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

Achim D. Brucker∗ Frédéric Tuong‡ Burkhart Wolff†

September 19, 2015

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

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

†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

1. **Introduction** 9

   1. **Motivation** 11

2. **Background** 13

   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

3. **A Proposal for Formal Semantics of OCL 2.5** 35

   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

3.5. A Standard Logical Calculus for OCL

#### 3.5.1. Global vs. Local Judgements

#### 3.5.2. Local Validity and Meta-logic

#### 3.5.3. Local Judgements and Strong Equality

#### 3.5.4. Laws to Establish Definedness (δ-closure)

3.6. Miscellaneous

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

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

### 4. Formalization II: Library Definitions

#### 4.1. Basic Types: Void and Integer

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

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

#### 4.1.3. Validity and Definedness Properties

#### 4.1.4. Arithmetical Operations on Integer

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

#### 4.2.1. Definition

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

#### 4.2.3. Test Statements on Basic Types.

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

#### 4.3.1. The Construction of the Set Type

#### 4.3.2. Validity and Definedness Properties

#### 4.3.3. Constants on Sets

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

#### 4.4.1. Computational Operations on Set

#### 4.4.2. Validity and Definedness Properties

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

#### 4.4.4. Context Passing

#### 4.4.5. Const

#### 4.5. Fundamental Predicates on Set: Strict Equality

#### 4.5.1. Definition

#### 4.5.2. Logic and Algebraic Layer on Set

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

#### 4.6.1. OclIncluding

#### 4.6.2. OclExcluding

#### 4.6.3. OclIncludes

#### 4.6.4. OclExcludes

#### 4.6.5. OclSize

#### 4.6.6. OclIsEmpty

#### 4.6.7. OclNotEmpty

#### 4.6.8. OclANY

#### 4.6.9. OclForall

#### 4.6.10. OclExists
7. The Employee Design Model

7.1. The Employee Design Model (UML)

7.1.1. Introduction

7.1.2. Example Data-Universe and its Infrastructure

7.1.3. Instantiation of the Generic Strict Equality

7.1.4. OclAsType

7.1.5. OclIsTypeOf

7.1.6. OclIsKindOf

7.1.7. OclAllInstances

7.1.8. The Accessors (any, boss, salary)

7.1.9. A Little Infra-structure on Example States

7.2. The Employee Design Model (OCL)

7.2.1. Standard State Infrastructure

7.2.2. Invariant

7.2.3. The Contract of a Recursive Query

7.2.4. The Contract of a Method

IV. Conclusion

8. Conclusion

8.1. Lessons Learned and Contributions

8.2. Lessons Learned

8.3. Conclusion and Future Work
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 \texttt{invalid}[^1]), with the exception of the logical connectives of type \texttt{Boolean} that constitute a three-valued propositional logic. At its core, OCL comprises four layers:

1. Operators (e.g., \_ and \texttt{and}, \_ + _) on built-in data structures such as \texttt{Boolean}, \texttt{Integer}, or typed sets (\texttt{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 \texttt{invalid} has a strict semantics, \texttt{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 \texttt{invalid} and \texttt{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

[^1]: In earlier versions of the OCL standard, this element was called \texttt{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) \cite{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.

![Diagram](image_url)

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., associations classes allow also for defining attributes and operations for such tuples. In a class diagram, association classes are represented by a dotted line connecting the class with the association. Associations classes can take part in other associations. Moreover, UML supports also n-ary associations (not shown in our example).

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

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

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

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

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

```
context Session::findRole(person: Person): Role
pre: self.participates.person->includes(person)
post: result=self.participants->one(p: Participant | p.person = person ).role
    and self.participants = self.participants@pre
    and self.name = self.name@pre
```
where in post-conditions, the operator @pre allows for accessing the previous state.

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 \( \Rightarrow \) allowing to form constructs like \( A_1 \Rightarrow \cdots \Rightarrow A_n \Rightarrow A_{n+1} \), which are viewed as a rule of the form “from assumptions \( A_1 \) to \( A_n \), infer conclusion \( A_{n+1} \)” and which is written in Isabelle as

\[
\begin{array}{c}
A_1 \cdots A_n \\
\Rightarrow \\
A_{n+1}
\end{array}
\]

(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:

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

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

\[
\text{label} : \phi \\
1. \phi_1 \\
\vdots \\
n. \phi_n
\] (2.4)

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

### 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 $\land$, $\rightarrow$, $\neg$ as well as the object-logical quantifiers $\forall x. P \, x$ and $\exists x. P \, x$; in contrast to first-order logic, quantifiers may range over arbitrary types, including total functions $f :: \alpha \Rightarrow \beta$. HOL is centered around extensional equality $= :: \alpha \Rightarrow \alpha \Rightarrow \text{bool}$. 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 λ-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 $\tau_\bot := \bot \mid \tau_\bot : \alpha$ that assigns to each type $\tau$ a type $\tau_\bot$ disjointly extended by the exceptional element $\bot$. The function $\tau^{-} : \alpha \rightarrow \alpha$ is the inverse of $\tau_\bot$ (unspecified for $\bot$). Partial functions $\alpha \rightarrow\beta$ are defined as functions $\alpha \Rightarrow\beta_\bot$ supporting the usual concepts of domain (dom $\bot$) and range (ran $\bot$).

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:

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

(2.5)

Isabelle’s syntax engine is instructed to accept the notation \{x \mid P\} for Collect \(\lambda x. P\) and the notation \(s \in S\) for member \(s S\). As can be inferred from the example, constant definitions are axioms that introduce a fresh constant symbol by some 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:

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

(2.6)

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

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

(2.7)

respectively

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

(2.8)

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

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

(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:

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

(2.10)

\[\text{To increase readability, we use a slightly simplified presentation.}\]
fun sort ::\((\alpha::\text{linorder})\) list \Rightarrow \alpha \text{ list} \\
where \begin{align*}
\text{sort} \ [\ ] & \ = \ [\ ] \\
\text{sort}(x\#xs) & \ = \ \text{ins} \ x \ (\text{sort} \ xs)
\end{align*}

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

Thus, Isabelle/HOL also provides a large collection of theories like sets, lists, 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 \textit{Boolean}, \textit{Integer}, and typed sets (\textit{Set}(T)). Following the tradition of HOL-OCL [6, 8], Featherweight OCL is based on the following principles:

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

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

3. Any Featherweight OCL type contains at least \texttt{invalid} and \texttt{null} (the type \texttt{Void} contains only these instances). The logic is consequently four-valued, and there is a \texttt{null}-element in the type \textit{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., \texttt{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 logically 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 \((\alpha \bot)\) is an instance of this type-class with \(\text{bot} \equiv \bot\) and \(\text{null} \equiv \lfloor \bot \rfloor\). Now, any OCL type can be represented by an HOL type of the form:

\[
V(\alpha) := \text{state} \times \text{state} \to \alpha :: \text{null}.
\]

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

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

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 \(\text{not } X.\text{oclIsUndefined()}\) and \(\nu X\) for \(\text{not } X.\text{oclIsInvalid()}\) 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:

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

we can therefore write:

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

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 \(\bot\), all expressions can be viewed as evaluations from \((\sigma, \sigma')\) to a type \(\alpha\) which must posses a \(\bot\) 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

\[
V(\alpha) := \text{state} \times \text{state} \to \alpha :: \{\text{bot}, \text{null}\},
\]

where state stands for the system state and \(\text{state} \times \text{state}\) 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 \(\_\_\text{a}\) by their counterparts \(\_\_\text{a} \_\text{pre}\). For example, \((\text{self.} \_\_\text{a} > 5)\_\text{pre}\) is just \((\text{self.} \_\_\text{a} \_\text{pre} > 5)\). 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 \texttt{not} and \texttt{and} as follows:

\[
I[\texttt{not } X] \tau = (\text{case } I[X] \tau \text{ of } \bot \Rightarrow \bot, ||\bot|| \Rightarrow ||\bot||, ||x|| \Rightarrow ||\neg x||)
\]

\[
I[X \texttt{ and } Y] \tau = (\text{case } I[X] \tau \text{ of } \bot \Rightarrow (\text{case } I[Y] \tau \text{ of } \bot \Rightarrow \bot, ||\bot|| \Rightarrow ||\bot||, ||\text{true}|| \Rightarrow ||\bot||, ||\text{false}|| \Rightarrow ||\text{false}||), ||\text{true}|| \Rightarrow (\text{case } I[Y] \tau \text{ of } \bot \Rightarrow \bot, ||\bot|| \Rightarrow ||\bot||, ||\text{true}|| \Rightarrow ||\bot||, ||\text{false}|| \Rightarrow ||\text{false}||), ||\text{false}|| \Rightarrow ||\text{false}||))
\]

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

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:

\[
I[x + y] \tau = \begin{cases} I[\delta x] \tau = ||\text{true}|| \wedge I[\delta y] \tau = ||\text{true}|| \\ \text{then } ||I[x] \tau|| + ||I[y] \tau|| \end{cases}
\]

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

$$\tau \models P \equiv (I[P]\tau = [true]) .$$

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:

$$\tau \models true \quad \neg(\tau \models false) \quad \neg(\tau \models invalid) \quad \neg(\tau \models null)$$

$$\tau \models \neg P \implies \neg(\tau \models P)$$

$$\tau \models P \text{ and } Q \implies \tau \models P \quad \tau \models P \text{ and } Q \implies \tau \models Q$$

$$\tau \models P \implies (\text{if } P \text{ then } B_1 \text{ else } B_2 \text{ endif})\tau = B_1 \tau$$

$$\tau \models \neg P \implies (\text{if } P \text{ then } B_1 \text{ else } B_2 \text{ endif})\tau = B_2 \tau$$

$$\tau \models P \implies \delta P \quad \tau \models \delta X \implies \tau \models \upsilon X$$

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 $\_ = \_), 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:

$$I[X \triangleq Y]\tau \equiv [[I[X]\tau = I[Y]\tau]]$$

It enjoys nearly the laws of a congruence:

$$\tau \models (x \triangleq x)$$

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

$$\tau \models (x \triangleq y) \implies \tau \models (y \triangleq z) \implies \tau \models (x \triangleq z)$$

$$\text{cp } P \implies \tau \models (x \triangleq y) \implies \tau \models (P \ x) \implies \tau \models (P \ y)$$

where the predicate $\text{cp}$ stands for context-passing, a property that is characterized by $P(X)$ equals $\lambda \tau. \ P(\lambda X. X\tau)\tau$. 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]. δ-closure rules for all logical connectives have the following format, e.g.:

\[
\tau \models \delta x \implies (\tau \models \text{not } x) = (\neg (\tau \models x)) \\
\tau \models \delta x \implies \tau \models \delta y \implies (\tau \models x \text{ and } y) = (\tau \models x \land \tau \models y) \\
\tau \models \delta x \implies \tau \models \delta y \\
\implies (\tau \models (x \text{ implies } y)) = ((\tau \models x) \implies (\tau \models y))
\]

Together with the general case-distinction

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

which is possible for any OCL type, a case distinction on the variables in a formula can be performed; due to strictness rules, formulae containing somewhere a variable \( x \) that is known to be invalid or null reduce usually quickly to contradictions. For example, we can infer from an invariant \( \tau \models x = y - 3 \) that we have \( \tau \models x = y - 3 \land \tau \models \delta x \land \tau \models \delta y \). We call the latter formula the \( \delta \)-closure of the former. Now, we can convert a formula like \( \tau \models x > 0 \lor 3 \times y > x \times x \) into the equivalent formula \( \tau \models x > 0 \lor \tau \models 3 \times y > x \times x \) 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:

\[
\begin{align*}
v \text{ invalid} &= \text{false} & v \text{ null} &= \text{true} \\
v \text{ true} &= \text{true} & v \text{ false} &= \text{true} \\
\delta \text{ invalid} &= \text{false} & \delta \text{ null} &= \text{false} \\
\delta \text{ true} &= \text{true} & \delta \text{ false} &= \text{true} \\
\text{not invalid} &= \text{invalid} & \text{not null} &= \text{null} \\
\text{not true} &= \text{false} & \text{not false} &= \text{true} \\
(\text{null and true}) &= \text{null} & (\text{null and false}) &= \text{false} \\
(\text{null and null}) &= \text{null} & (\text{null and invalid}) &= \text{invalid} \\
(\text{false and true}) &= \text{false} & (\text{false and false}) &= \text{false} \\
(\text{false and null}) &= \text{false} & (\text{false and invalid}) &= \text{false}
\end{align*}
\]
\[(\text{true and true}) = \text{true} \quad (\text{true and false}) = \text{false} \]
\[(\text{true and null}) = \text{null} \quad (\text{true and invalid}) = \text{invalid} \]
\[(\text{invalid and true}) = \text{invalid} \quad (\text{invalid and false}) = \text{false} \]
\[(\text{invalid and null}) = \text{invalid} \quad (\text{invalid and invalid}) = \text{invalid} \]

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

\[X \text{ and } X = X \quad X \text{ and } Y = Y \text{ and } X\]
\[false \text{ and } X = false \quad X \text{ and } false = false\]
\[true \text{ and } X = X \quad X \text{ and } true = X\]
\[X \text{ and } (Y \text{ and } Z) = X \text{ and } Y \text{ and } Z\]

as well as the dual equalities for \(\_\text{ or } \_\) 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 \(\_ + \_\)):

\[\text{invalid} + X = \text{invalid} \quad X + \text{invalid} = \text{invalid} \]
\[X + \text{null} = \text{invalid} \quad \text{null} + X = \text{invalid}\]
\[\text{null.oclAsType}(X) = \text{invalid}\]

Besides "classical" exceptional behavior:

\[1 / 0 = \text{invalid} \quad 1 / \text{null} = \text{invalid}\]
\[\text{null->isEmpty()} = \text{true}\]

Moreover, there is also the proposal to use \text{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 \text{not} Featherweight OCL at present) would boil down to:

\[\text{invalid} + X = \text{invalid} \quad X + \text{invalid} = \text{invalid} \]
\[X + \text{null} = \text{null} \quad \text{null} + X = \text{null}\]
\[\text{null.oclAsType}(X) = \text{null}\]
\[1 / 0 = \text{invalid} \quad 1 / \text{null} = \text{null}\]
\[\text{null->isEmpty()} = \text{null}\]

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
δ-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. This semantic alternative (this is not Featherweight OCL at present) would yield:

\[
\begin{align*}
\text{invalid} + X &= \text{invalid} & X + \text{invalid} &= \text{invalid} \\
X + \text{null} &= X & \text{null} + X &= X \\
\text{null}.\text{oclAsType}(X) &= \text{invalid} \\
1 / 0 &= \text{invalid} & 1 / \text{null} &= \text{invalid} \\
\text{null} \rightarrow \text{isEmpty}() &= \text{true}
\end{align*}
\]

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

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

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

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

an expression like \text{Set\{1,2\} \rightarrow 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\{Set\{2,null\}\}} \models \text{Set\{Set\{null,2\}\}})"

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

\footnote{In spreadsheet programs the interpretation of null varies from operation to operation; e.g., the \textit{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 $C_1, \ldots, C_n$), which become types of data in OCL. Class names declare two projector functions to the set of all objects in a state: $C_i\text{.allInstances()}$ and $C_i\text{.allInstances@pre()}$,
2. an inheritance relation $\prec$ 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 $A \in \{ V(\ldots, \bot), C_1, \ldots, C_n \}$),
4. type casts that can change the static type of an object of a class ($X.\text{oclAsType}(C_i)$ of type $C_j \rightarrow C_i$)
5. two dynamic type tests ($X.\text{oclIsTypeOf}(C_i)$ and $X.\text{oclIsKindOf}(C_i)$),
6. and last but not least, for each class name $C_i$ there is an instance of the overloaded referential equality (written $\_\approx\_$).

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:

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

(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 $A_{i_1}, \ldots, A_{i_k}$ are the attribute types (including inherited attributes) with class types substituted by oid. The function OidOf projects the first component, the oid, out of an object representation. Then the object universe will be constructed by the type definition:

$$\mathfrak{A} := C_1 + \cdots + C_n.$$  \hspace{1cm} (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 loosing information, such that casting up and casting down will not give the required identity:

$$X.\text{oclIsTypeOf}(C_k) \Leftrightarrow X.\text{oclAsType}(C_i).\text{oclAsType}(C_k) = X$$ \hspace{1cm} (2.14)

whenever $C_k < C_i$ and $X$ is valid. \hspace{1cm} (2.15)

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

Let $C_i$ be a class with a possibly empty set of subclasses $\{C_{j_1}, \ldots, C_{j_m}\}$.

- Then the class type extension $C_{\text{ext}}$ associated to $C_i$ is $A_{i_1} \times \cdots \times A_{i_k} \times (C_{j_{1\text{ext}}} + \cdots + C_{j_{m\text{ext}}})$ where $A_{i_k}$ ranges over the local attribute types of $C_i$ and $C_{j_{k\text{ext}}}$ ranges over all class type extensions of the subclass $C_j$ of $C_i$.  

27
• Then the class type for \( C_i \) is \( \text{oid} \times A_{i_1} \times \cdots \times A_{i_n} \times (C_{j_1}^{\text{ext}} + \cdots + C_{j_m}^{\text{ext}}) \perp \) where
\( A_{i_k} \) ranges over the inherited and local attribute types of \( C_i \) and \( C_{j_k}^{\text{ext}} \) 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 an concrete object universe,

• there are fixed principles that allow to derive the semantic theory of any concrete object universe, called the object-oriented datatype theory.

We will work out concrete examples for the construction of the object-universes in 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:

\[
\text{definition eval} \quad \text{extract } X \ f = (\lambda \tau. \ case X \, \tau \ of \ \bot \Rightarrow \text{invalid } \tau \quad \text{exception} \\
\quad | \ \bot_j \Rightarrow \text{invalid } \tau \quad \text{deref. null} \quad (2.16) \\
\quad | \ \bot, \underline{\text{obj}}_j \Rightarrow f (\text{oid}_\text{of } \text{obj} \ \tau)
\]

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

\[
\text{definition deref_oid}_C \ f = (\lambda \tau. \ case (\text{heap } (\text{fst, snd } \tau)) \ \text{oid of} \\
\quad \bot \Rightarrow \text{obj } \tau \\
\quad | \ \bot, \underline{\text{obj}} \Rightarrow \text{invalid } \tau \quad (2.17)
\]

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:

\[
\text{definition select}_a \ f = (\lambda \ mk \ C \ \text{oid} \ \cdot \cdot \cdot \bot \cdot \cdot \cdot \ C_X \ \text{ext} \Rightarrow \text{null} \\
\quad | \ mk C \ \text{oid} \ \cdot \cdot \cdot a_j \cdot \cdot \cdot \ C_X \ \text{ext} \Rightarrow f (\lambda x. \ \bot, \underline{x}_j) \ a) \quad (2.18)
\]

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:

\[
\text{definition in_pre_state} = \text{fst} \quad \text{first component} \\
\text{definition in_post_state} = \text{snd} \quad \text{second component} \quad (2.19)
\]

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:

\[
\text{definition } \_\text{getBase} :: C \Rightarrow A_{\text{base}} \\
\text{where } X.\text{getBase} = \text{eval_extract } X (\text{deref_oid}_C \ \text{in_post_state}} \\
\quad (\text{select_getBase } \text{reconst_basetype}) \quad (2.20)
\]

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:

\[
\text{definition } \_\text{getObject} :: C \Rightarrow A_{\text{object}} \\
\text{where } X.\text{getObject} = \text{eval_extract } X (\text{deref_oid}_C \ \text{in_post_state}} \\
\quad (\text{select_getObject } (\text{deref_oid}_C \ \text{in_post_state})) \quad (2.21)
\]
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 \( \text{in}_{\text{post}_\text{state}} \) is replaced by \( \text{in}_{\text{pre}_\text{state}} \).

Examples for the construction of accessors via associations can be found in Section 6.1.8, the construction of accessors via attributes in Section 7.1.8. The construction of casts and type tests \( \text{oclIsTypeOf()} \) and \( \text{oclIsKindOf()} \) is similarly.

In the following, we discuss the role of multiplicities on the types of the accessors. Depending on the specified multiplicity, the evaluation of an attribute can yield just a value (multiplicity \( 0..1 \) or \( 1 \)) or a collection type like 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 \( \text{null} \) to indicate an absence of value.

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

```ocl
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 \( \text{null} \) can belong to this collection. The OCL standard states that \( \text{null} \) can be owned by collections. However, if an attribute can evaluate to a collection containing \( \text{null} \), it is not clear how multiplicity constraints should be interpreted for this attribute. The question arises whether the \( \text{null} \) element should be counted or not when determining the cardinality of the collection. Recall that \( \text{null} \) denotes the absence of value in the case of a cardinality upper bound of one, so we would assume that \( \text{null} \) is not counted. On the other hand, the operation \( \text{size} \) defined for collections in OCL does count \( \text{null} \).

We propose to resolve this dilemma by regarding multiplicities as optional. This point of view complies with the UML standard, that does not require lower and upper bounds.
to be defined for multiplicities. In case a multiplicity is specified for an attribute, i.e., a lower and an upper bound are provided, we require 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 \( \mathbf{a} \) be an attribute of a class \( \mathbf{C} \) 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 \( \mathbf{a} \) to be equivalent to the following invariants written in OCL:

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

If the upper bound \( n \) is infinite, the second invariant is omitted. For the definition of these invariants we are making use of the conversion of single values to sets described in Section 2.5.2. If \( n \leq 1 \), the attribute \( \mathbf{a} \) 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 \( \mathbf{a} \) 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 \( \mathbf{T}.\text{allInstances()} \) is straightforward; the only difference is the property of the UML standard does define a default bound of one in case a lower or upper bound is not specified.

\[3\]
“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

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

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

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

where \( X' = I[[X]](\sigma, \sigma') \) and \( M = (\text{dom } \sigma \cap \text{dom } \sigma') - \{\text{OidOf } x | x \in X' \} \). Thus, if we require in a postcondition \( \text{Set{}} \rightarrow \text{oclIsModifiedOnly}() \) 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 \text{isQuery} property is true. So, whenever we have \( \tau \models X \rightarrow \text{excluding}(s.a) \rightarrow \text{oclIsModifiedOnly}() \) and \( \tau \models X \rightarrow \text{forAll}(\text{not} \rightarrow (x \neq s.a)) \), 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 \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 \@{\text{thm } "\text{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., \text{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.
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 (\lfloor (\cdot) \rfloor)
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 (\lfloor (\cdot) \rfloor)
where drop-lift [simp]: [[v]] = 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 \( \mathcal{A} \), and state transitions pairs of states . . .

record (\mathcal{A})state =
  heap :: oid → \mathcal{A}
  assoc\(_{s2}\) :: oid → (oid × oid) list
  assoc\(_{s3}\) :: oid → (oid × oid × oid) list
type-synonym (′A)st = ′A state × ′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 $\text{Set}\{\text{Set}\{2\},\text{null}\}$, 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 which assures that the invalid element is not allowed inside the collection; all raw-collections of this form were identified with the invalid element itself. The construction requires that the new collection type is not comparable with the raw-types (consisting of nested option type constructions), such that the data-invariant must be expressed in terms of the interface. In a second step, our base-types will be shown to be instances of this interface.

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

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

```plaintext
class bot =
  fixes bot :: ′a
  assumes nonEmpty : \exists x. x \neq bot

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

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, . . .).

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

instantiation option :: (bot)null
```
begin
  definition null-option-def: (null::'a::bot option) ≡ | bot |
instance (proof)
end

instantiation fun :: (type,bot) bot
begin
  definition bot-fun-def: bot ≡ (λ x. bot)
  instance (proof)
end

instantiation fun :: (type,null) null
begin
  definition null-fun-def: (null::'a ⇒ 'b::null) ≡ (λ x. null)
  instance (proof)
end

A trivial consequence of this adaption of the interface is that abstract and concrete versions of null are the same on base types (as could be expected).

3.1.5. The Semantic Space of OCL Types: Valuations

Valuations are now functions from a state pair (built upon data universe 'A) to an arbitrary null-type (i.e., containing at least a distinguished null and invalid element).

type-synonym ('A,'α) val = 'A st ⇒ 'α::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 ⇒ 'a (I J - K)
where I J x K ≡ 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 :: ('A,'α::bot) val
where invalid ≡ λ τ. bot

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

lemma textbook-invalid: I[invalid]τ = bot
Note that the definition:

\[
\text{null} :: (\forall A, \alpha::\text{null}) \text{ val}
\]

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:

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

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:

\[
\text{type-synonym } (\forall A) \text{Boolean} = (\forall A, \text{bool option option}) \text{ val}
\]

3.2.1. Basic Constants

\[
\text{lemma bot-Boolean-def : } (\text{bot}::(\forall A) \text{Boolean}) = (\lambda \tau. \bot)
\]

\[
\text{lemma null-Boolean-def : } (\text{null}::(\forall A) \text{Boolean}) = (\lambda \tau. \bot)
\]

\[
\text{definition true :: } (\forall A) \text{Boolean} \quad \text{where} \quad \text{true} \equiv \lambda \tau. [[[True]]]
\]

\[
\text{definition false :: } (\forall A) \text{Boolean} \quad \text{where} \quad \text{false} \equiv \lambda \tau. [[[False]]]
\]

\[
\text{lemma bool-split: } X \tau = \text{invalid} \tau \lor X \tau = \text{null} \tau \lor X \tau = \text{true} \tau \lor X \tau = \text{false} \tau
\]

\[
\text{lemma [simp]: } \text{false} (a, b) = [[[False]]]
\]

\[
\text{lemma [simp]: } \text{true} (a, b) = [[[True]]]
\]

\[
\text{lemma textbook-true: } I[[true]] \tau = [[[True]]]
\]
lemma textbook-false: $I[\text{false}] \, \tau = \lfloor \lfloor \text{False} \rfloor \rfloor$

\begin{table}[h]
\centering
\begin{tabular}{ll}
\hline
Name & Theorem \\
\hline
textbook-invalid & $I[\text{invalid}] \, \tau = \text{OCL-core.bot-class.bot}$ \\
textbook-null-fun & $I[\text{null}] \, \tau = \text{null}$ \\
textbook-true & $I[\text{true}] \, \tau = \lfloor \lfloor \text{True} \rfloor \rfloor$ \\
textbook-false & $I[\text{false}] \, \tau = \lfloor \lfloor \text{False} \rfloor \rfloor$
\hline
\end{tabular}
\caption{Basic semantic constant definitions of the logic (except null)}
\end{table}

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 :: ($'A', 'a::null)val \Rightarrow ('A)Boolean (v - [100]100)$
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: $(v \ X) \ \tau = (v \ (\lambda - . \ X \tau)) \ \tau$ (proof)

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

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]: \( \delta \) \( \text{null} = \text{false} \)  
(\text{proof})

lemma defined3[simp]: \( \delta \) \( \text{true} = \text{true} \)  
(\text{proof})

lemma defined4[simp]: \( \delta \) \( \text{false} = \text{true} \)  
(\text{proof})

lemma defined5[simp]: \( \delta \) \( X = \text{true} \)  
(\text{proof})

lemma defined6[simp]: \( \delta \) \( \text{\( X \)} = \text{true} \)  
(\text{proof})

lemma cp-defined: \( \delta \) \( X \) \( \tau = (\delta (\lambda \ - \ X \) \tau) \) \( \tau \)  
(\text{proof})

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

lemma textbook-defined: \( I \) \( J \) \( \delta \) \( X \) \( K \) \( \tau = \begin{cases} \text{\( I \) \( J \) \( \text{\( X \)} \) \( K \) \( \tau = \text{\( I \) \( J \)} \text{\( \bot \)} \) \( K \) \( \tau \)} & \text{\( \text{\( I \) \( J \)} \text{\( \text{\( X \)} \) \( K \) \( \tau = \text{\( I \) \( J \)} \text{\( \text{null} \)} \) \( K \) \( \tau \)}} \\ \text{\( I \) \( J \) \( \text{\( false \)} \) \( K \) \( \tau \)} & \text{\( \text{\( I \) \( J \)} \text{\( \text{true} \)} \) \( K \) \( \tau \)}} \end{cases} 
(\text{proof})

lemma textbook-valid: \( I \) \( J \) \( \text{\( \nu \)} \) \( X \) \( K \) \( \tau = \begin{cases} \text{\( I \) \( J \) \( \text{\( \nu \)} \) \( \text{\( X \)} \) \( K \) \( \tau = \text{\( I \) \( J \)} \text{\( \text{\( bot-class \)} \) \( \text{\( \text{bot} \)} \) \( \text{\( \text{null} \)} \) \( K \) \( \tau \)}} \\ \text{\( I \) \( J \) \( \text{\( false \)} \) \( K \) \( \tau \)} & \text{\( \text{\( I \) \( J \)} \text{\( \text{true} \)} \) \( K \) \( \tau \)}} \end{cases} 
(\text{proof})

\begin{table}[h]
\begin{tabular}{|c|c|}
\hline
Name & Theorem \\
\hline
\textit{textbook-defined} & \( I[\delta(X)] \tau = (\text{if \( I[X] \tau = I[\text{\( \text{bot} \)}] \tau \) \lor I[X] \tau = I[\text{\( \text{null} \)}] \tau} \\
& \text{\( \text{then \( I[\text{\( false \)}] \tau \) \text{else \( I[\text{\( true \)}] \tau \)}} \)) \\
\textit{textbook-valid} & \( I[\nu(X)] \tau = (\text{if \( I[X] \tau = I[\text{\( \text{\( bot-class \)} \) \( \text{\( \text{bot} \)} \) \( \text{\( bot \)} \) \( \text{null} \)} \) \( \text{null} \)} \( \tau \) \text{then \( I[\text{\( false \)}] \tau \) \text{else \( I[\text{\( true \)}] \tau \)}} \)) \\
\hline
\end{tabular}
\caption{Table 3.2.: Basic predicate definitions of the logic.}
\end{table}
3.3. The Equalities of OCL

The OCL contains a particular version of equality, written in Standard documents \( = \) and \( <> \) for its negation, which is referred as weak referential equality hereafter and for which we use the symbol \( \triangleq \) 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 \( a.boss \triangleq b.boss@pre \) instead of

   \[
   \begin{align*}
   a.boss &\triangleq b.boss@pre \quad \text{and} \quad (\ast \text{just the pointers are equal!} \ast) \\
   a.boss.name &\triangleq b.boss@pre.name@pre \\
   a.boss.age &\triangleq b.boss@pre.age@pre
   \end{align*}
   \]

   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

---

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Theorem</th>
</tr>
</thead>
<tbody>
<tr>
<td>defined1</td>
<td>( \delta ) invalid = false</td>
</tr>
<tr>
<td>defined2</td>
<td>( \delta ) null = false</td>
</tr>
<tr>
<td>defined3</td>
<td>( \delta ) true = true</td>
</tr>
<tr>
<td>defined4</td>
<td>( \delta ) false = true</td>
</tr>
<tr>
<td>defined5</td>
<td>( \delta ) (?X = true</td>
</tr>
<tr>
<td>defined6</td>
<td>( \delta ) (?X = true</td>
</tr>
</tbody>
</table>
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” $\alpha \cdot \alpha \to \text{bool}$—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:

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

(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.

\[
\text{definition } \text{StrongEq} ::= \forall st \Rightarrow \forall a \Rightarrow (\forall) \text{Boolean} \quad (\text{infixl } \triangleq 30)
\]

\[
\text{where } X \triangleq Y \equiv \lambda \tau. \ [X \tau = Y \tau]
\]

From this follow already elementary properties like:

\[
\text{lemma } [\text{simp}, \text{code-unfold}] : (\text{true } \triangleq \text{false}) = \text{false} \\
\langle \text{proof} \rangle
\]

\[
\text{lemma } [\text{simp}, \text{code-unfold}] : (\text{false } \triangleq \text{true}) = \text{false} \\
\langle \text{proof} \rangle
\]

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.

\[
\text{consts } \text{StrictRefEq} ::= \forall (\forall a)\text{val}, (\forall a)\text{val} \Rightarrow (\forall) \text{Boolean} \quad (\text{infixl } \triangleq 30)
\]
Here is a first instance of a definition of weak equality—for the special case of the type \( \mathbb{A} \) Boolean, it is just the strict extension of the logical equality:

\[
\text{defs (overloaded) } \text{StrictRefEq}_{\text{Boolean}}[\text{code-unfold}] : \\
(x: (\mathbb{A})\text{Boolean}) \equiv y \equiv \lambda \tau. \text{if } (\nu x) \tau = \text{true } \tau \land (\nu y) \tau = \text{true } \tau \\
\text{then } (x \equiv y) \tau \text{ else invalid } \tau
\]

which implies elementary properties like:

\[
\text{lemma [simp,code-unfold]} : (\text{true} \equiv \text{false}) = \text{false} \\
\langle \text{proof} \rangle
\]

\[
\text{lemma [simp,code-unfold]} : (\text{false} \equiv \text{true}) = \text{false} \\
\langle \text{proof} \rangle
\]

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

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

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

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

\[
\text{lemma [simp,code-unfold]} : ((\text{invalid}: (\mathbb{A})\text{Boolean}) \equiv \text{invalid}) = \text{invalid} \\
\langle \text{proof} \rangle
\]

Thus, the weak equality is not reflexive.

\[
\text{lemma null-non-false [simp,code-unfold]} : (\text{null} \equiv \text{false}) = \text{false} \\
\langle \text{proof} \rangle
\]

\[
\text{lemma null-non-true [simp,code-unfold]} : (\text{null} \equiv \text{true}) = \text{false} \\
\langle \text{proof} \rangle
\]

\[
\text{lemma false-non-null [simp,code-unfold]} : (\text{false} \equiv \text{null}) = \text{false} \\
\langle \text{proof} \rangle
\]

\[
\text{lemma true-non-null [simp,code-unfold]} : (\text{true} \equiv \text{null}) = \text{false} \\
\langle \text{proof} \rangle
\]

### 3.3.2. Fundamental Predicates on Strong Equality

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

\[
\text{lemma StrongEq-refl [simp]} : (X \triangleq X) = \text{true} \\
\langle \text{proof} \rangle
\]

\[
\text{lemma StrongEq-sym} : (X \triangleq Y) = (Y \triangleq X) \\
\langle \text{proof} \rangle
\]
lemma \textit{StrongEq-trans-strong} \ [\textit{simp}]:
\begin{align*}
\text{assumes } & A: (X \triangleq Y) = \text{true} \\
\text{and } & B: (Y \triangleq Z) = \text{true} \\
\text{shows } & (X \triangleq Z) = \text{true}
\end{align*}
\langle \text{proof} \rangle

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 \textit{context-
passing} or \textit{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:

\begin{align*}
\text{lemma } \textit{StrongEq-subst} \ : \\
\text{assumes } & cp: \ \forall X. P(X) \tau = P(\lambda \cdot X \tau) \\
\text{and } & eq: (X \triangleq Y) \tau = \text{true} \\
\text{shows } & (P X \triangleq P Y) \tau = \text{true}
\end{align*}
\langle \text{proof} \rangle

\begin{align*}
\text{lemma } \textit{defined7} \ [\textit{simp}]: & \ \delta (X \triangleq Y) = \text{true} \\
\langle \text{proof} \rangle
\end{align*}

\begin{align*}
\text{lemma } \textit{valid7} \ [\textit{simp}]: & \ \upsilon (X \triangleq Y) = \text{true} \\
\langle \text{proof} \rangle
\end{align*}

\begin{align*}
\text{lemma } \textit{cp-StrongEq} : & \ (X \triangleq Y) \tau = ((\lambda \cdot X \tau) \triangleq (\lambda \cdot Y \tau)) \tau
\end{align*}
\langle \text{proof} \rangle

\section*{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 that 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 \textit{invalid}
as least, \textit{null} as middle and \textit{true} resp. \textit{false} as unrelated top-elements.

\textbf{definition} \textit{OclNot} \ :: \ (\forall)\textit{Boolean} \Rightarrow \ (\forall)\textit{Boolean} \ (\textit{not})
where \( \text{not} \ X \equiv \lambda \tau . \text{case} \ X \ \tau \ \text{of} \)
\[
\bot \Rightarrow \bot \\
| \bot \Rightarrow | \bot \\
| x \Rightarrow | \neg x \\
\]

with term "not" we can express the notation:

**syntax**
\[
\text{notequal} \quad :: \ (\forall) \text{Boolean} \Rightarrow (\forall) \text{Boolean} \Rightarrow (\forall) \text{Boolean} \quad (\text{infix} <> 40)
\]

**translations**
\[
a <> b \iff \text{CONST OclNot}( a \equiv b)
\]

**lemma** cp-OclNot: \((\text{not} \ X)\tau = (\text{not} \ (\lambda \ -. \ X \ \tau)) \ \tau \)
\[
\langle \text{proof} \rangle
\]

**lemma** OclNot1[simp]: \(\text{not} \ \text{invalid} = \text{invalid} \)
\[
\langle \text{proof} \rangle
\]

**lemma** OclNot2[simp]: \(\text{not} \ \text{null} = \text{null} \)
\[
\langle \text{proof} \rangle
\]

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

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

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

**lemma** OclNot-inject: \(\ \forall \ x \ y. \ \text{not} \ x = \text{not} \ y \Rightarrow x = y \)
\[
\langle \text{proof} \rangle
\]

**definition** OclAnd :: \((\forall) \text{Boolean}, (\forall) \text{Boolean}] \Rightarrow (\forall) \text{Boolean} \quad (\text{infix} \ \text{and} 30) \)
where \( X \ \text{and} \ Y \equiv (\lambda \tau. \ \text{case} \ X \ \tau \ \text{of} \)
\[
[[\text{False}]] \Rightarrow [[\text{False}]] \\
| \bot \Rightarrow (\text{case} \ Y \ \tau \ \text{of} \\
| [[\text{False}]] \Rightarrow [[\text{False}]] \\
| \bot \Rightarrow \bot \\
| x \Rightarrow [[\neg x]] \\
| [[\text{True}]] \Rightarrow Y \ \tau)
\]

Note that \(\text{not}\) is \textit{not} defined as a strict function; proximity to lattice laws implies that we \textit{need} a definition of \(\text{not}\) that satisfies \(\text{not}(\text{not}(x))=x\).
In textbook notation, the logical core constructs \textit{not} and \textit{op and} were represented as follows:

\textbf{lemma textbook-OclNot:} \hspace{1cm} \\
\textit{not(X)} \tau = (\text{case } I[[X]] \tau \text{ of } \\
\hspace{1cm} \bot \Rightarrow \bot \\
\hspace{1cm} [\bot] \Rightarrow [\bot] \\
\hspace{1cm} [[x]] \Rightarrow [[\neg x]]) \\
\langle \text{proof} \rangle

\textbf{lemma textbook-OclAnd:} \hspace{1cm} \\
\textit{X and Y} \tau = (\text{case } I[[X]] \tau \text{ of } \\
\hspace{1cm} \bot \Rightarrow (\text{case } I[[Y]] \tau \text{ of } \\
\hspace{1cm} \bot \Rightarrow \bot \\
\hspace{1cm} [[\bot]] \Rightarrow [\bot] \\
\hspace{1cm} [[\text{True}]] \Rightarrow [[\bot]] \\
\hspace{1cm} [[\text{False}]] \Rightarrow [[\text{False}]]) \\
\hspace{1cm} [\bot] \Rightarrow (\text{case } I[[Y]] \tau \text{ of } \\
\hspace{1cm} \bot \Rightarrow (\text{case } I[[X]] \tau \text{ of } \\
\hspace{1cm} [\bot] \Rightarrow [\bot] \\
\hspace{1cm} [[\text{True}]] \Rightarrow [\bot] \\
\hspace{1cm} [[\text{False}]] \Rightarrow [[\text{True}]]) \\
\hspace{1cm} [[\text{False}]] \Rightarrow (\text{case } I[[Y]] \tau \text{ of } \\
\hspace{1cm} [\bot] \Rightarrow (\text{case } I[[X]] \tau \text{ of } \\
\hspace{1cm} [[\bot]] \Rightarrow [\bot] \\
\hspace{1cm} [[\text{False}]] \Rightarrow [[\text{True}]])) \\
\langle \text{proof} \rangle

\textbf{definition OclOr :: } ([\forall A] \text{Boolean}, ([\forall A] \text{Boolean}) \Rightarrow ([\forall A] \text{Boolean}) \text{ (infixl or 25)} \\
\text{where } X \text{ or Y } \equiv \text{not(not X and not Y)}

\textbf{definition OclImplies :: } ([\forall A] \text{Boolean}, ([\forall A] \text{Boolean}) \Rightarrow ([\forall A] \text{Boolean}) \text{ (infixl implies 25)} \\
\text{where } X \text{ implies Y } \equiv \text{not X or Y}

\textbf{lemma cp-OclAnd:} (X and Y) \tau = ((\lambda \cdot X \tau) \text{ and } (\lambda \cdot Y \tau)) \tau \\
\langle \text{proof} \rangle

\textbf{lemma cp-OclOr:} (X::([\forall A] \text{Boolean}) or Y) \tau = ((\lambda \cdot X \tau) or (\lambda \cdot Y \tau)) \tau \\
\langle \text{proof} \rangle

\textbf{lemma cp-OclImplies:} (X implies Y) \tau = ((\lambda \cdot X \tau) \text{ implies } (\lambda \cdot Y \tau)) \tau \\
\langle \text{proof} \rangle

\textbf{lemma OclAnd1[simp]:} (invalid and true) = invalid \\
\langle \text{proof} \rangle

\textbf{lemma OclAnd2[simp]:} (invalid and false) = false \\
\langle \text{proof} \rangle

\textbf{lemma OclAnd3[simp]:} (invalid and null) = invalid \\
\langle \text{proof} \rangle
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]: \( \forall \tau. X \tau \neq \text{false} \implies (\text{bot and } X) \tau = \text{bot } \tau \)
(\proof)

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

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

lemma OclAnd-null2 [simp]: \( \forall \tau. X \tau \neq \text{false} \implies X \tau \neq \text{bot} \implies (X \text{ and } \text{null}) \tau = \text{null } \tau \)
(\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]: \((Y \text{ or } \text{false}) = Y\)
(\proof)

lemma OclOr-true1 [simp]: \((\text{true or } Y) = \text{true}\)
(\proof)
lemma OclOr-true2: \( (Y \text{ or true}) = \text{true} \)

⟨proof⟩

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

⟨proof⟩

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

⟨proof⟩

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

⟨proof⟩

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

⟨proof⟩

lemma OclOr-assoc: \( (X \text{ or } (Y \text{ or } Z)) = (X \text{ or } Y \text{ or } Z) \)

⟨proof⟩

lemma OclImplies-true: \( (X \text{ implies true}) = \text{true} \)

⟨proof⟩

lemma deMorgan1: \( \neg(X \text{ and } Y) = (\neg X \text{ or } \neg Y) \)

⟨proof⟩

lemma deMorgan2: \( \neg(X \text{ or } Y) = (\neg X \text{ and } \neg Y) \)

⟨proof⟩

3.5. A Standard Logical Calculus for OCL

definition OclValid :: \( \forall st, \forall Boolean \Rightarrow \text{bool} \ ((\_ / \_ / \_)) 50 \)

where \( \tau \vdash P \equiv ((P \tau) = \text{true} \tau) \)

value \( \tau \vdash \text{true} <> \text{false} \)

value \( \tau \vdash \text{false} <> \text{true} \)

3.5.1. Global vs. Local Judgements

lemma transform1: \( P = \text{true} \implies \tau \vdash P \)

⟨proof⟩

lemma transform1-rev: \( \forall \tau. \ P \implies P = \text{true} \)

⟨proof⟩

lemma transform2: \( P = Q \implies ((\tau \vdash P) = (\tau \vdash Q)) \)

⟨proof⟩

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

51
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 $\tau \models P \implies \tau \models Q$

**3.5.2. Local Validity and Meta-logic**

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

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

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

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

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

$(\tau \models (x \equiv invalid)) \lor (\tau \models (x \equiv null)) \lor (\tau \models (x \equiv true)) \lor (\tau \models (x \equiv false))$

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

$(\tau \models \delta x) = ((\neg (\tau \models (x \equiv invalid))) \land (\neg (\tau \models (x \equiv null))))$

**lemma** *foundation5*:

$\tau \models (P and Q) \implies (\tau \models P) \land (\tau \models Q)$

**lemma** *foundation6*:

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

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

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

**lemma** *foundation7’*[simp]:

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

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:**
\[(\tau \models \delta x) \lor (\tau \models (x \triangleq \text{invalid})) \lor (\tau \models (x \triangleq \text{null}))\]

**Proof**

**Lemma foundation9:**
\[\tau \models \delta x \Rightarrow (\tau \models \text{not } x) = (\neg (\tau \models x))\]

**Proof**

**Lemma foundation10:**
\[\tau \models \delta x \Rightarrow \tau \models \delta y \Rightarrow (\tau \models (x \text{ and } y)) = ( (\tau \models x) \land (\tau \models y))\]

**Proof**

**Lemma foundation11:**
\[\tau \models \delta x \Rightarrow \tau \models \delta y \Rightarrow (\tau \models (x \text{ or } y)) = ( (\tau \models x) \lor (\tau \models y))\]

**Proof**

**Lemma foundation12:**
\[\tau \models \delta x \Rightarrow \tau \models \delta y \Rightarrow (\tau \models (x \text{ implies } y)) = ( (\tau \models x) \rightarrow (\tau \models y))\]

**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:**
\[\tau \models A \triangleq \text{invalid} = (\tau \models \text{not}(\nu A))\]

**Proof**

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

**Proof**

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

**Proof**

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

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

**Lemma foundation18:**
\[\tau \models (\nu X) = (X \tau \neq \text{invalid} \tau)\]
lemma foundation18: \( \tau \models (\nu X) = (X \tau \neq \text{bot}) \)

lemmas foundation19 = foundation18[TTHEN iffD1]

lemma foundation20: \( \tau \models (\delta X) \implies \tau \models \nu X \)

lemma foundation21: \( (\text{not } A \triangleq \text{not } B) = (A \triangleq B) \)

lemma foundation22: \( (\tau \models (X \triangleq Y)) = (X \tau = Y \tau) \)

lemma foundation23: \( (\tau \models P) = (\tau \models (\lambda - . P \tau)) \)

lemmas cp-validity=foundation23

lemma foundation24: \( (\tau \models \text{not}(X \triangleq Y)) = (X \tau \neq Y \tau) \)

lemma defined-not-I : \( \tau \models \delta (x) \implies \tau \models \delta (\text{not } x) \)

lemma valid-not-I : \( \tau \models \nu (x) \implies \tau \models \nu (\text{not } x) \)

lemma defined-and-I : \( \tau \models \delta (x) \implies \tau \models \delta (y) \implies \tau \models \delta (x \text{ and } y) \)

lemma valid-and-I : \( \tau \models \nu (x) \implies \tau \models \nu (y) \implies \tau \models \nu (x \text{ and } y) \)

3.5.3. Local Judgements and Strong Equality

lemma StrongEq-L-refl: \( \tau \models (x \triangleq x) \)

lemma StrongEq-L-sym: \( \tau \models (x \triangleq y) \implies \tau \models (y \triangleq x) \)

lemma StrongEq-L-trans: \( \tau \models (x \triangleq y) \implies \tau \models (y \triangleq z) \implies \tau \models (x \triangleq z) \)
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',\alpha) val ⇒ (\A',\beta) val) ⇒ bool

where cp P ≡ (∃ f. ∀ X \tau. P X \tau = f (X \tau) \tau)

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

lemma StrongEq-L-subst1: \( \forall \tau. cp P \Longrightarrow \tau \models (x \triangleleft y) \Longrightarrow \tau \models (P x \triangleleft P y) \)

lemma StrongEq-L-subst2: \( \forall \tau. cp P \Longrightarrow \tau \models (x \triangleleft y) \Longrightarrow \tau \models (P x) \models (P y) \)

lemma StrongEq-L-subst2-rev: \( \tau \models y \triangleleft x \Longrightarrow \tau \models (P x) \models (P y) \)

lemma StrongEq-L-subst3: assumes cp: cp P and eq: \( \tau \models x \triangleleft y \)

shows \( (\tau \models P x) = (\tau \models P y) \)

lemma cpI1: \( (\forall X \tau. f X \tau = f(\lambda -. X \tau) \tau) \Longrightarrow cp P \Longrightarrow cp(\lambda X. f (P X)) \)

lemma cpI2: \( (\forall X Y \tau. f X Y \tau = f(\lambda -. X \tau)(\lambda -. Y \tau) \tau) \Longrightarrow cp P \Longrightarrow cp Q \Longrightarrow cp(\lambda X. f (P X) (Q X)) \)

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

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

lemma cp-const: \( cp(\lambda -. c) \)
lemma cp-id : cp(λX. 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 (δ-closure)

For the logical connectives, we have — beyond ?τ ↔ ?P ⇒ ?τ = δ ?P — the following facts:

lemma OclNot-defargs:
τ |= (not P) ⇒ τ = δ P
⟨proof⟩

lemma OclNot-contrapos-nn:
assumes τ |= δ A
assumes τ |= not B
assumes τ |= A ⇒ τ |= B
shows τ |= 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 :: [(∀A)Boolean , (A,α::null) val, (A,α) val] ⇒ (A,α) val
(if (-) then (-) else (-) endif [10,10,10]50)
where (if C then B1 else B2 endif) = (λ τ. if (δ C) τ = true τ
ten (if (C τ) = true τ
then B1 τ
else B2 τ)
else invalid τ)

lemma cp-OclIf:((if C then B1 else B2 endif) τ =
(if (λ -. C τ) then (λ -. B1 τ) else (λ -. B2 τ) endif) τ)

56
lemmas cp-intro' [intro!, simp, code-unfold] =
  cp-intro
  cp-OclIf[THEN allI[THEN allI[THEN allI[THEN allI[THEN cpI]]]], of OclIf]

lemma OclIf-invalid [simp]: (if invalid then B₁ else B₂ endif) = invalid
  ⟨proof⟩

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

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

lemma OclIf-true' [simp]: τ \models P \implies (if P then B₁ else B₂ endif)τ = B₁ τ
  ⟨proof⟩

lemma OclIf-false [simp]: (if false then B₁ else B₂ endif) = B₂
  ⟨proof⟩

lemma OclIf-false' [simp]: τ \models not P \implies (if P then B₁ else B₂ endif)τ = B₂ τ
  ⟨proof⟩

lemma OclIf-idem1 [simp]: (if δ X then A else A endif) = A
  ⟨proof⟩

lemma OclIf-idem2 [simp]: (if ν 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 ≡ ∀ τ τ'. X τ = X τ'

lemma const-charn: const X \implies X τ = X τ'
  ⟨proof⟩

lemma const-subst:
  assumes const-X: const X
    and const-Y: const Y
    and eq : X τ = Y τ
    and cp-P: cp P
    and pp : P Y τ = P Y τ'

  ⟨proof⟩
shows $P \times \tau = P \times \tau'$

\text{lemma} const-imply2:
\text{assumes} \bigwedge\tau_1 \tau_2, P \tau_1 = P \tau_2 \Rightarrow Q \tau_1 = Q \tau_2
\text{shows} \text{const } P \Rightarrow \text{const } Q

\text{lemma} const-imply3:
\text{assumes} \bigwedge\tau_1 \tau_2, P \tau_1 = P \tau_2 \Rightarrow Q \tau_1 = Q \tau_2 \Rightarrow R \tau_1 = R \tau_2
\text{shows} \text{const } P \Rightarrow \text{const } Q \Rightarrow \text{const } R

\text{lemma} const-imply4:
\text{assumes} \bigwedge\tau_1 \tau_2, P \tau_1 = P \tau_2 \Rightarrow Q \tau_1 = Q \tau_2 \Rightarrow R \tau_1 = R \tau_2 \Rightarrow S \tau_1 = S \tau_2
\text{shows} \text{const } P \Rightarrow \text{const } Q \Rightarrow \text{const } R \Rightarrow \text{const } S

\text{lemma} const-lam: \text{const } (\lambda-.e)
\text{lemma} const-true: \text{const } true
\text{lemma} const-false: \text{const } false
\text{lemma} const-null: \text{const } null
\text{lemma} const-invalid: \text{const } invalid
\text{lemma} const-bot: \text{const } bot

\text{lemma} const-defined:
\text{assumes} \text{const } X
\text{shows} \text{const } (\delta X)
\text{lemma} const-valid:
\text{assumes} \text{const } X
\text{shows} \text{const } (\nu X)
lemma const-OclValid1:
assumes const x
shows \((\tau \models x) = (\tau' \models x)\)
\langle proof \rangle

lemma const-OclValid2:
assumes const x
shows \((\tau \models x) = (\tau' \models x)\)
\langle proof \rangle

lemma const-OclAnd :
assumes const X
assumes const X'
shows const (X and X')
\langle proof \rangle

lemma const-OclNot :
assumes const X
shows const (not X)
\langle proof \rangle

lemma const-OclOr :
assumes const X
assumes const X'
shows const (X or X')
\langle proof \rangle

lemma const-OclImplies :
assumes const X
assumes const X'
shows const (X implies X')
\langle proof \rangle

lemma const-StrongEq:
assumes const X
assumes const X'
shows const (X \triangleq X')
\langle proof \rangle

lemma const-OclIf :
assumes const B
and const C1
and const C2
shows const (if B then C1 else C2 endif)
\langle proof \rangle
lemmas \texttt{const-ss} = \texttt{const-bot} \texttt{const-null} \texttt{const-invalid} \texttt{const-false} \texttt{const-true} \texttt{const-lam} \texttt{const-defined} \texttt{const-valid} \texttt{const-StrongEq} \texttt{const-OclNot} \texttt{const-OclAnd} \texttt{const-OclOr} \texttt{const-OclImplies} \texttt{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 = (λ - . [0::int])

definition OclInt1 ::('A) Integer (1)
where 1 = (λ - . [1::int])

definition OclInt2 ::('A) Integer (2)
where 2 = (λ - . [2::int])

definition OclInt3 ::('A) Integer (3)
where 3 = (λ - . [3::int])

definition OclInt4 ::('A) Integer (4)
where 4 = (λ - . [4::int])

definition $OclInt5 :: (∀) Integer (5)$
where $5 = (λ \cdot \lfloor \lfloor 5 :: int \rfloor \rfloor)$

definition $OclInt6 :: (∀) Integer (6)$
where $6 = (λ \cdot \lfloor \lfloor 6 :: int \rfloor \rfloor)$

definition $OclInt7 :: (∀) Integer (7)$
where $7 = (λ \cdot \lfloor \lfloor 7 :: int \rfloor \rfloor)$

definition $OclInt8 :: (∀) Integer (8)$
where $8 = (λ \cdot \lfloor \lfloor 8 :: int \rfloor \rfloor)$

definition $OclInt9 :: (∀) Integer (9)$
where $9 = (λ \cdot \lfloor \lfloor 9 :: int \rfloor \rfloor)$

definition $OclInt10 :: (∀) Integer (10)$
where $10 = (λ \cdot \lfloor \lfloor 10 :: int \rfloor \rfloor)$

4.1.3. Validity and Definedness Properties

lemma $δ(\text{null} :: (∀) Integer) = \text{false}$ (proof)

lemma $ν(\text{null} :: (∀) Integer) = \text{true}$ (proof)

lemma [simp, code-unfold]: $δ (λ \cdot \lfloor [n] \rfloor) = \text{true}$ (proof)

lemma [simp, code-unfold]: $ν (λ \cdot \lfloor [n] \rfloor) = \text{true}$ (proof)

lemma [simp, code-unfold]: $δ 0 = \text{true}$ (proof)

lemma [simp, code-unfold]: $ν 0 = \text{true}$ (proof)

lemma [simp, code-unfold]: $δ 1 = \text{true}$ (proof)

lemma [simp, code-unfold]: $ν 1 = \text{true}$ (proof)

lemma [simp, code-unfold]: $δ 2 = \text{true}$ (proof)

lemma [simp, code-unfold]: $ν 2 = \text{true}$ (proof)

lemma [simp, code-unfold]: $δ 6 = \text{true}$ (proof)

lemma [simp, code-unfold]: $ν 6 = \text{true}$ (proof)

lemma [simp, code-unfold]: $δ 8 = \text{true}$ (proof)

lemma [simp, code-unfold]: $ν 8 = \text{true}$ (proof)

lemma [simp, code-unfold]: $δ 9 = \text{true}$ (proof)

lemma [simp, code-unfold]: $ν 9 = \text{true}$ (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**

\[ OclAdd_{\text{Integer}} :: (\forall \tau. \text{Integer} \Rightarrow (\forall \tau. \text{Integer} \Rightarrow (\forall \tau. \text{Integer})) \text{ (infix } ' + 40) \]

where

\[ x ' + y \equiv \lambda \tau. \text{if } (\delta x) \tau = \text{true } \tau \land (\delta y) \tau = \text{true } \tau \]

then \[ \lfloor \lfloor \lceil \lceil x \tau \rceil \rceil \rceil + \lfloor \lfloor \rceil \rceil \rceil \rceil \rceil \]

else invalid \(\tau\)

**Definition**

\[ OclLess_{\text{Integer}} :: (\forall \tau. \text{Integer} \Rightarrow (\forall \tau. \text{Integer} \Rightarrow (\forall \tau. \text{Boolean})) \text{ (infix } '< 40) \]

where

\[ x ' < y \equiv \lambda \tau. \text{if } (\delta x) \tau = \text{true } \tau \land (\delta y) \tau = \text{true } \tau \]

then \[ \lfloor \lfloor \lceil \lceil x \tau \rceil \rceil \rceil \rceil < \lfloor \lfloor \rceil \rceil \rceil \rceil \rceil \rceil \]

else invalid \(\tau\)

**Definition**

\[ OclLe_{\text{Integer}} :: (\forall \tau. \text{Integer} \Rightarrow (\forall \tau. \text{Integer} \Rightarrow (\forall \tau. \text{Boolean})) \text{ (infix } '< 40) \]

where

\[ x ' \leq y \equiv \lambda \tau. \text{if } (\delta x) \tau = \text{true } \tau \land (\delta y) \tau = \text{true } \tau \]

then \[ \lfloor \lfloor \lceil \lceil x \tau \rceil \rceil \rceil \rceil \leq \lfloor \lfloor \rceil \rceil \rceil \rceil \rceil \rceil \]

else invalid \(\tau\)

**Basic Properties**

**Lemma**

\[ OclAdd_{\text{Integer}}-\text{commute}: (X ' + Y) = (Y ' + X) \]

**Proof**

**Execution with Invalid or Null or Zero as Argument**

**Lemma**

\[ OclAdd_{\text{Integer}}-\text{strict1}[\text{simp,code-unfold}]: (x ' + invalid) = invalid \]

**Proof**

**Lemma**

\[ OclAdd_{\text{Integer}}-\text{strict2}[\text{simp,code-unfold}]: (invalid '+' x) = invalid \]

**Proof**

**Lemma**

\[ \text{simp,code-unfold}]: (x '+' null) = invalid \]

**Proof**

**Lemma**

\[ \text{simp,code-unfold}]: (null '+' x) = invalid \]

**Proof**

**Lemma**

\[ OclAdd_{\text{Integer}}-\text{zero1}[\text{simp,code-unfold}]: (x '+' 0) = (if \upsilon x \text{ and not } (\delta x) \text{ then invalid } \text{ else } x \text{ endif}) \]

**Proof**

**Lemma**

\[ OclAdd_{\text{Integer}}-\text{zero2}[\text{simp,code-unfold}]: (0 '+' x) = (if \upsilon x \text{ and not } (\delta x) \text{ then invalid } \text{ else } x \text{ endif}) \]

**Proof**

**Context Passing**

**Lemma**

\[ cp-OclAdd_{\text{Integer}}:(X ' + Y) \tau = ((\lambda - X \tau) ' + (\lambda - Y \tau)) \tau \]

**Proof**
lemma cp-OclLessInteger: \((X '≺ Y) \tau = ((\lambda \, X \, \tau) '≺ (\lambda \, Y \, \tau)) \tau\)  
\langle \text{proof} \rangle

lemma cp-OclLeInteger: \((X '≤ Y) \tau = ((\lambda \, X \, \tau) '≤ (\lambda \, Y \, \tau)) \tau\)  
\langle \text{proof} \rangle

**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`.

\[
\begin{align*}
\text{value } \tau \models (9 '≤ 10) \\
\text{value } \tau \models ((4 '↑ 4) '≤ 10) \\
\text{value } \neg(\tau \models ((4 '↑ (4 '↑ 4)) '≺ 10)) \\
\text{value } \tau \models \neg(v (\text{null} '↑ 1))
\end{align*}
\]

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 `∀ Boolean-case as strict extension of the strong equality:

defs (overloaded) StrictRefEq_{\text{Integer}}: 
\begin{align*}
(x::(\forall) \text{Integer}) \equiv y \equiv \lambda \tau. \text{ if } (v \, x) \tau = \text{true } \tau \land (v \, y) \tau = \text{true } \tau \\
\text{then } (x \equiv y) \tau \\
\text{else invalid } \tau
\end{align*}
\]

\[
\begin{align*}
\text{value } \tau \models 1 '≺ 2 \\
\text{value } \tau \models 2 '≺ 1 \\
\text{value } \tau \models 2 '≡ 2
\end{align*}
\]

4.2.2. Logic and Algebraic Layer on Basic Types

Validity and Definedness Properties (I)

**lemma** StrictRefEq_{\text{Boolean-defined-args-valid}}: 
\[
(\tau \models \delta((x::(\forall) \text{Boolean}) \equiv y)) = ((\tau \models (v \, x)) \land (\tau \models (v \, y)))
\]
\langle \text{proof} \rangle

**lemma** StrictRefEq_{\text{Integer-defined-args-valid}}: 
\[
(\tau \models \delta((x::(\forall) \text{Integer}) \equiv y)) = ((\tau \models (v \, x)) \land (\tau \models (v \, y)))
\]
\langle \text{proof} \rangle

Validity and Definedness Properties (II)

**lemma** StrictRefEq_{\text{Boolean-defargs}}: 
\[
(\tau \models ((x::(\forall) \text{Boolean}) \equiv y)) \implies (\tau \models (v \, x)) \land (\tau \models (v \, y))
\]
\begin{proof}

\textbf{lemma} \texttt{StrictRefEq\_Integer\_defargs}:
\[ \tau \vDash ((x::(A)\text{Integer}) \Downarrow y) \implies (\tau \vDash (v x)) \land (\tau \vDash (v y)) \]
\end{proof}

\textbf{Validity and Definedness Properties (III) Miscellaneous}

\textbf{lemma} \texttt{StrictRefEq\_Boolean\_strict''}:
\[ \delta ((x::(A)\text{Boolean}) \Downarrow y) = (v(x) \land v(y)) \]
\end{proof}

\textbf{lemma} \texttt{StrictRefEq\_Integer\_strict''}:
\[ \delta ((x::(A)\text{Integer}) \Downarrow y) = (v(x) \land v(y)) \]
\end{proof}

\textbf{lemma} \texttt{StrictRefEq\_Integer\_strict}:
\begin{quote}
\begin{verbatim}
assumes A: v (x::(A)\text{Integer}) = true
and B: v y = true
shows v ( x \Downarrow y) = true
\end{verbatim}
\end{quote}
\end{proof}

\textbf{lemma} \texttt{StrictRefEq\_Integer\_strict'}:
\begin{quote}
\begin{verbatim}
assumes A: v ((x::(A)\text{Integer})) \Downarrow y) = true
shows v x = true \land v y = true
\end{verbatim}
\end{quote}
\end{proof}

\textbf{Reflexivity}

\textbf{lemma} \texttt{StrictRefEq\_Boolean\_refl\_simp code-unfold}:
\[ ((x::(A)\text{Boolean}) \Downarrow x) = (if (v x) then true else invalid endif) \]
\end{proof}

\textbf{lemma} \texttt{StrictRefEq\_Integer\_refl\_simp code-unfold}:
\[ ((x::(A)\text{Integer}) \Downarrow x) = (if (v x) then true else invalid endif) \]
\end{proof}

\textbf{Execution with Invalid or Null as Argument}

\textbf{lemma} \texttt{StrictRefEq\_Boolean\_strict1\_simp code-unfold}:
\[ ((x::(A)\text{Boolean}) \Downarrow \text{invalid}) = \text{invalid} \]
\end{proof}

\textbf{lemma} \texttt{StrictRefEq\_Boolean\_strict2\_simp code-unfold}:
\[ (\text{invalid} \Downarrow (x::(A)\text{Boolean})) = \text{invalid} \]
\end{proof}

\textbf{lemma} \texttt{StrictRefEq\_Integer\_strict1\_simp code-unfold}:
\[ ((x::(A)\text{Integer}) \Downarrow \text{invalid}) = \text{invalid} \]
\end{proof}

\textbf{lemma} \texttt{StrictRefEq\_Integer\_strict2\_simp code-unfold}:
\[ (\text{invalid} \Downarrow (x::(A)\text{Integer})) = \text{invalid} \]
\end{proof}

65
\langle \text{proof} \rangle

\text{lemma} \ integer-non-null \ [\text{simp}]: \ ((\lambda . \ [\lfloor n \rfloor]) \triangleright (\text{null}::(\exists \text{Integer})) \triangleright \text{false} \ \langle \text{proof} \rangle

\text{lemma} \ null-non-integer \ [\text{simp}]: \ ((\text{null}::(\exists \text{Integer})) \triangleright (\lambda . \ [\lfloor n \rfloor]) \triangleright \text{false} \ \langle \text{proof} \rangle

\text{lemma} \ OclInt0-non-null \ [\text{simp, code-unfold}]: \ (0 \div \text{null}) \triangleright \text{false} \ \langle \text{proof} \rangle
\text{lemma} \ null-non-OclInt0 \ [\text{simp, code-unfold}]: \ (\text{null} \div 0) \triangleright \text{false} \ \langle \text{proof} \rangle
\text{lemma} \ OclInt1-non-null \ [\text{simp, code-unfold}]: \ (1 \div \text{null}) \triangleright \text{false} \ \langle \text{proof} \rangle
\text{lemma} \ null-non-OclInt1 \ [\text{simp, code-unfold}]: \ (\text{null} \div 1) \triangleright \text{false} \ \langle \text{proof} \rangle
\text{lemma} \ OclInt2-non-null \ [\text{simp, code-unfold}]: \ (2 \div \text{null}) \triangleright \text{false} \ \langle \text{proof} \rangle
\text{lemma} \ null-non-OclInt2 \ [\text{simp, code-unfold}]: \ (\text{null} \div 2) \triangleright \text{false} \ \langle \text{proof} \rangle
\text{lemma} \ OclInt6-non-null \ [\text{simp, code-unfold}]: \ (6 \div \text{null}) \triangleright \text{false} \ \langle \text{proof} \rangle
\text{lemma} \ null-non-OclInt6 \ [\text{simp, code-unfold}]: \ (\text{null} \div 6) \triangleright \text{false} \ \langle \text{proof} \rangle
\text{lemma} \ OclInt8-non-null \ [\text{simp, code-unfold}]: \ (8 \div \text{null}) \triangleright \text{false} \ \langle \text{proof} \rangle
\text{lemma} \ null-non-OclInt8 \ [\text{simp, code-unfold}]: \ (\text{null} \div 8) \triangleright \text{false} \ \langle \text{proof} \rangle
\text{lemma} \ OclInt9-non-null \ [\text{simp, code-unfold}]: \ (9 \div \text{null}) \triangleright \text{false} \ \langle \text{proof} \rangle
\text{lemma} \ null-non-OclInt9 \ [\text{simp, code-unfold}]: \ (\text{null} \div 9) \triangleright \text{false} \ \langle \text{proof} \rangle

\text{Const}
\text{lemma} \ [\text{simp, code-unfold}]: \ const(0) \ \langle \text{proof} \rangle
\text{lemma} \ [\text{simp, code-unfold}]: \ const(1) \ \langle \text{proof} \rangle
\text{lemma} \ [\text{simp, code-unfold}]: \ const(2) \ \langle \text{proof} \rangle
\text{lemma} \ [\text{simp, code-unfold}]: \ const(6) \ \langle \text{proof} \rangle
\text{lemma} \ [\text{simp, code-unfold}]: \ const(8) \ \langle \text{proof} \rangle
\text{lemma} \ [\text{simp, code-unfold}]: \ const(9) \ \langle \text{proof} \rangle

\text{Behavior vs StrongEq}
\text{lemma} \ \text{StrictRefEq}{_\text{Boolean}-vs-StrongEq}:
\tau \models (v \ x) \implies \tau \models (v \ y) \implies (\tau \models ((x::(\exists \text{Boolean}) \triangleright y) \triangleq (x \triangleq y)))
\langle \text{proof} \rangle

\text{lemma} \ \text{StrictRefEq}{_\text{Integer}-vs-StrongEq}:
\tau \models (v \ x) \implies \tau \models (v \ y) \implies (\tau \models ((x::(\exists \text{Integer}) \triangleright y) \triangleq (x \triangleq y)))
\langle \text{proof} \rangle

\text{Context Passing}
\text{lemma} \ \text{cp-StrictRefEq}{_\text{Boolean}}:\n((X::(\exists \text{Boolean}) \triangleright Y) \triangleright (\lambda . \ X \tau) \triangleright (\lambda . \ Y \tau)) \triangleright \tau
\langle \text{proof} \rangle

\text{lemma} \ \text{cp-StrictRefEq}{_\text{Integer}}:\n((X::(\exists \text{Integer}) \triangleright Y) \triangleright (\lambda . \ X \tau) \triangleright (\lambda . \ Y \tau)) \triangleright \tau
\langle \text{proof} \rangle
lemmas \text{cp-intro}^{\introl, \simp, \code-unfold} =
\text{cp-intro'}
\text{cp-StrictRefEq}_{\text{Boolean}}\text{[THEN allI[THEN allI[THEN allI[THEN cpI2]], of StrictRefEq]}]
\text{cp-StrictRefEq}_{\text{Integer}}\text{[THEN allI[THEN allI[THEN allI[THEN cpI2]], of StrictRefEq]}]
\text{cp-OclAdd}_{\text{Integer}}\text{[THEN allI[THEN allI[THEN allI[THEN cpI2]], of OclAdd_{Integer}]}]
\text{cp-OclLess}_{\text{Integer}}\text{[THEN allI[THEN allI[THEN allI[THEN cpI2]], of OclLess_{Integer}]}]
\text{cp-OclLe}_{\text{Integer}}\text{[THEN allI[THEN allI[THEN allI[THEN cpI2]], of OclLe_{Integer}]}]

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 \( \tau \mid = v(\text{true}) \)
value \( \tau \mid = \delta(\text{false}) \)
value \( \neg(\tau \mid = \delta(\text{null})) \)
value \( \neg(\tau \mid = \delta(\text{invalid})) \)
value \( \tau \mid = v((\text{null}::(A)\text{Boolean})) \)
value \( \neg(\tau \mid = v(\text{invalid})) \)
value \( \tau \mid = (\text{true} \land \text{true}) \)
value \( \tau \mid = ((\text{null} \lor \text{null}) \triangleq \text{null}) \)
value \( \tau \mid = ((\text{null} \lor \text{null}) = \text{null}) \)
value \( \tau \mid = ((\text{true} \triangleq \text{false}) \triangleq \text{false}) \)
value \( \tau \mid = ((\text{invalid} \triangleq \text{false}) \triangleq \text{false}) \)
value \( \tau \mid = ((\text{invalid} = \text{false}) \triangleq \text{invalid}) \)

Elementary computations on Integer
value \( \tau \mid = v \ 4 \)
value \( \tau \mid = \delta \ 4 \)
value \( \tau \mid = v ((\text{null}::(A)\text{Integer})) \)
value \( \tau \mid = (\text{invalid} \triangleq \text{invalid}) \)
value \( \tau \mid = (\text{null} \triangleq \text{null}) \)
value \( \tau \mid = (4 \triangleq 4) \)
value \( \neg(\tau \mid = (9 \triangleq 10)) \)
value \( \neg(\tau \mid = (\text{invalid} \triangleq 10)) \)
value \( \neg(\tau \mid = (\text{null} \triangleq 10)) \)
value \( \neg(\tau \mid = (\text{invalid} \triangleq (\text{invalid}::(A)\text{Integer}))) \)
value \( \neg(\tau \mid = v (\text{invalid} \triangleq (\text{invalid}::(A)\text{Integer}))) \)
value \( \neg(\tau \mid = (\text{invalid} \triangleright (\text{invalid}::(A)\text{Integer}))) \)
value \( \neg(\tau \mid = v (\text{invalid} \triangleright (\text{invalid}::(A)\text{Integer}))) \)
value \( \tau \mid = (\text{null} \land (\text{null}::(A)\text{Integer}))) \)
value \( \tau \mid = (\text{null} \land (\text{null}::(A)\text{Integer}))) \)
value \( \tau \mid = (4 \land 4) \)
value \( \neg(\tau \mid = (4 \triangleright 4)) \)
value \( \neg(\tau \mid = (4 \triangleright 10)) \)
value $\tau \models (4 <> 10)$
value $\neg (\tau \models (0 ' <> \text{null})))$
value $\neg (\tau \models (\delta \ (0 ' '< \text{null})))$

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

4.3.1. The Construction of the Set Type

**no-notation** $\text{None} \ (\bot)$
**notation** $\text{bot} \ (\bot)$

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 $\text{Set(Sequences(Pairs(X,Y))})$).

The former principle rules out the option to define $\alpha \text{Set}$ just by $(\forall x, (\alpha \text{ option option}) \text{set})\ \text{val}$. This would allow sets to contain junk elements such as $\{\bot\}$ 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 $\alpha \text{Set-0}$. It is shown that this type “fits” indeed into the abstract type interface discussed in the previous section.

**typedef** $\alpha \text{Set-0} = \{ X :: (\alpha :: \text{null}) \text{ set option option}. \ X = \text{bot} \lor X = \text{null} \lor (\forall x \in [[X]]. \ x \neq \text{bot})\}

**instatiation** $\text{Set-0 :: (null)bot}$
**begin**

**definition** $\text{bot-Set-0-def}: (\text{bot} :: (\alpha :: \text{null}) \text{ Set-0}) \equiv \text{Abs-Set-0 None}$

**instance** (proof)

**end**

**instatiation** $\text{Set-0 :: (null)null}$
**begin**

**definition** $\text{null-Set-0-def}: (\text{null} :: (\alpha :: \text{null}) \text{ Set-0}) \equiv \text{Abs-Set-0 \ [ None \ ]}$

**instance** (proof)
... and lifting this type to the format of a valuation gives us:

type-synonym \((\mathcal{A}, \alpha) \text{ Set} = (\mathcal{A}, \alpha \text{ Set-0}) \text{ val}\)

### 4.3.2. Validity and Definedness Properties

Every element in a defined set is valid.

**lemma** Set-inv-lemma: \(\tau \models (\delta X) \implies \forall x \in \llbracket \text{Rep-Set-0} (X \tau) \rrbracket. x \neq \bot\)

**proof**

**lemma** Set-inv-lemma':

**assumes** x-def : \(\tau \models (\delta X)\)

**and** e-mem : \(e \in \llbracket \text{Rep-Set-0} (X \tau) \rrbracket\)

**shows** \(\tau \models v (\lambda \cdot e)\)

**proof**

**lemma** abs-rep-simp':

**assumes** S-all-def : \((\tau :: (\mathcal{A} \text{ st}) \models (\delta S))\)

**shows** \(\text{Abs-Set-0} \llbracket \text{Rep-Set-0} (S \tau) \rrbracket = S \tau\)

**proof**

**lemma** S-lift':

**assumes** S-all-def : \((\tau :: (\mathcal{A} \text{ st}) \models (\delta S))\)

**shows** \(\exists S'. (\lambda a (\cdot :: (\mathcal{A} \text{ st}). a) \cdot \llbracket \text{Rep-Set-0} (S \tau) \rrbracket = (\lambda a (\cdot :: (\mathcal{A} \text{ st}). [a]) \cdot S')\)

**proof**

**lemma** invalid-set-OclNot-defined [simp,code-unfold]:\(\delta(\text{invalid} :: (\mathcal{A}, \alpha :: \text{null}) \text{ Set}) = \text{false}\)

**proof**

**lemma** null-set-OclNot-defined [simp,code-unfold]:\(\delta(\text{null} :: (\mathcal{A}, \alpha :: \text{null}) \text{ Set}) = \text{false}\)

**proof**

**lemma** invalid-set-valid [simp,code-unfold]:\(\nu(\text{invalid} :: (\mathcal{A}, \alpha :: \text{null}) \text{ Set}) = \text{false}\)

**proof**

**lemma** null-set-valid [simp,code-unfold]:\(\nu(\text{null} :: (\mathcal{A}, \alpha :: \text{null}) \text{ Set}) = \text{true}\)

**proof**

... which means that we can have a type \((\mathcal{A}, (\mathcal{A}, (\mathcal{A} \text{ Integer}) \text{ Set}) \text{ Set})\) corresponding exactly to Set(Set(Integer)) in OCL notation. Note that the parameter \(\mathcal{A}\) 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** mtSet::(\(\mathcal{A}, \alpha :: \text{null}) \text{ Set} \llbracket \text{Set}\rrbracket)\)

**where** \(\text{Set}\{\} \equiv (\lambda \tau. \text{Abs-Set-0} \llbracket \{\} :: \alpha \text{ set}\rrbracket)\)


lemma mtSet-defined[simp,code-unfold]: δ(Set{}) = true
⟨proof⟩

lemma mtSet-valid[simp,code-unfold]: υ(Set{}) = true
⟨proof⟩

lemma mtSet-rep-set: [[Rep-Set-0 (Set{})]] = {}
⟨proof⟩

lemma [simp,code-unfold]: const Set{}
⟨proof⟩

Note that the collection types in OCL allow for null to be included; however, there is
the null-collection into which inclusion yields invalid.

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 :: [(A,'a::null) Set,(A,'a) val] ⇒ (A,'a) Set
where OclIncluding x y = (λ τ. if (δ x) τ = true τ ∧ (υ y) τ = true τ
then Abs-Set-0 [[ [[Rep-Set-0 (x τ)] ∪ {y τ} ]] ]
else ⊥ )
notation OclIncluding (-->including('·'))

syntax
-OclFinset :: args => (A,'a::null) Set (Set{(-)})
translations
Set{x, xs} == CONST OclIncluding (Set{xs}) x
Set{x}   == CONST OclIncluding (Set{}) x

definition OclExcluding :: [(A,'a::null) Set,(A,'a) val] ⇒ (A,'a) Set
where OclExcluding x y = (λ τ. if (δ x) τ = true τ ∧ (υ y) τ = true τ
then Abs-Set-0 [[ [[Rep-Set-0 (x τ)] ∪ {y τ} ]] ]
else ⊥ )
notation OclExcluding (-->excluding('·'))

definition OclIncludes :: [(A,'a::null) Set,(A,'a) val] ⇒ A Boolean
where OclIncludes x y = (λ τ. if (δ x) τ = true τ ∧ (υ y) τ = true τ
then [[(y τ) ∈ [[Rep-Set-0 (x τ)]]] ]
else ⊥ )
notation OclIncludes (-->includes('·'))

definition OclExcludes :: [(A,'a::null) Set,(A,'a) val] ⇒ A Boolean
where OclExcludes x y = (not(OclIncludes x y))

70
notation \( OclExcludes \) (\( \rightarrow \) excludes\( \cdot \) )

The case of the size definition is somewhat special, we admit explicitly in Featherweight OCL the possibility of infinite sets. For the size definition, this requires an extra condition that assures that the cardinality of the set is actually a defined integer.

**Definition**

\[ \text{OclSize} :: (\alpha :: \text{null}) \rightarrow \text{Set} \Rightarrow \alpha \text{ Integer} \]

where

\[ \text{OclSize } x = (\lambda \tau. \text{if } (\delta x \tau) \tau = \text{true } \tau \land \text{finite}([\lceil \text{Rep-Set-0} (x \tau) \rceil]) \]

\[ \text{then } \lfloor \lfloor \text{int} (\lceil \lceil \text{Rep-Set-0} (x \tau) \rceil) \rceil \rfloor \]

\[ \text{else } \bot \)

notation \( \text{OclSize} \) (\( \rightarrow \) size\( \cdot \) )

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**

\[ \text{OclIsEmpty} :: (\alpha :: \text{null}) \rightarrow \text{Set} \Rightarrow \alpha \text{ Boolean} \]

where

\[ \text{OclIsEmpty } x = (\forall \nu x \text{ and } \text{not } (\delta x) \nu ) \lor (\text{OclSize } x = 0) \]

notation \( \text{OclIsEmpty} \) (\( \rightarrow \) isEmpty\( \cdot \) )

**Definition**

\[ \text{OclNotEmpty} :: (\alpha :: \text{null}) \rightarrow \text{Set} \Rightarrow \alpha \text{ Boolean} \]

where

\[ \text{OclNotEmpty } x = \text{not } (\text{OclIsEmpty } x) \]

notation \( \text{OclNotEmpty} \) (\( \rightarrow \) notEmpty\( \cdot \) )

**Definition**

\[ \text{OclANY} :: [(\alpha :: \text{null}) \rightarrow \text{Set}] \Rightarrow (\alpha , \alpha) \text{ val} \]

where

\[ \text{OclANY } x = (\lambda \nu x. \text{if } (\delta x \nu) \tau = \text{true } \tau \]

\[ \text{then } \text{true } \tau \]

\[ \text{else } \text{null } \tau \]

\[ \text{else } \bot \)

notation \( \text{OclANY} \) (\( \rightarrow \) any\( \cdot \) )

The definition of \( \text{OclForall} \) mimics the one of \( \text{op and} \): \( \text{OclForall} \) is not a strict operation.

**Definition**

\[ \text{OclForall} :: [(\alpha , \alpha :: \text{null}) \rightarrow (\alpha , \alpha) \text{ val}] \Rightarrow (\alpha) \text{ Boolean} \]

where

\[ \text{OclForall } S P = (\lambda \nu x. \text{if } (\delta x \nu) \tau = \text{true } \tau \]

\[ \text{then } \text{false } \tau \]

\[ \text{else } \text{null } \tau \]

\[ \text{else } \bot \)

syntax

\( \text{OclForall} \) (\( \rightarrow \) forAll\( \cdot \) )

translations

\( X \rightarrow \text{forAll}(x \mid P) = \text{CONST} \text{ OclForall } X (\%x. P) \)

Like \( \text{OclForall} \), \( \text{OclExists} \) is also not strict.
\textbf{definition} \textit{OclExists} :: \((\forall, \alpha::null) \text{ Set,}(\forall, \alpha)\text{val} \Rightarrow (\forall) \text{Boolean} \Rightarrow \forall \text{ Boolean}

\textbf{where} \textit{OclExists} S P = \neg(\text{OclForall} S (\lambda X. \neg (P X)))

\textbf{syntax}

-\textit{OclExists} :: \[(\forall, \alpha::null) \text{ Set,}(\forall, \alpha)\text{val} \Rightarrow \forall \text{ Boolean} \quad ((-\rightarrow)\text{exists}(\cdot|\cdot))

\textbf{translations}

\(X \rightarrow \text{exists}(x \mid P) := \text{CONST OclExists} X (\%x. P)\)

\textbf{definition} \textit{OclIterate} :: \[(\forall, \alpha::null) \text{ Set,}(\forall, \beta::null)\text{val},
(\forall, \alpha)\text{val} \Rightarrow (\forall, \beta)\text{val} \Rightarrow (\forall, \beta)\text{val} \Rightarrow (\forall, \beta)\text{val}

\textbf{where} \textit{OclIterate} S A F = (\lambda \tau. \text{if } (\delta S) \tau = \text{true } \tau \land (\nu A) \tau = \text{true } \tau \land \text{finite}[[[\text{Rep-Set-0} (S \tau)]]])

\textbf{then} \text{Finite-Set.fold} (F) (A) ((\lambda a \tau. a) \cdot [[[[\text{Rep-Set-0} (S \tau)]])\tau}
\textbf{else} \bot\)

\textbf{syntax}

-\textit{OclIterate} :: \[(\forall, \alpha::null) \text{ Set,}(\forall, \gamma)\text{val}
(\rightarrow)\text{iterate}(\cdot\rightarrow)\)\)

\textbf{translations}

\(X \rightarrow \text{iterate}(a; x = A \mid P) := \text{CONST OclIterate} X A (\%a. (\%x. P))\)

\textbf{definition} \textit{OclSelect} :: \[(\forall, \alpha::null)\text{Set,}(\forall, \alpha)\text{val} \Rightarrow (\forall)\text{Boolean} \Rightarrow (\forall, \alpha)\text{Set}

\textbf{where} \textit{OclSelect} S P = (\lambda \tau. \text{if } (\delta S) \tau = \text{true } \tau
\textbf{then} \text{if } (\exists x \in [[\text{Rep-Set-0} (S \tau)]]). P(\lambda . x) \tau = \bot \tau)
\textbf{then} \bot
\textbf{else} \text{Abs-Set-0} [[[x\in[[\text{Rep-Set-0} (S \tau)]]]. P(\lambda . x) \tau \neq \text{false } \tau)]
\textbf{else} \bot\)

\textbf{syntax}

-\textit{OclSelect} :: \[(\forall, \alpha::null) \text{ Set,}(\forall, \alpha)\text{val} \Rightarrow (\forall)\text{Boolean} \quad ((-\rightarrow)\text{select}(\cdot|\cdot))

\textbf{translations}

\(X \rightarrow \text{select}(x \mid P) := \text{CONST OclSelect} X (\% x. P)\)

\textbf{definition} \textit{OclReject} :: \[(\forall, \alpha::null)\text{Set,}(\forall, \alpha)\text{val} \Rightarrow (\forall)\text{Boolean} \Rightarrow (\forall, \alpha::null)\text{Set}

\textbf{where} \textit{OclReject} S P = \text{OclSelect} S (\neg o P)

\textbf{syntax}

-\textit{OclReject} :: \[(\forall, \alpha::null) \text{ Set,}(\forall, \alpha)\text{val} \Rightarrow (\forall)\text{Boolean} \quad ((-\rightarrow)\text{reject}(\cdot|\cdot))

\textbf{translations}

\(X \rightarrow \text{reject}(x \mid P) := \text{CONST OclReject} X (\% x. P)\)

\textbf{Definition (futur operators)}

\textbf{consts}

\textit{OclCount} :: \[(\forall, \alpha::null) \text{ Set,}(\forall, \alpha)\text{Set} \Rightarrow (\forall)\text{Integer}
\textit{OclSum} :: (\forall, \alpha::null) \text{ Set} \Rightarrow (\forall)\text{Integer}
\textit{OclIncludesAll} :: \[(\forall, \alpha::null) \text{ Set,}(\forall, \alpha)\text{Set} \Rightarrow (\forall)\text{Boolean}
\textit{OclExcludesAll} :: \[(\forall, \alpha::null) \text{ Set,}(\forall, \alpha)\text{Set} \Rightarrow (\forall)\text{Boolean}
\textit{OclComplement} :: (\forall, \alpha::null) \text{ Set} \Rightarrow (\forall, \alpha)\text{Set}
\textit{OclUnion} :: \[(\forall, \alpha::null) \text{ Set,}(\forall, \alpha)\text{Set} \Rightarrow (\forall, \alpha)\text{Set}
\textit{OclIntersection} :: \[(\forall, \alpha::null) \text{ Set,}(\forall, \alpha)\text{Set} \Rightarrow (\forall, \alpha)\text{Set}
notation
   OclCount (count'(-) )
notation
   OclSum (sum'(-) )
notation
   OclIncludesAll (includesAll'(-) )
notation
   OclExcludesAll (excludesAll'(-) )
notation
   OclComplement (complement'(-) )
notation
   OclUnion (union'(-) )
notation
   OclIntersection (intersection'(-) )

4.4.2. Validity and Definedness Properties

**OclIncluding**

lemma OclIncluding-defined-args-valid:
(τ ⊨ δ(X -> including(x))) = ((τ ⊨(δ X)) ∧ (∀ v x))
⟨proof⟩

lemma OclIncluding-valid-args-valid:
(τ ⊨ v(X -> including(x))) = ((τ ⊨(δ X)) ∧ (∀ v x))
⟨proof⟩

lemma OclIncluding-defined-args-valid'[simp, code-unfold]:
δ(X -> including(x)) = ((δ X) and (∀ v x))
⟨proof⟩

lemma OclIncluding-valid-args-valid''[simp, code-unfold]:
v(X -> including(x)) = ((δ X) and (∀ v x))
⟨proof⟩

**OclExcluding**

lemma OclExcluding-defined-args-valid:
(τ ⊨ δ(X -> excluding(x))) = ((τ ⊨(δ X)) ∧ (∀ v x))
⟨proof⟩

lemma OclExcluding-valid-args-valid:
(τ ⊨ v(X -> excluding(x))) = ((τ ⊨(δ X)) ∧ (∀ v x))
⟨proof⟩

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

\textit{proof}

\textit{lemma} \textbf{OclExcluding-valid-args-valid}[\textit{simp,code-unfold}]:
\[ v(X \rightarrow \text{excluding}(x)) = ((\delta X) \text{ and } (v \ x)) \]

\textit{proof}

\textbf{OclIncludes}

\textit{lemma} \textbf{OclIncludes-defined-args-valid}:
\[ (\tau \models \delta(X \rightarrow \text{includes}(x))) = ((\tau \models (\delta X)) \land (\tau \models (v \ x))) \]

\textit{proof}

\textit{lemma} \textbf{OclIncludes-valid-args-valid}:
\[ (\tau \models v(X \rightarrow \text{includes}(x))) = ((\tau \models (\delta X)) \land (\tau \models (v \ x))) \]

\textit{proof}

\textit{lemma} \textbf{OclIncludes-valid-args-valid}'[\textit{simp,code-unfold}]:
\[ \delta(X \rightarrow \text{includes}(x)) = ((\delta X) \text{ and } (v \ x)) \]

\textit{proof}

\textit{lemma} \textbf{OclIncludes-valid-args-valid}''[\textit{simp,code-unfold}]:
\[ v(X \rightarrow \text{includes}(x)) = ((\delta X) \text{ and } (v \ x)) \]

\textit{proof}

\textbf{OclExcludes}

\textit{lemma} \textbf{OclExcludes-defined-args-valid}:
\[ (\tau \models \delta(X \rightarrow \text{excludes}(x))) = ((\tau \models (\delta X)) \land (\tau \models (v \ x))) \]

\textit{proof}

\textit{lemma} \textbf{OclExcludes-valid-args-valid}:
\[ (\tau \models v(X \rightarrow \text{excludes}(x))) = ((\tau \models (\delta X)) \land (\tau \models (v \ x))) \]

\textit{proof}

\textit{lemma} \textbf{OclExcludes-valid-args-valid}'[\textit{simp,code-unfold}]:
\[ \delta(X \rightarrow \text{excludes}(x)) = ((\delta X) \text{ and } (v \ x)) \]

\textit{proof}

\textit{lemma} \textbf{OclExcludes-valid-args-valid}''[\textit{simp,code-unfold}]:
\[ v(X \rightarrow \text{excludes}(x)) = ((\delta X) \text{ and } (v \ x)) \]

\textit{proof}

\textbf{OclSize}

\textit{lemma} \textbf{OclSize-defined-args-valid}: \[ \tau \models \delta(X \rightarrow \text{size}()) \implies \tau \models \delta X \]

\textit{proof}

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

**shows** $(\tau \models \text{not}(\delta(S))) \lor \neg \text{finite} \ [\text{Rep-Set-0 } (S \ \tau)]$

⟨proof⟩

**lemma** $\tau \models \delta \ X \implies \neg \text{finite} \ [\text{Rep-Set-0 } (X \ \tau)] \implies \neg \tau \models \delta \ (X \rightarrow \text{size}())$

⟨proof⟩

**lemma size-defined:**

**assumes** $X$-finite: $\forall \tau. \ \text{finite} \ [\text{Rep-Set-0 } (X \ \tau)]$

**shows** $\delta \ (X \rightarrow \text{size}()) = \delta \ X$

⟨proof⟩

**lemma size-defined′:**

**assumes** $X$-finite: finite $[\text{Rep-Set-0 } (X \ \tau)]$

**shows** $(\tau \models \delta \ (X \rightarrow \text{size}()))) = (\tau \models \delta \ X)$

⟨proof⟩

**OclIsEmpty**

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

⟨proof⟩

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

⟨proof⟩

**lemma** OclIsEmpty-infinite: $\tau \models \delta \ X \implies \neg \text{finite} \ [\text{Rep-Set-0 } (X \ \tau)] \implies \neg \tau \models \delta \ (X \rightarrow \text{isEmpty}())$

⟨proof⟩

**OclNotEmpty**

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

⟨proof⟩

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

⟨proof⟩

**lemma** OclNotEmpty-infinite: $\tau \models \delta \ X \implies \neg \text{finite} \ [\text{Rep-Set-0 } (X \ \tau)] \implies \neg \tau \models \delta \ (X \rightarrow \text{notEmpty}())$

⟨proof⟩

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

⟨proof⟩

**OclANY**

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

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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

OclIncluding

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

OclExcluding

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

OclIncludes

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

OclExcludes

lemma OclExcludes-invalid[\text{simp,code-unfold}]: (\text{invalid} \rightarrow \text{excludes}(x)) = \text{invalid}

76
proof

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

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

OclSize

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

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

OclIsEmpty

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

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

OclNotEmpty

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

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

OclANY

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

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

OclForall

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

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

OclExists

lemma OclExists-invalid[simp,code-unfold](\text{invalid} \rightarrow \text{exists}(a \mid P a)) = \text{invalid}
lemma OclExists-null[simp,code-unfold]:null→exists(a | P a) = invalid
⟨proof⟩

OclIterate

lemma OclIterate-invalid[simp,code-unfold]:invalid→iterate(a; x = A | P a x) = invalid
⟨proof⟩

lemma OclIterate-null[simp,code-unfold]:null→iterate(a; x = A | P a x) = invalid
⟨proof⟩

lemma OclIterate-invalid-args[simp,code-unfold]:S→iterate(a; x = invalid | P a x) = invalid
⟨proof⟩

An open question is this ...

lemma S→iterate(a; x = null | P a x) = invalid
⟨proof⟩

lemma OclIterate-infinite:
assumes non-finite: τ |= not(δ(S→size()))
shows (OclIterate S A F) τ = invalid τ
⟨proof⟩

OclSelect

lemma OclSelect-invalid[simp,code-unfold]:invalid→select(a | P a) = invalid
⟨proof⟩

lemma OclSelect-null[simp,code-unfold]:null→select(a | P a) = invalid
⟨proof⟩

OclReject

lemma OclReject-invalid[simp,code-unfold]:invalid→reject(a | P a) = invalid
⟨proof⟩

lemma OclReject-null[simp,code-unfold]:null→reject(a | P a) = invalid
⟨proof⟩

4.4.4. Context Passing

lemma cp-OclIncluding:
(X→including(x)) τ = ((λ - . X τ)→including(λ - . x τ)) τ
⟨proof⟩

lemma cp-OclExcluding:
lemma \textit{cp-OclIncludes}: \\
(X \Rightarrow \text{excluding}(x)) \tau = ((\lambda \cdot . X \tau) \Rightarrow \text{excluding}(\lambda \cdot . x \tau)) \tau \\
\langle \text{proof} \rangle 

lemma \textit{cp-OclIncludes1}: \\
(X \Rightarrow \text{includes}(x)) \tau = (X \Rightarrow \text{includes}(\lambda \cdot . x \tau)) \tau \\
\langle \text{proof} \rangle 

lemma \textit{cp-OclExcludes}: \\
(X \Rightarrow \text{excludes}(x)) \tau = ((\lambda \cdot . X \tau) \Rightarrow \text{excludes}(\lambda \cdot . x \tau)) \tau \\
\langle \text{proof} \rangle 

lemma \textit{cp-OclSize}: X \Rightarrow \text{size}() \tau = ((\lambda \cdot . X \tau) \Rightarrow \text{size}()) \tau \\
\langle \text{proof} \rangle 

lemma \textit{cp-OclIsEmpty}: X \Rightarrow \text{isEmpty}() \tau = ((\lambda \cdot . X \tau) \Rightarrow \text{isEmpty}()) \tau \\
\langle \text{proof} \rangle 

lemma \textit{cp-OclNotEmpty}: X \Rightarrow \text{notEmpty}() \tau = ((\lambda \cdot . X \tau) \Rightarrow \text{notEmpty}()) \tau \\
\langle \text{proof} \rangle 

lemma \textit{cp-OclANY}: (S \Rightarrow \text{forAll}(x \mid P x)) \tau = ((\lambda \cdot . S \tau) \Rightarrow \text{forAll}(x \mid P (\lambda \cdot . x \tau))) \tau \\
\langle \text{proof} \rangle 

lemma \textit{cp-OclForall} \textbf{1} [simp,intro!]: \\
cp S \Rightarrow cp (\lambda X. ((S X) \Rightarrow \text{forAll}(x \mid P x))) \\
\langle \text{proof} \rangle 

lemma \textit{cp-OclForall1} \textbf{1}: \\
cp (\lambda X St x. P (\lambda \cdot . x) X St) \Rightarrow cp S \Rightarrow cp (\lambda X. (S X) \Rightarrow \text{forAll}(x \mid P x \mid X)) \\
\langle \text{proof} \rangle 

lemma \textit{cp-Oc1}\textbf{1}: \\
cp S \Rightarrow \\
(\forall x. cp(P x)) \Rightarrow \\
\langle \text{proof} \rangle 

lemma \textit{cp-OclExists}: \\
\langle \text{proof} \rangle 

79
\[(S \to \exists(x \mid P \, x)) \Rightarrow ((\lambda \cdot S \, x) \to \exists(x \mid P \, (\lambda \cdot x \, x)))\]
\langle \text{proof} \rangle

\textbf{lemma} \: cp-OclExists1 \: [\text{simp.intro}]:
\[cp \, S \Rightarrow cp \, (\lambda X. ((S \, X) \to \exists(x \mid P \, x)))\]
\langle \text{proof} \rangle

\textbf{lemma} \: cp-OclIterate: \: (X \to \text{iterate}(a; \, x = A \mid P \, a \, x)) \Rightarrow ((\lambda \cdot X \, x) \to \text{iterate}(a; \, x = A \mid P \, a \, x))\]
\langle \text{proof} \rangle

\textbf{lemma} \: cp-OclSelect: \: (X \to \text{select}(a \mid P \, a)) \Rightarrow ((\lambda \cdot X \, x) \to \text{select}(a \mid P \, a))\]
\langle \text{proof} \rangle

\textbf{lemma} \: cp-OclReject: \: (X \to \text{reject}(a \mid P \, a)) \Rightarrow ((\lambda \cdot X \, x) \to \text{reject}(a \mid P \, a))\]
\langle \text{proof} \rangle

\textbf{lemmas} \: cp-intro''[intro!,simp.code-unfold] =
\begin{align*}
\text{cp-OclIncluding} & \quad [\text{THEN allI[THEN allI[THEN allI[THEN cpI2]], of OclIncluding]}] \\
\text{cp-OclExcluding} & \quad [\text{THEN allI[THEN allI[THEN allI[THEN cpI2]], of OclExcluding]}] \\
\text{cp-OclIncludes} & \quad [\text{THEN allI[THEN allI[THEN allI[THEN cpI2]], of OclIncludes]}] \\
\text{cp-OclExcludes} & \quad [\text{THEN allI[THEN allI[THEN allI[THEN cpI2]], of OclExcludes]}] \\
\text{cp-OclSize} & \quad [\text{THEN allI[THEN allI[THEN cpI1], of OclSize]}] \\
\text{cp-OclIsEmpty} & \quad [\text{THEN allI[THEN allI[THEN cpI1], of OclIsEmpty]}] \\
\text{cp-OclNotEmpty} & \quad [\text{THEN allI[THEN allI[THEN cpI1], of OclNotEmpty]}] \\
\text{cp-OclANY} & \quad [\text{THEN allI[THEN allI[THEN cpI1], of OclANY]}]
\end{align*}

4.4.5. Const

\textbf{lemma} \: const-OclIncluding[simp.code-unfold] :
\begin{itemize}
\item \text{assumes} \: \text{const-x} : \text{const} \, x
\item \text{and} \: \text{const-S} : \text{const} \, S
\item \text{shows} \: \text{const} \, (S \to \text{including}(x))
\end{itemize}
\langle \text{proof} \rangle

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:

\textbf{defs} \: (overloaded) \: \text{StrictRefEq}_{\text{Set}} :
\[(x::(\mathcal{A},'\alpha::null)\text{Set}) \equiv y \equiv \lambda \, \tau. \text{if } (v \, x) \, \tau = true \land (v \, y) \, \tau = true \, \tau \]
\[
\begin{align*}
\text{then } (x \triangleq y) & \tau \\
\text{else } \text{invalid} & \tau
\end{align*}
\]

One might object here that for the case of objects, this is an empty definition. The answer is no, we will restrain later on states and objects such that any object has its oid stored inside the object (so the ref, under which an object can be referenced in the store will represented in the object itself). For such well-formed stores that satisfy this invariant (the WFF-invariant), the referential equality and the strong equality—and therefore the strict equality on sets in the sense above—coincides.

### 4.5.2. Logic and Algebraic Layer on Set

**Reflexivity**

To become operational, we derive:

**lemma** `StrictRefEqSet-ref[\text{simp,code-unfold}]`:

\[ (x::(\mathcal{A},'\alpha::null)\text{Set}) \equiv x = (\text{if } (v \, x) \text{ then } true \text{ else } \text{invalid endif}) \]

**Symmetry**

**lemma** `StrictRefEqSet-sym`:

\[ (x::(\mathcal{A},'\alpha::null)\text{Set}) \equiv y = (y \equiv x) \]

**Execution with Invalid or Null as Argument**

**lemma** `StrictRefEqSet-strict1[\text{simp,code-unfold}]`:

\[ ((x::(\mathcal{A},'\alpha::null)\text{Set}) \equiv \text{invalid}) = \text{invalid} \]

**lemma** `StrictRefEqSet-strict2[\text{simp,code-unfold}]`:

\[ (\text{invalid} \equiv (y::(\mathcal{A},'\alpha::null)\text{Set})) = \text{invalid} \]

**lemma** `StrictRefEqSet-strictEq-valid-args-valid`:

\[ (\tau \models \delta ((x::(\mathcal{A},'\alpha::null)\text{Set}) \equiv y)) = ((\tau \models (v \, x)) \land (\tau \models v \, y)) \]

**Behavior vs StrongEq**

**lemma** `StrictRefEqSet-vs-StrongEq`:

\[ \tau \models v \, x \implies \tau \models v \, y \implies (\tau \models (x::(\mathcal{A},'\alpha::null)\text{Set}) \equiv y) \triangleq (x \triangleq y)) \]

**Context Passing**

**lemma** `cp-StrictRefEqSet`:

\[ ((X::(\mathcal{A},'\alpha::null)\text{Set}) \equiv Y) \, \tau = ((\lambda \cdot \, X \, \tau) \equiv (\lambda \cdot \, Y \, \tau)) \, \tau \]
4.6. Execution on Set’s Operators (with mtSet and recursive case as arguments)

4.6.1. OclIncluding

**Lemma OclIncluding-finite-rep-set**:  
**Assumes**  
\(X\)-def: \(\tau \models \delta X\)  
and \(x\)-val: \(\tau \models v x\)  
**Shows** \(\text{finite } [[\text{Rep-Set-0} (X \rightarrow \text{including}(x) \ \tau)]] = \text{finite } [[\text{Rep-Set-0} (X \ \tau)]]\)

**Lemma OclIncluding-rep-set**:  
**Assumes** \(S\)-def: \(\tau \models \delta S\)  
**Shows** \(\text{finite } [[\text{Rep-Set-0} (S \rightarrow \text{including}(\lambda x. [[x]]) \ \tau)]] = \text{insert } [[x]] [[\text{Rep-Set-0} (S \ \tau)]]\)

**Lemma OclIncluding-notempty-rep-set**:  
**Assumes** \(X\)-def: \(\tau \models \delta X\)  
and \(a\)-val: \(\tau \models v a\)  
**Shows** \(\text{finite } [[\text{Rep-Set-0} (X \rightarrow \text{including}(a) \ \tau)]] \neq \{\}\)

**Lemma OclIncluding-includes**:  
**Assumes** \(\tau \models X \rightarrow \text{includes}(x)\)  
**Shows** \(X \rightarrow \text{including}(x) \ \tau = X \ \tau\)

4.6.2. OclExcluding

**Lemma OclExcluding-charn0[simp]**:  
**Assumes** \(val-x\)-\(\tau \models (v \ x)\)  
**Shows** \(\tau \models ((\text{Set}\{} \rightarrow \text{excluding}(x)) \triangleq \text{Set}\{\})\)

**Lemma OclExcluding-charn0-exec[simp, code-unfold]**:  
\((\text{Set}\{} \rightarrow \text{excluding}(x)) = (\text{if } (v \ x) \ \text{then Set}\{} \ \text{else invalid endif})\)

**Lemma OclExcluding-charn1**:  
**Assumes** \(def-X\)-\(\tau \models (\delta X)\)
and \( \text{val-}x : \tau \models (v \ x) \)
and \( \text{val-}y : \tau \models (v \ y) \)
and \( \text{neq} \ : \tau \models \text{not}(x \triangleq y) \)
shows \( \tau \models ((X \rightarrow \text{including}(x)) \rightarrow \text{excluding}(y)) \triangleq ((X \rightarrow \text{excluding}(y)) \rightarrow \text{including}(x)) \)

\( \langle \text{proof} \rangle \)

**Lemma OclExcluding-charn2:**

**assumes** \( \text{def-}\ X : \tau \models (\delta \ X) \)
and \( \text{val-}x : \tau \models (v \ x) \)
shows \( \tau \models ((((X \rightarrow \text{including}(x)) \rightarrow \text{excluding}(y)) \triangleq (X \rightarrow \text{excluding}(y)) \rightarrow \text{including}(x)) \)

\( \langle \text{proof} \rangle \)

One would like a generic theorem of the form:

**Lemma OclExcluding-charn-exec:**

")(X \rightarrow \text{including}(x::(\mathbb{A},'a::null)\text{val})\rightarrow\text{excluding}(y)) =
(if \( \delta \ X \) then if \( x \triangleq y \)
then \( X \rightarrow \text{excluding}(y) \)
else \( X \rightarrow \text{excluding}(y) \rightarrow \text{including}(x) \)
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 \( \text{OclExcluding-charn-exec} \) 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** \( \text{strict1}: (x \triangleq \text{invalid}) = \text{invalid} \)
and \( \text{strict2}: (\text{invalid} \triangleq y) = \text{invalid} \)
and \( \text{StrictRefEq-valid-args-valid}: \bigwedge (x::(\mathbb{A},'a::null)\text{val}) (y : \tau) . \)
(\( \tau \models \delta \ (x \triangleq y) = ((\tau \models (v \ x)) \land (\tau \models v \ y)) \))
and \( \text{cp-StrictRefEq}: \bigwedge \ (X::(\mathbb{A},'a::null)\text{val}) (Y : \tau) . \ (X \triangleq Y) \tau = ((\lambda -. \ X \tau) \triangleq (\lambda -. \ Y \tau)) \tau \)
and \( \text{StrictRefEq-vs-StrongEq}: \bigwedge (x::(\mathbb{A},'a::null)\text{val}) (y : \tau) . \)
\( \tau \models v \ x \Longrightarrow \tau \models v \ y \Longrightarrow (\tau \models ((x \triangleq y) \triangleq (x \triangleq y))) \)
shows \( (X \rightarrow \text{including}(x::(\mathbb{A},'a::null)\text{val})\rightarrow\text{excluding}(y)) =
(if \( \delta \ X \) then if \( x \triangleq y \)
then \( X \rightarrow \text{excluding}(y) \)
else \( X \rightarrow \text{excluding}(y) \rightarrow \text{including}(x) \)
endif
else invalid endif) \)

\( \langle \text{proof} \rangle \)

**Schematic Lemma OclExcluding-charn-exec\_Integer[simp,code-unfold]: ?X**

\( \langle \text{proof} \rangle \)

83
schematic-lemma OclExcluding-charn-exec\[simp,code-unfold\]: \(?X
⟨proof⟩

schematic-lemma OclExcluding-charn-exec\[simp,code-unfold\]: \(?X
⟨proof⟩

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

lemma OclExcluding-rep-set:
assumes S-def : \(\tau \models \delta S\)
shows \([\text{Rep-Set-}0 (S \rightarrow \text{excluding}(\lambda. \ [x]) \ \tau)]\) = \([\text{Rep-Set-}0 (S \ \tau)]\) − \([\{x\}]\)
⟨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\[simp,code-unfold\]:
\(\text{Set}\{\} \rightarrow \text{includes}(x) = (\text{if } v x \text{ then false else invalid endif})\)
⟨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: \(x \triangleq \text{invalid} = \text{invalid} \)

84
and \( \text{strict2}: (\text{invalid} \doteq y) = \text{invalid} \)
and \( \text{cp-StrictRefEq}: \land (X::(\mathcal{A},'a::\text{null})\text{val})\ Y\ \tau.\ (X \doteq Y)\ \tau = ((\lambda-.\ X\ \tau) \doteq (\lambda-.\ Y\ \tau))\ \tau \)
and \( \text{StrictRefEq-vs-StrongEq}: \land (x::(\mathcal{A},'a::\text{null})\text{val})\ y\ \tau.
\tau \models v\ x \implies \tau \models v\ y \implies (\tau \models ((x \doteq y) \triangleq (x \triangleq y))) \)
shows
\((X \rightarrow \text{including}(x::(\mathcal{A},'a::\text{null})\text{val}) \rightarrow \text{includes}(y)) =
\begin{cases} 
\text{if } \delta\ X \text{ then if } x \doteq y \text{ then true else } X \rightarrow \text{includes}(y) \text{ endif else invalid endif} 
\end{cases} \)

\( \langle \text{proof} \rangle \)

schematic-lemma \( \text{OclIncludes-execute} \) \([\text{simp,code-unfold}]: \) \?X

\( \langle \text{proof} \rangle \)

schematic-lemma \( \text{OclIncludes-execute} \) \([\text{simp,code-unfold}]: \) \?X

\( \langle \text{proof} \rangle \)

schematic-lemma \( \text{OclIncludes-execute} \) \([\text{simp,code-unfold}]: \) \?X

\( \langle \text{proof} \rangle \)

lemma \( \text{OclIncludes-including-generic} : \)
assumes \( \text{OclIncludes-execute-generic} \) \([\text{simp}]: \land X\ x\ y.\ (X \rightarrow \text{including}(x::(\mathcal{A},'a::\text{null})\text{val}) \rightarrow \text{includes}(y)) =
\begin{cases} 
\text{if } \delta\ X \text{ then if } x \doteq y \text{ then true else } X \rightarrow \text{includes}(y) \text{ endif else invalid endif} 
\end{cases} \)
and \( \text{StrictRefEq-strict}'' : \land x\ y.\ \delta ((x::(\mathcal{A},'a::\text{null})\text{val}) \doteq y) = (v(x) \text{ and } v(y)) \)
and \( a\text{-val} : \tau \models v\ a \)
and \( x\text{-val} : \tau \models v\ x \)
and \( \text{S-incl} : \tau \models (S) \rightarrow \text{includes}(x::(\mathcal{A},'a::\text{null})\text{val}) \)
shows \( \tau \models S \rightarrow \text{including}(a::(\mathcal{A},'a::\text{null})\text{val}) \rightarrow \text{includes}(x) \)

\( \langle \text{proof} \rangle \)

lemmas \( \text{OclIncludes-including} = \)
\( \text{OclIncludes-including-generic}[\text{OF OclIncludes-execute}\text{Integer}\text{StrictRefEq}\text{Integer-strict}''] \)

### 4.6.4. OclExcludes

### 4.6.5. OclSize

lemma \([\text{simp,code-unfold}]: \) \( \text{Set} \} \rightarrow \text{size}() = 0 \)

\( \langle \text{proof} \rangle \)

lemma \( \text{OclSize-including-exec}[\text{simp,code-unfold}]: \)
\( ((X \rightarrow \text{including}(x)) \rightarrow \text{size}()) = (\text{if } \delta\ X \text{ and } v\ x \text{ then } X \rightarrow \text{size}() + \text{ if } X \rightarrow \text{includes}(x) \text{ then } 0 \text{ else } 1 \text{ endif}) \)

\( \langle \text{proof} \rangle \)
4.6.6. OclIsEmpty

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

lemma OclIsEmpty-including [simp]:
assumes X-def: τ |\|= δ X
    and X-finite: finite [[Rep-Set-0 (X τ)]]
    and a-val: τ |\|= v a
shows X->including(a)->isEmpty() τ = false τ
⟨proof⟩

4.6.7. OclNotEmpty

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

lemma OclNotEmpty-including [simp, code-unfold]:
assumes X-def: τ |\|= δ X
    and X-finite: finite [[Rep-Set-0 (X τ)]]
    and a-val: τ |\|= v a
shows X->including(a)->notEmpty() τ = true τ
⟨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 δ 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]:
\[ ((\text{Set}) \rightarrow \exists z \mid P(z)) = \text{false} \]

\textbf{lemma} \( \text{OclExists-including-exec[\text{simp, code-unfold}] :} \)
\textbf{assumes} \( cp : cp P \)
\textbf{shows} \( ((S \rightarrow \text{including}(x)) \rightarrow \exists z \mid P(z)) = (\text{if } \delta S \text{ and } \nu x \text{ then } P x \text{ or } (S \rightarrow \exists z \mid P(z)) \text{ else invalid endif}) \)

\textbf{proof}

\textbf{4.6.11. OclIterate}

\textbf{lemma} \( \text{OclIterate-empty[\text{simp, code-unfold}]:} ((\text{Set}) \rightarrow \text{iterate}(a; x = A \mid P a x)) = A \)
\textbf{proof}

In particular, this does hold for \( A = \text{null} \).

\textbf{lemma} \( \text{OclIterate-including:} \)
\textbf{assumes} \( S\text{-finite}: \tau \models \delta(S \rightarrow \text{size}()) \)
\textbf{and} \( F\text{-valid-arg}: (v A) \tau = (v (F a A)) \tau \)
\textbf{and} \( F\text{-commute}: \text{comp-fun-commute } F \)
\textbf{and} \( F\text{-cp}: \lambda x y \tau. F x y \tau = F (\lambda . x \tau) y \tau \)
\textbf{shows} \( ((S \rightarrow \text{including}(a)) \rightarrow \text{iterate}(a; x = A \mid F a x)) \tau = ((S \rightarrow \text{excluding}(a)) \rightarrow \text{iterate}(a; x = F a A \mid F a x)) \tau \)
\textbf{proof}

\textbf{4.6.12. OclSelect}

\textbf{lemma} \( \text{OclSelect-mtSet-exec[\text{simp, code-unfold}]:} \text{OclSelect mtSet } P = \text{mtSet} \)
\textbf{proof}

\textbf{definition} \( \text{OclSelect-body ::} - \Rightarrow - \Rightarrow - \Rightarrow - \Rightarrow (\forall \text{, } \text{a option option } \text{Set}) \)
\( \equiv (\lambda P x \text{ acc. if } P x \Downarrow \text{false then acc else acc} \rightarrow \text{including}(x) \text{ endif}) \)

\textbf{lemma} \( \text{OclSelect-including-exec[\text{simp, code-unfold}]:} \)
\textbf{assumes} \( P\text{-cp : cp } P \)
\textbf{shows} \( \text{OclSelect } (X \rightarrow \text{including}(y)) \ P = \text{OclSelect-body } P \ y \ (\text{OclSelect } (X \rightarrow \text{excluding}(y)) \ P) \)
\( \text{(is } - \Rightarrow ?\text{select}) \)
\textbf{proof}

\textbf{4.6.13. OclReject}

\textbf{lemma} \( \text{OclReject-mtSet-exec[\text{simp, code-unfold}]:} \text{OclReject mtSet } P = \text{mtSet} \)
\textbf{proof}

\textbf{lemma} \( \text{OclReject-including-exec[\text{simp, code-unfold}]:} \)
\textbf{assumes} \( P\text{-cp : cp } P \)
\textbf{shows} \( \text{OclReject } (X \rightarrow \text{including}(y)) \ P = \text{OclSelect-body } (\text{not } o \ P) \ y \ (\text{OclReject } (X \rightarrow \text{excluding}(y)) \ P) \)
4.7. Execution on Set’s Operators (higher composition)

4.7.1. OclIncludes

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

4.7.2. OclSize

lemma \[simp,\ code-unfold\]:
\[ \delta \left(\text{Set}{} \rightarrow \text{size}()\right) = \text{true} \]

lemma \[simp,\ code-unfold\]:
\[ \delta \left((X \rightarrow \text{including}(x)) \rightarrow \text{size}()\right) = (\delta(X \rightarrow \text{size}()) \text{ and } v(x)) \]

lemma \[simp\]:
assumes X-finite: \[\forall \tau. \text{finite } \left[\left[\text{Rep-Set-0} \left(X \tau\right)\right]\right]\]
shows \[\delta \left((X \rightarrow \text{excluding}(x)) \rightarrow \text{size}()\right) = (\delta(X \rightarrow \text{size}()) \text{ and } v(x)) \]

4.7.3. OclForall

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

lemma OclForall-rep-set-true:
assumes \[\tau \models \delta X\]
shows \[\tau \models OclForall X P \tau \models (\forall x \in \left[\left[\text{Rep-Set-0} \left(X \tau\right)\right]\right]. \tau \models P (\lambda \tau. x))\]

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

lemma OclForall-not-includes :
assumes $x$-def : $\tau \models \delta x$
and $y$-def : $\tau \models \delta y$
shows $(\text{OclForall } x \ (\text{OclIncludes} \ y) \ \tau = \text{false} \ \tau) = (\neg \ [[\text{Rep-Set-0} \ (x \ \tau)] \subseteq [[\text{Rep-Set-0} \ (y \ \tau)]]))$
⟨proof⟩

lemma OclForall-iterate:
assumes $S$-finite: finite $[[\text{Rep-Set-0} \ (S \ \tau)]]$
shows $S \rightarrow \text{forAll} \ (x \mid P \ x) \ \tau = (S \rightarrow \text{iterate}(x; \ \text{acc} = \text{true} \mid \text{acc} \ \text{and} \ P \ x)) \ \tau$
⟨proof⟩

lemma OclForall-cong:
assumes $\forall x. \ x \in [[\text{Rep-Set-0} \ (X \ \tau)]] \implies \tau \models P \ (\lambda \tau. \ x) \implies \tau \models Q \ (\lambda \tau. \ x)$
assumes $P; \ \tau \models \text{OclForall} \ X \ P$
shows $\tau \models \text{OclForall} \ X \ Q$
⟨proof⟩

lemma OclForall-cong’:
assumes $\forall x. \ x \in [[\text{Rep-Set-0} \ (X \ \tau)]] \implies \tau \models P \ (\lambda \tau. \ x) \implies \tau \models Q \ (\lambda \tau. \ x) \implies \tau \models R \ (\lambda \tau. \ x)$
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 $x$-def : $\tau \models \delta x$
assumes $y$-def : $\tau \models \delta y$
shows $((x::(\mathbb{A},'\alpha::\text{null})\text{Set}) \hat{=} y) \ \tau =$
$(x \rightarrow \text{forAll}(z \mid y \rightarrow \text{includes}(z)) \ \text{and} \ (y \rightarrow \text{forAll}(z \mid x \rightarrow \text{includes}(z)))) \ \tau$
⟨proof⟩

lemma StrictRefEqSet-exec[simp,code-unfold] :
$((x::(\mathbb{A},'\alpha::\text{null})\text{Set}) \hat{=} y) =$
(if $\delta x$ then (if $\delta y$
then $((x \rightarrow \text{forAll}(z \mid y \rightarrow \text{includes}(z)) \ \text{and} \ (y \rightarrow \text{forAll}(z \mid x \rightarrow \text{includes}(z))))$)
else if $v \ y$
then false (* $x'\rightarrow\text{includes} = \text{null} \*)
else invalid
endif)
else if $v \ x$ (* $\text{null} = ??? \*)
then if $v \ y$ then not($\delta y$) else invalid endif
else invalid
endif
⟨proof⟩
lemma \textit{StrictRefEq}_{\textit{Set}-\textit{subst1}} : cp \ P \Rightarrow \tau \models v \ x \Rightarrow \tau \models v \ \ P \ y \Rightarrow \tau \models (x::{(\mathfrak{A},'\alpha::\text{null})}\text{Set}) \models y \Rightarrow (P \ x::{(\mathfrak{A},'\alpha::\text{null})}\text{Set}) \models P \ y
\langle \text{proof} \rangle

lemma \textit{OclIncluding-cong}' : 
\textit{shows} \tau \models \delta \ s \Rightarrow \tau \models \delta \ t \Rightarrow \tau \models v \ x \Rightarrow 
\tau \models ((s::{(\mathfrak{A},'\alpha::\text{null})}\text{Set}) \models t) \Rightarrow \tau \models (s \rightarrow \text{including}(x) \models (t \rightarrow \text{including}(x)))
\langle \text{proof} \rangle

lemma \textit{OclIncluding-cong} : \bigwedge (s::{(\mathfrak{A},'\alpha::\text{null})}\text{Set}) \ t \ y \ \tau. \ \tau \models \delta \ t \Rightarrow \tau \models v \ y \Rightarrow 
\tau \models s \models t \Rightarrow x = y \Rightarrow \tau \models s \rightarrow \text{including}(x) \models (t \rightarrow \text{including}(y))
\langle \text{proof} \rangle

lemma \textit{const-StrictRefEq}_{\textit{Set}-\text{including}} : \textit{const} a \Rightarrow \textit{const} S \Rightarrow \textit{const} X \Rightarrow \textit{const} (X \models S \rightarrow \text{including}(a))
\langle \text{proof} \rangle

\textbf{4.8. Test Statements}

lemma \textit{syntax-test} : \textit{Set}\{2,1\} = (\text{Set}\{} \rightarrow \text{including}(1) \rightarrow \text{including}(2))
\langle \text{proof} \rangle

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 \textit{null} for the non-existing Sets) :

lemma \textit{semantic-test2}:
\textit{assumes} H : \textit{Set}\{2\} \models \text{null} = (\text{false}::{(\mathfrak{A})\text{Boolean}})
\textit{shows} (\tau::{(\mathfrak{A})}\text{st}) \models (\text{Set}\{\text{Set}\{2\},\text{null}\} \rightarrow \text{includes}(\text{null}))
\langle \text{proof} \rangle

lemma \textit{short-cut}'[\textit{simp,code-unfold}] : (8 \models 6) = \text{false}
\langle \text{proof} \rangle

lemma \textit{short-cut}''[\textit{simp,code-unfold}] : (2 \models 1) = \text{false}
\langle \text{proof} \rangle

lemma \textit{short-cut}'''[\textit{simp,code-unfold}] : (1 \models 2) = \text{false}
\langle \text{proof} \rangle

Elementary computations on Sets.

\textit{declare} \ OclSelect-body-def \ [\textit{simp}]

\textit{value} \ \neg (\tau \models v(\text{invalid}::{(\mathfrak{A},'\alpha::\text{null})}\text{Set}))
\textit{value} \ \tau \models v(\text{null}::{(\mathfrak{A},'\alpha::\text{null})}\text{Set})
\textit{value} \ \neg (\tau \models \delta(\text{null}::{(\mathfrak{A},'\alpha::\text{null})}\text{Set}))
\textit{value} \ \tau \models v(\text{Set}\{\})
\textit{value} \ \tau \models v(\text{Set}\{\text{Set}\{2\},\text{null}\})
value $\tau \models \delta(Set\{Set\{2\},null\})$
value $\tau \models (Set\{2,1\} \rightarrow includes(1))$
value $\neg (\tau \models (Set\{2\} \rightarrow includes(1)))$
value $\neg (\tau \models (Set\{2,1\} \rightarrow includes(null)))$
value $\tau \models (Set\{2,null\} \rightarrow includes(null))$
value $\tau \models (Set\{null,2\} \rightarrow includes(null))$
value $\tau \models ((Set\{\} \rightarrow forAll(z \mid 0^<z))$
value $\tau \models ((Set\{2,1\}) \rightarrow forAll(z \mid 0^<z))$
value $\neg (\tau \models ((Set\{2,1\}) \rightarrow exists(z \mid 0^<z)))$
value $\neg (\tau \models \delta(Set\{2,null\} \rightarrow forAll(z \mid 0^<z))$
value $\neg (\tau \models ((Set\{2,null\}) \rightarrow exists(z \mid 0^<z)))$
value $\neg (\tau \models (Set\{null::'a Boolean\} \models Set\{\}))$
value $\neg (\tau \models (Set\{null::'a Integer\} \models Set\{\}))$
value $\tau \models (Set\{\lambda. x \models Set\{\lambda. x\})))$
value $\tau \models (Set\{\lambda. x \models Set\{\lambda. x\})))$

lemma $\neg (\tau \models (Set\{true\} \models Set\{false\}))$ (proof)
lemma $\neg (\tau \models (Set\{true,true\} \models Set\{false\}))$ (proof)
lemma $\neg (\tau \models (Set\{2\} \models Set\{1\}))$ (proof)
lemma $\tau \models (Set\{2,null,2\} \models Set\{null,2\})$ (proof)
lemma $\tau \models (Set\{1,null,2\} \rightarrow Set\{null,2\})$ (proof)
lemma $\tau \models (Set\{Set\{2,null\}\} \models Set\{Set\{null,2\}\})$ (proof)
lemma $\tau \models (Set\{Set\{2,\} \models Set\{Set\{null,2\}\}) (proof)$
lemma $\tau \models (Set\{null\} \rightarrow select(x \mid not x) \models Set\{null\})$ (proof)
lemma $\tau \models (Set\{null\} \rightarrow reject(x \mid not x) \models Set\{null\})$ (proof)
lemma $\text{const} (Set\{Set\{2,null\}, invalid\})$ (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 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.

\textbf{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:

\textbf{record} \((\mathcal{A})\text{state} = \)

heap :: "oid \rightarrow \mathcal{A}"
assocs\(_2::"oid\rightarrow(oid\times oid)\text{ list}"
assocs\(_3::"oid\rightarrow(oid\times oid\times oid)\text{ list}"

\textbf{type-synonym} \((\mathcal{A})\text{st} = \"\mathcal{A} \text{ state} \times \mathcal{A} \text{ 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).

\textbf{class} object = \textbf{fixes} oid-of :: \texttt{'}a \Rightarrow oid
Thus, if needed, we can constrain the object universe to objects by adding the following type class constraint:

\[
\text{typ } \mathcal{A} :: \text{object}
\]

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

\[
\text{instantiation } \text{option} :: (\text{object})\text{object}
\]

\[
\begin{definition}
\text{oid-of-option-def} : \text{oid-of } x = \text{oid-of } (\text{the } x)
\end{definition}
\]

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

5.2. Fundamental Predicates on Object: Strict Equality

Definition

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

\[
\begin{definition}
\text{StrictRefEqObject} :: (\mathcal{A},'a::{\text{object, null}})\text{val} \Rightarrow (\mathcal{A},'a)\text{val} \Rightarrow (\mathcal{A})\text{Boolean}
\end{definition}
\]

where

\[
\text{StrictRefEqObject } x \ y \\
\equiv \lambda \tau. \ if \ (v \ x) \tau = \text{true } \tau \land (v \ y) \tau = \text{true } \tau \then \if \ x \tau = \text{null } \lor \ y \tau = \text{null} \then \[(x \tau = \text{null } \land y \tau = \text{null} )\] \else \[(\text{oid-of } (x \tau)) = (\text{oid-of } (y \tau))\] \then \else \text{invalid } \tau
\]

5.2.1. Logic and Algebraic Layer on Object

Validity and Definedness Properties

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

\[
\text{lemma } \text{StrictRefEqObject-defargs}: \tau \models (\text{StrictRefEqObject } x \ (y::(\mathcal{A},'a::{\text{null, object}})\text{val})) \Rightarrow (\tau \models (v \ x)) \land (\tau \models (v \ y))
\]

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

Symmetry

\[
\text{lemma } \text{StrictRefEqObject-sym} :
\text{assumes } x\text{-val} : \tau \models v \ x
\text{shows } \tau \models \text{StrictRefEqObject } x \ x
\]

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

Execution with Invalid or Null as Argument

\[
\text{lemma } \text{StrictRefEqObject-strict1}[\text{simp, code-unfold}] : 
(\text{StrictRefEqObject } x \text{ invalid}) = \text{invalid}
\]

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

\[
\text{lemma } \text{StrictRefEqObject-strict2}[\text{simp, code-unfold}] :
\]

94
\[(\text{StrictRefEq}_\text{Object} \text{ invalid } x) = \text{invalid}\]

**Context Passing**

**lemma** cp-StrictRefEqObject:
\[(\text{StrictRefEq}_\text{Object} \ x \ y \ \tau) = (\text{StrictRefEq}_\text{Object} \ (\lambda \cdot. \ x \ \tau) \ (\lambda \cdot. \ y \ \tau)) \ \tau\]

**lemmas** cp-intro''[intro!, simp, code-unfold] =

cp-StrictRefEqObject[THEN allI[THEN allI[THEN allI[THEN cpI2]],
of StrictRefEqObject]]

**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** WFF :: (\(\forall :\text{object}\)\) st \Rightarrow \text{bool}

**where**
\[
\text{WFF} \ \tau = ((\forall \ x \in \text{ran} (\text{heap} (\text{fst} \ \tau)). \ [\text{heap} (\text{fst} \ \tau) (\text{oid-of} \ x)] = \ x) \land \\
(\forall \ x \in \text{ran} (\text{heap} (\text{snd} \ \tau)). \ [\text{heap} (\text{snd} \ \tau) (\text{oid-of} \ x)] = \ x))
\]

It turns out that WFF is a key-concept for linking strict referential equality to logical equality: in well-formed states (i.e. those states where the self (oid-of) field contains the pointer to which the object is associated to in the state), referential equality coincides with logical equality.

We turn now to the generic definition of referential equality on objects: Equality on objects in a state is reduced to equality on the references to these objects. As in HOL-OCL [6, 8], we will store the reference of an object inside the object in a (ghost) field. By establishing certain invariants (“consistent state”), it can be assured that there is a “one-to-one-correspondence” of objects to their references—and therefore the definition below behaves as we expect.

Generic Referential Equality enjoys the usual properties: (quasi) reflexivity, symmetry, transitivity, substitutivity for defined values. For type-technical reasons, for each concrete object type, the equality \(\doteq\) is defined by generic referential equality.

**theorem** StrictRefEqObject-vs-StrongEq:

**assumes** WFF: \(\text{WFF} \ \tau\)

**and** valid-x: \(\tau \models (\upsilon \ x)\)

**and** valid-y: \(\tau \models (\upsilon \ y)\)

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

shows \( (\tau \models (\text{StrictRefEq}_{\text{Object}} \ x \ y)) = (\tau \models (x \triangleq y)) \)

\( \langle \text{proof} \rangle \)

\textbf{Theorem:} \textit{StrictRefEq}_{\text{Object}}-\text{vs-StrongEq'}:
assumes \( \text{WFF}: \ WFF \ \tau \)
and \( \text{valid-x}: \ \tau \models (v \ x :: (\mathbb{A}::\text{object}, \alpha::\{\text{null}, \text{object}\})\text{val}) \)
and \( \text{valid-y}: \ \tau \models (v \ y) \)
and oid-preserve: \( \forall x. \ x \in \text{ran}(\text{heap}(\text{fst } \tau)) \lor x \in \text{ran}(\text{heap}(\text{snd } \tau)) \Rightarrow \)
\hspace{1cm} \( H \ x \neq \bot \Rightarrow \text{oid-of} (H \ x) = \text{oid-of} x \)
and xy-together: \( x \ \tau \in H \ \text{ran} (\text{heap}(\text{fst } \tau)) \land y \ \tau \in H \ \text{ran} (\text{heap}(\text{fst } \tau)) \lor \)
\hspace{1cm} \( x \ \tau \in H \ \text{ran} (\text{heap}(\text{snd } \tau)) \land y \ \tau \in H \ \text{ran} (\text{heap}(\text{snd } \tau)) \)

shows \( (\tau \models (\text{StrictRefEq}_{\text{Object}} \ x \ y)) = (\tau \models (x \triangleq y)) \)

\( \langle \text{proof} \rangle \)

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)

\textbf{Definition:} \( \tau_0 :: (\mathbb{A})\text{st} \)
where \( \tau_0 \equiv ((\text{heap} = \text{Map}.\text{empty}, \text{assocs}_2 = \text{Map}.\text{empty}, \text{assocs}_3 = \text{Map}.\text{empty}), \)
\hspace{1cm} \( (\text{heap} = \text{Map}.\text{empty}, \text{assocs}_2 = \text{Map}.\text{empty}, \text{assocs}_3 = \text{Map}.\text{empty}) \))

#### 5.3.2. OclAllInstances

To denote OCL types occurring in OCL expressions syntactically—as, for example, as “argument” of \( \text{oclAllInstances}() \)—we use the inverses of the injection functions into the object universes; we show that this is a sufficient “characterization.”

\textbf{Definition:} \( \text{OclAllInstances-generic} :: ((\mathbb{A}::\text{object}) \ \text{st} \Rightarrow \mathbb{A} \ \text{state}) \Rightarrow (\mathbb{A}::\text{object} \rightarrow \alpha) \Rightarrow (\mathbb{A}, \alpha \text{ option option}) \text{Set} \)
where \( \text{OclAllInstances-generic-fst-snd} \ H = \)
\hspace{1cm} \( (\lambda \tau. \text{Abs-Set-0} [\text{Some } (\text{(H } \ i \ \text{ran} (\text{fst-snd } \tau))). \text{val}) \}) \text{Set} \)

\textbf{Lemma:} \( \text{OclAllInstances-generic-defined}: \ \tau \models \delta (\text{OclAllInstances-generic pre-post} \ H) \)
\( \langle \text{proof} \rangle \)

\textbf{Lemma:} \( \text{OclAllInstances-generic-init-empty}: \)
assumes [simp]: \( \forall x. \ \text{pre-post} (x, x) = x \)
shows \( \tau_0 \models \text{OclAllInstances-generic pre-post} \ H \triangleq \text{Set}() \)
\( \langle \text{proof} \rangle \)

96
lemma represented-generic-objects-nonnul:
assumes $A: \tau \models ((\text{OclAllInstances-generic pre-post } (H::(\forall \text{object } \to 'a)))) \rightarrow \text{includes}(x)$
sows $\tau \models \text{not}(x \triangleq \text{null})$
(proof)

lemma represented-generic-objects-defined:
assumes $A: \tau \models ((\text{OclAllInstances-generic pre-post } (H::(\forall \text{object } \to 'a)))) \rightarrow \text{includes}(x)$
sows $\tau \models \delta \ (\text{OclAllInstances-generic pre-post } H) \land \tau \models \delta \ x$
(proof)

One way to establish the actual presence of an object representation in a state is:

lemma represented-generic-objects-in-state:
assumes $A: \tau \models (\text{OclAllInstances-generic pre-post } H) \rightarrow \text{includes}(x)$
sows $x \tau \in (\text{Some } o \ H) \ ' \ \text{ran} \ (\text{heap}(\text{pre-post } \tau))$
(proof)

lemma state-update-vs-allInstances-generic-empty:
assumes [simp]: $\forall a. \text{pre-post } (mk a) = a$
assumes $\forall x. \sigma' \oid = \text{Some } x \rightarrow x = \text{Object}$
and Type Object $\neq \text{None}$
sows $(\text{OclAllInstances-generic pre-post Type})$

$\forall a. \text{pre-post } (mk a) = a$

(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 [simp]: $\forall a. \text{pre-post } (mk a) = a$
assumes $\forall x. \sigma' \oid = \text{Some } x \rightarrow x = \text{Object}$
and Type Object $\neq \text{None}$
sows $(\text{OclAllInstances-generic pre-post Type})$

(proof)

lemma state-update-vs-allInstances-generic-including:
assumes [simp]: $\forall a. \text{pre-post } (mk a) = a$
assumes $\forall x. \sigma' \oid = \text{Some } x \rightarrow x = \text{Object}$
and Type Object $\neq \text{None}$
sows $(\text{OclAllInstances-generic pre-post Type})$

(proof)
\[ ((\lambda \cdot (\text{OclAllInstances-generic pre-post Type})
\quad (\text{mk } (\text{heap}=\sigma', \text{assocs}_2=A, \text{assocs}_3=B))) \Rightarrow \text{including}(\lambda \cdot \left\langle \text{drop} (\text{Type Object}) \right\rangle))
\]
\[ (\text{mk } (\text{heap}=\sigma'(\text{oid} \mapsto \text{Object}), \text{assocs}_2=A, \text{assocs}_3=B)) \]
\[ \langle \text{proof} \rangle \]

lemma state-update-vs-allInstances-generic-noincluding':
assumes [simp]: \( \forall a. \text{pre-post} (\text{mk} a) = a \)
assumes \( \forall x. \sigma' \text{ oid} = \text{Some } x \Rightarrow x = \text{Object} \)
and \text{Type Object} = \text{None}
shows (\text{OclAllInstances-generic pre-post Type})
\[ (\text{mk } (\text{heap}=\sigma'(\text{oid} \mapsto \text{Object}), \text{assocs}_2=A, \text{assocs}_3=B)) \]
\[ = \]
\[ (\text{OclAllInstances-generic pre-post Type})
\]
\[ (\text{mk } (\text{heap}=\sigma', \text{assocs}_2=A, \text{assocs}_3=B)) \]
\[ \langle \text{proof} \rangle \]

theorem state-update-vs-allInstances-generic-ntc:
assumes [simp]: \( \forall a. \text{pre-post} (\text{mk} a) = a \)
assumes oid-def: \( \text{oid} \notin \text{dom } \sigma' \)
and \text{non-type-conform}: \text{Type Object} = \text{None}
and \text{cp-ctxt}: \text{cp } P
and \text{const-ctxt}: \forall X. \text{const } X \Rightarrow \text{const } (P X)
shows (\text{OclAllInstances-generic pre-post Type})
\[ (\text{mk } (\text{heap}=\sigma'(\text{oid} \mapsto \text{Object}), \text{assocs}_2=A, \text{assocs}_3=B) \mid P) \]
\[ = \]
\[ (\text{mk } (\text{heap}=\sigma', \text{assocs}_2=A, \text{assocs}_3=B) \mid P) \]
\[ (\text{is } (\sigma \mid P ? \varphi) = (\sigma' \mid P ? \varphi)) \]
\[ \langle \text{proof} \rangle \]

theorem state-update-vs-allInstances-generic-tc:
assumes [simp]: \( \forall a. \text{pre-post} (\text{mk} a) = a \)
assumes oid-def: \( \text{oid} \notin \text{dom } \sigma' \)
and \text{type-conform}: \text{Type Object} \neq \text{None}
and \text{cp-ctxt}: \text{cp } P
and \text{const-ctxt}: \forall X. \text{const } X \Rightarrow \text{const } (P X)
shows (\text{OclAllInstances-generic pre-post Type})
\[ (\text{mk } (\text{heap}=\sigma'(\text{oid} \mapsto \text{Object}), \text{assocs}_2=A, \text{assocs}_3=B) \mid P) \]
\[ = \]
\[ (\text{mk } (\text{heap}=\sigma', \text{assocs}_2=A, \text{assocs}_3=B) \mid (\text{OclAllInstances-generic pre-post Type})\]
\[ \Rightarrow \text{including}(\lambda \cdot \left\langle \text{drop} (\text{Type Object}) \right\rangle) \]
\[ (\text{is } (\sigma \mid P ? \varphi) = (\sigma' \mid P ? \varphi')) \]
\[ \langle \text{proof} \rangle \]

declare OclAllInstances-generic-def [simp]
**OclAllInstances (@post)**

**definition** `OclAllInstances-at-post :: (A :: object → 'α) ⇒ (A, 'α option option) Set`

**where** `OclAllInstances-at-post = OclAllInstances-generic snd`

**lemma** `OclAllInstances-at-post-defined: τ ≜ δ (H .allInstances())`

**lemma** `τ0 ≜ H .allInstances() ≜ Set{}`

**lemma** `represented-at-post-objects-nonnull:
assumes A: τ ≜ ((H::(A::object → 'α)).allInstances()) −> includes(x)
shows τ ≜ not(x ≜ null)`

**lemma** `represented-at-post-objects-defined:
assumes A: τ ≜ ((H::(A::object → 'α)).allInstances()) −> includes(x)
shows τ ≜ δ (H .allInstances()) ∧ τ ≜ δ x`

One way to establish the actual presence of an object representation in a state is:

**lemma** `assumes A: τ ≜ H .allInstances() −> includes(x)
shows x τ ∈ (Some o H) . run (heap snd τ)`

**lemma** `state-update-vs-allInstances-at-post-empty:
shows (σ, (heap=empty, assocs₂=A, assocs₃=B)) |= Type .allInstances() ≜ Set{}`

Here comes a couple of operational rules that allow to infer the value of oclAllInstances from the context `τ`. These rules are a special-case in the sense that they are the only rules that relate statements with different `τ`'s. For that reason, new concepts like “constant contexts P” are necessary (for which we do not elaborate an own theory for reasons of space limitations; in examples, we will prove resulting constraints straight forward by hand).

**lemma** `state-update-vs-allInstances-at-post-including':
assumes A: τ ≜ H .allInstances() −> includes(x) and Type Object ≠ None
shows (Type .allInstances()) (σ, (heap=σ'(oid→Object), assocs₂=A, assocs₃=B)) = ((Type .allInstances()) −> including(λ - [ [ drop (Type Object) ] ])) (σ, (heap=σ', assocs₂=A, assocs₃=B))`
lemma state-update-vs-allInstances-at-post-including:
assumes $\forall x. \sigma' oid = \text{Some } x \implies x = \text{Object}$
and $\text{Type Object} \neq \text{None}$
shows ($\text{Type .allInstances()}$)
$\sigma, (heap=\sigma'(\text{oid}\to\text{Object}), \text{assoc}s_2=A, \text{assoc}s_3=B)$
$=\langle (\lambda -. (\text{Type .allInstances()}$)
$(\sigma, (heap=\sigma', \text{assoc}s_2=A, \text{assoc}s_3=B)) \implies \text{including}(\lambda -. [\text{drop } (\text{Type Object}$
$]])\rangle$)
$(\sigma, (heap=\sigma'(\text{oid}\to\text{Object}), \text{assoc}s_2=A, \text{assoc}s_3=B))$
\langle proof \rangle

lemma state-update-vs-allInstances-at-post-noincluding':
assumes $\forall x. \sigma' oid = \text{Some } x \implies x = \text{Object}$
and $\text{Type Object} = \text{None}$
shows ($\text{Type .allInstances()}$)
$\sigma, (heap=\sigma'(\text{oid}\to\text{Object}), \text{assoc}s_2=A, \text{assoc}s_3=B)$
$= (\text{Type .allInstances()}$)
$(\sigma, (heap=\sigma', \text{assoc}s_2=A, \text{assoc}s_3=B))$
\langle proof \rangle

theorem state-update-vs-allInstances-at-post-ntc:
assumes $\text{oid-def: oid} \notin \text{dom } \sigma'$
and $\text{non-type-conform: Type Object} = \text{None}$
and $\text{cp-ctxt: } \text{cp } P$
and $\text{const-ctxt: } \forall X. \text{const } X \implies \text{const } (P X)$
shows $((\sigma, (heap=\sigma'(\text{oid}\to\text{Object}), \text{assoc}s_2=A, \text{assoc}s_3=B)) \models (P(\text{Type .allInstances()})))$
$= ((\sigma, (heap=\sigma', \text{assoc}s_2=A, \text{assoc}s_3=B)) \models (P(\text{Type .allInstances()})))$
\langle proof \rangle

theorem state-update-vs-allInstances-at-post-tc:
assumes $\text{oid-def: oid} \notin \text{dom } \sigma'$
and $\text{type-conform: Type Object} \neq \text{None}$
and $\text{cp-ctxt: } \text{cp } P$
and $\text{const-ctxt: } \forall X. \text{const } X \implies \text{const } (P X)$
shows $((\sigma, (heap=\sigma'(\text{oid}\to\text{Object}), \text{assoc}s_2=A, \text{assoc}s_3=B)) \models (P(\text{Type .allInstances()})))$
$= ((\sigma, (heap=\sigma', \text{assoc}s_2=A, \text{assoc}s_3=B)) \models (P(\text{Type .allInstances()})))$
$\implies \text{including}(\lambda -. [(\text{Type Object}]))$)
\langle proof \rangle

OclAllInstances ($\text{@pre}$)
definition OclAllInstances-at-pre :: ($\forall \alpha :: \text{object} \to 'a) \Rightarrow ($\forall \alpha, 'a \text{ option option}) \text{ Set}$
$\forall .\text{allInstances}@pre('a))$
where \( \text{OclAllInstances-at-pre} = \text{OclAllInstances-generic fst} \)

**Lemma** \( \text{OclAllInstances-at-pre-defined: } \tau \models \delta (H\ .\ \text{allInstances@pre}()) \)

**Lemma** \( \tau_0 \models H\ .\ \text{allInstances@pre}() \triangleq \text{Set}\{\} \)

**Lemma** \( \text{represented-at-pre-objects-nonnul}: \)

**Assumes** \( A: \tau \models (((H::(\forall::\text{object} \to 'a)).\ \text{allInstances@pre}()) \to >\text{includes}(x)) \)

**Shows** \( \tau \models \neg(x \triangleq \text{null}) \)

**Lemma** \( \text{represented-at-pre-objects-defined}: \)

**Assumes** \( A: \tau \models (((H::(\forall::\text{object} \to 'a)).\ \text{allInstances@pre}()) \to >\text{includes}(x)) \)

**Shows** \( \tau \models \delta (H\ .\ \text{allInstances@pre}()) \land \tau \models \delta \ x \)

One way to establish the actual presence of an object representation in a state is:

**Lemma** \( \text{assumes A: } \tau \models H\ .\ \text{allInstances@pre}() \to >\text{includes}(x) \)

**Shows** \( x \quad \tau \in (\text{Some o H}) \cdot \text{run} (\text{heap(fst } \tau)) \)

**Lemma** \( \text{state-update-vs-allInstances-at-pre-empty:} \)

**Shows** \( (\text{\{heap=empty, assoc}\_2=A, assoc}\_3=B\}, \sigma) \models \text{Type} \ .\ \text{allInstances@pre}() = \text{Set}\{\} \)

Here comes a couple of operational rules that allow to infer the value of \( \text{oclAllInstances@pre} \) from the context \( \tau \). These rules are a special-case in the sense that they are the only rules that relate statements with different \( \tau \)'s. For that reason, new concepts like “constant contexts P” are necessary (for which we do not elaborate an own theory for reasons of space limitations; in examples, we will prove resulting constraints straightforward by hand).

**Lemma** \( \text{state-update-vs-allInstances-at-pre-including'}: \)

**Assumes** \( \forall x. \sigma' \quad \text{oid = Some } x \implies x = \text{Object} \)

**And** \( \text{Type Object } \neq \text{None} \)

**Shows** \( (\text{Type} \ .\ \text{allInstances@pre}(\sigma)) \)

\[
(\text{\{heap=\sigma'\{\text{oid}\to \text{Object}\}, assoc}\_2=A, assoc}\_3=B\}, \sigma) \\
= \\
(\text{\{Type} \ .\ \text{allInstances@pre}(\sigma) \to >\text{including}(\lambda\ .\ \text{drop} (\text{Type Object}) )) \\
\text{\{heap=\sigma', assoc}\_2=A, assoc}\_3=B\}, \sigma)
\]

**Proof**

**Lemma** \( \text{state-update-vs-allInstances-at-pre-including:} \)

**Assumes** \( \forall x. \sigma' \quad \text{oid = Some } x \implies x = \text{Object} \)
and Type Object \neq \text{None}

\text{shows} (\text{Type} . \text{allInstances}@\text{pre}())

(\{\text{heap}=\sigma'(\text{oid}\to\text{Object}), \text{assocs}_2=\text{A}, \text{assocs}_3=\text{B}\}, \sigma) =

(\text{\{\lambda - (\text{Type} . \text{allInstances}@\text{pre}())

(\{\text{heap}=\sigma', \text{assocs}_2=\text{A}, \text{assocs}_3=\text{B}\}, \sigma)\}) \rightarrow \text{including}(\lambda - [:\text{drop} (\text{Type} \text{Object})])\})

(\{\text{heap}=\sigma' (\text{oid}\to\text{Object}), \text{assocs}_2=\text{A}, \text{assocs}_3=\text{B}\}, \sigma)

\langle \text{proof} \rangle

\text{lemma} \text{state-update-vs-allInstances-at-pre-noincluding'}:
\text{assumes} \bigwedge x. \sigma' \text{oid} = \text{Some} x \implies x = \text{Object}
\text{and} Type Object = \text{None}

\text{shows} (\text{Type} . \text{allInstances}@\text{pre}())

(\{\text{heap}=\sigma'(\text{oid}\to\text{Object}), \text{assocs}_2=\text{A}, \text{assocs}_3=\text{B}\}, \sigma) =

(\text{\{\text{heap}=\sigma', \text{assocs}_2=\text{A}, \text{assocs}_3=\text{B}\}, \sigma)

\langle \text{proof} \rangle

\text{theorem} \text{state-update-vs-allInstances-at-pre-ntc}:
\text{assumes} \text{oid-def}: \text{oid} \notin \text{dom} \sigma'
\text{and} \text{non-type-conform}: Type Object = \text{None}
\text{and} \text{cp-ctxt}: \text{cp} \text{P}
\text{and} \text{const-ctxt}: \bigwedge X. \text{const} X \implies \text{const} (\text{P} \text{X})

\text{shows} ((\{\text{heap}=\sigma'(\text{oid}\to\text{Object}), \text{assocs}_2=\text{A}, \text{assocs}_3=\text{B}\}, \sigma) \models (\text{P}(\text{Type} . \text{allInstances}@\text{pre}())))

= (\{\text{heap}=\sigma', \text{assocs}_2=\text{A}, \text{assocs}_3=\text{B}\}, \sigma) \models (\text{P}(\text{Type} . \text{allInstances}@\text{pre}())))

\langle \text{proof} \rangle

\text{theorem} \text{state-update-vs-allInstances-at-pre-tc}:
\text{assumes} \text{oid-def}: \text{oid} \notin \text{dom} \sigma'
\text{and} \text{type-conform}: Type Object \neq \text{None}
\text{and} \text{cp-ctxt}: \text{cp} \text{P}
\text{and} \text{const-ctxt}: \bigwedge X. \text{const} X \implies \text{const} (\text{P} \text{X})

\text{shows} ((\{\text{heap}=\sigma'(\text{oid}\to\text{Object}), \text{assocs}_2=\text{A}, \text{assocs}_3=\text{B}\}, \sigma) \models (\text{P}(\text{Type} . \text{allInstances}@\text{pre}())))

= (\{\text{heap}=\sigma', \text{assocs}_2=\text{A}, \text{assocs}_3=\text{B}\}, \sigma) \models (\text{P}(\text{Type} . \text{allInstances}@\text{pre}())))

\langle \text{proof} \rangle

@\text{post or @pre}

\text{theorem} \text{StrictRefEqObject-vs-StrongEq''}:
\text{assumes} \text{WFF}: \text{WFF} \tau
\text{and} \text{valid-x}: \tau \models \text{(v x :: (A::object,'a::object option option)val)}
\text{and} \text{valid-y}: \tau \models \text{(v y)}

102
and \(\text{oid-preserve}: \forall x. x \in \text{ran}(\text{heap}(f\text{st}\ \tau)) \lor x \in \text{ran}(\text{heap}(\text{snd}\ \tau)) \implies \text{oid-of}(H\ x) = \text{oid-of}\ x\)

and \(xy\text{-together}: \tau \models ((H\ .\text{allInstances}() \to \text{includes}(x) \land H\ .\text{allInstances}() \to \text{includes}(y))
\lor
(H\ .\text{allInstances}@\text{pre}() \to \text{includes}(x) \land H\ .\text{allInstances}@\text{pre}() \to \text{includes}(y)))

shows \((\tau \models (\text{StrictRefEq}\text{Object}\ x\ y)) = (\tau \models (x \triangleq y))\)

\(\langle\text{proof}\rangle\)

### 5.3.3. OclIsNew, OclIsDeleted, OclIsMaintained, OclIsAbsent

definition \(\text{OclIsNew}: (\emptyset, \alpha::\{\text{null, object}\})\)\text{val} \to (\emptyset)\text{Boolean} \quad (\_\_\_.\text{oclIsNew}'(\_))

where \(\text{X} .\text{oclIsNew()} \equiv (\lambda\tau. \text{if}\ (\delta\ \text{X})\ \tau = \text{true}\ \tau
\text{then} \left[(\\text{oid-of}\ (X\ \tau) \notin \text{dom}(\text{heap}(\text{fst}\ \tau)) \land \text{oid-of}(X\ \tau) \in \text{dom}(\text{heap}(\text{snd}\ \tau))]\right]
\text{else}\ \text{invalid}\ \tau)

definition \(\text{OclIsDeleted}: (\emptyset, \alpha::\{\text{null, object}\})\)\text{val} \to (\emptyset)\text{Boolean} \quad (\_\_\_.\text{oclIsDeleted}'(\_))

where \(\text{X} .\text{oclIsDeleted()} \equiv (\lambda\tau. \text{if}\ (\delta\ \text{X})\ \tau = \text{true}\ \tau
\text{then} \left[(\\text{oid-of}\ (X\ \tau) \notin \text{dom}(\text{heap}(\text{fst}\ \tau)) \land \text{oid-of}(X\ \tau) \in \text{dom}(\text{heap}(\text{snd}\ \tau))]\right]
\text{else}\ \text{invalid}\ \tau)

definition \(\text{OclIsMaintained}: (\emptyset, \alpha::\{\text{null, object}\})\)\text{val} \to (\emptyset)\text{Boolean} \quad (\_\_\_.\text{oclIsMaintained}'(\_))

where \(\text{X} .\text{oclIsMaintained()} \equiv (\lambda\tau. \text{if}\ (\delta\ \text{X})\ \tau = \text{true}\ \tau
\text{then} \left[(\\text{oid-of}\ (X\ \tau) \notin \text{dom}(\text{heap}(\text{fst}\ \tau)) \land \text{oid-of}(X\ \tau) \notin \text{dom}(\text{heap}(\text{snd}\ \tau))]\right]
\text{else}\ \text{invalid}\ \tau)

definition \(\text{OclIsAbsent}: (\emptyset, \alpha::\{\text{null, object}\})\)\text{val} \to (\emptyset)\text{Boolean} \quad (\_\_\_.\text{oclIsAbsent}'(\_))

where \(\text{X} .\text{oclIsAbsent()} \equiv (\lambda\tau. \text{if}\ (\delta\ \text{X})\ \tau = \text{true}\ \tau
\text{then} \left[(\\text{oid-of}\ (X\ \tau) \notin \text{dom}(\text{heap}(\text{fst}\ \tau)) \land \text{oid-of}(X\ \tau) \notin \text{dom}(\text{heap}(\text{snd}\ \tau))]\right]
\text{else}\ \text{invalid}\ \tau)

lemma \(\text{state-split}: \tau \models \delta\ \text{X} \implies\)

\(\tau \models (X .\text{oclIsNew}()) \lor \tau \models (X .\text{oclIsDeleted}()) \lor \tau \models (X .\text{oclIsMaintained}()) \lor \tau \models (X .\text{oclIsAbsent}())\)

\(\langle\text{proof}\rangle\)

lemma \(\text{notNew-vs-others}: \tau \models \delta\ \text{X} \implies\)

\(-\tau \models (X .\text{oclIsNew}()) = (\tau \models (X .\text{oclIsDeleted}()) \lor \tau \models (X .\text{oclIsMaintained}()) \lor \tau \models (X .\text{oclIsAbsent}())\)

\(\langle\text{proof}\rangle\)
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.

\[
\text{OclIsModifiedOnly} \; :: \; (A : \text{object}, \alpha : \{\text{null, object}\}) \Rightarrow (\text{Set} \Rightarrow (\text{Boolean}))
\]

where

\[
X \rightarrow \text{OclIsModifiedOnly}(\cdot) \equiv (\lambda (\sigma, \sigma'). (\delta X)(\sigma, \sigma') = \text{true}) \land (\forall x \in [\text{Rep-Set-0}(X(\sigma, \sigma'))]. x \neq \text{null})
\]

\[
\text{let } X' = (\text{oid-of} \cdot [\text{Rep-Set-0}(X(\sigma, \sigma'))]);
\]

\[
S = (\text{dom}(\text{heap } \sigma) \cap \text{dom}(\text{heap } \sigma')) - X'
\]

\[
\text{in if } (\delta X)(\sigma, \sigma') = \text{true} \land (\forall x \in [\text{Rep-Set-0}(X(\sigma, \sigma'))]. x \neq \text{null})
\]

\[
\text{then } (\forall x \in S. (\text{heap } \sigma) x = (\text{heap } \sigma') x)
\]

\[
\text{else invalid } (\sigma, \sigma')
\]

Execution with Invalid or Null or Null Element as Argument

\[
\text{lemma invalid-} \rightarrow \text{OclIsModifiedOnly}() = \text{invalid}
\]

\[
\text{lemma null-} \rightarrow \text{OclIsModifiedOnly}() = \text{invalid}
\]

\[
\text{lemma}
\]

\[
\text{assumes } X-\text{null} : \tau \models X \rightarrow \text{includes}(\text{null})
\]

\[
\text{shows } \tau \models X \rightarrow \text{OclIsModifiedOnly}() \equiv \text{invalid}
\]

\[
\text{Context Passing}
\]

\[
\text{lemma cp-OclIsModifiedOnly} : X \rightarrow \text{OclIsModifiedOnly}() \tau = (\lambda \cdot X \tau) \rightarrow \text{OclIsModifiedOnly}() \tau
\]

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.

\[
\text{definition simp : OclSelf } x \; H \; \text{fst-snd} = (\lambda \tau . \text{if } (\delta x) \tau = \text{true} \tau
\]

\[
\text{then if oid-of } (x \tau) \in \text{dom}(\text{heap } \text{fst-snd } \tau) \land \text{oid-of } (x \tau) \in \text{dom}(\text{heap } \text{snd } \tau)
\]

\[
\text{then } H \; ([\text{heap}(\text{fst-snd } \tau))(\text{oid-of } (x \tau))]
\]

\[
\text{else invalid } \tau
\]

\[
\text{else invalid } \tau
\]

\[
\text{definition OclSelf-at-pre :: (A : object, } \alpha : \{\text{null, object}\}) \text{val ⇒}
\]
where \( x \odot \text{pre} \ H = \text{OclSelf} \ x \ H \ \text{fst} \)

definition \( \text{OclSelf-at-post} :: (\text{'A :: object, 'a :: \{null, object\}}) \Rightarrow (\text{'A} \Rightarrow \text{'a} \Rightarrow (\text{'A :: object, 'a :: \{null, object\}}) \Rightarrow ((-)@\text{pre}(-))) \)

where \( x \odot @ \text{post} \ H = \text{OclSelf} \ x \ H \ \text{snd} \)

### 5.3.6. Framing Theorem

**Lemma all-oid-diff:**

assumes \( \text{def-x} : \tau |\Delta=\delta \ x \)

assumes \( \text{def-X} : \tau |\Delta=\delta \ X \)

assumes \( \text{def-X'} : \forall x. x \in \text{\{Rep-Set-0 (X \tau)\}} \implies x \neq \text{null} \)

defines \( P \equiv (\lambda a. \neg \text{StrictRefEqObject x a}) \)

shows \( \tau |\Delta=\forall a (\text{oid-of (x} \tau) \notin \text{oid-of \{Rep-Set-0 (X \tau)\}}) \)

⟨proof⟩

**Theorem framing:**

assumes \( \text{modifiesclause:} \tau |\Delta= (X \Rightarrow \text{excluding(x)} \Rightarrow \text{oclIsModifiedOnly()} \)

and \( \text{oid-is-typerepr :} \tau |\Delta= (X \Rightarrow \forall a (\text{not (StrictRefEqObject x a)}) \)

shows \( \tau |\Delta= (x \odot \text{pre} P \triangleq (x \odot \text{post} P)) \)

⟨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 \( \text{modifiesclause:} \tau |\Delta= (X \Rightarrow \text{excluding(x)} \Rightarrow \text{oclIsModifiedOnly()} \)

and \( \text{oid-is-typerepr :} \tau |\Delta= (X \Rightarrow \forall a (\text{not (x} \triangleq a)) \)

and \( \text{oid-preserve:} \forall x. x \in \text{ran (heap(fst \ \tau))} \lor x \in \text{ran (heap(snd \ \tau))} \implies \text{oid-of (H x) = oid-of x} \)

and \( \text{zy-together:} \)

\( \tau |\Delta= \forall y \mid (H . \text{allInstances}() \Rightarrow \text{includes(x)} \text{ and H .} \text{allInstances}() \Rightarrow \text{includes(y)} \text{ or} \) \)

\( (H . \text{allInstances}@\text{pre}() \Rightarrow \text{includes(x)} \text{ and H .} \text{allInstances}@\text{pre}() \Rightarrow \text{includes(y)}) \)

shows \( \tau |\Delta= (x \odot \text{pre} P \triangleq (x \odot \text{post} P)) \)

⟨proof⟩

### 5.3.7. Miscellaneous

**Lemma pre-post-new: \( \tau |\Delta= (x . \text{oclIsNew}()) \Rightarrow \neg (\tau |\Delta= v(x \odot \text{pre} H1)) \land \neg (\tau |\Delta= v(x \odot \text{post} H2)) \)

⟨proof⟩

**Lemma pre-post-old: \( \tau |\Delta= (x . \text{oclIsDeleted}()) \Rightarrow \neg (\tau |\Delta= v(x \odot \text{pre} H1)) \land \neg (\tau |\Delta= v(x \odot \text{post} H2)) \)

⟨proof⟩
**lemma** pre-post-absent: \( \tau \models (x.\text{oclIsAbsent}()) \implies \neg (\tau \models v(x @\text{pre } H1)) \land \neg (\tau \models v(x @\text{post } H2)) \)

\langle \text{proof} \rangle

**lemma** pre-post-maintained: \( (\tau \models v(x @\text{pre } H1) \lor \tau \models v(x @\text{post } H2)) \implies (\tau \models (x.\text{oclIsMaintained}())) \)

\langle \text{proof} \rangle

**lemma** pre-post-maintained':
\( (\tau \models (x.\text{oclIsMaintained}()) \implies (\tau \models v(x @\text{pre } (\text{Some o } H1)) \land \tau \models v(x @\text{post } (\text{Some o } H2))) \)

\langle \text{proof} \rangle

**lemma** framing-same-state: \( (\sigma, \sigma) \models (x @\text{pre } H \equiv (x @\text{post } H)) \)

\langle \text{proof} \rangle

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).
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:

\[
\text{datatype } \text{typePerson} = \text{mkPerson} \text{ oid} \\
\text{int option}
\]

\[
\text{datatype } \text{typeOclAny} = \text{mkOclAny} \text{ oid} \\
\text{(int option) option}
\]

Now, we construct a concrete “universe of OclAny types” by injection into a sum type containing the class types. This type of OclAny will be used as instance for all respective type-variables.

\[
\text{datatype } \text{A} = \text{inPerson} \text{ typePerson} | \text{inOclAny} \text{ typeOclAny}
\]

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.

\[
\text{type-synonym } \text{Boolean} = \text{A} \text{ Boolean} \\
\text{type-synonym } \text{Integer} = \text{A} \text{ Integer} \\
\text{type-synonym } \text{Void} = \text{A} \text{ Void} \\
\text{type-synonym } \text{OclAny} = (\text{A}, \text{typeOclAny option option}) \text{ val} \\
\text{type-synonym } \text{Person} = (\text{A}, \text{typePerson option option}) \text{ val} \\
\text{type-synonym } \text{Set-Integer} = (\text{A}, \text{int option option}) \text{ Set} \\
\text{type-synonym } \text{Set-Person} = (\text{A}, \text{typePerson option option}) \text{ Set}
\]

Just a little check:

\[
\text{typ } \text{Boolean}
\]

To reuse key-elements of the library like referential equality, we have to show that the
object universe belongs to the type class “oclany,” i.e., each class type has to provide a function oid-of yielding the object id (oid) of the object.

instantiation type Person :: object
begin
   definition oid-of-type Person-def: oid-of x = (case x of mkPerson oid - ⇒ oid)
   instance ⟨proof⟩
end

instantiation type OclAny :: object
begin
   definition oid-of-type OclAny-def: oid-of x = (case x of mkOclAny oid - ⇒ oid)
   instance ⟨proof⟩
end

instantiation A :: object
begin
   definition oid-of-A-def: oid-of x = (case x of
      in Person person ⇒ oid-of person
      | in OclAny oclany ⇒ oid-of oclany)
   instance ⟨proof⟩
end

6.1.3. 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 ⇒ PersonQ::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.

6.1.4. OclAsType

Definition

consts OclAsType\_OclAny :: 'a ⇒ OclAny ((-) . oclAsType 'OclAny')
consts OclAsType\_Person :: 'a ⇒ Person ((-) . oclAsType 'Person')

definition OclAsType\_OclAny\_A = (λu. [ case u of in\_OclAny a ⇒ a
                             | in\_Person (mk\_Person oid a) ⇒ mk\_OclAny oid [a] ])

lemma OclAsType\_OclAny\_A\_some: OclAsType\_OclAny\_A x ≠ None
⟨proof⟩

defs (overloaded) OclAsType\_OclAny\_OclAny:
(X::OclAny) . oclAsType (OclAny) ≡ X

defs (overloaded) OclAsType\_OclAny\_Person:
(X::Person) . oclAsType (OclAny) ≡
(λτ. case X τ of
  ⊥ ⇒ invalid τ
  | [⊥] ⇒ null τ
  | [mk\_Person oid a ] ⇒ [mk\_OclAny oid a ])

definition OclAsType\_Person\_A = (λu. case u of in\_Person p ⇒ [p]
                             | in\_OclAny (mk\_OclAny oid [a]) ⇒ [mk\_Person oid a]
                             | - ⇒ None)

defs (overloaded) OclAsType\_Person\_OclAny:
(X::OclAny) . oclAsType (Person) ≡
(λτ. case X τ of
  ⊥ ⇒ invalid τ
  | [⊥] ⇒ null τ
  | [mk\_OclAny oid ⊥ ] ⇒ invalid τ (* down–cast exception *)
  | [mk\_OclAny oid [a] ] ⇒ [mk\_Person oid a ])

defs (overloaded) OclAsType\_Person\_Person:
(X::Person) . oclAsType (Person) ≡ X

lemmas [simp] =
OclAsType\_OclAny\_OclAny
OclAsType\_Person\_Person

Context Passing

lemma cp\_OclAsType\_OclAny\_Person\_Person: cp P ⇒ cp (λX. (P (X::Person)::Person) . oclAsType (OclAny))
⟨proof⟩
lemma \( cp\text{-}OclAsType\_OclAny\_OclAny\_OclAny \): \( cp \ P \Rightarrow cp(\lambda X. \ (P \ (X::OclAny)::OclAny))\)
\( \text{oclAsType}(\text{OclAny}) \)
\( \{\text{proof}\} \)

lemma \( cp\text{-}OclAsType\_Person\_Person\_Person \): \( cp \ P \Rightarrow cp(\lambda X. \ (P \ (X::Person)::Person))\)
\( \text{oclAsType}(\text{Person}) \)
\( \{\text{proof}\} \)

lemma \( cp\text{-}OclAsType\_Person\_OclAny\_OclAny \): \( cp \ P \Rightarrow cp(\lambda X. \ (P \ (X::OclAny)::OclAny))\)
\( \text{oclAsType}(\text{Person}) \)
\( \{\text{proof}\} \)

lemma \( cp\text{-}OclAsType\_OclAny\_Person\_Person \): \( cp \ P \Rightarrow cp(\lambda X. \ (P \ (X::Person)::OclAny))\)
\( \text{oclAsType}(\text{OclAny}) \)
\( \{\text{proof}\} \)

lemma \( cp\text{-}OclAsType\_OclAny\_Person\_OclAny \): \( cp \ P \Rightarrow cp(\lambda X. \ (P \ (X::OclAny)::OclAny))\)
\( \text{oclAsType}(\text{Person}) \)
\( \{\text{proof}\} \)

lemma \( cp\text{-}OclAsType\_Person\_OclAny\_OclAny \): \( cp \ P \Rightarrow cp(\lambda X. \ (P \ (X::OclAny)::OclAny))\)
\( \text{oclAsType}(\text{Person}) \)
\( \{\text{proof}\} \)

lemma \( cp\text{-}OclAsType\_OclAny\_OclAny\_Person \): \( cp \ P \Rightarrow cp(\lambda X. \ (P \ (X::Person)::OclAny))\)
\( \text{oclAsType}(\text{OclAny}) \)
\( \{\text{proof}\} \)

lemma \( cp\text{-}OclAsType\_Person\_OclAny\_OclAny \): \( cp \ P \Rightarrow cp(\lambda X. \ (P \ (X::OclAny)::OclAny))\)
\( \text{oclAsType}(\text{Person}) \)
\( \{\text{proof}\} \)

lemma \( cp\text{-}OclAsType\_OclAny\_Person\_OclAny \): \( cp \ P \Rightarrow cp(\lambda X. \ (P \ (X::Person)::OclAny))\)
\( \text{oclAsType}(\text{Person}) \)
\( \{\text{proof}\} \)

lemma \( cp\text{-}OclAsType\_OclAny\_OclAny\_Person \): \( cp \ P \Rightarrow cp(\lambda X. \ (P \ (X::Person)::OclAny))\)
\( \text{oclAsType}(\text{OclAny}) \)
\( \{\text{proof}\} \)

lemmas \( \text{[simp]} \) =
\( cp\text{-}OclAsType\_OclAny\_Person\_Person \)
\( cp\text{-}OclAsType\_OclAny\_OclAny\_OclAny \)
\( cp\text{-}OclAsType\_Person\_Person\_Person \)
\( cp\text{-}OclAsType\_Person\_OclAny\_OclAny \)
\( cp\text{-}OclAsType\_OclAny\_Person\_Person \)
\( cp\text{-}OclAsType\_Person\_OclAny\_OclAny \)
\( cp\text{-}OclAsType\_Person\_Person\_OclAny \)
\( cp\text{-}OclAsType\_Person\_OclAny\_Person \)
\( \{\text{proof}\} \)

Execution with Invalid or Null as Argument

lemma \( OclAsType\_OclAny\_OclAny\text{-}\text{strict} : (\text{invalid}::\text{OclAny}) \ .\text{oclAsType}(\text{OclAny}) = \text{invalid} \)
\( \{\text{proof}\} \)

lemma \( OclAsType\_OclAny\_OclAny\text{-}\text{nullstrict} : (\text{null}::\text{OclAny}) \ .\text{oclAsType}(\text{OclAny}) = \text{null} \)
\( \{\text{proof}\} \)

lemma \( OclAsType\_OclAny\_Person\text{-}\text{strict}[\text{simp}] : (\text{invalid}::\text{Person}) \ .\text{oclAsType}(\text{OclAny}) = \text{invalid} \)
\( \{\text{proof}\} \)

lemma \( OclAsType\_OclAny\_Person\text{-}\text{nullstrict}[\text{simp}] : (\text{null}::\text{Person}) \ .\text{oclAsType}(\text{OclAny}) = \text{null} \)
\( \{\text{proof}\} \)

lemma \( OclAsType\_Person\text{-}\text{OclAny}\text{-}\text{strict}[\text{simp}] : (\text{invalid}::\text{OclAny}) \ .\text{oclAsType}(\text{Person}) = \text{invalid} \)
proof

lemma OclAsTypePerson-OclAny-nullstrict[simp]: (null::OclAny).oclAsType(Person) = null
proof

lemma OclAsTypePerson-Person-strict: (invalid::Person).oclAsType(Person) = invalid
proof

lemma OclAsTypePerson-Person-nullstrict: (null::Person).oclAsType(Person) = null
proof

6.1.5. OclIsTypeOf

Definition

consts OclIsTypeOfOclAny :: 'a ⇒ Boolean\((\_,\_).oclIsTypeOf\(['OclAny']\))
consts OclIsTypeOfPerson :: 'a ⇒ Boolean\((\_,\_).oclIsTypeOf\(['Person']\))

defs (overloaded) OclIsTypeOfOclAny-OclAny:
\[(X::OclAny).oclIsTypeOf(OclAny) \equiv (\lambda \tau.\ \text{case } X \ \tau \ of \ \left\{ \begin{array}{ll} \bot \Rightarrow \text{invalid } \tau \\
| \bot \Rightarrow \text{true } \tau \ (\ast \ \text{invalid } ?? \ *) \\
| \text{mkOclAny \ oid } \bot \Rightarrow \text{true } \tau \\
| \text{mkOclAny \ oid } [\ - ] \Rightarrow \text{false } \tau \\
\right.\)\]

defs (overloaded) OclIsTypeOfOclAny-Person:
\[(X::Person).oclIsTypeOf(OclAny) \equiv (\lambda \tau.\ \text{case } X \ \tau \ of \ \left\{ \begin{array}{ll} \bot \Rightarrow \text{invalid } \tau \\
| \bot \Rightarrow \text{true } \tau \ (\ast \ \text{invalid } ?? \ *) \\
| [\ - ] \Rightarrow \text{false } \tau \\
\right.\)\]

defs (overloaded) OclIsTypeOfPerson-OclAny:
\[(X::OclAny).oclIsTypeOf(Person) \equiv (\lambda \tau.\ \text{case } X \ \tau \ of \ \left\{ \begin{array}{ll} \bot \Rightarrow \text{invalid } \tau \\
| \bot \Rightarrow \text{true } \tau \\
| \text{mkOclAny \ oid } \bot \Rightarrow \text{false } \tau \\
| \text{mkOclAny \ oid } [\ - ] \Rightarrow \text{true } \tau \\
\right.\)\]

defs (overloaded) OclIsTypeOfPerson-Person:
\[(X::Person).oclIsTypeOf(Person) \equiv (\lambda \tau.\ \text{case } X \ \tau \ of \ \left\{ \begin{array}{ll} \bot \Rightarrow \text{invalid } \tau \\
| [\ - ] \Rightarrow \text{true } \tau \\
\right.\)\]
Context Passing

\[
\text{lemma } \text{cp-OclIsTypeOf}\text{OclAny-Person-Person}: \quad \text{cp}(\lambda X. (P(X::\text{Person})::\text{Person}).\text{oclIsTypeOf}(\text{OclAny}))
\]

(\text{proof})

\[
\text{lemma } \text{cp-OclIsTypeOf}\text{OclAny-OclAny-OclAny}: \quad \text{cp}(\lambda X. (P(X::\text{OclAny})::\text{OclAny}).\text{oclIsTypeOf}(\text{OclAny}))
\]

(\text{proof})

\[
\text{lemma } \text{cp-OclIsTypeOf}\text{Person-Person-Person}: \quad \text{cp}(\lambda X. (P(X::\text{Person})::\text{Person}).\text{oclIsTypeOf}(\text{Person}))
\]

(\text{proof})

\[
\text{lemma } \text{cp-OclIsTypeOf}\text{Person-OclAny-OclAny}: \quad \text{cp}(\lambda X. (P(X::\text{OclAny})::\text{OclAny}).\text{oclIsTypeOf}(\text{Person}))
\]

(\text{proof})

\[
\text{lemma } \text{cp-OclIsTypeOf}\text{Person-Person-OclAny}: \quad \text{cp}(\lambda X. (P(X::\text{Person})::\text{OclAny}).\text{oclIsTypeOf}(\text{Person}))
\]

(\text{proof})

\[
\text{lemma } \text{cp-OclIsTypeOf}\text{Person-OclAny-Person}: \quad \text{cp}(\lambda X. (P(X::\text{OclAny})::\text{Person}).\text{oclIsTypeOf}(\text{Person}))
\]

(\text{proof})

\[
\text{lemmas } [\text{simp}] = \\
\text{cp-OclIsTypeOf}\text{OclAny-Person-Person} \\
\text{cp-OclIsTypeOf}\text{OclAny-OclAny-OclAny} \\
\text{cp-OclIsTypeOf}\text{Person-Person-Person} \\
\text{cp-OclIsTypeOf}\text{Person-OclAny-OclAny} \\
\text{cp-OclIsTypeOf}\text{OclAny-Person-OclAny} \\
\text{cp-OclIsTypeOf}\text{OclAny-OclAny-Person} \\
\text{cp-OclIsTypeOf}\text{Person-Person-OclAny} \\
\text{cp-OclIsTypeOf}\text{Person-OclAny-Person}
\]

Execution with Invalid or Null as Argument

\[
\text{lemma } \text{OclIsTypeOf}\text{OclAny-OclAny-strict1}[\text{simp}]: \\
(\text{invalid}::\text{OclAny}) . \text{oclIsTypeOf}(\text{OclAny}) = \text{invalid}
\]

(\text{proof})

\[
\text{lemma } \text{OclIsTypeOf}\text{OclAny-OclAny-strict2}[\text{simp}]: \\
(\text{null}::\text{OclAny}) . \text{oclIsTypeOf}(\text{OclAny}) = \text{true}
\]

(\text{proof})

\[
\text{lemma } \text{OclIsTypeOf}\text{OclAny-Person-strict1}[\text{simp}]: \\
(\text{invalid}::\text{Person}) . \text{oclIsTypeOf}(\text{OclAny}) = \text{invalid}
\]
lemma OclIsTypeOf_OclAny-Person-strict2[simp]:
  (null::Person) .oclIsTypeOf(OclAny) = true
⟨proof⟩

lemma OclIsTypeOf_Person-OclAny-strict1[simp]:
  (invalid::OclAny) .oclIsTypeOf(Person) = invalid
⟨proof⟩

lemma OclIsTypeOf_Person-Person-strict1[simp]:
  (invalid::Person) .oclIsTypeOf(Person) = invalid
⟨proof⟩

lemma OclIsTypeOf_Person-Person-strict2[simp]:
  (null::Person) .oclIsTypeOf(Person) = true
⟨proof⟩

Up Down Casting

lemma actualType-larger-staticType:
assumes isdef: τ |= (δ X)
shows τ |= (X::Person) .oclIsTypeOf(OclAny) ≜ false
⟨proof⟩

lemma down-cast-type:
assumes isOclAny: τ |= (X::OclAny) .oclIsTypeOf(OclAny)
and non-null: τ |= (δ X)
shows τ |= (X .oclAsType(Person)) ≜ invalid
⟨proof⟩

lemma down-cast-type’:
assumes isOclAny: τ |= (X::OclAny) .oclIsTypeOf(OclAny)
and non-null: τ |= (δ X)
shows τ |= not (v (X .oclAsType(Person)))
⟨proof⟩

lemma up-down-cast :
assumes isdef: τ |= (δ X)
shows τ |= ((X::Person) .oclAsType(OclAny) .oclAsType(Person) ≜ X)
⟨proof⟩

lemma up-down-cast-Person-OclAny-Person [simp]:
shows ((X::Person) .oclAsType(OclAny) .oclAsType(Person) = X)
⟨proof⟩

lemma up-down-cast-Person-OclAny-Person’:
assumes τ |= v X
shows τ |= (((X :: Person) .oclAsType(OclAny) .oclAsType(Person)) ≜ X)
⟨proof⟩
lemma up-down-cast-Person-OclAny-Person'': assumes \( \tau \models v (X :: \text{Person}) \)
shows \( \tau \models (X .\text{oclIsTypeOf(Person)} \implies (X .\text{oclAsType(OclAny)} .\text{oclAsType(Person)}) \Rightarrow X) \)
\( \langle \text{proof} \rangle \)

6.1.6. OclIsKindOf

Definition

consts \( \text{OclIsKindOf}_{\text{OclAny}} :: \alpha \Rightarrow \text{Boolean} \)
consts \( \text{OclIsKindOf}_{\text{Person}} :: \alpha \Rightarrow \text{Boolean} \)

defs (overloaded) \( \text{OclIsKindOf}_{\text{OclAny}} - \text{OclAny}: \)
\( (X :: \text{OclAny}) .\text{oclIsKindOf(OclAny)} \equiv (\lambda \tau. \text{case } X \, \tau \text{ of} \)
\( \bot \Rightarrow \text{invalid } \tau \)
\( | - \Rightarrow \text{true } \tau) \)
defs (overloaded) \( \text{OclIsKindOf}_{\text{Person}} - \text{OclAny}: \)
\( (X :: \text{Person}) .\text{oclIsKindOf(OclAny)} \equiv (\lambda \tau. \text{case } X \, \tau \text{ of} \)
\( \bot \Rightarrow \text{invalid } \tau \)
\( | - \Rightarrow \text{true } \tau) \)
defs (overloaded) \( \text{OclIsKindOf}_{\text{Person}} - \text{OclAny}: \)
\( (X :: \text{OclAny}) .\text{oclIsKindOf(Person)} \equiv (\lambda \tau. \text{case } X \, \tau \text{ of} \)
\( \bot \Rightarrow \text{invalid } \tau \)
\( | [\bot] \Rightarrow \text{true } \tau \)
\( | [\text{mkOclAny oid } \bot] \Rightarrow \text{false } \tau \)
\( | [\text{mkOclAny oid } [-]] \Rightarrow \text{true } \tau) \)
defs (overloaded) \( \text{OclIsKindOf}_{\text{Person}} - \text{Person}: \)
\( (X :: \text{Person}) .\text{oclIsKindOf(Person)} \equiv (\lambda \tau. \text{case } X \, \tau \text{ of} \)
\( \bot \Rightarrow \text{invalid } \tau \)
\( | - \Rightarrow \text{true } \tau) \)

Context Passing

lemma \( \text{cp-OclIsKindOf}_{\text{OclAny}} - \text{Person-Person}: \)
\( \text{cp} (\lambda X. (P(X :: \text{Person}) :: \text{Person}).\text{oclIsKindOf(OclAny)}) \)
\( \langle \text{proof} \rangle \)
lemma \( \text{cp-OclIsKindOf}_{\text{OclAny}} - \text{OclAny-OclAny}: \)
\( \text{cp} (\lambda X. (P(X :: \text{OclAny}) :: \text{OclAny}).\text{oclIsKindOf(OclAny)}) \)
\( \langle \text{proof} \rangle \)
lemma \( \text{cp-OclIsKindOf}_{\text{Person}} - \text{Person-Person}: \)
\( \text{cp} (\lambda X. (P(X :: \text{Person}) :: \text{Person}).\text{oclIsKindOf(Person)}) \)
\( \langle \text{proof} \rangle \)
lemmas [simp] =
  cp-OclIsKindOf_Person-OclAny-OclAny
  cp-OclIsKindOf_Person-OclAny-Person
  cp-OclIsKindOf_OclAny-Person-OclAny
  cp-OclIsKindOf_OclAny-Person-Person
  cp-OclIsKindOf_Person-Person-OclAny
  cp-OclIsKindOf_Person-OclAny-Person
  cp-OclIsKindOf_Person-OclAny-OclAny
  cp-OclIsKindOf_OclAny-OclAny-Person
  cp-OclIsKindOf_OclAny-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_Person-person-strict1[simp] : (invalid::Person) .oclIsKindOf(OclAny) = invalid
  ⟨proof⟩

lemma OclIsKindOf_Person-Person-strict2[simp] : (null::Person) .oclIsKindOf(OclAny) = true
  ⟨proof⟩

lemma OclIsKindOf_Person-Person-strict1[simp] : (invalid::OclAny) .oclIsKindOf(Person) = invalid
  ⟨proof⟩
lemma $\text{OclIsKindOf}_{\text{Person}}$.OclAny-strict2[\text{simp}]: (null::OclAny).oclIsKindOf(Person) = true
\\\$$\langle\text{proof}\rangle$$

lemma $\text{OclIsKindOf}_{\text{Person}}$.Person-strict1[\text{simp}]: (invalid::Person).oclIsKindOf(Person) = invalid
\\\$$\langle\text{proof}\rangle$$

lemma $\text{OclIsKindOf}_{\text{Person}}$.Person-strict2[\text{simp}]: (null::Person).oclIsKindOf(Person) = true
\\\$$\langle\text{proof}\rangle$$

Up Down Casting

lemma actualKind-larger-staticKind:
assumes isdef: $\tau \vdash (\delta X)$
shows $\tau \vdash (X::\text{Person}).\text{oclIsKindOf}(\text{OclAny}) \triangleq \text{true}$
\\\$$\langle\text{proof}\rangle$$

lemma down-cast-kind:
assumes isOclAny: $\neg \tau \vdash (X::\text{OclAny}).\text{oclIsKindOf}(\text{Person})$
and non-null: $\tau \vdash (\delta X)$
shows $\tau \vdash (X.\text{oclAsType}(\text{Person})) \triangleq \text{invalid}$
\\\$$\langle\text{proof}\rangle$$

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 $\equiv \text{OclAsType}_{\text{Person}}$ _\text{A}$_\text{A}$
definition OclAny $\equiv \text{OclAsType}_{\text{OclAny}}$ _\text{A}$_\text{A}$
lemmas [\text{simp}] = Person-def OclAny-def

lemma OclAllInstances-genericOclAny-exec: OclAllInstances-generic pre-post OclAny = (\lambda \tau. \text{Abs-Set-0} [[ Some ' OclAny ' ran (heap (pre-post \tau)) ]])
\\\$$\langle\text{proof}\rangle$$

lemma OclAllInstances-at-postOclAny-exec: OclAny.allInstances() = (\lambda \tau. \text{Abs-Set-0} [[ Some ' OclAny ' ran (heap (snd \tau)) ]])
\\\$$\langle\text{proof}\rangle$$

lemma OclAllInstances-at-preOclAny-exec: OclAny.allInstances@pre() = (\lambda \tau. \text{Abs-Set-0} [[ Some ' OclAny ' ran (heap (fst \tau)) ]])
\\\$$\langle\text{proof}\rangle$$

OclIsTypeOf

lemma OclAny-allInstances-generic-oclIsTypeOfOclAny1:
assumes [\text{simp}]: $\forall x. \text{pre-post}\ (x, x) = x$
shows $\exists \tau. \ (\tau \models ((\text{OclAllInstances-generic pre-post OclAny}) \rightarrow \text{forAll}(X|X.\text{oclIsTypeOf}(\text{OclAny}))))$

⟨proof⟩

lemma OclAny-allInstances-at-post-oclIsTypeOfOclAny1:
$\exists \tau. \ (\tau \models (\text{OclAny}.\text{allInstances}() \rightarrow \text{forAll}(X|X.\text{oclIsTypeOf}(\text{OclAny}))))$

⟨proof⟩

lemma OclAny-allInstances-at-pre-oclIsTypeOfOclAny1:
$\exists \tau. \ (\tau \models (\text{OclAny}.\text{allInstances}@\text{pre}() \rightarrow \text{forAll}(X|X.\text{oclIsTypeOf}(\text{OclAny}))))$

⟨proof⟩

lemma OclAny-allInstances-generic-oclIsTypeOfOclAny2:
assumes [simp]: $\forall x. \text{pre-post}(x, x) = x$
shows $\exists \tau. \ (\tau \models \neg ((\text{OclAllInstances-generic pre-post OclAny}) \rightarrow \text{forAll}(X|X.\text{oclIsTypeOf}(\text{OclAny}))))$

⟨proof⟩

lemma OclAny-allInstances-at-post-oclIsTypeOfOclAny2:
$\exists \tau. \ (\tau \models \neg (\text{OclAny}.\text{allInstances}() \rightarrow \text{forAll}(X|X.\text{oclIsTypeOf}(\text{OclAny}))))$

⟨proof⟩

lemma OclAny-allInstances-at-pre-oclIsTypeOfOclAny2:
$\exists \tau. \ (\tau \models \neg (\text{OclAny}.\text{allInstances}@\text{pre}() \rightarrow \text{forAll}(X|X.\text{oclIsTypeOf}(\text{OclAny}))))$

⟨proof⟩

lemma Person-allInstances-generic-oclIsTypeOfPerson:
$\tau \models ((\text{OclAllInstances-generic pre-post Person}) \rightarrow \text{forAll}(X|X.\text{oclIsTypeOf}(\text{Person})))$

⟨proof⟩

lemma Person-allInstances-at-post-oclIsTypeOfPerson:
$\tau \models (\text{Person}.\text{allInstances}() \rightarrow \text{forAll}(X|X.\text{oclIsTypeOf}(\text{Person})))$

⟨proof⟩

lemma Person-allInstances-at-pre-oclIsTypeOfPerson:
$\tau \models (\text{Person}.\text{allInstances}@\text{pre}() \rightarrow \text{forAll}(X|X.\text{oclIsTypeOf}(\text{Person})))$

⟨proof⟩

OclIsKindOf

lemma OclAny-allInstances-generic-oclIsKindOfOclAny:
$\tau \models ((\text{OclAllInstances-generic pre-post OclAny}) \rightarrow \text{forAll}(X|X.\text{oclIsKindOf}(\text{OclAny})))$

⟨proof⟩

lemma OclAny-allInstances-at-post-oclIsKindOfOclAny:
$\tau \models (\text{OclAny}.\text{allInstances}() \rightarrow \text{forAll}(X|X.\text{oclIsKindOf}(\text{OclAny})))$

⟨proof⟩

lemma OclAny-allInstances-at-pre-oclIsKindOfOclAny:
\( \tau \models (\text{OclAny}.\text{allInstances}@\text{pre}() \rightarrow \text{forAll}(X | X.\text{oclIsKindOf}(\text{OclAny}))) \)

(\textit{proof})

\textbf{lemma \textit{Person-allInstances-generic-oclIsKindOfOclAny}:}
\( \tau \models ((\text{OclAllInstances-generic pre-post Person}) \rightarrow \text{forAll}(X | X.\text{oclIsKindOf}(\text{OclAny}))) \)

(\textit{proof})

\textbf{lemma \textit{Person-allInstances-at-post-oclIsKindOfOclAny}:}
\( \tau \models (\text{Person}.\text{allInstances}() \rightarrow \text{forAll}(X | X.\text{oclIsKindOf}(\text{OclAny}))) \)

(\textit{proof})

\textbf{lemma \textit{Person-allInstances-at-pre-oclIsKindOfOclAny}:}
\( \tau \models (\text{Person}.\text{allInstances}@\text{pre}() \rightarrow \text{forAll}(X | X.\text{oclIsKindOf}(\text{OclAny}))) \)

(\textit{proof})

\textbf{lemma \textit{Person-allInstances-generic-oclIsKindOfPerson}:}
\( \tau \models ((\text{OclAllInstances-generic pre-post Person}) \rightarrow \text{forAll}(X | X.\text{oclIsKindOf}(\text{Person}))) \)

(\textit{proof})

\textbf{lemma \textit{Person-allInstances-at-post-oclIsKindOfPerson}:}
\( \tau \models (\text{Person}.\text{allInstances}() \rightarrow \text{forAll}(X | X.\text{oclIsKindOf}(\text{Person}))) \)

(\textit{proof})

\textbf{lemma \textit{Person-allInstances-at-pre-oclIsKindOfPerson}:}
\( \tau \models (\text{Person}.\text{allInstances}@\text{pre}() \rightarrow \text{forAll}(X | X.\text{oclIsKindOf}(\text{Person}))) \)

(\textit{proof})

\subsection{The Accessors (any, boss, salary)}

Should be generated entirely from a class-diagram.

\textbf{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 \texttt{EmployeeDesignModel\_UMLPart}, where we stored an \texttt{oid} inside the class as “pointer.”

\textbf{definition} \texttt{oid\_PersonBOSS :: oid where oid\_PersonBOSS = 10}

From there on, we can already define an empty state which must contain for \texttt{oid\_PersonBOSS} the empty relation (encoded as association list, since there are associations with a Sequence-like structure).

\textbf{definition} \texttt{eval-extract :: (\&,(a::object) option option) val}
\( \Rightarrow (\texttt{oid} \Rightarrow (\&\texttt{a},\texttt{c::null}) \texttt{val}) \)
\( \Rightarrow (\&\texttt{a},\texttt{c::null}) \texttt{val} \)

\textbf{where} \texttt{eval-extract X f = (\lambda \tau. case X \tau of}
\( \downarrow \Rightarrow \texttt{invalid \tau} \) (* exception propagation *)
\( | \downarrow \downarrow \Rightarrow \texttt{invalid \tau} \) (* dereferencing null pointer *)

121
definition choose2-1 = fst
definition choose2-2 = snd
definition choose3-1 = fst
definition choose3-2 = fst o snd
definition choose3-3 = snd o snd

definition deref-assocs2 :: (A state × A state ⇒ A state)
⇒ (oid × oid ⇒ oid × oid)
⇒ oid
⇒ (oid list ⇒ oid ⇒ (A,f)val)
⇒ oid
⇒ (A, f::null)val

where deref-assocs2 pre-post to-from assoc-oid f oid =
(λτ. case (assocs2 (pre-post τ)) assoc-oid of
   [ S ] ⇒ f (map (choose2-2 o to-from)
                     (filter (λ p. choose2-1(to-from p)=oid) S))
   oid τ
   | - ⇒ invalid τ)

The pre-post-parameter is configured with fst or snd, the to-from-parameter either
with the identity id or the following combinator switch:

definition switch2-1 = id
definition switch2-2 = (λ(x,y). (y,x))
definition switch3-1 = id
definition switch3-2 = (λ(x,y,z). (x,z,y))
definition switch3-3 = (λ(x,y,z). (y,x,z))
definition switch3-4 = (λ(x,y,z). (y,z,x))
definition switch3-5 = (λ(x,y,z). (z,x,y))
definition switch3-6 = (λ(x,y,z). (z,y,x))

definition select-object :: ((A, b::null)val)
⇒ ((A, b)val ⇒ (A, c)val ⇒ (A, b)val)
⇒ ((A, b)val ⇒ (A, d)val)
⇒ (oid ⇒ (A, c::null)val)
⇒ oid list
⇒ oid
⇒ (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

122
\textbf{definition} \texttt{deref-oid}_{\text{Person}} :: (\text{A state} \times \text{A state} \Rightarrow \text{A state}) \\
\Rightarrow (\text{type}_{\text{Person}} \Rightarrow (\text{A, 'c::null)}val) \\
\Rightarrow \text{oid} \\
\Rightarrow (\text{A, 'c::null)}val \\
\textbf{where} \texttt{deref-oid}_{\text{Person}} \texttt{fst-snd} f \texttt{oid} = (\lambda \tau. \text{case } (\text{heap } (\text{fst-snd } \tau)) \texttt{oid} \texttt{of} \\
\begin{array}{ll} 
\texttt{in}_{\text{Person}} \texttt{obj} & \Rightarrow f \texttt{obj } \tau \\
\texttt{-} & \Rightarrow \texttt{invalid } \tau 
\end{array}

\textbf{definition} \texttt{deref-oid}_{\text{OclAny}} :: (\text{A state} \times \text{A state} \Rightarrow \text{A state}) \\
\Rightarrow (\text{type}_{\text{OclAny}} \Rightarrow (\text{A, 'c::null)}val) \\
\Rightarrow \text{oid} \\
\Rightarrow (\text{A, 'c::null)}val \\
\textbf{where} \texttt{deref-oid}_{\text{OclAny}} \texttt{fst-snd} f \texttt{oid} = (\lambda \tau. \text{case } (\text{heap } (\text{fst-snd } \tau)) \texttt{oid} \texttt{of} \\
\begin{array}{ll} 
\texttt{in}_{\text{OclAny}} \texttt{obj} & \Rightarrow f \texttt{obj } \tau \\
\texttt{-} & \Rightarrow \texttt{invalid } \tau 
\end{array}

\text{pointer undefined in state or not referencing a type conform object representation}

\textbf{definition} \texttt{select}_{\text{OclAny}} \texttt{ANY} \texttt{f} = (\lambda X. \text{case } X \texttt{of} \\
(\text{mk}_{\text{OclAny}} - \bot) \Rightarrow \texttt{null} \\
(\text{mk}_{\text{OclAny}} - [\texttt{any}]) \Rightarrow f (\lambda x - [x]) \texttt{any})

\textbf{definition} \texttt{select}_{\text{Person}} \texttt{BOSS} \texttt{f} = \texttt{select-object mtSet OclIncluding OclANY} (f (\lambda x - [x]))

\textbf{definition} \texttt{select}_{\text{Person}} \texttt{SALARY} \texttt{f} = (\lambda X. \text{case } X \texttt{of} \\
(\text{mk}_{\text{Person}} - \bot) \Rightarrow \texttt{null} \\
(\text{mk}_{\text{Person}} - [\texttt{salary}]) \Rightarrow f (\lambda x - [x]) \texttt{salary})

\textbf{definition} \texttt{deref-assocs}_{2} \texttt{BOSS} \texttt{fst-snd} f = (\lambda \texttt{mk}_{\text{Person}} \texttt{oid} - \Rightarrow \texttt{deref-assocs}_{2} \texttt{fst-snd} \texttt{switch}_{2-1} \texttt{oid}_{\text{Person}} \texttt{BOSS} f \texttt{oid})

\textbf{definition} \texttt{in\text{\_pre\text{-state}} = \text{fst}} \\
\textbf{definition} \texttt{in\text{\_post\text{-state}} = \text{snd}}

\textbf{definition} \texttt{reconst\text{\_basetype} = (\lambda \text{convert } x. \text{convert } x)}

\textbf{definition} \texttt{dot}_{\text{OclAny}} \texttt{ANY} :: \text{OclAny} \Rightarrow - ((1(-).any) 50) \\
\textbf{where} \texttt{X}.\text{any} = \text{eval\text{-extract }X} \\
(\text{deref-oid}_{\text{OclAny}} \texttt{in\text{-post\text{-state}}} \\
(\text{select}_{\text{OclAny}} \texttt{ANY} \texttt{reconst\text{\_basetype}}))

\textbf{definition} \texttt{dot}_{\text{Person}} \texttt{BOSS} :: \text{Person} \Rightarrow \text{Person} ((1(-).boss) 50) \\
\textbf{where} \texttt{X}.\text{boss} = \text{eval\text{-extract }X} \\
(\text{deref-oid}_{\text{Person}} \texttt{in\text{-post\text{-state}}})
(deref-assocs_{2 BOSS \text{ in-post-state}}
(deref-oid_{Person \text{ in-post-state}})))

definition \textit{dot}_{\textit{Person}}_{\textit{SALARY}} :: \textit{Person} \Rightarrow \textit{Integer} \ ((I\cdot . \textit{salary} 50)\)
where \((X) . \textit{salary} = \text{eval-extract } \ X
(deref-oid_{Person \text{ in-post-state}}
(deref-assocs_{2 BOSS \text{ in-post-state}}
(deref-oid_{Person \text{ in-post-state}})
(reconst-basetype)))\)

definition \textit{dot}_{\textit{OclAny\textit{ANY}}\textit{-at-pre}} :: \textit{OclAny} \Rightarrow - \ ((I\cdot . \textit{any}@pre 50)\)
where \((X) . \textit{any}@pre = \text{eval-extract } \ X
(deref-oid_{\textit{OclAny\textit{ANY}} \text{ in-pre-state}}
(deref-assocs_{2 BOSS \text{ in-pre-state}}
(deref-oid_{\textit{Person \text{ in-pre-state}}}
(reconst-basetype)))\)

definition \textit{dot}_{\textit{Person\textit{BOSS}}\textit{-at-pre}} :: \textit{Person} \Rightarrow \textit{Person} \ ((I\cdot . \textit{boss}@pre 50)\)
where \((X) . \textit{boss}@pre = \text{eval-extract } \ X
(deref-oid_{\textit{Person \text{ in-pre-state}}}
(deref-assocs_{2 BOSS \text{ in-pre-state}}
(deref-oid_{\textit{Person \text{ in-pre-state}}})
(reconst-basetype)))\)

definition \textit{dot}_{\textit{Person\textit{SALARY}}\textit{-at-pre}} :: \textit{Person} \Rightarrow \textit{Integer} \ ((I\cdot . \textit{salary}@pre 50)\)
where \((X) . \textit{salary}@pre = \text{eval-extract } \ X
(deref-oid_{\textit{Person \text{ in-pre-state}}}
(deref-assocs_{2 BOSS \text{ in-pre-state}}
(deref-oid_{\textit{Person \text{ in-pre-state}}})
(reconst-basetype)))\)

lemmas [\textit{simp} =
\textit{dot}_{\textit{OclAny\textit{ANY}}\textit{-def}}
\textit{dot}_{\textit{Person\textit{BOSS}}\textit{-def}}
\textit{dot}_{\textit{Person\textit{SALARY}}\textit{-def}}
\textit{dot}_{\textit{OclAny\textit{ANY}}\textit{-at-pre-def}}
\textit{dot}_{\textit{Person\textit{BOSS}}\textit{-at-pre-def}}
\textit{dot}_{\textit{Person\textit{SALARY}}\textit{-at-pre-def}}

Context Passing

lemmas [\textit{simp} = \textit{eval-extract-def}

lemma \textit{cp-dot}_{\textit{OclAny\textit{ANY}}} : ((X).any) \ \tau = ((\lambda - X \ \tau).any) \ \tau \ \langle \text{proof} \rangle
lemma \textit{cp-dot}_{\textit{Person\textit{BOSS}}} : ((X).boss) \ \tau = ((\lambda - X \ \tau).boss) \ \tau \ \langle \text{proof} \rangle
lemma \textit{cp-dot}_{\textit{Person\textit{SALARY}}} : ((X).salary) \ \tau = ((\lambda - X \ \tau).salary) \ \tau \ \langle \text{proof} \rangle

lemma \textit{cp-dot}_{\textit{OclAny\textit{ANY}}\textit{-at-pre}} : ((X).any@pre) \ \tau = ((\lambda - X \ \tau).any@pre) \ \tau \ \langle \text{proof} \rangle
lemma \textit{cp-dot}_{\textit{Person\textit{BOSS}}\textit{-at-pre}} : ((X).boss@pre) \ \tau = ((\lambda - X \ \tau).boss@pre) \ \tau \ \langle \text{proof} \rangle
lemma \textit{cp-dot}_{\textit{Person\textit{SALARY}}\textit{-at-pre}} : ((X).salary@pre) \ \tau = ((\lambda - X \ \tau).salary@pre) \ \tau \ \langle \text{proof} \rangle
lemmas \textit{cp-dot}_{\text{OclAny}}\textit{ANY}\cdot \textit{I} [\text{simp}, \text{intro}]=
\begin{align*}
\textit{cp-dot}_{\text{OclAny}}\textit{ANY}\cdot \textit{I} & \quad \text{THEN all}[\text{THEN all}], \\
& \quad \text{of } \lambda \, X \cdot, \, X \cdot \lambda - \tau, \tau, \text{THEN cpII}
\end{align*}

lemmas \textit{cp-dot}_{\text{OclAny}}\textit{ANY}\cdot \textit{at-pre}\cdot \textit{I} [\text{simp}, \text{intro}]=
\begin{align*}
\textit{cp-dot}_{\text{OclAny}}\textit{ANY}\cdot \textit{at-pre} & \quad \text{THEN all}[\text{THEN all}], \\
& \quad \text{of } \lambda \, X \cdot, \, X \cdot \lambda - \tau, \tau, \text{THEN cpII}
\end{align*}

lemmas \textit{cp-dot}_{\text{Person}}\textit{BOSS}\cdot \textit{I} [\text{simp}, \text{intro}]=
\begin{align*}
\textit{cp-dot}_{\text{Person}}\textit{BOSS}\cdot \textit{I} & \quad \text{THEN all}[\text{THEN all}], \\
& \quad \text{of } \lambda \, X \cdot, \, X \cdot \lambda - \tau, \tau, \text{THEN cpII}
\end{align*}

lemmas \textit{cp-dot}_{\text{Person}}\textit{BOSS}\cdot \textit{at-pre}\cdot \textit{I} [\text{simp}, \text{intro}]=
\begin{align*}
\textit{cp-dot}_{\text{Person}}\textit{BOSS}\cdot \textit{at-pre} & \quad \text{THEN all}[\text{THEN all}], \\
& \quad \text{of } \lambda \, X \cdot, \, X \cdot \lambda - \tau, \tau, \text{THEN cpII}
\end{align*}

lemmas \textit{cp-dot}_{\text{Person}}\textit{SALARY}\cdot \textit{I} [\text{simp}, \text{intro}]=
\begin{align*}
\textit{cp-dot}_{\text{Person}}\textit{SALARY}\cdot \textit{I} & \quad \text{THEN all}[\text{THEN all}], \\
& \quad \text{of } \lambda \, X \cdot, \, X \cdot \lambda - \tau, \tau, \text{THEN cpII}
\end{align*}

lemmas \textit{cp-dot}_{\text{Person}}\textit{SALARY}\cdot \textit{at-pre}\cdot \textit{I} [\text{simp}, \text{intro}]=
\begin{align*}
\textit{cp-dot}_{\text{Person}}\textit{SALARY}\cdot \textit{at-pre} & \quad \text{THEN all}[\text{THEN all}], \\
& \quad \text{of } \lambda \, X \cdot, \, X \cdot \lambda - \tau, \tau, \text{THEN cpII}
\end{align*}

Execution with Invalid or Null as Argument

lemma \textit{dot}_{\text{OclAny}}\textit{ANY}\cdot \textit{nullstrict} [\text{simp}]: (null).any = invalid 
(proof)

lemma \textit{dot}_{\text{OclAny}}\textit{ANY}\cdot \textit{at-pre-nullstrict} [\text{simp}]: (null).any@pre = invalid 
(proof)

lemma \textit{dot}_{\text{OclAny}}\textit{ANY}\cdot \textit{strict} [\text{simp}]: (invalid).any = invalid 
(proof)

lemma \textit{dot}_{\text{OclAny}}\textit{ANY}\cdot \textit{at-pre-strict} [\text{simp}]: (invalid).any@pre = invalid 
(proof)

lemma \textit{dot}_{\text{Person}}\textit{BOSS}\cdot \textit{nullstrict} [\text{simp}]: (null).boss = invalid 
(proof)

lemma \textit{dot}_{\text{Person}}\textit{BOSS}\cdot \textit{at-pre-nullstrict} [\text{simp}]: (null).boss@pre = invalid 
(proof)

lemma \textit{dot}_{\text{Person}}\textit{BOSS}\cdot \textit{strict} [\text{simp}]: (invalid).boss = invalid 
(proof)

lemma \textit{dot}_{\text{Person}}\textit{BOSS}\cdot \textit{at-pre-strict} [\text{simp}]: (invalid).boss@pre = invalid 
(proof)

lemma \textit{dot}_{\text{Person}}\textit{SALARY}\cdot \textit{nullstrict} [\text{simp}]: (null).salary = invalid 
(proof)

lemma \textit{dot}_{\text{Person}}\textit{SALARY}\cdot \textit{at-pre-nullstrict} [\text{simp}]: (null).salary@pre = invalid 
(proof)

lemma \textit{dot}_{\text{Person}}\textit{SALARY}\cdot \textit{strict} [\text{simp}]: (invalid).salary = invalid 
(proof)
Figure 6.2.: (a) pre-state $\sigma_1$ and (b) post-state $\sigma'_1$.

\textbf{lemma} \( \text{dotPerson,\$SALARY$}$-at-pre-strict [simp] : \((\text{invalid}, \text{salary} @ \text{pre} = \text{invalid})\) \\

\textbf{6.1.9. A Little Infra-structure on Example States}

The example we are defining in this section comes from the figure 6.2

\begin{verbatim}
definition OclInt1000 (1000) where OclInt1000 = (\_ - . \lfloor \lfloor 1000 \rfloor \rfloor )
definition OclInt1200 (1200) where OclInt1200 = (\_ - . \lfloor \lfloor 1200 \rfloor \rfloor )
definition OclInt1300 (1300) where OclInt1300 = (\_ - . \lfloor \lfloor 1300 \rfloor \rfloor )
definition OclInt1800 (1800) where OclInt1800 = (\_ - . \lfloor \lfloor 1800 \rfloor \rfloor )
definition OclInt2600 (2600) where OclInt2600 = (\_ - . \lfloor \lfloor 2600 \rfloor \rfloor )
definition OclInt2900 (2900) where OclInt2900 = (\_ - . \lfloor \lfloor 2900 \rfloor \rfloor )
definition OclInt3200 (3200) where OclInt3200 = (\_ - . \lfloor \lfloor 3200 \rfloor \rfloor )
definition OclInt3500 (3500) where OclInt3500 = (\_ - . \lfloor \lfloor 3500 \rfloor \rfloor )

definition oid0 \equiv 0
#define oid1 \equiv 1
#define oid2 \equiv 2
#define oid3 \equiv 3
#define oid4 \equiv 4
#define oid5 \equiv 5
#define oid6 \equiv 6
#define oid7 \equiv 7
#define oid8 \equiv 8

definition person1 \equiv \text{mkPerson} oid0 \lfloor \lfloor 1300 \rfloor \rfloor 
definition person2 \equiv \text{mkPerson} oid1 \lfloor \lfloor 1800 \rfloor \rfloor 
definition person3 \equiv \text{mkPerson} oid2 \text{None}
definition person4 \equiv \text{mkPerson} oid3 \lfloor \lfloor 2900 \rfloor \rfloor 
definition person5 \equiv \text{mkPerson} oid4 \lfloor \lfloor 3500 \rfloor \rfloor 
definition person6 \equiv \text{mkPerson} oid5 \lfloor \lfloor 2500 \rfloor \rfloor 
definition person7 \equiv \text{mkOclAny} oid6 \lfloor \lfloor 3200 \rfloor \rfloor 
definition person8 \equiv \text{mkOclAny} oid7 \text{None}
definition person9 \equiv \text{mkPerson} oid8 \lfloor \lfloor 0 \rfloor \rfloor

definition
\end{verbatim}
\[\sigma_1 \equiv \{ \text{heap} = \text{empty}(oid0 \mapsto \text{inPerson}(\text{mkPerson} \ oid0 \ [1000])); \text{ oid1} \mapsto \text{inPerson}(\text{mkPerson} \ oid1 \ [1200])), \text{ oid2} \mapsto \text{oid2} \}
\]
\[\text{oid3} \mapsto \text{inPerson}(\text{mkPerson} \ oid3 \ [2600])), \text{ oid4} \mapsto \text{inPerson} \text{ person5}) \text{ oid5} \mapsto \text{inPerson}(\text{mkPerson} \ oid5 \ [2300])), \text{ oid6} \mapsto \text{oid6} \}
\]
\[\text{oid7} \mapsto \text{oid7} \}\text{ oid8} \mapsto \text{inPerson} \text{ person9})\]
\[\text{assocs}_2 = \text{empty}(\text{oid}_{\text{Person}} \text{BOSS} \mapsto [(\text{oid0}, \text{oid1}), (\text{oid3}, \text{oid4}), (\text{oid5}, \text{oid3})]), \text{assocs}_3 = \text{empty} \}
\]

**definition** \[\sigma_1 \equiv \{ \text{heap} = \text{empty}(\text{oid0} \mapsto \text{inPerson} \text{ person1}) \]
\[\text{oid1} \mapsto \text{inPerson} \text{ person2}) \text{ oid2} \mapsto \text{inPerson} \text{ person3}) \text{ oid3} \mapsto \text{inPerson} \text{ person4}) \text{ oid4} \mapsto \text{oid4} \}
\[\text{oid5} \mapsto \text{inPerson} \text{ person6}) \text{ oid6} \mapsto \text{inOclAny} \text{ person7}) \text{ oid7} \mapsto \text{inOclAny} \text{ person8}) \text{ oid8} \mapsto \text{inPerson} \text{ person9})\]
\[\text{assocs}_2 = \text{empty}(\text{oid}_{\text{Person}} \text{BOSS} \mapsto [(\text{oid0}, \text{oid1}), (\text{oid3}, \text{oid6}), (\text{oid6}, \text{oid6})]), \text{assocs}_3 = \text{empty} \]

**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} \text{ \sigma_1) = \{ \text{ oid0}, \text{oid1}, (\text{oid2} \mapsto \text{oid3}), \text{oid4}, \text{oid5}, (\text{oid6}, \text{oid7} \mapsto \text{oid8}) \}
\]

(proof)

**lemma** [simp,code-unfold]: \(\text{dom} \text{ (heap} \text{ \sigma_1') = \{ oid0, oid1, oid2, oid3, (oid4 \mapsto oid5, oid6, oid7, oid8) \}
\]

(proof)

**definition** \(X_{\text{Person}1} :: \text{Person} \equiv \lambda \cdot [\text{ person1 }]\)
**definition** \(X_{\text{Person}2} :: \text{Person} \equiv \lambda \cdot [\text{ person2 }]\)
**definition** \(X_{\text{Person}3} :: \text{Person} \equiv \lambda \cdot [\text{ person3 }]\)
**definition** \(X_{\text{Person}4} :: \text{Person} \equiv \lambda \cdot [\text{ person4 }]\)
**definition** \(X_{\text{Person}5} :: \text{Person} \equiv \lambda \cdot [\text{ person5 }]\)
**definition** \(X_{\text{Person}6} :: \text{Person} \equiv \lambda \cdot [\text{ person6 }]\)
**definition** \(X_{\text{Person}7} :: \text{OclAny} \equiv \lambda \cdot [\text{ person7 }]\)
**definition** \(X_{\text{Person}8} :: \text{OclAny} \equiv \lambda \cdot [\text{ person8 }]\)
**definition** \(X_{\text{Person}9} :: \text{Person} \equiv \lambda \cdot [\text{ person9 }]\)

**lemma** [code-unfold]: \((x::\text{Person}) \downarrow y = \text{StrictRefEqObject} \ x \ y\) (proof)
lemma [code-unfold]: \((x::\text{OclAny}) \doteq y) = \text{StrictRefEq}_{\text{OclObject}} \ x \ y\langle \text{proof}\rangle

lemmas [simp,code-unfold] =
\text{OclAsType}_{\text{OclAny}} - \text{OclAny}
\text{OclAsType}_{\text{OclAny}} - \text{Person}
\text{OclAsType}_{\text{Person}} - \text{OclAny}
\text{OclAsType}_{\text{Person}} - \text{Person}
\text{OclIsTypeOf}_{\text{OclAny}} - \text{OclAny}
\text{OclIsTypeOf}_{\text{OclAny}} - \text{Person}
\text{OclIsTypeOf}_{\text{Person}} - \text{OclAny}
\text{OclIsTypeOf}_{\text{Person}} - \text{Person}
\text{OclIsKindOf}_{\text{OclAny}} - \text{OclAny}
\text{OclIsKindOf}_{\text{OclAny}} - \text{Person}
\text{OclIsKindOf}_{\text{Person}} - \text{OclAny}
\text{OclIsKindOf}_{\text{Person}} - \text{Person}

value \bigwedge s_{\text{pre}} . (s_{\text{pre}}, s_1) \models (X_{\text{Person}1}. \text{salary}<> 1000)
value \bigwedge s_{\text{pre}} . (s_{\text{pre}}, s_1') \models (X_{\text{Person}1}. \text{salary} \doteq 1300)
value \bigwedge s_{\text{post}} . (\sigma_1, s_{\text{post}}) \models (X_{\text{Person}1}. \text{salary}@\text{pre} \doteq 1000)
value \bigwedge s_{\text{post}} . (\sigma_1', s_{\text{post}}) \models (X_{\text{Person}1}. \text{salary}@\text{pre} <> 1300)

lemma \langle \text{proof}\rangle
(\sigma_1, \sigma_1') \models (X_{\text{Person}1}. \text{oclIsMaintained}())

lemma \langle \text{proof}\rangle
\bigwedge s_{\text{pre}} s_{\text{post}} . (s_{\text{pre}}, s_{\text{post}}) \models ((X_{\text{Person}1}. \text{oclAsType}(\text{OclAny}). \text{oclAsType}(\text{Person})))
\doteq X_{\text{Person}1})

value \bigwedge s_{\text{pre}} s_{\text{post}} . (s_{\text{pre}}, s_{\text{post}}) \models (X_{\text{Person}1}. \text{oclIsTypeOf}(\text{Person}))
value \bigwedge s_{\text{pre}} s_{\text{post}} . (s_{\text{pre}}, s_{\text{post}}) \models \text{not}(X_{\text{Person}1}. \text{oclIsTypeOf}(\text{OclAny}))
value \bigwedge s_{\text{pre}} s_{\text{post}} . (s_{\text{pre}}, s_{\text{post}}) \models (X_{\text{Person}1}. \text{oclIsKindOf}(\text{Person}))
value \bigwedge s_{\text{pre}} s_{\text{post}} . (s_{\text{pre}}, s_{\text{post}}) \models (X_{\text{Person}1}. \text{oclIsKindOf}(\text{OclAny}))
value \bigwedge s_{\text{pre}} s_{\text{post}} . (s_{\text{pre}}, s_{\text{post}}) \models \text{not}(X_{\text{Person}1}. \text{oclAsType}(\text{OclAny}). \text{oclIsTypeOf}(\text{OclAny}))

value \bigwedge s_{\text{pre}} . (s_{\text{pre}}, s_1') \models (X_{\text{Person}2}. \text{salary} \doteq 1800)
value \bigwedge s_{\text{post}} . (\sigma_1, s_{\text{post}}) \models (X_{\text{Person}2}. \text{salary}@\text{pre} \doteq 1200)

lemma \langle \text{proof}\rangle
(\sigma_1, \sigma_1') \models (X_{\text{Person}2}. \text{oclIsMaintained}())

value \bigwedge s_{\text{pre}} . (s_{\text{pre}}, s_1') \models (X_{\text{Person}3}. \text{salary} \doteq \text{null})
value \bigwedge s_{\text{post}} . (\sigma_1, s_{\text{post}}) \models \text{not}(\text{v}(X_{\text{Person}3}. \text{salary}@\text{pre}))

lemma \langle \text{proof}\rangle
(\sigma_1, \sigma_1') \models (X_{\text{Person}3}. \text{oclIsNew}())
lemma \( (\sigma_1,\sigma'_1) \models (\text{Person4}.oclIsMaintained()) \)

(proof)

value \( \land_{\text{pre}} \cdot (s_{\text{pre}},\sigma'_1) \models \text{not}(v(\text{Person5}.\text{salar}y)) \)
value \( \land_{\text{post}} \cdot (\sigma_1,s_{\text{post}}) \models (\text{Person5}.\text{salar}y \land \text{pre} \equiv 3500) \)
lemma \( (\sigma_1,\sigma'_1) \models (\text{Person5}.oclIsDeleted()) \)

(proof)

lemma \( (\sigma_1,\sigma'_1) \models (\text{Person6}.oclIsMaintained()) \)

(proof)

value \( \land_{\text{pre}} s_{\text{post}} \cdot (s_{\text{pre}},s_{\text{post}}) \models v(\text{Person7}.oclAsType(\text{Person})) \)
lemma \( \land_{\text{pre}} s_{\text{post}} \cdot (s_{\text{pre}},s_{\text{post}}) \models ((\text{Person7}.oclAsType(\text{Person}).oclAsType(\text{OclAny}).oclAsType(\text{Person})).oclAsType(\text{Person})) \)

\( \equiv (\text{Person7}.\text{oclAsType}(\text{Person})) \)
lemma \( (\sigma_1,\sigma'_1) \models (\text{Person7}.oclIsNew()) \)

(proof)

value \( \land_{\text{pre}} s_{\text{post}} \cdot (s_{\text{pre}},s_{\text{post}}) \models (\text{Person8} \land \text{Person7}) \)
value \( \land_{\text{pre}} s_{\text{post}} \cdot (s_{\text{pre}},s_{\text{post}}) \models \text{not}(v(\text{Person8}.oclAsType(\text{Person}))) \)
value \( \land_{\text{pre}} s_{\text{post}} \cdot (s_{\text{pre}},s_{\text{post}}) \models (\text{Person8}.oclIsTypeOf(\text{OclAny})) \)
value \( \land_{\text{pre}} s_{\text{post}} \cdot (s_{\text{pre}},s_{\text{post}}) \models \text{not}(\text{Person8}.oclIsTypeOf(\text{Person})) \)
value \( \land_{\text{pre}} s_{\text{post}} \cdot (s_{\text{pre}},s_{\text{post}}) \models \text{not}(\text{Person8}.oclIsKindOf(\text{Person})) \)
value \( \land_{\text{pre}} s_{\text{post}} \cdot (s_{\text{pre}},s_{\text{post}}) \models \text{not}(\text{Person8}.oclIsKindOf(\text{OclAny})) \)

lemma \( \sigma\text{-modifiedonly}: (\sigma_1,\sigma'_1) \models (\text{Set}\{\text{Person1}.oclAsType(\text{OclAny}).\text{Person2}.oclAsType(\text{OclAny}).\text{Person3}.oclAsType(\text{OclAny}).\text{Person4}.oclAsType(\text{OclAny}).\text{Person5}.oclAsType(\text{OclAny}).\text{Person6}.oclAsType(\text{OclAny}).\text{Person7}.oclAsType(\text{OclAny}).\text{Person8}.oclAsType(\text{OclAny}).\text{Person9}.oclAsType(\text{OclAny})\}) \rightarrow \text{oclIsModifiedOnly}() \)

(proof)

lemma \( (\sigma_1,\sigma'_1) \models ((\text{Person9} \land \text{pre} \cdot (\lambda x. \{\text{oclAsType}_{\text{Person}} \cap x\})) \equiv \text{Person9}) \)

(proof)
lemma \((\sigma_1, \sigma_1') \models ((X_{\textsc{Person}} \cdot \text{oclAsType}(\textsc{OclAny})) \cdot \text{pre} (\lambda x. \lfloor \text{OclAsType}\textsc{OclAny} - A \cdot x \rfloor)) \equiv (X_{\textsc{Person}} \cdot \text{oclAsType}(\textsc{OclAny})) \cdot \text{post} (\lambda x. \lfloor \text{OclAsType}\textsc{OclAny} - A \cdot x \rfloor))\)

⟨proof⟩

\begin{align*}
\text{lemma } \sigma_1, \sigma_1' & \models ((X_{\textsc{Person}} \cdot \text{oclAsType}(\textsc{OclAny})) \cdot \text{post} (\lambda x. \lfloor \text{OclAsType}\textsc{OclAny} - A \cdot x \rfloor)) \equiv X_{\textsc{Person}} \\
\langle \text{proof} \rangle
\end{align*}

\begin{align*}
\text{lemma } \text{perm-}\sigma_1' : \sigma_1' &= (\{ \text{heap} = \text{empty} \}) \\
&= (\text{oid8} \mapsto \text{in}_{\textsc{Person}} \text{person9}) \\
&= (\text{oid7} \mapsto \text{in}_{\textsc{OclAny}} \text{person8}) \\
&= (\text{oid6} \mapsto \text{in}_{\textsc{OclAny}} \text{person7}) \\
&= (\text{oid5} \mapsto \text{in}_{\textsc{Person}} \text{person6}) \\
&= (\text{oid4} \mapsto \text{in}_{\textsc{Person}} \text{person5}) \\
&= (\text{oid3} \mapsto \text{in}_{\textsc{Person}} \text{person4}) \\
&= (\text{oid2} \mapsto \text{in}_{\textsc{Person}} \text{person3}) \\
&= (\text{oid1} \mapsto \text{in}_{\textsc{Person}} \text{person2}) \\
&= (\text{oid0} \mapsto \text{in}_{\textsc{Person}} \text{person1}) \\
&\quad , \text{assocs}_2 = \text{assocs}_2 \sigma_1' \\
&\quad , \text{assocs}_3 = \text{assocs}_3 \sigma_1' \}

\langle \text{proof} \rangle
\end{align*}

\begin{align*}
\text{declare } \text{const-ss [simp]}
\end{align*}

lemma \(\land \sigma_1.
(\sigma_1, \sigma_1') \models (\textsc{Person} \cdot \text{allInstances}()) \equiv \text{Set} \{ X_{\textsc{Person}} 1, X_{\textsc{Person}} 2, X_{\textsc{Person}} 9, X_{\textsc{Person}} 4 (\ast, X_{\textsc{Person}} 5 \ast), X_{\textsc{Person}} 6, \\
X_{\textsc{Person}} 7 \cdot \text{oclAsType}(\textsc{Person}) (\ast, X_{\textsc{Person}} 8 \ast), X_{\textsc{Person}} 9 \})
\langle \text{proof} \rangle
\end{align*}

lemma \(\land \sigma_1.
(\sigma_1, \sigma_1') \models (\textsc{OclAny} \cdot \text{allInstances}()) \equiv \text{Set} \{ X_{\textsc{Person}} 1 \cdot \text{oclAsType}(\textsc{OclAny}), X_{\textsc{Person}} 2 \cdot \text{oclAsType}(\textsc{OclAny}), \\
X_{\textsc{Person}} 3 \cdot \text{oclAsType}(\textsc{OclAny}), X_{\textsc{Person}} 4 \cdot \text{oclAsType}(\textsc{OclAny}) (\ast, X_{\textsc{Person}} 5 \ast), X_{\textsc{Person}} 6 \cdot \text{oclAsType}(\textsc{OclAny}), \\
X_{\textsc{Person}} 7, X_{\textsc{Person}} 8, X_{\textsc{Person}} 9 \cdot \text{oclAsType}(\textsc{OclAny}) \})
\langle \text{proof} \rangle
\end{align*}

end

\subsection{The Employee Analysis Model (OCL)}

\begin{align*}
\text{theory}
\text{Employee-AnalysisModel-OCLPart}
\text{imports}
\text{Employee-AnalysisModel-UMLPart}
\text{begin}
\end{align*}

130
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.

\[
\text{axiomatization } \text{inv-Person} :: \text{Person} \Rightarrow \text{Boolean}
\]

\[
\begin{align*}
A : (\tau \models (\delta \text{self})) & \quad \rightarrow \\
(\tau \models \text{inv-Person}(\text{self})) = \\
& ((\tau \models (\text{self} . \text{boss} \not= \text{null})) \lor \\
& (\tau \models (\text{self} . \text{boss} \not< \text{null}) \land (\tau \models ((\text{self} . \text{salary}) \not\leq (\text{self} . \text{boss} . \text{salary}))) \land \\
& (\tau \models (\text{inv-Person}(\text{self} . \text{boss})))))
\end{align*}
\]

\[
\text{axiomatization } \text{inv-Person-at-pre} :: \text{Person} \Rightarrow \text{Boolean}
\]

\[
\begin{align*}
B : (\tau \models (\delta \text{self})) & \quad \rightarrow \\
(\tau \models \text{inv-Person-at-pre}(\text{self})) = \\
& ((\tau \models (\text{self} . \text{boss}@\text{pre} \not= \text{null})) \lor \\
& (\tau \models (\text{self} . \text{boss}@\text{pre} \not< \text{null}) \land \\
& (\tau \models (\text{self} . \text{boss}@\text{pre} . \text{salary}@\text{pre} \not\leq \text{self} . \text{salary}@\text{pre}) \land \\
& (\tau \models (\text{inv-Person-at-pre}(\text{self} . \text{boss}@\text{pre})))))
\end{align*}
\]

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!)

\[
\text{coinductive } \text{inv} :: \text{Person} \Rightarrow (\exists \text{st} \Rightarrow \text{bool} \ \text{where} \\
(\tau \models (\delta \text{self})) \rightarrow ((\tau \models (\text{self} . \text{boss} \not= \text{null})) \lor \\
(\tau \models (\text{self} . \text{boss} \not< \text{null}) \land (\tau \models (\text{self} . \text{boss} . \text{salary} \not\leq \text{self} . \text{salary})) \land \\
(\text{inv(}\text{self} . \text{boss})\tau ))))
\rightarrow (\text{inv self } \tau)
\]

6.2.3. The Contract of a Recursive Query

The original specification of a recursive query:

\[
\begin{array}{l}
\text{context Person::contents():Set(Integer)} \\
\text{post: result = if self. boss = null then Set{1} else self. boss. contents()->including(1) endif}
\end{array}
\]

\[
\text{consts dot-contents :: Person \Rightarrow Set-Integer } ((1(-).contents()) 50)
\]

\[
\text{axiomatization where dot-contents-def:}
\]

\[
(\tau \models ((\text{self}).\text{contents()} \not= \text{result})) =
\]

\[
(\text{if (}\delta \text{self}) \tau = \text{true } \tau \\
\text{then ((}\tau \models \text{true}))
\]

\[
131
\]
\[(\tau \models (\text{result} \triangleq \text{if } (\text{self}.\text{boss} \triangleq \text{null}) \text{ then } \{\text{self}.\text{salary}\} \text{ else } (\text{self}.\text{boss}.\text{contents()} \to \text{including}(\text{self}.\text{salary})) \text{ endif}))\]

else \( \tau \models \text{result} \triangleq \text{invalid} \)

\textbf{consts} \(\text{dot-contents-AT-pre} :: \text{Person} \Rightarrow \text{Set-Integer} ((1(-).\text{contents}@\text{pre}(\_)) 50)\)

\textbf{axiomatization where} \(\text{dot-contents-AT-pre-def}::\)
\(\tau \models (\text{self}).\text{contents}@\text{pre}() \triangleq \text{result} =\)
\(\text{if } (\delta \text{self}) \tau = \text{true } \tau \text{ then } \tau \models \text{true } \land \)
\(\tau \models (\text{result} \triangleq \text{if } (\text{self}).\text{boss}@\text{pre} \triangleq \text{null } \text{(* post *)} \text{ then } \{\text{self}.\text{salary}@\text{pre}\} \text{ else } (\text{self}).\text{boss}@\text{pre}.\text{contents}@\text{pre}() \to \text{including}(\text{self}.\text{salary}@\text{pre}) \text{ endif})\)
\(\text{else } \tau \models \text{result} \triangleq \text{invalid})\)

These \(\text{@pre}\) variants on methods are only available on queries, i.e., operations without side-effect.

\subsection*{6.2.4. The Contract of a Method}

The specification in high-level OCL input syntax reads as follows:

\begin{tabular}{l}
\textbf{context} \text{Person}::\text{insert}(x:\text{Integer}) \\
\textbf{post}:: \text{contents}():\text{Set}(\text{Integer}) \\
\text{contents}() = \text{contents}@\text{pre}() \to \text{including}(x)
\end{tabular}

\textbf{consts} \(\text{dot-insert} :: \text{Person} \Rightarrow \text{Integer} \Rightarrow \text{Void} ((1(-).\text{insert}(\_)) 50)\)

\textbf{axiomatization where} \(\text{dot-insert-def}::\)
\(\tau \models ((\text{self}).\text{insert}(x) \triangleq \text{result})) =\)
\(\text{if } (\delta \text{self}) \tau = \text{true } \land (\nu x) \tau = \text{true } \tau \text{ then } \tau \models \text{true } \land \)
\(\tau \models ((\text{self}).\text{contents}() \triangleq (\text{self}).\text{contents}@\text{pre}() \to \text{including}(x)) \text{ else } \tau \models ((\text{self}).\text{insert}(x) \triangleq \text{invalid})\)

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.
Our data universe consists in the concrete class diagram just of node’s, and implicitly of the class object. Each class implies the existence of a class type defined for the corresponding object representations as follows:

\[
\text{datatype typePerson} = \text{mkPerson oid}
\]
\[
\hspace{1cm} \text{int option}
\]
\[
\hspace{1cm} \text{oid option}
\]

\[
\text{datatype typeOclAny} = \text{mkOclAny oid}
\]
\[
\hspace{1cm} (\text{int option} \times \text{oid option}) \text{ option}
\]

Now, we construct a concrete “universe of OclAny types” by injection into a sum type containing the class types. This type of OclAny will be used as instance for all respective type-variables.

\[
\text{datatype } \exists = \text{inPerson typePerson } | \text{inOclAny typeOclAny}
\]

Having fixed the object universe, we can introduce type synonyms that exactly correspond to OCL types. Again, we exploit that our representation of OCL is a “shallow embedding” with a one-to-one correspondence of OCL-types to types of the meta-language HOL.

\[
\text{type-synonym Boolean } = \exists \text{ Boolean}
\]
\[
\text{type-synonym Integer } = \exists \text{ Integer}
\]
\[
\text{type-synonym Void } = \exists \text{ Void}
\]
\[
\text{type-synonym OclAny } = (\exists, \text{typeOclAny option option}) \text{ val}
\]
\[
\text{type-synonym Person } = (\exists, \text{typePerson option option}) \text{ val}
\]
\[
\text{type-synonym Set-Integer } = (\exists, \text{int option option}) \text{ Set}
\]
\[
\text{type-synonym Set-Person } = (\exists, \text{typePerson option option}) \text{ Set}
\]

Just a little check:

\[
\text{typ Boolean}
\]

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 \text{oid-of} yielding the object id (oid) of the object.
instantiation type\textit{Person} ::= object
\begin{definition}
oid-of-type\textit{Person}-def: oid-of \(x\) = (case \(x\) of \(\text{mk}\textit{Person} \\text{oid} \rightarrow \text{oid})
\end{definition}
\begin{instance}
\end{instance}
\end{definition}

\begin{definition}
oid-of-type\textit{OclAny}-def: oid-of \(x\) = (case \(x\) of \(\text{mk}\textit{OclAny} \\text{oid} \rightarrow \text{oid})
\end{definition}
\begin{instance}
\end{instance}
\end{definition}

\begin{definition}
oid-of-\(\mathfrak{A}\)-def: oid-of \(x\) = (case \(x\) of \(\text{in}\textit{Person} \text{person} \Rightarrow \text{oid-of person}
\mid \text{in}\textit{OclAny} \text{oclany} \Rightarrow \text{oid-of oclany})
\end{definition}
\begin{instance}
\end{instance}
\end{definition}

\subsection{Instantiation of the Generic Strict Equality}
We instantiate the referential equality on \textit{Person} and \textit{OclAny}
\begin{definition}[overloaded]
\textit{StrictRefEq}\textit{Object}\textit{-Person} : (x::\textit{Person}) \= y \equiv \textit{StrictRefEq}\textit{Object} x y
\end{definition}
\begin{definition}[overloaded]
\textit{StrictRefEq}\textit{Object}\textit{-OclAny} : (x::\textit{OclAny}) \= y \equiv \textit{StrictRefEq}\textit{Object} x y
\end{definition}
\begin{lemmas}
\textit{cp-StrictRefEq}\textit{Object}\textit{-Person}[\text{of } x::\textit{Person} y::\textit{Person} \tau, simplified \textit{StrictRefEq}\textit{Object}\textit{-Person}[\text{symmetric}]]
\textit{cp-intro}(9) \[\text{of } P::\textit{Person} \Rightarrow \textit{PersonQ}::\textit{Person} \Rightarrow \textit{Person}, simplified \textit{StrictRefEq}\textit{Object}\textit{-Person}[\text{symmetric}]]
\textit{StrictRefEq}\textit{Object}\textit{-def}\textit{arys} \[\text{of } - x::\textit{Person} y::\textit{Person}, simplified \textit{StrictRefEq}\textit{Object}\textit{-Person}[\text{symmetric}]]
\textit{StrictRefEq}\textit{Object}\textit{-strict1} \[\text{of } x::\textit{Person}, simplified \textit{StrictRefEq}\textit{Object}\textit{-Person}[\text{symmetric}]]
\textit{StrictRefEq}\textit{Object}\textit{-strict2} \[\text{of } x::\textit{Person}, simplified \textit{StrictRefEq}\textit{Object}\textit{-Person}[\text{symmetric}]]
\end{lemmas}

For each Class \(C\), we will have a casting operation \texttt{oclAsType}(\(C\)), a test on the actual type \texttt{oclIsTypeOf}(\(C\)) as well as its relaxed form \texttt{oclIsKindOf}(\(C\)) (corresponding exactly to Java’s \texttt{instanceof}-operator.

Thus, since we have two class-types in our concrete class hierarchy, we have two operations to declare and to provide two overloading definitions for the two static types.
7.1.4. OclAsType

Definition

consts \( OclAsType_{\text{OclAny}} :: 'a \Rightarrow \text{OclAny}((-) \cdot oclAsType('\text{OclAny}')) \)

consts \( OclAsType_{\text{Person}} :: 'a \Rightarrow \text{Person}((-) \cdot oclAsType('\text{Person}')) \)

definition \( OclAsType_{\text{OclAny}} - \mathcal{A} = (\lambda u. \begin{cases} \text{in}_\text{OclAny} a \Rightarrow a \\ \text{in}_\text{Person} (mk\text{Person} oid a b) \Rightarrow mk\text{OclAny} oid [(a, b)] \end{cases}) \)

lemma \( OclAsType_{\text{OclAny}} - \mathcal{A} - \text{some}: OclAsType_{\text{OclAny}} - \mathcal{A} x \neq \text{None} \)

defs (overloaded) \( OclAsType_{\text{OclAny}} - \text{OclAny}: \)

\[ (X :: \text{OclAny}) \cdot oclAsType(\text{OclAny}) \equiv X \]

defs (overloaded) \( OclAsType_{\text{Person}} - \text{Person}: \)

\[ (X :: \text{Person}) \cdot oclAsType(\text{OclAny}) \equiv \]

\( (\lambda \tau. \begin{cases} \bot \Rightarrow \text{invalid} \tau \\ [\bot] \Rightarrow \text{null} \tau \\ [\text{mk}\text{Person} oid a b] \Rightarrow [\text{mk}\text{OclAny} oid [(a, b)]] \end{cases}) \)

definition \( OclAsType_{\text{Person}} - \mathcal{A} = (\lambda u. \begin{cases} \text{in}_\text{Person} p \Rightarrow [\text{p}] \\ \text{in}_\text{OclAny} (mk\text{OclAny} oid [(a, b)]) \Rightarrow [\text{mk}\text{Person} oid a b] \\ \_ \Rightarrow \text{None} \end{cases}) \)

defs (overloaded) \( OclAsType_{\text{Person}} - \text{OclAny}: \)

\[ (X :: \text{OclAny}) \cdot oclAsType(\text{Person}) \equiv \]

\( (\lambda \tau. \begin{cases} \bot \Rightarrow \text{invalid} \tau \\ [\bot] \Rightarrow \text{null} \tau \\ [\text{mk}\text{OclAny} oid \bot] \Rightarrow \text{invalid} \tau \text{ (* down-cast exception *)} \\ [\text{mk}\text{OclAny} oid [(a, b)]] \Rightarrow [\text{mk}\text{Person} oid a b] \end{cases}) \)

defs (overloaded) \( OclAsType_{\text{Person}} - \text{Person}: \)

\[ (X :: \text{Person}) \cdot oclAsType(\text{Person}) \equiv X \]

lemmas [simp] =

\( OclAsType_{\text{OclAny}} - \text{OclAny} \)

\( OclAsType_{\text{Person}} - \text{Person} \)

Context Passing

lemma \( \text{cp-OclAsType}_{\text{OclAny}} - \text{Person} - \text{Person}: \text{cp} P \implies \text{cp}(\lambda X. (P (X :: \text{Person}) :: \text{Person}) \cdot oclAsType(\text{OclAny}))) \)

⟨proof⟩

lemma \( \text{cp-OclAsType}_{\text{OclAny}} - \text{OclAny} - \text{OclAny}: \text{cp} P \implies \text{cp}(\lambda X. (P (X :: \text{OclAny}) :: \text{OclAny}) \cdot oclAsType(\text{OclAny}))) \)

136
proof

lemma cp-OclAsType_Person-Person-Person: cp P \implies cp(\lambda X. (P (X::Person)::Person))

(\proof)

lemma cp-OclAsType_Person-OclAny-OclAny: cp P \implies cp(\lambda X. (P (X::OclAny)::OclAny))

(\proof)

lemma cp-OclAsType_OclAny-Person-Person: cp P \implies cp(\lambda X. (P (X::Person)::Person))

(\proof)

lemma cp-OclAsType_Person-Person-OclAny: cp P \implies cp(\lambda X. (P (X::Person)::OclAny))

(\proof)

lemma cp-OclAsType_OclAny-OclAny-Person: cp P \implies cp(\lambda X. (P (X::OclAny)::Person))

(\proof)

lemma cp-OclAsType_OclAny-Person-Person: cp P \implies cp(\lambda X. (P (X::Person)::Person))

(\proof)

lemmas [simp] =
  cp-OclAsType_OclAny-Person-Person
  cp-OclAsType_OclAny-OclAny-OclAny
  cp-OclAsType_Person-Person-Person
  cp-OclAsType_Person-OclAny-OclAny

Execution with Invalid or Null as Argument

lemma OclAsType_OclAny-OclAny-strict : (invalid::OclAny) .oclAsType(OclAny) = invalid

(\proof)

lemma OclAsType_OclAny-OclAny-nullstrict : (null::OclAny) .oclAsType(OclAny) = null

(\proof)

lemma OclAsType_OclAny-Person-strict[simp] : (invalid::Person) .oclAsType(OclAny) = invalid

(\proof)

lemma OclAsType_OclAny-Person-nullstrict[simp] : (null::Person) .oclAsType(OclAny) = null

(\proof)

lemma OclAsType_Person-OclAny-strict[simp] : (invalid::OclAny) .oclAsType(Person) = invalid

(\proof)

137
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

cons OclIsTypeOf_OclAny :: ′α ⇒ Boolean ((·).oclIsTypeOf′(OclAny′))
cons 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 ?? *)
            | [mkOclAny oid ⊥] ⇒ true τ
            | [mkOclAny 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
            | [mkOclAny oid ⊥] ⇒ false τ
            | [mkOclAny 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 P x P (X::Person)::Person).oclIsTypeOf(OclAny)) ⟨proof⟩
lemma cp-OclIsTypeOf_OclAny-OclAny: cp(\(\lambda X. (P(X :: \text{OclAny}) :: \text{OclAny}). \text{oclIsTypeOf}(\text{OclAny})\))
(\text{proof})

lemma cp-OclIsTypeOf_Person-Person-Person: cp(\(\lambda X. (P(X :: \text{Person}) :: \text{Person}). \text{oclIsTypeOf}(\text{Person})\))
(\text{proof})

lemma cp-OclIsTypeOf_Person-OclAny-OclAny: cp(\(\lambda X. (P(X :: \text{OclAny}) :: \text{OclAny}). \text{oclIsTypeOf}(\text{Person})\))
(\text{proof})

lemma cp-OclIsTypeOf_Person-OclAny-Person: cp(\(\lambda X. (P(X :: \text{OclAny}) :: \text{Person}). \text{oclIsTypeOf}(\text{Person})\))
(\text{proof})

lemma cp-OclIsTypeOf_Person-Person-Person: cp(\(\lambda X. (P(X :: \text{Person}) :: \text{Person}). \text{oclIsTypeOf}(\text{Person})\))
(\text{proof})

lemma cp-OclIsTypeOf_Person-OclAny-OclAny: cp(\(\lambda X. (P(X :: \text{Person}) :: \text{OclAny}). \text{oclIsTypeOf}(\text{Person})\))
(\text{proof})

lemma cp-OclIsTypeOf_Person-OclAny-Person: cp(\(\lambda X. (P(X :: \text{Person}) :: \text{Person}). \text{oclIsTypeOf}(\text{Person})\))
(\text{proof})

lemma cp-OclIsTypeOf_Person-OclAny-Person: cp(\(\lambda X. (P(X :: \text{Person}) :: \text{Person}). \text{oclIsTypeOf}(\text{Person})\))
(\text{proof})

lemmas [simp] =

\text{cp-OclIsTypeOf}_OclAny-Person-Person
\text{cp-OclIsTypeOf}_OclAny-OclAny-OclAny
\text{cp-OclIsTypeOf}_Person-Person-Person
\text{cp-OclIsTypeOf}_Person-OclAny-OclAny
\text{cp-OclIsTypeOf}_Person-Person-OclAny
\text{cp-OclIsTypeOf}_OclAny-Person-OclAny
\text{cp-OclIsTypeOf}_OclAny-Person-Person
\text{cp-OclIsTypeOf}_OclAny-Person-OclAny
\text{cp-OclIsTypeOf}_Person-OclAny-Person
\text{cp-OclIsTypeOf}_Person-Person-OclAny
\text{cp-OclIsTypeOf}_Person-Person-Person
\text{cp-OclIsTypeOf}_Person-OclAny-OclAny

\text{Execution with Invalid or Null as Argument}

lemma OclIsTypeOf_OclAny-OclAny-strict1[simp]:
\(\text{invalid} :: \text{OclAny}. \text{oclIsTypeOf}(\text{OclAny}) = \text{invalid}\)
(\text{proof})

lemma OclIsTypeOf_OclAny-OclAny-strict2[simp]:
\(\text{null} :: \text{OclAny}. \text{oclIsTypeOf}(\text{OclAny}) = \text{true}\)
(\text{proof})

lemma OclIsTypeOf_OclAny-Person-strict1[simp]:
\(\text{invalid} :: \text{Person}. \text{oclIsTypeOf}(\text{OclAny}) = \text{invalid}\)
(\text{proof})

lemma OclIsTypeOf_OclAny-Person-strict2[simp]:
\(\text{null} :: \text{Person}. \text{oclIsTypeOf}(\text{OclAny}) = \text{true}\)
(\text{proof})
lemma OclIsTypeOf_person-OclAny-strict1\[simp\]:
\[
\text{(invalid::OclAny).oclIsTypeOf(Person) = invalid}
\]
\langle proof \rangle

lemma OclIsTypeOf_person-OclAny-strict2\[simp\]:
\[
\text{(null::OclAny).oclIsTypeOf(Person) = true}
\]
\langle proof \rangle

lemma OclIsTypeOf_person-Person-strict1\[simp\]:
\[
\text{(invalid::Person).oclIsTypeOf(Person) = invalid}
\]
\langle proof \rangle

lemma OclIsTypeOf_person-Person-strict2\[simp\]:
\[
\text{(null::Person).oclIsTypeOf(Person) = true}
\]
\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 \( \tau \models \text{not } (v \ (X.oclAsType(Person))) \)
\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]:
\( (X::Person).oclAsType(OclAny).oclAsType(Person) = X) \)
\langle proof \rangle

lemma up-down-cast-Person-OclAny-Person\' : assumes \( \tau \models v \ X \)
shows \( \tau \models ((X :: Person).oclAsType(OclAny).oclAsType(Person)) \models X) \)
\langle proof \rangle

lemma up-down-cast-Person-OclAny-Person\'' : assumes \( \tau \models v \ (X :: Person) \)
shows \( \tau \models (X .oclIsTypeOf(Person) \text{ implies } (X .oclAsType(OclAny).oclAsType(Person)) \models X) \)
\langle proof \rangle
7.1.6. OclIsKindOf

Definition

\textbf{consts} \textit{OclIsKindOf} \texttt{OclAny} :: \texttt{\'\alpha} \Rightarrow \texttt{Boolean} ((\ldots).\textit{oclIsKindOf}(\textit{OclAny}))

\textbf{consts} \textit{OclIsKindOf} \texttt{Person} :: \texttt{\'\alpha} \Rightarrow \texttt{Boolean} ((\ldots).\textit{oclIsKindOf}(\textit{Person}))

\textbf{defs (overloaded)} \textit{OclIsKindOf} \texttt{OclAny-}\texttt{OclAny}:
\begin{align*}
(X::\texttt{OclAny}) . \textit{oclIsKindOf}(\texttt{OclAny}) & \equiv \\
(\lambda\tau. \text{case } X \tau \text{ of } \\
\quad \bot \Rightarrow \text{invalid } \tau \\
\quad | - \Rightarrow \text{true } \tau)
\end{align*}

\textbf{defs (overloaded)} \textit{OclIsKindOf} \texttt{OclAny-}\texttt{Person}:
\begin{align*}
(X::\texttt{Person}) . \textit{oclIsKindOf}(\texttt{OclAny}) & \equiv \\
(\lambda\tau. \text{case } X \tau \text{ of } \\
\quad \bot \Rightarrow \text{invalid } \tau \\
\quad | - \Rightarrow \text{true } \tau)
\end{align*}

\textbf{defs (overloaded)} \textit{OclIsKindOf} \texttt{Person-}\texttt{OclAny}:
\begin{align*}
(X::\texttt{OclAny}) . \textit{oclIsKindOf}(\texttt{Person}) & \equiv \\
(\lambda\tau. \text{case } X \tau \text{ of } \\
\quad \bot \Rightarrow \text{invalid } \tau \\
\quad | \lfloor \bot \rfloor \Rightarrow \text{true } \tau \\
\quad | \lfloor \lfloor \text{mk}\texttt{OclAny} oid \bot \rfloor \rfloor \Rightarrow \text{false } \tau \\
\quad | \lfloor \lfloor \text{mk}\texttt{OclAny} oid \lfloor - \rfloor \rfloor \Rightarrow \text{true } \tau)
\end{align*}

\textbf{defs (overloaded)} \textit{OclIsKindOf} \texttt{Person-}\texttt{Person}:
\begin{align*}
(X::\texttt{Person}) . \textit{oclIsKindOf}(\texttt{Person}) & \equiv \\
(\lambda\tau. \text{case } X \tau \text{ of } \\
\quad \bot \Rightarrow \text{invalid } \tau \\
\quad | - \Rightarrow \text{true } \tau)
\end{align*}

\textbf{Context Passing}

\textbf{lemma} \textit{cp-OclIsKindOf} \texttt{OclAny-}\texttt{Person-Person}:
\begin{align*}
\textit{cp} & \quad P \\
\textit{cp}(\lambda X. (P(X::\texttt{Person})::\texttt{Person}).\textit{oclIsKindOf}(\texttt{OclAny})) & \Rightarrow
\end{align*}

(\textit{proof})

\textbf{lemma} \textit{cp-OclIsKindOf} \texttt{OclAny-}\texttt{OclAny-}\texttt{OclAny}:
\begin{align*}
\textit{cp} & \quad P \\
\textit{cp}(\lambda X. (P(X::\texttt{OclAny})::\texttt{OclAny}).\textit{oclIsKindOf}(\texttt{OclAny})) & \Rightarrow
\end{align*}

(\textit{proof})

\textbf{lemma} \textit{cp-OclIsKindOf} \texttt{Person-}\texttt{Person-Person}:
\begin{align*}
\textit{cp} & \quad P \\
\textit{cp}(\lambda X. (P(X::\texttt{Person})::\texttt{Person}).\textit{oclIsKindOf}(\texttt{Person})) & \Rightarrow
\end{align*}

(\textit{proof})

\textbf{lemma} \textit{cp-OclIsKindOf} \texttt{Person-}\texttt{OclAny-}\texttt{OclAny}:
\begin{align*}
\textit{cp} & \quad P \\
\textit{cp}(\lambda X. (P(X::\texttt{OclAny})::\texttt{OclAny}).\textit{oclIsKindOf}(\texttt{Person})) & \Rightarrow
\end{align*}

(\textit{proof})

141
lemma \[ \text{cp-OclIsKindOf}_{\text{OclAny}-\text{Person-OclAny}}: \text{cp}(\lambda X. (P(X::\text{Person})::\text{OclAny}).\text{oclIsKindOf}(\text{OclAny})) \implies \text{cp} \]
lemma \[ \text{cp-OclIsKindOf}_{\text{OclAny-OclAny-Person}}: \text{cp}(\lambda X. (P(X::\text{OclAny})::\text{Person}).\text{oclIsKindOf}(\text{OclAny})) \implies \text{cp} \]
lemma \[ \text{cp-OclIsKindOf}_{\text{Person-Person-\text{OclAny}}}: \text{cp}(\lambda X. (P(X::\text{Person})::\text{OclAny}).\text{oclIsKindOf}(\text{Person})) \implies \text{cp} \]
lemma \[ \text{cp-OclIsKindOf}_{\text{Person-\text{OclAny}-\text{Person}}}: \text{cp}(\lambda X. (P(X::\text{OclAny})::\text{Person}).\text{oclIsKindOf}(\text{Person})) \implies \text{cp} \]

lemmas [simp] =
\text{cp-OclIsKindOf}_{\text{OclAny-\text{Person-Person}}}
\text{cp-OclIsKindOf}_{\text{OclAny-OclAny-\text{OclAny}}}
\text{cp-OclIsKindOf}_{\text{Person-\text{Person-Person}}}
\text{cp-OclIsKindOf}_{\text{Person-\text{OclAny-\text{OclAny}}}}
\text{cp-OclIsKindOf}_{\text{Person-\text{OclAny-Person}}}
\text{cp-OclIsKindOf}_{\text{Person-\text{OclAny-\text{OclAny}}}}

\text{Execution with Invalid or Null as Argument}

lemma \text{OclIsKindOf}_{\text{OclAny-\text{OclAny-strict1 [simp]}}}: (\text{invalid}::\text{OclAny}).\text{oclIsKindOf}(\text{OclAny}) = \text{invalid}
\langle \text{proof} \rangle
lemma \text{OclIsKindOf}_{\text{OclAny-\text{OclAny-strict2 [simp]}}}: (\text{null}::\text{OclAny}).\text{oclIsKindOf}(\text{OclAny}) = \text{true}
\langle \text{proof} \rangle
lemma \text{OclIsKindOf}_{\text{OclAny-\text{Person-strict1 [simp]}}}: (\text{invalid}::\text{Person}).\text{oclIsKindOf}(\text{OclAny}) = \text{invalid}
\langle \text{proof} \rangle
lemma \text{OclIsKindOf}_{\text{OclAny-\text{Person-strict2 [simp]}}}: (\text{null}::\text{Person}).\text{oclIsKindOf}(\text{OclAny}) = \text{true}
\langle \text{proof} \rangle
lemma \text{OclIsKindOf}_{\text{Person-\text{OclAny-strict1 [simp]}}}: (\text{invalid}::\text{OclAny}).\text{oclIsKindOf}(\text{Person}) = \text{invalid}
\langle \text{proof} \rangle
lemma \text{OclIsKindOf}_{\text{Person-\text{OclAny-strict2 [simp]}}}: (\text{null}::\text{OclAny}).\text{oclIsKindOf}(\text{Person}) = \text{true}
\langle \text{proof} \rangle
lemma \text{OclIsKindOf}_{\text{Person-\text{Person-strict1 [simp]}}}: (\text{invalid}::\text{Person}).\text{oclIsKindOf}(\text{Person}) =
invalid

\begin{proof}

\textbf{lemma} \textit{OclIsKindOf\_Person\_Person\_strict2[simp]}: \((\text{null}::\text{Person})\ .\text{oclIsKindOf}(\text{Person}) = \text{true} \)

\begin{proof}

\textbf{Up Down Casting}

\textbf{lemma} \textit{actualKind-larger-staticKind}:

\textbf{assumes} \textit{isdef}: \(\tau \models (\delta \ X)\)

\textbf{shows} \(\tau \models (X::\text{Person})\ .\text{oclIsKindOf}(\text{OclAny}) \triangleq \text{true} \)

\begin{proof}

\textbf{lemma} \textit{down-cast-kind}:

\textbf{assumes} \textit{isOclAny}: \(\neg \tau \models (X::\text{OclAny})\ .\text{oclIsKindOf}(\text{Person})\)

\textbf{and} \textit{non-null}: \(\tau \models (\delta \ X)\)

\textbf{shows} \(\tau \models (X\ .\text{oclAsType}(\text{Person})) \triangleq \text{invalid} \)

\begin{proof}

\textbf{7.1.7. OclAllInstances}

To denote OCL-types occurring in OCL expressions syntactically—as, for example, as “argument” of \texttt{oclAllInstances()}—we use the inverses of the injection functions into the object universes; we show that this is sufficient “characterization.”

\textbf{definition} \textit{Person} \equiv \text{OclAsType}\_\text{Person}\_\text{A}

\textbf{definition} \textit{OclAny} \equiv \text{OclAsType}\_\text{OclAny}\_\text{A}

\textbf{lemmas} [\textit{simp}] = \textit{Person-def OclAny-def}

\textbf{lemma} \textit{OclAllInstances-generic\_OclAny-exec}:

\textit{OclAllInstances-generic pre-post OclAny} =

\((\lambda\tau.\ \text{Abs-Set-0}[\text{heap}(\text{pre-post}\ \tau)])\)

\begin{proof}

\textbf{lemma} \textit{OclAllInstances-at-post\_OclAny-exec}:

\textit{OclAny.allInstances}() =

\((\lambda\tau.\ \text{Abs-Set-0}[\text{heap}(\text{snd}\ \tau)])\)

\begin{proof}

\textbf{lemma} \textit{OclAllInstances-at-pre\_OclAny-exec}:

\textit{OclAny.allInstances@pre()} =

\((\lambda\tau.\ \text{Abs-Set-0}[\text{heap}(\text{fst}\ \tau)])\)

\begin{proof}

\textbf{OclIsTypeOf}

\textbf{lemma} \textit{OclAny-allInstances-generic-oclIsTypeOf\_OclAny}\_1:

\textbf{assumes} [\textit{simp}]: \(\forall x.\ \text{pre-post}\ (x, x) = x\)

\textbf{shows} \(\exists \tau.\ \tau \models ((\text{OclAllInstances-generic}\ \text{pre-post}\ \text{OclAny})\rightarrow\text{forall}(X|X\ .\text{oclIsTypeOf}(\text{OclAny})))\)

\begin{proof}

\textbf{lemma} \textit{OclAny-allInstances-at-post-oclIsTypeOf\_OclAny}\_1:
\exists \tau. (\tau \models (\text{OclAny}.\text{allInstances}() \rightarrow \text{forAll}(X | X.\text{oclIsTypeOf}(\text{OclAny}))))

\langle \text{proof} \rangle

\text{lemma OclAny-allInstances-at-pre-oclIsTypeOf OclAny}^1:
\exists \tau. (\tau \models (\text{OclAny}.\text{allInstances}@\text{pre}() \rightarrow \text{forAll}(X | X.\text{oclIsTypeOf}(\text{OclAny}))))

\langle \text{proof} \rangle

\text{lemma OclAny-allInstances-generic-oclIsTypeOf OclAny}^2:
\text{assumes [simp]}: \forall x. \text{pre-post}(x, x) = x
\text{shows} \exists \tau. (\tau \models \text{not)((OclAllInstances-generic pre-post OclAny) \rightarrow \text{forAll}(X | X.\text{oclIsTypeOf}(\text{OclAny}))))

\langle \text{proof} \rangle

\text{lemma OclAny-allInstances-at-post-oclIsTypeOf OclAny}^2:
\exists \tau. (\tau \models \text{not}((\text{OclAllInstances} generic \text{pre-post} \text{OclAny}) \rightarrow \text{forAll}(X | X.\text{oclIsTypeOf}(\text{OclAny}))))

\langle \text{proof} \rangle

\text{lemma OclAny-allInstances-at-pre-oclIsTypeOf OclAny}^2:
\exists \tau. (\tau \models \text{not}((\text{OclAllInstances} generic \text{pre-post} \text{OclAny}) \rightarrow \text{forAll}(X | X.\text{oclIsTypeOf}(\text{OclAny}))))

\langle \text{proof} \rangle

\text{lemma Person-allInstances-generic-oclIsTypeOf Person}:
\tau \models ((\text{OclAllInstances-generic pre-post Person}) \rightarrow \text{forAll}(X | X.\text{oclIsTypeOf}(\text{Person})))

\langle \text{proof} \rangle

\text{lemma Person-allInstances-at-post-oclIsTypeOf Person}:
\tau \models (\text{Person}.\text{allInstances}() \rightarrow \text{forAll}(X | X.\text{oclIsTypeOf}(\text{Person})))

\langle \text{proof} \rangle

\text{lemma Person-allInstances-at-pre-oclIsTypeOf Person}:
\tau \models (\text{Person}.\text{allInstances}@\text{pre}() \rightarrow \text{forAll}(X | X.\text{oclIsTypeOf}(\text{Person})))

\langle \text{proof} \rangle

\text{OclIsKindOf}

\text{lemma OclAny-allInstances-generic-oclIsKindOf OclAny}:
\tau \models ((\text{OclAllInstances-generic pre-post OclAny}) \rightarrow \text{forAll}(X | X.\text{oclIsKindOf}(\text{OclAny})))

\langle \text{proof} \rangle

\text{lemma OclAny-allInstances-at-post-oclIsKindOf OclAny}:
\tau \models (\text{OclAny}.\text{allInstances}() \rightarrow \text{forAll}(X | X.\text{oclIsKindOf}(\text{OclAny})))

\langle \text{proof} \rangle

\text{lemma OclAny-allInstances-at-pre-oclIsKindOf OclAny}:
\tau \models (\text{OclAny}.\text{allInstances}@\text{pre}() \rightarrow \text{forAll}(X | X.\text{oclIsKindOf}(\text{OclAny})))

\langle \text{proof} \rangle

\text{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

\text{OclIsKindOf}
lemma Person-allInstances-at-post-oclIsKindOf_OclAny:
\( \tau \models (\text{Person}.\text{allInstances}) \rightarrow \forall X | X.\text{oclIsKindOf}(\text{OclAny})) \)
\( \langle \text{proof} \rangle \)

lemma Person-allInstances-at-pre-oclIsKindOf_OclAny:
\( \tau \models (\text{Person}.\text{allInstances}@\text{pre}) \rightarrow \forall X | X.\text{oclIsKindOf}(\text{OclAny})) \)
\( \langle \text{proof} \rangle \)

lemma Person-allInstances-generic-oclIsKindOf_Person:
\( \tau \models (\text{OclAllInstances-generic pre-post Person}) \rightarrow \forall X | X.\text{oclIsKindOf}(\text{Person})) \)
\( \langle \text{proof} \rangle \)

lemma Person-allInstances-at-post-oclIsKindOf_Person:
\( \tau \models (\text{Person}.\text{allInstances}) \rightarrow \forall X | X.\text{oclIsKindOf}(\text{Person})) \)
\( \langle \text{proof} \rangle \)

lemma Person-allInstances-at-pre-oclIsKindOf_Person:
\( \tau \models (\text{Person}.\text{allInstances}@\text{pre}) \rightarrow \forall X | X.\text{oclIsKindOf}(\text{Person})) \)
\( \langle \text{proof} \rangle \)

7.1.8. The Accessors (any, boss, salary)

Should be generated entirely from a class-diagram.

Definition
definition eval-extract :: (\( A, \{a::object\} \text{ option option} \) val
\( \rightarrow (\text{oid} \Rightarrow (\{ A, c::\text{null} \} \text{ val})
\( \rightarrow (\{ A, c::\text{null} \} \text{ val})
where eval-extract X f = (\lambda \tau. \text{ case } X \tau \text{ of }
\bot \Rightarrow \text{invalid } \tau \) (* exception propagation *)
| [ ] \bot \Rightarrow \text{invalid } \tau \) (* dereferencing null pointer *)
| [ ] obj \Rightarrow f \text{ (oid-of obj) } \tau)

definition deref-oid_Person :: (\( A \text{ state} \times A \text{ state} \Rightarrow A \text{ state} \)
\( \Rightarrow (\text{type}_\text{Person} \Rightarrow (\{ A, c::\text{null} \} \text{ val})
\Rightarrow \text{oid}
\Rightarrow (\{ A, c::\text{null} \} \text{ val})
where deref-oid_Person fisnd f oid = (\lambda \tau. \text{ case } \text{ heap } (fisnd \tau) \text{ oid of }
\text{ in_Person } \text{ obj } \Rightarrow f \text{ obj } \tau
\mid - \Rightarrow \text{invalid } \tau)

definition deref-oid_OclAny :: (\( A \text{ state} \times A \text{ state} \Rightarrow A \text{ state} \)
\( \Rightarrow (\{ A, c::\text{null} \} \text{ val})
where deref-oid_OclAny fisnd f oid = (\lambda \tau. \text{ case } \text{ heap } (fisnd \tau) \text{ oid of }
\text{ in_Person } \text{ obj } \Rightarrow f \text{ obj } \tau
\mid - \Rightarrow \text{invalid } \tau)
\( \Rightarrow (\text{type}_{\text{OclAny}} \Rightarrow (\mathfrak{A}, 'c::\text{null})\text{val}) \)
\( \Rightarrow \text{oid} \)
\( \Rightarrow (\mathfrak{A}, 'c::\text{null})\text{val} \)

where \( \text{deref-oid}_{\text{OclAny}} \text{fst-snd f oid } = (\lambda \tau. \text{case heap (fst-snd } \tau) \text{ oid of} \)
\( \begin{align*}
\begin{array}{l}
\text{in}_{\text{OclAny}} \text{ obj } \Rightarrow f \text{ obj } \tau \\
- \Rightarrow \text{invalid } \tau
\end{array}
\end{align*} \)

pointer undefined in state or not referencing a type conform object representation

\text{definition} \ select_{\text{OclAny}} \text{ANY } f = (\lambda X. \text{case } X \text{ of} \)
\( (\text{mk}_{\text{OclAny}} - - \perp) \Rightarrow \text{null} \)
\( | (\text{mk}_{\text{OclAny}} - - \text{[any]}) \Rightarrow f (\lambda x - - \text{[x]} \text{ any}) \)

\text{definition} \ select_{\text{Person}} \text{BOSS } f = (\lambda X. \text{case } X \text{ of} \)
\( (\text{mk}_{\text{Person}} - - \perp) \Rightarrow \text{null} \)
\( | (\text{mk}_{\text{Person}} - - \text{[boss]}) \Rightarrow f (\lambda x - - \text{[x]} \text{ boss}) \)

\text{definition} \ select_{\text{Person}} \text{SALARY } f = (\lambda X. \text{case } X \text{ of} \)
\( (\text{mk}_{\text{Person}} - - \perp) \Rightarrow \text{null} \)
\( | (\text{mk}_{\text{Person}} - - \text{[salary] -}) \Rightarrow f (\lambda x - - \text{[x]} \text{ salary}) \)

\text{definition} \ in-pre-state = \text{fst} \)
\text{definition} \ in-post-state = \text{snd} \)

\text{definition} \ reconst-basetype = (\lambda \text{convert x. convert x}) \)

\text{definition} \ dot_{\text{OclAny}} \text{ANY } :: \text{OclAny } \Rightarrow - ((1\text{-any}) 50) \)
where \( (X).\text{any} = \text{eval-extract } X \)
\( (\text{deref-oid}_{\text{OclAny}} \text{ in-post-state} \)
\( (\text{select}_{\text{OclAny}} \text{ANY } \text{reconst-basetype}) \)) \)

\text{definition} \ dot_{\text{Person}} \text{BOSS } :: \text{Person } \Rightarrow \text{Person } ((1\text{-boss}) 50) \)
where \( (X).\text{boss} = \text{eval-extract } X \)
\( (\text{deref-oid}_{\text{Person}} \text{ in-post-state} \)
\( (\text{select}_{\text{Person}} \text{BOSS} \)
\( (\text{deref-oid}_{\text{Person}} \text{ in-post-state}) \)) \)

\text{definition} \ dot_{\text{Person}} \text{SALARY } :: \text{Person } \Rightarrow \text{Integer } ((1\text{-salary}) 50) \)
where \( (X).\text{salary} = \text{eval-extract } X \)
\( (\text{deref-oid}_{\text{Person}} \text{ in-post-state} \)
\( (\text{select}_{\text{Person}} \text{SALARY} \)
\( (\text{reconst-basetype}) \)) \)

\text{definition} \ dot_{\text{OclAny}} \text{ANY at-pre } :: \text{OclAny } \Rightarrow - ((1\text{-any@pre}) 50) \)
where \( (X).\text{any@pre} = \text{eval-extract } X \)
\( (\text{deref-oid}_{\text{OclAny}} \text{ in-pre-state} \)
\[
(\text{select}_{\text{OclAny}} \text{ANY})
\]

**definition** \( \text{dot}_{\text{Person}} \text{BOSS-at-pre} :: \text{Person} \Rightarrow \text{Person} \ ((1\ (-). \text{boss} @ \text{pre}) 50) \)

**where** \( (X). \text{boss} @ \text{pre} = \text{eval-extract} X \)

\[
(\text{deref-oid}_{\text{Person}} \text{ in-pre-state} \\
(\text{select}_{\text{Person}} \text{BOSS} \\
(\text{deref-oid}_{\text{Person}} \text{ in-pre-state})))
\]

**definition** \( \text{dot}_{\text{Person}} \text{SALARY-at-pre} :: \text{Person} \Rightarrow \text{Integer} \ ((1\ (-). \text{salary} @ \text{pre}) 50) \)

**where** \( (X). \text{salary} @ \text{pre} = \text{eval-extract} X \)

\[
(\text{deref-oid}_{\text{Person}} \text{ in-pre-state} \\
(\text{select}_{\text{Person}} \text{SALARY} \\
\text{reconst-basetype}))
\]

**lemmas** [simp] =

\[ \text{dot}_{\text{OclAny}} \text{ANY}-\text{def} \]
\[ \text{dot}_{\text{Person}} \text{BOSS}-\text{def} \]
\[ \text{dot}_{\text{Person}} \text{SALARY}-\text{def} \]
\[ \text{dot}_{\text{OclAny}} \text{ANY}-\text{at-pre-def} \]
\[ \text{dot}_{\text{Person}} \text{BOSS-at-pre-def} \]
\[ \text{dot}_{\text{Person}} \text{SALARY-at-pre-def} \]

**Context Passing**

**lemmas** [simp] = \( \text{eval-extract-def} \)

**lemma** \( \text{cp-dot}_{\text{OclAny}} \text{ANY}: ((X). \text{any} \tau) \tau = ((\lambda\ -. X \tau). \text{any}) \tau \) \( \langle \text{proof} \rangle \)

**lemma** \( \text{cp-dot}_{\text{Person}} \text{BOSS}: ((X). \text{boss} \tau) \tau = ((\lambda\ -. X \tau). \text{boss}) \tau \) \( \langle \text{proof} \rangle \)

**lemma** \( \text{cp-dot}_{\text{Person}} \text{SALARY}: ((X). \text{salary} \tau) \tau = ((\lambda\ -. X \tau). \text{salary}) \tau \) \( \langle \text{proof} \rangle \)

**lemma** \( \text{cp-dot}_{\text{OclAny}} \text{ANY}-\text{at-pre}: ((X). \text{any}@\text{pre} \tau) \tau = ((\lambda\ -. X \tau). \text{any}@\text{pre}) \tau \) \( \langle \text{proof} \rangle \)

**lemma** \( \text{cp-dot}_{\text{Person}} \text{BOSS-at-pre}: ((X). \text{boss}@\text{pre} \tau) \tau = ((\lambda\ -. X \tau). \text{boss}@\text{pre}) \tau \) \( \langle \text{proof} \rangle \)

**lemma** \( \text{cp-dot}_{\text{Person}} \text{SALARY-at-pre}: ((X). \text{salary}@\text{pre} \tau) \tau = ((\lambda\ -. X \tau). \text{salary}@\text{pre}) \tau \) \( \langle \text{proof} \rangle \)

**lemmas** \( \text{cp-dot}_{\text{OclAny}} \text{ANY}-\text{I} \) [simp, intro] =

\[ \text{cp-dot}_{\text{OclAny}} \text{ANY}[\text{THEN all}\text{I}[\text{THEN all}\text{I}], \]
\[ \text{of } \lambda X \cdot. X \lambda - \tau. \tau, \text{THEN cpI}] \]

**lemmas** \( \text{cp-dot}_{\text{OclAny}} \text{ANY}-\text{at-pre-I} \) [simp, intro] =

\[ \text{cp-dot}_{\text{OclAny}} \text{ANY}-\text{at-pre}[\text{THEN all}\text{I}[\text{THEN all}\text{I}], \]
\[ \text{of } \lambda X \cdot. X \lambda - \tau. \tau, \text{THEN cpI}] \]

**lemmas** \( \text{cp-dot}_{\text{Person}} \text{BOSS-I} \) [simp, intro] =

\[ \text{cp-dot}_{\text{Person}} \text{BOSS}[\text{THEN all}\text{I}[\text{THEN all}\text{I}], \]
\[ \text{of } \lambda X \cdot. X \lambda - \tau. \tau, \text{THEN cpI}] \]

**lemmas** \( \text{cp-dot}_{\text{Person}} \text{BOSS-at-pre-I} \) [simp, intro] =

\[ \text{cp-dot}_{\text{Person}} \text{BOSS-at-pre}[\text{THEN all}\text{I}[\text{THEN all}\text{I}], \]
\[ \text{of } \lambda X \cdot. X \lambda - \tau. \tau, \text{THEN cpI}] \]

147
lemmas $cp\cdot person\cdot SALARY\cdot I$ [simp, intro!] =
$cp\cdot person\cdot SALARY\cdot [\text{THEN} \ allI\ [\text{THEN} \ allI],$
\hspace{1cm}
of $\lambda \ X\ -\ X\ -\ \tau. \ \tau, \ \text{THEN} \ cpII$.

lemmas $cp\cdot person\cdot SALARY\cdot \text{at-pre-I}$ [simp, intro!] =
$cp\cdot person\cdot SALARY\cdot \text{at-pre}[\text{THEN} \ allI\ [\text{THEN} \ allI],$
\hspace{1cm}
of $\lambda \ X\ -\ X\ -\ \tau. \ \tau, \ \text{THEN} \ cpII.$

Execution with Invalid or Null as Argument

lemma $dot\cdot OclAny\cdot ANY\cdot \text{nullstrict}$ [simp]: $(null)\cdot any = invalid$
⟨proof⟩
lemma $dot\cdot OclAny\cdot ANY\cdot \text{at-pre-nullstrict}$ [simp] : $(null)\cdot any@pre = invalid$
⟨proof⟩
lemma $dot\cdot OclAny\cdot ANY\cdot \text{strict}$ [simp] : $(invalid)\cdot any = invalid$
⟨proof⟩
lemma $dot\cdot OclAny\cdot ANY\cdot \text{at-pre-strict}$ [simp] : $(invalid)\cdot any@pre = invalid$
⟨proof⟩

lemma $dot\cdot person\cdot BOSS\cdot \text{nullstrict}$ [simp]: $(null)\cdot boss = invalid$
⟨proof⟩
lemma $dot\cdot person\cdot BOSS\cdot \text{at-pre-nullstrict}$ [simp] : $(null)\cdot boss@pre = invalid$
⟨proof⟩
lemma $dot\cdot person\cdot BOSS\cdot \text{strict}$ [simp] : $(invalid)\cdot boss = invalid$
⟨proof⟩
lemma $dot\cdot person\cdot BOSS\cdot \text{at-pre-strict}$ [simp] : $(invalid)\cdot boss@pre = invalid$
⟨proof⟩

lemma $dot\cdot person\cdot SALARY\cdot \text{nullstrict}$ [simp]: $(null)\cdot salary = invalid$
⟨proof⟩
lemma $dot\cdot person\cdot SALARY\cdot \text{at-pre-nullstrict}$ [simp] : $(null)\cdot salary@pre = invalid$
⟨proof⟩
lemma $dot\cdot person\cdot SALARY\cdot \text{strict}$ [simp] : $(invalid)\cdot salary = invalid$
⟨proof⟩
lemma $dot\cdot person\cdot SALARY\cdot \text{at-pre-strict}$ [simp] : $(invalid)\cdot salary@pre = invalid$
⟨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 $OclInt1000 = (\lambda \ - . \ [[1000]])$
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 $OclInt3500 = (\lambda \ - . \ [[3500]])$

148
Figure 7.2.: (a) pre-state $\sigma_1$ and (b) post-state $\sigma'_1$. 

\[ \begin{align*} 
\text{definition } oid0 \equiv 0 \\
\text{definition } oid1 \equiv 1 \\
\text{definition } oid2 \equiv 2 \\
\text{definition } oid3 \equiv 3 \\
\text{definition } oid4 \equiv 4 \\
\text{definition } oid5 \equiv 5 \\
\text{definition } oid6 \equiv 6 \\
\text{definition } oid7 \equiv 7 \\
\text{definition } oid8 \equiv 8 \\
\text{definition } person1 \equiv \mkPerson{oid0 \ [1300 \ \| oid1]} \\
\text{definition } person2 \equiv \mkPerson{oid1 \ [1800 \ \| oid1]} \\
\text{definition } person3 \equiv \mkPerson{oid2 \ None \ None} \\
\text{definition } person4 \equiv \mkPerson{oid3 \ [2900 \ \| None]} \\
\text{definition } person5 \equiv \mkPerson{oid4 \ [3500 \ \| None]} \\
\text{definition } person6 \equiv \mkPerson{oid5 \ [2500 \ \| oid6]} \\
\text{definition } person7 \equiv \mkOclAny{oid6 \ [(3200, oid6) \ | \ Nothing]} \\
\text{definition } person8 \equiv \mkOclAny{oid7 \ None} \\
\text{definition } person9 \equiv \mkPerson{oid8 \ [0 \ \| None]} \\
\text{definition } \\
\sigma_1 \equiv (\{ \text{heap} = \emptyset (oid0 \mapsto in\_Person (\mkPerson{oid0 \ [1000 \ \| oid1])) \} (oid1 \mapsto in\_Person (\mkPerson{oid1 \ [1200 \ \| None}))) \\
* (oid2) \\
* (oid3 \mapsto in\_Person (\mkPerson{oid3 \ [2600 \ \| oid4]))) \\
* (oid4 \mapsto in\_Person person5) \\
* (oid5 \mapsto in\_Person (\mkPerson{oid5 \ [2300 \ \| oid3]))) \\
* (oid6) \\
* (oid7) \\
* (oid8 \mapsto in\_Person person9), \\
\text{assocs}_2 = \emptyset, \\
\text{assocs}_3 = \emptyset ] \\
\text{definition } \\
\sigma_1' \equiv (\{ \text{heap} = \emptyset (oid0 \mapsto in\_Person person1) \)
(oid1 ↦ inPerson person2)
(oid2 ↦ inPerson person3)
(oid3 ↦ inPerson person4)
(*oid4*)
(oid5 ↦ inPerson person6)
(oid6 ↦ inOclAny person7)
(oid7 ↦ inOclAny person8)
(oid8 ↦ inPerson person9),
assocs2 = empty,
assocs3 = empty |

definition σ₀ ≡ ( heap = empty, assocs₂ = empty, assocs₃ = empty )

lemma basic-τ-wff: WFF(σ₁,σ₁')
⟨proof⟩

lemma [simp,code-unfold]: dom (heap σ₁) = { oid₀,oid₁,(*,oid₂*)oid₃,oid₄,oid₅(*,oid₆,oid₇*),oid₈ }
⟨proof⟩

lemma [simp,code-unfold]: dom (heap σ₁') = { oid₀,oid₁,oid₂,oid₃,(*,oid₄*)oid₅,oid₆,oid₇,oid₈ }
⟨proof⟩

definition X_person₁ :: Person ≡ λ - [[ person₁ ]]
definition X_person₂ :: Person ≡ λ - [[ person₂ ]]
definition X_person₃ :: Person ≡ λ - [[ person₃ ]]
definition X_person₄ :: Person ≡ λ - [[ person₄ ]]
definition X_person₅ :: Person ≡ λ - [[ person₅ ]]
definition X_person₆ :: Person ≡ λ - [[ person₆ ]]
definition X_person₇ :: OclAny ≡ λ - [[ person₇ ]]
definition X_person₈ :: OclAny ≡ λ - [[ person₈ ]]
definition X_person₉ :: Person ≡ λ - [[ person₉ ]]

lemma [code-unfold]: ((x::Person) ≦ y) = StrictRefEqObject x y ⟨proof⟩
lemma [code-unfold]: ((x::OclAny) ≦ y) = StrictRefEqObject x y ⟨proof⟩

lemmas [simp,code-unfold] =
OclAsTypeOclAny-OclAny
OclAsTypeOclAny-Person
OclAsTypePerson-OclAny
OclAsTypePerson-Person

OclIsTypeOfOclAny-OclAny
OclIsTypeOfOclAny-Person
OclIsTypeOfPerson-OclAny
OclIsTypeOfPerson-Person

OclIsKindOfOclAny-OclAny
OclIsKindOfOclAny-Person
\[ OclIsKindOf\text{Person}.OclAny \]

\[ OclIsKindOf\text{Person}.\text{Person} \]

\[ \text{value} \bigwedge \text{sprec} . (\text{sprec},\sigma_1') = (X_{\text{Person} 1}.\text{salary} \not\equiv 1000) \]

\[ \text{value} \bigwedge \text{sprec} . (\text{sprec},\sigma_1') = (X_{\text{Person} 1}.\text{salary} = 1300) \]

\[ \text{value} \bigwedge \text{spost} . (\sigma_1,\text{spost}) = (X_{\text{Person} 1}.\text{salary}\text{pre} \not\equiv 1000) \]

\[ \text{value} \bigwedge \text{spost} . (\sigma_1,\text{spost}) = (X_{\text{Person} 1}.\text{salary}\text{pre} \not\equiv 1300) \]

\[ \text{value} \bigwedge \text{sprec} . (\text{sprec},\sigma_1') = (X_{\text{Person} 1}.\text{boss} \not\equiv X_{\text{Person} 1}) \]

\[ \text{value} \bigwedge \text{sprec} . (\text{sprec},\sigma_1') = (X_{\text{Person} 1}.\text{boss}\text{.boss} \not\equiv X_{\text{Person} 1}) \]

\[ \text{value} \bigwedge \text{sprec} . (\text{sprec},\sigma_1') = (X_{\text{Person} 1}.\text{boss}\text{.boss} \not\equiv X_{\text{Person} 2}) \]

\[ \text{value} \bigwedge \text{spost} . (\sigma_1,\text{spost}) = (X_{\text{Person} 1}.\text{boss}\text{pre}\text{.salary} \equiv 1800) \]

\[ \text{value} \bigwedge \text{spost} . (\sigma_1,\text{spost}) = (X_{\text{Person} 1}.\text{boss}\text{pre}\text{.salary} \equiv 1200) \]

\[ \text{value} \bigwedge \text{spost} . (\sigma_1,\text{spost}) = (X_{\text{Person} 1}.\text{boss}\text{pre}\text{.salary} \equiv 1800) \]

\[ \text{value} \bigwedge \text{spost} . (\sigma_1,\text{spost}) = (X_{\text{Person} 1}.\text{boss}\text{pre}\text{.salary} \equiv X_{\text{Person} 2}) \]

\[ \text{value} \bigwedge \text{spost} . (\sigma_1,\text{spost}) = (X_{\text{Person} 1}.\text{boss}\text{pre}\text{.salary} \equiv \text{null}) \]

\[ \text{value} \bigwedge \text{spost} . (\sigma_1,\text{spost}) = \text{not}(v(X_{\text{Person} 1}.\text{boss}\text{pre}\text{.boss}\text{pre}\text{.boss}\text{pre})) \]

\[ \text{lemma} \ (\sigma_1,\sigma_1') = (X_{\text{Person} 1}.\text{oclIsMaintained}) \]

\[ \text{lemma} \bigwedge \text{sprec} \text{spost} . (\text{sprec},\text{spost}) = ((X_{\text{Person} 1}.\text{oclAsType}\text{OclAny}).\text{oclAsType}\text{Person}) \]

\[ \text{lemma} \bigwedge \text{sprec} \text{spost} . (\text{sprec},\text{spost}) = (X_{\text{Person} 1}.\text{oclIsKindOf}\text{Person}) \]

\[ \text{value} \bigwedge \text{sprec} \text{spost} . (\text{sprec},\text{spost}) = (X_{\text{Person} 2}.\text{salary} \equiv 1800) \]

\[ \text{value} \bigwedge \text{spost} . (\sigma_1,\text{spost}) = (X_{\text{Person} 2}.\text{salary}\text{pre} \equiv 1200) \]

\[ \text{value} \bigwedge \text{spost} . (\sigma_1,\text{spost}) = (X_{\text{Person} 2}.\text{boss} \equiv X_{\text{Person} 2}) \]

\[ \text{value} \bigwedge \text{spost} . (\sigma_1,\text{spost}) = (X_{\text{Person} 2}.\text{boss}\text{salary}\text{pre} \equiv 1200) \]

\[ \text{value} \bigwedge \text{spost} . (\sigma_1,\text{spost}) = (X_{\text{Person} 2}.\text{boss}\text{pre} \equiv \text{null}) \]

\[ \text{value} \bigwedge \text{spost} . (\sigma_1,\text{spost}) = (X_{\text{Person} 2}.\text{boss}\text{pre} \equiv X_{\text{Person} 2}) \]

\[ \text{value} \bigwedge \text{spost} . (\sigma_1,\text{spost}) = (X_{\text{Person} 2}.\text{boss}\text{pre} \not\equiv (X_{\text{Person} 2}.\text{boss})) \]

\[ \text{value} \bigwedge \text{spost} . (\sigma_1,\text{spost}) = \text{not}(v(X_{\text{Person} 2}.\text{boss}\text{pre} \not\equiv \text{null})) \]

\[ \text{value} \bigwedge \text{spost} . (\sigma_1,\text{spost}) = \text{not}(v(X_{\text{Person} 2}.\text{boss}\text{pre}\text{.salary}\text{pre})) \]

\[ \text{lemma} \ (\sigma_1,\sigma_1') = (X_{\text{Person} 2}.\text{oclIsMaintained}) \]

\[ \text{value} \bigwedge \text{sprec} . (\text{sprec},\sigma_1') = (X_{\text{Person} 3}.\text{salary} \equiv \text{null}) \]

\[ \text{value} \bigwedge \text{spost} . (\sigma_1,\text{spost}) = \text{not}(v(X_{\text{Person} 3}.\text{salary}\text{pre})) \]
value $\land s_{pre} \cdot (s_{pre,\sigma_1'}) \models (X_{\text{Person}^3}.\text{boss} \not= \text{null})$
value $\land s_{pre} \cdot (s_{pre,\sigma_1'}) \models \text{not}(v(X_{\text{Person}^3}.\text{boss}.\text{salary}))$
value $\land s_{post} \cdot (\sigma_1,\sigma_{post}) \models \text{not}(v(X_{\text{Person}^3}.\text{boss}@pre))$

\text{lemma} $\langle \text{proof} \rangle$

\begin{align*}
value & \land s_{post} \cdot (\sigma_1,\sigma_{post}) \models (X_{\text{Person}^4}.\text{boss}@pre \not= X_{\text{Person}^5}) \\
value & \land s_{post} \cdot (\sigma_1,\sigma_{post}) \models \text{not}(v(X_{\text{Person}^4}.\text{boss}@pre).\text{salary}@pre \not= 3500) \\
value & \land s_{pre} \cdot (s_{pre,\sigma_1'}) \models \text{not}(v(X_{\text{Person}^5}.\text{boss})) \\

\text{lemma} & \langle \text{proof} \rangle
\end{align*}

\begin{align*}
value & \land s_{pre} \cdot (s_{pre,\sigma_1'}) \models \text{not}(v(X_{\text{Person}^6}.\text{boss}.\text{salary}@pre)) \\
value & \land s_{post} \cdot (\sigma_1,\sigma_{post}) \models (X_{\text{Person}^6}.\text{boss}@pre \not= X_{\text{Person}^4}) \\
value & \land s_{post} \cdot (\sigma_1,\sigma_{post}) \models (X_{\text{Person}^6}.\text{boss}@pre.\text{salary}@pre \not= 2900) \\
value & \land s_{post} \cdot (\sigma_1,\sigma_{post}) \models (X_{\text{Person}^6}.\text{boss}@pre.\text{salary}@pre \not= 2600) \\
value & \land s_{post} \cdot (\sigma_1,\sigma_{post}) \models (X_{\text{Person}^6}.\text{boss}@pre.\text{boss}@pre \not= X_{\text{Person}^5}) \\

\text{lemma} & \langle \text{proof} \rangle
\end{align*}

\begin{align*}
value & \land s_{pre} \land s_{post} \cdot (s_{pre,\sigma_1}',s_{post}) \models v(X_{\text{Person}^7}.\text{oclAsType}(\text{Person})) \\
value & \land s_{post} \cdot (\sigma_1,\sigma_{post}) \models \text{not}(v(X_{\text{Person}^7}.\text{oclAsType}(\text{Person}).\text{boss}@pre)) \\

\text{lemma} & \langle \text{proof} \rangle
\end{align*}

\begin{align*}
value & \land s_{pre} \land s_{post} \cdot (s_{pre,\sigma_1}',s_{post}) \models (X_{\text{Person}^7}.\text{oclAsType}(\text{Person}).\text{oclAsType}(\text{OclAny}) \\
& \text{oclAsType}(\text{Person})) \not= (X_{\text{Person}^7}.\text{oclAsType}(\text{Person}))) \\

\text{lemma} & \langle \text{proof} \rangle
\end{align*}

\begin{align*}
value & \land s_{pre} \land s_{post} \cdot (s_{pre,\sigma_1}',s_{post}) \models (X_{\text{Person}^8} \not=< X_{\text{Person}^7}) \\
value & \land s_{pre} \land s_{post} \cdot (s_{pre,\sigma_1}',s_{post}) \models \text{not}(v(X_{\text{Person}^8}.\text{oclAsType}(\text{Person}))) \\
value & \land s_{pre} \land s_{post} \cdot (s_{pre,\sigma_1}',s_{post}) \models (X_{\text{Person}^8}.\text{oclIsTypeOf}(\text{OclAny})) \\
value & \land s_{pre} \land s_{post} \cdot (s_{pre,\sigma_1}',s_{post}) \models \text{not}(X_{\text{Person}^8}.\text{oclIsTypeOf}(\text{Person})) \\
value & \land s_{pre} \land s_{post} \cdot (s_{pre,\sigma_1}',s_{post}) \models \text{not}(X_{\text{Person}^8}.\text{oclIsKindOf}(\text{Person}))
\end{align*}
\[\text{value } \land_{\text{pre } s_{\text{post}}} \ (s_{\text{pre } s_{\text{post}}}) = (X_{\text{Person} 8} . oclIsKindOf(OclAny))\]

**lemma** \(\sigma\)-modifiedonly: \(\sigma_1, \sigma_1' \models (\text{Set}\{ X_{\text{Person} 1} . oclAsType(OclAny), X_{\text{Person} 2} . oclAsType(OclAny), X_{\text{Person} 3} . oclAsType(OclAny)*, X_{\text{Person} 4} . oclAsType(OclAny), X_{\text{Person} 5} . oclAsType(OclAny)*, X_{\text{Person} 6} . oclAsType(OclAny), X_{\text{Person} 7} . oclAsType(OclAny)*, X_{\text{Person} 8} . oclAsType(OclAny)*\}) \rightarrow oclIsModifiedOnly()\)

(proof)

**lemma** \(\sigma_1, \sigma_1' \models (\text{Set}\{ X_{\text{Person} 9} . oclAsType(OclAny)\}) \rightarrow oclIsModifiedOnly()\)

(proof)

**lemma** \(\sigma_1, \sigma_1' \models (\text{Set}\{ X_{\text{Person} 9} . oclAsType(OclAny)\}) \rightarrow oclIsModifiedOnly()\)

(proof)

**lemma** perm-\(\sigma_1': \sigma_1' = \emptyset\) heap = empty

\(\begin{align*}
oid 8 & \rightarrow in_{\text{Person}} \text{person9} \\
oid 7 & \rightarrow in_{\text{OclAny}} \text{person8} \\
oid 6 & \rightarrow in_{\text{OclAny}} \text{person7} \\
oid 5 & \rightarrow in_{\text{Person}} \text{person6} \\
oid 4 & \rightarrow in_{\text{Person}} \text{person4} \\
oid 3 & \rightarrow in_{\text{Person}} \text{person3} \\
oid 2 & \rightarrow in_{\text{Person}} \text{person2} \\
oid 1 & \rightarrow in_{\text{Person}} \text{person1} \\
oid 0 & \rightarrow in_{\text{Person}} \text{person0} \\
\text{assocs}_2 & = \text{assocs}_2 \sigma_1' \\
\text{assocs}_3 & = \text{assocs}_3 \sigma_1' \end{align*}\)

(proof)

**declare** const-ss [simp]

**lemma** \(\forall_1.\) \(\sigma_1, \sigma_1' \models (\text{Set}\{ X_{\text{Person} 1}, X_{\text{Person} 2}, X_{\text{Person} 3}, X_{\text{Person} 4}(*, X_{\text{Person} 5}*), X_{\text{Person} 6}, X_{\text{Person} 7} . oclAsType(Person)\}) \rightarrow oclIsModifiedOnly()\)

(proof)

**lemma** \(\forall_1.\) \(\sigma_1, \sigma_1' \models (\text{Set}\{ X_{\text{Person} 1} . oclAsType(OclAny), X_{\text{Person} 2} . oclAsType(OclAny)\})

153
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 ⇒ Boolean
where A : (τ | δ self) →→
(τ | inv-Person(self)) =
(τ | (self .boss = null)) ∨
(τ | (self .boss <> null) ∧ (τ | ((self .salary ‘≤ (self .boss .salary)) ∧
(τ | inv-Person(self .boss)))))

axiomatization inv-Person-at-pre :: Person ⇒ Boolean
where B : (τ | δ self) →→
(τ | inv-Person-at-pre(self)) =
(τ | (self .boss@pre = null)) ∨
(τ | (self .boss@pre <> null) ∧
(τ | (self .boss@pre .salary@pre ‘≤ self .salary@pre)) ∧
(τ | inv-Person-at-pre(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 ⇒ (A)st ⇒ bool where
(τ | δ self) →→ ((τ | (self .boss = null)) ∨
(τ | (self .boss <> null) ∧ (τ | (self .boss .salary ‘≤ self .salary)) ∧
( inv(self .boss)τ )])
⇒ ( inv self τ)
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 \Rightarrow Set-Integer ((I(-).contents(') )) 50)
```

```
axiomatization where dot-contents-def:
(\(\tau \models ((\text{self}).\text{contents}()) \triangleq \text{result})\)) =
(\(\text{if } (\delta \text{ self}) \tau = \text{true }\tau\)
 then \(\tau \models \text{(result } \triangleq \text{if } (\text{self} . \text{boss } \not= \text{null})\)
 then \(\text{Set} \{\text{self} . \text{salary}\})\)
 else \(\text{self} . \text{boss} . \text{contents}() \rightarrow \text{including}(\text{self} . \text{salary}))\)
 endif))
else \(\tau \models \text{result } \triangleq \text{invalid}\))
```

```
consts dot-contents-AT-pre :: Person \Rightarrow Set-Integer ((I(-).contents@pre(')) 50)
```

```
axiomatization where dot-contents-AT-pre-def:
(\(\tau \models (\text{self}).\text{contents}@pre() \triangleq \text{result})\)) =
(\(\text{if } (\delta \text{ self}) \tau = \text{true }\tau\)
 then \(\tau \models \text{(result } \triangleq \text{if } (\text{self} . \text{boss@pre } \not= \text{null})\)
 then \(\text{Set} \{\text{self} . \text{salary}@pre\})\)
 else \(\text{self} . \text{boss@pre} . \text{contents}@pre() \rightarrow \text{including}(\text{self} . \text{salary}@pre))\)
 endif))
else \(\tau \models \text{result } \triangleq \text{invalid}\))
```

These \(\@\text{pre}\) 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 \Rightarrow Integer \Rightarrow Void ((I(-).insert(')) 50)
```

```
axiomatization where dot-insert-def:
(\(\tau \models ((\text{self}).\text{insert}(x) \triangleq \text{result})\)) =
```
(if (δ self) \(\tau = true\) \(\land (\forall x) \tau = true\) 
then \(\tau \models true \land \tau\) 
\(\tau \models ((self).contents() \triangleq (self).contents@pre(\rightarrow including(x))\)
else \(\tau \models ((self).insert(x) \triangleq invalid))\) 
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.\footnote{Our two examples of EmployeeDesignModel (see Chapter 7) sketch how this construction can be captured by an automated process.} 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 \(\_ = \_\) throughout this document) and the strong equality (written \(\_ \equiv \_\)), 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 \(\_ \rightarrow \text{oclIsModifiedOnly}\) and its consequences for strong and weak equality.
6. A semantic view on subtyping clarifying the role of static and dynamic type (aka apparent and actual type in Java terminology), and its consequences for casts, dynamic type-tests, and static types.

7. A semantic view on path expressions, that clarify the role of invalid and null as well as the tricky issues related to de-referentiation in pre- and post state.

8. An optional extension of the OCL semantics by infinite sets that provide means to represent “the set of potential objects or values” to state properties over them (this will be an important feature if OCL is intended to become a full-blown code annotation language in the spirit of JML [25] for semi-automated code verification, and has been considered desirable in the Aachen Meeting [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]), than 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 δ-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


163


