<proof>*

**lemma** *OclAsTypeOclAny-Person-strict[simp]* :  $(invalid::Person) .oclAsType(OclAny) = invalid$   
*<proof>*

**lemma** *OclAsTypeOclAny-Person-nullstrict[simp]* :  $(null::Person) .oclAsType(OclAny) = null$   
*<proof>*

**lemma** *OclAsTypePerson-OclAny-strict[simp]* :  $(invalid::OclAny) .oclAsType(Person) = invalid$

*<proof>*

**lemma** *OclAsType<sub>Person</sub>-OclAny-nullstrict*[simp] : (null::OclAny) .oclasType(Person) = null  
*<proof>*

**lemma** *OclAsType<sub>Person</sub>-Person-strict* : (invalid::Person) .oclasType(Person) = invalid  
*<proof>*

**lemma** *OclAsType<sub>Person</sub>-Person-nullstrict* : (null::Person) .oclasType(Person) = null  
*<proof>*

### 6.1.5. OclIsTypeOf

#### Definition

**consts** *OclIsTypeOf<sub>OclAny</sub>* :: 'α ⇒ Boolean ((-).oclasTypeOf'(OclAny'))  
**consts** *OclIsTypeOf<sub>Person</sub>* :: 'α ⇒ Boolean ((-).oclasTypeOf'(Person'))

**defs** (overloaded) *OclIsTypeOf<sub>OclAny</sub>-OclAny*:  
(X::OclAny) .oclasTypeOf(OclAny) ≡  
(λτ. case X τ of  
 ⊥ ⇒ invalid τ  
 | [⊥] ⇒ true τ (\* invalid ?? \*)  
 | [[mk<sub>OclAny</sub> oid ⊥]] ⇒ true τ  
 | [[mk<sub>OclAny</sub> oid [-]]] ⇒ false τ)

**defs** (overloaded) *OclIsTypeOf<sub>OclAny</sub>-Person*:  
(X::Person) .oclasTypeOf(OclAny) ≡  
(λτ. case X τ of  
 ⊥ ⇒ invalid τ  
 | [⊥] ⇒ true τ (\* invalid ?? \*)  
 | [[-]] ⇒ false τ)

**defs** (overloaded) *OclIsTypeOf<sub>Person</sub>-OclAny*:  
(X::OclAny) .oclasTypeOf(Person) ≡  
(λτ. case X τ of  
 ⊥ ⇒ invalid τ  
 | [⊥] ⇒ true τ  
 | [[mk<sub>OclAny</sub> oid ⊥]] ⇒ false τ  
 | [[mk<sub>OclAny</sub> oid [-]]] ⇒ true τ)

**defs** (overloaded) *OclIsTypeOf<sub>Person</sub>-Person*:  
(X::Person) .oclasTypeOf(Person) ≡  
(λτ. case X τ of  
 ⊥ ⇒ invalid τ  
 | - ⇒ true τ)

## Context Passing

**lemma**  $cp\text{-}OclIsTypeOf_{OclAny}\text{-}Person\text{-}Person:$   $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::Person)::Person).oclIsTypeOf(OclAny))$   
 $\langle proof \rangle$

**lemma**  $cp\text{-}OclIsTypeOf_{OclAny}\text{-}OclAny\text{-}OclAny:$   $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::OclAny)::OclAny).oclIsTypeOf(OclAny))$   
 $\langle proof \rangle$

**lemma**  $cp\text{-}OclIsTypeOf_{Person}\text{-}Person\text{-}Person:$   $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::Person)::Person).oclIsTypeOf(Person))$   
 $\langle proof \rangle$

**lemma**  $cp\text{-}OclIsTypeOf_{Person}\text{-}OclAny\text{-}OclAny:$   $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::OclAny)::OclAny).oclIsTypeOf(Person))$   
 $\langle proof \rangle$

**lemma**  $cp\text{-}OclIsTypeOf_{OclAny}\text{-}Person\text{-}OclAny:$   $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::Person)::OclAny).oclIsTypeOf(OclAny))$   
 $\langle proof \rangle$

**lemma**  $cp\text{-}OclIsTypeOf_{OclAny}\text{-}OclAny\text{-}Person:$   $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::OclAny)::Person).oclIsTypeOf(OclAny))$   
 $\langle proof \rangle$

**lemma**  $cp\text{-}OclIsTypeOf_{Person}\text{-}Person\text{-}OclAny:$   $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::Person)::OclAny).oclIsTypeOf(Person))$   
 $\langle proof \rangle$

**lemma**  $cp\text{-}OclIsTypeOf_{Person}\text{-}OclAny\text{-}Person:$   $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::OclAny)::Person).oclIsTypeOf(Person))$   
 $\langle proof \rangle$

**lemmas**  $[simp] =$

$cp\text{-}OclIsTypeOf_{OclAny}\text{-}Person\text{-}Person$   
 $cp\text{-}OclIsTypeOf_{OclAny}\text{-}OclAny\text{-}OclAny$   
 $cp\text{-}OclIsTypeOf_{Person}\text{-}Person\text{-}Person$   
 $cp\text{-}OclIsTypeOf_{Person}\text{-}OclAny\text{-}OclAny$

$cp\text{-}OclIsTypeOf_{OclAny}\text{-}Person\text{-}OclAny$   
 $cp\text{-}OclIsTypeOf_{OclAny}\text{-}OclAny\text{-}Person$   
 $cp\text{-}OclIsTypeOf_{Person}\text{-}Person\text{-}OclAny$   
 $cp\text{-}OclIsTypeOf_{Person}\text{-}OclAny\text{-}Person$

## Execution with Invalid or Null as Argument

**lemma**  $OclIsTypeOf_{OclAny}\text{-}OclAny\text{-}strict1[simp]:$   
 $(invalid::OclAny).oclIsTypeOf(OclAny) = invalid$   
 $\langle proof \rangle$

**lemma**  $OclIsTypeOf_{OclAny}\text{-}OclAny\text{-}strict2[simp]:$   
 $(null::OclAny).oclIsTypeOf(OclAny) = true$   
 $\langle proof \rangle$

**lemma**  $OclIsTypeOf_{OclAny}\text{-}Person\text{-}strict1[simp]:$   
 $(invalid::Person).oclIsTypeOf(OclAny) = invalid$

$\langle proof \rangle$   
**lemma** *OclIsTypeOf OclAny-Person-strict2*[simp]:  
 $(null::Person) .oclIsTypeOf(OclAny) = true$   
 $\langle proof \rangle$   
**lemma** *OclIsTypeOf Person-OclAny-strict1*[simp]:  
 $(invalid::OclAny) .oclIsTypeOf(Person) = invalid$   
 $\langle proof \rangle$   
**lemma** *OclIsTypeOf Person-OclAny-strict2*[simp]:  
 $(null::OclAny) .oclIsTypeOf(Person) = true$   
 $\langle proof \rangle$   
**lemma** *OclIsTypeOf Person-Person-strict1*[simp]:  
 $(invalid::Person) .oclIsTypeOf(Person) = invalid$   
 $\langle proof \rangle$   
**lemma** *OclIsTypeOf Person-Person-strict2*[simp]:  
 $(null::Person) .oclIsTypeOf(Person) = true$   
 $\langle proof \rangle$

## Up Down Casting

**lemma** *actualType-larger-staticType*:  
**assumes** *isdef*:  $\tau \models (\delta X)$   
**shows**  $\tau \models (X::Person) .oclIsTypeOf(OclAny) \triangleq false$   
 $\langle proof \rangle$

**lemma** *down-cast-type*:  
**assumes** *isOclAny*:  $\tau \models (X::OclAny) .oclIsTypeOf(OclAny)$   
**and** *non-null*:  $\tau \models (\delta X)$   
**shows**  $\tau \models (X .oclAsType(Person)) \triangleq invalid$   
 $\langle proof \rangle$

**lemma** *down-cast-type'*:  
**assumes** *isOclAny*:  $\tau \models (X::OclAny) .oclIsTypeOf(OclAny)$   
**and** *non-null*:  $\tau \models (\delta X)$   
**shows**  $\tau \models not (v (X .oclAsType(Person)))$   
 $\langle proof \rangle$

**lemma** *up-down-cast* :  
**assumes** *isdef*:  $\tau \models (\delta X)$   
**shows**  $\tau \models ((X::Person) .oclAsType(OclAny) .oclAsType(Person)) \triangleq X$   
 $\langle proof \rangle$

**lemma** *up-down-cast-Person-OclAny-Person* [simp]:  
**shows**  $((X::Person) .oclAsType(OclAny) .oclAsType(Person)) = X$   
 $\langle proof \rangle$

**lemma** *up-down-cast-Person-OclAny-Person'*: **assumes**  $\tau \models v X$   
**shows**  $\tau \models (((X :: Person) .oclAsType(OclAny) .oclAsType(Person))) \doteq X$   
 $\langle proof \rangle$

**lemma** *up-down-cast-Person-OclAny-Person''*: **assumes**  $\tau \models v (X :: \text{Person})$   
**shows**  $\tau \models (X . \text{oclIsTypeOf}(\text{Person}) \text{ implies } (X . \text{oclAsType}(\text{OclAny}) . \text{oclAsType}(\text{Person})) \doteq X)$   
 $\langle \text{proof} \rangle$

## 6.1.6. OclIsKindOf

### Definition

**consts**  $\text{OclIsKindOf}_{\text{OclAny}} :: 'a \Rightarrow \text{Boolean } ((-).\text{oclIsKindOf}'(\text{OclAny}'))$   
**consts**  $\text{OclIsKindOf}_{\text{Person}} :: 'a \Rightarrow \text{Boolean } ((-).\text{oclIsKindOf}'(\text{Person}'))$

**defs (overloaded)**  $\text{OclIsKindOf}_{\text{OclAny-OclAny}}$ :  
 $(X :: \text{OclAny}) . \text{oclIsKindOf}(\text{OclAny}) \equiv$   
 $(\lambda\tau. \text{case } X \ \tau \ \text{of}$   
 $\quad \perp \Rightarrow \text{invalid } \tau$   
 $\quad | \_ \Rightarrow \text{true } \tau)$

**defs (overloaded)**  $\text{OclIsKindOf}_{\text{OclAny-Person}}$ :  
 $(X :: \text{Person}) . \text{oclIsKindOf}(\text{OclAny}) \equiv$   
 $(\lambda\tau. \text{case } X \ \tau \ \text{of}$   
 $\quad \perp \Rightarrow \text{invalid } \tau$   
 $\quad | \_ \Rightarrow \text{true } \tau)$

**defs (overloaded)**  $\text{OclIsKindOf}_{\text{Person-OclAny}}$ :  
 $(X :: \text{OclAny}) . \text{oclIsKindOf}(\text{Person}) \equiv$   
 $(\lambda\tau. \text{case } X \ \tau \ \text{of}$   
 $\quad \perp \Rightarrow \text{invalid } \tau$   
 $\quad | [\perp] \Rightarrow \text{true } \tau$   
 $\quad | [[\text{mk}_{\text{OclAny}} \ \text{oid } \perp]] \Rightarrow \text{false } \tau$   
 $\quad | [[\text{mk}_{\text{OclAny}} \ \text{oid } \_]] \Rightarrow \text{true } \tau)$

**defs (overloaded)**  $\text{OclIsKindOf}_{\text{Person-Person}}$ :  
 $(X :: \text{Person}) . \text{oclIsKindOf}(\text{Person}) \equiv$   
 $(\lambda\tau. \text{case } X \ \tau \ \text{of}$   
 $\quad \perp \Rightarrow \text{invalid } \tau$   
 $\quad | \_ \Rightarrow \text{true } \tau)$

### Context Passing

**lemma**  $\text{cp-OclIsKindOf}_{\text{OclAny-Person-Person}}$ :  $\text{cp} \quad P \quad \Rightarrow$   
 $\text{cp}(\lambda X.(P(X :: \text{Person}) :: \text{Person}). \text{oclIsKindOf}(\text{OclAny}))$   
 $\langle \text{proof} \rangle$

**lemma**  $\text{cp-OclIsKindOf}_{\text{OclAny-OclAny-OclAny}}$ :  $\text{cp} \quad P \quad \Rightarrow$   
 $\text{cp}(\lambda X.(P(X :: \text{OclAny}) :: \text{OclAny}). \text{oclIsKindOf}(\text{OclAny}))$   
 $\langle \text{proof} \rangle$

**lemma**  $\text{cp-OclIsKindOf}_{\text{Person-Person-Person}}$ :  $\text{cp} \quad P \quad \Rightarrow$   
 $\text{cp}(\lambda X.(P(X :: \text{Person}) :: \text{Person}). \text{oclIsKindOf}(\text{Person}))$   
 $\langle \text{proof} \rangle$

**lemma**  $cp\text{-}OclIsKindOf_{Person-OclAny-OclAny}$ :  $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::OclAny)::OclAny).oclIsKindOf(Person))$   
 $\langle proof \rangle$

**lemma**  $cp\text{-}OclIsKindOf_{OclAny-Person-OclAny}$ :  $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::Person)::OclAny).oclIsKindOf(OclAny))$   
 $\langle proof \rangle$

**lemma**  $cp\text{-}OclIsKindOf_{OclAny-OclAny-Person}$ :  $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::OclAny)::Person).oclIsKindOf(OclAny))$   
 $\langle proof \rangle$

**lemma**  $cp\text{-}OclIsKindOf_{Person-Person-OclAny}$ :  $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::Person)::OclAny).oclIsKindOf(Person))$   
 $\langle proof \rangle$

**lemma**  $cp\text{-}OclIsKindOf_{Person-OclAny-Person}$ :  $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::OclAny)::Person).oclIsKindOf(Person))$   
 $\langle proof \rangle$

**lemmas**  $[simp]$  =

$cp\text{-}OclIsKindOf_{OclAny-Person-Person}$   
 $cp\text{-}OclIsKindOf_{OclAny-OclAny-OclAny}$   
 $cp\text{-}OclIsKindOf_{Person-Person-Person}$   
 $cp\text{-}OclIsKindOf_{Person-OclAny-OclAny}$

$cp\text{-}OclIsKindOf_{OclAny-Person-OclAny}$   
 $cp\text{-}OclIsKindOf_{OclAny-OclAny-Person}$   
 $cp\text{-}OclIsKindOf_{Person-Person-OclAny}$   
 $cp\text{-}OclIsKindOf_{Person-OclAny-Person}$

## Execution with Invalid or Null as Argument

**lemma**  $OclIsKindOf_{OclAny-OclAny-strict1}$   $[simp]$  :  $(invalid::OclAny).oclIsKindOf(OclAny) =$   
 $invalid$   
 $\langle proof \rangle$

**lemma**  $OclIsKindOf_{OclAny-OclAny-strict2}$   $[simp]$  :  $(null::OclAny).oclIsKindOf(OclAny) =$   
 $true$   
 $\langle proof \rangle$

**lemma**  $OclIsKindOf_{OclAny-Person-strict1}$   $[simp]$  :  $(invalid::Person).oclIsKindOf(OclAny) =$   
 $invalid$   
 $\langle proof \rangle$

**lemma**  $OclIsKindOf_{OclAny-Person-strict2}$   $[simp]$  :  $(null::Person).oclIsKindOf(OclAny) = true$   
 $\langle proof \rangle$

**lemma**  $OclIsKindOf_{Person-OclAny-strict1}$   $[simp]$ :  $(invalid::OclAny).oclIsKindOf(Person) =$   
 $invalid$   
 $\langle proof \rangle$

**lemma**  $OclIsKindOf_{Person-OclAny-strict2}[simp]: (null::OclAny) .oclIsKindOf(Person) = true$   
 ⟨proof⟩

**lemma**  $OclIsKindOf_{Person-Person-strict1}[simp]: (invalid::Person) .oclIsKindOf(Person) = invalid$   
 ⟨proof⟩

**lemma**  $OclIsKindOf_{Person-Person-strict2}[simp]: (null::Person) .oclIsKindOf(Person) = true$   
 ⟨proof⟩

## Up Down Casting

**lemma**  $actualKind-larger-staticKind:$

**assumes**  $isdef: \tau \models (\delta X)$

**shows**  $\tau \models (X::Person) .oclIsKindOf(OclAny) \triangleq true$   
 ⟨proof⟩

**lemma**  $down-cast-kind:$

**assumes**  $isOclAny: \neg \tau \models (X::OclAny) .oclIsKindOf(Person)$

**and**  $non-null: \tau \models (\delta X)$

**shows**  $\tau \models (X .oclAsType(Person)) \triangleq invalid$   
 ⟨proof⟩

### 6.1.7. 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.”

**definition**  $Person \equiv OclAsType_{Person-\mathfrak{A}}$

**definition**  $OclAny \equiv OclAsType_{OclAny-\mathfrak{A}}$

**lemmas**  $[simp] = Person-def\ OclAny-def$

**lemma**  $OclAllInstances-generic_{OclAny-exec}: OclAllInstances-generic\ pre-post\ OclAny =$   
 $(\lambda\tau. Abs-Set-0 \llbracket Some\ 'OclAny'\ ran\ (heap\ (pre-post\ \tau)) \rrbracket)$   
 ⟨proof⟩

**lemma**  $OclAllInstances-at-post_{OclAny-exec}: OclAny .allInstances() =$   
 $(\lambda\tau. Abs-Set-0 \llbracket Some\ 'OclAny'\ ran\ (heap\ (snd\ \tau)) \rrbracket)$   
 ⟨proof⟩

**lemma**  $OclAllInstances-at-pre_{OclAny-exec}: OclAny .allInstances@pre() =$   
 $(\lambda\tau. Abs-Set-0 \llbracket Some\ 'OclAny'\ ran\ (heap\ (fst\ \tau)) \rrbracket)$   
 ⟨proof⟩

## OclIsTypeOf

**lemma**  $OclAny-allInstances-generic-oclIsTypeOf_{OclAny}1:$

**assumes**  $[simp]: \bigwedge x. pre-post\ (x, x) = x$

**shows**  $\exists \tau. (\tau \models ((\text{OclAllInstances-generic } \text{pre-post } \text{OclAny}) \rightarrow \text{forAll}(X|X \text{ .oclIsTypeOf}(\text{OclAny}))))$   
 ⟨proof⟩

**lemma** *OclAny-allInstances-at-post-oclIsTypeOf<sub>OclAny</sub>1*:  
 $\exists \tau. (\tau \models (\text{OclAny .allInstances}() \rightarrow \text{forAll}(X|X \text{ .oclIsTypeOf}(\text{OclAny}))))$   
 ⟨proof⟩

**lemma** *OclAny-allInstances-at-pre-oclIsTypeOf<sub>OclAny</sub>1*:  
 $\exists \tau. (\tau \models (\text{OclAny .allInstances@pre}() \rightarrow \text{forAll}(X|X \text{ .oclIsTypeOf}(\text{OclAny}))))$   
 ⟨proof⟩

**lemma** *OclAny-allInstances-generic-oclIsTypeOf<sub>OclAny</sub>2*:  
**assumes** [simp]:  $\bigwedge x. \text{pre-post } (x, x) = x$   
**shows**  $\exists \tau. (\tau \models \text{not } ((\text{OclAllInstances-generic } \text{pre-post } \text{OclAny}) \rightarrow \text{forAll}(X|X \text{ .oclIsTypeOf}(\text{OclAny}))))$   
 ⟨proof⟩

**lemma** *OclAny-allInstances-at-post-oclIsTypeOf<sub>OclAny</sub>2*:  
 $\exists \tau. (\tau \models \text{not } (\text{OclAny .allInstances}() \rightarrow \text{forAll}(X|X \text{ .oclIsTypeOf}(\text{OclAny}))))$   
 ⟨proof⟩

**lemma** *OclAny-allInstances-at-pre-oclIsTypeOf<sub>OclAny</sub>2*:  
 $\exists \tau. (\tau \models \text{not } (\text{OclAny .allInstances@pre}() \rightarrow \text{forAll}(X|X \text{ .oclIsTypeOf}(\text{OclAny}))))$   
 ⟨proof⟩

**lemma** *Person-allInstances-generic-oclIsTypeOf<sub>Person</sub>*:  
 $\tau \models ((\text{OclAllInstances-generic } \text{pre-post } \text{Person}) \rightarrow \text{forAll}(X|X \text{ .oclIsTypeOf}(\text{Person})))$   
 ⟨proof⟩

**lemma** *Person-allInstances-at-post-oclIsTypeOf<sub>Person</sub>*:  
 $\tau \models (\text{Person .allInstances}() \rightarrow \text{forAll}(X|X \text{ .oclIsTypeOf}(\text{Person})))$   
 ⟨proof⟩

**lemma** *Person-allInstances-at-pre-oclIsTypeOf<sub>Person</sub>*:  
 $\tau \models (\text{Person .allInstances@pre}() \rightarrow \text{forAll}(X|X \text{ .oclIsTypeOf}(\text{Person})))$   
 ⟨proof⟩

## OclsKindOf

**lemma** *OclAny-allInstances-generic-oclIsKindOf<sub>OclAny</sub>*:  
 $\tau \models ((\text{OclAllInstances-generic } \text{pre-post } \text{OclAny}) \rightarrow \text{forAll}(X|X \text{ .oclIsKindOf}(\text{OclAny})))$   
 ⟨proof⟩

**lemma** *OclAny-allInstances-at-post-oclIsKindOf<sub>OclAny</sub>*:  
 $\tau \models (\text{OclAny .allInstances}() \rightarrow \text{forAll}(X|X \text{ .oclIsKindOf}(\text{OclAny})))$   
 ⟨proof⟩

**lemma** *OclAny-allInstances-at-pre-oclIsKindOf<sub>OclAny</sub>*:



$\tau \models (\text{OclAny} .\text{allInstances}@pre() \rightarrow \text{forAll}(X|X .\text{oclIsKindOf}(\text{OclAny})))$   
 $\langle \text{proof} \rangle$

**lemma** *Person-allInstances-generic-oclIsKindOf OclAny:*  
 $\tau \models ((\text{OclAllInstances-generic pre-post Person}) \rightarrow \text{forAll}(X|X .\text{oclIsKindOf}(\text{OclAny})))$   
 $\langle \text{proof} \rangle$

**lemma** *Person-allInstances-at-post-oclIsKindOf OclAny:*  
 $\tau \models (\text{Person} .\text{allInstances}() \rightarrow \text{forAll}(X|X .\text{oclIsKindOf}(\text{OclAny})))$   
 $\langle \text{proof} \rangle$

**lemma** *Person-allInstances-at-pre-oclIsKindOf OclAny:*  
 $\tau \models (\text{Person} .\text{allInstances}@pre() \rightarrow \text{forAll}(X|X .\text{oclIsKindOf}(\text{OclAny})))$   
 $\langle \text{proof} \rangle$

**lemma** *Person-allInstances-generic-oclIsKindOf Person:*  
 $\tau \models ((\text{OclAllInstances-generic pre-post Person}) \rightarrow \text{forAll}(X|X .\text{oclIsKindOf}(\text{Person})))$   
 $\langle \text{proof} \rangle$

**lemma** *Person-allInstances-at-post-oclIsKindOf Person:*  
 $\tau \models (\text{Person} .\text{allInstances}() \rightarrow \text{forAll}(X|X .\text{oclIsKindOf}(\text{Person})))$   
 $\langle \text{proof} \rangle$

**lemma** *Person-allInstances-at-pre-oclIsKindOf Person:*  
 $\tau \models (\text{Person} .\text{allInstances}@pre() \rightarrow \text{forAll}(X|X .\text{oclIsKindOf}(\text{Person})))$   
 $\langle \text{proof} \rangle$

### 6.1.8. The Accessors (any, boss, salary)

Should be generated entirely from a class-diagram.

#### 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 `Employee_DesignModel.UMLPart`, where we stored an oid inside the class as “pointer.”

**definition**  $\text{oid}_{\text{Person}}\text{BOSS} :: \text{oid}$  **where**  $\text{oid}_{\text{Person}}\text{BOSS} = 10$

From there on, we can already define an empty state which must contain for  $\text{oid}_{\text{Person}}\text{BOSS}$  the empty relation (encoded as association list, since there are associations with a Sequence-like structure).

**definition**  $\text{eval-extract} :: (\mathfrak{A}, ('a::\text{object}) \text{option option}) \text{val}$   
 $\Rightarrow (\text{oid} \Rightarrow (\mathfrak{A}, 'c::\text{null}) \text{val})$   
 $\Rightarrow (\mathfrak{A}, 'c::\text{null}) \text{val}$

**where**  $\text{eval-extract} X f = (\lambda \tau . \text{case } X \tau \text{ of}$   
 $\quad \perp \Rightarrow \text{invalid } \tau \quad (* \text{exception propagation} *)$   
 $\quad | \lfloor \perp \rfloor \Rightarrow \text{invalid } \tau \quad (* \text{dereferencing null pointer} *)$

| [[ *obj* ]]  $\Rightarrow f$  (*oid-of obj*)  $\tau$ )

**definition** *choose<sub>2-1</sub>* = *fst*

**definition** *choose<sub>2-2</sub>* = *snd*

**definition** *choose<sub>3-1</sub>* = *fst*

**definition** *choose<sub>3-2</sub>* = *fst o snd*

**definition** *choose<sub>3-3</sub>* = *snd o snd*

**definition** *deref-assocs<sub>2</sub>* :: ('*A* state  $\times$  '*A* state  $\Rightarrow$  '*A* state)  
 $\Rightarrow$  (*oid*  $\times$  *oid*  $\Rightarrow$  *oid*  $\times$  *oid*)  
 $\Rightarrow$  *oid*  
 $\Rightarrow$  (*oid list*  $\Rightarrow$  *oid*  $\Rightarrow$  ('*A*, '*f*)*val*)  
 $\Rightarrow$  *oid*  
 $\Rightarrow$  ('*A*, '*f*::*null*)*val*

**where** *deref-assocs<sub>2</sub>* *pre-post to-from assoc-oid f oid* =  
 $(\lambda \tau. \text{case } (\text{assocs}_2 \text{ (pre-post } \tau)) \text{ assoc-oid of}$   
 $\quad [ S ] \Rightarrow f (\text{map } (\text{choose}_{2-2} \circ \text{to-from})$   
 $\quad \quad (\text{filter } (\lambda p. \text{choose}_{2-1}(\text{to-from } p)=\text{oid}) S))$   
 $\quad \quad \text{oid } \tau$   
 $\quad | - \Rightarrow \text{invalid } \tau)$

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** *switch<sub>2-1</sub>* = *id*

**definition** *switch<sub>2-2</sub>* =  $(\lambda(x,y). (y,x))$

**definition** *switch<sub>3-1</sub>* = *id*

**definition** *switch<sub>3-2</sub>* =  $(\lambda(x,y,z). (x,z,y))$

**definition** *switch<sub>3-3</sub>* =  $(\lambda(x,y,z). (y,x,z))$

**definition** *switch<sub>3-4</sub>* =  $(\lambda(x,y,z). (y,z,x))$

**definition** *switch<sub>3-5</sub>* =  $(\lambda(x,y,z). (z,x,y))$

**definition** *switch<sub>3-6</sub>* =  $(\lambda(x,y,z). (z,y,x))$

**definition** *select-object* :: (('*A*, '*b*::*null*)*val*)  
 $\Rightarrow$  (('*A*, '*b*)*val*  $\Rightarrow$  ('*A*, '*c*)*val*  $\Rightarrow$  ('*A*, '*b*)*val*)  
 $\Rightarrow$  (('*A*, '*b*)*val*  $\Rightarrow$  ('*A*, '*d*)*val*)  
 $\Rightarrow$  (*oid*  $\Rightarrow$  ('*A*, '*c*::*null*)*val*)  
 $\Rightarrow$  *oid list*  
 $\Rightarrow$  *oid*  
 $\Rightarrow$  ('*A*, '*d*)*val*

**where** *select-object* *mt incl smash deref l oid* = *smash(foldl incl mt (map deref l))*  
 (\* *smash* returns *null* with *mt* in input (in this case, object contains *null* pointer) \*)

The continuation *f* is usually instantiated with a smashing function which is either the identity *id* or, for 0..1 cardinalities of associations, the *OclANY*-selector which also handles the *null*-cases appropriately. A standard use-case for this combinator is for example:

**term** (*select-object mtSet OclIncluding OclANY f l oid*)::('*A*, '*a*::*null*)*val*

**definition**  $deref-oid_{Person} :: (\mathfrak{A} \text{ state} \times \mathfrak{A} \text{ state} \Rightarrow \mathfrak{A} \text{ state})$   
 $\Rightarrow (type_{Person} \Rightarrow (\mathfrak{A}, 'c::null)val)$   
 $\Rightarrow oid$   
 $\Rightarrow (\mathfrak{A}, 'c::null)val$   
**where**  $deref-oid_{Person} \text{ fst-snd } f \text{ oid} = (\lambda\tau. \text{ case } (heap \text{ (fst-snd } \tau)) \text{ oid of}$   
 $\quad | \text{ in}_{Person} \text{ obj } \Rightarrow f \text{ obj } \tau$   
 $\quad | - \Rightarrow \text{ invalid } \tau)$

**definition**  $deref-oid_{OclAny} :: (\mathfrak{A} \text{ state} \times \mathfrak{A} \text{ state} \Rightarrow \mathfrak{A} \text{ state})$   
 $\Rightarrow (type_{OclAny} \Rightarrow (\mathfrak{A}, 'c::null)val)$   
 $\Rightarrow oid$   
 $\Rightarrow (\mathfrak{A}, 'c::null)val$   
**where**  $deref-oid_{OclAny} \text{ fst-snd } f \text{ oid} = (\lambda\tau. \text{ case } (heap \text{ (fst-snd } \tau)) \text{ oid of}$   
 $\quad | \text{ in}_{OclAny} \text{ obj } \Rightarrow f \text{ obj } \tau$   
 $\quad | - \Rightarrow \text{ invalid } \tau)$

pointer undefined in state or not referencing a type conform object representation

**definition**  $select_{OclAny} \mathcal{ANY} f = (\lambda X. \text{ case } X \text{ of}$   
 $\quad (mk_{OclAny} - \perp) \Rightarrow \text{ null}$   
 $\quad | (mk_{OclAny} - [any]) \Rightarrow f (\lambda x -. [[x]]) \text{ any})$

**definition**  $select_{Person} \mathcal{BOSS} f = \text{ select-object mtSet OclIncluding OclANY } (f (\lambda x -. [[x]]))$

**definition**  $select_{Person} \mathcal{SALARY} f = (\lambda X. \text{ case } X \text{ of}$   
 $\quad (mk_{Person} - \perp) \Rightarrow \text{ null}$   
 $\quad | (mk_{Person} - [salary]) \Rightarrow f (\lambda x -. [[x]]) \text{ salary})$

**definition**  $deref-assocs_2 \mathcal{BOSS} \text{ fst-snd } f = (\lambda mk_{Person} \text{ oid} - \Rightarrow$   
 $\text{ deref-assocs}_2 \text{ fst-snd switch}_2\text{-1 } oid_{Person} \mathcal{BOSS} f \text{ oid})$

**definition**  $\text{ in-pre-state} = \text{ fst}$

**definition**  $\text{ in-post-state} = \text{ snd}$

**definition**  $\text{ reconst-basetype} = (\lambda \text{ convert } x. \text{ convert } x)$

**definition**  $\text{ dot}_{OclAny} \mathcal{ANY} :: OclAny \Rightarrow - \text{ ((1(-).any) 50)}$   
**where**  $(X).any = \text{ eval-extract } X$   
 $(\text{ deref-oid}_{OclAny} \text{ in-post-state}$   
 $\quad (\text{ select}_{OclAny} \mathcal{ANY}$   
 $\quad \text{ reconst-basetype}))$

**definition**  $\text{ dot}_{Person} \mathcal{BOSS} :: Person \Rightarrow Person \text{ ((1(-).boss) 50)}$   
**where**  $(X).boss = \text{ eval-extract } X$   
 $(\text{ deref-oid}_{Person} \text{ in-post-state})$

$(\text{deref-assocs}_2 \text{BOSS in-post-state}$   
 $(\text{select}_{\text{Person}} \text{BOSS}$   
 $(\text{deref-oid}_{\text{Person}} \text{in-post-state}))))$

**definition**  $\text{dot}_{\text{Person}} \text{SALARY} :: \text{Person} \Rightarrow \text{Integer} ((1(-).\text{salary}) 50)$   
**where**  $(X).\text{salary} = \text{eval-extract } X$   
 $(\text{deref-oid}_{\text{Person}} \text{in-post-state}$   
 $(\text{select}_{\text{Person}} \text{SALARY}$   
 $\text{reconst-basetype}))$

**definition**  $\text{dot}_{\text{OclAny}} \text{ANY-at-pre} :: \text{OclAny} \Rightarrow - ((1(-).\text{any@pre}) 50)$   
**where**  $(X).\text{any@pre} = \text{eval-extract } X$   
 $(\text{deref-oid}_{\text{OclAny}} \text{in-pre-state}$   
 $(\text{select}_{\text{OclAny}} \text{ANY}$   
 $\text{reconst-basetype}))$

**definition**  $\text{dot}_{\text{Person}} \text{BOSS-at-pre} :: \text{Person} \Rightarrow \text{Person} ((1(-).\text{boss@pre}) 50)$   
**where**  $(X).\text{boss@pre} = \text{eval-extract } X$   
 $(\text{deref-oid}_{\text{Person}} \text{in-pre-state}$   
 $(\text{deref-assocs}_2 \text{BOSS in-pre-state}$   
 $(\text{select}_{\text{Person}} \text{BOSS}$   
 $(\text{deref-oid}_{\text{Person}} \text{in-pre-state}))))$

**definition**  $\text{dot}_{\text{Person}} \text{SALARY-at-pre} :: \text{Person} \Rightarrow \text{Integer} ((1(-).\text{salary@pre}) 50)$   
**where**  $(X).\text{salary@pre} = \text{eval-extract } X$   
 $(\text{deref-oid}_{\text{Person}} \text{in-pre-state}$   
 $(\text{select}_{\text{Person}} \text{SALARY}$   
 $\text{reconst-basetype}))$

**lemmas**  $[\text{simp}] =$   
 $\text{dot}_{\text{OclAny}} \text{ANY-def}$   
 $\text{dot}_{\text{Person}} \text{BOSS-def}$   
 $\text{dot}_{\text{Person}} \text{SALARY-def}$   
 $\text{dot}_{\text{OclAny}} \text{ANY-at-pre-def}$   
 $\text{dot}_{\text{Person}} \text{BOSS-at-pre-def}$   
 $\text{dot}_{\text{Person}} \text{SALARY-at-pre-def}$

## Context Passing

**lemmas**  $[\text{simp}] = \text{eval-extract-def}$

**lemma**  $\text{cp-dot}_{\text{OclAny}} \text{ANY}: ((X).\text{any}) \tau = ((\lambda-. X \tau).\text{any}) \tau \langle \text{proof} \rangle$

**lemma**  $\text{cp-dot}_{\text{Person}} \text{BOSS}: ((X).\text{boss}) \tau = ((\lambda-. X \tau).\text{boss}) \tau \langle \text{proof} \rangle$

**lemma**  $\text{cp-dot}_{\text{Person}} \text{SALARY}: ((X).\text{salary}) \tau = ((\lambda-. X \tau).\text{salary}) \tau \langle \text{proof} \rangle$

**lemma**  $\text{cp-dot}_{\text{OclAny}} \text{ANY-at-pre}: ((X).\text{any@pre}) \tau = ((\lambda-. X \tau).\text{any@pre}) \tau \langle \text{proof} \rangle$

**lemma**  $\text{cp-dot}_{\text{Person}} \text{BOSS-at-pre}: ((X).\text{boss@pre}) \tau = ((\lambda-. X \tau).\text{boss@pre}) \tau \langle \text{proof} \rangle$

**lemma**  $\text{cp-dot}_{\text{Person}} \text{SALARY-at-pre}: ((X).\text{salary@pre}) \tau = ((\lambda-. X \tau).\text{salary@pre}) \tau \langle \text{proof} \rangle$

**lemmas**  $cp\text{-}dot_{OclAny}AN\mathcal{Y}\text{-}I$  [*simp*, *intro!*]=  
 $cp\text{-}dot_{OclAny}AN\mathcal{Y}[THEN\ allI[THEN\ allI],$   
*of*  $\lambda X \cdot X \lambda \cdot \tau. \tau, THEN\ cpI1]$

**lemmas**  $cp\text{-}dot_{OclAny}AN\mathcal{Y}\text{-}at\text{-}pre\text{-}I$  [*simp*, *intro!*]=  
 $cp\text{-}dot_{OclAny}AN\mathcal{Y}\text{-}at\text{-}pre[THEN\ allI[THEN\ allI],$   
*of*  $\lambda X \cdot X \lambda \cdot \tau. \tau, THEN\ cpI1]$

**lemmas**  $cp\text{-}dot_{Person}BOSS\text{-}I$  [*simp*, *intro!*]=  
 $cp\text{-}dot_{Person}BOSS[THEN\ allI[THEN\ allI],$   
*of*  $\lambda X \cdot X \lambda \cdot \tau. \tau, THEN\ cpI1]$

**lemmas**  $cp\text{-}dot_{Person}BOSS\text{-}at\text{-}pre\text{-}I$  [*simp*, *intro!*]=  
 $cp\text{-}dot_{Person}BOSS\text{-}at\text{-}pre[THEN\ allI[THEN\ allI],$   
*of*  $\lambda X \cdot X \lambda \cdot \tau. \tau, THEN\ cpI1]$

**lemmas**  $cp\text{-}dot_{Person}SALARY\text{-}I$  [*simp*, *intro!*]=  
 $cp\text{-}dot_{Person}SALARY[THEN\ allI[THEN\ allI],$   
*of*  $\lambda X \cdot X \lambda \cdot \tau. \tau, THEN\ cpI1]$

**lemmas**  $cp\text{-}dot_{Person}SALARY\text{-}at\text{-}pre\text{-}I$  [*simp*, *intro!*]=  
 $cp\text{-}dot_{Person}SALARY\text{-}at\text{-}pre[THEN\ allI[THEN\ allI],$   
*of*  $\lambda X \cdot X \lambda \cdot \tau. \tau, THEN\ cpI1]$

## Execution with Invalid or Null as Argument

**lemma**  $dot_{OclAny}AN\mathcal{Y}\text{-}nullstrict$  [*simp*]:  $(null).any = invalid$   
*<proof>*

**lemma**  $dot_{OclAny}AN\mathcal{Y}\text{-}at\text{-}pre\text{-}nullstrict$  [*simp*]:  $(null).any@pre = invalid$   
*<proof>*

**lemma**  $dot_{OclAny}AN\mathcal{Y}\text{-}strict$  [*simp*]:  $(invalid).any = invalid$   
*<proof>*

**lemma**  $dot_{OclAny}AN\mathcal{Y}\text{-}at\text{-}pre\text{-}strict$  [*simp*]:  $(invalid).any@pre = invalid$   
*<proof>*

**lemma**  $dot_{Person}BOSS\text{-}nullstrict$  [*simp*]:  $(null).boss = invalid$   
*<proof>*

**lemma**  $dot_{Person}BOSS\text{-}at\text{-}pre\text{-}nullstrict$  [*simp*]:  $(null).boss@pre = invalid$   
*<proof>*

**lemma**  $dot_{Person}BOSS\text{-}strict$  [*simp*]:  $(invalid).boss = invalid$   
*<proof>*

**lemma**  $dot_{Person}BOSS\text{-}at\text{-}pre\text{-}strict$  [*simp*]:  $(invalid).boss@pre = invalid$   
*<proof>*

**lemma**  $dot_{Person}SALARY\text{-}nullstrict$  [*simp*]:  $(null).salary = invalid$   
*<proof>*

**lemma**  $dot_{Person}SALARY\text{-}at\text{-}pre\text{-}nullstrict$  [*simp*]:  $(null).salary@pre = invalid$   
*<proof>*

**lemma**  $dot_{Person}SALARY\text{-}strict$  [*simp*]:  $(invalid).salary = invalid$   
*<proof>*

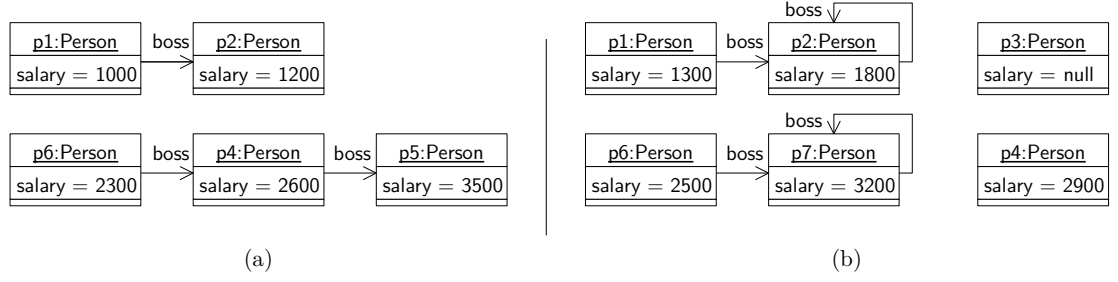


Figure 6.2.: (a) pre-state  $\sigma_1$  and (b) post-state  $\sigma'_1$ .

**lemma**  $\text{dot}_{Person} \text{SALARY-at-pre-strict}$  [simp] :  $(invalid).salary@pre = invalid$   
*<proof>*

### 6.1.9. A Little Infra-structure on Example States

The example we are defining in this section comes from the figure 6.2.

**definition**  $OclInt1000$  (1000) **where**  $OclInt1000 = (\lambda . . [[1000]])$   
**definition**  $OclInt1200$  (1200) **where**  $OclInt1200 = (\lambda . . [[1200]])$   
**definition**  $OclInt1300$  (1300) **where**  $OclInt1300 = (\lambda . . [[1300]])$   
**definition**  $OclInt1800$  (1800) **where**  $OclInt1800 = (\lambda . . [[1800]])$   
**definition**  $OclInt2600$  (2600) **where**  $OclInt2600 = (\lambda . . [[2600]])$   
**definition**  $OclInt2900$  (2900) **where**  $OclInt2900 = (\lambda . . [[2900]])$   
**definition**  $OclInt3200$  (3200) **where**  $OclInt3200 = (\lambda . . [[3200]])$   
**definition**  $OclInt3500$  (3500) **where**  $OclInt3500 = (\lambda . . [[3500]])$

**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**  $person1 \equiv mk_{Person} oid0 [1300]$   
**definition**  $person2 \equiv mk_{Person} oid1 [1800]$   
**definition**  $person3 \equiv mk_{Person} oid2 None$   
**definition**  $person4 \equiv mk_{Person} oid3 [2900]$   
**definition**  $person5 \equiv mk_{Person} oid4 [3500]$   
**definition**  $person6 \equiv mk_{Person} oid5 [2500]$   
**definition**  $person7 \equiv mk_{OclAny} oid6 [[3200]]$   
**definition**  $person8 \equiv mk_{OclAny} oid7 None$   
**definition**  $person9 \equiv mk_{Person} oid8 [0]$

**definition**

$$\begin{aligned}
\sigma_1 \equiv (& \text{heap} = \text{empty}(\text{oid0} \mapsto \text{in}_{\text{Person}} (\text{mk}_{\text{Person}} \text{oid0} [1000]))) \\
& (\text{oid1} \mapsto \text{in}_{\text{Person}} (\text{mk}_{\text{Person}} \text{oid1} [1200])) \\
& (*\text{oid2}*) \\
& (\text{oid3} \mapsto \text{in}_{\text{Person}} (\text{mk}_{\text{Person}} \text{oid3} [2600])) \\
& (\text{oid4} \mapsto \text{in}_{\text{Person}} \text{person5}) \\
& (\text{oid5} \mapsto \text{in}_{\text{Person}} (\text{mk}_{\text{Person}} \text{oid5} [2300])) \\
& (*\text{oid6}*) \\
& (*\text{oid7}*) \\
& (\text{oid8} \mapsto \text{in}_{\text{Person}} \text{person9}), \\
& \text{assocs}_2 = \text{empty}(\text{oid}_{\text{Person}}\text{BOSS} \mapsto [(\text{oid0},\text{oid1}),(\text{oid3},\text{oid4}),(\text{oid5},\text{oid3})]), \\
& \text{assocs}_3 = \text{empty} )
\end{aligned}$$

**definition**

$$\begin{aligned}
\sigma_1' \equiv (& \text{heap} = \text{empty}(\text{oid0} \mapsto \text{in}_{\text{Person}} \text{person1}) \\
& (\text{oid1} \mapsto \text{in}_{\text{Person}} \text{person2}) \\
& (\text{oid2} \mapsto \text{in}_{\text{Person}} \text{person3}) \\
& (\text{oid3} \mapsto \text{in}_{\text{Person}} \text{person4}) \\
& (*\text{oid4}*) \\
& (\text{oid5} \mapsto \text{in}_{\text{Person}} \text{person6}) \\
& (\text{oid6} \mapsto \text{in}_{\text{OclAny}} \text{person7}) \\
& (\text{oid7} \mapsto \text{in}_{\text{OclAny}} \text{person8}) \\
& (\text{oid8} \mapsto \text{in}_{\text{Person}} \text{person9}), \\
& \text{assocs}_2 = \text{empty}(\text{oid}_{\text{Person}}\text{BOSS} \mapsto \\
& [(\text{oid0},\text{oid1}),(\text{oid1},\text{oid1}),(\text{oid5},\text{oid6}),(\text{oid6},\text{oid6})]), \\
& \text{assocs}_3 = \text{empty} )
\end{aligned}$$

**definition**  $\sigma_0 \equiv (\text{heap} = \text{empty}, \text{assocs}_2 = \text{empty}, \text{assocs}_3 = \text{empty} )$

**lemma** *basic- $\tau$ -wff*:  $WFF(\sigma_1, \sigma_1')$

*<proof>*

**lemma** [*simp, code-unfold*]:  $\text{dom}(\text{heap } \sigma_1) = \{\text{oid0}, \text{oid1}, (*, \text{oid2}*)\text{oid3}, \text{oid4}, \text{oid5}(*, \text{oid6}, \text{oid7}*), \text{oid8}\}$

*<proof>*

**lemma** [*simp, code-unfold*]:  $\text{dom}(\text{heap } \sigma_1') = \{\text{oid0}, \text{oid1}, \text{oid2}, \text{oid3}, (*, \text{oid4}*)\text{oid5}, \text{oid6}, \text{oid7}, \text{oid8}\}$

*<proof>*

**definition**  $X_{\text{Person}1} :: \text{Person} \equiv \lambda - . [ [ \text{person1} ] ]$

**definition**  $X_{\text{Person}2} :: \text{Person} \equiv \lambda - . [ [ \text{person2} ] ]$

**definition**  $X_{\text{Person}3} :: \text{Person} \equiv \lambda - . [ [ \text{person3} ] ]$

**definition**  $X_{\text{Person}4} :: \text{Person} \equiv \lambda - . [ [ \text{person4} ] ]$

**definition**  $X_{\text{Person}5} :: \text{Person} \equiv \lambda - . [ [ \text{person5} ] ]$

**definition**  $X_{\text{Person}6} :: \text{Person} \equiv \lambda - . [ [ \text{person6} ] ]$

**definition**  $X_{\text{Person}7} :: \text{OclAny} \equiv \lambda - . [ [ \text{person7} ] ]$

**definition**  $X_{\text{Person}8} :: \text{OclAny} \equiv \lambda - . [ [ \text{person8} ] ]$

**definition**  $X_{\text{Person}9} :: \text{Person} \equiv \lambda - . [ [ \text{person9} ] ]$

**lemma** [*code-unfold*]:  $((x :: \text{Person}) \doteq y) = \text{StrictRefEq}_{\text{Object}} x y$  *<proof>*

**lemma** [code-unfold]:  $((x::OclAny) \doteq y) = StrictRefEqObject\ x\ y$   $\langle proof \rangle$

**lemmas** [simp,code-unfold] =

$OclAsType_{OclAny-OclAny}$

$OclAsType_{OclAny-Person}$

$OclAsType_{Person-OclAny}$

$OclAsType_{Person-Person}$

$OclIsTypeOf_{OclAny-OclAny}$

$OclIsTypeOf_{OclAny-Person}$

$OclIsTypeOf_{Person-OclAny}$

$OclIsTypeOf_{Person-Person}$

$OclIsKindOf_{OclAny-OclAny}$

$OclIsKindOf_{OclAny-Person}$

$OclIsKindOf_{Person-OclAny}$

$OclIsKindOf_{Person-Person}$

**value**  $\bigwedge_{s_{pre}} \cdot (s_{pre}, \sigma_1') \models (X_{Person1} .salary \langle \rangle \mathbf{1000})$

**value**  $\bigwedge_{s_{pre}} \cdot (s_{pre}, \sigma_1') \models (X_{Person1} .salary \doteq \mathbf{1300})$

**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models (X_{Person1} .salary@pre \doteq \mathbf{1000})$

**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models (X_{Person1} .salary@pre \langle \rangle \mathbf{1300})$

**lemma**  $(\sigma_1, \sigma_1') \models (X_{Person1} .oclIsMaintained())$   
 $\langle proof \rangle$

**lemma**  $\bigwedge_{s_{pre}\ s_{post}} \cdot (s_{pre}, s_{post}) \models ((X_{Person1} .oclAsType(OclAny) .oclAsType(Person)) \doteq X_{Person1})$

$\langle proof \rangle$

**value**  $\bigwedge_{s_{pre}\ s_{post}} \cdot (s_{pre}, s_{post}) \models (X_{Person1} .oclIsTypeOf(Person))$

**value**  $\bigwedge_{s_{pre}\ s_{post}} \cdot (s_{pre}, s_{post}) \models not(X_{Person1} .oclIsTypeOf(OclAny))$

**value**  $\bigwedge_{s_{pre}\ s_{post}} \cdot (s_{pre}, s_{post}) \models (X_{Person1} .oclIsKindOf(Person))$

**value**  $\bigwedge_{s_{pre}\ s_{post}} \cdot (s_{pre}, s_{post}) \models (X_{Person1} .oclIsKindOf(OclAny))$

**value**  $\bigwedge_{s_{pre}\ s_{post}} \cdot (s_{pre}, s_{post}) \models not(X_{Person1} .oclAsType(OclAny) .oclIsTypeOf(OclAny))$

**value**  $\bigwedge_{s_{pre}} \cdot (s_{pre}, \sigma_1') \models (X_{Person2} .salary \doteq \mathbf{1800})$

**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models (X_{Person2} .salary@pre \doteq \mathbf{1200})$

**lemma**  $(\sigma_1, \sigma_1') \models (X_{Person2} .oclIsMaintained())$

$\langle proof \rangle$

**value**  $\bigwedge_{s_{pre}} \cdot (s_{pre}, \sigma_1') \models (X_{Person3} .salary \doteq null)$

**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models not(v(X_{Person3} .salary@pre))$

**lemma**  $(\sigma_1, \sigma_1') \models (X_{Person3} .oclIsNew())$

$\langle proof \rangle$



**lemma**  $(\sigma_1, \sigma_1') \models (X_{Person4} .oclIsMaintained())$   
 ⟨proof⟩

**value**  $\bigwedge_{s_{pre}} \cdot (s_{pre}, \sigma_1') \models not(v(X_{Person5} .salary))$   
**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models (X_{Person5} .salary@pre \doteq 3500)$   
**lemma**  $(\sigma_1, \sigma_1') \models (X_{Person5} .oclIsDeleted())$   
 ⟨proof⟩

**lemma**  $(\sigma_1, \sigma_1') \models (X_{Person6} .oclIsMaintained())$   
 ⟨proof⟩

**value**  $\bigwedge_{s_{pre} s_{post}} \cdot (s_{pre}, s_{post}) \models v(X_{Person7} .oclAsType(Person))$   
**lemma**  $\bigwedge_{s_{pre} s_{post}} \cdot (s_{pre}, s_{post}) \models ((X_{Person7} .oclAsType(Person) .oclAsType(OclAny) .oclAsType(Person)) \doteq (X_{Person7} .oclAsType(Person)))$

⟨proof⟩

**lemma**  $(\sigma_1, \sigma_1') \models (X_{Person7} .oclIsNew())$   
 ⟨proof⟩

**value**  $\bigwedge_{s_{pre} s_{post}} \cdot (s_{pre}, s_{post}) \models (X_{Person8} <> X_{Person7})$   
**value**  $\bigwedge_{s_{pre} s_{post}} \cdot (s_{pre}, s_{post}) \models not(v(X_{Person8} .oclAsType(Person)))$   
**value**  $\bigwedge_{s_{pre} s_{post}} \cdot (s_{pre}, s_{post}) \models (X_{Person8} .oclIsTypeOf(OclAny))$   
**value**  $\bigwedge_{s_{pre} s_{post}} \cdot (s_{pre}, s_{post}) \models not(X_{Person8} .oclIsTypeOf(Person))$   
**value**  $\bigwedge_{s_{pre} s_{post}} \cdot (s_{pre}, s_{post}) \models not(X_{Person8} .oclIsKindOf(Person))$   
**value**  $\bigwedge_{s_{pre} s_{post}} \cdot (s_{pre}, s_{post}) \models (X_{Person8} .oclIsKindOf(OclAny))$

**lemma**  $\sigma$ -modifiedonly:  $(\sigma_1, \sigma_1') \models (Set\{ X_{Person1} .oclAsType(OclAny) , X_{Person2} .oclAsType(OclAny) (*, X_{Person3} .oclAsType(OclAny)* , X_{Person4} .oclAsType(OclAny) (*, X_{Person5} .oclAsType(OclAny)* , X_{Person6} .oclAsType(OclAny) (*, X_{Person7} .oclAsType(OclAny)* (*, X_{Person8} .oclAsType(OclAny)* (*, X_{Person9} .oclAsType(OclAny)*)\} \rightarrow oclIsModifiedOnly())$

⟨proof⟩

**lemma**  $(\sigma_1, \sigma_1') \models ((X_{Person9} @pre (\lambda x. \lfloor OclAsType_{Person-9} x \rfloor)) \doteq X_{Person9})$   
 ⟨proof⟩

**lemma**  $(\sigma_1, \sigma_1') \models ((X_{Person9} \text{ @post } (\lambda x. \lfloor OclAsType_{Person} \mathfrak{A} x \rfloor)) \triangleq X_{Person9})$   
 ⟨proof⟩

**lemma**  $(\sigma_1, \sigma_1') \models (((X_{Person9} \text{ .oclAsType}(OclAny)) \text{ @pre } (\lambda x. \lfloor OclAsType_{OclAny} \mathfrak{A} x \rfloor)) \triangleq$   
 $((X_{Person9} \text{ .oclAsType}(OclAny)) \text{ @post } (\lambda x. \lfloor OclAsType_{OclAny} \mathfrak{A} x \rfloor)))$   
 ⟨proof⟩

**lemma**  $perm\text{-}\sigma_1' : \sigma_1' = () \text{ heap} = \text{empty}$   
 $(oid8 \mapsto in_{Person} \text{ person9})$   
 $(oid7 \mapsto in_{OclAny} \text{ person8})$   
 $(oid6 \mapsto in_{OclAny} \text{ person7})$   
 $(oid5 \mapsto in_{Person} \text{ person6})$   
 $(*oid4*)$   
 $(oid3 \mapsto in_{Person} \text{ person4})$   
 $(oid2 \mapsto in_{Person} \text{ person3})$   
 $(oid1 \mapsto in_{Person} \text{ person2})$   
 $(oid0 \mapsto in_{Person} \text{ person1})$   
 $, \text{ assocS}_2 = \text{assocS}_2 \sigma_1'$   
 $, \text{ assocS}_3 = \text{assocS}_3 \sigma_1' \rangle$

⟨proof⟩

**declare** *const-ss* [simp]

**lemma**  $\wedge \sigma_1.$   
 $(\sigma_1, \sigma_1') \models (Person \text{ .allInstances}() \doteq \text{Set}\{ X_{Person1}, X_{Person2}, X_{Person3}, X_{Person4}(*,$   
 $X_{Person5*}), X_{Person6},$   
 $X_{Person7} \text{ .oclAsType}(Person)(* , X_{Person8*}), X_{Person9} \})$   
 ⟨proof⟩

**lemma**  $\wedge \sigma_1.$   
 $(\sigma_1, \sigma_1') \models (OclAny \text{ .allInstances}() \doteq \text{Set}\{ X_{Person1} \text{ .oclAsType}(OclAny), X_{Person2}$   
 $\text{ .oclAsType}(OclAny),$   
 $X_{Person3} \text{ .oclAsType}(OclAny), X_{Person4} \text{ .oclAsType}(OclAny)$   
 $(* , X_{Person5*}), X_{Person6} \text{ .oclAsType}(OclAny),$   
 $X_{Person7}, X_{Person8}, X_{Person9} \text{ .oclAsType}(OclAny) \})$   
 ⟨proof⟩

end

## 6.2. The Employee Analysis Model (OCL)

**theory**  
*Employee-AnalysisModel-OCLPart*  
**imports**  
*Employee-AnalysisModel-UMLPart*  
**begin**

### 6.2.1. Standard State Infrastructure

Ideally, these definitions are automatically generated from the class model.

### 6.2.2. 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.

**axiomatization**  $inv\text{-}Person :: Person \Rightarrow Boolean$

**where**  $A : (\tau \models (\delta \text{ self})) \longrightarrow$   
 $(\tau \models inv\text{-}Person(\text{self})) =$   
 $((\tau \models (\text{self} .boss \doteq null)) \vee$   
 $(\tau \models (\text{self} .boss \langle \rangle null) \wedge (\tau \models ((\text{self} .salary) ' \leq (\text{self} .boss .salary))) \wedge$   
 $(\tau \models (inv\text{-}Person(\text{self} .boss))))$

**axiomatization**  $inv\text{-}Person\text{-}at\text{-}pre :: Person \Rightarrow Boolean$

**where**  $B : (\tau \models (\delta \text{ self})) \longrightarrow$   
 $(\tau \models inv\text{-}Person\text{-}at\text{-}pre(\text{self})) =$   
 $((\tau \models (\text{self} .boss@pre \doteq null)) \vee$   
 $(\tau \models (\text{self} .boss@pre \langle \rangle null) \wedge$   
 $(\tau \models (\text{self} .boss@pre .salary@pre ' \leq \text{self} .salary@pre)) \wedge$   
 $(\tau \models (inv\text{-}Person\text{-}at\text{-}pre(\text{self} .boss@pre))))$

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**  $inv :: Person \Rightarrow (\mathcal{A})st \Rightarrow bool$  **where**

$(\tau \models (\delta \text{ self})) \implies ((\tau \models (\text{self} .boss \doteq null)) \vee$   
 $(\tau \models (\text{self} .boss \langle \rangle null) \wedge (\tau \models (\text{self} .boss .salary ' \leq \text{self} .salary)) \wedge$   
 $( (inv(\text{self} .boss))\tau ))$   
 $\implies ( inv \text{ self } \tau )$

### 6.2.3. The Contract of a Recursive Query

The original specification of a recursive query :

```
context Person::contents():Set(Integer)
post:  result = if self.boss = null
        then Set{i}
        else self.boss.contents()->including(i)
endif
```

**consts**  $dot\text{-}contents :: Person \Rightarrow Set\text{-}Integer ((1(-).contents'()) 50)$

**axiomatization where**  $dot\text{-}contents\text{-}def:$

$(\tau \models ((\text{self}).contents() \triangleq result)) =$   
 $(if (\delta \text{ self}) \tau = true \tau$   
 $then ((\tau \models true) \wedge$

```

( $\tau \models$  ( $result \triangleq$   $if$  ( $self.boss \doteq null$ )
  then ( $Set\{self.salary\}$ )
  else ( $self.boss.contents()$ -> $including(self.salary)$ )
   $endif$ ))
else  $\tau \models result \triangleq invalid$ )

```

**consts** *dot-contents-AT-pre* :: *Person*  $\Rightarrow$  *Set-Integer* (( $1(-).contents@pre'()$ ) 50)

**axiomatization where** *dot-contents-AT-pre-def*:

```

( $\tau \models (self).contents@pre() \triangleq result$ ) =
( $if$  ( $\delta self$ )  $\tau = true$   $\tau$ 
  then  $\tau \models true \wedge$ 
     $\tau \models (result \triangleq$   $if$  ( $self.boss@pre \doteq null$ )
      then  $Set\{(self).salary@pre\}$ 
      else ( $self.boss@pre.contents@pre()$ -> $including(self.salary@pre)$ )
       $endif$ )
    else  $\tau \models result \triangleq invalid$ )

```

These @pre variants on methods are only available on queries, i. e., operations without side-effect.

#### 6.2.4. The Contract of a Method

The specification in high-level OCL input syntax reads as follows:

---

```

context Person ::  $insert(x: Integer)$ 
post:  $contents(): Set(Integer)$ 
 $contents() = contents@pre()->including(x)$ 

```

---

**consts** *dot-insert* :: *Person*  $\Rightarrow$  *Integer*  $\Rightarrow$  *Void* (( $1(-).insert'(-')$ ) 50)

**axiomatization where** *dot-insert-def*:

```

( $\tau \models ((self).insert(x) \triangleq result)$ ) =
( $if$  ( $\delta self$ )  $\tau = true$   $\tau \wedge (v x) \tau = true$   $\tau$ 
  then  $\tau \models true \wedge$ 
     $\tau \models ((self).contents() \triangleq (self).contents@pre()->including(x))$ 
  else  $\tau \models ((self).insert(x) \triangleq invalid)$ )

```

**end**

# 7. The Employee Design Model

## 7.1. The Employee Design Model (UML)

```
theory
  Employee-DesignModel-UMLPart
imports
  ../OCL-main
begin
```

### 7.1.1. 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.

### Outlining the Example

We are presenting here a “design-model” of the (slightly modified) example Figure 7.3, page 20 of the OCL standard [33]. To be precise, this theory contains the formalization of the data-part covered by the UML class model (see Figure 7.1):

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).

### 7.1.2. Example Data-Universe and its Infrastructure

Ideally, the following is generated automatically from a UML class model.

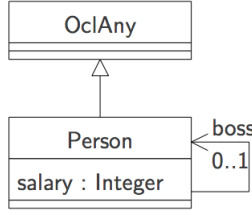


Figure 7.1.: A simple UML class model drawn from Figure 7.3, page 20 of [33].

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:

```

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.

```

datatype  $\mathfrak{A}$  = 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.

```

type-synonym Boolean    =  $\mathfrak{A}$  Boolean
type-synonym Integer   =  $\mathfrak{A}$  Integer
type-synonym Void      =  $\mathfrak{A}$  Void
type-synonym OclAny    = ( $\mathfrak{A}$ , typeOclAny option option) val
type-synonym Person    = ( $\mathfrak{A}$ , typePerson option option) val
type-synonym Set-Integer = ( $\mathfrak{A}$ , int option option) Set
type-synonym Set-Person = ( $\mathfrak{A}$ , typePerson option option) Set
  
```

Just a little check:

```

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.

```

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 - - ⇒ oid)
  instance ⟨proof⟩
end

```

```

instantiation  $\mathcal{A}$  :: object
begin
  definition oid-of- $\mathcal{A}$ -def: oid-of x = (case x of
    inPerson person ⇒ oid-of person
    | inOclAny oclany ⇒ oid-of oclany)
  instance ⟨proof⟩
end

```

### 7.1.3. Instantiation of the Generic Strict Equality

We instantiate the referential equality on *Person* and *OclAny*

```

defs(overloaded) StrictRefEqObject-Person : (x::Person) ≐ y ≡ StrictRefEqObject x y
defs(overloaded) StrictRefEqObject-OclAny : (x::OclAny) ≐ y ≡ StrictRefEqObject x y

```

**lemmas**

```

cp-StrictRefEqObject[of x::Person y::Person τ,
  simplified StrictRefEqObject-Person[symmetric]]
cp-intro(9) [of P::Person ⇒ Person Q::Person ⇒ Person,
  simplified StrictRefEqObject-Person[symmetric] ]
StrictRefEqObject-def [of x::Person y::Person,
  simplified StrictRefEqObject-Person[symmetric]]
StrictRefEqObject-defargs [of - x::Person y::Person,
  simplified StrictRefEqObject-Person[symmetric]]
StrictRefEqObject-strict1
  [of x::Person,
  simplified StrictRefEqObject-Person[symmetric]]
StrictRefEqObject-strict2
  [of x::Person,
  simplified StrictRefEqObject-Person[symmetric]]

```

For each Class *C*, we will have a casting operation `.oclAsType(C)`, a test on the actual type `.oclIsTypeOf(C)` as well as its relaxed form `.oclIsKindOf(C)` (corresponding exactly to Java's `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.

## 7.1.4. OclAsType

### Definition

**consts**  $OclAsType_{OclAny} :: 'α \Rightarrow OclAny \ ((-).oclAsType'(OclAny'))$   
**consts**  $OclAsType_{Person} :: 'α \Rightarrow Person \ ((-).oclAsType'(Person'))$

**definition**  $OclAsType_{OclAny}\text{-}\mathfrak{A} = (\lambda u. \lfloor \text{case } u \text{ of } in_{OclAny} \ a \Rightarrow a$   
 $\quad \mid in_{Person} \ (mk_{Person} \ oid \ a \ b) \Rightarrow mk_{OclAny} \ oid \ [(a,b)] \rfloor)$

**lemma**  $OclAsType_{OclAny}\text{-}\mathfrak{A}\text{-some}$ :  $OclAsType_{OclAny}\text{-}\mathfrak{A} \ x \neq None$   
 $\langle proof \rangle$

**defs (overloaded)**  $OclAsType_{OclAny}\text{-}OclAny$ :  
 $(X :: OclAny).oclAsType(OclAny) \equiv X$

**defs (overloaded)**  $OclAsType_{OclAny}\text{-}Person$ :  
 $(X :: Person).oclAsType(OclAny) \equiv$   
 $(\lambda \tau. \text{case } X \ \tau \text{ of}$   
 $\quad \perp \Rightarrow \text{invalid } \tau$   
 $\quad \mid \lfloor \perp \rfloor \Rightarrow \text{null } \tau$   
 $\quad \mid \lfloor \lfloor mk_{Person} \ oid \ a \ b \rfloor \rfloor \Rightarrow \lfloor \lfloor (mk_{OclAny} \ oid \ [(a,b)]) \rfloor \rfloor)$

**definition**  $OclAsType_{Person}\text{-}\mathfrak{A} = (\lambda u. \text{case } u \text{ of } in_{Person} \ p \Rightarrow \lfloor p \rfloor$   
 $\quad \mid in_{OclAny} \ (mk_{OclAny} \ oid \ [(a,b)]) \Rightarrow \lfloor mk_{Person} \ oid \ a \ b \rfloor$   
 $\quad \mid - \Rightarrow None)$

**defs (overloaded)**  $OclAsType_{Person}\text{-}OclAny$ :  
 $(X :: OclAny).oclAsType(Person) \equiv$   
 $(\lambda \tau. \text{case } X \ \tau \text{ of}$   
 $\quad \perp \Rightarrow \text{invalid } \tau$   
 $\quad \mid \lfloor \perp \rfloor \Rightarrow \text{null } \tau$   
 $\quad \mid \lfloor \lfloor mk_{OclAny} \ oid \ \perp \rfloor \rfloor \Rightarrow \text{invalid } \tau \ \ (* \text{ down-cast exception } *)$   
 $\quad \mid \lfloor \lfloor mk_{OclAny} \ oid \ [(a,b)] \rfloor \rfloor \Rightarrow \lfloor \lfloor mk_{Person} \ oid \ a \ b \rfloor \rfloor)$

**defs (overloaded)**  $OclAsType_{Person}\text{-}Person$ :  
 $(X :: Person).oclAsType(Person) \equiv X$

**lemmas**  $[simp] =$   
 $OclAsType_{OclAny}\text{-}OclAny$   
 $OclAsType_{Person}\text{-}Person$

### Context Passing

**lemma**  $cp\text{-}OclAsType_{OclAny}\text{-}Person\text{-}Person$ :  $cp \ P \Longrightarrow cp(\lambda X. (P \ (X :: Person) :: Person)$   
 $.oclAsType(OclAny))$   
 $\langle proof \rangle$

**lemma**  $cp\text{-}OclAsType_{OclAny}\text{-}OclAny\text{-}OclAny$ :  $cp \ P \Longrightarrow cp(\lambda X. (P \ (X :: OclAny) :: OclAny)$   
 $.oclAsType(OclAny))$



*<proof>*

**lemma** *cp-OclAsType<sub>Person</sub>-Person-Person*:  $cp\ P \implies cp(\lambda X. (P\ (X::Person)::Person))$   
*.oclAsType(Person)*

*<proof>*

**lemma** *cp-OclAsType<sub>Person</sub>-OclAny-OclAny*:  $cp\ P \implies cp(\lambda X. (P\ (X::OclAny)::OclAny))$   
*.oclAsType(Person)*

*<proof>*

**lemma** *cp-OclAsType<sub>OclAny</sub>-Person-OclAny*:  $cp\ P \implies cp(\lambda X. (P\ (X::Person)::OclAny))$   
*.oclAsType(OclAny)*

*<proof>*

**lemma** *cp-OclAsType<sub>OclAny</sub>-OclAny-Person*:  $cp\ P \implies cp(\lambda X. (P\ (X::OclAny)::Person))$   
*.oclAsType(OclAny)*

*<proof>*

**lemma** *cp-OclAsType<sub>Person</sub>-Person-OclAny*:  $cp\ P \implies cp(\lambda X. (P\ (X::Person)::OclAny))$   
*.oclAsType(Person)*

*<proof>*

**lemma** *cp-OclAsType<sub>Person</sub>-OclAny-Person*:  $cp\ P \implies cp(\lambda X. (P\ (X::OclAny)::Person))$   
*.oclAsType(Person)*

*<proof>*

**lemmas** *[simp]* =

*cp-OclAsType<sub>OclAny</sub>-Person-Person*  
*cp-OclAsType<sub>OclAny</sub>-OclAny-OclAny*  
*cp-OclAsType<sub>Person</sub>-Person-Person*  
*cp-OclAsType<sub>Person</sub>-OclAny-OclAny*

*cp-OclAsType<sub>OclAny</sub>-Person-OclAny*  
*cp-OclAsType<sub>OclAny</sub>-OclAny-Person*  
*cp-OclAsType<sub>Person</sub>-Person-OclAny*  
*cp-OclAsType<sub>Person</sub>-OclAny-Person*

## Execution with Invalid or Null as Argument

**lemma** *OclAsType<sub>OclAny</sub>-OclAny-strict* :  $(invalid::OclAny) .oclAsType(OclAny) = invalid$   
*<proof>*

**lemma** *OclAsType<sub>OclAny</sub>-OclAny-nullstrict* :  $(null::OclAny) .oclAsType(OclAny) = null$   
*<proof>*

**lemma** *OclAsType<sub>OclAny</sub>-Person-strict[simp]* :  $(invalid::Person) .oclAsType(OclAny) = invalid$   
*<proof>*

**lemma** *OclAsType<sub>OclAny</sub>-Person-nullstrict[simp]* :  $(null::Person) .oclAsType(OclAny) = null$   
*<proof>*

**lemma** *OclAsType<sub>Person</sub>-OclAny-strict[simp]* :  $(invalid::OclAny) .oclAsType(Person) = invalid$   
*<proof>*

**lemma**  $OclAsType_{Person-OclAny-nullstrict}[simp] : (null::OclAny) .oclAsType(Person) = null$   
 ⟨proof⟩

**lemma**  $OclAsType_{Person-Person-strict} : (invalid::Person) .oclAsType(Person) = invalid$   
 ⟨proof⟩

**lemma**  $OclAsType_{Person-Person-nullstrict} : (null::Person) .oclAsType(Person) = null$   
 ⟨proof⟩

### 7.1.5. OclIsTypeOf

#### Definition

**consts**  $OclIsTypeOf_{OclAny} :: 'α ⇒ Boolean ((-) .oclIsTypeOf'(OclAny'))$

**consts**  $OclIsTypeOf_{Person} :: 'α ⇒ Boolean ((-) .oclIsTypeOf'(Person'))$

**defs (overloaded)**  $OclIsTypeOf_{OclAny-OclAny}$ :  
 $(X::OclAny) .oclIsTypeOf(OclAny) ≡$   
 $(λτ. case X τ of$   
 $⊥ ⇒ invalid τ$   
 $| [⊥] ⇒ true τ (* invalid ?? *)$   
 $| [[mk_{OclAny} oid ⊥]] ⇒ true τ$   
 $| [[mk_{OclAny} oid [-]]] ⇒ false τ)$

**defs (overloaded)**  $OclIsTypeOf_{OclAny-Person}$ :  
 $(X::Person) .oclIsTypeOf(OclAny) ≡$   
 $(λτ. case X τ of$   
 $⊥ ⇒ invalid τ$   
 $| [⊥] ⇒ true τ (* invalid ?? *)$   
 $| [[-]] ⇒ false τ)$

**defs (overloaded)**  $OclIsTypeOf_{Person-OclAny}$ :  
 $(X::OclAny) .oclIsTypeOf(Person) ≡$   
 $(λτ. case X τ of$   
 $⊥ ⇒ invalid τ$   
 $| [⊥] ⇒ true τ$   
 $| [[mk_{OclAny} oid ⊥]] ⇒ false τ$   
 $| [[mk_{OclAny} oid [-]]] ⇒ true τ)$

**defs (overloaded)**  $OclIsTypeOf_{Person-Person}$ :  
 $(X::Person) .oclIsTypeOf(Person) ≡$   
 $(λτ. case X τ of$   
 $⊥ ⇒ invalid τ$   
 $| - ⇒ true τ)$

#### Context Passing

**lemma**  $cp-OclIsTypeOf_{OclAny-Person-Person} : cp \quad P \quad ⇒$   
 $cp(λX.(P(X::Person)::Person) .oclIsTypeOf(OclAny))$   
 ⟨proof⟩

**lemma**  $cp-OclIsTypeOf_{OclAny-OclAny-OclAny}$ :  $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::OclAny)::OclAny).oclIsTypeOf(OclAny))$   
 $\langle proof \rangle$

**lemma**  $cp-OclIsTypeOf_{Person-Person-Person}$ :  $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::Person)::Person).oclIsTypeOf(Person))$   
 $\langle proof \rangle$

**lemma**  $cp-OclIsTypeOf_{Person-OclAny-OclAny}$ :  $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::OclAny)::OclAny).oclIsTypeOf(Person))$   
 $\langle proof \rangle$

**lemma**  $cp-OclIsTypeOf_{OclAny-Person-OclAny}$ :  $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::Person)::OclAny).oclIsTypeOf(OclAny))$   
 $\langle proof \rangle$

**lemma**  $cp-OclIsTypeOf_{OclAny-OclAny-Person}$ :  $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::OclAny)::Person).oclIsTypeOf(OclAny))$   
 $\langle proof \rangle$

**lemma**  $cp-OclIsTypeOf_{Person-Person-OclAny}$ :  $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::Person)::OclAny).oclIsTypeOf(Person))$   
 $\langle proof \rangle$

**lemma**  $cp-OclIsTypeOf_{Person-OclAny-Person}$ :  $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::OclAny)::Person).oclIsTypeOf(Person))$   
 $\langle proof \rangle$

**lemmas**  $[simp] =$   
 $cp-OclIsTypeOf_{OclAny-Person-Person}$   
 $cp-OclIsTypeOf_{OclAny-OclAny-OclAny}$   
 $cp-OclIsTypeOf_{Person-Person-Person}$   
 $cp-OclIsTypeOf_{Person-OclAny-OclAny}$   
  
 $cp-OclIsTypeOf_{OclAny-Person-OclAny}$   
 $cp-OclIsTypeOf_{OclAny-OclAny-Person}$   
 $cp-OclIsTypeOf_{Person-Person-OclAny}$   
 $cp-OclIsTypeOf_{Person-OclAny-Person}$

## Execution with Invalid or Null as Argument

**lemma**  $OclIsTypeOf_{OclAny-OclAny-strict1}[simp]$ :  
 $(invalid::OclAny).oclIsTypeOf(OclAny) = invalid$   
 $\langle proof \rangle$

**lemma**  $OclIsTypeOf_{OclAny-OclAny-strict2}[simp]$ :  
 $(null::OclAny).oclIsTypeOf(OclAny) = true$   
 $\langle proof \rangle$

**lemma**  $OclIsTypeOf_{OclAny-Person-strict1}[simp]$ :  
 $(invalid::Person).oclIsTypeOf(OclAny) = invalid$   
 $\langle proof \rangle$

**lemma**  $OclIsTypeOf_{OclAny-Person-strict2}[simp]$ :  
 $(null::Person).oclIsTypeOf(OclAny) = true$   
 $\langle proof \rangle$

**lemma** *OclIsTypeOf<sub>Person</sub>-OclAny-strict1*[simp]:  
 (*invalid*::OclAny) .ocIsTypeOf(Person) = *invalid*  
 ⟨proof⟩

**lemma** *OclIsTypeOf<sub>Person</sub>-OclAny-strict2*[simp]:  
 (*null*::OclAny) .ocIsTypeOf(Person) = *true*  
 ⟨proof⟩

**lemma** *OclIsTypeOf<sub>Person</sub>-Person-strict1*[simp]:  
 (*invalid*::Person) .ocIsTypeOf(Person) = *invalid*  
 ⟨proof⟩

**lemma** *OclIsTypeOf<sub>Person</sub>-Person-strict2*[simp]:  
 (*null*::Person) .ocIsTypeOf(Person) = *true*  
 ⟨proof⟩

## Up Down Casting

**lemma** *actualType-larger-staticType*:  
**assumes** *isdef*:  $\tau \models (\delta X)$   
**shows**  $\tau \models (X::Person) .ocIsTypeOf(OclAny) \triangleq false$   
 ⟨proof⟩

**lemma** *down-cast-type*:  
**assumes** *isOclAny*:  $\tau \models (X::OclAny) .ocIsTypeOf(OclAny)$   
**and** *non-null*:  $\tau \models (\delta X)$   
**shows**  $\tau \models (X .oclAsType(Person)) \triangleq invalid$   
 ⟨proof⟩

**lemma** *down-cast-type'*:  
**assumes** *isOclAny*:  $\tau \models (X::OclAny) .ocIsTypeOf(OclAny)$   
**and** *non-null*:  $\tau \models (\delta X)$   
**shows**  $\tau \models not (v (X .oclAsType(Person)))$   
 ⟨proof⟩

**lemma** *up-down-cast* :  
**assumes** *isdef*:  $\tau \models (\delta X)$   
**shows**  $\tau \models ((X::Person) .oclAsType(OclAny) .oclAsType(Person) \triangleq X)$   
 ⟨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**  $\tau \models v X$   
**shows**  $\tau \models (((X :: Person) .oclAsType(OclAny) .oclAsType(Person)) \doteq X)$   
 ⟨proof⟩

**lemma** *up-down-cast-Person-OclAny-Person''*: **assumes**  $\tau \models v (X :: Person)$   
**shows**  $\tau \models (X .ocIsTypeOf(Person) \text{ implies } (X .oclAsType(OclAny) .oclAsType(Person)) \doteq X)$

*<proof>*

## 7.1.6. OclIsKindOf

### Definition

**consts**  $OclIsKindOf_{OclAny} :: 'α \Rightarrow Boolean ((-).oclIsKindOf'(OclAny'))$   
**consts**  $OclIsKindOf_{Person} :: 'α \Rightarrow Boolean ((-).oclIsKindOf'(Person'))$

**defs (overloaded)**  $OclIsKindOf_{OclAny-OclAny}$ :  
 $(X::OclAny) .oclIsKindOf(OclAny) \equiv$   
 $(\lambda\tau. \text{case } X \ \tau \text{ of}$   
 $\quad \perp \Rightarrow \text{invalid } \tau$   
 $\quad | - \Rightarrow \text{true } \tau)$

**defs (overloaded)**  $OclIsKindOf_{OclAny-Person}$ :  
 $(X::Person) .oclIsKindOf(OclAny) \equiv$   
 $(\lambda\tau. \text{case } X \ \tau \text{ of}$   
 $\quad \perp \Rightarrow \text{invalid } \tau$   
 $\quad | - \Rightarrow \text{true } \tau)$

**defs (overloaded)**  $OclIsKindOf_{Person-OclAny}$ :  
 $(X::OclAny) .oclIsKindOf(Person) \equiv$   
 $(\lambda\tau. \text{case } X \ \tau \text{ of}$   
 $\quad \perp \Rightarrow \text{invalid } \tau$   
 $\quad | [\perp] \Rightarrow \text{true } \tau$   
 $\quad | [[mk_{OclAny} \ \text{oid } \perp]] \Rightarrow \text{false } \tau$   
 $\quad | [[mk_{OclAny} \ \text{oid } [-]]] \Rightarrow \text{true } \tau)$

**defs (overloaded)**  $OclIsKindOf_{Person-Person}$ :  
 $(X::Person) .oclIsKindOf(Person) \equiv$   
 $(\lambda\tau. \text{case } X \ \tau \text{ of}$   
 $\quad \perp \Rightarrow \text{invalid } \tau$   
 $\quad | - \Rightarrow \text{true } \tau)$

### Context Passing

**lemma**  $cp-OclIsKindOf_{OclAny-Person-Person}$ :  $cp$   $P$   $\Rightarrow$   
 $cp(\lambda X.(P(X::Person)::Person).oclIsKindOf(OclAny))$   
*<proof>*

**lemma**  $cp-OclIsKindOf_{OclAny-OclAny-OclAny}$ :  $cp$   $P$   $\Rightarrow$   
 $cp(\lambda X.(P(X::OclAny)::OclAny).oclIsKindOf(OclAny))$   
*<proof>*

**lemma**  $cp-OclIsKindOf_{Person-Person-Person}$ :  $cp$   $P$   $\Rightarrow$   
 $cp(\lambda X.(P(X::Person)::Person).oclIsKindOf(Person))$   
*<proof>*

**lemma**  $cp-OclIsKindOf_{Person-OclAny-OclAny}$ :  $cp$   $P$   $\Rightarrow$   
 $cp(\lambda X.(P(X::OclAny)::OclAny).oclIsKindOf(Person))$   
*<proof>*

**lemma**  $cp-OclIsKindOf_{OclAny-Person-OclAny}$ :  $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::Person)::OclAny).oclIsKindOf(OclAny))$   
 <proof>

**lemma**  $cp-OclIsKindOf_{OclAny-OclAny-Person}$ :  $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::OclAny)::Person).oclIsKindOf(OclAny))$   
 <proof>

**lemma**  $cp-OclIsKindOf_{Person-Person-OclAny}$ :  $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::Person)::OclAny).oclIsKindOf(Person))$   
 <proof>

**lemma**  $cp-OclIsKindOf_{Person-OclAny-Person}$ :  $cp$   $P$   $\implies$   
 $cp(\lambda X.(P(X::OclAny)::Person).oclIsKindOf(Person))$   
 <proof>

**lemmas** [simp] =  
 $cp-OclIsKindOf_{OclAny-Person-Person}$   
 $cp-OclIsKindOf_{OclAny-OclAny-OclAny}$   
 $cp-OclIsKindOf_{Person-Person-Person}$   
 $cp-OclIsKindOf_{Person-OclAny-OclAny}$   
  
 $cp-OclIsKindOf_{OclAny-Person-OclAny}$   
 $cp-OclIsKindOf_{OclAny-OclAny-Person}$   
 $cp-OclIsKindOf_{Person-Person-OclAny}$   
 $cp-OclIsKindOf_{Person-OclAny-Person}$

## Execution with Invalid or Null as Argument

**lemma**  $OclIsKindOf_{OclAny-OclAny-strict1}$  [simp] :  $(invalid::OclAny) .oclIsKindOf(OclAny) =$   
 $invalid$   
 <proof>

**lemma**  $OclIsKindOf_{OclAny-OclAny-strict2}$  [simp] :  $(null::OclAny) .oclIsKindOf(OclAny) =$   
 $true$   
 <proof>

**lemma**  $OclIsKindOf_{OclAny-Person-strict1}$  [simp] :  $(invalid::Person) .oclIsKindOf(OclAny) =$   
 $invalid$   
 <proof>

**lemma**  $OclIsKindOf_{OclAny-Person-strict2}$  [simp] :  $(null::Person) .oclIsKindOf(OclAny) = true$   
 <proof>

**lemma**  $OclIsKindOf_{Person-OclAny-strict1}$  [simp] :  $(invalid::OclAny) .oclIsKindOf(Person) =$   
 $invalid$   
 <proof>

**lemma**  $OclIsKindOf_{Person-OclAny-strict2}$  [simp] :  $(null::OclAny) .oclIsKindOf(Person) = true$   
 <proof>

**lemma**  $OclIsKindOf_{Person-Person-strict1}$  [simp] :  $(invalid::Person) .oclIsKindOf(Person) =$

*invalid*  
 ⟨proof⟩

**lemma** *OclIsKindOf<sub>Person</sub>-Person-strict2*[simp]: (null::Person) .oclIsKindOf(Person) = true  
 ⟨proof⟩

## Up Down Casting

**lemma** *actualKind-larger-staticKind*:  
**assumes** *isdef*:  $\tau \models (\delta X)$   
**shows**  $\tau \models (X::Person) .oclIsKindOf(OclAny) \triangleq true$   
 ⟨proof⟩

**lemma** *down-cast-kind*:  
**assumes** *isOclAny*:  $\neg \tau \models (X::OclAny) .oclIsKindOf(Person)$   
**and** *non-null*:  $\tau \models (\delta X)$   
**shows**  $\tau \models (X .oclAsType(Person)) \triangleq invalid$   
 ⟨proof⟩

### 7.1.7. 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.”

**definition** *Person*  $\equiv OclAsType_{Person} \mathfrak{A}$

**definition** *OclAny*  $\equiv OclAsType_{OclAny} \mathfrak{A}$

**lemmas** [simp] = *Person-def OclAny-def*

**lemma** *OclAllInstances-generic<sub>OclAny</sub>-exec*: *OclAllInstances-generic pre-post OclAny* =  
 ( $\lambda \tau. Abs-Set-0 \llbracket Some \text{ ‘ } OclAny \text{ ‘ } ran (heap (pre-post \tau)) \rrbracket$ )  
 ⟨proof⟩

**lemma** *OclAllInstances-at-post<sub>OclAny</sub>-exec*: *OclAny .allInstances()* =  
 ( $\lambda \tau. Abs-Set-0 \llbracket Some \text{ ‘ } OclAny \text{ ‘ } ran (heap (snd \tau)) \rrbracket$ )  
 ⟨proof⟩

**lemma** *OclAllInstances-at-pre<sub>OclAny</sub>-exec*: *OclAny .allInstances@pre()* =  
 ( $\lambda \tau. Abs-Set-0 \llbracket Some \text{ ‘ } OclAny \text{ ‘ } ran (heap (fst \tau)) \rrbracket$ )  
 ⟨proof⟩

## OclIsTypeOf

**lemma** *OclAny-allInstances-generic-oclIsTypeOf<sub>OclAny</sub>1*:  
**assumes** [simp]:  $\bigwedge x. pre-post (x, x) = x$   
**shows**  $\exists \tau. (\tau \models ((OclAllInstances-generic \text{ pre-post } OclAny) \rightarrow forAll(X|X .oclIsTypeOf(OclAny))))$   
 ⟨proof⟩

**lemma** *OclAny-allInstances-at-post-oclIsTypeOf<sub>OclAny</sub>1*:

$\exists \tau. (\tau \models (\text{OclAny} . \text{allInstances}()) \rightarrow \text{forAll}(X|X . \text{oclIsTypeOf}(\text{OclAny})))$   
 ⟨proof⟩

**lemma** *OclAny-allInstances-at-pre-oclIsTypeOf<sub>OclAny</sub>1*:  
 $\exists \tau. (\tau \models (\text{OclAny} . \text{allInstances}@pre()) \rightarrow \text{forAll}(X|X . \text{oclIsTypeOf}(\text{OclAny})))$   
 ⟨proof⟩

**lemma** *OclAny-allInstances-generic-oclIsTypeOf<sub>OclAny</sub>2*:  
**assumes** [simp]:  $\bigwedge x. \text{pre-post}(x, x) = x$   
**shows**  $\exists \tau. (\tau \models \text{not } ((\text{OclAllInstances-generic pre-post OclAny}) \rightarrow \text{forAll}(X|X . \text{oclIsTypeOf}(\text{OclAny}))))$   
 ⟨proof⟩

**lemma** *OclAny-allInstances-at-post-oclIsTypeOf<sub>OclAny</sub>2*:  
 $\exists \tau. (\tau \models \text{not } (\text{OclAny} . \text{allInstances}()) \rightarrow \text{forAll}(X|X . \text{oclIsTypeOf}(\text{OclAny})))$   
 ⟨proof⟩

**lemma** *OclAny-allInstances-at-pre-oclIsTypeOf<sub>OclAny</sub>2*:  
 $\exists \tau. (\tau \models \text{not } (\text{OclAny} . \text{allInstances}@pre()) \rightarrow \text{forAll}(X|X . \text{oclIsTypeOf}(\text{OclAny})))$   
 ⟨proof⟩

**lemma** *Person-allInstances-generic-oclIsTypeOf<sub>Person</sub>*:  
 $\tau \models ((\text{OclAllInstances-generic pre-post Person}) \rightarrow \text{forAll}(X|X . \text{oclIsTypeOf}(\text{Person})))$   
 ⟨proof⟩

**lemma** *Person-allInstances-at-post-oclIsTypeOf<sub>Person</sub>*:  
 $\tau \models (\text{Person} . \text{allInstances}()) \rightarrow \text{forAll}(X|X . \text{oclIsTypeOf}(\text{Person})))$   
 ⟨proof⟩

**lemma** *Person-allInstances-at-pre-oclIsTypeOf<sub>Person</sub>*:  
 $\tau \models (\text{Person} . \text{allInstances}@pre()) \rightarrow \text{forAll}(X|X . \text{oclIsTypeOf}(\text{Person})))$   
 ⟨proof⟩

## OclIsKindOf

**lemma** *OclAny-allInstances-generic-oclIsKindOf<sub>OclAny</sub>*:  
 $\tau \models ((\text{OclAllInstances-generic pre-post OclAny}) \rightarrow \text{forAll}(X|X . \text{oclIsKindOf}(\text{OclAny})))$   
 ⟨proof⟩

**lemma** *OclAny-allInstances-at-post-oclIsKindOf<sub>OclAny</sub>*:  
 $\tau \models (\text{OclAny} . \text{allInstances}()) \rightarrow \text{forAll}(X|X . \text{oclIsKindOf}(\text{OclAny})))$   
 ⟨proof⟩

**lemma** *OclAny-allInstances-at-pre-oclIsKindOf<sub>OclAny</sub>*:  
 $\tau \models (\text{OclAny} . \text{allInstances}@pre()) \rightarrow \text{forAll}(X|X . \text{oclIsKindOf}(\text{OclAny})))$   
 ⟨proof⟩

**lemma** *Person-allInstances-generic-oclIsKindOf<sub>OclAny</sub>*:  
 $\tau \models ((\text{OclAllInstances-generic pre-post Person}) \rightarrow \text{forAll}(X|X . \text{oclIsKindOf}(\text{OclAny})))$



$\langle proof \rangle$

**lemma** *Person-allInstances-at-post-oclIsKindOf OclAny:*

$\tau \models (Person .allInstances() \rightarrow \text{forall}(X|X .oclIsKindOf(OclAny)))$

$\langle proof \rangle$

**lemma** *Person-allInstances-at-pre-oclIsKindOf OclAny:*

$\tau \models (Person .allInstances@pre() \rightarrow \text{forall}(X|X .oclIsKindOf(OclAny)))$

$\langle proof \rangle$

**lemma** *Person-allInstances-generic-oclIsKindOf Person:*

$\tau \models ((OclAllInstances-generic \text{ pre-post } Person) \rightarrow \text{forall}(X|X .oclIsKindOf(Person)))$

$\langle proof \rangle$

**lemma** *Person-allInstances-at-post-oclIsKindOf Person:*

$\tau \models (Person .allInstances() \rightarrow \text{forall}(X|X .oclIsKindOf(Person)))$

$\langle proof \rangle$

**lemma** *Person-allInstances-at-pre-oclIsKindOf Person:*

$\tau \models (Person .allInstances@pre() \rightarrow \text{forall}(X|X .oclIsKindOf(Person)))$

$\langle proof \rangle$

### 7.1.8. The Accessors (any, boss, salary)

Should be generated entirely from a class-diagram.

#### Definition

**definition** *eval-extract* :: ( $\mathfrak{A}, ('a::object) \text{ option option}$ ) *val*

$\Rightarrow (oid \Rightarrow (\mathfrak{A}, 'c::null) \text{ val})$

$\Rightarrow (\mathfrak{A}, 'c::null) \text{ val}$

**where** *eval-extract*  $X f = (\lambda \tau. \text{case } X \tau \text{ of}$

$\perp \Rightarrow \text{invalid } \tau \text{ (* exception propagation *)}$

$| \lfloor \perp \rfloor \Rightarrow \text{invalid } \tau \text{ (* dereferencing null pointer *)}$

$| \lfloor \lfloor \text{obj} \rfloor \rfloor \Rightarrow f \text{ (oid-of obj) } \tau$

**definition** *deref-oid<sub>Person</sub>* :: ( $\mathfrak{A} \text{ state} \times \mathfrak{A} \text{ state} \Rightarrow \mathfrak{A} \text{ state}$ )

$\Rightarrow (\text{type}_{Person} \Rightarrow (\mathfrak{A}, 'c::null) \text{ val})$

$\Rightarrow \text{oid}$

$\Rightarrow (\mathfrak{A}, 'c::null) \text{ val}$

**where** *deref-oid<sub>Person</sub>*  $\text{fst-snd } f \text{ oid} = (\lambda \tau. \text{case } (\text{heap } (\text{fst-snd } \tau)) \text{ oid of}$

$\lfloor \text{in}_{Person} \text{ obj} \rfloor \Rightarrow f \text{ obj } \tau$

$| - \Rightarrow \text{invalid } \tau$

**definition** *deref-oid<sub>OclAny</sub>* :: ( $\mathfrak{A} \text{ state} \times \mathfrak{A} \text{ state} \Rightarrow \mathfrak{A} \text{ state}$ )

$$\begin{aligned} &\Rightarrow (\text{type}_{OclAny} \Rightarrow (\mathfrak{A}, 'c::\text{null})\text{val}) \\ &\Rightarrow \text{oid} \\ &\Rightarrow (\mathfrak{A}, 'c::\text{null})\text{val} \end{aligned}$$

**where**  $\text{deref-oid}_{OclAny} \text{fst-snd } f \text{ oid} = (\lambda\tau. \text{case } (\text{heap } (\text{fst-snd } \tau)) \text{ oid of}$   
 $\quad | \text{in}_{OclAny} \text{ obj } | \Rightarrow f \text{ obj } \tau$   
 $\quad | - \quad \quad \quad \Rightarrow \text{invalid } \tau)$

pointer undefined in state or not referencing a type conform object representation

**definition**  $\text{select}_{OclAny} \mathcal{ANY} f = (\lambda X. \text{case } X \text{ of}$   
 $\quad (\text{mk}_{OclAny} - \perp) \Rightarrow \text{null}$   
 $\quad | (\text{mk}_{OclAny} - [\text{any}]) \Rightarrow f (\lambda x -. \llbracket x \rrbracket) \text{ any})$

**definition**  $\text{select}_{Person} \mathcal{BOSS} f = (\lambda X. \text{case } X \text{ of}$   
 $\quad (\text{mk}_{Person} - - \perp) \Rightarrow \text{null} \text{ (* object contains null pointer *)}$   
 $\quad | (\text{mk}_{Person} - - [\text{boss}]) \Rightarrow f (\lambda x -. \llbracket x \rrbracket) \text{ boss})$

**definition**  $\text{select}_{Person} \mathcal{SALARY} f = (\lambda X. \text{case } X \text{ of}$   
 $\quad (\text{mk}_{Person} - \perp -) \Rightarrow \text{null}$   
 $\quad | (\text{mk}_{Person} - [\text{salary}] -) \Rightarrow f (\lambda x -. \llbracket x \rrbracket) \text{ salary})$

**definition**  $\text{in-pre-state} = \text{fst}$

**definition**  $\text{in-post-state} = \text{snd}$

**definition**  $\text{reconst-basetype} = (\lambda \text{convert } x. \text{convert } x)$

**definition**  $\text{dot}_{OclAny} \mathcal{ANY} :: OclAny \Rightarrow - \text{ ((1(-).any) 50)}$   
**where**  $(X).\text{any} = \text{eval-extract } X$   
 $\quad (\text{deref-oid}_{OclAny} \text{ in-post-state}$   
 $\quad (\text{select}_{OclAny} \mathcal{ANY}$   
 $\quad \text{reconst-basetype}))$

**definition**  $\text{dot}_{Person} \mathcal{BOSS} :: Person \Rightarrow Person \text{ ((1(-).boss) 50)}$   
**where**  $(X).\text{boss} = \text{eval-extract } X$   
 $\quad (\text{deref-oid}_{Person} \text{ in-post-state}$   
 $\quad (\text{select}_{Person} \mathcal{BOSS}$   
 $\quad (\text{deref-oid}_{Person} \text{ in-post-state})))$

**definition**  $\text{dot}_{Person} \mathcal{SALARY} :: Person \Rightarrow Integer \text{ ((1(-).salary) 50)}$   
**where**  $(X).\text{salary} = \text{eval-extract } X$   
 $\quad (\text{deref-oid}_{Person} \text{ in-post-state}$   
 $\quad (\text{select}_{Person} \mathcal{SALARY}$   
 $\quad \text{reconst-basetype}))$

**definition**  $\text{dot}_{OclAny} \mathcal{ANY-at-pre} :: OclAny \Rightarrow - \text{ ((1(-).any@pre) 50)}$   
**where**  $(X).\text{any@pre} = \text{eval-extract } X$   
 $\quad (\text{deref-oid}_{OclAny} \text{ in-pre-state})$

(*select*<sub>OclAny</sub>*ANY*  
reconst-basetype))

**definition** *dot*<sub>Person</sub>*BOSS-at-pre*:: *Person*  $\Rightarrow$  *Person* ((1(-).*boss@pre*) 50)  
**where** (*X*).*boss@pre* = *eval-extract* *X*  
 (*deref-oid*<sub>Person</sub> *in-pre-state*  
 (*select*<sub>Person</sub>*BOSS*  
 (*deref-oid*<sub>Person</sub> *in-pre-state*)))

**definition** *dot*<sub>Person</sub>*SALARY-at-pre*:: *Person*  $\Rightarrow$  *Integer* ((1(-).*salary@pre*) 50)  
**where** (*X*).*salary@pre* = *eval-extract* *X*  
 (*deref-oid*<sub>Person</sub> *in-pre-state*  
 (*select*<sub>Person</sub>*SALARY*  
 reconst-basetype))

**lemmas** [*simp*] =  
*dot*<sub>OclAny</sub>*ANY-def*  
*dot*<sub>Person</sub>*BOSS-def*  
*dot*<sub>Person</sub>*SALARY-def*  
*dot*<sub>OclAny</sub>*ANY-at-pre-def*  
*dot*<sub>Person</sub>*BOSS-at-pre-def*  
*dot*<sub>Person</sub>*SALARY-at-pre-def*

## Context Passing

**lemmas** [*simp*] = *eval-extract-def*

**lemma** *cp-dot*<sub>OclAny</sub>*ANY*: ((*X*).*any*)  $\tau$  = (( $\lambda$ -. *X*  $\tau$ ).*any*)  $\tau$   $\langle$ *proof* $\rangle$

**lemma** *cp-dot*<sub>Person</sub>*BOSS*: ((*X*).*boss*)  $\tau$  = (( $\lambda$ -. *X*  $\tau$ ).*boss*)  $\tau$   $\langle$ *proof* $\rangle$

**lemma** *cp-dot*<sub>Person</sub>*SALARY*: ((*X*).*salary*)  $\tau$  = (( $\lambda$ -. *X*  $\tau$ ).*salary*)  $\tau$   $\langle$ *proof* $\rangle$

**lemma** *cp-dot*<sub>OclAny</sub>*ANY-at-pre*: ((*X*).*any@pre*)  $\tau$  = (( $\lambda$ -. *X*  $\tau$ ).*any@pre*)  $\tau$   $\langle$ *proof* $\rangle$

**lemma** *cp-dot*<sub>Person</sub>*BOSS-at-pre*: ((*X*).*boss@pre*)  $\tau$  = (( $\lambda$ -. *X*  $\tau$ ).*boss@pre*)  $\tau$   $\langle$ *proof* $\rangle$

**lemma** *cp-dot*<sub>Person</sub>*SALARY-at-pre*: ((*X*).*salary@pre*)  $\tau$  = (( $\lambda$ -. *X*  $\tau$ ).*salary@pre*)  $\tau$   $\langle$ *proof* $\rangle$

**lemmas** *cp-dot*<sub>OclAny</sub>*ANY-I* [*simp*, *intro!*] =  
*cp-dot*<sub>OclAny</sub>*ANY*[*THEN allI*[*THEN allI*],  
 of  $\lambda$  *X* -. *X*  $\lambda$  -  $\tau$ .  $\tau$ , *THEN cpI1*]

**lemmas** *cp-dot*<sub>OclAny</sub>*ANY-at-pre-I* [*simp*, *intro!*] =  
*cp-dot*<sub>OclAny</sub>*ANY-at-pre*[*THEN allI*[*THEN allI*],  
 of  $\lambda$  *X* -. *X*  $\lambda$  -  $\tau$ .  $\tau$ , *THEN cpI1*]

**lemmas** *cp-dot*<sub>Person</sub>*BOSS-I* [*simp*, *intro!*] =  
*cp-dot*<sub>Person</sub>*BOSS*[*THEN allI*[*THEN allI*],  
 of  $\lambda$  *X* -. *X*  $\lambda$  -  $\tau$ .  $\tau$ , *THEN cpI1*]

**lemmas** *cp-dot*<sub>Person</sub>*BOSS-at-pre-I* [*simp*, *intro!*] =  
*cp-dot*<sub>Person</sub>*BOSS-at-pre*[*THEN allI*[*THEN allI*],  
 of  $\lambda$  *X* -. *X*  $\lambda$  -  $\tau$ .  $\tau$ , *THEN cpI1*]

**lemmas** *cp-dot\_Person\_SALARY-I* [*simp, intro!*]=  
*cp-dot\_Person\_SALARY*[*THEN allI[THEN allI]*,  
*of λ X -. X λ - τ. τ, THEN cpI1*]  
**lemmas** *cp-dot\_Person\_SALARY-at-pre-I* [*simp, intro!*]=  
*cp-dot\_Person\_SALARY-at-pre*[*THEN allI[THEN allI]*,  
*of λ X -. X λ - τ. τ, THEN cpI1*]

### Execution with Invalid or Null as Argument

**lemma** *dot\_OclAny\_ANY-nullstrict* [*simp*]: (*null*).*any* = *invalid*  
*<proof>*  
**lemma** *dot\_OclAny\_ANY-at-pre-nullstrict* [*simp*]: (*null*).*any@pre* = *invalid*  
*<proof>*  
**lemma** *dot\_OclAny\_ANY-strict* [*simp*]: (*invalid*).*any* = *invalid*  
*<proof>*  
**lemma** *dot\_OclAny\_ANY-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>*

### 7.1.9. A Little Infra-structure on Example States

The example we are defining in this section comes from the figure 7.2.

**definition** *OclInt1000* (**1000**) **where** *OclInt1000* = ( $\lambda \cdot . \llbracket 1000 \rrbracket$ )  
**definition** *OclInt1200* (**1200**) **where** *OclInt1200* = ( $\lambda \cdot . \llbracket 1200 \rrbracket$ )  
**definition** *OclInt1300* (**1300**) **where** *OclInt1300* = ( $\lambda \cdot . \llbracket 1300 \rrbracket$ )  
**definition** *OclInt1800* (**1800**) **where** *OclInt1800* = ( $\lambda \cdot . \llbracket 1800 \rrbracket$ )  
**definition** *OclInt2600* (**2600**) **where** *OclInt2600* = ( $\lambda \cdot . \llbracket 2600 \rrbracket$ )  
**definition** *OclInt2900* (**2900**) **where** *OclInt2900* = ( $\lambda \cdot . \llbracket 2900 \rrbracket$ )  
**definition** *OclInt3200* (**3200**) **where** *OclInt3200* = ( $\lambda \cdot . \llbracket 3200 \rrbracket$ )  
**definition** *OclInt3500* (**3500**) **where** *OclInt3500* = ( $\lambda \cdot . \llbracket 3500 \rrbracket$ )

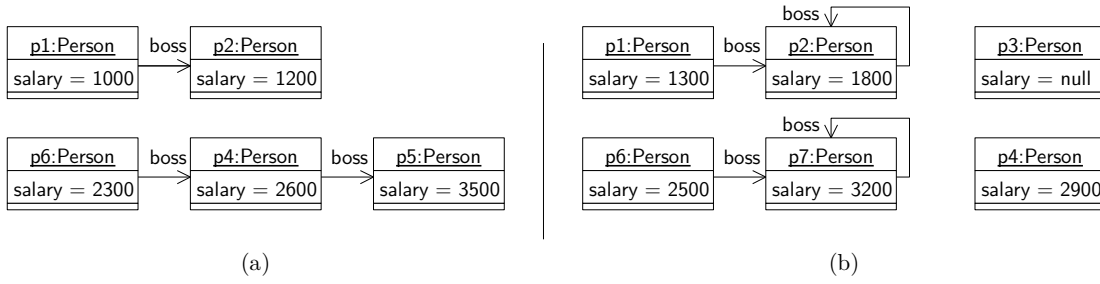


Figure 7.2.: (a) pre-state  $\sigma_1$  and (b) post-state  $\sigma'_1$ .

**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**  $person1 \equiv mk_{Person} \text{ } oid0 \ [1300] \ [oid1]$   
**definition**  $person2 \equiv mk_{Person} \text{ } oid1 \ [1800] \ [oid1]$   
**definition**  $person3 \equiv mk_{Person} \text{ } oid2 \ \text{None} \ \text{None}$   
**definition**  $person4 \equiv mk_{Person} \text{ } oid3 \ [2900] \ \text{None}$   
**definition**  $person5 \equiv mk_{Person} \text{ } oid4 \ [3500] \ \text{None}$   
**definition**  $person6 \equiv mk_{Person} \text{ } oid5 \ [2500] \ [oid6]$   
**definition**  $person7 \equiv mk_{OclAny} \text{ } oid6 \ [([3200], [oid6])]$   
**definition**  $person8 \equiv mk_{OclAny} \text{ } oid7 \ \text{None}$   
**definition**  $person9 \equiv mk_{Person} \text{ } oid8 \ [0] \ \text{None}$

**definition**

$$\begin{aligned}
 \sigma_1 \equiv & \ ( \ \text{heap} = \text{empty}(oid0 \mapsto in_{Person} (mk_{Person} \text{ } oid0 \ [1000] \ [oid1])) \\
 & \ (oid1 \mapsto in_{Person} (mk_{Person} \text{ } oid1 \ [1200] \ \text{None})) \\
 & \ (*oid2*) \\
 & \ (oid3 \mapsto in_{Person} (mk_{Person} \text{ } oid3 \ [2600] \ [oid4])) \\
 & \ (oid4 \mapsto in_{Person} \text{ } person5) \\
 & \ (oid5 \mapsto in_{Person} (mk_{Person} \text{ } oid5 \ [2300] \ [oid3])) \\
 & \ (*oid6*) \\
 & \ (*oid7*) \\
 & \ (oid8 \mapsto in_{Person} \text{ } person9), \\
 & \ \text{assocs}_2 = \text{empty}, \\
 & \ \text{assocs}_3 = \text{empty} \ )
 \end{aligned}$$

**definition**

$$\sigma'_1 \equiv \ ( \ \text{heap} = \text{empty}(oid0 \mapsto in_{Person} \text{ } person1)$$

```

      (oid1 ↦ inPerson person2)
      (oid2 ↦ inPerson person3)
      (oid3 ↦ inPerson person4)
      (*oid4*)
      (oid5 ↦ inPerson person6)
      (oid6 ↦ inOclAny person7)
      (oid7 ↦ inOclAny person8)
      (oid8 ↦ inPerson person9),
    assoc2 = empty,
    assoc3 = empty )

```

**definition**  $\sigma_0 \equiv (\text{heap} = \text{empty}, \text{assoc}_2 = \text{empty}, \text{assoc}_3 = \text{empty})$

**lemma** *basic- $\tau$ -wff*:  $WFF(\sigma_1, \sigma_1')$   
*<proof>*

**lemma** [*simp, code-unfold*]:  $\text{dom}(\text{heap } \sigma_1) = \{\text{oid0}, \text{oid1}, (*, \text{oid2}*)\text{oid3}, \text{oid4}, \text{oid5}(*, \text{oid6}, \text{oid7}*), \text{oid8}\}$   
*<proof>*

**lemma** [*simp, code-unfold*]:  $\text{dom}(\text{heap } \sigma_1') = \{\text{oid0}, \text{oid1}, \text{oid2}, \text{oid3}, (*, \text{oid4}*)\text{oid5}, \text{oid6}, \text{oid7}, \text{oid8}\}$   
*<proof>*

**definition**  $X_{\text{Person}1} :: \text{Person} \equiv \lambda - . \llbracket \text{person1} \rrbracket$

**definition**  $X_{\text{Person}2} :: \text{Person} \equiv \lambda - . \llbracket \text{person2} \rrbracket$

**definition**  $X_{\text{Person}3} :: \text{Person} \equiv \lambda - . \llbracket \text{person3} \rrbracket$

**definition**  $X_{\text{Person}4} :: \text{Person} \equiv \lambda - . \llbracket \text{person4} \rrbracket$

**definition**  $X_{\text{Person}5} :: \text{Person} \equiv \lambda - . \llbracket \text{person5} \rrbracket$

**definition**  $X_{\text{Person}6} :: \text{Person} \equiv \lambda - . \llbracket \text{person6} \rrbracket$

**definition**  $X_{\text{Person}7} :: \text{OclAny} \equiv \lambda - . \llbracket \text{person7} \rrbracket$

**definition**  $X_{\text{Person}8} :: \text{OclAny} \equiv \lambda - . \llbracket \text{person8} \rrbracket$

**definition**  $X_{\text{Person}9} :: \text{Person} \equiv \lambda - . \llbracket \text{person9} \rrbracket$

**lemma** [*code-unfold*]:  $((x :: \text{Person}) \doteq y) = \text{StrictRefEq}_{\text{Object}} x y$  *<proof>*

**lemma** [*code-unfold*]:  $((x :: \text{OclAny}) \doteq y) = \text{StrictRefEq}_{\text{Object}} x y$  *<proof>*

**lemmas** [*simp, code-unfold*] =

*OclAsType<sub>OclAny</sub>-OclAny*

*OclAsType<sub>OclAny</sub>-Person*

*OclAsType<sub>Person</sub>-OclAny*

*OclAsType<sub>Person</sub>-Person*

*OclIsTypeOf<sub>OclAny</sub>-OclAny*

*OclIsTypeOf<sub>OclAny</sub>-Person*

*OclIsTypeOf<sub>Person</sub>-OclAny*

*OclIsTypeOf<sub>Person</sub>-Person*

*OclIsKindOf<sub>OclAny</sub>-OclAny*

*OclIsKindOf<sub>OclAny</sub>-Person*

*OclIsKindOf<sub>Person</sub>-OclAny*  
*OclIsKindOf<sub>Person</sub>-Person*

**value**  $\bigwedge_{s_{pre}} \cdot (s_{pre}, \sigma_1') \models (X_{Person1} .salary <> \mathbf{1000})$   
**value**  $\bigwedge_{s_{pre}} \cdot (s_{pre}, \sigma_1') \models (X_{Person1} .salary \doteq \mathbf{1300})$   
**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models (X_{Person1} .salary@pre \doteq \mathbf{1000})$   
**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models (X_{Person1} .salary@pre <> \mathbf{1300})$   
**value**  $\bigwedge_{s_{pre}} \cdot (s_{pre}, \sigma_1') \models (X_{Person1} .boss <> X_{Person1})$   
**value**  $\bigwedge_{s_{pre}} \cdot (s_{pre}, \sigma_1') \models (X_{Person1} .boss .salary \doteq \mathbf{1800})$   
**value**  $\bigwedge_{s_{pre}} \cdot (s_{pre}, \sigma_1') \models (X_{Person1} .boss .boss <> X_{Person1})$   
**value**  $\bigwedge_{s_{pre}} \cdot (s_{pre}, \sigma_1') \models (X_{Person1} .boss .boss \doteq X_{Person2})$   
**value**  $(\sigma_1, \sigma_1') \models (X_{Person1} .boss@pre .salary \doteq \mathbf{1800})$   
**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models (X_{Person1} .boss@pre .salary@pre \doteq \mathbf{1200})$   
**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models (X_{Person1} .boss@pre .salary@pre <> \mathbf{1800})$   
**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models (X_{Person1} .boss@pre \doteq X_{Person2})$   
**value**  $(\sigma_1, \sigma_1') \models (X_{Person1} .boss@pre .boss \doteq X_{Person2})$   
**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models (X_{Person1} .boss@pre .boss@pre \doteq null)$   
**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models not(v(X_{Person1} .boss@pre .boss@pre .boss@pre))$

**lemma**  $(\sigma_1, \sigma_1') \models (X_{Person1} .oclIsMaintained())$   
*<proof>*

**lemma**  $\bigwedge_{s_{pre} s_{post}} \cdot (s_{pre}, s_{post}) \models ((X_{Person1} .oclAsType(OclAny) .oclAsType(Person)) \doteq X_{Person1})$   
*<proof>*

**value**  $\bigwedge_{s_{pre} s_{post}} \cdot (s_{pre}, s_{post}) \models (X_{Person1} .oclIsTypeOf(Person))$   
**value**  $\bigwedge_{s_{pre} s_{post}} \cdot (s_{pre}, s_{post}) \models not(X_{Person1} .oclIsTypeOf(OclAny))$   
**value**  $\bigwedge_{s_{pre} s_{post}} \cdot (s_{pre}, s_{post}) \models (X_{Person1} .oclIsKindOf(Person))$   
**value**  $\bigwedge_{s_{pre} s_{post}} \cdot (s_{pre}, s_{post}) \models (X_{Person1} .oclIsKindOf(OclAny))$   
**value**  $\bigwedge_{s_{pre} s_{post}} \cdot (s_{pre}, s_{post}) \models not(X_{Person1} .oclAsType(OclAny) .oclIsTypeOf(OclAny))$

**value**  $\bigwedge_{s_{pre}} \cdot (s_{pre}, \sigma_1') \models (X_{Person2} .salary \doteq \mathbf{1800})$   
**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models (X_{Person2} .salary@pre \doteq \mathbf{1200})$   
**value**  $\bigwedge_{s_{pre}} \cdot (s_{pre}, \sigma_1') \models (X_{Person2} .boss \doteq X_{Person2})$   
**value**  $(\sigma_1, \sigma_1') \models (X_{Person2} .boss .salary@pre \doteq \mathbf{1200})$   
**value**  $(\sigma_1, \sigma_1') \models (X_{Person2} .boss .boss@pre \doteq null)$   
**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models (X_{Person2} .boss@pre \doteq null)$   
**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models (X_{Person2} .boss@pre <> X_{Person2})$   
**value**  $(\sigma_1, \sigma_1') \models (X_{Person2} .boss@pre <> (X_{Person2} .boss))$   
**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models not(v(X_{Person2} .boss@pre .boss))$   
**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models not(v(X_{Person2} .boss@pre .salary@pre))$   
**lemma**  $(\sigma_1, \sigma_1') \models (X_{Person2} .oclIsMaintained())$   
*<proof>*

**value**  $\bigwedge_{s_{pre}} \cdot (s_{pre}, \sigma_1') \models (X_{Person3} .salary \doteq null)$   
**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models not(v(X_{Person3} .salary@pre))$

**value**  $\bigwedge_{s_{pre}} \cdot (s_{pre}, \sigma_1') \models (X_{Person3} .boss \doteq null)$   
**value**  $\bigwedge_{s_{pre}} \cdot (s_{pre}, \sigma_1') \models not(v(X_{Person3} .boss .salary))$   
**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models not(v(X_{Person3} .boss@pre))$   
**lemma**  $(\sigma_1, \sigma_1') \models (X_{Person3} .oclIsNew())$   
*<proof>*

**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models (X_{Person4} .boss@pre \doteq X_{Person5})$   
**value**  $(\sigma_1, \sigma_1') \models not(v(X_{Person4} .boss@pre .salary))$   
**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models (X_{Person4} .boss@pre .salary@pre \doteq \mathbf{3500})$   
**lemma**  $(\sigma_1, \sigma_1') \models (X_{Person4} .oclIsMaintained())$   
*<proof>*

**value**  $\bigwedge_{s_{pre}} \cdot (s_{pre}, \sigma_1') \models not(v(X_{Person5} .salary))$   
**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models (X_{Person5} .salary@pre \doteq \mathbf{3500})$   
**value**  $\bigwedge_{s_{pre}} \cdot (s_{pre}, \sigma_1') \models not(v(X_{Person5} .boss))$   
**lemma**  $(\sigma_1, \sigma_1') \models (X_{Person5} .oclIsDeleted())$   
*<proof>*

**value**  $\bigwedge_{s_{pre}} \cdot (s_{pre}, \sigma_1') \models not(v(X_{Person6} .boss .salary@pre))$   
**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models (X_{Person6} .boss@pre \doteq X_{Person4})$   
**value**  $(\sigma_1, \sigma_1') \models (X_{Person6} .boss@pre .salary \doteq \mathbf{2900})$   
**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models (X_{Person6} .boss@pre .salary@pre \doteq \mathbf{2600})$   
**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models (X_{Person6} .boss@pre .boss@pre \doteq X_{Person5})$   
**lemma**  $(\sigma_1, \sigma_1') \models (X_{Person6} .oclIsMaintained())$   
*<proof>*

**value**  $\bigwedge_{s_{pre} s_{post}} \cdot (s_{pre}, s_{post}) \models v(X_{Person7} .oclAsType(Person))$   
**value**  $\bigwedge_{s_{post}} \cdot (\sigma_1, s_{post}) \models not(v(X_{Person7} .oclAsType(Person) .boss@pre))$   
**lemma**  $\bigwedge_{s_{pre} s_{post}} \cdot (s_{pre}, s_{post}) \models ((X_{Person7} .oclAsType(Person) .oclAsType(OclAny) .oclAsType(Person)) \doteq (X_{Person7} .oclAsType(Person)))$   
*<proof>*

**lemma**  $(\sigma_1, \sigma_1') \models (X_{Person7} .oclIsNew())$   
*<proof>*

**value**  $\bigwedge_{s_{pre} s_{post}} \cdot (s_{pre}, s_{post}) \models (X_{Person8} <> X_{Person7})$   
**value**  $\bigwedge_{s_{pre} s_{post}} \cdot (s_{pre}, s_{post}) \models not(v(X_{Person8} .oclAsType(Person)))$   
**value**  $\bigwedge_{s_{pre} s_{post}} \cdot (s_{pre}, s_{post}) \models (X_{Person8} .oclIsTypeOf(OclAny))$   
**value**  $\bigwedge_{s_{pre} s_{post}} \cdot (s_{pre}, s_{post}) \models not(X_{Person8} .oclIsTypeOf(Person))$   
**value**  $\bigwedge_{s_{pre} s_{post}} \cdot (s_{pre}, s_{post}) \models not(X_{Person8} .oclIsKindOf(Person))$



**value**  $\wedge_{s_{pre} s_{post}. (s_{pre}, s_{post})} \models (X_{Person8} .oclIsKindOf(OclAny))$

**lemma**  $\sigma$ -modifiedonly:  $(\sigma_1, \sigma_1') \models (Set\{ X_{Person1} .oclAsType(OclAny)$   
 $, X_{Person2} .oclAsType(OclAny)$   
 $(*, X_{Person3} .oclAsType(OclAny)*)$   
 $, X_{Person4} .oclAsType(OclAny)$   
 $(*, X_{Person5} .oclAsType(OclAny)*)$   
 $, X_{Person6} .oclAsType(OclAny)$   
 $(*, X_{Person7} .oclAsType(OclAny)*)$   
 $(*, X_{Person8} .oclAsType(OclAny)*)$   
 $(*, X_{Person9} .oclAsType(OclAny)*)\} \rightarrow oclIsModifiedOnly())$

$\langle proof \rangle$

**lemma**  $(\sigma_1, \sigma_1') \models ((X_{Person9} @pre (\lambda x. [OclAsType_{Person}\text{-}\mathfrak{A} x])) \triangleq X_{Person9})$

$\langle proof \rangle$

**lemma**  $(\sigma_1, \sigma_1') \models ((X_{Person9} @post (\lambda x. [OclAsType_{Person}\text{-}\mathfrak{A} x])) \triangleq X_{Person9})$

$\langle proof \rangle$

**lemma**  $(\sigma_1, \sigma_1') \models (((X_{Person9} .oclAsType(OclAny)) @pre (\lambda x. [OclAsType_{OclAny}\text{-}\mathfrak{A} x])) \triangleq$   
 $((X_{Person9} .oclAsType(OclAny)) @post (\lambda x. [OclAsType_{OclAny}\text{-}\mathfrak{A} x])))$

$\langle proof \rangle$

**lemma**  $perm\text{-}\sigma_1' : \sigma_1' = (\mid heap = empty$   
 $(oid8 \mapsto in_{Person} person9)$   
 $(oid7 \mapsto in_{OclAny} person8)$   
 $(oid6 \mapsto in_{OclAny} person7)$   
 $(oid5 \mapsto in_{Person} person6)$   
 $(*oid4*)$   
 $(oid3 \mapsto in_{Person} person4)$   
 $(oid2 \mapsto in_{Person} person3)$   
 $(oid1 \mapsto in_{Person} person2)$   
 $(oid0 \mapsto in_{Person} person1)$   
 $, assocS_2 = assocS_2 \sigma_1'$   
 $, assocS_3 = assocS_3 \sigma_1' \mid)$

$\langle proof \rangle$

**declare**  $const\text{-}ss [simp]$

**lemma**  $\wedge_{\sigma_1.}$

$(\sigma_1, \sigma_1') \models (Person .allInstances() \doteq Set\{ X_{Person1}, X_{Person2}, X_{Person3}, X_{Person4}(*,$   
 $X_{Person5}*), X_{Person6},$   
 $X_{Person7} .oclAsType(Person)(* , X_{Person8}*), X_{Person9} \})$

$\langle proof \rangle$

**lemma**  $\wedge_{\sigma_1.}$

$(\sigma_1, \sigma_1') \models (OclAny .allInstances() \doteq Set\{ X_{Person1} .oclAsType(OclAny), X_{Person2} .oclAsType(OclAny),$

$$X_{Person3} .oclAsType(OclAny), X_{Person4} .oclAsType(OclAny) \\ (*, X_{Person5*}), X_{Person6} .oclAsType(OclAny), \\ X_{Person7}, X_{Person8}, X_{Person9} .oclAsType(OclAny) \}$$

⟨proof⟩

end

## 7.2. The Employee Design Model (OCL)

**theory**

*Employee-DesignModel-OCLPart*

**imports**

*Employee-DesignModel-UMLPart*

**begin**

### 7.2.1. Standard State Infrastructure

Ideally, these definitions are automatically generated from the class model.

### 7.2.2. 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.

**axiomatization** *inv-Person* :: *Person*  $\Rightarrow$  *Boolean*

**where**  $A : (\tau \models (\delta \text{ self})) \rightarrow$

$(\tau \models \text{inv-Person}(\text{self})) =$

$((\tau \models (\text{self} .\text{boss} \doteq \text{null})) \vee$

$(\tau \models (\text{self} .\text{boss} \langle \rangle \text{null}) \wedge (\tau \models ((\text{self} .\text{salary}) \leq (\text{self} .\text{boss} .\text{salary}))) \wedge$

$(\tau \models (\text{inv-Person}(\text{self} .\text{boss}))))))$

**axiomatization** *inv-Person-at-pre* :: *Person*  $\Rightarrow$  *Boolean*

**where**  $B : (\tau \models (\delta \text{ self})) \rightarrow$

$(\tau \models \text{inv-Person-at-pre}(\text{self})) =$

$((\tau \models (\text{self} .\text{boss@pre} \doteq \text{null})) \vee$

$(\tau \models (\text{self} .\text{boss@pre} \langle \rangle \text{null}) \wedge$

$(\tau \models (\text{self} .\text{boss@pre} .\text{salary@pre} \leq \text{self} .\text{salary@pre})) \wedge$

$(\tau \models (\text{inv-Person-at-pre}(\text{self} .\text{boss@pre}))))))$

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*  $\Rightarrow$   $(\mathfrak{A})st \Rightarrow \text{bool}$  **where**

$(\tau \models (\delta \text{ self})) \Rightarrow ((\tau \models (\text{self} .\text{boss} \doteq \text{null})) \vee$

$(\tau \models (\text{self} .\text{boss} \langle \rangle \text{null}) \wedge (\tau \models (\text{self} .\text{boss} .\text{salary} \leq \text{self} .\text{salary})) \wedge$

$(\text{inv}(\text{self} .\text{boss})\tau))$

$\Rightarrow (\text{inv self } \tau)$

### 7.2.3. The Contract of a Recursive Query

The original specification of a recursive query :

---

```

context Person::contents():Set(Integer)
post:  result = if self.boss = null
           then Set{i}
           else self.boss.contents()->including(i)
           endif

```

---

**consts** dot-contents :: Person ⇒ Set-Integer ((1(-).contents'()) 50)

**axiomatization where** dot-contents-def:

```

(τ ⊨ ((self).contents() ≐ result)) =
  (if (δ self) τ = true τ
   then ((τ ⊨ true) ∧
         (τ ⊨ (result ≐ if (self .boss ≐ null)
                          then (Set{self .salary})
                          else (self .boss .contents()->including(self .salary))
                          endif))))
  else τ ⊨ result ≐ invalid)

```

**consts** dot-contents-AT-pre :: Person ⇒ Set-Integer ((1(-).contents@pre'()) 50)

**axiomatization where** dot-contents-AT-pre-def:

```

(τ ⊨ (self).contents@pre() ≐ result) =
  (if (δ self) τ = true τ
   then τ ⊨ true ∧
        (* pre *)
        τ ⊨ (result ≐ if (self).boss@pre ≐ null (* post *)
                        then Set{(self).salary@pre}
                        else (self).boss@pre .contents@pre()->including(self .salary@pre)
                        endif)
   else τ ⊨ result ≐ invalid)

```

These @pre variants on methods are only available on queries, i. e., operations without side-effect.

### 7.2.4. The Contract of a Method

The specification in high-level OCL input syntax reads as follows:

---

```

context Person::insert(x:Integer)
post:  contents():Set(Integer)
        contents() = contents@pre()->including(x)

```

---

**consts** dot-insert :: Person ⇒ Integer ⇒ Void ((1(-).insert'(-)) 50)

**axiomatization where** dot-insert-def:

```

(τ ⊨ ((self).insert(x) ≐ result)) =

```

```

(if ( $\delta$  self)  $\tau = \text{true}$   $\tau \wedge (\nu x) \tau = \text{true}$   $\tau$ 
  then  $\tau \models \text{true} \wedge$ 
     $\tau \models ((\text{self}).\text{contents}() \triangleq (\text{self}).\text{contents}@pre() \rightarrow \text{including}(x))$ 
  else  $\tau \models ((\text{self}).\text{insert}(x) \triangleq \text{invalid})$ 

```

**end**

**Part IV.**  
**Conclusion**



## 8. Conclusion

### 8.1. Lessons Learned and Contributions

We provided a typed and type-safe shallow embedding of the core of UML [31, 32] and OCL [33]. Shallow embedding means that types of OCL were injectively, i. e., 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, i. e., closed-world object-oriented datatype theories, as long as it follows the described methodology.<sup>1</sup> 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 3.5.2) 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 [19].
3. the complicated life resulting from the two necessary equalities: the standard’s “strict weak referential equality” as default (written  $_ \doteq _$  throughout this document) and the strong equality (written  $_ \triangleq _$ ), 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.

---

<sup>1</sup>Our two examples of `Employee_DesignModel` (see Chapter 7) sketch how this construction can be captured by an automated process.

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 [15]).

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()`.

## 8.2. Lessons Learned

While our paper and pencil arguments, given in [13], 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 [36] or SMT-solvers like Z3 [20] completely impractical. Concretely, if the expression `not(null)` is defined `invalid` (as is the case in the present standard [33]), 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 [16]. 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  $\delta$ -closure laws (necessary for a transition into a two-valued



presentation of OCL specifications ready for interpretation in SMT solvers (see [14] for details)) are valid in Featherweight OCL.

### 8.3. 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 necessary steps for turning Featherweight OCL into a fully fledged tool for OCL, e. g., similar to HOL-OCL as well as for supporting test case generation similar to HOL-TestGen [9]. There are essentially five extensions necessary:

- extension of the library to support all OCL data types, e. g., `OrderedSet(T)` or `Sequence(T)`. This formalization of the OCL standard library can be used for checking the consistency of the formal semantics (known as “Annex A”) with the informal and semi-formal requirements in the normative part of the OCL standard.
- development of a compiler that compiles a textual or CASE tool representation (e. g., using XMI or the textual syntax of the USE tool [35]) of class models. Such compiler could also generate the necessary casts when 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 [14]. 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 an efficient test case generation approach.
- a setup in Featherweight OCL of the Nitpick animator [3]. It remains to be shown that the standard, Kodkod [36] 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

- [1] P. B. Andrews. *Introduction to Mathematical Logic and Type Theory: To Truth through Proof*. Kluwer Academic Publishers, Dordrecht, 2nd edition, 2002. ISBN 1-402-00763-9.
- [2] C. Barrett and C. Tinelli. Cvc3. In W. Damm and H. Hermanns, editors, *CAV*, volume 4590 of *Lecture Notes in Computer Science*, pages 298–302. Springer-Verlag, 2007. ISBN 978-3-540-73367-6. doi: 10.1007/978-3-540-73368-3\_34.
- [3] J. C. Blanchette and T. Nipkow. Nitpick: A counterexample generator for higher-order logic based on a relational model finder. In M. Kaufmann and L. C. Paulson, editors, *ITP*, volume 6172 of *Lecture Notes in Computer Science*, pages 131–146. Springer-Verlag, 2010. ISBN 978-3-642-14051-8. doi: 10.1007/978-3-642-14052-5\_11.
- [4] A. D. Brucker. *An Interactive Proof Environment for Object-oriented Specifications*. PhD thesis, ETH Zurich, Mar. 2007. URL <http://www.brucker.ch/bibliography/abstract/brucker-interactive-2007>. ETH Dissertation No. 17097.
- [5] A. D. Brucker and B. Wolff. A proposal for a formal OCL semantics in Isabelle/HOL. In V. A. Carreño, C. A. Muñoz, and S. Tahar, editors, *Theorem Proving in Higher Order Logics (TPHOLs)*, number 2410 in *Lecture Notes in Computer Science*, pages 99–114. Springer-Verlag, Heidelberg, 2002. ISBN 3-540-44039-9. doi: 10.1007/3-540-45685-6\_8. URL <http://www.brucker.ch/bibliography/abstract/brucker.ea-proposal-2002>.
- [6] A. D. Brucker and B. Wolff. The HOL-OCL book. Technical Report 525, ETH Zurich, 2006. URL <http://www.brucker.ch/bibliography/abstract/brucker.ea-hol-ocl-book-2006>.
- [7] A. D. Brucker and B. Wolff. An extensible encoding of object-oriented data models in hol. *Journal of Automated Reasoning*, 41:219–249, 2008. ISSN 0168-7433. doi: 10.1007/s10817-008-9108-3. URL <http://www.brucker.ch/bibliography/abstract/brucker.ea-extensible-2008-b>.
- [8] A. D. Brucker and B. Wolff. HOL-OCL – A Formal Proof Environment for UML/OCL. In J. Fiadeiro and P. Inverardi, editors, *Fundamental Approaches to Software Engineering (FASE08)*, number 4961 in *Lecture Notes in Computer Science*, pages 97–100. Springer-Verlag, Heidelberg, 2008. doi: 10.1007/978-3-540-78743-3\_8. URL <http://www.brucker.ch/bibliography/abstract/brucker.ea-hol-ocl-2008>.

- [9] A. D. Brucker and B. Wolff. HOL-TestGen: An interactive test-case generation framework. In M. Chechik and M. Wirsing, editors, *Fundamental Approaches to Software Engineering (FASE09)*, number 5503 in Lecture Notes in Computer Science, pages 417–420. Springer-Verlag, Heidelberg, 2009. doi: 10.1007/978-3-642-00593-0\_28. URL <http://www.brucker.ch/bibliography/abstract/brucker.ea-hol-testgen-2009>.
- [10] A. D. Brucker and B. Wolff. Semantics, calculi, and analysis for object-oriented specifications. *Acta Informatica*, 46(4):255–284, July 2009. ISSN 0001-5903. doi: 10.1007/s00236-009-0093-8. URL <http://www.brucker.ch/bibliography/abstract/brucker.ea-semantics-2009>.
- [11] A. D. Brucker, J. Doser, and B. Wolff. Semantic issues of OCL: Past, present, and future. *Electronic Communications of the EASST*, 5, 2006. ISSN 1863-2122. URL <http://www.brucker.ch/bibliography/abstract/brucker.ea-semantic-2006-b>.
- [12] A. D. Brucker, J. Doser, and B. Wolff. A model transformation semantics and analysis methodology for SecureUML. In O. Nierstrasz, J. Whittle, D. Harel, and G. Reggio, editors, *MoDELS 2006: Model Driven Engineering Languages and Systems*, number 4199 in Lecture Notes in Computer Science, pages 306–320. Springer-Verlag, Heidelberg, 2006. doi: 10.1007/11880240\_22. URL <http://www.brucker.ch/bibliography/abstract/brucker.ea-transformation-2006>. An extended version of this paper is available as ETH Technical Report, no. 524.
- [13] A. D. Brucker, M. P. Krieger, and B. Wolff. Extending OCL with null-references. In S. Gosh, editor, *Models in Software Engineering*, number 6002 in Lecture Notes in Computer Science, pages 261–275. Springer-Verlag, Heidelberg, 2009. doi: 10.1007/978-3-642-12261-3\_25. URL <http://www.brucker.ch/bibliography/abstract/brucker.ea-ocl-null-2009>. Selected best papers from all satellite events of the MoDELS 2009 conference.
- [14] A. D. Brucker, M. P. Krieger, D. Longuet, and B. Wolff. A specification-based test case generation method for UML/OCL. In J. Dingel and A. Solberg, editors, *MoDELS Workshops*, number 6627 in Lecture Notes in Computer Science, pages 334–348. Springer-Verlag, Heidelberg, 2010. ISBN 978-3-642-21209-3. doi: 10.1007/978-3-642-21210-9\_33. URL <http://www.brucker.ch/bibliography/abstract/brucker.ea-ocl-testing-2010>. Selected best papers from all satellite events of the MoDELS 2010 conference. Workshop on OCL and Textual Modelling.
- [15] A. D. Brucker, D. Chiorean, T. Clark, B. Demuth, M. Gogolla, D. Plotnikov, B. Rumpe, E. D. Willink, and B. Wolff. Report on the Aachen OCL meeting. In J. Cabot, M. Gogolla, I. Rath, and E. Willink, editors, *Proceedings of the MODELS 2013 OCL Workshop (OCL 2013)*, volume 1092 of *CEUR Workshop Proceedings*, pages 103–111. CEUR-WS.org, 2013. URL <http://www.brucker.ch/bibliography/abstract/brucker.ea-summary-aachen-2013>.

- [16] A. D. Brucker, D. Longuet, F. Tuong, and B. Wolff. On the semantics of object-oriented data structures and path expressions. In *OCL@MoDELS*, pages 23–32, 2013.
- [17] A. Church. A formulation of the simple theory of types. *Journal of Symbolic Logic*, 5(2):56–68, June 1940.
- [18] T. Clark and J. Warmer, editors. *Object Modeling with the OCL: The Rationale behind the Object Constraint Language*, volume 2263 of *Lecture Notes in Computer Science*, Heidelberg, 2002. Springer-Verlag. ISBN 3-540-43169-1.
- [19] S. Cook, A. Kleppe, R. Mitchell, B. Rumpe, J. Warmer, and A. Wills. The amsterdam manifesto on OCL. In Clark and Warmer [18], pages 115–149. ISBN 3-540-43169-1.
- [20] L. M. de Moura and N. Bjørner. Z3: An efficient SMT solver. In C. R. Ramakrishnan and J. Rehof, editors, *TACAS*, volume 4963 of *Lecture Notes in Computer Science*, pages 337–340, Heidelberg, 2008. Springer-Verlag. ISBN 978-3-540-78799-0. doi: 10.1007/978-3-540-78800-3\_24.
- [21] M. Gogolla and M. Richters. Expressing UML class diagrams properties with OCL. In Clark and Warmer [18], pages 85–114. ISBN 3-540-43169-1.
- [22] A. Hamie, F. Civello, J. Howse, S. Kent, and R. Mitchell. Reflections on the Object Constraint Language. In J. Bézivin and P.-A. Muller, editors, *The Unified Modeling Language. «UML»'98: Beyond the Notation*, volume 1618 of *Lecture Notes in Computer Science*, pages 162–172, Heidelberg, 1998. Springer-Verlag. ISBN 3-540-66252-9. doi: 10.1007/b72309.
- [23] P. Kosiuczenko. Specification of invariability in OCL. In O. Nierstrasz, J. Whittle, D. Harel, and G. Reggio, editors, *Model Driven Engineering Languages and Systems (MoDELS)*, volume 4199 of *Lecture Notes in Computer Science*, pages 676–691, Heidelberg, 2006. Springer-Verlag. ISBN 978-3-540-45772-5. doi: 10.1007/11880240\_47.
- [24] M. P. Krieger, A. Knapp, and B. Wolff. Generative programming and component engineering. In E. Visser and J. Järvi, editors, *International Conference on Generative Programming and Component Engineering (GPCE 2010)*, pages 53–62. ACM, Oct. 2010. ISBN 978-1-4503-0154-1.
- [25] G. T. Leavens, E. Poll, C. Clifton, Y. Cheon, C. Ruby, D. R. Cok, P. Müller, J. Kiniry, and P. Chalin. JML reference manual (revision 1.2), Feb. 2007. Available from <http://www.jmlspecs.org>.
- [26] L. Mandel and M. V. Cengarle. On the expressive power of OCL. In J. M. Wing, J. Woodcock, and J. Davies, editors, *World Congress on Formal Methods in the Development of Computing Systems (FM)*, volume 1708 of *Lecture Notes in*

- Computer Science*, pages 854–874, Heidelberg, 1999. Springer-Verlag. ISBN 3-540-66587-0.
- [27] T. Nipkow, L. C. Paulson, and M. Wenzel. *Isabelle/HOL—A Proof Assistant for Higher-Order Logic*, volume 2283 of *Lecture Notes in Computer Science*. Springer-Verlag, Heidelberg, 2002. doi: 10.1007/3-540-45949-9.
  - [28] Object Management Group. Object constraint language specification (version 1.1), Sept. 1997. Available as OMG document ad/97-08-08.
  - [29] Object Management Group. UML 2.0 OCL specification, Oct. 2003. Available as OMG document ptc/03-10-14.
  - [30] Object Management Group. UML 2.0 OCL specification, Apr. 2006. Available as OMG document formal/06-05-01.
  - [31] Object Management Group. UML 2.4.1: Infrastructure specification, Aug. 2011. Available as OMG document formal/2011-08-05.
  - [32] Object Management Group. UML 2.4.1: Superstructure specification, Aug. 2011. Available as OMG document formal/2011-08-06.
  - [33] Object Management Group. UML 2.3.1 OCL specification, Feb. 2012. Available as OMG document formal/2012-01-01.
  - [34] A. Riazanov and A. Voronkov. Vampire. In H. Ganzinger, editor, *CADE*, volume 1632 of *Lecture Notes in Computer Science*, pages 292–296. Springer-Verlag, 1999. ISBN 3-540-66222-7. doi: 10.1007/3-540-48660-7\_26.
  - [35] M. Richters. *A Precise Approach to Validating UML Models and OCL Constraints*. PhD thesis, Universität Bremen, Logos Verlag, Berlin, BISS Monographs, No. 14, 2002.
  - [36] E. Torlak and D. Jackson. Kodkod: A relational model finder. In O. Grumberg and M. Huth, editors, *TACAS*, volume 4424 of *Lecture Notes in Computer Science*, pages 632–647, Heidelberg, 2007. Springer-Verlag. ISBN 978-3-540-71208-4. doi: 10.1007/978-3-540-71209-1\_49.
  - [37] M. Wenzel and B. Wolff. Building formal method tools in the Isabelle/Isar framework. In K. Schneider and J. Brandt, editors, *TPHOLs 2007*, number 4732 in *Lecture Notes in Computer Science*, pages 352–367. Springer-Verlag, Heidelberg, 2007. doi: 10.1007/978-3-540-74591-4\_26.
  - [38] M. M. Wenzel. *Isabelle/Isar — a versatile environment for human-readable formal proof documents*. PhD thesis, TU München, München, Feb. 2002. URL <http://tumb1.biblio.tu-muenchen.de/publ/diss/in/2002/wenzel.html>.