Featherweight OCL

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

Achim D. Brucker* Frédéric Tuong‡ Burkhart Wolff†

January 15, 2014

*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

Part I.

Introduction

1. Motivation

The Unified Modeling Language (UML) [31, 32] is one of the few modeling languages that is widely used in industry. UML is defined, in an open process, by the Object Management Group (OMG), i. e., an industry consortium. While UML is mostly known as diagrammatic modeling language (e. g., visualizing class models), it also comprises a textual language, called Object Constraint Language (OCL) [33]. OCL is a textual annotation language, originally conceived as a three-valued logic, that turns substantial parts of UML into a formal language. Unfortunately the semantics of this specification language, captured in the "Annex A" (originally, based on the work of Richters [35]) of the OCL standard leads to different interpretations of corner cases. Many of these corner cases had been subject to formal analysis since more than nearly fifteen years (see, e. g., [5, 11, 19, 22, 26]).

At its origins [28, 35], OCL was conceived as a strict semantics for undefinedness (e. g., denoted by the element `invalid`[1]), with the exception of the logical connectives of type `Boolean` that constitute a three-valued propositional logic. At its core, OCL comprises four layers:

1. Operators (e. g., `_ and _`, `_ + _`) on built-in data structures such as `Boolean`, `Integer`, or typed sets (`Set(_)`.

2. Operators on the user-defined data model (e. g., defined as part of a UML class model) such as accessors, type casts and tests.

3. Arbitrary, user-defined, side-effect-free methods,

4. Specification for invariants on states and contracts for operations to be specified via pre- and post-conditions.

Motivated by the need for aligning OCL closer with UML, recent versions of the OCL standard [30, 33] added a second exception element. While the first exception element `invalid` has a strict semantics, `null` has a non strict semantic interpretation. Unfortunately, this extension results in several inconsistencies and contradictions. These problems are reflected in difficulties to define interpreters, code-generators, specification animators or theorem provers for OCL in a uniform manner and resulting incompatibilities of various tools.

For the OCL community, the semantics of `invalid` and `null` as well as many related issues resulted in the challenge to define a consistent version of the OCL standard that is well aligned with the recent developments of the UML. A syntactical and semantical

[1] In earlier versions of the OCL standard, this element was called `OclUndefined`.

consistent standard requires a major revision of both the informal and formal parts of the standard. To discuss the future directions of the standard, several OCL experts met in November 2013 in Aachen to discuss possible mid-term improvements of OCL, strategies of standardization of OCL within the OMG, and a vision for possible long-term developments of the language [15]. During this meeting, a Request for Proposals (RFP) for OCL 2.5 was finalized and meanwhile proposed. In particular, this RFP requires that the future OCL 2.5 standard document shall be generated from a machine-checked source. This will ensure

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

In this document, we present a formalization using Isabelle/HOL [27] of a core language of OCL. The semantic theory, based on a "shallow embedding", is called *Featherweight OCL*, since it focuses on a formal treatment of the key-elements of the language (rather than a full treatment of all operators and thus, a "complete" implementation). In contrast to full OCL, it comprises just the logic captured in `Boolean`, the basic data type `Integer`, the collection type `Set`, as well as the generic construction principle of class models, which is instantiated and demonstrated for two examples (an automated support for this type-safe construction is again out of the scope of Featherweight OCL). This formal semantics definition is intended to be a proposal for the standardization process of OCL 2.5, which should ultimately replace parts of the mandatory part of the standard document [33] as well as replace completely its informative "Annex A."

2. Background

2.1. A Guided Tour Through UML/OCL

The Unified Modeling Language (UML) [31, 32] comprises a variety of model types for describing static (e. g., class models, object models) and dynamic (e. g., state-machines, activity graphs) system properties. One of the more prominent model types of the UML is the *class model* (visualized as *class diagram*) for modeling the underlying data model of a system in an object-oriented manner. As a running example, we model a part of a conference management system. Such a system usually supports the conference organizing process, e. g., creating a conference Website, reviewing submissions, registering attendees, organizing the different sessions and tracks, and indexing and producing the resulting proceedings. In this example, we constrain ourselves to the process of organizing conference sessions; Figure 2.1 shows the class model. We model the hierarchy of roles of our system as a hierarchy of classes (e. g., `Hearer`, `Speaker`, or `Chair`) using an *inheritance* relation (also called *generalization*). In particular, *inheritance* establishes a *subtyping* relationship, i. e., every `Speaker` (*subclass*) is also a `Hearer` (*superclass*).

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

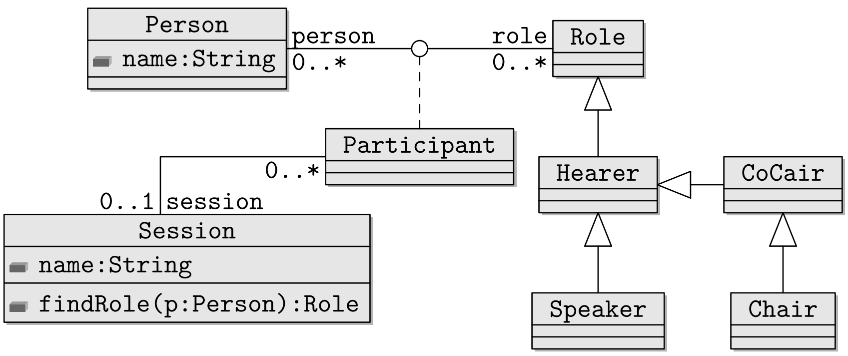


Figure 2.1.: A simple UML class model representing a conference system for organizing conference sessions: persons can participate, in different roles, in a session.

Relations between classes (called *associations* in UML) can be represented in a class diagram by connecting lines, e. g., `Participant` and `Session` or `Person` and `Role`. Associations may be labeled by a particular constraint called *multiplicity*, e. g., `0..*` or `0..1`, which means that in a relation between participants and sessions, each `Participant` object is associated to at most one `Session` object, while each `Session` object may be associated to arbitrarily many `Participant` objects. Furthermore, associations may be labeled by projection functions like `person` and `role`; these implicit function definitions allow for OCL-expressions like `self.person`, where `self` is a variable of the class `Role`. The expression `self.person` denotes persons being related to the specific object `self` of type role. A particular feature of the UML are *association classes* (`Participant` in our example) which represent a concrete tuple of the relation within a system state as an object; i. e., 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 $\mathrm{o}_{[\mathrm{C}]}$ for an object o into another class type C) that allows for converting the static type of objects along the class hierarchy. The dynamic type of an object can be understood as its "initial static type" and is unchanged by casts. We complete our example by describing the behavior of the operation `findRole` as follows:

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

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

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

A key idea of defining the semantics of UML and extensions like SecureUML [12] is to translate the diagrammatic UML features into a combination of more elementary features of UML and OCL expressions [21]. For example, associations are usually represented by collection-valued class attributes together with OCL constraints expressing the multiplicity. Thus, having a semantics for a subset of UML and OCL is tantamount for the foundation of the entire method.

2.2. Formal Foundation

2.2.1. Isabelle

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

Isabelle's inference rules are based on the built-in meta-level implication $\_ \Longrightarrow \_$ allowing to form constructs like $A_1 \Longrightarrow \cdots \Longrightarrow A_n \Longrightarrow A_{n+1}$, which are viewed as a *rule* of the form "from assumptions A_1 to A_n, infer conclusion A_{n+1}" and which is written in Isabelle as

$$[\![A_1; \ldots; A_n]\!] \Longrightarrow A_{n+1} \qquad \text{or, in mathematical notation,} \qquad \frac{A_1 \qquad \cdots \qquad A_n}{A_{n+1}}\ . \tag{2.1}$$

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:

$$\bigwedge x_1, \ldots, x_m.\ [\![A_1; \ldots; A_n]\!] \Longrightarrow A_{n+1}\ . \tag{2.2}$$

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 ϕ, using the Isar [38] language, will look as follows in Isabelle:

```
lemma label:   φ
  apply(case_tac)
  apply(simp_all)
done
```
(2.3)

This proof script instructs Isabelle to prove ϕ 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* ϕ. Proof states were usually denoted by:

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

Subgoals and goals may be extracted from the proof state into theorems of the form $[\![\phi_1; \ldots; \phi_n]\!] \Longrightarrow \phi$ 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 $\_ \wedge \_$, $\_ \to \_$, $\neg \_$ 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 $\tau_\perp := \perp \mid \llcorner\_\lrcorner : \alpha$ that assigns to each type τ a type $\tau_\perp$ *disjointly extended* by the exceptional element $\perp$. The function $\ulcorner\_\urcorner : \alpha_\perp \to \alpha$ is the inverse of $\llcorner\_\lrcorner$ (unspecified for $\perp$). Partial functions $\alpha \rightharpoonup \beta$ are defined as functions $\alpha \Rightarrow \beta_\perp$ supporting the usual concepts of domain ($\text{dom}\ \_$) and range ($\text{ran}\ \_$).

As another example of a conservative extension, typed sets were built in the Isabelle libraries conservatively on top of the kernel of HOL as functions to bool; consequently, the constant definitions for membership is as follows:[1]

$$
\begin{array}{llll}
\textsf{types} & \alpha\,\text{set} & = \alpha \Rightarrow \text{bool} & \\
\textsf{definition} & \text{Collect} & :: (\alpha \Rightarrow \text{bool}) \Rightarrow \alpha\,\text{set} & \text{— set comprehension} \\
\textsf{where} & \text{Collect}\ S & \equiv S & \\
\textsf{definition} & \text{member} & :: \alpha \Rightarrow \alpha \Rightarrow \text{bool} & \text{— membership test} \\
\textsf{where} & \text{member}\ s\ S & \equiv S s &
\end{array}
\tag{2.5}
$$

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:

$$
\begin{array}{lll}
\textsf{datatype} & \text{option} & = \text{None} \mid \text{Some}\,\alpha \\
\textsf{datatype} & \alpha\,\text{list} & = \text{Nil} \mid \text{Cons}\ a\ l
\end{array}
\tag{2.6}
$$

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

$$
\text{case}\ x\ \text{of}\ \ \text{None} \Rightarrow F\ \mid \text{Some}\,a \Rightarrow G\,a \tag{2.7}
$$

respectively

$$
\text{case}\ x\ \text{of}\ \ [] \Rightarrow F\ \mid \text{Cons}\ a\,r \Rightarrow G\,a\,r\,. \tag{2.8}
$$

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

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

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

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

[1] To increase readability, we use a slightly simplified presentation.

$$
\begin{array}{lll}
\textsf{fun} & \text{sort} & ::(\alpha :: \text{linorder})\ \text{list} \Rightarrow \alpha\ \text{list} \\
\textsf{where} & \text{sort}\,[\,] & = [\,] \\
 & \text{sort}(x\#xs) & = \text{ins}\ x\ (\text{sort}\ xs)
\end{array}
\tag{2.11}
$$

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

Thus, Isabelle/HOL also provides a large collection of theories like sets, lists, multisets, orderings, and various arithmetic theories which only contain rules derived from conservative definitions. In particular, Isabelle manages a set of *executable types and operators*, i. e., types and operators for which a compilation to SML, OCaml or Haskell is possible. Setups for arithmetic types such as int have been done; moreover any datatype and any recursive function were included in this executable set (providing that they only consist of executable operators). Similarly, Isabelle manages a large set of (higher-order) rewrite rules into which recursive function definitions were included. Provided that this rule set represents a terminating and confluent rewrite system, the Isabelle simplifier provides also a highly potent decision procedure for many fragments of theories underlying the constraints to be processed when constructing test theorems.

2.3. Featherweight OCL: Design Goals

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

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

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

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

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

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

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

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

8. It supports equational reasoning and congruence reasoning, but this requires a differentiation of the different equalities like strict equality, strong equality, meta-equality (HOL). Strict equality and strong equality require a subcalculus, "cp" (a detailed discussion of the different equalities as well as the subcalculus "cp"—for three-valued OCL 2.0—is given in [10]), which is nasty but can be hidden from the user inside tools.

2.4. The Theory Organization

The semantic theory is organized in a quite conventional manner in three layers. The first layer, called the *denotational semantics* comprises a set of definitions of the operators of the language. Presented as *definitional axioms* inside Isabelle/HOL, this part assures the 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 σ to post-state σ', 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 (σ, σ') of pre-and post-state. The precise form of states is irrelevant for this paper (compare [13]) and will be left abstract in this presentation. We construct in Isabelle a type-class null that contains two distinguishable elements bot and null. Any type of the form $(\alpha_\perp)_\perp$ is an instance of this type-class with bot $\equiv \perp$ and null $\equiv \lfloor \perp \rfloor$. Now, any OCL type can be represented by an HOL type of the form:

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

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

$$I[\![\texttt{invalid} :: V(\alpha)]\!]\tau \equiv \text{bot} \qquad I[\![\texttt{null} :: V(\alpha)]\!]\tau \equiv \text{null}$$
$$I[\![\texttt{true} :: \texttt{Boolean}]\!]\tau = \lfloor\lfloor \text{true} \rfloor\rfloor \qquad I[\![\texttt{false}]\!]\tau = \lfloor\lfloor \text{false} \rfloor\rfloor$$
$$I[\![X\,\texttt{.oclIsUndefined()}]\!]\tau = (\text{if } I[\![X]\!]\tau \in \{\text{bot}, \text{null}\} \text{ then } I[\![\texttt{true}]\!]\tau \text{ else } I[\![\texttt{false}]\!]\tau)$$
$$I[\![X\,\texttt{.oclIsInvalid()}]\!]\tau = (\text{if } I[\![X]\!]\tau = \text{bot then } I[\![\texttt{true}]\!]\tau \text{ else } I[\![\texttt{false}]\!]\tau)$$

where $I[\![E]\!]$ is the semantic interpretation function commonly used in mathematical textbooks and τ stands for pairs of pre- and post state (σ, σ'). For reasons of conciseness, we will write $\delta\ X$ for `not` X`.oclIsUndefined()` and $\upsilon\ X$ for `not` X`.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:

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

we can therefore write:

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

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 $\perp$, all expressions can be viewed as *evaluations* from (σ, σ') to a type α which must posses a $\perp$ and a null-element. Given that such constraints can be expressed in Isabelle/HOL via *type classes* (written: $\alpha :: \kappa$), all types for OCL-expressions are of a form captured by

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

where state stands for the system state and state $\times$ 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 $\_.\,\text{a}$ `@pre`. For example, $(\mathit{self}.\,\text{a} > 5)_{\text{pre}}$ is just $(\mathit{self}.\,\text{a}\,\texttt{@pre} > 5)$. This way, also invariants and pre-conditions can be interpreted by the same interpretation function and have the same type of an evaluation $V(\alpha)$.

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

$$
\begin{array}{lll}
I[\![\texttt{not}\ X]\!]\tau & = (\mathrm{case}\, I[\![X]\!]\tau\, \mathrm{of} & \\
 & \quad \bot & \Rightarrow \bot \\
 & \quad |\lfloor\bot\rfloor & \Rightarrow \lfloor\bot\rfloor \\
 & \quad |\lfloor\lfloor x\rfloor\rfloor & \Rightarrow \lfloor\lfloor\neg x\rfloor\rfloor)
\end{array}
$$

$$
\begin{array}{llll}
I[\![X\ \texttt{and}\ Y]\!]\tau & = (\mathrm{case}\, I[\![X]\!]\tau\, \mathrm{of} & & \\
 & \quad \bot & \Rightarrow (\mathrm{case}\, I[\![Y]\!]\tau\, \mathrm{of} & \\
 & & \quad \bot & \Rightarrow \bot \\
 & & \quad |\lfloor\bot\rfloor & \Rightarrow \bot \\
 & & \quad |\lfloor\lfloor \mathrm{true}\rfloor\rfloor & \Rightarrow \bot \\
 & & \quad |\lfloor\lfloor \mathrm{false}\rfloor\rfloor & \Rightarrow \lfloor\lfloor \mathrm{false}\rfloor\rfloor) \\
 & \quad |\lfloor\bot\rfloor & \Rightarrow (\mathrm{case}\, I[\![Y]\!]\tau\, \mathrm{of} & \\
 & & \quad \bot & \Rightarrow \bot \\
 & & \quad |\lfloor\bot\rfloor & \Rightarrow \lfloor\bot\rfloor \\
 & & \quad |\lfloor\lfloor \mathrm{true}\rfloor\rfloor & \Rightarrow \lfloor\bot\rfloor \\
 & & \quad |\lfloor\lfloor \mathrm{false}\rfloor\rfloor & \Rightarrow \lfloor\lfloor \mathrm{false}\rfloor\rfloor) \\
 & \quad |\lfloor\lfloor \mathrm{true}\rfloor\rfloor & \Rightarrow (\mathrm{case}\, I[\![Y]\!]\tau\, \mathrm{of} & \\
 & & \quad \bot & \Rightarrow \bot \\
 & & \quad |\lfloor\bot\rfloor & \Rightarrow \lfloor\bot\rfloor \\
 & & \quad |\lfloor\lfloor y\rfloor\rfloor & \Rightarrow \lfloor\lfloor y\rfloor\rfloor) \\
 & \quad |\lfloor\lfloor \mathrm{false}\rfloor\rfloor & \Rightarrow \lfloor\lfloor \mathrm{false}\rfloor\rfloor) &
\end{array}
$$

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

The default semantics for an OCL library operator is strict semantics; this means that the result of an operation f is invalid if one of its arguments is invalid. For a semantics comprising null, we suggest to stay conform to the standard and define the addition for integers as follows:

$$
\begin{array}{ll}
I[\![x \texttt{ + } y]\!]\tau = & \mathrm{if}\ I[\![\delta\ x]\!]\tau = \lfloor\lfloor \mathrm{true}\rfloor\rfloor \wedge I[\![\delta\ y]\!]\tau = \lfloor\lfloor \mathrm{true}\rfloor\rfloor \\
 & \mathrm{then} \lfloor\lfloor\lceil\lceil I[\![x]\!]\tau\rceil\rceil + \lceil\lceil I[\![y]\!]\tau\rceil\rceil\rfloor\rfloor \\
 & \mathrm{else}\ \bot
\end{array}
$$

where the operator "`+`" on the left-hand side of the equation denotes the OCL addition of type $[V((\mathrm{int}_\bot)_\bot), V((\mathrm{int}_\bot)_\bot)] \Rightarrow V((\mathrm{int}_\bot)_\bot)$ while the "$+$" on the right-hand side of the equation of type $[\mathrm{int}, \mathrm{int}] \Rightarrow \mathrm{int}$ 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*:

$$(\sigma, \sigma') \vDash P\,,$$

where σ is the pre-state and σ' 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 (σ, σ') (i. e., τ for short) yields true. Formally this means:

$$\tau \vDash P \equiv \big(I[\![P]\!]\tau = \lfloor\lfloor \text{true} \rfloor\rfloor\big) .$$

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:

$$\tau \models \texttt{true} \qquad \neg(\tau \models \texttt{false}) \qquad \neg(\tau \models \texttt{invalid}) \qquad \neg(\tau \models \texttt{null})$$
$$\tau \models \texttt{not}\ P \Longrightarrow \neg(\tau \models P)$$
$$\tau \models P\ \texttt{and}\ Q \Longrightarrow \tau \models P \qquad \tau \models P\ \texttt{and}\ Q \Longrightarrow \tau \models Q$$
$$\tau \models P \Longrightarrow (\texttt{if}\ P\ \texttt{then}\ B_1\ \texttt{else}\ B_2\ \texttt{endif})\tau = B_1\,\tau$$
$$\tau \models \texttt{not}\ P \Longrightarrow (\texttt{if}\ P\ \texttt{then}\ B_1\ \texttt{else}\ B_2\ \texttt{endif})\tau = B_2\,\tau$$
$$\tau \models P \Longrightarrow \tau \models \delta\, P \qquad \tau \models \delta\, X \Longrightarrow \tau \models \upsilon\, X$$

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 $\_ \doteq \_$), which is an object-oriented concept that attempts to approximate and to implement the former. Strict referential equality, which is the default in the OCL language and is written `_ = _` in the standard, is an overloaded concept and has to be defined for each OCL type individually; for objects resulting from class definitions, it is implemented by comparing the references to the objects. In contrast, strong logical equality is a polymorphic concept which is defined once and for all by:

$$I[\![X \triangleq Y]\!]\tau \equiv \lfloor\lfloor I[\![X]\!]\tau = I[\![Y]\!]\tau \rfloor\rfloor$$

It enjoys nearly the laws of a congruence:

$$\tau \models (x \triangleq x)$$
$$\tau \models (x \triangleq y) \Longrightarrow \tau \models (y \triangleq x)$$
$$\tau \models (x \triangleq y) \Longrightarrow \tau \models (y \triangleq z) \Longrightarrow \tau \models (x \triangleq z)$$
$$\operatorname{cp} P \Longrightarrow \tau \models (x \triangleq y) \Longrightarrow \tau \models (P\, x) \Longrightarrow \tau \models (P\, y)$$

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

$$\tau \models \delta\, x \Longrightarrow (\tau \models \texttt{not}\, x) = (\neg(\tau \models x))$$
$$\tau \models \delta\, x \Longrightarrow \tau \models \delta\, y \Longrightarrow (\tau \models x \,\texttt{and}\, y) = (\tau \models x \wedge \tau \models y)$$
$$\tau \models \delta\, x \Longrightarrow \tau \models \delta\, y$$
$$\Longrightarrow (\tau \models (x \,\texttt{implies}\, y)) = ((\tau \models x) \longrightarrow (\tau \models y))$$

Together with the general case-distinction

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

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

2.4.3. Algebraic Layer

Based on the logical layer, we build a system with simpler rules which are amenable to automated reasoning. We restrict ourselves to pure equations on OCL expressions, where the used equality is the meta-(HOL-)equality.

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

$$\begin{array}{cc}
\upsilon\, \texttt{invalid} = \texttt{false} & \upsilon\, \texttt{null} = \texttt{true} \\
\upsilon\, \texttt{true} = \texttt{true} & \upsilon\, \texttt{false} = \texttt{true} \\
\delta\, \texttt{invalid} = \texttt{false} & \delta\, \texttt{null} = \texttt{false} \\
\delta\, \texttt{true} = \texttt{true} & \delta\, \texttt{false} = \texttt{true} \\
\texttt{not}\, \texttt{invalid} = \texttt{invalid} & \texttt{not}\, \texttt{null} = \texttt{null} \\
\texttt{not}\, \texttt{true} = \texttt{false} & \texttt{not}\, \texttt{false} = \texttt{true} \\
(\texttt{null}\, \texttt{and}\, \texttt{true}) = \texttt{null} & (\texttt{null}\, \texttt{and}\, \texttt{false}) = \texttt{false} \\
(\texttt{null}\, \texttt{and}\, \texttt{null}) = \texttt{null} & (\texttt{null}\, \texttt{and}\, \texttt{invalid}) = \texttt{invalid} \\
(\texttt{false}\, \texttt{and}\, \texttt{true}) = \texttt{false} & (\texttt{false}\, \texttt{and}\, \texttt{false}) = \texttt{false} \\
(\texttt{false}\, \texttt{and}\, \texttt{null}) = \texttt{false} & (\texttt{false}\, \texttt{and}\, \texttt{invalid}) = \texttt{false}
\end{array}$$

$$(\texttt{true and true}) = \texttt{true} \qquad (\texttt{true and false}) = \texttt{false}$$
$$(\texttt{true and null}) = \texttt{null} \qquad (\texttt{true and invalid}) = \texttt{invalid}$$
$$(\texttt{invalid and true}) = \texttt{invalid}$$
$$(\texttt{invalid and false}) = \texttt{false}$$
$$(\texttt{invalid and null}) = \texttt{invalid}$$
$$(\texttt{invalid and invalid}) = \texttt{invalid}$$

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

$$X \texttt{ and } X = X \qquad X \texttt{ and } Y = Y \texttt{ and } X$$
$$\texttt{false and } X = \texttt{false} \qquad X \texttt{ and false} = \texttt{false}$$
$$\texttt{true and } X = X \qquad X \texttt{ and true} = X$$
$$X \texttt{ and } (Y \texttt{ and } Z) = X \texttt{ and } Y \texttt{ and } Z$$

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

$$\texttt{invalid + } X = \texttt{invalid} \qquad X \texttt{ + invalid} = \texttt{invalid}$$
$$X \texttt{ + null} = \texttt{invalid} \qquad \texttt{null + } X = \texttt{invalid}$$
$$\texttt{null.oclAsType(}X\texttt{)} = \texttt{invalid}$$

besides “classical” exceptional behavior:

$$\texttt{1 / 0} = \texttt{invalid} \qquad \texttt{1 / null} = \texttt{invalid}$$
$$\texttt{null->isEmpty()} = \texttt{true}$$

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

$$\texttt{invalid + } X = \texttt{invalid} \qquad X \texttt{ + invalid} = \texttt{invalid}$$
$$X \texttt{ + null} = \texttt{null} \qquad \texttt{null + } X = \texttt{null}$$
$$\texttt{null.oclAsType(}X\texttt{)} = \texttt{null}$$
$$\texttt{1 / 0} = \texttt{invalid} \qquad \texttt{1 / null} = \texttt{null}$$
$$\texttt{null->isEmpty()} = \texttt{null}$$

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.[2] This semantic alternative (this is *not* Featherweight OCL at present) would yield:

$$\texttt{invalid + } X = \texttt{invalid} \qquad X \texttt{ + invalid} = \texttt{invalid}$$
$$X \texttt{ + null} = X \qquad \texttt{null + } X = X$$
$$\texttt{null.oclAsType(}X\texttt{)} = \texttt{invalid}$$
$$\texttt{1 / 0} = \texttt{invalid} \qquad \texttt{1 / null} = \texttt{invalid}$$
$$\texttt{null->isEmpty()} = \texttt{true}$$

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

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

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

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

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

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

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

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

2.5. Object-oriented Datatype Theories

As mentioned earlier, the OCL is composed of

1. operators on built-in data structures such as Boolean, Integer or Set(_), and

2. operators of the user-defined data model such as accessors, type casts and tests.

In the following, we will refine the concepts of a user-defined data-model (implied by a *class-model*, visualized by a class-diagram) as well as the notion of state used in the previous section to much more detail. In contrast to wide-spread opinions, UML class diagrams represent in a compact and visual manner quite complex, object-oriented datatypes 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`.allInstances()` and C_i`.allInstancesOpre()`,

2. an inheritance relation $\_ < \_$ on classes and a collection of attributes A associated to classes,

3. two families of accessors; for each attribute a in a class definition (denoted $X.a :: C_i \to A$ and $X.a$ `@pre` $:: C_i \to A$ for $A \in \{V(\ldots_\perp), C_1, \ldots, C_n\}$),

4. type casts that can change the static type of an object of a class (X`.oclAsType(`C_i`)` of type $C_j \to C_i$)

5. two dynamic type tests (X`.oclIsTypeOf(`C_i`)` and X`.oclIsKindOf(`C_i`)`),

6. and last but not least, for each class name C_i there is an instance of the overloaded referential equality (written $\_ \doteq \_$).

Assuming a strong static type discipline in the sense of Hindley-Milner types, Featherweight OCL has no "syntactic subtyping." This does not mean that subtyping cannot be expressed *semantically* in Featherweight OCL; by giving a formal semantics to type-casts, subtyping becomes an issue of the front-end that can make implicit type-coersions explicit by introducing explicit type-casts. Our perspective shifts the emphasis on the semantic properties of casting, and the necessary universe of object representations (induced by a class model) that allows to establish them.

2.5.1. Object Universes

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

$$\text{typedef} \qquad \alpha \ \text{state} := \{\sigma :: \text{oid} \rightharpoonup \alpha \mid \text{inv}_\sigma(\sigma)\} \tag{2.12}$$

where inv_σ is a to be discussed invariant on states.

The key point is that we need a common type α 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: $C_i := (\mathrm{oid} \times A_{i_1} \times \cdots \times A_{i_k})$ 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:

$$\mathfrak{A} := C_1 + \cdots + C_n\,. \tag{2.13}$$

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:

$$X\texttt{.oclIsTypeOf(}C_k\texttt{) implies } X\texttt{.oclAsType(}C_i\texttt{).oclAsType(}C_k\texttt{)} \doteq X \tag{2.14}$$

$$\text{whenever } C_k < C_i \text{ and } X \text{ is valid.} \tag{2.15}$$

To overcome this limitation, we introduce an auxiliary type $C_{i\mathrm{ext}}$ 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* $C_{i\mathrm{ext}}$ associated to C_i is $A_{i_1} \times \cdots \times A_{i_n} \times (C_{j_1\mathrm{ext}} + \cdots + C_{j_m\mathrm{ext}})_\bot$ where A_{i_k} ranges over the local attribute types of C_i and $C_{j_l\mathrm{ext}}$ ranges over all class type extensions of the subclass C_j of C_i.

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

Example instances of this scheme—outlining a compiler—can be found in Section 6.1 and Section 7.1.

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

With respect to our semantic construction here, which above all means is intended to be type-safe, this has the following consequences:

- there is a generic theory of states, which must be formulated independently from a concrete object universe,
- there is a principle of translation (captured by the inductive scheme for class type extensions and class types above) that converts a given class model into 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:

$$
\begin{array}{l}
\textsf{definition}\\
\text{eval\_extract}\; X\; f = (\lambda\,\tau.\ \text{case}\; X\;\tau\;\text{of}\ \ \begin{array}{lll}
\ \ \bot & \Rightarrow \texttt{invalid}\;\tau & \text{exception}\\
\mid\ \lfloor\bot\rfloor & \Rightarrow \texttt{invalid}\;\tau & \text{deref. null}\\
\mid\ \lfloor\lfloor obj\rfloor\rfloor & \Rightarrow f\;(\text{oid\_of}\;\;obj)\;\tau)
\end{array}
\end{array}
\tag{2.16}
$$

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

$$
\begin{array}{l}
\textsf{definition}\ \text{deref\_oid}_C\;\ \mathit{fst\_snd}\; f\;\mathit{oid} = (\lambda\,\tau.\ \text{case}\;(\text{heap}\;(\mathit{fst\_snd}\;\tau))\;\mathit{oid}\;\text{ of}\\
\qquad\qquad\qquad\qquad\qquad\qquad\begin{array}{ll}
\ \ \lfloor \text{in}_C\;\mathit{obj}\rfloor & \Rightarrow f\;\mathit{obj}\;\tau\\
\mid\ \_ & \Rightarrow \texttt{invalid}\;\tau)
\end{array}
\end{array}
\tag{2.17}
$$

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:

$$
\textsf{definition}\ \text{select}_a\;\ f = (\lambda\ \begin{array}{lll}
\ \ \text{mk}_C\;\;\mathit{oid}\quad \cdots\bot\cdots & C_{X\text{ext}} & \Rightarrow \texttt{null}\\
\mid\ \text{mk}_C\;\;\mathit{oid}\quad \cdots\lfloor a\rfloor\cdots & C_{X\text{ext}} & \Rightarrow f\;(\lambda\ x\ \_.\ \lfloor\lfloor x\rfloor\rfloor)\;a)
\end{array}
\tag{2.18}
$$

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:

$$
\begin{array}{llll}
\textsf{definition} & \text{in\_pre\_state} & = \text{fst} & \text{first component}\\
\textsf{definition} & \text{in\_post\_state} & = \text{snd} & \text{second component}\\
\textsf{definition} & \text{reconst\_basetype} & = \text{id} & \text{identity function}
\end{array}
\tag{2.19}
$$

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

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

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

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

The variant for an accessor yielding a collection is omitted here; its construction follows by the application of the principles of the former two. The respective variants $\_.\,a$ `@pre` were produced when in_post_state is replaced by in_pre_state.

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

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

Single-Valued Attributes

If the upper bound specified by the attribute's multiplicity is one, then an evaluation of the attribute yields a single value. Thus, the evaluation result is *not* a collection. If the lower bound specified by the multiplicity is zero, the evaluation is not required to yield a non-null value. In this case an evaluation of the attribute can return `null` to indicate an absence of value.

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

```
context OclAny::asSet():T
  post: if self = null then result = Set{}
        else result = Set{self} endif
```

Collection-Valued Attributes

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

We propose to resolve this dilemma by regarding multiplicities as optional. This point of view complies with the UML standard, that does not require lower and upper bounds to be defined for multiplicities.[3] In case a multiplicity is specified for an attribute, i. e., a lower and an upper bound are provided, we require any collection the attribute evaluates to not contain `null`. This allows for a straightforward interpretation of the multiplicity constraint. If bounds are not provided for an attribute, we consider the attribute values to not be restricted in any way. Because in particular the cardinality of the attribute's values is not bounded, the result of an evaluation of the attribute is of collection type. As the range of values that the attribute can assume is not restricted, the attribute can evaluate to a collection containing `null`. The attribute can also evaluate to `invalid`. Allowing multiplicities to be optional in this way gives the modeler the freedom to define attributes that can assume the full ranges of values provided by their types. However, we do not permit the omission of multiplicities for association ends, since the values of association ends are not only restricted by multiplicities, but also by other constraints enforcing the semantics of associations. Hence, the values of association ends cannot be completely unrestricted.

The Precise Meaning of Multiplicity Constraints

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

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

If the upper bound n is infinite, the second invariant is omitted. For the definition of these invariants we are making use of the conversion of single values to sets described in Section 2.5.2. If $n \leq 1$, the attribute `a` evaluates to a single value, which is then converted to a `Set` on which the `size` operation is called.

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

2.5.3. Other Operations on States

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

[3] We are however aware that a well-formedness rule of the UML standard does define a default bound of one in case a lower or upper bound is not specified.

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

OCL does not guarantee that an operation only modifies the path-expressions mentioned in the postcondition, i. e., it allows arbitrary relations from pre-states to post-states. This framing problem is well-known (one of the suggested solutions is [23]). We define

```
(S:Set(OclAny))->oclIsModifiedOnly():Boolean
```

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

$$I[\![X\texttt{->oclIsModifiedOnly()}]\!](\sigma,\sigma') \equiv \begin{cases} \bot & \text{if } X' = \bot \lor \text{null} \in X' \\ \llcorner\forall\, i{\in}M.\ \sigma\ i = \sigma'\ i\lrcorner & \text{otherwise}\,. \end{cases}$$

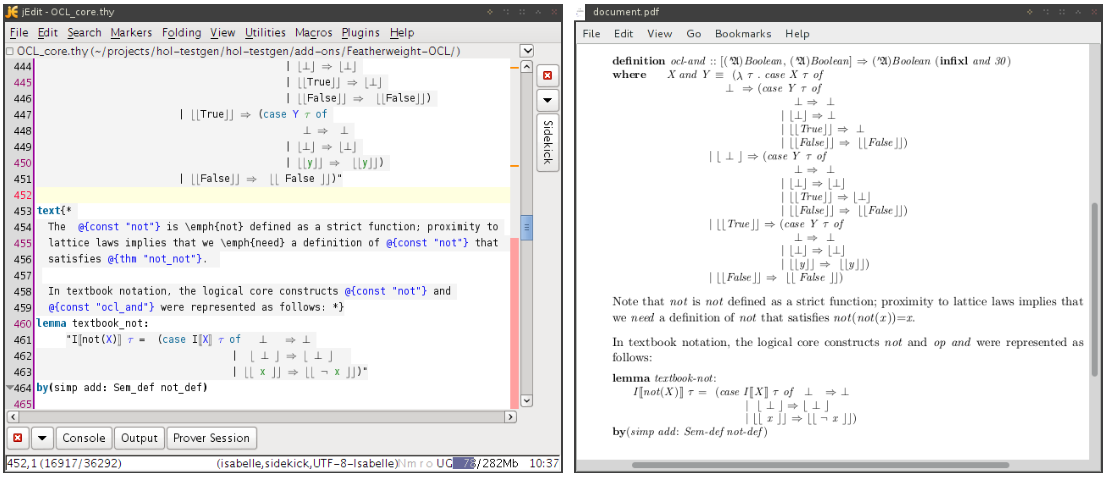
where $X' = I[\![X]\!](\sigma,\sigma')$ and $M = (\mathrm{dom}\ \sigma \cap \mathrm{dom}\ \sigma') - \{\mathrm{OidOf}\, x \mid\ x \in \ulcorner X' \urcorner\}$. Thus, if we require in a postcondition `Set{}->oclIsModifiedOnly()` and exclude via `_.oclIsNew()` and `_.oclIsDeleted()` the existence of new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

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 @{thm "not_not"} will instruct Isabelle to lock-up the (formally proven) theorem of name ocl_not_not and to replace the antiquotation with the actual theorem, i. e., `not (not x) = x`.

Figure 2.2 illustrates this approach: Figure 2.2a shows the jEdit-based development environment of Isabelle with an excerpt of one of the core theories of Featherweight OCL. Figure 2.2b shows the generated PDF document where all antiquotations are replaced. Moreover, the document generation tools allows for defining syntactic sugar as well as skipping technical details of the formalization.



(a) The Isabelle jEdit environment. (b) The generated formal document.

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

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

1. that all formal context is syntactically correct and well-typed, and

2. all formal definitions and the derived logical rules are semantically consistent.

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

Part II.

A Proposal for Formal Semantics of OCL 2.5

3. Formalization I: Core Definitions

theory
  OCL-core
imports
  Main
begin

3.1. Preliminaries

3.1.1. Notations for the Option Type

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

notation *Some* $(\lfloor(\text{-})\rfloor)$
notation *None* $(\bot)$

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

fun $\quad$ $drop :: {'\alpha}\ option \Rightarrow {'\alpha}\ (\lceil(\text{-})\rceil)$
where $\ drop\text{-}lift[simp]\text{: } \lceil\lfloor v\rfloor\rceil = v$

3.1.2. Minimal Notions of State and State Transitions

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

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

type-synonym $oid = nat$

We refrained from the alternative:

type-synonym $oid = ind$

which is slightly more abstract but non-executable.

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

record $('\mathfrak{A})state =$
$\quad heap \ :: oid \rightharpoonup {'\mathfrak{A}}$
$\quad assocs_2 :: oid \rightharpoonup (oid \times oid)\ list$
$\quad assocs_3 :: oid \rightharpoonup (oid \times oid \times oid)\ list$

type-synonym $('\mathfrak{A})st = '\mathfrak{A}\ state \times '\mathfrak{A}\ state$

3.1.3. Prerequisite: An Abstract Interface for OCL Types

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

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

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

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

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

3.1.4. Accommodation of Basic Types to the Abstract Interface

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

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

instantiation $option :: (bot)null$

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

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

  instance $\langle proof \rangle$
end

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

 instance $\langle proof \rangle$
end

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

3.1.5. The Semantic Space of OCL Types: Valuations

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

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

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

definition $Sem :: 'a \Rightarrow 'a\ (I[\![\text{-}]\!])$
where $I[\![x]\!] \equiv x$

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

definition $invalid :: ('\mathfrak{A},'\alpha::bot)\ val$
where $invalid \equiv \lambda\ \tau.\ bot$

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

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

⟨*proof*⟩

Note that the definition :

```
definition null     :: "('𝔄,'α::null) val"
where     "null     ≡ λ τ. null"
```

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

lemma *textbook-null-fun*: $I[\![null::('\mathfrak{A},'\alpha::null)\ val]\!]\ \tau = (null::'\alpha::null)$
⟨*proof*⟩

3.2. Definition of the Boolean Type

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

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

3.2.1. Basic Constants

lemma *bot-Boolean-def* : $(bot::('\mathfrak{A})Boolean) = (\lambda\ \tau.\ \bot)$
⟨*proof*⟩

lemma *null-Boolean-def* : $(null::('\mathfrak{A})Boolean) = (\lambda\ \tau.\ \lfloor\bot\rfloor)$
⟨*proof*⟩

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

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

lemma *bool-split*: $X\ \tau = invalid\ \tau \lor X\ \tau = null\ \tau \lor$
$X\ \tau = true\ \tau \quad \lor X\ \tau = false\ \tau$
⟨*proof*⟩

lemma [*simp*]: $false\ (a,\ b) = \lfloor\lfloor False\rfloor\rfloor$
⟨*proof*⟩

lemma [*simp*]: $true\ (a,\ b) = \lfloor\lfloor True\rfloor\rfloor$
⟨*proof*⟩

lemma *textbook-true*: $I[\![true]\!]\ \tau = \lfloor\lfloor True\rfloor\rfloor$
⟨*proof*⟩

lemma *textbook-false*: $I[\![false]\!]\ \tau = \lfloor\lfloor False\rfloor\rfloor$
⟨*proof*⟩

Name	Theorem
textbook-invalid	$I[\![invalid]\!]\ ?\tau = OCL\text{-}core.bot\text{-}class.bot$
textbook-null-fun	$I[\![null]\!]\ ?\tau = null$
textbook-true	$I[\![true]\!]\ ?\tau = \lfloor\lfloor True\rfloor\rfloor$
textbook-false	$I[\![false]\!]\ ?\tau = \lfloor\lfloor False\rfloor\rfloor$

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

3.2.2. Validity and Definedness

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

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

lemma *valid1*[*simp*]: $\upsilon\ invalid = false$
⟨*proof*⟩

lemma *valid2*[*simp*]: $\upsilon\ null = true$
⟨*proof*⟩

lemma *valid3*[*simp*]: $\upsilon\ true = true$
⟨*proof*⟩

lemma *valid4*[*simp*]: $\upsilon\ false = true$
⟨*proof*⟩

lemma *cp-valid*: $(\upsilon\ X)\ \tau = (\upsilon\ (\lambda\ \text{-}.\ X\ \tau))\ \tau$
⟨*proof*⟩

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

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

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

lemma *defined2*[*simp*]: δ *null* = *false*
⟨*proof*⟩

lemma *defined3*[*simp*]: δ *true* = *true*
⟨*proof*⟩

lemma *defined4*[*simp*]: δ *false* = *true*
⟨*proof*⟩

lemma *defined5*[*simp*]: $\delta\ \delta\ X = true$
⟨*proof*⟩

lemma *defined6*[*simp*]: $\delta\ \upsilon\ X = true$
⟨*proof*⟩

lemma *valid5*[*simp*]: $\upsilon\ \upsilon\ X = true$
⟨*proof*⟩

lemma *valid6*[*simp*]: $\upsilon\ \delta\ X = true$
⟨*proof*⟩

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

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

lemma *textbook-defined*: $I[\![\delta(X)]\!]\ \tau = (\mathit{if}\ I[\![X]\!]\ \tau = I[\![bot]\!]\ \tau\ \ \lor I[\![X]\!]\ \tau = I[\![null]\!]\ \tau$
$\mathit{then}\ I[\![false]\!]\ \tau$
$\mathit{else}\ I[\![true]\!]\ \tau)$
⟨*proof*⟩

lemma *textbook-valid*: $I[\![\upsilon(X)]\!]\ \tau = (\mathit{if}\ I[\![X]\!]\ \tau = I[\![bot]\!]\ \tau$
$\mathit{then}\ I[\![false]\!]\ \tau$
$\mathit{else}\ I[\![true]\!]\ \tau)$
⟨*proof*⟩

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

Name	Theorem
textbook-defined	$I[\![\delta\ X]\!]\ \tau = (\mathit{if}\ I[\![X]\!]\ \tau = I[\![OCL\text{-}core.bot\text{-}class.bot]\!]\ \tau \lor I[\![X]\!]\ \tau = I[\![null]\!]\ \tau\ \mathit{then}\ I[\![false]\!]\ \tau\ \mathit{else}\ I[\![true]\!]\ \tau)$
textbook-valid	$I[\![\upsilon\ X]\!]\ \tau = (\mathit{if}\ I[\![X]\!]\ \tau = I[\![OCL\text{-}core.bot\text{-}class.bot]\!]\ \tau\ \mathit{then}\ I[\![false]\!]\ \tau\ \mathit{else}\ I[\![true]\!]\ \tau)$

Table 3.2.: Basic predicate definitions of the logic.

Name	Theorem
defined1	$\delta\ invalid = false$
defined2	$\delta\ null = false$
defined3	$\delta\ true = true$
defined4	$\delta\ false = true$
defined5	$\delta\ \delta\ ?X = true$
defined6	$\delta\ \upsilon\ ?X = true$

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

3.3. The Equalities of OCL

The OCL contains a particular version of equality, written in Standard documents `_ = _` and `_ <> _` for its negation, which is referred as *weak referential equality* hereafter and for which we use the symbol $\_ \doteq \_$ throughout the formal part of this document. Its semantics is motivated by the desire of fast execution, and similarity to languages like Java and C, but does not satisfy the needs of logical reasoning over OCL expressions and specifications. We therefore introduce a second equality, referred as *strong equality* or *logical equality* and written $\_ \triangleq \_$ which is not present in the current standard but was discussed in prior texts on OCL like the Amsterdam Manifesto [19] and was identified as desirable extension of OCL in the Aachen Meeting [15] in the future 2.5 OCL Standard. The purpose of strong equality is to define and reason over OCL. It is therefore a natural task in Featherweight OCL to formally investigate the somewhat quite complex relationship between these two.

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

1. The pragmatic reason is fairly simple: users of object-oriented languages want something like a "shallow object value equality". You will want to say a.boss $\triangleq$ b.boss@pre instead of

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

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

2. The fundamental reason goes as follows: whatever you do to reason consistently over a language, you need the concept of equality: you need to know what expressions can be replaced by others because they *mean the same thing.* People call

this also "Leibniz Equality" because this philosopher brought this principle first explicitly to paper and shed some light over it. It is the theoretic foundation of what you do in an optimizing compiler: you replace expressions by *equal* ones, which you hope are easier to evaluate. In a typed language, strong equality exists uniformly over all types, it is "polymorphic" $\_ = \_ :: \alpha * \alpha \to bool$—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:

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

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

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

3.3.1. Definition

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

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

definition $StrongEq$::$[{}'\mathfrak{A}\ st \Rightarrow {}'\alpha, {}'\mathfrak{A}\ st \Rightarrow {}'\alpha] \Rightarrow ({}'\mathfrak{A})Boolean$ (**infixl** $\triangleq$ *30*)
where $X \triangleq Y \equiv \lambda\,\tau.\ \lfloor\lfloor X\ \tau = Y\ \tau\ \rfloor\rfloor$

From this follow already elementary properties like:

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

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

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

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

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

defs $StrictRefEq_{Boolean}$[*code-unfold*] :
$$(x::('\mathfrak{A})Boolean) \doteq y \equiv \lambda\ \tau.\ if\ (\upsilon\ x)\ \tau = true\ \tau \wedge (\upsilon\ y)\ \tau = true\ \tau\ then\ (x \triangleq y)\tau\ else\ invalid\ \tau$$

which implies elementary properties like:

lemma [*simp*,*code-unfold*] : $(true \doteq false) = false$
⟨*proof*⟩
lemma [*simp*,*code-unfold*] : $(false \doteq true) = false$
⟨*proof*⟩

lemma [*simp*,*code-unfold*] : $(invalid \doteq false) = invalid$
⟨*proof*⟩
lemma [*simp*,*code-unfold*] : $(invalid \doteq true) = invalid$
⟨*proof*⟩

lemma [*simp*,*code-unfold*] : $(false \doteq invalid) = invalid$
⟨*proof*⟩
lemma [*simp*,*code-unfold*] : $(true \doteq invalid) = invalid$
⟨*proof*⟩

lemma [*simp*,*code-unfold*] : $((invalid::('\mathfrak{A})Boolean) \doteq invalid) = invalid$
⟨*proof*⟩

Thus, the weak equality is *not* reflexive.

lemma *null-non-false* [*simp*,*code-unfold*]:$(null \doteq false) = false$
⟨*proof*⟩

lemma *null-non-true* [*simp*,*code-unfold*]:$(null \doteq true) = false$
⟨*proof*⟩

lemma *false-non-null* [*simp*,*code-unfold*]:$(false \doteq null) = false$
⟨*proof*⟩

lemma *true-non-null* [*simp*,*code-unfold*]:$(true \doteq null) = false$
⟨*proof*⟩

3.3.2. Fundamental Predicates on Strong Equality

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

lemma *StrongEq-refl* [*simp*]: $(X \triangleq X) = true$
⟨*proof*⟩

lemma *StrongEq-sym*: $(X \triangleq Y) = (Y \triangleq X)$
⟨*proof*⟩

lemma *StrongEq-trans-strong* [*simp*]:
  assumes A: $(X \triangleq Y) = \mathit{true}$
  and B: $(Y \triangleq Z) = \mathit{true}$
  shows $(X \triangleq Z) = \mathit{true}$
  ⟨*proof*⟩

it is only in a limited sense a congruence, at least from the point of view of this semantic theory. The point is that it is only a congruence on OCL expressions, not arbitrary HOL expressions (with which we can mix Featherweight OCL expressions). A semantic—not syntactic—characterization of OCL expressions is that they are *context-passing* or *context-invariant*, i. e., the context of an entire OCL expression, i. e. the pre and post state it referes to, is passed constantly and unmodified to the sub-expressions, i. e., all sub-expressions inside an OCL expression refer to the same context. Expressed formally, this boils down to:

lemma *StrongEq-subst* :
  assumes cp: $\bigwedge X.\ P(X)\tau = P(\lambda\ \text{-}.\ X\ \tau)\tau$
  and eq: $(X \triangleq Y)\tau = \mathit{true}\ \tau$
  shows $(P\ X \triangleq P\ Y)\tau = \mathit{true}\ \tau$
  ⟨*proof*⟩

lemma *defined7*[*simp*]: $\delta\ (X \triangleq Y) = \mathit{true}$
  ⟨*proof*⟩

lemma *valid7*[*simp*]: $\upsilon\ (X \triangleq Y) = \mathit{true}$
  ⟨*proof*⟩

lemma *cp-StrongEq*: $(X \triangleq Y)\ \tau = ((\lambda\ \text{-}.\ X\ \tau) \triangleq (\lambda\ \text{-}.\ Y\ \tau))\ \tau$
⟨*proof*⟩

3.4. Logical Connectives and their Universal Properties

It is a design goal to give OCL a semantics that is as closely as possible to a “logical system” in a known sense; a specification logic where the logical connectives can not be understood other 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 *invalid* as least, *null* as middle and *true* resp. *false* as unrelated top-elements.

definition *OclNot* :: $('\mathfrak{A})\mathit{Boolean} \Rightarrow ('\mathfrak{A})\mathit{Boolean}$ (*not*)

where $\quad$ $not\ X \equiv\ \lambda\ \tau\ .\ case\ X\ \tau\ of$

$$
\begin{array}{ll}
\quad\bot & \Rightarrow \bot \\
\mid \lfloor \bot \rfloor & \Rightarrow \lfloor \bot \rfloor \\
\mid \lfloor\lfloor\ x\ \rfloor\rfloor & \Rightarrow \lfloor\lfloor\ \neg\ x\ \rfloor\rfloor
\end{array}
$$

with term "not" we can express the notation:

syntax
$notequal \quad :: (\prime\mathfrak{A})Boolean \Rightarrow (\prime\mathfrak{A})Boolean \Rightarrow (\prime\mathfrak{A})Boolean$ (**infix** <> *40*)
translations
$a <> b == CONST\ OclNot(\ a \doteq b)$

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

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

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

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

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

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

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

definition *OclAnd* :: $[(\prime\mathfrak{A})Boolean, (\prime\mathfrak{A})Boolean] \Rightarrow (\prime\mathfrak{A})Boolean$ (**infixl** *and 30*)
where $\quad$ $X\ and\ Y \equiv\ (\lambda\ \tau\ .\ case\ X\ \tau\ of$

$$
\begin{array}{lll}
\quad\lfloor\lfloor False \rfloor\rfloor \Rightarrow & & \lfloor\lfloor False \rfloor\rfloor \\
\mid \bot & \Rightarrow (case\ Y\ \tau\ of & \\
 & \quad \lfloor\lfloor False \rfloor\rfloor \Rightarrow \lfloor\lfloor False \rfloor\rfloor & \\
 & \mid \text{-} \qquad \Rightarrow \bot) & \\
\mid \lfloor\bot\rfloor & \Rightarrow (case\ Y\ \tau\ of & \\
 & \quad \lfloor\lfloor False \rfloor\rfloor \Rightarrow \lfloor\lfloor False \rfloor\rfloor & \\
 & \mid \bot \qquad \Rightarrow \bot & \\
 & \mid \text{-} \qquad \Rightarrow \lfloor\bot\rfloor) & \\
\mid \lfloor\lfloor True \rfloor\rfloor & \Rightarrow & Y\ \tau)
\end{array}
$$

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

In textbook notation, the logical core constructs *not* and *op and* were represented as follows:

lemma *textbook-OclNot*:

$$
\begin{array}{lll}
I[\![not(X)]\!]\ \tau = & (case\ I[\![X]\!]\ \tau\ of & \bot \ \Rightarrow \bot \\
 & \mid\ \lfloor \bot \rfloor \Rightarrow \lfloor \bot \rfloor & \\
 & \mid\ \lfloor\lfloor x \rfloor\rfloor \Rightarrow \lfloor\lfloor \neg\ x \rfloor\rfloor) &
\end{array}
$$

$\langle proof \rangle$

lemma *textbook-OclAnd*:

$$
\begin{array}{l}
I[\![X\ and\ Y]\!]\ \tau = (case\ I[\![X]\!]\ \tau\ of \\
\qquad \bot\ \Rightarrow (case\ I[\![Y]\!]\ \tau\ of \\
\qquad\qquad \bot \Rightarrow\ \bot \\
\qquad\qquad \mid \lfloor\bot\rfloor \Rightarrow \bot \\
\qquad\qquad \mid \lfloor\lfloor True\rfloor\rfloor \Rightarrow\ \bot \\
\qquad\qquad \mid \lfloor\lfloor False\rfloor\rfloor \Rightarrow\ \lfloor\lfloor False\rfloor\rfloor) \\
\qquad \mid \lfloor \bot \rfloor \Rightarrow (case\ I[\![Y]\!]\ \tau\ of \\
\qquad\qquad \bot \Rightarrow\ \bot \\
\qquad\qquad \mid \lfloor\bot\rfloor \Rightarrow \lfloor\bot\rfloor \\
\qquad\qquad \mid \lfloor\lfloor True\rfloor\rfloor \Rightarrow \lfloor\bot\rfloor \\
\qquad\qquad \mid \lfloor\lfloor False\rfloor\rfloor \Rightarrow\ \lfloor\lfloor False\rfloor\rfloor) \\
\qquad \mid \lfloor\lfloor True\rfloor\rfloor \Rightarrow (case\ I[\![Y]\!]\ \tau\ of \\
\qquad\qquad \bot \Rightarrow\ \bot \\
\qquad\qquad \mid \lfloor\bot\rfloor \Rightarrow \lfloor\bot\rfloor \\
\qquad\qquad \mid \lfloor\lfloor y\rfloor\rfloor \Rightarrow\ \lfloor\lfloor y\rfloor\rfloor) \\
\qquad \mid \lfloor\lfloor False\rfloor\rfloor \Rightarrow\ \lfloor\lfloor\ False\ \rfloor\rfloor)
\end{array}
$$

$\langle proof \rangle$

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

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

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

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

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

lemma *OclAnd1*[*simp*]: (*invalid and true*) = *invalid*
$\langle proof \rangle$
lemma *OclAnd2*[*simp*]: (*invalid and false*) = *false*
$\langle proof \rangle$
lemma *OclAnd3*[*simp*]: (*invalid and null*) = *invalid*
$\langle proof \rangle$

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*]: $\bigwedge\tau.\ X\ \tau \neq \mathit{false}\ \tau \Longrightarrow (\mathit{bot}\ \mathit{and}\ X)\ \tau = \mathit{bot}\ \tau$
⟨*proof*⟩

lemma *OclAnd-bot2*[*simp*]: $\bigwedge\tau.\ X\ \tau \neq \mathit{false}\ \tau \Longrightarrow (X\ \mathit{and}\ \mathit{bot})\ \tau = \mathit{bot}\ \tau$
⟨*proof*⟩

lemma *OclAnd-null1*[*simp*]: $\bigwedge\tau.\ X\ \tau \neq \mathit{false}\ \tau \Longrightarrow X\ \tau \neq \mathit{bot}\ \tau \Longrightarrow (\mathit{null}\ \mathit{and}\ X)\ \tau = \mathit{null}\ \tau$
⟨*proof*⟩

lemma *OclAnd-null2*[*simp*]: $\bigwedge\tau.\ X\ \tau \neq \mathit{false}\ \tau \Longrightarrow X\ \tau \neq \mathit{bot}\ \tau \Longrightarrow (X\ \mathit{and}\ \mathit{null})\ \tau = \mathit{null}\ \tau$
⟨*proof*⟩

lemma *OclAnd-assoc*: $(X\ \mathit{and}\ (Y\ \mathit{and}\ Z)) = (X\ \mathit{and}\ Y\ \mathit{and}\ Z)$
⟨*proof*⟩

lemma *OclOr1*[*simp*]: $(\mathit{invalid}\ \mathit{or}\ \mathit{true}) = \mathit{true}$
⟨*proof*⟩
lemma *OclOr2*[*simp*]: $(\mathit{invalid}\ \mathit{or}\ \mathit{false}) = \mathit{invalid}$
⟨*proof*⟩
lemma *OclOr3*[*simp*]: $(\mathit{invalid}\ \mathit{or}\ \mathit{null}) = \mathit{invalid}$
⟨*proof*⟩
lemma *OclOr4*[*simp*]: $(\mathit{invalid}\ \mathit{or}\ \mathit{invalid}) = \mathit{invalid}$
⟨*proof*⟩

lemma *OclOr5*[*simp*]: $(\mathit{null}\ \mathit{or}\ \mathit{true}) = \mathit{true}$
⟨*proof*⟩
lemma *OclOr6*[*simp*]: $(\mathit{null}\ \mathit{or}\ \mathit{false}) = \mathit{null}$
⟨*proof*⟩
lemma *OclOr7*[*simp*]: $(\mathit{null}\ \mathit{or}\ \mathit{null}) = \mathit{null}$
⟨*proof*⟩
lemma *OclOr8*[*simp*]: $(\mathit{null}\ \mathit{or}\ \mathit{invalid}) = \mathit{invalid}$
⟨*proof*⟩

lemma *OclOr-idem*[*simp*]: $(X\ \mathit{or}\ X) = X$
⟨*proof*⟩

lemma *OclOr-commute*: $(X\ \mathit{or}\ Y) = (Y\ \mathit{or}\ X)$
⟨*proof*⟩

lemma *OclOr-false1*[*simp*]: $(\mathit{false}\ \mathit{or}\ Y) = Y$
⟨*proof*⟩

lemma *OclOr-false2*[*simp*]: $(Y\ \mathit{or}\ \mathit{false}) = Y$
⟨*proof*⟩

lemma *OclOr-true1*[*simp*]: $(\mathit{true}\ \mathit{or}\ Y) = \mathit{true}$
⟨*proof*⟩

lemma *OclOr-true2*: $(Y \ or \ true) = true$
$\langle proof \rangle$

lemma *OclOr-bot1*[*simp*]: $\bigwedge\tau. \ X \ \tau \neq true \ \tau \Longrightarrow (bot \ or \ X) \ \tau = bot \ \tau$
$\langle proof \rangle$

lemma *OclOr-bot2*[*simp*]: $\bigwedge\tau. \ X \ \tau \neq true \ \tau \Longrightarrow (X \ or \ bot) \ \tau = bot \ \tau$
$\langle proof \rangle$

lemma *OclOr-null1*[*simp*]: $\bigwedge\tau. \ X \ \tau \neq true \ \tau \Longrightarrow X \ \tau \neq bot \ \tau \Longrightarrow (null \ or \ X) \ \tau = null \ \tau$
$\langle proof \rangle$

lemma *OclOr-null2*[*simp*]: $\bigwedge\tau. \ X \ \tau \neq true \ \tau \Longrightarrow X \ \tau \neq bot \ \tau \Longrightarrow (X \ or \ null) \ \tau = null \ \tau$
$\langle proof \rangle$

lemma *OclOr-assoc*: $(X \ or \ (Y \ or \ Z)) = (X \ or \ Y \ or \ Z)$
$\langle proof \rangle$

lemma *OclImplies-true*: $(X \ implies \ true) = true$
$\langle proof \rangle$

lemma *deMorgan1*: $not(X \ and \ Y) = ((not \ X) \ or \ (not \ Y))$
$\langle proof \rangle$

lemma *deMorgan2*: $not(X \ or \ Y) = ((not \ X) \ and \ (not \ Y))$
$\langle proof \rangle$

3.5. A Standard Logical Calculus for OCL

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

value $\tau \models true <> false$
value $\tau \models false <> true$

3.5.1. Global vs. Local Judgements

lemma *transform1*: $P = true \Longrightarrow \tau \models P$
$\langle proof \rangle$

lemma *transform1-rev*: $\forall \ \tau. \ \tau \models P \Longrightarrow P = true$
$\langle proof \rangle$

lemma *transform2*: $(P = Q) \Longrightarrow ((\tau \models P) = (\tau \models Q))$
$\langle proof \rangle$

lemma *transform2-rev*: $\forall \ \tau. \ (\tau \models \delta \ P) \wedge (\tau \models \delta \ Q) \wedge (\tau \models P) = (\tau \models Q) \Longrightarrow P = Q$

$\langle proof \rangle$

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 $H : P = true \Longrightarrow Q = true$
shows $\tau \models P \Longrightarrow \tau \models Q$
$\langle proof \rangle$

3.5.2. Local Validity and Meta-logic

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

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

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

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

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

lemma *def-split-local*:
$(\tau \models \delta\ x) = ((\neg(\tau \models (x \triangleq invalid))) \wedge (\neg\ (\tau \models (x \triangleq null))))$
$\langle proof \rangle$

lemma *foundation5*:
$\tau \models (P\ and\ Q) \Longrightarrow (\tau \models P) \wedge (\tau \models Q)$
$\langle proof \rangle$

lemma *foundation6*:
$\tau \models P \Longrightarrow \tau \models \delta\ P$
$\langle proof \rangle$

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

lemma *foundation7'*[*simp*]:
$(\tau \models not\ (\upsilon\ x)) = (\neg\ (\tau \models \upsilon\ x))$
$\langle proof \rangle$

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

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

lemma *foundation9*:
$\tau \models \delta\ x \Longrightarrow (\tau \models not\ x) = (\neg\ (\tau \models x))$
$\langle proof \rangle$

lemma *foundation10*:
$\tau \models \delta\ x \Longrightarrow \tau \models \delta\ y \Longrightarrow (\tau \models (x\ and\ y)) = (\ (\tau \models x) \wedge (\tau \models y))$
$\langle proof \rangle$

lemma *foundation11*:
$\tau \models \delta\ x \Longrightarrow\ \ \tau \models \delta\ y \Longrightarrow (\tau \models (x\ or\ y)) = (\ (\tau \models x) \vee (\tau \models y))$
$\langle proof \rangle$

lemma *foundation12*:
$\tau \models \delta\ x \Longrightarrow\ \ \tau \models \delta\ y \Longrightarrow (\tau \models (x\ implies\ y)) = (\ (\tau \models x) \longrightarrow (\tau \models y))$
$\langle proof \rangle$

lemma *foundation13*:$(\tau \models A \triangleq true) \quad = (\tau \models A)$
$\langle proof \rangle$

lemma *foundation14*:$(\tau \models A \triangleq false) \quad = (\tau \models not\ A)$
$\langle proof \rangle$

lemma *foundation15*:$(\tau \models A \triangleq invalid) = (\tau \models not(\upsilon\ A))$
$\langle proof \rangle$

lemma *foundation16*: $\tau \models (\delta\ X) = (X\ \tau \neq bot \wedge X\ \tau \neq null)$
$\langle proof \rangle$

lemma *foundation16'*: $(\tau \models (\delta\ X)) = (X\ \tau \neq invalid\ \tau \wedge X\ \tau \neq null\ \tau)$
$\langle proof \rangle$

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

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

lemma *foundation18*: $\tau \models (\upsilon\ X) = (X\ \tau \neq invalid\ \tau)$

⟨*proof*⟩

lemma *foundation18'*: $\tau \models (\upsilon\ X) = (X\ \tau \neq bot)$
⟨*proof*⟩

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

lemma *foundation20* : $\tau \models (\delta\ X) \Longrightarrow \tau \models \upsilon\ X$
⟨*proof*⟩

lemma *foundation21*: $(not\ A \triangleq not\ B) = (A \triangleq B)$
⟨*proof*⟩

lemma *foundation22*: $(\tau \models (X \triangleq Y)) = (X\ \tau = Y\ \tau)$
⟨*proof*⟩

lemma *foundation23*: $(\tau \models P) = (\tau \models (\lambda\ \text{-}\ .\ P\ \tau))$
⟨*proof*⟩

lemmas *cp-validity=foundation23*

lemma *foundation24*:$(\tau \models not(X \triangleq Y)) = (X\ \tau \neq Y\ \tau)$
⟨*proof*⟩

lemma *defined-not-I* : $\tau \models \delta\ (x) \Longrightarrow \tau \models \delta\ (not\ x)$
⟨*proof*⟩

lemma *valid-not-I* : $\tau \models \upsilon\ (x) \Longrightarrow \tau \models \upsilon\ (not\ x)$
⟨*proof*⟩

lemma *defined-and-I* : $\tau \models \delta\ (x) \Longrightarrow \tau \models \delta\ (y) \Longrightarrow \tau \models \delta\ (x\ and\ y)$
⟨*proof*⟩

lemma *valid-and-I* : $\tau \models \upsilon\ (x) \Longrightarrow \tau \models \upsilon\ (y) \Longrightarrow \tau \models \upsilon\ (x\ and\ y)$
⟨*proof*⟩

3.5.3. Local Judgements and Strong Equality

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

lemma *StrongEq-L-sym*: $\tau \models (x \triangleq y) \Longrightarrow \tau \models (y \triangleq x)$
⟨*proof*⟩

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

$\langle proof \rangle$

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 $cp \quad :: (('\mathfrak{A},'\alpha)\ val \Rightarrow ('\mathfrak{A},'\beta)\ val) \Rightarrow bool$
where $\quad cp\ P \equiv (\exists\ f. \forall\ X\ \tau.\ P\ X\ \tau = f\ (X\ \tau)\ \tau)$

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

lemma *StrongEq-L-subst1*: $\bigwedge \tau.\ cp\ P \Longrightarrow \tau \models (x \triangleq y) \Longrightarrow \tau \models (P\ x \triangleq P\ y)$
$\langle proof \rangle$

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

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

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

lemma *cpI1*:
$(\forall\ X\ \tau.\ f\ X\ \tau = f(\lambda\text{-}.\ X\ \tau)\ \tau) \Longrightarrow cp\ P \Longrightarrow cp(\lambda X.\ f\ (P\ X))$
$\langle proof \rangle$

lemma *cpI2*:
$(\forall\ X\ Y\ \tau.\ f\ X\ Y\ \tau = f(\lambda\text{-}.\ X\ \tau)(\lambda\text{-}.\ Y\ \tau)\ \tau) \Longrightarrow$
$cp\ P \Longrightarrow cp\ Q \Longrightarrow cp(\lambda X.\ f\ (P\ X)\ (Q\ X))$
$\langle proof \rangle$

lemma *cpI3*:
$(\forall\ X\ Y\ Z\ \tau.\ f\ X\ Y\ Z\ \tau = f(\lambda\text{-}.\ X\ \tau)(\lambda\text{-}.\ Y\ \tau)(\lambda\text{-}.\ Z\ \tau)\ \tau) \Longrightarrow$
$cp\ P \Longrightarrow cp\ Q \Longrightarrow cp\ R \Longrightarrow cp(\lambda X.\ f\ (P\ X)\ (Q\ X)\ (R\ X))$
$\langle proof \rangle$

lemma *cpI4*:
$(\forall\ W\ X\ Y\ Z\ \tau.\ f\ W\ X\ Y\ Z\ \tau = f(\lambda\text{-}.\ W\ \tau)(\lambda\text{-}.\ X\ \tau)(\lambda\text{-}.\ Y\ \tau)(\lambda\text{-}.\ Z\ \tau)\ \tau) \Longrightarrow$
$cp\ P \Longrightarrow cp\ Q \Longrightarrow cp\ R \Longrightarrow cp\ S \Longrightarrow cp(\lambda X.\ f\ (P\ X)\ (Q\ X)\ (R\ X)\ (S\ X))$
$\langle proof \rangle$

lemma *cp-const* : $cp(\lambda\text{-}.\ c)$
$\langle proof \rangle$

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

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

3.5.4. Laws to Establish Definedness (δ-closure)

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

lemma *OclNot-defargs*:
$\tau \models (not\ P) \Longrightarrow \tau \models \delta\ P$
⟨*proof*⟩

lemma *OclNot-contrapos-nn*:
assumes $\tau \models \delta\ A$
assumes $\tau \models not\ B$
assumes $\tau \models A \Longrightarrow \tau \models B$
shows $\tau \models not\ A$
⟨*proof*⟩

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

3.6. Miscellaneous

3.6.1. OCL's if then else endif

definition *OclIf* :: $[(\mathfrak{'A})Boolean\ ,\ (\mathfrak{'A},'\alpha{::}null)\ val,\ (\mathfrak{'A},'\alpha)\ val] \Rightarrow (\mathfrak{'A},'\alpha)\ val$
$(if\ (\text{-})\ then\ (\text{-})\ else\ (\text{-})\ endif\ [10,10,10]50)$
where $(if\ C\ then\ B_1\ else\ B_2\ endif) = (\lambda\ \tau.\ if\ (\delta\ C)\ \tau = true\ \tau$
$then\ (if\ (C\ \tau) = true\ \tau$
$then\ B_1\ \tau$
$else\ B_2\ \tau)$
$else\ invalid\ \tau)$

lemma *cp-OclIf*:$((if\ C\ then\ B_1\ else\ B_2\ endif)\ \tau =$
$(if\ (\lambda\ \text{-}.\ C\ \tau)\ then\ (\lambda\ \text{-}.\ B_1\ \tau)\ else\ (\lambda\ \text{-}.\ B_2\ \tau)\ endif)\ \tau)$

⟨*proof*⟩

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

lemma *OclIf-invalid* [*simp*]: (*if invalid then* B_1 *else* B_2 *endif*) = *invalid*
⟨*proof*⟩

lemma *OclIf-null* [*simp*]: (*if null then* B_1 *else* B_2 *endif*) = *invalid*
⟨*proof*⟩

lemma *OclIf-true* [*simp*]: (*if true then* B_1 *else* B_2 *endif*) = B_1
⟨*proof*⟩

lemma *OclIf-true'* [*simp*]: $\tau \models P \Longrightarrow$ (*if P then* B_1 *else* B_2 *endif*)τ = B_1 τ
⟨*proof*⟩

lemma *OclIf-false* [*simp*]: (*if false then* B_1 *else* B_2 *endif*) = B_2
⟨*proof*⟩

lemma *OclIf-false'* [*simp*]: $\tau \models$ *not P* $\Longrightarrow$ (*if P then* B_1 *else* B_2 *endif*)τ = B_2 τ
⟨*proof*⟩

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

lemma *OclIf-idem2*[*simp*]:(*if* υ *X then A else A endif*) = *A*
⟨*proof*⟩

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

⟨*proof*⟩

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

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

lemma *const-charn*: *const X* $\Longrightarrow X\ \tau = X\ \tau'$
⟨*proof*⟩

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

shows $P\ X\ \tau = P\ X\ \tau'$
⟨*proof*⟩

lemma *const-imply2* :
assumes $\bigwedge \tau 1\ \tau 2.\ P\ \tau 1 = P\ \tau 2 \Longrightarrow Q\ \tau 1 = Q\ \tau 2$
shows $const\ P \Longrightarrow const\ Q$
⟨*proof*⟩

lemma *const-imply3* :
assumes $\bigwedge \tau 1\ \tau 2.\ P\ \tau 1 = P\ \tau 2 \Longrightarrow Q\ \tau 1 = Q\ \tau 2 \Longrightarrow R\ \tau 1 = R\ \tau 2$
shows $const\ P \Longrightarrow const\ Q \Longrightarrow const\ R$
⟨*proof*⟩

lemma *const-imply4* :
assumes $\bigwedge \tau 1\ \tau 2.\ P\ \tau 1 = P\ \tau 2 \Longrightarrow Q\ \tau 1 = Q\ \tau 2 \Longrightarrow R\ \tau 1 = R\ \tau 2 \Longrightarrow S\ \tau 1 = S\ \tau 2$
shows $const\ P \Longrightarrow const\ Q \Longrightarrow const\ R \Longrightarrow const\ S$
⟨*proof*⟩

lemma *const-lam* : $const\ (\lambda\text{-}.\ e)$
⟨*proof*⟩

lemma *const-true* : *const true*
⟨*proof*⟩

lemma *const-false* : *const false*
⟨*proof*⟩

lemma *const-null* : *const null*
⟨*proof*⟩

lemma *const-invalid* : *const invalid*
⟨*proof*⟩

lemma *const-bot* : *const bot*
⟨*proof*⟩

lemma *const-defined* :
assumes *const X*
shows $const\ (\delta\ X)$
⟨*proof*⟩

lemma *const-valid* :
assumes *const X*
shows $const\ (\upsilon\ X)$
⟨*proof*⟩

lemma *const-OclValid1*:
assumes *const x*
shows $(\tau \models \delta\ x) = (\tau' \models \delta\ x)$
⟨*proof*⟩

lemma *const-OclValid2*:
assumes *const x*
shows $(\tau \models \upsilon\ x) = (\tau' \models \upsilon\ x)$
⟨*proof*⟩

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

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

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

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

lemma *const-StrongEq*:
assumes *const X*
assumes *const X'*
shows $const(X \triangleq X')$
⟨*proof*⟩

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

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

end

4. Formalization II: Library Definitions

theory *OCL-lib*
imports *OCL-core*
begin

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

4.1. Basic Types: Void and Integer

4.1.1. The Construction of the Void Type

type-synonym $('\mathfrak{A})\,Void = ('\mathfrak{A},unit\ option)\ val$

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 $('\mathfrak{A})Integer = ('\mathfrak{A},int\ option\ option)\ val$

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

definition $OclInt0 :: ('\mathfrak{A})Integer\ (\mathbf{0})$
where $\mathbf{0} = (\lambda\ \text{-}\ .\ \lfloor\lfloor 0::int\rfloor\rfloor)$

definition $OclInt1 :: ('\mathfrak{A})Integer\ (\mathbf{1})$
where $\mathbf{1} = (\lambda\ \text{-}\ .\ \lfloor\lfloor 1::int\rfloor\rfloor)$

definition $OclInt2 :: ('\mathfrak{A})Integer\ (\mathbf{2})$
where $\mathbf{2} = (\lambda\ \text{-}\ .\ \lfloor\lfloor 2::int\rfloor\rfloor)$

definition $OclInt3 :: ('\mathfrak{A})Integer\ (\mathbf{3})$
where $\mathbf{3} = (\lambda\ \text{-}\ .\ \lfloor\lfloor 3::int\rfloor\rfloor)$

definition $OclInt4 :: ('\mathfrak{A})Integer\ (\mathbf{4})$
where $\mathbf{4} = (\lambda\ \text{-}\ .\ \lfloor\lfloor 4::int\rfloor\rfloor)$

definition *OclInt5* ::($'\mathfrak{A}$)*Integer* (**5**)
where **5** = (λ - . $\lfloor\lfloor$*5*::*int*$\rfloor\rfloor$)

definition *OclInt6* ::($'\mathfrak{A}$)*Integer* (**6**)
where **6** = (λ - . $\lfloor\lfloor$*6*::*int*$\rfloor\rfloor$)

definition *OclInt7* ::($'\mathfrak{A}$)*Integer* (**7**)
where **7** = (λ - . $\lfloor\lfloor$*7*::*int*$\rfloor\rfloor$)

definition *OclInt8* ::($'\mathfrak{A}$)*Integer* (**8**)
where **8** = (λ - . $\lfloor\lfloor$*8*::*int*$\rfloor\rfloor$)

definition *OclInt9* ::($'\mathfrak{A}$)*Integer* (**9**)
where **9** = (λ - . $\lfloor\lfloor$*9*::*int*$\rfloor\rfloor$)

definition *OclInt10* ::($'\mathfrak{A}$)*Integer* (**10**)
where **10** = (λ - . $\lfloor\lfloor$*10*::*int*$\rfloor\rfloor$)

4.1.3. Validity and Definedness Properties

lemma δ(*null*::($'\mathfrak{A}$)*Integer*) = *false* ⟨*proof*⟩
lemma υ(*null*::($'\mathfrak{A}$)*Integer*) = *true* ⟨*proof*⟩

lemma [*simp*,*code-unfold*]: δ (λ-. $\lfloor\lfloor n\rfloor\rfloor$) = *true*
⟨*proof*⟩

lemma [*simp*,*code-unfold*]: υ (λ-. $\lfloor\lfloor n\rfloor\rfloor$) = *true*
⟨*proof*⟩

lemma [*simp*,*code-unfold*]: δ **0** = *true* ⟨*proof*⟩
lemma [*simp*,*code-unfold*]: υ **0** = *true* ⟨*proof*⟩
lemma [*simp*,*code-unfold*]: δ **1** = *true* ⟨*proof*⟩
lemma [*simp*,*code-unfold*]: υ **1** = *true* ⟨*proof*⟩
lemma [*simp*,*code-unfold*]: δ **2** = *true* ⟨*proof*⟩
lemma [*simp*,*code-unfold*]: υ **2** = *true* ⟨*proof*⟩
lemma [*simp*,*code-unfold*]: δ **6** = *true* ⟨*proof*⟩
lemma [*simp*,*code-unfold*]: υ **6** = *true* ⟨*proof*⟩
lemma [*simp*,*code-unfold*]: δ **8** = *true* ⟨*proof*⟩
lemma [*simp*,*code-unfold*]: υ **8** = *true* ⟨*proof*⟩
lemma [*simp*,*code-unfold*]: δ **9** = *true* ⟨*proof*⟩
lemma [*simp*,*code-unfold*]: υ **9** = *true* ⟨*proof*⟩

4.1.4. Arithmetical Operations on Integer

Definition

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

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

definition $OclAdd_{Integer}$ ::$('\mathfrak{A})Integer \Rightarrow ('\mathfrak{A})Integer \Rightarrow ('\mathfrak{A})Integer$ (**infix** '+ 40)
where x '+ $y \equiv \lambda\ \tau.\ if\ (\delta\ x)\ \tau = true\ \tau \wedge (\delta\ y)\ \tau = true\ \tau$
$then\ \lfloor\lfloor\lceil\lceil x\ \tau\rceil\rceil + \lceil\lceil y\ \tau\rceil\rceil\rfloor\rfloor$
$else\ invalid\ \tau$

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

definition $OclLe_{Integer}$ ::$('\mathfrak{A})Integer \Rightarrow ('\mathfrak{A})Integer \Rightarrow ('\mathfrak{A})Boolean$ (**infix** '≤ 40)
where x '≤ $y \equiv \lambda\ \tau.\ if\ (\delta\ x)\ \tau = true\ \tau \wedge (\delta\ y)\ \tau = true\ \tau$
$then\ \lfloor\lfloor\lceil\lceil x\ \tau\rceil\rceil \leq \lceil\lceil y\ \tau\rceil\rceil\rfloor\rfloor$
$else\ invalid\ \tau$

Basic Properties

lemma $OclAdd_{Integer}$-*commute*: (X '+ Y) = (Y '+ X)
⟨*proof*⟩

Execution with Invalid or Null or Zero as Argument

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

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

lemma [*simp*,*code-unfold*] : (x '+ *null*) = *invalid*
⟨*proof*⟩

lemma [*simp*,*code-unfold*] : (*null* '+ x) = *invalid*
⟨*proof*⟩

lemma $OclAdd_{Integer}$-*zero1*[*simp*,*code-unfold*] :
(x '+ **0**) = (*if* υ x *and not* (δ x) *then invalid else* x *endif*)
⟨*proof*⟩

lemma $OclAdd_{Integer}$-*zero2*[*simp*,*code-unfold*] :
(**0** '+ x) = (*if* υ x *and not* (δ x) *then invalid else* x *endif*)
⟨*proof*⟩

Context Passing

lemma *cp*-$OclAdd_{Integer}$:(X '+ Y) τ = ((λ -. X τ) '+ (λ -. Y τ)) τ
⟨*proof*⟩

lemma $\mathit{cp\text{-}OclLess}_{\mathit{Integer}}$:$(X \text{ `}< Y)\ \tau = ((\lambda \text{ -. } X\ \tau) \text{ `}< (\lambda \text{ -. } Y\ \tau))\ \tau$
$\langle \mathit{proof} \rangle$

lemma $\mathit{cp\text{-}OclLe}_{\mathit{Integer}}$:$(X \text{ `}\leq Y)\ \tau = ((\lambda \text{ -. } X\ \tau) \text{ `}\leq (\lambda \text{ -. } Y\ \tau))\ \tau$
$\langle \mathit{proof} \rangle$

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*.

value $\tau \models (\ \mathbf{9} \text{ `}\leq \mathbf{10}\ )$
value $\tau \models ((\ \mathbf{4} \text{ `}+ \mathbf{4}\ ) \text{ `}\leq \mathbf{10}\ )$
value $\neg(\tau \models ((\ \mathbf{4} \text{ `}+ (\ \mathbf{4} \text{ `}+ \mathbf{4}\ ))\ \text{ `}< \mathbf{10}\ ))$
value $\tau \models \mathit{not}\ (\upsilon\ (\mathit{null} \text{ `}+ \mathbf{1}))$

4.2. Fundamental Predicates on Basic Types: Strict Equality

4.2.1. Definition

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

defs $\mathit{StrictRefEq}_{\mathit{Integer}}[\mathit{code\text{-}unfold}]$:
$(x::('\mathfrak{A})\mathit{Integer}) \doteq y \equiv \lambda\ \tau.\ \mathit{if}\ (\upsilon\ x)\ \tau = \mathit{true}\ \tau \wedge (\upsilon\ y)\ \tau = \mathit{true}\ \tau$
$\mathit{then}\ (x \triangleq y)\ \tau$
$\mathit{else}\ \mathit{invalid}\ \tau$

value $\tau \models \mathbf{1} <> \mathbf{2}$
value $\tau \models \mathbf{2} <> \mathbf{1}$
value $\tau \models \mathbf{2} \doteq \mathbf{2}$

4.2.2. Logic and Algebraic Layer on Basic Types

Validity and Definedness Properties (I)

lemma $\mathit{StrictRefEq}_{\mathit{Boolean}}$-*defined-args-valid*:
$(\tau \models \delta((x::('\mathfrak{A})\mathit{Boolean}) \doteq y)) = ((\tau \models(\upsilon\ x)) \wedge (\tau \models(\upsilon\ y)))$
$\langle \mathit{proof} \rangle$

lemma $\mathit{StrictRefEq}_{\mathit{Integer}}$-*defined-args-valid*:
$(\tau \models \delta((x::('\mathfrak{A})\mathit{Integer}) \doteq y)) = ((\tau \models(\upsilon\ x)) \wedge (\tau \models(\upsilon\ y)))$
$\langle \mathit{proof} \rangle$

Validity and Definedness Properties (II)

lemma $\mathit{StrictRefEq}_{\mathit{Boolean}}$-*defargs*:
$\tau \models ((x::('\mathfrak{A})\mathit{Boolean}) \doteq y) \Longrightarrow (\tau \models (\upsilon\ x)) \wedge (\tau \models(\upsilon\ y))$

$\langle proof \rangle$

lemma $StrictRefEq_{Integer}$*-defargs*:
$\tau \models ((x::('\mathfrak{A})Integer) \doteq y) \Longrightarrow (\tau \models (\upsilon\ x)) \wedge (\tau \models (\upsilon\ y))$
$\langle proof \rangle$

Validity and Definedness Properties (III) Miscellaneous

lemma $StrictRefEq_{Boolean}$*-strict''* : $\delta\ ((x::('\mathfrak{A})Boolean) \doteq y) = (\upsilon(x)\ and\ \upsilon(y))$
$\langle proof \rangle$

lemma $StrictRefEq_{Integer}$*-strict''* : $\delta\ ((x::('\mathfrak{A})Integer) \doteq y) = (\upsilon(x)\ and\ \upsilon(y))$
$\langle proof \rangle$

lemma $StrictRefEq_{Integer}$*-strict* :
  assumes A: $\upsilon\ (x::('\mathfrak{A})Integer) = true$
  and B: $\upsilon\ y = true$
  shows $\upsilon\ (x \doteq y) = true$
  $\langle proof \rangle$

lemma $StrictRefEq_{Integer}$*-strict'* :
  assumes A: $\upsilon\ (((x::('\mathfrak{A})Integer)) \doteq y) = true$
  shows $\upsilon\ x = true \wedge \upsilon\ y = true$
  $\langle proof \rangle$

Reflexivity

lemma $StrictRefEq_{Boolean}$*-refl*[*simp*,*code-unfold*] :
$((x::('\mathfrak{A})Boolean) \doteq x) = (if\ (\upsilon\ x)\ then\ true\ else\ invalid\ endif)$
$\langle proof \rangle$

lemma $StrictRefEq_{Integer}$*-refl*[*simp*,*code-unfold*] :
$((x::('\mathfrak{A})Integer) \doteq x) = (if\ (\upsilon\ x)\ then\ true\ else\ invalid\ endif)$
$\langle proof \rangle$

Execution with Invalid or Null as Argument

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

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

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

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

$\langle proof \rangle$

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

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

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

Const

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

Behavior vs StrongEq

lemma *StrictRefEq$_{Boolean}$-vs-StrongEq*:
$\tau \models(\upsilon\ x) \Longrightarrow \tau \models(\upsilon\ y) \Longrightarrow (\tau \models (((x::('\mathfrak{A})Boolean) \doteq y) \triangleq (x \triangleq y)))$
$\langle proof \rangle$

lemma *StrictRefEq$_{Integer}$-vs-StrongEq*:
$\tau \models(\upsilon\ x) \Longrightarrow \tau \models(\upsilon\ y) \Longrightarrow (\tau \models (((x::('\mathfrak{A})Integer) \doteq y) \triangleq (x \triangleq y)))$
$\langle proof \rangle$

Context Passing

lemma *cp-StrictRefEq$_{Boolean}$*:
$((X::('\mathfrak{A})Boolean) \doteq Y)\ \tau = ((\lambda\ \text{-}.\ X\ \tau) \doteq (\lambda\ \text{-}.\ Y\ \tau))\ \tau$
$\langle proof \rangle$

lemma *cp-StrictRefEq$_{Integer}$*:
$((X::('\mathfrak{A})Integer) \doteq Y)\ \tau = ((\lambda\ \text{-}.\ X\ \tau) \doteq (\lambda\ \text{-}.\ Y\ \tau))\ \tau$
$\langle proof \rangle$

lemmas *cp-intro'*[*intro*!,*simp*,*code-unfold*] =
cp-intro'
$cp\text{-}StrictRefEq_{Boolean}[THEN\ allI[THEN\ allI[THEN\ allI[THEN\ cpI2]],\ of\ StrictRefEq]]$
$cp\text{-}StrictRefEq_{Integer}[THEN\ allI[THEN\ allI[THEN\ allI[THEN\ cpI2]],\ of\ StrictRefEq]]$
$cp\text{-}OclAdd_{Integer}[THEN\ allI[THEN\ allI[THEN\ allI[THEN\ cpI2]],\ of\ OclAdd_{Integer}]]$
$cp\text{-}OclLess_{Integer}[THEN\ allI[THEN\ allI[THEN\ allI[THEN\ cpI2]],\ of\ OclLess_{Integer}]]$
$cp\text{-}OclLe_{Integer}[THEN\ allI[THEN\ allI[THEN\ allI[THEN\ cpI2]],\ of\ OclLe_{Integer}]]$

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

Elementary computations on Integer

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

value $\tau \models (\mathbf{4} <> \mathbf{10})$
value $\neg(\tau \models (\mathbf{0}\ \text{‘}{<}\ \mathit{null}))$
value $\neg(\tau \models (\delta\ (\mathbf{0}\ \text{‘}{<}\ \mathit{null})))$

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

4.3.1. The Construction of the Set Type

no-notation *None* $(\bot)$
notation *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 $\mathit{Set}(\mathit{Set}(\mathit{Sequences}(\mathit{Pairs}(X,Y))))$).

The former principle rules out the option to define $'\alpha$ *Set* just by $('\mathfrak{A}, ('\alpha\ \mathit{option}\ \mathit{option})\ \mathit{set})\ \mathit{val}$. 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 $'\alpha$ *Set-0*. It is shown that this type "fits" indeed into the abstract type interface discussed in the previous section.

typedef $'\alpha\ \mathit{Set\text{-}0} = \{X{::}('\alpha{::}\mathit{null})\ \mathit{set}\ \mathit{option}\ \mathit{option}.$
$X = \mathit{bot} \vee X = \mathit{null} \vee (\forall x{\in}\lceil\lceil X\rceil\rceil.\ x \neq \mathit{bot})\}$
$\langle \mathit{proof} \rangle$

instantiation *Set-0* :: (*null*)*bot*
begin

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

instance $\langle \mathit{proof} \rangle$
end

instantiation *Set-0* :: (*null*)*null*
begin

definition *null-Set-0-def*: $(\mathit{null}{::}('a{::}\mathit{null})\ \mathit{Set\text{-}0}) \equiv \mathit{Abs\text{-}Set\text{-}0}\ \lfloor\ \mathit{None}\ \rfloor$

instance $\langle \mathit{proof} \rangle$

end

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

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

4.3.2. Validity and Definedness Properties

Every element in a defined set is valid.

lemma *Set-inv-lemma*: $\tau \models (\delta\ X) \Longrightarrow \forall x \in \lceil\lceil Rep\text{-}Set\text{-}0\ (X\ \tau)\rceil\rceil.\ x \neq bot$
⟨*proof*⟩

lemma *Set-inv-lemma'* :
assumes *x-def* : $\tau \models \delta\ X$
and *e-mem* : $e \in \lceil\lceil Rep\text{-}Set\text{-}0\ (X\ \tau)\rceil\rceil$
shows $\tau \models \upsilon\ (\lambda\text{-}.\ e)$
⟨*proof*⟩

lemma *abs-rep-simp'* :
assumes *S-all-def* : $\tau \models \delta\ S$
shows $Abs\text{-}Set\text{-}0\ \lfloor\lfloor\lceil\lceil Rep\text{-}Set\text{-}0\ (S\ \tau)\rceil\rceil\rfloor\rfloor = S\ \tau$
⟨*proof*⟩

lemma *S-lift'* :
assumes *S-all-def* : $(\tau :: '\mathfrak{A}\ st) \models \delta\ S$
shows $\exists S'.\ (\lambda a\ (\text{-}::'\mathfrak{A}\ st).\ a)$ ` $\lceil\lceil Rep\text{-}Set\text{-}0\ (S\ \tau)\rceil\rceil = (\lambda a\ (\text{-}::'\mathfrak{A}\ st).\ \lfloor a\rfloor)$ ` S'
⟨*proof*⟩

lemma *invalid-set-OclNot-defined* [*simp*,*code-unfold*]:$\delta(invalid::('\mathfrak{A},'\alpha::null)\ Set) = false$
⟨*proof*⟩
lemma *null-set-OclNot-defined* [*simp*,*code-unfold*]:$\delta(null::('\mathfrak{A},'\alpha::null)\ Set) = false$
⟨*proof*⟩
lemma *invalid-set-valid* [*simp*,*code-unfold*]:$\upsilon(invalid::('\mathfrak{A},'\alpha::null)\ Set) = false$
⟨*proof*⟩
lemma *null-set-valid* [*simp*,*code-unfold*]:$\upsilon(null::('\mathfrak{A},'\alpha::null)\ Set) = true$
⟨*proof*⟩

... which means that we can have a type $('\mathfrak{A},('\mathfrak{A},('\mathfrak{A})$ *Integer*$)$ *Set*$)$ *Set* corresponding exactly to Set(Set(Integer)) in OCL notation. Note that the parameter $'\mathfrak{A}$ still refers to the object universe; making the OCL semantics entirely parametric in the object universe makes it possible to study (and prove) its properties independently from a concrete class diagram.

4.3.3. Constants on Sets

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

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

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

lemma *mtSet-rep-set*: $\lceil\lceil Rep\text{-}Set\text{-}0\ (Set\{\}\ \tau)\rceil\rceil = \{\}$
⟨*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* $:: [('\mathfrak{A},'\alpha::null)\ Set,('\mathfrak{A},'\alpha)\ val] \Rightarrow ('\mathfrak{A},'\alpha)\ Set$
where $OclIncluding\ x\ y = (\lambda\ \tau.\ if\ (\delta\ x)\ \tau = true\ \tau \wedge (\upsilon\ y)\ \tau = true\ \tau$
$then\ Abs\text{-}Set\text{-}0\ \lfloor\lfloor\ \lceil\lceil Rep\text{-}Set\text{-}0\ (x\ \tau)\rceil\rceil\ \cup \{y\ \tau\}\ \rfloor\rfloor$
$else\ \bot\ )$
notation *OclIncluding* (-->*including*'(-'))

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

definition *OclExcluding* $:: [('\mathfrak{A},'\alpha::null)\ Set,('\mathfrak{A},'\alpha)\ val] \Rightarrow ('\mathfrak{A},'\alpha)\ Set$
where $OclExcluding\ x\ y = (\lambda\ \tau.\ if\ (\delta\ x)\ \tau = true\ \tau \wedge (\upsilon\ y)\ \tau = true\ \tau$
$then\ Abs\text{-}Set\text{-}0\ \lfloor\lfloor\ \lceil\lceil Rep\text{-}Set\text{-}0\ (x\ \tau)\rceil\rceil - \{y\ \tau\}\ \rfloor\rfloor$
$else\ \bot\ )$
notation *OclExcluding* (-->*excluding*'(-'))

definition *OclIncludes* $:: [('\mathfrak{A},'\alpha::null)\ Set,('\mathfrak{A},'\alpha)\ val] \Rightarrow\ '\mathfrak{A}\ Boolean$
where $OclIncludes\ x\ y = (\lambda\ \tau.\ if\ (\delta\ x)\ \tau = true\ \tau \wedge (\upsilon\ y)\ \tau = true\ \tau$
$then\ \lfloor\lfloor(y\ \tau) \in \lceil\lceil Rep\text{-}Set\text{-}0\ (x\ \tau)\rceil\rceil\ \rfloor\rfloor$
$else\ \bot\ )$
notation *OclIncludes* (-->*includes*'(-'))

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

notation $OclExcludes$ $(\text{-->}excludes'(\text{-}'))$

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

definition $OclSize :: ('\mathfrak{A},'\alpha::null)Set \Rightarrow '\mathfrak{A}\ Integer$
where $OclSize\ x = (\lambda\ \tau.\ if\ (\delta\ x)\ \tau = true\ \tau \wedge finite(\lceil\lceil Rep\text{-}Set\text{-}0\ (x\ \tau)\rceil\rceil)$
$then\ \lfloor\lfloor\ int(card\ \lceil\lceil Rep\text{-}Set\text{-}0\ (x\ \tau)\rceil\rceil)\ \rfloor\rfloor$
$else\ \perp\ )$
notation
$OclSize$ $(\text{-->}size'('))$

The following definition follows the requirement of the standard to treat null as neutral element of sets. It is a well-documented exception from the general strictness rule and the rule that the distinguished argument self should be non-null.

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

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

definition $OclANY :: [('\mathfrak{A},'\alpha::null)\ Set] \Rightarrow ('\mathfrak{A},'\alpha)\ val$
where $OclANY\ x = (\lambda\ \tau.\ if\ (\upsilon\ x)\ \tau = true\ \tau$
$then\ if\ (\delta\ x\ and\ OclNotEmpty\ x)\ \tau = true\ \tau$
$then\ SOME\ y.\ y \in \lceil\lceil Rep\text{-}Set\text{-}0\ (x\ \tau)\rceil\rceil$
$else\ null\ \tau$
$else\ \perp\ )$
notation $OclANY$ $(\text{-->}any'('))$

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

definition $OclForall :: [('\mathfrak{A},'\alpha::null)Set,('\mathfrak{A},'\alpha)val \Rightarrow ('\mathfrak{A})Boolean] \Rightarrow '\mathfrak{A}\ Boolean$
where $OclForall\ S\ P = (\lambda\ \tau.\ if\ (\delta\ S)\ \tau = true\ \tau$
$then\ if\ (\exists\, x \in \lceil\lceil Rep\text{-}Set\text{-}0\ (S\ \tau)\rceil\rceil.\ P(\lambda\ \text{-}.\ x)\ \tau = false\ \tau)$
$then\ false\ \tau$
$else\ if\ (\exists\, x \in \lceil\lceil Rep\text{-}Set\text{-}0\ (S\ \tau)\rceil\rceil.\ P(\lambda\ \text{-}.\ x)\ \tau = \perp\ \tau)$
$then\ \perp\ \tau$
$else\ if\ (\exists\, x \in \lceil\lceil Rep\text{-}Set\text{-}0\ (S\ \tau)\rceil\rceil.\ P(\lambda\ \text{-}.\ x)\ \tau = null\ \tau)$
$then\ null\ \tau$
$else\ true\ \tau$
$else\ \perp)$
syntax
$\text{-}OclForall :: [('\mathfrak{A},'\alpha::null)\ Set,id,('\mathfrak{A})Boolean] \Rightarrow '\mathfrak{A}\ Boolean$ $((\text{-})\text{-->}forAll'(\text{-}|\text{-}'))$
translations
$X\text{-->}forAll(x \mid P) == CONST\ OclForall\ X\ (\%x.\ P)$

Like OclForall, OclExists is also not strict.

definition *OclExists* $:: [('\mathfrak{A},'\alpha{::}null)\ Set,('\mathfrak{A},'\alpha)val \Rightarrow ('\mathfrak{A})Boolean] \Rightarrow {'\mathfrak{A}}\ Boolean$
where $OclExists\ S\ P = not(OclForall\ S\ (\lambda\ X.\ not\ (P\ X)))$

syntax
$\text{-}OclExist :: [('\mathfrak{A},'\alpha{::}null)\ Set,id,('\mathfrak{A})Boolean] \Rightarrow {'\mathfrak{A}}\ Boolean \quad ((\text{-}){-}{>}exists'(\text{-}|\text{-}'))$
translations
$X{-}{>}exists(x \mid P) == CONST\ OclExists\ X\ (\%x.\ P)$

definition *OclIterate* $:: [('\mathfrak{A},'\alpha{::}null)\ Set,('\mathfrak{A},'\beta{::}null)val,$
$('\mathfrak{A},'\alpha)val \Rightarrow ('\mathfrak{A},'\beta)val \Rightarrow ('\mathfrak{A},'\beta)val] \Rightarrow ('\mathfrak{A},'\beta)val$
where $OclIterate\ S\ A\ F = (\lambda\ \tau.\ if\ (\delta\ S)\ \tau = true\ \tau \wedge (\upsilon\ A)\ \tau = true\ \tau \wedge finite\lceil\lceil Rep\text{-}Set\text{-}0\ (S\ \tau)\rceil\rceil$
$then\ (Finite\text{-}Set.fold\ (F)\ (A)\ ((\lambda a\ \tau.\ a)\ `\ \lceil\lceil Rep\text{-}Set\text{-}0\ (S\ \tau)\rceil\rceil))\tau$
$else\ \bot)$
syntax
$\text{-}OclIterate :: [('\mathfrak{A},'\alpha{::}null)\ Set,\ idt,\ idt,\ '\alpha,\ '\beta] => ('\mathfrak{A},'\gamma)val$
$(\text{-}\ {-}{>}iterate'(\text{-};\text{-}{=}\text{-}\mid\text{-}')\ )$
translations
$X{-}{>}iterate(a;\ x = A \mid P) == CONST\ OclIterate\ X\ A\ (\%a.\ (\%\ x.\ P))$

definition *OclSelect* $:: [('\mathfrak{A},'\alpha{::}null)Set,('\mathfrak{A},'\alpha)val \Rightarrow ('\mathfrak{A})Boolean] \Rightarrow ('\mathfrak{A},'\alpha)Set$
where $OclSelect\ S\ P = (\lambda\tau.\ if\ (\delta\ S)\ \tau = true\ \tau$
$then\ if\ (\exists\, x \in \lceil\lceil Rep\text{-}Set\text{-}0\ (S\ \tau)\rceil\rceil.\ P(\lambda\ \text{-}.\ x)\ \tau = \bot\ \tau)$
$then\ \bot$
$else\ Abs\text{-}Set\text{-}0\ \lfloor\lfloor\{x \in \lceil\lceil\ Rep\text{-}Set\text{-}0\ (S\ \tau)\rceil\rceil.\ P\ (\lambda\text{-}.\ x)\ \tau \neq false\ \tau\}\rfloor\rfloor$
$else\ \bot)$
syntax
$\text{-}OclSelect :: [('\mathfrak{A},'\alpha{::}null)\ Set,id,('\mathfrak{A})Boolean] \Rightarrow {'\mathfrak{A}}\ Boolean \quad ((\text{-}){-}{>}select'(\text{-}|\text{-}'))$
translations
$X{-}{>}select(x \mid P) == CONST\ OclSelect\ X\ (\%\ x.\ P)$

definition *OclReject* $:: [('\mathfrak{A},'\alpha{::}null)Set,('\mathfrak{A},'\alpha)val \Rightarrow ('\mathfrak{A})Boolean] \Rightarrow ('\mathfrak{A},'\alpha{::}null)Set$
where $OclReject\ S\ P = OclSelect\ S\ (not\ o\ P)$
syntax
$\text{-}OclReject :: [('\mathfrak{A},'\alpha{::}null)\ Set,id,('\mathfrak{A})Boolean] \Rightarrow {'\mathfrak{A}}\ Boolean \quad ((\text{-}){-}{>}reject'(\text{-}|\text{-}'))$
translations
$X{-}{>}reject(x \mid P) == CONST\ OclReject\ X\ (\%\ x.\ P)$

Definition (futur operators)

consts
$OclCount :: [('\mathfrak{A},'\alpha{::}null)\ Set,('\mathfrak{A},'\alpha)\ Set] \Rightarrow {'\mathfrak{A}}\ Integer$
$OclSum :: ('\mathfrak{A},'\alpha{::}null)\ Set \Rightarrow {'\mathfrak{A}}\ Integer$
$OclIncludesAll :: [('\mathfrak{A},'\alpha{::}null)\ Set,('\mathfrak{A},'\alpha)\ Set] \Rightarrow {'\mathfrak{A}}\ Boolean$
$OclExcludesAll :: [('\mathfrak{A},'\alpha{::}null)\ Set,('\mathfrak{A},'\alpha)\ Set] \Rightarrow {'\mathfrak{A}}\ Boolean$
$OclComplement :: ('\mathfrak{A},'\alpha{::}null)\ Set \Rightarrow ('\mathfrak{A},'\alpha)\ Set$
$OclUnion :: [('\mathfrak{A},'\alpha{::}null)\ Set,('\mathfrak{A},'\alpha)\ Set] \Rightarrow ('\mathfrak{A},'\alpha)\ Set$
$OclIntersection :: [('\mathfrak{A},'\alpha{::}null)\ Set,('\mathfrak{A},'\alpha)\ Set] \Rightarrow ('\mathfrak{A},'\alpha)\ Set$

notation
OclCount $(\text{-->}count'(\text{-}'))$
notation
OclSum $(\text{-->}sum'('))$
notation
OclIncludesAll $(\text{-->}includesAll'(\text{-}'))$
notation
OclExcludesAll $(\text{-->}excludesAll'(\text{-}'))$
notation
OclComplement $(\text{-->}complement'('))$
notation
OclUnion $(\text{-->}union'(\text{-}'))$
notation
OclIntersection $(\text{-->}intersection'(\text{-}'))$

4.4.2. Validity and Definedness Properties

OclIncluding

lemma *OclIncluding-defined-args-valid*:
$(\tau \models \delta(X\text{->}including(x))) = ((\tau \models(\delta\ X)) \wedge (\tau \models(\upsilon\ x)))$
⟨*proof*⟩

lemma *OclIncluding-valid-args-valid*:
$(\tau \models \upsilon(X\text{->}including(x))) = ((\tau \models(\delta\ X)) \wedge (\tau \models(\upsilon\ x)))$
⟨*proof*⟩

lemma *OclIncluding-defined-args-valid'*[*simp*,*code-unfold*]:
$\delta(X\text{->}including(x)) = ((\delta\ X)\ and\ (\upsilon\ x))$
⟨*proof*⟩

lemma *OclIncluding-valid-args-valid''*[*simp*,*code-unfold*]:
$\upsilon(X\text{->}including(x)) = ((\delta\ X)\ and\ (\upsilon\ x))$
⟨*proof*⟩

OclExcluding

lemma *OclExcluding-defined-args-valid*:
$(\tau \models \delta(X\text{->}excluding(x))) = ((\tau \models(\delta\ X)) \wedge (\tau \models(\upsilon\ x)))$
⟨*proof*⟩

lemma *OclExcluding-valid-args-valid*:
$(\tau \models \upsilon(X\text{->}excluding(x))) = ((\tau \models(\delta\ X)) \wedge (\tau \models(\upsilon\ x)))$
⟨*proof*⟩

lemma *OclExcluding-valid-args-valid'*[*simp*,*code-unfold*]:

$\delta(X{-}{>}excluding(x)) = ((\delta\ X)\ and\ (\upsilon\ x))$
$\langle proof \rangle$

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

OclIncludes

lemma *OclIncludes-defined-args-valid*:
$(\tau \models \delta(X{-}{>}includes(x))) = ((\tau \models(\delta\ X)) \land (\tau \models(\upsilon\ x)))$
$\langle proof \rangle$

lemma *OclIncludes-valid-args-valid*:
$(\tau \models \upsilon(X{-}{>}includes(x))) = ((\tau \models(\delta\ X)) \land (\tau \models(\upsilon\ x)))$
$\langle proof \rangle$

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

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

OclExcludes

lemma *OclExcludes-defined-args-valid*:
$(\tau \models \delta(X{-}{>}excludes(x))) = ((\tau \models(\delta\ X)) \land (\tau \models(\upsilon\ x)))$
$\langle proof \rangle$

lemma *OclExcludes-valid-args-valid*:
$(\tau \models \upsilon(X{-}{>}excludes(x))) = ((\tau \models(\delta\ X)) \land (\tau \models(\upsilon\ x)))$
$\langle proof \rangle$

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

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

OclSize

lemma *OclSize-defined-args-valid*: $\tau \models \delta\ (X{-}{>}size()) \Longrightarrow \tau \models \delta\ X$
$\langle proof \rangle$

lemma *OclSize-infinite*:

assumes *non-finite*:$\tau \models not(\delta(S{-}{>}size()))$
shows $(\tau \models not(\delta(S))) \lor \neg$ *finite* $\lceil\lceil Rep\text{-}Set\text{-}0\ (S\ \tau)\rceil\rceil$
⟨*proof*⟩

lemma $\tau \models \delta\ X \Longrightarrow \neg$ *finite* $\lceil\lceil Rep\text{-}Set\text{-}0\ (X\ \tau)\rceil\rceil \Longrightarrow \neg\ \tau \models \delta\ (X{-}{>}size())$
⟨*proof*⟩

lemma *size-defined*:
assumes *X-finite*: $\bigwedge\tau.$ *finite* $\lceil\lceil Rep\text{-}Set\text{-}0\ (X\ \tau)\rceil\rceil$
shows $\delta\ (X{-}{>}size()) = \delta\ X$
⟨*proof*⟩

lemma *size-defined′*:
assumes *X-finite*: *finite* $\lceil\lceil Rep\text{-}Set\text{-}0\ (X\ \tau)\rceil\rceil$
shows $(\tau \models \delta\ (X{-}{>}size())) = (\tau \models \delta\ X)$
⟨*proof*⟩

OclIsEmpty

lemma *OclIsEmpty-defined-args-valid*:$\tau \models \delta\ (X{-}{>}isEmpty()) \Longrightarrow \tau \models \upsilon\ X$
⟨*proof*⟩

lemma $\tau \models \delta\ (null{-}{>}isEmpty())$
⟨*proof*⟩

lemma *OclIsEmpty-infinite*: $\tau \models \delta\ X \Longrightarrow \neg$ *finite* $\lceil\lceil Rep\text{-}Set\text{-}0\ (X\ \tau)\rceil\rceil \Longrightarrow \neg\ \tau \models \delta\ (X{-}{>}isEmpty())$
⟨*proof*⟩

OclNotEmpty

lemma *OclNotEmpty-defined-args-valid*:$\tau \models \delta\ (X{-}{>}notEmpty()) \Longrightarrow \tau \models \upsilon\ X$
⟨*proof*⟩

lemma $\tau \models \delta\ (null{-}{>}notEmpty())$
⟨*proof*⟩

lemma *OclNotEmpty-infinite*: $\tau \models \delta\ X \Longrightarrow \neg$ *finite* $\lceil\lceil Rep\text{-}Set\text{-}0\ (X\ \tau)\rceil\rceil \Longrightarrow \neg\ \tau \models \delta\ (X{-}{>}notEmpty())$
⟨*proof*⟩

lemma *OclNotEmpty-has-elt* : $\tau \models \delta\ X \Longrightarrow$
$\tau \models X{-}{>}notEmpty() \Longrightarrow$
$\exists\, e.\ e \in \lceil\lceil Rep\text{-}Set\text{-}0\ (X\ \tau)\rceil\rceil$
⟨*proof*⟩

OclANY

lemma *OclANY-defined-args-valid*: $\tau \models \delta\ (X{-}{>}any()) \Longrightarrow \tau \models \delta\ X$
⟨*proof*⟩

lemma $\tau \models \delta\ X \Longrightarrow \tau \models X{-}{>}isEmpty() \Longrightarrow \neg\ \tau \models \delta\ (X{-}{>}any())$
$\langle proof \rangle$

lemma *OclANY-valid-args-valid*:
$(\tau \models \upsilon(X{-}{>}any())) = (\tau \models \upsilon\ X)$
$\langle proof \rangle$

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

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

OclIncluding

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

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

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

OclExcluding

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

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

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

OclIncludes

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

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

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

OclExcludes

lemma *OclExcludes-invalid[simp,code-unfold]*:$(invalid{-}{>}excludes(x)) = invalid$

⟨*proof*⟩

lemma *OclExcludes-invalid-args*[*simp*,*code-unfold*]:$(X{-}{>}excludes(invalid)) = invalid$
⟨*proof*⟩

lemma *OclExcludes-null*[*simp*,*code-unfold*]:$(null{-}{>}excludes(x)) = invalid$
⟨*proof*⟩

OclSize

lemma *OclSize-invalid*[*simp*,*code-unfold*]:$(invalid{-}{>}size()) = invalid$
⟨*proof*⟩

lemma *OclSize-null*[*simp*,*code-unfold*]:$(null{-}{>}size()) = invalid$
⟨*proof*⟩

OclIsEmpty

lemma *OclIsEmpty-invalid*[*simp*,*code-unfold*]:$(invalid{-}{>}isEmpty()) = invalid$
⟨*proof*⟩

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

OclNotEmpty

lemma *OclNotEmpty-invalid*[*simp*,*code-unfold*]:$(invalid{-}{>}notEmpty()) = invalid$
⟨*proof*⟩

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

OclANY

lemma *OclANY-invalid*[*simp*,*code-unfold*]:$(invalid{-}{>}any()) = invalid$
⟨*proof*⟩

lemma *OclANY-null*[*simp*,*code-unfold*]:$(null{-}{>}any()) = null$
⟨*proof*⟩

OclForall

lemma *OclForall-invalid*[*simp*,*code-unfold*]:$invalid{-}{>}forAll(a|\ P\ a) = invalid$
⟨*proof*⟩

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

OclExists

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

⟨*proof*⟩

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

OclIterate

lemma $OclIterate\text{-}invalid[simp,code\text{-}unfold]{:}invalid{-}{>}iterate(a;\ x = A \mid P\ a\ x) = invalid$
⟨*proof*⟩

lemma $OclIterate\text{-}null[simp,code\text{-}unfold]{:}null{-}{>}iterate(a;\ x = A \mid P\ a\ x) = invalid$
⟨*proof*⟩

lemma $OclIterate\text{-}invalid\text{-}args[simp,code\text{-}unfold]{:}S{-}{>}iterate(a;\ x = invalid \mid P\ a\ x) = invalid$
⟨*proof*⟩

An open question is this ...

lemma $S{-}{>}iterate(a;\ x = null \mid P\ a\ x) = invalid$
⟨*proof*⟩

lemma $OclIterate\text{-}infinite$:
assumes $non\text{-}finite$: $\tau \models not(\delta(S{-}{>}size()))$
shows $(OclIterate\ S\ A\ F)\ \tau = invalid\ \tau$
⟨*proof*⟩

OclSelect

lemma $OclSelect\text{-}invalid[simp,code\text{-}unfold]{:}invalid{-}{>}select(a \mid P\ a) = invalid$
⟨*proof*⟩

lemma $OclSelect\text{-}null[simp,code\text{-}unfold]{:}null{-}{>}select(a \mid P\ a) = invalid$
⟨*proof*⟩

OclReject

lemma $OclReject\text{-}invalid[simp,code\text{-}unfold]{:}invalid{-}{>}reject(a \mid P\ a) = invalid$
⟨*proof*⟩

lemma $OclReject\text{-}null[simp,code\text{-}unfold]{:}null{-}{>}reject(a \mid P\ a) = invalid$
⟨*proof*⟩

4.4.4. Context Passing

lemma $cp\text{-}OclIncluding$:
$(X{-}{>}including(x))\ \tau = ((\lambda\ \text{-}.\ X\ \tau){-}{>}including(\lambda\ \text{-}.\ x\ \tau))\ \tau$
⟨*proof*⟩

lemma $cp\text{-}OclExcluding$:

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

lemma *cp-OclIncludes*:
$(X{-}{>}includes(x))\ \tau = ((\lambda\ \text{-}.\ X\ \tau){-}{>}includes(\lambda\ \text{-}.\ x\ \tau))\ \tau$
$\langle proof \rangle$

lemma *cp-OclIncludes1*:
$(X{-}{>}includes(x))\ \tau = (X{-}{>}includes(\lambda\ \text{-}.\ x\ \tau))\ \tau$
$\langle proof \rangle$

lemma *cp-OclExcludes*:
$(X{-}{>}excludes(x))\ \tau = ((\lambda\ \text{-}.\ X\ \tau){-}{>}excludes(\lambda\ \text{-}.\ x\ \tau))\ \tau$
$\langle proof \rangle$

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

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

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

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

lemma *cp-OclForall*:
$(S{-}{>}forAll(x \mid P\ x))\ \tau = ((\lambda\ \text{-}.\ S\ \tau){-}{>}forAll(x \mid P\ (\lambda\ \text{-}.\ x\ \tau)))\ \tau$
$\langle proof \rangle$

lemma *cp-OclForall1* [*simp*,*intro*!]:
$cp\ S \Longrightarrow cp\ (\lambda X.\ ((S\ X){-}{>}forAll(x \mid P\ x)))$
$\langle proof \rangle$

lemma
$cp\ (\lambda X\ St\ x.\ P\ (\lambda\tau.\ x)\ X\ St) \Longrightarrow cp\ S \Longrightarrow cp\ (\lambda X.\ (S\ X){-}{>}forAll(x|P\ x\ X))$
$\langle proof \rangle$

lemma
$cp\ S \Longrightarrow$
$(\bigwedge x.\ cp(P\ x)) \Longrightarrow$
$cp(\lambda X.\ ((S\ X){-}{>}forAll(x \mid P\ x\ X)))$
$\langle proof \rangle$

lemma *cp-OclExists*:

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

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

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

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

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

lemmas *cp-intro''*[*intro*!,*simp*,*code-unfold*] =
cp-intro'
cp-OclIncluding [*THEN allI*[*THEN allI*[*THEN allI*[*THEN cpI2*]], *of OclIncluding*]]
cp-OclExcluding [*THEN allI*[*THEN allI*[*THEN allI*[*THEN cpI2*]], *of OclExcluding*]]
cp-OclIncludes [*THEN allI*[*THEN allI*[*THEN allI*[*THEN cpI2*]], *of OclIncludes*]]
cp-OclExcludes [*THEN allI*[*THEN allI*[*THEN allI*[*THEN cpI2*]], *of OclExcludes*]]
cp-OclSize [*THEN allI*[*THEN allI*[*THEN cpI1*], *of OclSize*]]
cp-OclIsEmpty [*THEN allI*[*THEN allI*[*THEN cpI1*], *of OclIsEmpty*]]
cp-OclNotEmpty [*THEN allI*[*THEN allI*[*THEN cpI1*], *of OclNotEmpty*]]
cp-OclANY [*THEN allI*[*THEN allI*[*THEN cpI1*], *of OclANY*]]

4.4.5. Const

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

4.5. Fundamental Predicates on Set: Strict Equality

4.5.1. Definition

After the part of foundational operations on sets, we detail here equality on sets. Strong equality is inherited from the OCL core, but we have to consider the case of the strict equality. We decide to overload strict equality in the same way we do for other value's in OCL:

defs $StrictRefEq_{Set}$:

$$
\begin{aligned}
(x::('\mathfrak{A},'\alpha::null)Set) \doteq y \equiv \lambda\ \tau.\ & if\ (\upsilon\ x)\ \tau = true\ \tau \wedge (\upsilon\ y)\ \tau = true\ \tau \\
& then\ (x \triangleq y)\tau \\
& else\ invalid\ \tau
\end{aligned}
$$

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 $StrictRefEq_{Set}$-*refl*[*simp*,*code-unfold*]:
$((x::('\mathfrak{A},'\alpha::null)Set) \doteq x) = (if\ (\upsilon\ x)\ then\ true\ else\ invalid\ endif)$
⟨*proof*⟩

Symmetry

lemma $StrictRefEq_{Set}$-*sym*:
$((x::('\mathfrak{A},'\alpha::null)Set) \doteq y) = (y \doteq x)$
⟨*proof*⟩

Execution with Invalid or Null as Argument

lemma $StrictRefEq_{Set}$-*strict1*[*simp*,*code-unfold*]: $((x::('\mathfrak{A},'\alpha::null)Set) \doteq invalid)= invalid$
⟨*proof*⟩

lemma $StrictRefEq_{Set}$-*strict2*[*simp*,*code-unfold*]: $(invalid \doteq (y::('\mathfrak{A},'\alpha::null)Set))= invalid$
⟨*proof*⟩

lemma $StrictRefEq_{Set}$-*strictEq-valid-args-valid*:
$(\tau \models \delta\ ((x::('\mathfrak{A},'\alpha::null)Set) \doteq y)) = ((\tau \models (\upsilon\ x)) \wedge (\tau \models \upsilon\ y))$
⟨*proof*⟩

Behavior vs StrongEq

lemma $StrictRefEq_{Set}$-*vs-StrongEq*:
$\tau \models \upsilon\ x \Longrightarrow \tau \models \upsilon\ y \Longrightarrow (\tau \models (((x::('\mathfrak{A},'\alpha::null)Set) \doteq y) \triangleq (x \triangleq y)))$
⟨*proof*⟩

Context Passing

lemma *cp*-$StrictRefEq_{Set}$:$((X::('\mathfrak{A},'\alpha::null)Set) \doteq Y)\ \tau = ((\lambda\text{-}.\ X\ \tau) \doteq (\lambda\text{-}.\ Y\ \tau))\ \tau$
⟨*proof*⟩

Const

lemma *const-StrictRefEq*$_{Set}$:
assumes $const\ (X :: (\text{-},\text{-}::null)\ Set)$
assumes $const\ X'$
shows $const\ (X \doteq X')$
⟨*proof*⟩

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

4.6.1. OclIncluding

lemma *OclIncluding-finite-rep-set* :
assumes $X\text{-}def : \tau \models \delta\ X$
and $x\text{-}val : \tau \models \upsilon\ x$
shows $finite\ \lceil\lceil Rep\text{-}Set\text{-}0\ \ (X{-}{>}including(x)\ \tau)\rceil\rceil = finite\ \lceil\lceil Rep\text{-}Set\text{-}0\ \ (X\ \tau)\rceil\rceil$
⟨*proof*⟩

lemma *OclIncluding-rep-set*:
assumes $S\text{-}def: \tau \models \delta\ S$
shows $\lceil\lceil Rep\text{-}Set\text{-}0\ \ (S{-}{>}including(\lambda\text{-}.\ \lfloor\lfloor x\rfloor\rfloor)\ \tau)\rceil\rceil = insert\ \lfloor\lfloor x\rfloor\rfloor\ \lceil\lceil Rep\text{-}Set\text{-}0\ \ (S\ \tau)\rceil\rceil$
⟨*proof*⟩

lemma *OclIncluding-notempty-rep-set*:
assumes $X\text{-}def: \tau \models \delta\ X$
and $a\text{-}val: \tau \models \upsilon\ a$
shows $\lceil\lceil Rep\text{-}Set\text{-}0\ \ (X{-}{>}including(a)\ \tau)\rceil\rceil \neq \{\}$
⟨*proof*⟩

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

4.6.2. OclExcluding

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

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

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

and $\quad$ *val-x*: $\tau \models (\upsilon\ x)$
and $\quad$ *val-y*: $\tau \models (\upsilon\ y)$
and $\quad$ *neq* : $\tau \models not(x \triangleq y)$
shows $\quad \tau \models ((X{-}{>}including(x)){-}{>}excluding(y)) \triangleq ((X{-}{>}excluding(y)){-}{>}including(x))$
⟨*proof*⟩

lemma *OclExcluding-charn2*:
assumes *def-X*: $\tau \models (\delta\ X)$
and $\quad$ *val-x*: $\tau \models (\upsilon\ x)$
shows $\quad \tau \models (((X{-}{>}including(x)){-}{>}excluding(x)) \triangleq (X{-}{>}excluding(x)))$
⟨*proof*⟩

One would like a generic theorem of the form:

```
lemma OclExcluding_charn_exec:
       "(X−>including(x::('𝔄,'a::null)val)−>excluding(y)) =
        (if  δ X then if x ≐y
                      then X−>excluding(y)
                       else  X−>excluding(y)−>including(x)
                      endif
                 else  invalid  endif)"
```

Unfortunately, this does not hold in general, since referential equality is an overloaded concept and has to be defined for each type individually. Consequently, it is only valid for concrete type instances for Boolean, Integer, and Sets thereof...

The computational law *OclExcluding-charn-exec* becomes generic since it uses strict equality which in itself is generic. It is possible to prove the following generic theorem and instantiate it later (using properties that link the polymorphic logical strong equality with the concrete instance of strict quality).

lemma *OclExcluding-charn-exec*:
assumes *strict1*: $(x \doteq invalid) = invalid$
and $\quad$ *strict2*: $(invalid \doteq y) = invalid$
and $\quad$ *StrictRefEq-valid-args-valid*: $\bigwedge (x{::}('\mathfrak{A},'a{::}null)val)\ y\ \tau.$
$\quad (\tau \models \delta\ (x \doteq y)) = ((\tau \models (\upsilon\ x)) \wedge (\tau \models \upsilon\ y))$
and $\quad$ *cp-StrictRefEq*: $\bigwedge (X{::}('\mathfrak{A},'a{::}null)val)\ Y\ \tau.\ (X \doteq Y)\ \tau = ((\lambda\text{-}.\ X\ \tau) \doteq (\lambda\text{-}.\ Y\ \tau))\ \tau$
and $\quad$ *StrictRefEq-vs-StrongEq*: $\bigwedge (x{::}('\mathfrak{A},'a{::}null)val)\ y\ \tau.$
$\quad \tau \models \upsilon\ x \Longrightarrow \tau \models \upsilon\ y \Longrightarrow (\tau \models ((x \doteq y) \triangleq (x \triangleq y)))$
shows $(X{-}{>}including(x{::}('\mathfrak{A},'a{::}null)val){-}{>}excluding(y)) =$
$\quad (if\ \ \delta\ X\ then\ if\ x \doteq y$
$\quad\quad then\ X{-}{>}excluding(y)$
$\quad\quad else\ X{-}{>}excluding(y){-}{>}including(x)$
$\quad\quad endif$
$\quad else\ invalid\ endif)$
⟨*proof*⟩

schematic-lemma *OclExcluding-charn-exec*$_{Integer}$[*simp*,*code-unfold*]: *?X*
⟨*proof*⟩

schematic-lemma *OclExcluding-charn-exec*$_{Boolean}$[*simp*,*code-unfold*]: *?X*
⟨*proof*⟩

schematic-lemma *OclExcluding-charn-exec*$_{Set}$[*simp*,*code-unfold*]: *?X*
⟨*proof*⟩

lemma *OclExcluding-finite-rep-set* :
assumes *X-def* : $\tau \models \delta\ X$
and *x-val* : $\tau \models \upsilon\ x$
shows $finite\ \lceil\lceil Rep\text{-}Set\text{-}0\ \ (X{-}{>}excluding(x)\ \tau)\rceil\rceil = finite\ \lceil\lceil Rep\text{-}Set\text{-}0\ \ (X\ \tau)\rceil\rceil$
⟨*proof*⟩

lemma *OclExcluding-rep-set*:
assumes *S-def*: $\tau \models \delta\ S$
shows $\lceil\lceil Rep\text{-}Set\text{-}0\ \ (S{-}{>}excluding(\lambda\text{-}.\ \lfloor\lfloor x\rfloor\rfloor)\ \tau)\rceil\rceil = \lceil\lceil Rep\text{-}Set\text{-}0\ \ (S\ \tau)\rceil\rceil - \{\lfloor\lfloor x\rfloor\rfloor\}$
⟨*proof*⟩

4.6.3. OclIncludes

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

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

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

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

Here is again a generic theorem similar as above.

lemma *OclIncludes-execute-generic*:

assumes *strict1*: $(x \doteq invalid) = invalid$
and *strict2*: $(invalid \doteq y) = invalid$
and *cp-StrictRefEq*: $\bigwedge (X::('\mathfrak{A},'a::null)val)\ Y\ \tau.\ (X \doteq Y)\ \tau = ((\lambda\text{-}.\ X\ \tau) \doteq (\lambda\text{-}.\ Y\ \tau))\ \tau$
and *StrictRefEq-vs-StrongEq*: $\bigwedge (x::('\mathfrak{A},'a::null)val)\ y\ \tau.$
$\tau \models \upsilon\ x \Longrightarrow \tau \models \upsilon\ y \Longrightarrow (\tau \models ((x \doteq y) \triangleq (x \triangleq y)))$
shows
$(X{-}{>}including(x::('\mathfrak{A},'a::null)val){-}{>}includes(y)) =$
$(if\ \delta\ X\ then\ if\ x \doteq y\ then\ true\ else\ X{-}{>}includes(y)\ endif\ else\ invalid\ endif)$
⟨*proof*⟩

schematic-lemma *OclIncludes-execute*$_{Integer}$[*simp*,*code-unfold*]: *?X*
⟨*proof*⟩

schematic-lemma *OclIncludes-execute*$_{Boolean}$[*simp*,*code-unfold*]: *?X*
⟨*proof*⟩

schematic-lemma *OclIncludes-execute*$_{Set}$[*simp*,*code-unfold*]: *?X*
⟨*proof*⟩

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

lemmas *OclIncludes-including*$_{Integer}$ =
OclIncludes-including-generic[*OF OclIncludes-execute*$_{Integer}$ *StrictRefEq*$_{Integer}$*-strict''*]

4.6.4. OclExcludes

4.6.5. OclSize

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

lemma *OclSize-including-exec*[*simp*,*code-unfold*]:
$((X\ {-}{>}including(x))\ {-}{>}size()) = (if\ \delta\ X\ and\ \upsilon\ x\ then$
$X\ {-}{>}size()\ \text{‘}{+}\ if\ X\ {-}{>}includes(x)\ then\ \mathbf{0}\ else\ \mathbf{1}\ endif$
$else$
$invalid$
$endif)$

⟨*proof*⟩

4.6.6. OclIsEmpty

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

lemma *OclIsEmpty-including* [*simp*]:
assumes *X-def*: $\tau \models \delta\ X$
  and *X-finite*: $finite\ \lceil\lceil Rep\text{-}Set\text{-}0\ (X\ \tau)\rceil\rceil$
  and *a-val*: $\tau \models \upsilon\ a$
shows $X{-}{>}including(a){-}{>}isEmpty()\ \tau = false\ \tau$
⟨*proof*⟩

4.6.7. OclNotEmpty

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

lemma *OclNotEmpty-including* [*simp*,*code-unfold*]:
assumes *X-def*: $\tau \models \delta\ X$
  and *X-finite*: $finite\ \lceil\lceil Rep\text{-}Set\text{-}0\ (X\ \tau)\rceil\rceil$
  and *a-val*: $\tau \models \upsilon\ a$
shows $X{-}{>}including(a){-}{>}notEmpty()\ \tau = true\ \tau$
⟨*proof*⟩

4.6.8. OclANY

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

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

4.6.9. OclForall

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

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

4.6.10. OclExists

lemma *OclExists-mtSet-exec*[*simp*,*code-unfold*] :
$((Set\{\})\text{−>}exists(z \mid P(z))) = false$
⟨*proof*⟩

lemma *OclExists-including-exec*[*simp*,*code-unfold*] :
assumes *cp*: *cp P*
shows $((S\text{−>}including(x))\text{−>}exists(z \mid P(z))) = (if\ \delta\ S\ and\ \upsilon\ x$
$then\ P\ x\ or\ (S\text{−>}exists(z \mid P(z)))$
$else\ invalid$
$endif)$
⟨*proof*⟩

4.6.11. OclIterate

lemma *OclIterate-empty*[*simp*,*code-unfold*]: $((Set\{\})\text{−>}iterate(a;\ x = A \mid P\ a\ x)) = A$
⟨*proof*⟩

In particular, this does hold for A = null.

lemma *OclIterate-including*:
assumes *S-finite*: $\tau \models \delta(S\text{−>}size())$
and *F-valid-arg*: $(\upsilon\ A)\ \tau = (\upsilon\ (F\ a\ A))\ \tau$
and *F-commute*: *comp-fun-commute F*
and *F-cp*: $\bigwedge x\ y\ \tau.\ F\ x\ y\ \tau = F\ (\lambda\ \text{-}.\ x\ \tau)\ y\ \tau$
shows $((S\text{−>}including(a))\text{−>}iterate(a;\ x = A \mid F\ a\ x))\ \tau =$
$((S\text{−>}excluding(a))\text{−>}iterate(a;\ x = F\ a\ A \mid F\ a\ x))\ \tau$
⟨*proof*⟩

4.6.12. OclSelect

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

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

lemma *OclSelect-including-exec*[*simp*,*code-unfold*]:
assumes *P-cp* : *cp P*
shows $OclSelect\ (X\text{−>}including(y))\ P = OclSelect\text{-}body\ P\ y\ (OclSelect\ (X\text{−>}excluding(y))\ P)$
(**is** - = *?select*)
⟨*proof*⟩

4.6.13. OclReject

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

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

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

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

4.7.1. OclIncludes

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

4.7.2. OclSize

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

lemma [*simp*,*code-unfold*]: $\delta\ ((X\ {-}{>}including(x))\ {-}{>}size()) = (\delta(X{-}{>}size())\ and\ \upsilon(x))$
⟨*proof*⟩

lemma [*simp*,*code-unfold*]: $\delta\ ((X\ {-}{>}excluding(x))\ {-}{>}size()) = (\delta(X{-}{>}size())\ and\ \upsilon(x))$
⟨*proof*⟩

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

4.7.3. OclForall

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

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

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

$\langle proof \rangle$

lemma *OclForall-not-includes* :
assumes *x-def* : $\tau \models \delta\ x$
and *y-def* : $\tau \models \delta\ y$
shows $(OclForall\ x\ (OclIncludes\ y)\ \tau = false\ \tau) = (\neg \lceil\lceil Rep\text{-}Set\text{-}0\ (x\ \tau)\rceil\rceil \subseteq \lceil\lceil Rep\text{-}Set\text{-}0\ (y\ \tau)\rceil\rceil)$
$\langle proof \rangle$

lemma *OclForall-iterate*:
assumes *S-finite*: $finite\ \lceil\lceil Rep\text{-}Set\text{-}0\ (S\ \tau)\rceil\rceil$
shows $S{-}{>}forAll(x \mid P\ x)\ \tau = (S{-}{>}iterate(x;\ acc = true \mid acc\ and\ P\ x))\ \tau$
$\langle proof \rangle$

lemma *OclForall-cong*:
assumes $\bigwedge x.\ x \in \lceil\lceil Rep\text{-}Set\text{-}0\ (X\ \tau)\rceil\rceil \Longrightarrow \tau \models P\ (\lambda\tau.\ x) \Longrightarrow \tau \models Q\ (\lambda\tau.\ x)$
assumes P: $\tau \models OclForall\ X\ P$
shows $\tau \models OclForall\ X\ Q$
$\langle proof \rangle$

lemma *OclForall-cong'*:
assumes $\bigwedge x.\ x \in \lceil\lceil Rep\text{-}Set\text{-}0\ (X\ \tau)\rceil\rceil \Longrightarrow \tau \models P\ (\lambda\tau.\ x) \Longrightarrow \tau \models Q\ (\lambda\tau.\ x) \Longrightarrow \tau \models R\ (\lambda\tau.\ x)$
assumes P: $\tau \models OclForall\ X\ P$
assumes Q: $\tau \models OclForall\ X\ Q$
shows $\tau \models OclForall\ X\ R$
$\langle proof \rangle$

4.7.4. Strict Equality

lemma *StrictRefEq*$_{Set}$*-defined* :
assumes *x-def*: $\tau \models \delta\ x$
assumes *y-def*: $\tau \models \delta\ y$
shows $((x{::}('\mathfrak{A},'\alpha{::}null)Set) \doteq y)\ \tau =$
$(x{-}{>}forAll(z|\ y{-}{>}includes(z))\ and\ (y{-}{>}forAll(z|\ x{-}{>}includes(z))))\ \tau$
$\langle proof \rangle$

lemma *StrictRefEq*$_{Set}$*-exec*[*simp*,*code-unfold*] :
$((x{::}('\mathfrak{A},'\alpha{::}null)Set) \doteq y) =$
(if $\delta\ x$ *then (if* $\delta\ y$
then $((x{-}{>}forAll(z|\ y{-}{>}includes(z))\ and\ (y{-}{>}forAll(z|\ x{-}{>}includes(z)))))$
else if $\upsilon\ y$
then false $(*\ x'{-}{>}includes = null\ *)$
else invalid
endif
endif)
else if $\upsilon\ x$ $(*\ null = ???\ *)$
then if $\upsilon\ y$ *then not*$(\delta\ y)$ *else invalid endif*
else invalid

$endif$
$endif)$
$\langle proof \rangle$

lemma $StrictRefEq_{Set}$-L-$subst1$: $cp\ P \Longrightarrow \tau \models \upsilon\ x \Longrightarrow \tau \models \upsilon\ y \Longrightarrow \tau \models \upsilon\ P\ x \Longrightarrow \tau \models \upsilon\ P\ y \Longrightarrow$
$\tau \models (x::('\mathfrak{A},'\alpha::null)Set) \doteq y \Longrightarrow \tau \models (P\ x ::('\mathfrak{A},'\alpha::null)Set) \doteq P\ y$
$\langle proof \rangle$

lemma $OclIncluding$-$cong'$:
shows $\tau \models \delta\ s \Longrightarrow \tau \models \delta\ t \Longrightarrow \tau \models \upsilon\ x \Longrightarrow$
$\tau \models ((s::('\mathfrak{A},'a::null)Set) \doteq t) \Longrightarrow \tau \models (s{-}{>}including(x) \doteq (t{-}{>}including(x)))$
$\langle proof \rangle$

lemma $OclIncluding$-$cong$: $\bigwedge(s::('\mathfrak{A},'a::null)Set)\ t\ x\ y\ \tau.\ \tau \models \delta\ t \Longrightarrow \tau \models \upsilon\ y \Longrightarrow$
$\tau \models s \doteq t \Longrightarrow x = y \Longrightarrow \tau \models s{-}{>}including(x) \doteq (t{-}{>}including(y))$
$\langle proof \rangle$

lemma $const$-$StrictRefEq_{Set}$-$including$: $const\ a \Longrightarrow const\ S \Longrightarrow const\ X \Longrightarrow$
$const\ (X \doteq S{-}{>}including(a))$
$\langle proof \rangle$

4.8. Test Statements

lemma $syntax$-$test$: $Set\{\mathbf{2},\mathbf{1}\} = (Set\{\}{-}{>}including(\mathbf{1}){-}{>}including(\mathbf{2}))$
$\langle proof \rangle$

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 *null* for the non-existing Sets) :

lemma $semantic$-$test2$:
assumes $H{:}(Set\{\mathbf{2}\} \doteq null) = (false::('\mathfrak{A})Boolean)$
shows $(\tau::('\mathfrak{A})st) \models (Set\{Set\{\mathbf{2}\},null\}{-}{>}includes(null))$
$\langle proof \rangle$

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

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

Elementary computations on Sets.

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

value $\neg\ (\tau \models \upsilon(invalid::('\mathfrak{A},'\alpha::null)\ Set))$
value $\tau \models \upsilon(null::('\mathfrak{A},'\alpha::null)\ Set)$

value $\neg\ (\tau \models \delta(null::(\mathfrak{A}, '\alpha::null)\ Set))$
value $\quad \tau \models \upsilon(Set\{\})$
value $\quad \tau \models \upsilon(Set\{Set\{\mathbf{2}\},null\})$
value $\quad \tau \models \delta(Set\{Set\{\mathbf{2}\},null\})$
value $\quad \tau \models (Set\{\mathbf{2},\mathbf{1}\}{-}{>}includes(\mathbf{1}))$
value $\neg\ (\tau \models (Set\{\mathbf{2}\}{-}{>}includes(\mathbf{1})))$
value $\neg\ (\tau \models (Set\{\mathbf{2},\mathbf{1}\}{-}{>}includes(null)))$
value $\quad \tau \models (Set\{\mathbf{2},null\}{-}{>}includes(null))$
value $\quad \tau \models (Set\{null,\mathbf{2}\}{-}{>}includes(null))$

value $\quad \tau \models ((Set\{\}){-}{>}forAll(z \mid \mathbf{0}\ `{<}\ z))$

value $\quad \tau \models ((Set\{\mathbf{2},\mathbf{1}\}){-}{>}forAll(z \mid \mathbf{0}\ `{<}\ z))$
value $\neg\ (\tau \models ((Set\{\mathbf{2},\mathbf{1}\}){-}{>}exists(z \mid z\ `{<}\ \mathbf{0}\ )))$
value $\neg\ (\tau \models \delta(Set\{\mathbf{2},null\}){-}{>}forAll(z \mid \mathbf{0}\ `{<}\ z))$
value $\neg\ (\tau \models ((Set\{\mathbf{2},null\}){-}{>}forAll(z \mid \mathbf{0}\ `{<}\ z)))$
value $\quad \tau \models ((Set\{\mathbf{2},null\}){-}{>}exists(z \mid \mathbf{0}\ `{<}\ z))$

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

value $\quad (\tau \models (Set\{\lambda\text{-}.\ \lfloor\lfloor x\rfloor\rfloor\} \doteq Set\{\lambda\text{-}.\ \lfloor\lfloor x\rfloor\rfloor\}))$
value $\quad (\tau \models (Set\{\lambda\text{-}.\ \lfloor x\rfloor\} \doteq Set\{\lambda\text{-}.\ \lfloor x\rfloor\}))$

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

lemma $\quad const\ (Set\{Set\{\mathbf{2},null\},\ invalid\})\ \langle proof\rangle$

end

5. Formalization III: State Operations and Objects

theory *OCL-state*
imports *OCL-lib*
begin

5.1. Introduction: States over Typed Object Universes

In the following, we will refine the concepts of a user-defined data-model (implied by a class-diagram) as well as the notion of state used in the previous section to much more detail. Surprisingly, even without a concrete notion of an objects and a universe of object representation, the generic infrastructure of state-related operations is fairly rich.

5.1.1. Recall: The Generic Structure of States

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

type-synonym *oid* = *nat*

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

This leads to the definitions:

record ('$\mathfrak{A}$)state =
heap :: "oid ⇀ '$\mathfrak{A}$ "
assocs$_2$ :: "oid ⇀ (oid × oid) list "
assocs$_3$ :: "oid ⇀ (oid × oid × oid) list "

type-synonym ('$\mathfrak{A}$)st = "'$\mathfrak{A}$ state × '$\mathfrak{A}$ state"

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

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

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

typ $'\mathfrak{A}$ :: *object*

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

instantiation *option* :: $(object)object$
begin
  definition *oid-of-option-def*: *oid-of* x = *oid-of* (*the* x)
  instance ⟨*proof*⟩
end

5.2. Fundamental Predicates on Object: Strict Equality

Definition

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

definition $StrictRefEq_{Object}$ :: $('\mathfrak{A},'a::\{object,null\})val \Rightarrow ('\mathfrak{A},'a)val \Rightarrow ('\mathfrak{A})Boolean$
where $StrictRefEq_{Object}\ x\ y$

$$\equiv \lambda\ \tau.\ if\ (\upsilon\ x)\ \tau = true\ \tau \land (\upsilon\ y)\ \tau = true\ \tau \\ then\ if\ x\ \tau = null \lor y\ \tau = null \\ then\ \lfloor\lfloor x\ \tau = null \land y\ \tau = null\rfloor\rfloor \\ else\ \lfloor\lfloor(oid\text{-}of\ (x\ \tau)) = (oid\text{-}of\ (y\ \tau))\ \rfloor\rfloor \\ else\ invalid\ \tau$$

5.2.1. Logic and Algebraic Layer on Object

Validity and Definedness Properties

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

lemma $StrictRefEq_{Object}$*-defargs*:
$\tau \models (StrictRefEq_{Object}\ x\ (y::('\mathfrak{A},'a::\{null,object\})val)) \Longrightarrow (\tau \models(\upsilon\ x)) \land (\tau \models(\upsilon\ y))$
⟨*proof*⟩

Symmetry

lemma $StrictRefEq_{Object}$*-sym* :
assumes *x-val* : $\tau \models \upsilon\ x$
shows $\tau \models StrictRefEq_{Object}\ x\ x$
⟨*proof*⟩

Execution with Invalid or Null as Argument

lemma $StrictRefEq_{Object}$*-strict1*[*simp*,*code-unfold*] :
$(StrictRefEq_{Object}\ x\ invalid) = invalid$
⟨*proof*⟩

lemma $StrictRefEq_{Object}$*-strict2*[*simp*,*code-unfold*] :

($StrictRefEq_{Object}$ *invalid* x) = *invalid*
⟨*proof*⟩

Context Passing

lemma *cp-StrictRefEq*$_{Object}$:
($StrictRefEq_{Object}$ x y τ) = ($StrictRefEq_{Object}$ (λ-. x τ) (λ-. y τ)) τ
⟨*proof*⟩

lemmas *cp-intro*''[*intro*!,*simp*,*code-unfold*] =
cp-intro''
cp-StrictRefEq$_{Object}$[*THEN allI*[*THEN allI*[*THEN allI*[*THEN cpI2*]],
of StrictRefEq$_{Object}$]]

Behavior vs StrongEq

It remains to clarify the role of the state invariant $\text{inv}_\sigma(\sigma)$ mentioned above that states the condition that there is a "one-to-one" correspondence between object representations and oid's: $\forall oid \in \text{dom}\,\sigma.\ oid = \text{OidOf}\ \ulcorner\sigma(oid)\urcorner$. 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* :: ('$\mathfrak{A}$::*object*)*st* $\Rightarrow$ *bool*
where *WFF* τ = (($\forall$ x $\in$ *ran*(*heap*(*fst* τ)). ⌈*heap*(*fst* τ) (*oid-of* x)⌉ = x) $\wedge$
($\forall$ x $\in$ *ran*(*heap*(*snd* τ)). ⌈*heap*(*snd* τ) (*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 *StrictRefEq*$_{Object}$*-vs-StrongEq*:
assumes *WFF*: *WFF* τ
and *valid-x*: τ $\models$(υ x)
and *valid-y*: τ $\models$(υ y)
and *x-present-pre*: x τ $\in$ *ran* (*heap*(*fst* τ))

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

shows $(\tau \models (StrictRefEq_{Object}\ x\ y)) = (\tau \models (x \triangleq y))$
⟨*proof*⟩

theorem *StrictRefEq$_{Object}$-vs-StrongEq'*:
assumes *WFF*: *WFF* τ
and *valid-x*: $\tau \models (\upsilon\ (x :: ('\mathfrak{A}::object,'\alpha::\{null,object\})val))$
and *valid-y*: $\tau \models (\upsilon\ y)$
and *oid-preserve*: $\bigwedge x.\ x \in ran\ (heap(fst\ \tau)) \lor x \in ran\ (heap(snd\ \tau)) \Longrightarrow$
$H\ x \neq \bot \Longrightarrow oid\text{-}of\ (H\ x) = oid\text{-}of\ x$
and *xy-together*: $x\ \tau \in H\ `\ ran\ (heap(fst\ \tau)) \land y\ \tau \in H\ `\ ran\ (heap(fst\ \tau)) \lor$
$x\ \tau \in H\ `\ ran\ (heap(snd\ \tau)) \land y\ \tau \in H\ `\ ran\ (heap(snd\ \tau))$

shows $(\tau \models (StrictRefEq_{Object}\ x\ y)) = (\tau \models (x \triangleq y))$
⟨*proof*⟩

So, if two object descriptions live in the same state (both pre or post), the referential equality on objects implies in a WFF state the logical equality.

5.3. Operations on Object

5.3.1. Initial States (for testing and code generation)

definition $\tau_0 :: ('\mathfrak{A})st$
where $\tau_0 \equiv ((\!|heap=Map.empty,\ assocs_2=\ Map.empty,\ assocs_3=\ Map.empty|\!),$
$(\!|heap=Map.empty,\ assocs_2=\ Map.empty,\ assocs_3=\ Map.empty|\!))$

5.3.2. OclAllInstances

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

definition *OclAllInstances-generic* $:: (('\mathfrak{A}::object)\ st \Rightarrow '\mathfrak{A}\ state) \Rightarrow ('\mathfrak{A}::object \rightharpoonup '\alpha) \Rightarrow$
$('\mathfrak{A},\ '\alpha\ option\ option)\ Set$
where *OclAllInstances-generic fst-snd H* $=$
$(\lambda\tau.\ Abs\text{-}Set\text{-}0\ \lfloor\lfloor\ Some\ `\ ((H\ `\ ran\ (heap\ (fst\text{-}snd\ \tau))) - \{\ None\ \})\ \rfloor\rfloor)$

lemma *OclAllInstances-generic-defined*: $\tau \models \delta\ (OclAllInstances\text{-}generic\ pre\text{-}post\ H)$
⟨*proof*⟩

lemma *OclAllInstances-generic-init-empty*:
assumes [*simp*]: $\bigwedge x.\ pre\text{-}post\ (x,\ x) = x$
shows $\tau_0 \models OclAllInstances\text{-}generic\ pre\text{-}post\ H \triangleq Set\{\}$
⟨*proof*⟩

lemma *represented-generic-objects-nonnull*:
assumes A: $\tau \models ((OclAllInstances\text{-}generic\ pre\text{-}post\ (H{::}('\mathfrak{A}{::}object \rightharpoonup '\alpha))) \; {-}{>}includes(x))$
shows $\tau \models not(x \triangleq null)$
⟨*proof*⟩

lemma *represented-generic-objects-defined*:
assumes A: $\tau \models ((OclAllInstances\text{-}generic\ pre\text{-}post\ (H{::}('\mathfrak{A}{::}object \rightharpoonup '\alpha))) \; {-}{>}includes(x))$
shows $\tau \models \delta\ (OclAllInstances\text{-}generic\ pre\text{-}post\ H) \wedge \tau \models \delta\ x$
⟨*proof*⟩

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

lemma *represented-generic-objects-in-state*:
assumes A: $\tau \models (OclAllInstances\text{-}generic\ pre\text{-}post\ H){-}{>}includes(x)$
shows $x\ \tau \in (Some\ o\ H)\ `\ ran\ (heap(pre\text{-}post\ \tau))$
⟨*proof*⟩

lemma *state-update-vs-allInstances-generic-empty*:
assumes [*simp*]: $\bigwedge a.\ pre\text{-}post\ (mk\ a) = a$
shows $(mk\ (\!|heap{=}empty,\ assocs_2{=}A,\ assocs_3{=}B|\!)) \models OclAllInstances\text{-}generic\ pre\text{-}post\ Type \doteq Set\{\}$
⟨*proof*⟩

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

lemma *state-update-vs-allInstances-generic-including'*:
assumes [*simp*]: $\bigwedge a.\ pre\text{-}post\ (mk\ a) = a$
assumes $\bigwedge x.\ \sigma'\ oid = Some\ x \Longrightarrow x = Object$
and $Type\ Object \neq None$
shows $(OclAllInstances\text{-}generic\ pre\text{-}post\ Type)$
$(mk\ (\!|heap{=}\sigma'(oid{\mapsto}Object),\ assocs_2{=}A,\ assocs_3{=}B|\!))$
$=$
$((OclAllInstances\text{-}generic\ pre\text{-}post\ Type){-}{>}including(\lambda\ \text{-}.\ \lfloor\lfloor\ drop\ (Type\ Object)\ \rfloor\rfloor))$
$(mk\ (\!|heap{=}\sigma',assocs_2{=}A,\ assocs_3{=}B|\!))$
⟨*proof*⟩

lemma *state-update-vs-allInstances-generic-including*:
assumes [*simp*]: $\bigwedge a.\ pre\text{-}post\ (mk\ a) = a$
assumes $\bigwedge x.\ \sigma'\ oid = Some\ x \Longrightarrow x = Object$
and $Type\ Object \neq None$
shows $(OclAllInstances\text{-}generic\ pre\text{-}post\ Type)$
$(mk\ (\!|heap{=}\sigma'(oid{\mapsto}Object),\ assocs_2{=}A,\ assocs_3{=}B|\!))$
$=$

$((\lambda\text{-}.\ (\mathit{OclAllInstances\text{-}generic\ pre\text{-}post\ Type})$
$(\mathit{mk}\ (\!|\mathit{heap}{=}\sigma',\ \mathit{assocs}_2{=}A,\ \mathit{assocs}_3{=}B|\!)))\mathit{-{>}including}(\lambda\ \text{-}.\ \lfloor\lfloor\ \mathit{drop}\ (\mathit{Type\ Object})$
$\rfloor\rfloor))$
$(\mathit{mk}\ (\!|\mathit{heap}{=}\sigma'(\mathit{oid}{\mapsto}\mathit{Object}),\ \mathit{assocs}_2{=}A,\ \mathit{assocs}_3{=}B|\!))$
⟨*proof*⟩

lemma *state-update-vs-allInstances-generic-noincluding'*:
assumes [*simp*]: $\bigwedge a.\ \mathit{pre\text{-}post}\ (\mathit{mk}\ a) = a$
assumes $\bigwedge x.\ \sigma'\ \mathit{oid} = \mathit{Some}\ x \Longrightarrow x = \mathit{Object}$
and $\mathit{Type\ Object} = \mathit{None}$
shows $(\mathit{OclAllInstances\text{-}generic\ pre\text{-}post\ Type})$
$(\mathit{mk}\ (\!|\mathit{heap}{=}\sigma'(\mathit{oid}{\mapsto}\mathit{Object}),\ \mathit{assocs}_2{=}A,\ \mathit{assocs}_3{=}B|\!))$
$=$
$(\mathit{OclAllInstances\text{-}generic\ pre\text{-}post\ Type})$
$(\mathit{mk}\ (\!|\mathit{heap}{=}\sigma',\ \mathit{assocs}_2{=}A,\ \mathit{assocs}_3{=}B|\!))$
⟨*proof*⟩

theorem *state-update-vs-allInstances-generic-ntc*:
assumes [*simp*]: $\bigwedge a.\ \mathit{pre\text{-}post}\ (\mathit{mk}\ a) = a$
assumes *oid-def*: $\mathit{oid}\notin \mathit{dom}\ \sigma'$
and *non-type-conform*: $\mathit{Type\ Object} = \mathit{None}$
and *cp-ctxt*: $\mathit{cp}\ P$
and *const-ctxt*: $\bigwedge X.\ \mathit{const}\ X \Longrightarrow \mathit{const}\ (P\ X)$
shows $(\mathit{mk}\ (\!|\mathit{heap}{=}\sigma'(\mathit{oid}{\mapsto}\mathit{Object}),\mathit{assocs}_2{=}A,\mathit{assocs}_3{=}B|\!)\ \models\ P\ (\mathit{OclAllInstances\text{-}generic}$
$\mathit{pre\text{-}post\ Type})) =$
$(\mathit{mk}\ (\!|\mathit{heap}{=}\sigma',\ \mathit{assocs}_2{=}A,\ \mathit{assocs}_3{=}B|\!)\ \models P\ (\mathit{OclAllInstances\text{-}generic\ pre\text{-}post}$
$\mathit{Type}))$
(**is** $(?\tau \models P\ ?\varphi) = (?\tau' \models P\ ?\varphi))$
⟨*proof*⟩

theorem *state-update-vs-allInstances-generic-tc*:
assumes [*simp*]: $\bigwedge a.\ \mathit{pre\text{-}post}\ (\mathit{mk}\ a) = a$
assumes *oid-def*: $\mathit{oid}\notin \mathit{dom}\ \sigma'$
and *type-conform*: $\mathit{Type\ Object} \neq \mathit{None}$
and *cp-ctxt*: $\mathit{cp}\ P$
and *const-ctxt*: $\bigwedge X.\ \mathit{const}\ X \Longrightarrow \mathit{const}\ (P\ X)$
shows $(\mathit{mk}\ (\!|\mathit{heap}{=}\sigma'(\mathit{oid}{\mapsto}\mathit{Object}),\mathit{assocs}_2{=}A,\mathit{assocs}_3{=}B|\!)\ \models\ P\ (\mathit{OclAllInstances\text{-}generic}$
$\mathit{pre\text{-}post\ Type})) =$
$(\mathit{mk}\ (\!|\mathit{heap}{=}\sigma',\ \mathit{assocs}_2{=}A,\ \mathit{assocs}_3{=}B|\!)\ \models P\ ((\mathit{OclAllInstances\text{-}generic\ pre\text{-}post}$
$\mathit{Type})$
$\mathit{-{>}including}(\lambda\ \text{-}.\ \lfloor(\mathit{Type\ Object})\rfloor)))$
(**is** $(?\tau \models P\ ?\varphi) = (?\tau' \models P\ ?\varphi'))$
⟨*proof*⟩

declare *OclAllInstances-generic-def* [*simp*]

OclAllInstances (@post)

definition $\mathit{OclAllInstances\text{-}at\text{-}post} :: ('\mathfrak{A} :: \mathit{object} \rightharpoonup '\alpha) \Rightarrow ('\mathfrak{A}, '\alpha\ \mathit{option}\ \mathit{option})\ \mathit{Set}$
$(\text{-}\ .\mathit{allInstances}'(')$)
where $\mathit{OclAllInstances\text{-}at\text{-}post} = \mathit{OclAllInstances\text{-}generic}\ \mathit{snd}$

lemma $\mathit{OclAllInstances\text{-}at\text{-}post\text{-}defined}$: $\tau \models \delta\ (H\ .\mathit{allInstances}())$
$\langle \mathit{proof} \rangle$

lemma $\tau_0 \models H\ .\mathit{allInstances}() \triangleq \mathit{Set}\{\}$
$\langle \mathit{proof} \rangle$

lemma $\mathit{represented\text{-}at\text{-}post\text{-}objects\text{-}nonnull}$:
assumes A: $\tau \models (((H::('\mathfrak{A}::\mathit{object} \rightharpoonup '\alpha)).\mathit{allInstances}())\ {-}{>}\mathit{includes}(x))$
shows $\tau \models \mathit{not}(x \triangleq \mathit{null})$
$\langle \mathit{proof} \rangle$

lemma $\mathit{represented\text{-}at\text{-}post\text{-}objects\text{-}defined}$:
assumes A: $\tau \models (((H::('\mathfrak{A}::\mathit{object} \rightharpoonup '\alpha)).\mathit{allInstances}())\ {-}{>}\mathit{includes}(x))$
shows $\tau \models \delta\ (H\ .\mathit{allInstances}()) \wedge \tau \models \delta\ x$
$\langle \mathit{proof} \rangle$

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

lemma
assumes A: $\tau \models H\ .\mathit{allInstances}(){-}{>}\mathit{includes}(x)$
shows $x\ \tau \in (\mathit{Some}\ o\ H)\ `\ \mathit{ran}\ (\mathit{heap}(\mathit{snd}\ \tau))$
$\langle \mathit{proof} \rangle$

lemma $\mathit{state\text{-}update\text{-}vs\text{-}allInstances\text{-}at\text{-}post\text{-}empty}$:
shows $(\sigma, (\!|\mathit{heap}{=}\mathit{empty},\ \mathit{assocs}_2{=}A,\ \mathit{assocs}_3{=}B|\!)) \models \mathit{Type}\ .\mathit{allInstances}() \doteq \mathit{Set}\{\}$
$\langle \mathit{proof} \rangle$

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 $\mathit{state\text{-}update\text{-}vs\text{-}allInstances\text{-}at\text{-}post\text{-}including}'$:
assumes $\bigwedge x.\ \sigma'\ \mathit{oid} = \mathit{Some}\ x \Longrightarrow x = \mathit{Object}$
and $\mathit{Type}\ \mathit{Object} \neq \mathit{None}$
shows $(\mathit{Type}\ .\mathit{allInstances}())$
$(\sigma, (\!|\mathit{heap}{=}\sigma'(\mathit{oid}{\mapsto}\mathit{Object}),\ \mathit{assocs}_2{=}A,\ \mathit{assocs}_3{=}B|\!))$
$=$
$((\mathit{Type}\ .\mathit{allInstances}()){-}{>}\mathit{including}(\lambda\ \text{-}.\ \lfloor\lfloor\ \mathit{drop}\ (\mathit{Type}\ \mathit{Object})\ \rfloor\rfloor))$
$(\sigma, (\!|\mathit{heap}{=}\sigma',\mathit{assocs}_2{=}A,\ \mathit{assocs}_3{=}B|\!))$
$\langle \mathit{proof} \rangle$

lemma *state-update-vs-allInstances-at-post-including*:
assumes $\bigwedge x.\ \sigma'\ oid = Some\ x \Longrightarrow x = Object$
and $Type\ Object \neq None$
shows $(Type\ .allInstances())$
$(\sigma, (\!|heap{=}\sigma'(oid{\mapsto}Object),\ assocs_2{=}A,\ assocs_3{=}B|\!))$
$=$
$((\lambda\text{-}.\ (Type\ .allInstances())$
$(\sigma, (\!|heap{=}\sigma',\ assocs_2{=}A,\ assocs_3{=}B|\!)))\text{->}including(\lambda\ \text{-}.\ \lfloor\lfloor\ drop\ (Type\ Object)$
$\rfloor\rfloor))$
$(\sigma, (\!|heap{=}\sigma'(oid{\mapsto}Object),\ assocs_2{=}A,\ assocs_3{=}B|\!))$
$\langle proof\rangle$

lemma *state-update-vs-allInstances-at-post-noincluding'*:
assumes $\bigwedge x.\ \sigma'\ oid = Some\ x \Longrightarrow x = Object$
and $Type\ Object = None$
shows $(Type\ .allInstances())$
$(\sigma, (\!|heap{=}\sigma'(oid{\mapsto}Object),\ assocs_2{=}A,\ assocs_3{=}B|\!))$
$=$
$(Type\ .allInstances())$
$(\sigma, (\!|heap{=}\sigma',\ assocs_2{=}A,\ assocs_3{=}B|\!))$
$\langle proof\rangle$

theorem *state-update-vs-allInstances-at-post-ntc*:
assumes *oid-def*: $oid{\notin}dom\ \sigma'$
and *non-type-conform*: $Type\ Object = None$
and *cp-ctxt*: $cp\ P$
and *const-ctxt*: $\bigwedge X.\ const\ X \Longrightarrow const\ (P\ X)$
shows $((\sigma, (\!|heap{=}\sigma'(oid{\mapsto}Object), assocs_2{=}A, assocs_3{=}B|\!)) \models (P(Type\ .allInstances()))) =$
$((\sigma, (\!|heap{=}\sigma',\ assocs_2{=}A,\ assocs_3{=}B|\!)) \qquad \models (P(Type\ .allInstances())))$
$\langle proof\rangle$

theorem *state-update-vs-allInstances-at-post-tc*:
assumes *oid-def*: $oid{\notin}dom\ \sigma'$
and *type-conform*: $Type\ Object \neq None$
and *cp-ctxt*: $cp\ P$
and *const-ctxt*: $\bigwedge X.\ const\ X \Longrightarrow const\ (P\ X)$
shows $((\sigma, (\!|heap{=}\sigma'(oid{\mapsto}Object), assocs_2{=}A, assocs_3{=}B|\!)) \models (P(Type\ .allInstances()))) =$
$((\sigma, (\!|heap{=}\sigma',\ assocs_2{=}A,\ assocs_3{=}B|\!)) \qquad \models (P((Type\ .allInstances())$
$\text{->}including(\lambda\ \text{-}.\ \lfloor(Type\ Object)\rfloor))))$
$\langle proof\rangle$

OclAllInstances (@pre)

definition $OclAllInstances\text{-}at\text{-}pre :: ('\mathfrak{A} :: object \rightharpoonup '\alpha) \Rightarrow ('\mathfrak{A}, '\alpha\ option\ option)\ Set$
$(\text{-}\ .allInstances@pre'('))$

where $OclAllInstances\text{-}at\text{-}pre = OclAllInstances\text{-}generic\ fst$

lemma *OclAllInstances-at-pre-defined*: $\tau \models \delta\ (H\ .allInstances@pre())$
⟨*proof*⟩

lemma $\tau_0 \models H\ .allInstances@pre() \triangleq Set\{\}$
⟨*proof*⟩

lemma *represented-at-pre-objects-nonnull*:
assumes A: $\tau \models (((H::('\mathfrak{A}::object \rightharpoonup '\alpha)).allInstances@pre()) \ {-}{>}includes(x))$
shows $\tau \models not(x \triangleq null)$
⟨*proof*⟩

lemma *represented-at-pre-objects-defined*:
assumes A: $\tau \models (((H::('\mathfrak{A}::object \rightharpoonup '\alpha)).allInstances@pre()) \ {-}{>}includes(x))$
shows $\tau \models \delta\ (H\ .allInstances@pre()) \wedge \tau \models \delta\ x$
⟨*proof*⟩

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

lemma
assumes A: $\tau \models H\ .allInstances@pre(){-}{>}includes(x)$
shows $x\ \tau \in (Some\ o\ H)\ `\ ran\ (heap(fst\ \tau))$
⟨*proof*⟩

lemma *state-update-vs-allInstances-at-pre-empty*:
shows $((\!|heap{=}empty,\ assocs_2{=}A,\ assocs_3{=}B|\!),\ \sigma) \models Type\ .allInstances@pre() \doteq Set\{\}$
⟨*proof*⟩

Here comes a couple of operational rules that allow to infer the value of oclAllInstances@pre 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-pre-including′*:
assumes $\bigwedge x.\ \sigma'\ oid = Some\ x \Longrightarrow x = Object$
and $Type\ Object \neq None$
shows $(Type\ .allInstances@pre())$
$((\!|heap{=}\sigma'(oid{\mapsto}Object),\ assocs_2{=}A,\ assocs_3{=}B|\!),\ \sigma)$
$=$
$((Type\ .allInstances@pre()){-}{>}including(\lambda\ \text{-}.\ \lfloor\lfloor\ drop\ (Type\ Object)\ \rfloor\rfloor))$
$((\!|heap{=}\sigma',assocs_2{=}A,\ assocs_3{=}B|\!),\ \sigma)$
⟨*proof*⟩

lemma *state-update-vs-allInstances-at-pre-including*:
assumes $\bigwedge x.\ \sigma'\ oid = Some\ x \Longrightarrow x = Object$

and *Type Object* $\neq$ *None*
shows $(Type\ .allInstances@pre())$
$((\!|heap{=}\sigma'(oid{\mapsto}Object),\ assocs_2{=}A,\ assocs_3{=}B|\!),\ \sigma)$
$=$
$((\lambda\text{-}.\ (Type\ .allInstances@pre())$
$((\!|heap{=}\sigma',\ assocs_2{=}A,\ assocs_3{=}B|\!),\ \sigma))\text{−}{>}including(\lambda\ \text{-}.\ \lfloor\lfloor\ drop\ (Type\ Object)$
$\rfloor\rfloor))$
$((\!|heap{=}\sigma'(oid{\mapsto}Object),\ assocs_2{=}A,\ assocs_3{=}B|\!),\ \sigma)$
⟨*proof*⟩

lemma *state-update-vs-allInstances-at-pre-noincluding'*:
assumes $\bigwedge x.\ \sigma'\ oid = Some\ x \Longrightarrow x = Object$
and *Type Object* = *None*
shows $(Type\ .allInstances@pre())$
$((\!|heap{=}\sigma'(oid{\mapsto}Object),\ assocs_2{=}A,\ assocs_3{=}B|\!),\ \sigma)$
$=$
$(Type\ .allInstances@pre())$
$((\!|heap{=}\sigma',\ assocs_2{=}A,\ assocs_3{=}B|\!),\ \sigma)$
⟨*proof*⟩

theorem *state-update-vs-allInstances-at-pre-ntc*:
assumes *oid-def*: $oid \notin dom\ \sigma'$
and *non-type-conform*: *Type Object* = *None*
and *cp-ctxt*: *cp P*
and *const-ctxt*: $\bigwedge X.\ const\ X \Longrightarrow const\ (P\ X)$
shows $(((\!|heap{=}\sigma'(oid{\mapsto}Object),assocs_2{=}A,assocs_3{=}B|\!),\ \sigma) \models (P(Type\ .allInstances@pre())))$
$=$
$(((\!|heap{=}\sigma',\ assocs_2{=}A,\ assocs_3{=}B|\!),\ \sigma) \models (P(Type\ .allInstances@pre())))$
⟨*proof*⟩

theorem *state-update-vs-allInstances-at-pre-tc*:
assumes *oid-def*: $oid \notin dom\ \sigma'$
and *type-conform*: *Type Object* $\neq$ *None*
and *cp-ctxt*: *cp P*
and *const-ctxt*: $\bigwedge X.\ const\ X \Longrightarrow const\ (P\ X)$
shows $(((\!|heap{=}\sigma'(oid{\mapsto}Object),assocs_2{=}A,assocs_3{=}B|\!),\ \sigma) \models (P(Type\ .allInstances@pre())))$
$=$
$(((\!|heap{=}\sigma',\ assocs_2{=}A,\ assocs_3{=}B|\!),\ \sigma) \models (P((Type\ .allInstances@pre())$
$\text{−}{>}including(\lambda\ \text{-}.\ \lfloor(Type\ Object)\rfloor))))$
⟨*proof*⟩

@post or @pre

theorem *StrictRefEq*$_{Object}$*-vs-StrongEq''*:
assumes *WFF*: *WFF* τ
and *valid-x*: $\tau \models (\upsilon\ (x :: ('\mathfrak{A}{::}object,'\alpha{::}object\ option\ option)val))$
and *valid-y*: $\tau \models (\upsilon\ y)$

and *oid-preserve*: $\bigwedge x.\ x \in ran\ (heap(fst\ \tau)) \vee x \in ran\ (heap(snd\ \tau)) \Longrightarrow$
$oid\text{-}of\ (H\,x) = oid\text{-}of\ x$
and *xy-together*: $\tau \models ((H\ .allInstances()\text{-}\!\!>includes(x)\ and\ H\ .allInstances()\text{-}\!\!>includes(y))$
or
$(H\ .allInstances@pre()\text{-}\!\!>includes(x)\ and\ H\ .allInstances@pre()\text{-}\!\!>includes(y)))$

shows $(\tau \models (StrictRefEq_{Object}\ x\ y)) = (\tau \models (x \triangleq y))$
$\langle proof \rangle$

5.3.3. OclIsNew, OclIsDeleted, OclIsMaintained, OclIsAbsent

definition $OclIsNew$:: $('\mathfrak{A}, '\alpha{::}\{null,object\})val \Rightarrow ('\mathfrak{A})Boolean \quad ((\text{-}).oclIsNew'(')))$
where $X\ .oclIsNew() \equiv (\lambda\tau\ .\ if\ (\delta\ X)\ \tau = true\ \tau$
$then\ \lfloor\lfloor oid\text{-}of\ (X\ \tau) \notin dom(heap(fst\ \tau)) \wedge$
$oid\text{-}of\ (X\ \tau) \in dom(heap(snd\ \tau))\rfloor\rfloor$
$else\ invalid\ \tau)$

The following predicates — which are not part of the OCL standard descriptions — complete the goal of oclIsNew by describing where an object belongs.

definition $OclIsDeleted$:: $('\mathfrak{A}, '\alpha{::}\{null,object\})val \Rightarrow ('\mathfrak{A})Boolean \quad ((\text{-}).oclIsDeleted'(')))$
where $X\ .oclIsDeleted() \equiv (\lambda\tau\ .\ if\ (\delta\ X)\ \tau = true\ \tau$
$then\ \lfloor\lfloor oid\text{-}of\ (X\ \tau) \in dom(heap(fst\ \tau)) \wedge$
$oid\text{-}of\ (X\ \tau) \notin dom(heap(snd\ \tau))\rfloor\rfloor$
$else\ invalid\ \tau)$

definition $OclIsMaintained$:: $('\mathfrak{A}, '\alpha{::}\{null,object\})val \Rightarrow ('\mathfrak{A})Boolean((\text{-}).oclIsMaintained'(')))$
where $X\ .oclIsMaintained() \equiv (\lambda\tau\ .\ if\ (\delta\ X)\ \tau = true\ \tau$
$then\ \lfloor\lfloor oid\text{-}of\ (X\ \tau) \in dom(heap(fst\ \tau)) \wedge$
$oid\text{-}of\ (X\ \tau) \in dom(heap(snd\ \tau))\rfloor\rfloor$
$else\ invalid\ \tau)$

definition $OclIsAbsent$:: $('\mathfrak{A}, '\alpha{::}\{null,object\})val \Rightarrow ('\mathfrak{A})Boolean \quad ((\text{-}).oclIsAbsent'(')))$
where $X\ .oclIsAbsent() \equiv (\lambda\tau\ .\ if\ (\delta\ X)\ \tau = true\ \tau$
$then\ \lfloor\lfloor oid\text{-}of\ (X\ \tau) \notin dom(heap(fst\ \tau)) \wedge$
$oid\text{-}of\ (X\ \tau) \notin dom(heap(snd\ \tau))\rfloor\rfloor$
$else\ invalid\ \tau)$

lemma *state-split* : $\tau \models \delta\ X \Longrightarrow$
$\tau \models (X\ .oclIsNew()) \vee \tau \models (X\ .oclIsDeleted()) \vee$
$\tau \models (X\ .oclIsMaintained()) \vee \tau \models (X\ .oclIsAbsent())$
$\langle proof \rangle$

lemma *notNew-vs-others* : $\tau \models \delta\ X \Longrightarrow$
$(\neg\ \tau \models (X\ .oclIsNew())) = (\tau \models (X\ .oclIsDeleted()) \vee$
$\tau \models (X\ .oclIsMaintained()) \vee \tau \models (X\ .oclIsAbsent()))$
$\langle proof \rangle$

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.

definition $OclIsModifiedOnly$ ::$('\mathfrak{A}::object,'\alpha::\{null,object\})Set \Rightarrow '\mathfrak{A}\ Boolean$
$(\text{-}{-}{>}oclIsModifiedOnly'('))$
where $X{-}{>}oclIsModifiedOnly() \equiv (\lambda(\sigma,\sigma').$
$let\ X' = (oid\text{-}of\ `\ \lceil\lceil Rep\text{-}Set\text{-}0(X(\sigma,\sigma'))\rceil\rceil);$
$S = ((dom\ (heap\ \sigma) \cap dom\ (heap\ \sigma')) - X')$
$in\ if\ (\delta\ X)\ (\sigma,\sigma') = true\ (\sigma,\sigma') \wedge (\forall x{\in}\lceil\lceil Rep\text{-}Set\text{-}0(X(\sigma,\sigma'))\rceil\rceil.\ x \neq null)$
$then\ \lfloor\lfloor\forall\ x \in S.\ (heap\ \sigma)\ x = (heap\ \sigma')\ x\rfloor\rfloor$
$else\ invalid\ (\sigma,\sigma'))$

Execution with Invalid or Null or Null Element as Argument

lemma $invalid{-}{>}oclIsModifiedOnly() = invalid$
$\langle proof \rangle$

lemma $null{-}{>}oclIsModifiedOnly() = invalid$
$\langle proof \rangle$

lemma
assumes $X\text{-}null : \tau \models X{-}{>}includes(null)$
shows $\tau \models X{-}{>}oclIsModifiedOnly() \triangleq invalid$
$\langle proof \rangle$

Context Passing

lemma $cp\text{-}OclIsModifiedOnly : X{-}{>}oclIsModifiedOnly()\ \tau = (\lambda\text{-}.\ X\ \tau){-}{>}oclIsModifiedOnly()$
τ
$\langle proof \rangle$

5.3.5. OclSelf

The following predicate—which is not part of the OCL standard—explicitly retrieves in the pre or post state the original OCL expression given as argument.

definition $[simp]$: $OclSelf\ x\ H\ fst\text{-}snd = (\lambda\tau\ .\ if\ (\delta\ x)\ \tau = true\ \tau$
$then\ if\ oid\text{-}of\ (x\ \tau) \in dom(heap(fst\ \tau)) \wedge oid\text{-}of\ (x\ \tau) \in dom(heap\ (snd\ \tau))$
$then\ \ H\ \lceil(heap(fst\text{-}snd\ \tau))(oid\text{-}of\ (x\ \tau))\rceil$
$else\ invalid\ \tau$
$else\ invalid\ \tau)$

definition $OclSelf\text{-}at\text{-}pre$ :: $('\mathfrak{A}::object,'\alpha::\{null,object\})val \Rightarrow$

$('\mathfrak{A} \Rightarrow '\alpha) \Rightarrow$
$('\mathfrak{A}::object,'\alpha::\{null,object\})val$ $((\text{-})@pre(\text{-}))$
where x $@pre$ H $=$ $OclSelf$ x H fst

definition $OclSelf\text{-}at\text{-}post$ :: $('\mathfrak{A}::object,'\alpha::\{null,object\})val \Rightarrow$
$('\mathfrak{A} \Rightarrow '\alpha) \Rightarrow$
$('\mathfrak{A}::object,'\alpha::\{null,object\})val$ $((\text{-})@post(\text{-}))$
where x $@post$ H $=$ $OclSelf$ x H snd

5.3.6. Framing Theorem

lemma $all\text{-}oid\text{-}diff$:
assumes $def\text{-}x : \tau \models \delta\ x$
assumes $def\text{-}X : \tau \models \delta\ X$
assumes $def\text{-}X' : \bigwedge x.\ x \in \lceil\lceil Rep\text{-}Set\text{-}0\ (X\ \tau)\rceil\rceil \Longrightarrow x \neq null$

defines $P \equiv (\lambda a.\ not\ (StrictRefEq_{Object}\ x\ a))$
shows $(\tau \models X\text{->}forAll(a|\ P\ a)) = (oid\text{-}of\ (x\ \tau) \notin oid\text{-}of\ `\ \lceil\lceil Rep\text{-}Set\text{-}0\ (X\ \tau)\rceil\rceil)$
⟨proof⟩

theorem $framing$:
assumes $modifiesclause{:}\tau \models (X\text{->}excluding(x))\text{->}oclIsModifiedOnly()$
and $oid\text{-}is\text{-}typerepr : \tau \models X\text{->}forAll(a|\ not\ (StrictRefEq_{Object}\ x\ a))$
shows $\tau \models (x\ @pre\ P\ \triangleq\ (x\ @post\ P))$
⟨proof⟩

As corollary, the framing property can be expressed with only the strong equality as comparison operator.

theorem $framing'$:
assumes $wff : WFF\ \tau$
assumes $modifiesclause{:}\tau \models (X\text{->}excluding(x))\text{->}oclIsModifiedOnly()$
and $oid\text{-}is\text{-}typerepr : \tau \models X\text{->}forAll(a|\ not\ (x \triangleq a))$
and $oid\text{-}preserve$: $\bigwedge x.\ x \in ran\ (heap(fst\ \tau)) \lor x \in ran\ (heap(snd\ \tau)) \Longrightarrow$
$oid\text{-}of\ (H\ x) = oid\text{-}of\ x$
and $xy\text{-}together$:
$\tau \models X\text{->}forAll(y \mid (H\ .allInstances()\text{->}includes(x)\ and\ H\ .allInstances()\text{->}includes(y))\ or$
$(H\ .allInstances@pre()\text{->}includes(x)\ and\ H\ .allInstances@pre()\text{->}includes(y)))$
shows $\tau \models (x\ @pre\ P\ \triangleq\ (x\ @post\ P))$
⟨proof⟩

5.3.7. Miscellaneous

lemma $pre\text{-}post\text{-}new$: $\tau \models (x\ .oclIsNew()) \Longrightarrow \neg\ (\tau \models \upsilon(x\ @pre\ H1)) \land \neg\ (\tau \models \upsilon(x\ @post\ H2))$
⟨proof⟩

lemma $pre\text{-}post\text{-}old$: $\tau \models (x\ .oclIsDeleted()) \Longrightarrow \neg\ (\tau \models \upsilon(x\ @pre\ H1)) \land \neg\ (\tau \models \upsilon(x\ @post\ H2))$
⟨proof⟩

lemma *pre-post-absent*: $\tau \models (x\ .oclIsAbsent()) \Longrightarrow \neg\ (\tau \models \upsilon(x\ @pre\ H1)) \wedge \neg\ (\tau \models \upsilon(x\ @post\ H2))$
⟨*proof*⟩

lemma *pre-post-maintained*: $(\tau \models \upsilon(x\ @pre\ H1) \vee \tau \models \upsilon(x\ @post\ H2)) \Longrightarrow \tau \models (x\ .oclIsMaintained())$
⟨*proof*⟩

lemma *pre-post-maintained'*:
$\tau \models (x\ .oclIsMaintained()) \Longrightarrow (\tau \models \upsilon(x\ @pre\ (Some\ o\ H1)) \wedge \tau \models \upsilon(x\ @post\ (Some\ o\ H2)))$
⟨*proof*⟩

lemma *framing-same-state*: $(\sigma, \sigma) \models (x\ @pre\ H \triangleq (x\ @post\ H))$
⟨*proof*⟩

end

theory *OCL-tools*
imports *OCL-core*
begin

end

theory *OCL-main*
imports *OCL-lib OCL-state OCL-tools*
begin

end

Part III.

Examples

6. The Employee Analysis Model

6.1. The Employee Analysis Model (UML)

theory
Employee-AnalysisModel-UMLPart
imports
../OCL-main
begin

6.1.1. Introduction

For certain concepts like classes and class-types, only a generic definition for its resulting semantics can be given. Generic means, there is a function outside HOL that "compiles" a concrete, closed-world class diagram into a "theory" of this data model, consisting of a bunch of definitions for classes, accessors, method, casts, and tests for actual types, as well as proofs for the fundamental properties of these operations in this concrete data model.

Such generic function or "compiler" can be implemented in Isabelle on the ML level. This has been done, for a semantics following the open-world assumption, for UML 2.0 in [4, 7]. In this paper, we follow another approach for UML 2.4: we define the concepts of the compilation informally, and present a concrete example which is verified in Isabelle/HOL.

Outlining the Example

We are presenting here an "analysis-model" of the (slightly modified) example Figure 7.3, page 20 of the OCL standard [33]. Here, analysis model means that associations were really represented as relation on objects on the state—as is intended by the standard—rather by pointers between objects as is done in our "design model" (see Section 7.1). To be precise, this theory contains the formalization of the data-part covered by the UML class model (see Figure 6.1):

This means that the association (attached to the association class `EmployeeRanking`) with the association ends `boss` and `employees` is implemented by the attribute `boss` and the operation `employees` (to be discussed in the OCL part captured by the subsequent theory).

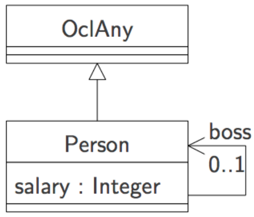


Figure 6.1.: A simple UML class model drawn from Figure 7.3, page 20 of [33].

6.1.2. Example Data-Universe and its Infrastructure

Ideally, the following is generated automatically from a UML class model.

Our data universe consists in the concrete class diagram just of node's, and implicitly of the class object. Each class implies the existence of a class type defined for the corresponding object representations as follows:

datatype $\mathit{type}_{Person} = \mathit{mk}_{Person}\ \mathit{oid}$
$\qquad\qquad\qquad\quad \mathit{int\ option}$

datatype $\mathit{type}_{OclAny} = \mathit{mk}_{OclAny}\ \mathit{oid}$
$\qquad\qquad\qquad\quad (\mathit{int\ option})\ \mathit{option}$

Now, we construct a concrete "universe of OclAny types" by injection into a sum type containing the class types. This type of OclAny will be used as instance for all respective type-variables.

datatype $\mathfrak{A} = \mathit{in}_{Person}\ \mathit{type}_{Person} \mid \mathit{in}_{OclAny}\ \mathit{type}_{OclAny}$

Having fixed the object universe, we can introduce type synonyms that exactly correspond to OCL types. Again, we exploit that our representation of OCL is a "shallow embedding" with a one-to-one correspondance of OCL-types to types of the meta-language HOL.

type-synonym *Boolean* $= \mathfrak{A}\ \mathit{Boolean}$
type-synonym *Integer* $= \mathfrak{A}\ \mathit{Integer}$
type-synonym *Void* $= \mathfrak{A}\ \mathit{Void}$
type-synonym *OclAny* $= (\mathfrak{A}, \mathit{type}_{OclAny}\ \mathit{option\ option})\ \mathit{val}$
type-synonym *Person* $= (\mathfrak{A}, \mathit{type}_{Person}\ \mathit{option\ option})\ \mathit{val}$
type-synonym *Set-Integer* $= (\mathfrak{A}, \mathit{int\ option\ option})\ \mathit{Set}$
type-synonym *Set-Person* $= (\mathfrak{A}, \mathit{type}_{Person}\ \mathit{option\ option})\ \mathit{Set}$

Just a little check:

typ *Boolean*

To reuse key-elements of the library like referential equality, we have to show that the object universe belongs to the type class "oclany," i. e., each class type has to provide a function *oid-of* yielding the object id (oid) of the object.

instantiation $type_{Person}$ :: *object*
begin
  definition *oid-of-type*$_{Person}$*-def*: *oid-of* x = (*case* x *of* mk_{Person} *oid* - ⇒ *oid*)
  instance ⟨*proof*⟩
end

instantiation $type_{OclAny}$ :: *object*
begin
  definition *oid-of-type*$_{OclAny}$*-def*: *oid-of* x = (*case* x *of* mk_{OclAny} *oid* - ⇒ *oid*)
  instance ⟨*proof*⟩
end

instantiation $\mathfrak{A}$ :: *object*
begin
  definition *oid-of-*$\mathfrak{A}$*-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**) $StrictRefEq_{Object}$*-*$_{Person}$: $(x::Person) \doteq y \equiv StrictRefEq_{Object}\ x\ y$
defs(**overloaded**) $StrictRefEq_{Object}$*-*$_{OclAny}$: $(x::OclAny) \doteq y \equiv StrictRefEq_{Object}\ x\ y$

lemmas
  cp-$StrictRefEq_{Object}$[*of* x::*Person* y::*Person* τ,
    simplified $StrictRefEq_{Object}$*-*$_{Person}$[*symmetric*]]
  cp-intro(*9*) [*of* P::*Person* ⇒*PersonQ*::*Person* ⇒*Person*,
    simplified $StrictRefEq_{Object}$*-*$_{Person}$[*symmetric*]]
  $StrictRefEq_{Object}$*-def* [*of* x::*Person* y::*Person*,
    simplified $StrictRefEq_{Object}$*-*$_{Person}$[*symmetric*]]
  $StrictRefEq_{Object}$*-defargs* [*of* - x::*Person* y::*Person*,
    simplified $StrictRefEq_{Object}$*-*$_{Person}$[*symmetric*]]
  $StrictRefEq_{Object}$*-strict1*
    [*of* x::*Person*,
    simplified $StrictRefEq_{Object}$*-*$_{Person}$[*symmetric*]]
  $StrictRefEq_{Object}$*-strict2*
    [*of* x::*Person*,
    simplified $StrictRefEq_{Object}$*-*$_{Person}$[*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 $OclAsType_{OclAny}$ :: $'\alpha \Rightarrow OclAny$ ((-) $.oclAsType'(OclAny')$)
consts $OclAsType_{Person}$ :: $'\alpha \Rightarrow Person$ ((-) $.oclAsType'(Person')$)

definition $OclAsType_{OclAny}$-$\mathfrak{A}$ $= (\lambda u.\ \lfloor case\ u\ of\ in_{OclAny}\ a \Rightarrow a$
$\mid in_{Person}\ (mk_{Person}\ oid\ a) \Rightarrow mk_{OclAny}\ oid\ \lfloor a \rfloor \rfloor)$

lemma $OclAsType_{OclAny}$-$\mathfrak{A}$-$some$: $OclAsType_{OclAny}$-$\mathfrak{A}\ x \neq None$
$\langle proof \rangle$

defs (**overloaded**) $OclAsType_{OclAny}$-$OclAny$:
$(X{::}OclAny)\ .oclAsType(OclAny) \equiv X$

defs (**overloaded**) $OclAsType_{OclAny}$-$Person$:
$(X{::}Person)\ .oclAsType(OclAny) \equiv$
$(\lambda\tau.\ case\ X\ \tau\ of$
$\perp \Rightarrow invalid\ \tau$
$\mid \lfloor \perp \rfloor \Rightarrow null\ \tau$
$\mid \lfloor \lfloor mk_{Person}\ oid\ a \rfloor \rfloor \Rightarrow \lfloor \lfloor (mk_{OclAny}\ oid\ \lfloor a \rfloor) \rfloor \rfloor)$

definition $OclAsType_{Person}$-$\mathfrak{A}$ $= (\lambda u.\ case\ u\ of\ in_{Person}\ p \Rightarrow \lfloor p \rfloor$
$\mid in_{OclAny}\ (mk_{OclAny}\ oid\ \lfloor a \rfloor) \Rightarrow \lfloor mk_{Person}\ oid\ a \rfloor$
$\mid - \Rightarrow None)$

defs (**overloaded**) $OclAsType_{Person}$-$OclAny$:
$(X{::}OclAny)\ .oclAsType(Person) \equiv$
$(\lambda\tau.\ case\ X\ \tau\ of$
$\perp \Rightarrow invalid\ \tau$
$\mid \lfloor \perp \rfloor \Rightarrow null\ \tau$
$\mid \lfloor \lfloor mk_{OclAny}\ oid\ \perp \rfloor \rfloor \Rightarrow invalid\ \tau$ $\quad (*\ down{-}cast\ exception\ *)$
$\mid \lfloor \lfloor mk_{OclAny}\ oid\ \lfloor a \rfloor \rfloor \rfloor \Rightarrow \lfloor \lfloor mk_{Person}\ oid\ a \rfloor \rfloor)$

defs (**overloaded**) $OclAsType_{Person}$-$Person$:
$(X{::}Person)\ .oclAsType(Person) \equiv X$

lemmas [$simp$] =
$OclAsType_{OclAny}$-$OclAny$
$OclAsType_{Person}$-$Person$

Context Passing

lemma cp-$OclAsType_{OclAny}$-$Person$-$Person$: $cp\ P \Longrightarrow cp(\lambda X.\ (P\ (X{::}Person){::}Person)\ .oclAsType(OclAny))$
$\langle proof \rangle$

lemma *cp-OclAsType*$_{OclAny}$*-OclAny-OclAny*: *cp* $P \Longrightarrow$ *cp*$(\lambda X.$ (*P* (*X*::*OclAny*)::*OclAny*) .*oclAsType*(*OclAny*))
⟨*proof*⟩
lemma *cp-OclAsType*$_{Person}$*-Person-Person*: *cp* $P \Longrightarrow$ *cp*$(\lambda X.$ (*P* (*X*::*Person*)::*Person*) .*oclAsType*(*Person*))
⟨*proof*⟩
lemma *cp-OclAsType*$_{Person}$*-OclAny-OclAny*: *cp* $P \Longrightarrow$ *cp*$(\lambda X.$ (*P* (*X*::*OclAny*)::*OclAny*) .*oclAsType*(*Person*))
⟨*proof*⟩

lemma *cp-OclAsType*$_{OclAny}$*-Person-OclAny*: *cp* $P \Longrightarrow$ *cp*$(\lambda X.$ (*P* (*X*::*Person*)::*OclAny*) .*oclAsType*(*OclAny*))
⟨*proof*⟩
lemma *cp-OclAsType*$_{OclAny}$*-OclAny-Person*: *cp* $P \Longrightarrow$ *cp*$(\lambda X.$ (*P* (*X*::*OclAny*)::*Person*) .*oclAsType*(*OclAny*))
⟨*proof*⟩
lemma *cp-OclAsType*$_{Person}$*-Person-OclAny*: *cp* $P \Longrightarrow$ *cp*$(\lambda X.$ (*P* (*X*::*Person*)::*OclAny*) .*oclAsType*(*Person*))
⟨*proof*⟩
lemma *cp-OclAsType*$_{Person}$*-OclAny-Person*: *cp* $P \Longrightarrow$ *cp*$(\lambda X.$ (*P* (*X*::*OclAny*)::*Person*) .*oclAsType*(*Person*))
⟨*proof*⟩

lemmas [*simp*] =
cp-OclAsType$_{OclAny}$*-Person-Person*
cp-OclAsType$_{OclAny}$*-OclAny-OclAny*
cp-OclAsType$_{Person}$*-Person-Person*
cp-OclAsType$_{Person}$*-OclAny-OclAny*

cp-OclAsType$_{OclAny}$*-Person-OclAny*
cp-OclAsType$_{OclAny}$*-OclAny-Person*
cp-OclAsType$_{Person}$*-Person-OclAny*
cp-OclAsType$_{Person}$*-OclAny-Person*

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*

$\langle proof \rangle$

lemma $OclAsType_{Person}$-$OclAny$-$nullstrict[simp]$: $(null::OclAny)$ $.oclAsType(Person) = null$
$\langle proof \rangle$

lemma $OclAsType_{Person}$-$Person$-$strict$: $(invalid::Person)$ $.oclAsType(Person) = invalid$
$\langle proof \rangle$
lemma $OclAsType_{Person}$-$Person$-$nullstrict$: $(null::Person)$ $.oclAsType(Person) = null$
$\langle proof \rangle$

6.1.5. OclIsTypeOf

Definition

consts $OclIsTypeOf_{OclAny}$ :: $'\alpha \Rightarrow Boolean$ $((\text{-}).oclIsTypeOf'(OclAny'))$
consts $OclIsTypeOf_{Person}$ :: $'\alpha \Rightarrow Boolean$ $((\text{-}).oclIsTypeOf'(Person'))$

defs (**overloaded**) $OclIsTypeOf_{OclAny}$-$OclAny$:
$(X::OclAny)$ $.oclIsTypeOf(OclAny) \equiv$
$(\lambda\tau.$ $case$ X τ of
$\perp \Rightarrow invalid$ τ
$|$ $\lfloor\perp\rfloor \Rightarrow true$ τ $(*$ $invalid$ $??$ $*)$
$|$ $\lfloor\lfloor mk_{OclAny}$ oid $\perp$ $\rfloor\rfloor \Rightarrow true$ τ
$|$ $\lfloor\lfloor mk_{OclAny}$ oid $\lfloor\text{-}\rfloor$ $\rfloor\rfloor \Rightarrow false$ $\tau)$

defs (**overloaded**) $OclIsTypeOf_{OclAny}$-$Person$:
$(X::Person)$ $.oclIsTypeOf(OclAny) \equiv$
$(\lambda\tau.$ $case$ X τ of
$\perp \Rightarrow invalid$ τ
$|$ $\lfloor\perp\rfloor \Rightarrow true$ τ $(*$ $invalid$ $??$ $*)$
$|$ $\lfloor\lfloor$ - $\rfloor\rfloor \Rightarrow false$ $\tau)$

defs (**overloaded**) $OclIsTypeOf_{Person}$-$OclAny$:
$(X::OclAny)$ $.oclIsTypeOf(Person) \equiv$
$(\lambda\tau.$ $case$ X τ of
$\perp \Rightarrow invalid$ τ
$|$ $\lfloor\perp\rfloor \Rightarrow true$ τ
$|$ $\lfloor\lfloor mk_{OclAny}$ oid $\perp$ $\rfloor\rfloor \Rightarrow false$ τ
$|$ $\lfloor\lfloor mk_{OclAny}$ oid $\lfloor\text{-}\rfloor$ $\rfloor\rfloor \Rightarrow true$ $\tau)$

defs (**overloaded**) $OclIsTypeOf_{Person}$-$Person$:
$(X::Person)$ $.oclIsTypeOf(Person) \equiv$
$(\lambda\tau.$ $case$ X τ of
$\perp \Rightarrow invalid$ τ
$|$ - $\Rightarrow true$ $\tau)$

Context Passing

lemma $cp\text{-}OclIsTypeOf_{OclAny}\text{-}Person\text{-}Person$: $cp\ P \Longrightarrow cp(\lambda X.(P(X::Person)::Person).oclIsTypeOf(OclAny))$
⟨proof⟩
lemma $cp\text{-}OclIsTypeOf_{OclAny}\text{-}OclAny\text{-}OclAny$: $cp\ P \Longrightarrow cp(\lambda X.(P(X::OclAny)::OclAny).oclIsTypeOf(OclAny))$
⟨proof⟩
lemma $cp\text{-}OclIsTypeOf_{Person}\text{-}Person\text{-}Person$: $cp\ P \Longrightarrow cp(\lambda X.(P(X::Person)::Person).oclIsTypeOf(Person))$
⟨proof⟩
lemma $cp\text{-}OclIsTypeOf_{Person}\text{-}OclAny\text{-}OclAny$: $cp\ P \Longrightarrow cp(\lambda X.(P(X::OclAny)::OclAny).oclIsTypeOf(Person))$
⟨proof⟩

lemma $cp\text{-}OclIsTypeOf_{OclAny}\text{-}Person\text{-}OclAny$: $cp\ P \Longrightarrow cp(\lambda X.(P(X::Person)::OclAny).oclIsTypeOf(OclAny))$
⟨proof⟩
lemma $cp\text{-}OclIsTypeOf_{OclAny}\text{-}OclAny\text{-}Person$: $cp\ P \Longrightarrow cp(\lambda X.(P(X::OclAny)::Person).oclIsTypeOf(OclAny))$
⟨proof⟩
lemma $cp\text{-}OclIsTypeOf_{Person}\text{-}Person\text{-}OclAny$: $cp\ P \Longrightarrow cp(\lambda X.(P(X::Person)::OclAny).oclIsTypeOf(Person))$
⟨proof⟩
lemma $cp\text{-}OclIsTypeOf_{Person}\text{-}OclAny\text{-}Person$: $cp\ P \Longrightarrow cp(\lambda X.(P(X::OclAny)::Person).oclIsTypeOf(Person))$
⟨proof⟩

lemmas [*simp*] =
$cp\text{-}OclIsTypeOf_{OclAny}\text{-}Person\text{-}Person$
$cp\text{-}OclIsTypeOf_{OclAny}\text{-}OclAny\text{-}OclAny$
$cp\text{-}OclIsTypeOf_{Person}\text{-}Person\text{-}Person$
$cp\text{-}OclIsTypeOf_{Person}\text{-}OclAny\text{-}OclAny$

$cp\text{-}OclIsTypeOf_{OclAny}\text{-}Person\text{-}OclAny$
$cp\text{-}OclIsTypeOf_{OclAny}\text{-}OclAny\text{-}Person$
$cp\text{-}OclIsTypeOf_{Person}\text{-}Person\text{-}OclAny$
$cp\text{-}OclIsTypeOf_{Person}\text{-}OclAny\text{-}Person$

Execution with Invalid or Null as Argument

lemma $OclIsTypeOf_{OclAny}\text{-}OclAny\text{-}strict1$[*simp*]:
$(invalid::OclAny)\ .oclIsTypeOf(OclAny) = invalid$
⟨proof⟩
lemma $OclIsTypeOf_{OclAny}\text{-}OclAny\text{-}strict2$[*simp*]:
$(null::OclAny)\ .oclIsTypeOf(OclAny) = true$
⟨proof⟩
lemma $OclIsTypeOf_{OclAny}\text{-}Person\text{-}strict1$[*simp*]:
$(invalid::Person)\ .oclIsTypeOf(OclAny) = invalid$

$\langle proof \rangle$
lemma $OclIsTypeOf_{OclAny}$*-Person-strict2*[*simp*]:
$(null::Person)\ .oclIsTypeOf(OclAny) = true$
$\langle proof \rangle$
lemma $OclIsTypeOf_{Person}$*-OclAny-strict1*[*simp*]:
$(invalid::OclAny)\ .oclIsTypeOf(Person) = invalid$
$\langle proof \rangle$
lemma $OclIsTypeOf_{Person}$*-OclAny-strict2*[*simp*]:
$(null::OclAny)\ .oclIsTypeOf(Person) = true$
$\langle proof \rangle$
lemma $OclIsTypeOf_{Person}$*-Person-strict1*[*simp*]:
$(invalid::Person)\ .oclIsTypeOf(Person) = invalid$
$\langle proof \rangle$
lemma $OclIsTypeOf_{Person}$*-Person-strict2*[*simp*]:
$(null::Person)\ .oclIsTypeOf(Person) = true$
$\langle proof \rangle$

Up Down Casting

lemma *actualType-larger-staticType*:
assumes *isdef*: $\tau \models (\delta\ X)$
shows $\tau \models (X::Person)\ .oclIsTypeOf(OclAny) \triangleq false$
$\langle proof \rangle$

lemma *down-cast-type*:
assumes *isOclAny*: $\tau \models (X::OclAny)\ .oclIsTypeOf(OclAny)$
and *non-null*: $\tau \models (\delta\ X)$
shows $\tau \models (X\ .oclAsType(Person)) \triangleq invalid$
$\langle proof \rangle$

lemma *down-cast-type'*:
assumes *isOclAny*: $\tau \models (X::OclAny)\ .oclIsTypeOf(OclAny)$
and *non-null*: $\tau \models (\delta\ X)$
shows $\tau \models not\ (\upsilon\ (X\ .oclAsType(Person)))$
$\langle proof \rangle$

lemma *up-down-cast* :
assumes *isdef*: $\tau \models (\delta\ X)$
shows $\tau \models ((X::Person)\ .oclAsType(OclAny)\ .oclAsType(Person) \triangleq X)$
$\langle proof \rangle$

lemma *up-down-cast-Person-OclAny-Person* [*simp*]:
shows $((X::Person)\ .oclAsType(OclAny)\ .oclAsType(Person) = X)$
$\langle proof \rangle$

lemma *up-down-cast-Person-OclAny-Person'*: **assumes** $\tau \models \upsilon\ X$
shows $\tau \models (((X :: Person)\ .oclAsType(OclAny)\ .oclAsType(Person)) \doteq X)$
$\langle proof \rangle$

lemma *up-down-cast-Person-OclAny-Person''*: **assumes** $\tau \models \upsilon\ (X :: Person)$
shows $\tau \models (X\ .oclIsTypeOf(Person)\ implies\ (X\ .oclAsType(OclAny)\ .oclAsType(Person)) \doteq X)$
$\langle proof \rangle$

6.1.6. OclIsKindOf

Definition

consts $OclIsKindOf_{OclAny} :: {}'\alpha \Rightarrow Boolean\ ((\text{-}).oclIsKindOf'(OclAny'))$
consts $OclIsKindOf_{Person} :: {}'\alpha \Rightarrow Boolean\ ((\text{-}).oclIsKindOf'(Person'))$

defs (**overloaded**) $OclIsKindOf_{OclAny}$-*OclAny*:
$$(X{::}OclAny)\ .oclIsKindOf(OclAny) \equiv (\lambda\tau.\ case\ X\ \tau\ of\ \bot \Rightarrow invalid\ \tau \mid \text{-} \Rightarrow true\ \tau)$$

defs (**overloaded**) $OclIsKindOf_{OclAny}$-*Person*:
$$(X{::}Person)\ .oclIsKindOf(OclAny) \equiv (\lambda\tau.\ case\ X\ \tau\ of\ \bot \Rightarrow invalid\ \tau \mid \text{-} \Rightarrow true\ \tau)$$

defs (**overloaded**) $OclIsKindOf_{Person}$-*OclAny*:
$$(X{::}OclAny)\ .oclIsKindOf(Person) \equiv (\lambda\tau.\ case\ X\ \tau\ of\ \bot \Rightarrow invalid\ \tau \mid \lfloor\bot\rfloor \Rightarrow true\ \tau \mid \lfloor\lfloor mk_{OclAny}\ oid\ \bot\ \rfloor\rfloor \Rightarrow false\ \tau \mid \lfloor\lfloor mk_{OclAny}\ oid\ \lfloor\text{-}\rfloor\ \rfloor\rfloor \Rightarrow true\ \tau)$$

defs (**overloaded**) $OclIsKindOf_{Person}$-*Person*:
$$(X{::}Person)\ .oclIsKindOf(Person) \equiv (\lambda\tau.\ case\ X\ \tau\ of\ \bot \Rightarrow invalid\ \tau \mid \text{-} \Rightarrow true\ \tau)$$

Context Passing

lemma *cp-*$OclIsKindOf_{OclAny}$*-Person-Person*: $cp\ P \Longrightarrow cp(\lambda X.(P(X{::}Person){::}Person).oclIsKindOf(OclAny))$
$\langle proof \rangle$
lemma *cp-*$OclIsKindOf_{OclAny}$*-OclAny-OclAny*: $cp\ P \Longrightarrow cp(\lambda X.(P(X{::}OclAny){::}OclAny).oclIsKindOf(OclAny))$
$\langle proof \rangle$
lemma *cp-*$OclIsKindOf_{Person}$*-Person-Person*: $cp\ P \Longrightarrow cp(\lambda X.(P(X{::}Person){::}Person).oclIsKindOf(Person))$
$\langle proof \rangle$

lemma *cp-OclIsKindOf*$_{Person}$*-OclAny-OclAny*: $cp\ P \Longrightarrow cp(\lambda X.(P(X::OclAny)::OclAny).oclIsKindOf(Person))$
⟨*proof*⟩

lemma *cp-OclIsKindOf*$_{OclAny}$*-Person-OclAny*: $cp\ P \Longrightarrow cp(\lambda X.(P(X::Person)::OclAny).oclIsKindOf(OclAny))$
⟨*proof*⟩
lemma *cp-OclIsKindOf*$_{OclAny}$*-OclAny-Person*: $cp\ P \Longrightarrow cp(\lambda X.(P(X::OclAny)::Person).oclIsKindOf(OclAny))$
⟨*proof*⟩
lemma *cp-OclIsKindOf*$_{Person}$*-Person-OclAny*: $cp\ P \Longrightarrow cp(\lambda X.(P(X::Person)::OclAny).oclIsKindOf(Person))$
⟨*proof*⟩
lemma *cp-OclIsKindOf*$_{Person}$*-OclAny-Person*: $cp\ P \Longrightarrow cp(\lambda X.(P(X::OclAny)::Person).oclIsKindOf(Person))$
⟨*proof*⟩

lemmas [*simp*] =
cp-OclIsKindOf$_{OclAny}$*-Person-Person*
cp-OclIsKindOf$_{OclAny}$*-OclAny-OclAny*
cp-OclIsKindOf$_{Person}$*-Person-Person*
cp-OclIsKindOf$_{Person}$*-OclAny-OclAny*

cp-OclIsKindOf$_{OclAny}$*-Person-OclAny*
cp-OclIsKindOf$_{OclAny}$*-OclAny-Person*
cp-OclIsKindOf$_{Person}$*-Person-OclAny*
cp-OclIsKindOf$_{Person}$*-OclAny-Person*

Execution with Invalid or Null as Argument

lemma *OclIsKindOf*$_{OclAny}$*-OclAny-strict1*[*simp*] : $(invalid::OclAny)\ .oclIsKindOf(OclAny) = invalid$
⟨*proof*⟩

lemma *OclIsKindOf*$_{OclAny}$*-OclAny-strict2*[*simp*] : $(null::OclAny)\ .oclIsKindOf(OclAny) = true$
⟨*proof*⟩

lemma *OclIsKindOf*$_{OclAny}$*-Person-strict1*[*simp*] : $(invalid::Person)\ .oclIsKindOf(OclAny) = invalid$
⟨*proof*⟩

lemma *OclIsKindOf*$_{OclAny}$*-Person-strict2*[*simp*] : $(null::Person)\ .oclIsKindOf(OclAny) = true$
⟨*proof*⟩

lemma *OclIsKindOf*$_{Person}$*-OclAny-strict1*[*simp*]: $(invalid::OclAny)\ .oclIsKindOf(Person) = invalid$
⟨*proof*⟩

lemma $\mathit{OclIsKindOf}_{\mathit{Person}}$*-OclAny-strict2*[*simp*]: (*null*::*OclAny*) *.oclIsKindOf*(*Person*) = *true*
⟨*proof*⟩

lemma $\mathit{OclIsKindOf}_{\mathit{Person}}$*-Person-strict1*[*simp*]: (*invalid*::*Person*) *.oclIsKindOf*(*Person*) = *invalid*
⟨*proof*⟩

lemma $\mathit{OclIsKindOf}_{\mathit{Person}}$*-Person-strict2*[*simp*]: (*null*::*Person*) *.oclIsKindOf*(*Person*) = *true*
⟨*proof*⟩

Up Down Casting

lemma *actualKind-larger-staticKind*:
assumes *isdef*: $\tau \models (\delta\ X)$
shows $\tau \models (X{::}\mathit{Person})\ .\mathit{oclIsKindOf}(\mathit{OclAny}) \triangleq \mathit{true}$
⟨*proof*⟩

lemma *down-cast-kind*:
assumes *isOclAny*: $\neg\ \tau \models (X{::}\mathit{OclAny})\ .\mathit{oclIsKindOf}(\mathit{Person})$
and *non-null*: $\tau \models (\delta\ X)$
shows $\tau \models (X\ .\mathit{oclAsType}(\mathit{Person})) \triangleq \mathit{invalid}$
⟨*proof*⟩

6.1.7. OclAllInstances

To denote OCL-types occuring 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 $\mathit{Person} \equiv \mathit{OclAsType}_{\mathit{Person}}\text{-}\mathfrak{A}$
definition $\mathit{OclAny} \equiv \mathit{OclAsType}_{\mathit{OclAny}}\text{-}\mathfrak{A}$
lemmas [*simp*] = *Person-def OclAny-def*

lemma $\mathit{OclAllInstances\text{-}generic}_{\mathit{OclAny}}$*-exec*: *OclAllInstances-generic pre-post OclAny* =
$(\lambda\tau.\ \ \mathit{Abs\text{-}Set\text{-}0}\ \ \lfloor\lfloor\ \mathit{Some}\ `\ \mathit{OclAny}\ `\ \mathit{ran}\ (\mathit{heap}\ (\mathit{pre\text{-}post}\ \tau))\ \rfloor\rfloor)$
⟨*proof*⟩

lemma $\mathit{OclAllInstances\text{-}at\text{-}post}_{\mathit{OclAny}}$*-exec*: *OclAny .allInstances*() =
$(\lambda\tau.\ \ \mathit{Abs\text{-}Set\text{-}0}\ \ \lfloor\lfloor\ \mathit{Some}\ `\ \mathit{OclAny}\ `\ \mathit{ran}\ (\mathit{heap}\ (\mathit{snd}\ \tau))\ \rfloor\rfloor)$
⟨*proof*⟩

lemma $\mathit{OclAllInstances\text{-}at\text{-}pre}_{\mathit{OclAny}}$*-exec*: *OclAny .allInstances@pre*() =
$(\lambda\tau.\ \ \mathit{Abs\text{-}Set\text{-}0}\ \ \lfloor\lfloor\ \mathit{Some}\ `\ \mathit{OclAny}\ `\ \mathit{ran}\ (\mathit{heap}\ (\mathit{fst}\ \tau))\ \rfloor\rfloor)$
⟨*proof*⟩

OclIsTypeOf

lemma $\mathit{OclAny\text{-}allInstances\text{-}generic\text{-}oclIsTypeOf}_{\mathit{OclAny}}\mathit{1}$:
assumes [*simp*]: $\bigwedge x.\ \mathit{pre\text{-}post}\ (x,\ x) = x$

shows $\exists \tau.\ (\tau \models ((OclAllInstances\text{-}generic\ \ pre\text{-}post\ \ OclAny) {-}{>} forAll(X|X\ .oclIsTypeOf(OclAny))))$
$\langle proof \rangle$

lemma $OclAny\text{-}allInstances\text{-}at\text{-}post\text{-}oclIsTypeOf_{OclAny}1$:
$\exists \tau.\ (\tau \models \quad (OclAny\ .allInstances() {-}{>} forAll(X|X\ .oclIsTypeOf(OclAny))))$
$\langle proof \rangle$

lemma $OclAny\text{-}allInstances\text{-}at\text{-}pre\text{-}oclIsTypeOf_{OclAny}1$:
$\exists \tau.\ (\tau \models \quad (OclAny\ .allInstances@pre() {-}{>} forAll(X|X\ .oclIsTypeOf(OclAny))))$
$\langle proof \rangle$

lemma $OclAny\text{-}allInstances\text{-}generic\text{-}oclIsTypeOf_{OclAny}2$:
assumes $[simp]$: $\bigwedge x.\ pre\text{-}post\ (x, x) = x$
shows $\exists \tau.\ (\tau \models not\ ((OclAllInstances\text{-}generic\ \ pre\text{-}post\ \ OclAny) {-}{>} forAll(X|X\ .oclIsTypeOf(OclAny))))$
$\langle proof \rangle$

lemma $OclAny\text{-}allInstances\text{-}at\text{-}post\text{-}oclIsTypeOf_{OclAny}2$:
$\exists \tau.\ (\tau \models not\ (OclAny\ .allInstances() {-}{>} forAll(X|X\ .oclIsTypeOf(OclAny))))$
$\langle proof \rangle$

lemma $OclAny\text{-}allInstances\text{-}at\text{-}pre\text{-}oclIsTypeOf_{OclAny}2$:
$\exists \tau.\ (\tau \models not\ (OclAny\ .allInstances@pre() {-}{>} forAll(X|X\ .oclIsTypeOf(OclAny))))$
$\langle proof \rangle$

lemma $Person\text{-}allInstances\text{-}generic\text{-}oclIsTypeOf_{Person}$:
$\tau \models ((OclAllInstances\text{-}generic\ pre\text{-}post\ Person) {-}{>} forAll(X|X\ .oclIsTypeOf(Person)))$
$\langle proof \rangle$

lemma $Person\text{-}allInstances\text{-}at\text{-}post\text{-}oclIsTypeOf_{Person}$:
$\tau \models (Person\ .allInstances() {-}{>} forAll(X|X\ .oclIsTypeOf(Person)))$
$\langle proof \rangle$

lemma $Person\text{-}allInstances\text{-}at\text{-}pre\text{-}oclIsTypeOf_{Person}$:
$\tau \models (Person\ .allInstances@pre() {-}{>} forAll(X|X\ .oclIsTypeOf(Person)))$
$\langle proof \rangle$

OclIsKindOf

lemma $OclAny\text{-}allInstances\text{-}generic\text{-}oclIsKindOf_{OclAny}$:
$\tau \models ((OclAllInstances\text{-}generic\ pre\text{-}post\ OclAny) {-}{>} forAll(X|X\ .oclIsKindOf(OclAny)))$
$\langle proof \rangle$

lemma $OclAny\text{-}allInstances\text{-}at\text{-}post\text{-}oclIsKindOf_{OclAny}$:
$\tau \models (OclAny\ .allInstances() {-}{>} forAll(X|X\ .oclIsKindOf(OclAny)))$
$\langle proof \rangle$

lemma $OclAny\text{-}allInstances\text{-}at\text{-}pre\text{-}oclIsKindOf_{OclAny}$:

$\tau \models (OclAny\ .allInstances@pre()\text{->}forAll(X|X\ .oclIsKindOf(OclAny)))$
⟨*proof*⟩

lemma *Person-allInstances-generic-oclIsKindOf*$_{OclAny}$:
$\tau \models ((OclAllInstances\text{-}generic\ pre\text{-}post\ Person)\text{->}forAll(X|X\ .oclIsKindOf(OclAny)))$
⟨*proof*⟩

lemma *Person-allInstances-at-post-oclIsKindOf*$_{OclAny}$:
$\tau \models (Person\ .allInstances()\text{->}forAll(X|X\ .oclIsKindOf(OclAny)))$
⟨*proof*⟩

lemma *Person-allInstances-at-pre-oclIsKindOf*$_{OclAny}$:
$\tau \models (Person\ .allInstances@pre()\text{->}forAll(X|X\ .oclIsKindOf(OclAny)))$
⟨*proof*⟩

lemma *Person-allInstances-generic-oclIsKindOf*$_{Person}$:
$\tau \models ((OclAllInstances\text{-}generic\ pre\text{-}post\ Person)\text{->}forAll(X|X\ .oclIsKindOf(Person)))$
⟨*proof*⟩

lemma *Person-allInstances-at-post-oclIsKindOf*$_{Person}$:
$\tau \models (Person\ .allInstances()\text{->}forAll(X|X\ .oclIsKindOf(Person)))$
⟨*proof*⟩

lemma *Person-allInstances-at-pre-oclIsKindOf*$_{Person}$:
$\tau \models (Person\ .allInstances@pre()\text{->}forAll(X|X\ .oclIsKindOf(Person)))$
⟨*proof*⟩

6.1.8. The Accessors (any, boss, salary)

Should be generated entirely from a class-diagram.

Definition (of the association Employee-Boss)

We start with a oid for the association; this oid can be used in presence of association classes to represent the association inside an object, pretty much similar to the Employee_DesignModel_UMLPart, where we stored an `oid` inside the class as “pointer.”

definition $oid_{Person}\mathcal{BOSS}$ *::oid* **where** $oid_{Person}\mathcal{BOSS} = 10$

From there on, we can already define an empty state which must contain for $oid_{Person}\mathcal{BOSS}$ the empty relation (encoded as association list, since there are associations with a Sequence-like structure).

definition *eval-extract* :: $('\mathfrak{A},('a::object)\ option\ option)\ val$
$\Rightarrow (oid \Rightarrow ('\mathfrak{A},'c::null)\ val)$
$\Rightarrow ('\mathfrak{A},'c::null)\ val$
where $eval\text{-}extract\ X\ f = (\lambda\ \tau.\ case\ X\ \tau\ of$
$\perp \Rightarrow invalid\ \tau \quad (*\ exception\ propagation\ *)$
$|\ \lfloor\ \perp\ \rfloor \Rightarrow invalid\ \tau\ (*\ dereferencing\ null\ pointer\ *)$

$| \lfloor\lfloor\ obj\ \rfloor\rfloor \Rightarrow f\ (oid\text{-}of\ obj)\ \tau)$

definition $choose_2\text{-}1 = fst$
definition $choose_2\text{-}2 = snd$
definition $choose_3\text{-}1 = fst$
definition $choose_3\text{-}2 = fst\ o\ snd$
definition $choose_3\text{-}3 = snd\ o\ snd$

definition $deref\text{-}assocs_2 :: ('\mathfrak{A}\ state \times '\mathfrak{A}\ state \Rightarrow '\mathfrak{A}\ state)$
$\Rightarrow (oid \times oid \Rightarrow oid \times oid)$
$\Rightarrow oid$
$\Rightarrow (oid\ list \Rightarrow oid \Rightarrow ('\mathfrak{A},'f)val)$
$\Rightarrow oid$
$\Rightarrow ('\mathfrak{A},\ 'f::null)val$
where $deref\text{-}assocs_2\ pre\text{-}post\ to\text{-}from\ assoc\text{-}oid\ f\ oid =$
$(\lambda\tau.\ case\ (assocs_2\ (pre\text{-}post\ \tau))\ assoc\text{-}oid\ of$
$\lfloor\ S\ \rfloor \Rightarrow f\ (map\ (choose_2\text{-}2 \circ to\text{-}from)$
$(filter\ (\lambda\ p.\ choose_2\text{-}1(to\text{-}from\ p){=}oid)\ S))$
$oid\ \tau$
$|\ \text{-} \quad \Rightarrow invalid\ \tau)$

The *pre-post*-parameter is configured with *fst* or *snd*, the *to-from*-parameter either with the identity *id* or the following combinator *switch*:

definition $switch_2\text{-}1 = id$
definition $switch_2\text{-}2 = (\lambda(x,y).\ (y,x))$
definition $switch_3\text{-}1 = id$
definition $switch_3\text{-}2 = (\lambda(x,y,z).\ (x,z,y))$
definition $switch_3\text{-}3 = (\lambda(x,y,z).\ (y,x,z))$
definition $switch_3\text{-}4 = (\lambda(x,y,z).\ (y,z,x))$
definition $switch_3\text{-}5 = (\lambda(x,y,z).\ (z,x,y))$
definition $switch_3\text{-}6 = (\lambda(x,y,z).\ (z,y,x))$

definition $select\text{-}object :: (('\mathfrak{A},\ 'b::null)val)$
$\Rightarrow (('\mathfrak{A},'b)val \Rightarrow ('\mathfrak{A},'c)val \Rightarrow ('\mathfrak{A},\ 'b)val)$
$\Rightarrow (('\mathfrak{A},\ 'b)val \Rightarrow ('\mathfrak{A},\ 'd)val)$
$\Rightarrow (oid \Rightarrow ('\mathfrak{A},'c::null)val)$
$\Rightarrow oid\ list$
$\Rightarrow oid$
$\Rightarrow ('\mathfrak{A},\ 'd)val$
where $select\text{-}object\ \ mt\ incl\ smash\ deref\ l\ oid\ = smash(foldl\ incl\ mt\ (map\ deref\ l))$
(* *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 $(select\text{-}object\ mtSet\ OclIncluding\ OclANY\ f\ \ l\ oid\ ){::}('\mathfrak{A},\ 'a{::}null)val$

definition $\mathit{deref\text{-}oid}_{Person}$ :: $(\mathfrak{A}\ \mathit{state} \times \mathfrak{A}\ \mathit{state} \Rightarrow \mathfrak{A}\ \mathit{state})$
$\Rightarrow (\mathit{type}_{Person} \Rightarrow (\mathfrak{A}, {'}c{::}\mathit{null})\mathit{val})$
$\Rightarrow \mathit{oid}$
$\Rightarrow (\mathfrak{A}, {'}c{::}\mathit{null})\mathit{val}$
where $\mathit{deref\text{-}oid}_{Person}\ \mathit{fst\text{-}snd}\ f\ \mathit{oid} = (\lambda\tau.\ \mathit{case}\ (\mathit{heap}\ (\mathit{fst\text{-}snd}\ \tau))\ \mathit{oid}\ \mathit{of}$
$\lfloor\ \mathit{in}_{Person}\ \mathit{obj}\ \rfloor \Rightarrow f\ \mathit{obj}\ \tau$
$\mid$ - $\Rightarrow \mathit{invalid}\ \tau)$

definition $\mathit{deref\text{-}oid}_{OclAny}$ :: $(\mathfrak{A}\ \mathit{state} \times \mathfrak{A}\ \mathit{state} \Rightarrow \mathfrak{A}\ \mathit{state})$
$\Rightarrow (\mathit{type}_{OclAny} \Rightarrow (\mathfrak{A}, {'}c{::}\mathit{null})\mathit{val})$
$\Rightarrow \mathit{oid}$
$\Rightarrow (\mathfrak{A}, {'}c{::}\mathit{null})\mathit{val}$
where $\mathit{deref\text{-}oid}_{OclAny}\ \mathit{fst\text{-}snd}\ f\ \mathit{oid} = (\lambda\tau.\ \mathit{case}\ (\mathit{heap}\ (\mathit{fst\text{-}snd}\ \tau))\ \mathit{oid}\ \mathit{of}$
$\lfloor\ \mathit{in}_{OclAny}\ \mathit{obj}\ \rfloor \Rightarrow f\ \mathit{obj}\ \tau$
$\mid$ - $\Rightarrow \mathit{invalid}\ \tau)$

pointer undefined in state or not referencing a type conform object representation

definition $\mathit{select}_{OclAny}\mathcal{ANY}\ f = (\lambda\ X.\ \mathit{case}\ X\ \mathit{of}$
$(\mathit{mk}_{OclAny}$ - $\perp) \Rightarrow \mathit{null}$
$\mid (\mathit{mk}_{OclAny}$ - $\lfloor \mathit{any} \rfloor) \Rightarrow f\ (\lambda x$ -. $\lfloor\lfloor x \rfloor\rfloor)\ \mathit{any})$

definition $\mathit{select}_{Person}\mathcal{BOSS}\ f = \mathit{select\text{-}object}\ \mathit{mtSet}\ \mathit{OclIncluding}\ \mathit{OclANY}\ (f\ (\lambda x$ -. $\lfloor\lfloor x \rfloor\rfloor))$

definition $\mathit{select}_{Person}\mathcal{SALARY}\ f = (\lambda\ X.\ \mathit{case}\ X\ \mathit{of}$
$(\mathit{mk}_{Person}$ - $\perp) \Rightarrow \mathit{null}$
$\mid (\mathit{mk}_{Person}$ - $\lfloor \mathit{salary} \rfloor) \Rightarrow f\ (\lambda x$ -. $\lfloor\lfloor x \rfloor\rfloor)\ \mathit{salary})$

definition $\mathit{deref\text{-}assocs}_2\mathcal{BOSS}\ \mathit{fst\text{-}snd}\ f = (\lambda\ \mathit{mk}_{Person}\ \mathit{oid}$ - $\Rightarrow$
$\mathit{deref\text{-}assocs}_2\ \mathit{fst\text{-}snd}\ \mathit{switch}_2\text{-}1\ \mathit{oid}_{Person}\mathcal{BOSS}\ f\ \mathit{oid})$

definition $\mathit{in\text{-}pre\text{-}state} = \mathit{fst}$
definition $\mathit{in\text{-}post\text{-}state} = \mathit{snd}$

definition $\mathit{reconst\text{-}basetype} = (\lambda\ \mathit{convert}\ x.\ \mathit{convert}\ x)$

definition $\mathit{dot}_{OclAny}\mathcal{ANY}$ :: $\mathit{OclAny} \Rightarrow$ - $((1(\text{-}).\mathit{any})\ 50)$
where $(X).\mathit{any} = \mathit{eval\text{-}extract}\ X$
$(\mathit{deref\text{-}oid}_{OclAny}\ \mathit{in\text{-}post\text{-}state}$
$(\mathit{select}_{OclAny}\mathcal{ANY}$
$\mathit{reconst\text{-}basetype}))$

definition $\mathit{dot}_{Person}\mathcal{BOSS}$ :: $\mathit{Person} \Rightarrow \mathit{Person}\ ((1(\text{-}).\mathit{boss})\ 50)$
where $(X).\mathit{boss} = \mathit{eval\text{-}extract}\ X$
$(\mathit{deref\text{-}oid}_{Person}\ \mathit{in\text{-}post\text{-}state}$

$(\mathit{deref\text{-}assocs_2}\mathcal{BOSS}\ \mathit{in\text{-}post\text{-}state}$
$(\mathit{select}_{Person}\mathcal{BOSS}$
$(\mathit{deref\text{-}oid}_{Person}\ \mathit{in\text{-}post\text{-}state}))))$

definition $\mathit{dot}_{Person}\mathcal{SALARY} :: \mathit{Person} \Rightarrow \mathit{Integer}\ \ ((1(\text{-}).\mathit{salary})\ 50)$
where $(X).\mathit{salary} = \mathit{eval\text{-}extract}\ X$
$(\mathit{deref\text{-}oid}_{Person}\ \mathit{in\text{-}post\text{-}state}$
$(\mathit{select}_{Person}\mathcal{SALARY}$
$\mathit{reconst\text{-}basetype}))$

definition $\mathit{dot}_{OclAny}\mathcal{ANY}\text{-}\mathit{at\text{-}pre} :: \mathit{OclAny} \Rightarrow \text{-}\ \ ((1(\text{-}).\mathit{any@pre})\ 50)$
where $(X).\mathit{any@pre} = \mathit{eval\text{-}extract}\ X$
$(\mathit{deref\text{-}oid}_{OclAny}\ \mathit{in\text{-}pre\text{-}state}$
$(\mathit{select}_{OclAny}\mathcal{ANY}$
$\mathit{reconst\text{-}basetype}))$

definition $\mathit{dot}_{Person}\mathcal{BOSS}\text{-}\mathit{at\text{-}pre}:: \mathit{Person} \Rightarrow \mathit{Person}\ \ ((1(\text{-}).\mathit{boss@pre})\ 50)$
where $(X).\mathit{boss@pre} = \mathit{eval\text{-}extract}\ X$
$(\mathit{deref\text{-}oid}_{Person}\ \mathit{in\text{-}pre\text{-}state}$
$(\mathit{deref\text{-}assocs_2}\mathcal{BOSS}\ \mathit{in\text{-}pre\text{-}state}$
$(\mathit{select}_{Person}\mathcal{BOSS}$
$(\mathit{deref\text{-}oid}_{Person}\ \mathit{in\text{-}pre\text{-}state}))))$

definition $\mathit{dot}_{Person}\mathcal{SALARY}\text{-}\mathit{at\text{-}pre}:: \mathit{Person} \Rightarrow \mathit{Integer}\ \ ((1(\text{-}).\mathit{salary@pre})\ 50)$
where $(X).\mathit{salary@pre} = \mathit{eval\text{-}extract}\ X$
$(\mathit{deref\text{-}oid}_{Person}\ \mathit{in\text{-}pre\text{-}state}$
$(\mathit{select}_{Person}\mathcal{SALARY}$
$\mathit{reconst\text{-}basetype}))$

lemmas $[\mathit{simp}] =$
$\mathit{dot}_{OclAny}\mathcal{ANY}\text{-}\mathit{def}$
$\mathit{dot}_{Person}\mathcal{BOSS}\text{-}\mathit{def}$
$\mathit{dot}_{Person}\mathcal{SALARY}\text{-}\mathit{def}$
$\mathit{dot}_{OclAny}\mathcal{ANY}\text{-}\mathit{at\text{-}pre\text{-}def}$
$\mathit{dot}_{Person}\mathcal{BOSS}\text{-}\mathit{at\text{-}pre\text{-}def}$
$\mathit{dot}_{Person}\mathcal{SALARY}\text{-}\mathit{at\text{-}pre\text{-}def}$

Context Passing

lemmas $[\mathit{simp}] = \mathit{eval\text{-}extract\text{-}def}$

lemma $\mathit{cp\text{-}dot}_{OclAny}\mathcal{ANY}$: $((X).\mathit{any})\ \tau = ((\lambda\text{-}.\ X\ \tau).\mathit{any})\ \tau\ \langle \mathit{proof}\rangle$
lemma $\mathit{cp\text{-}dot}_{Person}\mathcal{BOSS}$: $((X).\mathit{boss})\ \tau = ((\lambda\text{-}.\ X\ \tau).\mathit{boss})\ \tau\ \langle \mathit{proof}\rangle$
lemma $\mathit{cp\text{-}dot}_{Person}\mathcal{SALARY}$: $((X).\mathit{salary})\ \tau = ((\lambda\text{-}.\ X\ \tau).\mathit{salary})\ \tau\ \langle \mathit{proof}\rangle$

lemma $\mathit{cp\text{-}dot}_{OclAny}\mathcal{ANY}\text{-}\mathit{at\text{-}pre}$: $((X).\mathit{any@pre})\ \tau = ((\lambda\text{-}.\ X\ \tau).\mathit{any@pre})\ \tau\ \langle \mathit{proof}\rangle$
lemma $\mathit{cp\text{-}dot}_{Person}\mathcal{BOSS}\text{-}\mathit{at\text{-}pre}$: $((X).\mathit{boss@pre})\ \tau = ((\lambda\text{-}.\ X\ \tau).\mathit{boss@pre})\ \tau\ \langle \mathit{proof}\rangle$
lemma $\mathit{cp\text{-}dot}_{Person}\mathcal{SALARY}\text{-}\mathit{at\text{-}pre}$: $((X).\mathit{salary@pre})\ \tau = ((\lambda\text{-}.\ X\ \tau).\mathit{salary@pre})\ \tau\ \langle \mathit{proof}\rangle$

lemmas *cp-dot*$_{OclAny}\mathcal{ANY}$*-I* [*simp*, *intro*!]=
cp-dot$_{OclAny}\mathcal{ANY}$[*THEN allI*[*THEN allI*],
of λ *X* -. *X* λ - τ. τ, *THEN cpI1*]
lemmas *cp-dot*$_{OclAny}\mathcal{ANY}$*-at-pre-I* [*simp*, *intro*!]=
cp-dot$_{OclAny}\mathcal{ANY}$*-at-pre*[*THEN allI*[*THEN allI*],
of λ *X* -. *X* λ - τ. τ, *THEN cpI1*]

lemmas *cp-dot*$_{Person}\mathcal{BOSS}$*-I* [*simp*, *intro*!]=
cp-dot$_{Person}\mathcal{BOSS}$[*THEN allI*[*THEN allI*],
of λ *X* -. *X* λ - τ. τ, *THEN cpI1*]
lemmas *cp-dot*$_{Person}\mathcal{BOSS}$*-at-pre-I* [*simp*, *intro*!]=
cp-dot$_{Person}\mathcal{BOSS}$*-at-pre*[*THEN allI*[*THEN allI*],
of λ *X* -. *X* λ - τ. τ, *THEN cpI1*]

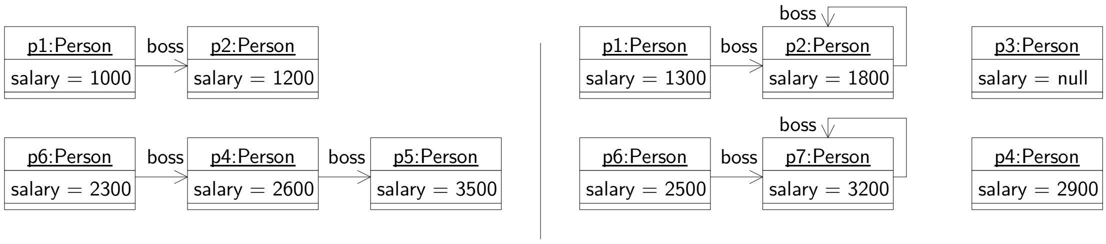
lemmas *cp-dot*$_{Person}\mathcal{SALARY}$*-I* [*simp*, *intro*!]=
cp-dot$_{Person}\mathcal{SALARY}$[*THEN allI*[*THEN allI*],
of λ *X* -. *X* λ - τ. τ, *THEN cpI1*]
lemmas *cp-dot*$_{Person}\mathcal{SALARY}$*-at-pre-I* [*simp*, *intro*!]=
cp-dot$_{Person}\mathcal{SALARY}$*-at-pre*[*THEN allI*[*THEN allI*],
of λ *X* -. *X* λ - τ. τ, *THEN cpI1*]

Execution with Invalid or Null as Argument

lemma *dot*$_{OclAny}\mathcal{ANY}$*-nullstrict* [*simp*]: (*null*).*any* = *invalid*
⟨*proof*⟩
lemma *dot*$_{OclAny}\mathcal{ANY}$*-at-pre-nullstrict* [*simp*] : (*null*).*any@pre* = *invalid*
⟨*proof*⟩
lemma *dot*$_{OclAny}\mathcal{ANY}$*-strict* [*simp*] : (*invalid*).*any* = *invalid*
⟨*proof*⟩
lemma *dot*$_{OclAny}\mathcal{ANY}$*-at-pre-strict* [*simp*] : (*invalid*).*any@pre* = *invalid*
⟨*proof*⟩

lemma *dot*$_{Person}\mathcal{BOSS}$*-nullstrict* [*simp*]: (*null*).*boss* = *invalid*
⟨*proof*⟩
lemma *dot*$_{Person}\mathcal{BOSS}$*-at-pre-nullstrict* [*simp*] : (*null*).*boss@pre* = *invalid*
⟨*proof*⟩
lemma *dot*$_{Person}\mathcal{BOSS}$*-strict* [*simp*] : (*invalid*).*boss* = *invalid*
⟨*proof*⟩
lemma *dot*$_{Person}\mathcal{BOSS}$*-at-pre-strict* [*simp*] : (*invalid*).*boss@pre* = *invalid*
⟨*proof*⟩

lemma *dot*$_{Person}\mathcal{SALARY}$*-nullstrict* [*simp*]: (*null*).*salary* = *invalid*
⟨*proof*⟩
lemma *dot*$_{Person}\mathcal{SALARY}$*-at-pre-nullstrict* [*simp*] : (*null*).*salary@pre* = *invalid*
⟨*proof*⟩
lemma *dot*$_{Person}\mathcal{SALARY}$*-strict* [*simp*] : (*invalid*).*salary* = *invalid*
⟨*proof*⟩



(a) (b)

Figure 6.2.: (a) pre-state σ_1 and (b) post-state σ_1'.

lemma $dot_{Person}\mathcal{SALARY}$*-at-pre-strict* [*simp*] : (*invalid*).*salary@pre* = *invalid*
⟨*proof*⟩

6.1.9. A Little Infra-structure on Example States

The example we are defining in this section comes from the figure 6.2.

definition *OclInt1000* (**1000**) **where** *OclInt1000* = (λ - . $\lfloor\lfloor 1000 \rfloor\rfloor$)
definition *OclInt1200* (**1200**) **where** *OclInt1200* = (λ - . $\lfloor\lfloor 1200 \rfloor\rfloor$)
definition *OclInt1300* (**1300**) **where** *OclInt1300* = (λ - . $\lfloor\lfloor 1300 \rfloor\rfloor$)
definition *OclInt1800* (**1800**) **where** *OclInt1800* = (λ - . $\lfloor\lfloor 1800 \rfloor\rfloor$)
definition *OclInt2600* (**2600**) **where** *OclInt2600* = (λ - . $\lfloor\lfloor 2600 \rfloor\rfloor$)
definition *OclInt2900* (**2900**) **where** *OclInt2900* = (λ - . $\lfloor\lfloor 2900 \rfloor\rfloor$)
definition *OclInt3200* (**3200**) **where** *OclInt3200* = (λ - . $\lfloor\lfloor 3200 \rfloor\rfloor$)
definition *OclInt3500* (**3500**) **where** *OclInt3500* = (λ - . $\lfloor\lfloor 3500 \rfloor\rfloor$)

definition *oid0* ≡ *0*
definition *oid1* ≡ *1*
definition *oid2* ≡ *2*
definition *oid3* ≡ *3*
definition *oid4* ≡ *4*
definition *oid5* ≡ *5*
definition *oid6* ≡ *6*
definition *oid7* ≡ *7*
definition *oid8* ≡ *8*

definition *person1* ≡ mk_{Person} *oid0* $\lfloor 1300 \rfloor$
definition *person2* ≡ mk_{Person} *oid1* $\lfloor 1800 \rfloor$
definition *person3* ≡ mk_{Person} *oid2 None*
definition *person4* ≡ mk_{Person} *oid3* $\lfloor 2900 \rfloor$
definition *person5* ≡ mk_{Person} *oid4* $\lfloor 3500 \rfloor$
definition *person6* ≡ mk_{Person} *oid5* $\lfloor 2500 \rfloor$
definition *person7* ≡ mk_{OclAny} *oid6* $\lfloor\lfloor 3200 \rfloor\rfloor$
definition *person8* ≡ mk_{OclAny} *oid7 None*
definition *person9* ≡ mk_{Person} *oid8* $\lfloor 0 \rfloor$

definition

$\sigma_1 \equiv (\!|$ *heap* $=$ *empty*$($*oid0* $\mapsto in_{Person}$ $(mk_{Person}$ *oid0* $\lfloor 1000 \rfloor))$
$($*oid1* $\mapsto in_{Person}$ $(mk_{Person}$ *oid1* $\lfloor 1200 \rfloor))$
$(*$*oid2*$*)$
$($*oid3* $\mapsto in_{Person}$ $(mk_{Person}$ *oid3* $\lfloor 2600 \rfloor))$
$($*oid4* $\mapsto in_{Person}$ *person5*$)$
$($*oid5* $\mapsto in_{Person}$ $(mk_{Person}$ *oid5* $\lfloor 2300 \rfloor))$
$(*$*oid6*$*)$
$(*$*oid7*$*)$
$($*oid8* $\mapsto in_{Person}$ *person9*$)$,
$assocs_2$ $=$ *empty*$(oid_{Person}\mathcal{BOSS} \mapsto [($*oid0*,*oid1*$)$,$($*oid3*,*oid4*$)$,$($*oid5*,*oid3*$)])$,
$assocs_3$ $=$ *empty* $|\!)$

definition
$\sigma_1{}' \equiv (\!|$ *heap* $=$ *empty*$($*oid0* $\mapsto in_{Person}$ *person1*$)$
$($*oid1* $\mapsto in_{Person}$ *person2*$)$
$($*oid2* $\mapsto in_{Person}$ *person3*$)$
$($*oid3* $\mapsto in_{Person}$ *person4*$)$
$(*$*oid4*$*)$
$($*oid5* $\mapsto in_{Person}$ *person6*$)$
$($*oid6* $\mapsto in_{OclAny}$ *person7*$)$
$($*oid7* $\mapsto in_{OclAny}$ *person8*$)$
$($*oid8* $\mapsto in_{Person}$ *person9*$)$,
$assocs_2$ $=$ *empty*$(oid_{Person}\mathcal{BOSS} \mapsto$
$[($*oid0*,*oid1*$)$,$($*oid1*,*oid1*$)$,$($*oid5*,*oid6*$)$,$($*oid6*,*oid6*$)])$,
$assocs_3$ $=$ *empty* $|\!)$

definition $\sigma_0 \equiv (\!|$ *heap* $=$ *empty*, $assocs_2$ $=$ *empty*, $assocs_3$ $=$ *empty* $|\!)$

lemma *basic-τ-wff*: *WFF*$(\sigma_1,\sigma_1{}')$
⟨*proof*⟩

lemma [*simp*,*code-unfold*]: *dom* (*heap* σ_1) $=$ {*oid0*,*oid1*,(*,*oid2**)*oid3*,*oid4*,*oid5*(*,*oid6*,*oid7**),*oid8*}
⟨*proof*⟩

lemma [*simp*,*code-unfold*]: *dom* (*heap* $\sigma_1{}'$) $=$ {*oid0*,*oid1*,*oid2*,*oid3*,(*,*oid4**)*oid5*,*oid6*,*oid7*,*oid8*}
⟨*proof*⟩

definition $X_{Person}1$ :: *Person* $\equiv \lambda$ - .$\lfloor\lfloor$ *person1* $\rfloor\rfloor$
definition $X_{Person}2$ :: *Person* $\equiv \lambda$ - .$\lfloor\lfloor$ *person2* $\rfloor\rfloor$
definition $X_{Person}3$ :: *Person* $\equiv \lambda$ - .$\lfloor\lfloor$ *person3* $\rfloor\rfloor$
definition $X_{Person}4$ :: *Person* $\equiv \lambda$ - .$\lfloor\lfloor$ *person4* $\rfloor\rfloor$
definition $X_{Person}5$ :: *Person* $\equiv \lambda$ - .$\lfloor\lfloor$ *person5* $\rfloor\rfloor$
definition $X_{Person}6$ :: *Person* $\equiv \lambda$ - .$\lfloor\lfloor$ *person6* $\rfloor\rfloor$
definition $X_{Person}7$ :: *OclAny* $\equiv \lambda$ - .$\lfloor\lfloor$ *person7* $\rfloor\rfloor$
definition $X_{Person}8$ :: *OclAny* $\equiv \lambda$ - .$\lfloor\lfloor$ *person8* $\rfloor\rfloor$
definition $X_{Person}9$ :: *Person* $\equiv \lambda$ - .$\lfloor\lfloor$ *person9* $\rfloor\rfloor$

lemma [*code-unfold*]: $((x::Person) \doteq y) = StrictRefEq_{Object}\ x\ y$ ⟨*proof*⟩

lemma [*code-unfold*]: $((x::OclAny) \doteq y) = StrictRefEq_{Object}\ x\ y$ ⟨*proof*⟩

lemmas [*simp*,*code-unfold*] =
$OclAsType_{OclAny}$-*OclAny*
$OclAsType_{OclAny}$-*Person*
$OclAsType_{Person}$-*OclAny*
$OclAsType_{Person}$-*Person*

$OclIsTypeOf_{OclAny}$-*OclAny*
$OclIsTypeOf_{OclAny}$-*Person*
$OclIsTypeOf_{Person}$-*OclAny*
$OclIsTypeOf_{Person}$-*Person*

$OclIsKindOf_{OclAny}$-*OclAny*
$OclIsKindOf_{OclAny}$-*Person*
$OclIsKindOf_{Person}$-*OclAny*
$OclIsKindOf_{Person}$-*Person*

value $\bigwedge s_{pre}\ .\ (s_{pre},\sigma_1') \models (X_{Person}1\ .salary <> \mathbf{1000})$
value $\bigwedge s_{pre}\ .\ (s_{pre},\sigma_1') \models (X_{Person}1\ .salary \doteq \mathbf{1300})$
value $\bigwedge s_{post}.\ (\sigma_1,s_{post}) \models (X_{Person}1\ .salary@pre \doteq \mathbf{1000})$
value $\bigwedge s_{post}.\ (\sigma_1,s_{post}) \models (X_{Person}1\ .salary@pre <> \mathbf{1300})$

lemma $(\sigma_1,\sigma_1') \models (X_{Person}1\ .oclIsMaintained())$
⟨*proof*⟩

lemma $\bigwedge s_{pre}\ s_{post}.\ (s_{pre},s_{post}) \models ((X_{Person}1\ .oclAsType(OclAny)\ .oclAsType(Person)) \doteq X_{Person}1)$
⟨*proof*⟩
value $\bigwedge s_{pre}\ s_{post}.\ (s_{pre},s_{post}) \models (X_{Person}1\ .oclIsTypeOf(Person))$
value $\bigwedge s_{pre}\ s_{post}.\ (s_{pre},s_{post}) \models not(X_{Person}1\ .oclIsTypeOf(OclAny))$
value $\bigwedge s_{pre}\ s_{post}.\ (s_{pre},s_{post}) \models (X_{Person}1\ .oclIsKindOf(Person))$
value $\bigwedge s_{pre}\ s_{post}.\ (s_{pre},s_{post}) \models (X_{Person}1\ .oclIsKindOf(OclAny))$
value $\bigwedge s_{pre}\ s_{post}.\ (s_{pre},s_{post}) \models not(X_{Person}1\ .oclAsType(OclAny)\ .oclIsTypeOf(OclAny))$

value $\bigwedge s_{pre}\ .\ (s_{pre},\sigma_1') \models (X_{Person}2\ .salary \doteq \mathbf{1800})$
value $\bigwedge s_{post}.\ (\sigma_1,s_{post}) \models (X_{Person}2\ .salary@pre \doteq \mathbf{1200})$
lemma $(\sigma_1,\sigma_1') \models (X_{Person}2\ .oclIsMaintained())$
⟨*proof*⟩

value $\bigwedge s_{pre}\ .\ (s_{pre},\sigma_1') \models (X_{Person}3\ .salary \doteq null)$
value $\bigwedge s_{post}.\ (\sigma_1,s_{post}) \models not(\upsilon(X_{Person}3\ .salary@pre))$
lemma $(\sigma_1,\sigma_1') \models (X_{Person}3\ .oclIsNew())$
⟨*proof*⟩

lemma $(\sigma_1,\sigma_1') \models (X_{Person}4\ .oclIsMaintained())$
⟨*proof*⟩

value $\bigwedge s_{pre}\ .\ (s_{pre},\sigma_1') \models not(\upsilon(X_{Person}5\ .salary))$
value $\bigwedge\ s_{post}.\ (\sigma_1,s_{post}) \models (X_{Person}5\ .salary@pre \doteq \mathbf{3500})$
lemma $(\sigma_1,\sigma_1') \models (X_{Person}5\ .oclIsDeleted())$
⟨*proof*⟩

lemma $(\sigma_1,\sigma_1') \models (X_{Person}6\ .oclIsMaintained())$
⟨*proof*⟩

value $\bigwedge s_{pre}\ s_{post}.\ (s_{pre},s_{post}) \models \upsilon(X_{Person}7\ .oclAsType(Person))$
lemma $\bigwedge s_{pre}\ s_{post}.\ (s_{pre},s_{post}) \models ((X_{Person}7\ .oclAsType(Person)\ .oclAsType(OclAny)$
$.oclAsType(Person))$
$\doteq (X_{Person}7\ .oclAsType(Person)))$
⟨*proof*⟩
lemma $(\sigma_1,\sigma_1') \models (X_{Person}7\ .oclIsNew())$
⟨*proof*⟩

value $\bigwedge s_{pre}\ s_{post}.\ (s_{pre},s_{post}) \models (X_{Person}8\ <> X_{Person}7)$
value $\bigwedge s_{pre}\ s_{post}.\ (s_{pre},s_{post}) \models not(\upsilon(X_{Person}8\ .oclAsType(Person)))$
value $\bigwedge s_{pre}\ s_{post}.\ (s_{pre},s_{post}) \models (X_{Person}8\ .oclIsTypeOf(OclAny))$
value $\bigwedge s_{pre}\ s_{post}.\ (s_{pre},s_{post}) \models not(X_{Person}8\ .oclIsTypeOf(Person))$
value $\bigwedge s_{pre}\ s_{post}.\ (s_{pre},s_{post}) \models not(X_{Person}8\ .oclIsKindOf(Person))$
value $\bigwedge s_{pre}\ s_{post}.\ (s_{pre},s_{post}) \models (X_{Person}8\ .oclIsKindOf(OclAny))$

lemma σ-*modifiedonly*: $(\sigma_1,\sigma_1') \models (Set\{\ X_{Person}1\ .oclAsType(OclAny)$
$,\ X_{Person}2\ .oclAsType(OclAny)$
$(*,\ X_{Person}3\ .oclAsType(OclAny)*)$
$,\ X_{Person}4\ .oclAsType(OclAny)$
$(*,\ X_{Person}5\ .oclAsType(OclAny)*)$
$,\ X_{Person}6\ .oclAsType(OclAny)$
$(*,\ X_{Person}7\ .oclAsType(OclAny)*)$
$(*,\ X_{Person}8\ .oclAsType(OclAny)*)$
$(*,\ X_{Person}9\ .oclAsType(OclAny)*)\}{-}{>}oclIsModifiedOnly())$
⟨*proof*⟩

lemma $(\sigma_1,\sigma_1') \models ((X_{Person}9\ @pre\ (\lambda x.\ \lfloor OclAsType_{Person}\text{-}\mathfrak{A}\ x\rfloor))\ \triangleq X_{Person}9)$
⟨*proof*⟩

lemma $(\sigma_1,\sigma_1{}') \models ((X_{Person}9 \text{ @}post\ (\lambda x.\ \lfloor OclAsType_{Person}\text{-}\mathfrak{A}\ x\rfloor))\ \triangleq X_{Person}9)$
⟨*proof*⟩

lemma $(\sigma_1,\sigma_1{}') \models (((X_{Person}9\ .oclAsType(OclAny))\ \text{@}pre\ (\lambda x.\ \lfloor OclAsType_{OclAny}\text{-}\mathfrak{A}\ x\rfloor)) \triangleq$
$((X_{Person}9\ .oclAsType(OclAny))\ \text{@}post\ (\lambda x.\ \lfloor OclAsType_{OclAny}\text{-}\mathfrak{A}\ x\rfloor)))$
⟨*proof*⟩

lemma *perm-*$\sigma_1{}'$: $\sigma_1{}' = (\!|\ heap = empty$
$(oid8 \mapsto in_{Person}\ person9)$
$(oid7 \mapsto in_{OclAny}\ person8)$
$(oid6 \mapsto in_{OclAny}\ person7)$
$(oid5 \mapsto in_{Person}\ person6)$
$(*oid4*)$
$(oid3 \mapsto in_{Person}\ person4)$
$(oid2 \mapsto in_{Person}\ person3)$
$(oid1 \mapsto in_{Person}\ person2)$
$(oid0 \mapsto in_{Person}\ person1)$
$,\ assocs_2 = assocs_2\ \sigma_1{}'$
$,\ assocs_3 = assocs_3\ \sigma_1{}'\ |\!)$
⟨*proof*⟩

declare *const-ss* [*simp*]

lemma $\bigwedge\sigma_1.$
$(\sigma_1,\sigma_1{}') \models (Person\ .allInstances() \doteq Set\{\ X_{Person}1,\ X_{Person}2,\ X_{Person}3,\ X_{Person}4(*,$
$X_{Person}5*),\ X_{Person}6,$
$X_{Person}7\ .oclAsType(Person)(*,\ X_{Person}8*),\ X_{Person}9\ \})$
⟨*proof*⟩

lemma $\bigwedge\sigma_1.$
$(\sigma_1,\sigma_1{}') \models (OclAny\ .allInstances() \doteq Set\{\ X_{Person}1\ .oclAsType(OclAny),\ X_{Person}2$
$.oclAsType(OclAny),$
$X_{Person}3\ .oclAsType(OclAny),\ X_{Person}4\ .oclAsType(OclAny)$
$(*,\ X_{Person}5*),\ X_{Person}6\ .oclAsType(OclAny),$
$X_{Person}7,\ X_{Person}8,\ X_{Person}9\ .oclAsType(OclAny)\ \})$
⟨*proof*⟩

end

6.2. The Employee Analysis Model (OCL)

theory
Employee-AnalysisModel-OCLPart
imports
Employee-AnalysisModel-UMLPart
begin

6.2.1. Standard State Infrastructure

Ideally, these definitions are automatically generated from the class model.

6.2.2. Invariant

These recursive predicates can be defined conservatively by greatest fix-point constructions—automatically. See [4, 6] for details. For the purpose of this example, we state them as axioms here.

axiomatization *inv-Person* :: *Person* $\Rightarrow$ *Boolean*
where $A : (\tau \models (\delta\ self)) \longrightarrow$
$(\tau \models inv\text{-}Person(self)) =$
$((\tau \models (self\ .boss \doteq null)) \vee$
$(\ \tau \models (self\ .boss <> null) \wedge (\tau \models ((self\ .salary)\ \ `\leq\ \ (self\ .boss\ .salary)))\ \ \wedge$
$(\tau \models (inv\text{-}Person(self\ .boss)))))$

axiomatization *inv-Person-at-pre* :: *Person* $\Rightarrow$ *Boolean*
where $B : (\tau \models (\delta\ self)) \longrightarrow$
$(\tau \models inv\text{-}Person\text{-}at\text{-}pre(self)) =$
$((\tau \models (self\ .boss@pre \doteq null)) \vee$
$(\ \tau \models (self\ .boss@pre <> null) \wedge$
$(\tau \models (self\ .boss@pre\ .salary@pre\ `\leq self\ .salary@pre))\ \ \wedge$
$(\tau \models (inv\text{-}Person\text{-}at\text{-}pre(self\ .boss@pre)))))$

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* $\Rightarrow$ $(\mathfrak{A})st \Rightarrow$ *bool* **where**
$(\tau \models (\delta\ self)) \Longrightarrow ((\tau \models (self\ .boss \doteq null)) \vee$
$(\tau \models (self\ .boss <> null) \wedge (\tau \models (self\ .boss\ .salary\ `\leq self\ .salary))\ \ \wedge$
$(\ (inv(self\ .boss))\tau\ )))$
$\Longrightarrow (\ inv\ self\ \tau)$

6.2.3. The Contract of a Recursive Query

The original specification of a recursive query :

```
context Person::contents():Set(Integer)
post:  result = if self.boss = null
                then Set{i}
                else self.boss.contents()->including(i)
                endif
```

consts *dot-contents* :: *Person* $\Rightarrow$ *Set-Integer* $((1(\text{-}).contents'(')) \ 50)$

axiomatization where *dot-contents-def*:
$(\tau \models ((self).contents() \triangleq result)) =$
$(if\ (\delta\ self)\ \tau = true\ \tau$
$then\ ((\tau \models true) \wedge$

$(\tau \models (result \triangleq if\ \ (self\ \ .boss \doteq null)$
$then\ \ (Set\{self\ \ .salary\})$
$else\ \ (self\ \ .boss\ \ .contents() -> including(self\ \ .salary))$
$endif)))$
$else\ \tau \models result \triangleq invalid)$

consts *dot-contents-AT-pre* :: *Person* ⇒ *Set-Integer* ((*1*(-).*contents*@*pre*′(′)) *50*)

axiomatization where *dot-contents-AT-pre-def*:
$(\tau \models (self).contents@pre() \triangleq result) =$
$(if\ \ (\delta\ self)\ \tau = true\ \tau$
$then\ \tau \models true \wedge \qquad (*\ pre\ *)$
$\tau \models (result \triangleq if\ \ (self).boss@pre \doteq null\ \ (*\ post\ *)$
$then\ Set\{(self).salary@pre\}$
$else\ \ (self).boss@pre\ \ .contents@pre() -> including(self\ \ .salary@pre)$
$endif)$
$else\ \tau \models result \triangleq invalid)$

These `@pre` variants on methods are only available on queries, i. e., operations without side-effect.

6.2.4. The Contract of a Method

The specification in high-level OCL input syntax reads as follows:

```
context Person::insert(x:Integer)
post: contents():Set(Integer)
contents() = contents@pre()->including(x)
```

consts *dot-insert* :: *Person* ⇒ *Integer* ⇒ *Void* ((*1*(-).*insert*′(-′)) *50*)

axiomatization where *dot-insert-def*:
$(\tau \models ((self).insert(x) \triangleq result)) =$
$(if\ \ (\delta\ self)\ \tau = true\ \tau \wedge (\upsilon\ x)\ \tau = true\ \tau$
$then\ \tau \models true \wedge$
$\tau \models ((self).contents() \triangleq (self).contents@pre() -> including(x))$
$else\ \tau \models ((self).insert(x) \triangleq invalid))$

end

7. The Employee Design Model

7.1. The Employee Design Model (UML)

theory
Employee-DesignModel-UMLPart
imports
../OCL-main
begin

7.1.1. Introduction

For certain concepts like classes and class-types, only a generic definition for its resulting semantics can be given. Generic means, there is a function outside HOL that "compiles" a concrete, closed-world class diagram into a "theory" of this data model, consisting of a bunch of definitions for classes, accessors, method, casts, and tests for actual types, as well as proofs for the fundamental properties of these operations in this concrete data model.

Such generic function or "compiler" can be implemented in Isabelle on the ML level. This has been done, for a semantics following the open-world assumption, for UML 2.0 in [4, 7]. In this paper, we follow another approach for UML 2.4: we define the concepts of the compilation informally, and present a concrete example which is verified in Isabelle/HOL.

Outlining the Example

We are presenting here a "design-model" of the (slightly modified) example Figure 7.3, page 20 of the OCL standard [33]. To be precise, this theory contains the formalization of the data-part covered by the UML class model (see Figure 7.1):

This means that the association (attached to the association class `EmployeeRanking`) with the association ends `boss` and `employees` is implemented by the attribute `boss` and the operation `employees` (to be discussed in the OCL part captured by the subsequent theory).

7.1.2. Example Data-Universe and its Infrastructure

Ideally, the following is generated automatically from a UML class model.

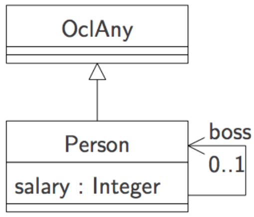


Figure 7.1.: A simple UML class model drawn from Figure 7.3, page 20 of [33].

Our data universe consists in the concrete class diagram just of node's, and implicitly of the class object. Each class implies the existence of a class type defined for the corresponding object representations as follows:

datatype $\mathit{type}_{Person} = \mathit{mk}_{Person}\ \mathit{oid}$
$\quad\quad\quad\quad \mathit{int\ option}$
$\quad\quad\quad\quad \mathit{oid\ option}$

datatype $\mathit{type}_{OclAny} = \mathit{mk}_{OclAny}\ \mathit{oid}$
$\quad\quad\quad\quad (\mathit{int\ option} \times \mathit{oid\ option})\ \mathit{option}$

Now, we construct a concrete "universe of OclAny types" by injection into a sum type containing the class types. This type of OclAny will be used as instance for all respective type-variables.

datatype $\mathfrak{A} = \mathit{in}_{Person}\ \mathit{type}_{Person} \mid \mathit{in}_{OclAny}\ \mathit{type}_{OclAny}$

Having fixed the object universe, we can introduce type synonyms that exactly correspond to OCL types. Again, we exploit that our representation of OCL is a "shallow embedding" with a one-to-one correspondance of OCL-types to types of the meta-language HOL.

type-synonym $\mathit{Boolean} = \mathfrak{A}\ \mathit{Boolean}$
type-synonym $\mathit{Integer} = \mathfrak{A}\ \mathit{Integer}$
type-synonym $\mathit{Void} = \mathfrak{A}\ \mathit{Void}$
type-synonym $\mathit{OclAny} = (\mathfrak{A}, \mathit{type}_{OclAny}\ \mathit{option\ option})\ \mathit{val}$
type-synonym $\mathit{Person} = (\mathfrak{A}, \mathit{type}_{Person}\ \mathit{option\ option})\ \mathit{val}$
type-synonym $\mathit{Set\text{-}Integer} = (\mathfrak{A}, \mathit{int\ option\ option})\ \mathit{Set}$
type-synonym $\mathit{Set\text{-}Person} = (\mathfrak{A}, \mathit{type}_{Person}\ \mathit{option\ option})\ \mathit{Set}$

Just a little check:

typ *Boolean*

To reuse key-elements of the library like referential equality, we have to show that the object universe belongs to the type class "oclany," i. e., each class type has to provide a function *oid-of* yielding the object id (oid) of the object.

instantiation $type_{Person}$ :: *object*
begin
  definition *oid-of-type*$_{Person}$*-def*: *oid-of* x = (*case* x *of* mk_{Person} *oid* - - $\Rightarrow$ *oid*)
  instance ⟨*proof*⟩
end

instantiation $type_{OclAny}$ :: *object*
begin
  definition *oid-of-type*$_{OclAny}$*-def*: *oid-of* x = (*case* x *of* mk_{OclAny} *oid* - $\Rightarrow$ *oid*)
  instance ⟨*proof*⟩
end

instantiation $\mathfrak{A}$ :: *object*
begin
  definition *oid-of-*$\mathfrak{A}$*-def*: *oid-of* x = (*case* x *of*
    in_{Person} *person* $\Rightarrow$ *oid-of person*
    | in_{OclAny} *oclany* $\Rightarrow$ *oid-of oclany*)
  instance ⟨*proof*⟩
end

7.1.3. Instantiation of the Generic Strict Equality

We instantiate the referential equality on *Person* and *OclAny*

defs(**overloaded**) $StrictRefEq_{Object}$*-*$_{Person}$: $(x::Person) \doteq y \equiv StrictRefEq_{Object}\ x\ y$
defs(**overloaded**) $StrictRefEq_{Object}$*-*$_{OclAny}$: $(x::OclAny) \doteq y \equiv StrictRefEq_{Object}\ x\ y$

lemmas
  cp-$StrictRefEq_{Object}$[*of* x::*Person* y::*Person* τ,
    simplified $StrictRefEq_{Object}$*-*$_{Person}$[*symmetric*]]
  cp-intro(*9*) [*of* P::*Person* $\Rightarrow$*Person*Q::*Person* $\Rightarrow$*Person*,
    simplified $StrictRefEq_{Object}$*-*$_{Person}$[*symmetric*]]
  $StrictRefEq_{Object}$*-def* [*of* x::*Person* y::*Person*,
    simplified $StrictRefEq_{Object}$*-*$_{Person}$[*symmetric*]]
  $StrictRefEq_{Object}$*-defargs* [*of* - x::*Person* y::*Person*,
    simplified $StrictRefEq_{Object}$*-*$_{Person}$[*symmetric*]]
  $StrictRefEq_{Object}$*-strict1*
    [*of* x::*Person*,
    simplified $StrictRefEq_{Object}$*-*$_{Person}$[*symmetric*]]
  $StrictRefEq_{Object}$*-strict2*
    [*of* x::*Person*,
    simplified $StrictRefEq_{Object}$*-*$_{Person}$[*symmetric*]]

For each Class C, we will have a casting operation `.oclAsType(`C`)`, a test on the actual type `.oclIsTypeOf(`C`)` as well as its relaxed form `.oclIsKindOf(`C`)` (corresponding exactly to Java's `instanceof`-operator.

Thus, since we have two class-types in our concrete class hierarchy, we have two operations to declare and to provide two overloading definitions for the two static types.

7.1.4. OclAsType

Definition

consts $OclAsType_{OclAny}$ :: $'\alpha \Rightarrow OclAny$ ((-) *.oclAsType'(OclAny')*)
consts $OclAsType_{Person}$ :: $'\alpha \Rightarrow Person$ ((-) *.oclAsType'(Person')*)

definition $OclAsType_{OclAny}$-$\mathfrak{A}$ = ($\lambda u.$ $\lfloor$*case u of* in_{OclAny} $a \Rightarrow a$
$\quad | \ in_{Person}\ (mk_{Person}\ oid\ a\ b) \Rightarrow mk_{OclAny}\ oid\ \lfloor(a,b)\rfloor\rfloor)$

lemma $OclAsType_{OclAny}$-$\mathfrak{A}$-*some*: $OclAsType_{OclAny}$-$\mathfrak{A}$ $x \neq None$
⟨*proof*⟩

defs (**overloaded**) $OclAsType_{OclAny}$-*OclAny*:
$(X::OclAny)$ *.oclAsType*$(OclAny) \equiv X$

defs (**overloaded**) $OclAsType_{OclAny}$-*Person*:
$(X::Person)$ *.oclAsType*$(OclAny) \equiv$
$(\lambda\tau.$ *case* $X\ \tau$ *of*
$\quad \bot \quad \Rightarrow invalid\ \tau$
$\quad | \lfloor\bot\rfloor \Rightarrow null\ \tau$
$\quad | \lfloor\lfloor mk_{Person}\ oid\ a\ b\ \rfloor\rfloor \Rightarrow\ \lfloor\lfloor\ (mk_{OclAny}\ oid\ \lfloor(a,b)\rfloor)\ \rfloor\rfloor)$

definition $OclAsType_{Person}$-$\mathfrak{A}$ = ($\lambda u.$ *case u of* $in_{Person}\ p \Rightarrow \lfloor p\rfloor$
$\quad | \ in_{OclAny}\ (mk_{OclAny}\ oid\ \lfloor(a,b)\rfloor) \Rightarrow \lfloor mk_{Person}\ oid\ a\ b\rfloor$
$\quad | \ \text{-} \Rightarrow None)$

defs (**overloaded**) $OclAsType_{Person}$-*OclAny*:
$(X::OclAny)$ *.oclAsType*$(Person) \equiv$
$(\lambda\tau.$ *case* $X\ \tau$ *of*
$\quad \bot \quad \Rightarrow invalid\ \tau$
$\quad | \lfloor\bot\rfloor \Rightarrow null\ \tau$
$\quad | \lfloor\lfloor mk_{OclAny}\ oid\ \bot\ \rfloor\rfloor \Rightarrow\ invalid\ \tau \quad (*\ down{-}cast\ exception\ *)$
$\quad | \lfloor\lfloor mk_{OclAny}\ oid\ \lfloor(a,b)\rfloor\ \rfloor\rfloor \Rightarrow\ \lfloor\lfloor mk_{Person}\ oid\ a\ b\ \rfloor\rfloor)$

defs (**overloaded**) $OclAsType_{Person}$-*Person*:
$(X::Person)$ *.oclAsType*$(Person) \equiv X$

lemmas [*simp*] =
$OclAsType_{OclAny}$-*OclAny*
$OclAsType_{Person}$-*Person*

Context Passing

lemma *cp*-$OclAsType_{OclAny}$-*Person-Person*: $cp\ P \Longrightarrow cp(\lambda X.\ (P\ (X::Person)::Person)$ *.oclAsType*$(OclAny))$
⟨*proof*⟩
lemma *cp*-$OclAsType_{OclAny}$-*OclAny-OclAny*: $cp\ P \Longrightarrow cp(\lambda X.\ (P\ (X::OclAny)::OclAny)$ *.oclAsType*$(OclAny))$

$\langle proof \rangle$

lemma $cp\text{-}OclAsType_{Person}\text{-}Person\text{-}Person$: $cp\ P \Longrightarrow cp(\lambda X.\ (P\ (X::Person)::Person)\ .oclAsType(Person))$

$\langle proof \rangle$

lemma $cp\text{-}OclAsType_{Person}\text{-}OclAny\text{-}OclAny$: $cp\ P \Longrightarrow cp(\lambda X.\ (P\ (X::OclAny)::OclAny)\ .oclAsType(Person))$

$\langle proof \rangle$

lemma $cp\text{-}OclAsType_{OclAny}\text{-}Person\text{-}OclAny$: $cp\ P \Longrightarrow cp(\lambda X.\ (P\ (X::Person)::OclAny)\ .oclAsType(OclAny))$

$\langle proof \rangle$

lemma $cp\text{-}OclAsType_{OclAny}\text{-}OclAny\text{-}Person$: $cp\ P \Longrightarrow cp(\lambda X.\ (P\ (X::OclAny)::Person)\ .oclAsType(OclAny))$

$\langle proof \rangle$

lemma $cp\text{-}OclAsType_{Person}\text{-}Person\text{-}OclAny$: $cp\ P \Longrightarrow cp(\lambda X.\ (P\ (X::Person)::OclAny)\ .oclAsType(Person))$

$\langle proof \rangle$

lemma $cp\text{-}OclAsType_{Person}\text{-}OclAny\text{-}Person$: $cp\ P \Longrightarrow cp(\lambda X.\ (P\ (X::OclAny)::Person)\ .oclAsType(Person))$

$\langle proof \rangle$

lemmas [*simp*] =

$cp\text{-}OclAsType_{OclAny}\text{-}Person\text{-}Person$
$cp\text{-}OclAsType_{OclAny}\text{-}OclAny\text{-}OclAny$
$cp\text{-}OclAsType_{Person}\text{-}Person\text{-}Person$
$cp\text{-}OclAsType_{Person}\text{-}OclAny\text{-}OclAny$

$cp\text{-}OclAsType_{OclAny}\text{-}Person\text{-}OclAny$
$cp\text{-}OclAsType_{OclAny}\text{-}OclAny\text{-}Person$
$cp\text{-}OclAsType_{Person}\text{-}Person\text{-}OclAny$
$cp\text{-}OclAsType_{Person}\text{-}OclAny\text{-}Person$

Execution with Invalid or Null as Argument

lemma $OclAsType_{OclAny}\text{-}OclAny\text{-}strict$: $(invalid::OclAny)\ .oclAsType(OclAny) = invalid$

$\langle proof \rangle$

lemma $OclAsType_{OclAny}\text{-}OclAny\text{-}nullstrict$: $(null::OclAny)\ .oclAsType(OclAny) = null$

$\langle proof \rangle$

lemma $OclAsType_{OclAny}\text{-}Person\text{-}strict[simp]$: $(invalid::Person)\ .oclAsType(OclAny) = invalid$

$\langle proof \rangle$

lemma $OclAsType_{OclAny}\text{-}Person\text{-}nullstrict[simp]$: $(null::Person)\ .oclAsType(OclAny) = null$

$\langle proof \rangle$

lemma $OclAsType_{Person}\text{-}OclAny\text{-}strict[simp]$: $(invalid::OclAny)\ .oclAsType(Person) = invalid$

$\langle proof \rangle$

lemma $OclAsType_{Person}$-$OclAny$-$nullstrict[simp]$: $(null::OclAny)$ $.oclAsType(Person) = null$
$\langle proof \rangle$

lemma $OclAsType_{Person}$-$Person$-$strict$: $(invalid::Person)$ $.oclAsType(Person) = invalid$
$\langle proof \rangle$
lemma $OclAsType_{Person}$-$Person$-$nullstrict$: $(null::Person)$ $.oclAsType(Person) = null$
$\langle proof \rangle$

7.1.5. OclIsTypeOf

Definition

consts $OclIsTypeOf_{OclAny}$ :: $'\alpha \Rightarrow Boolean$ $((\text{-}).oclIsTypeOf'(OclAny'))$
consts $OclIsTypeOf_{Person}$ :: $'\alpha \Rightarrow Boolean$ $((\text{-}).oclIsTypeOf'(Person'))$

defs (**overloaded**) $OclIsTypeOf_{OclAny}$-$OclAny$:
$(X::OclAny)$ $.oclIsTypeOf(OclAny) \equiv$
$(\lambda\tau.$ $case$ X τ of
$\bot$ $\Rightarrow invalid$ τ
$|$ $\lfloor\bot\rfloor \Rightarrow true$ τ $(*$ $invalid$ $??$ $*)$
$|$ $\lfloor\lfloor mk_{OclAny}$ oid $\bot$ $\rfloor\rfloor \Rightarrow true$ τ
$|$ $\lfloor\lfloor mk_{OclAny}$ oid $\lfloor\text{-}\rfloor$ $\rfloor\rfloor \Rightarrow false$ $\tau)$

defs (**overloaded**) $OclIsTypeOf_{OclAny}$-$Person$:
$(X::Person)$ $.oclIsTypeOf(OclAny) \equiv$
$(\lambda\tau.$ $case$ X τ of
$\bot$ $\Rightarrow invalid$ τ
$|$ $\lfloor\bot\rfloor \Rightarrow true$ τ $(*$ $invalid$ $??$ $*)$
$|$ $\lfloor\lfloor$ - $\rfloor\rfloor \Rightarrow false$ $\tau)$

defs (**overloaded**) $OclIsTypeOf_{Person}$-$OclAny$:
$(X::OclAny)$ $.oclIsTypeOf(Person) \equiv$
$(\lambda\tau.$ $case$ X τ of
$\bot$ $\Rightarrow invalid$ τ
$|$ $\lfloor\bot\rfloor \Rightarrow true$ τ
$|$ $\lfloor\lfloor mk_{OclAny}$ oid $\bot$ $\rfloor\rfloor \Rightarrow false$ τ
$|$ $\lfloor\lfloor mk_{OclAny}$ oid $\lfloor\text{-}\rfloor$ $\rfloor\rfloor \Rightarrow true$ $\tau)$

defs (**overloaded**) $OclIsTypeOf_{Person}$-$Person$:
$(X::Person)$ $.oclIsTypeOf(Person) \equiv$
$(\lambda\tau.$ $case$ X τ of
$\bot \Rightarrow invalid$ τ
$|$ - $\Rightarrow true$ $\tau)$

Context Passing

lemma cp-$OclIsTypeOf_{OclAny}$-$Person$-$Person$: cp P $\Longrightarrow$ $cp(\lambda X.(P(X::Person)::Person).oclIsTypeOf(OclAny))$
$\langle proof \rangle$

lemma *cp-OclIsTypeOf*$_{OclAny}$*-OclAny-OclAny*: *cp* *P* $\Longrightarrow$ $cp(\lambda X.(P(X::OclAny)::OclAny).oclIsTypeOf(OclAny))$
⟨*proof*⟩
lemma *cp-OclIsTypeOf*$_{Person}$*-Person-Person*: *cp* *P* $\Longrightarrow$ $cp(\lambda X.(P(X::Person)::Person).oclIsTypeOf(Person))$
⟨*proof*⟩
lemma *cp-OclIsTypeOf*$_{Person}$*-OclAny-OclAny*: *cp* *P* $\Longrightarrow$ $cp(\lambda X.(P(X::OclAny)::OclAny).oclIsTypeOf(Person))$
⟨*proof*⟩

lemma *cp-OclIsTypeOf*$_{OclAny}$*-Person-OclAny*: *cp* *P* $\Longrightarrow$ $cp(\lambda X.(P(X::Person)::OclAny).oclIsTypeOf(OclAny))$
⟨*proof*⟩
lemma *cp-OclIsTypeOf*$_{OclAny}$*-OclAny-Person*: *cp* *P* $\Longrightarrow$ $cp(\lambda X.(P(X::OclAny)::Person).oclIsTypeOf(OclAny))$
⟨*proof*⟩
lemma *cp-OclIsTypeOf*$_{Person}$*-Person-OclAny*: *cp* *P* $\Longrightarrow$ $cp(\lambda X.(P(X::Person)::OclAny).oclIsTypeOf(Person))$
⟨*proof*⟩
lemma *cp-OclIsTypeOf*$_{Person}$*-OclAny-Person*: *cp* *P* $\Longrightarrow$ $cp(\lambda X.(P(X::OclAny)::Person).oclIsTypeOf(Person))$
⟨*proof*⟩

lemmas [*simp*] =
cp-OclIsTypeOf$_{OclAny}$*-Person-Person*
cp-OclIsTypeOf$_{OclAny}$*-OclAny-OclAny*
cp-OclIsTypeOf$_{Person}$*-Person-Person*
cp-OclIsTypeOf$_{Person}$*-OclAny-OclAny*

cp-OclIsTypeOf$_{OclAny}$*-Person-OclAny*
cp-OclIsTypeOf$_{OclAny}$*-OclAny-Person*
cp-OclIsTypeOf$_{Person}$*-Person-OclAny*
cp-OclIsTypeOf$_{Person}$*-OclAny-Person*

Execution with Invalid or Null as Argument

lemma *OclIsTypeOf*$_{OclAny}$*-OclAny-strict1*[*simp*]:
$(invalid::OclAny)\ .oclIsTypeOf(OclAny) = invalid$
⟨*proof*⟩
lemma *OclIsTypeOf*$_{OclAny}$*-OclAny-strict2*[*simp*]:
$(null::OclAny)\ .oclIsTypeOf(OclAny) = true$
⟨*proof*⟩
lemma *OclIsTypeOf*$_{OclAny}$*-Person-strict1*[*simp*]:
$(invalid::Person)\ .oclIsTypeOf(OclAny) = invalid$
⟨*proof*⟩
lemma *OclIsTypeOf*$_{OclAny}$*-Person-strict2*[*simp*]:
$(null::Person)\ .oclIsTypeOf(OclAny) = true$
⟨*proof*⟩

lemma $OclIsTypeOf_{Person}$-*OclAny-strict1* [*simp*]:
$(invalid::OclAny)$ $.oclIsTypeOf(Person) = invalid$
$\langle proof \rangle$
lemma $OclIsTypeOf_{Person}$-*OclAny-strict2* [*simp*]:
$(null::OclAny)$ $.oclIsTypeOf(Person) = true$
$\langle proof \rangle$
lemma $OclIsTypeOf_{Person}$-*Person-strict1* [*simp*]:
$(invalid::Person)$ $.oclIsTypeOf(Person) = invalid$
$\langle proof \rangle$
lemma $OclIsTypeOf_{Person}$-*Person-strict2* [*simp*]:
$(null::Person)$ $.oclIsTypeOf(Person) = true$
$\langle proof \rangle$

Up Down Casting

lemma *actualType-larger-staticType*:
assumes *isdef*: $\tau \models (\delta\ X)$
shows $\tau \models (X::Person)\ .oclIsTypeOf(OclAny) \triangleq false$
$\langle proof \rangle$

lemma *down-cast-type*:
assumes *isOclAny*: $\tau \models (X::OclAny)\ .oclIsTypeOf(OclAny)$
and *non-null*: $\tau \models (\delta\ X)$
shows $\tau \models (X\ .oclAsType(Person)) \triangleq invalid$
$\langle proof \rangle$

lemma *down-cast-type'*:
assumes *isOclAny*: $\tau \models (X::OclAny)\ .oclIsTypeOf(OclAny)$
and *non-null*: $\tau \models (\delta\ X)$
shows $\tau \models not\ (\upsilon\ (X\ .oclAsType(Person)))$
$\langle proof \rangle$

lemma *up-down-cast* :
assumes *isdef*: $\tau \models (\delta\ X)$
shows $\tau \models ((X::Person)\ .oclAsType(OclAny)\ .oclAsType(Person) \triangleq X)$
$\langle proof \rangle$

lemma *up-down-cast-Person-OclAny-Person* [*simp*]:
shows $((X::Person)\ .oclAsType(OclAny)\ .oclAsType(Person) = X)$
$\langle proof \rangle$

lemma *up-down-cast-Person-OclAny-Person'*: **assumes** $\tau \models \upsilon\ X$
shows $\tau \models (((X :: Person)\ .oclAsType(OclAny)\ .oclAsType(Person)) \doteq X)$
$\langle proof \rangle$

lemma *up-down-cast-Person-OclAny-Person''*: **assumes** $\tau \models \upsilon\ (X :: Person)$
shows $\tau \models (X\ .oclIsTypeOf(Person)\ implies\ (X\ .oclAsType(OclAny)\ .oclAsType(Person)) \doteq X)$

$\langle proof \rangle$

7.1.6. OclIsKindOf

Definition

consts $OclIsKindOf_{OclAny}$ :: $'\alpha \Rightarrow Boolean$ $((\text{-}).oclIsKindOf'(OclAny'))$
consts $OclIsKindOf_{Person}$ :: $'\alpha \Rightarrow Boolean$ $((\text{-}).oclIsKindOf'(Person'))$

defs (**overloaded**) $OclIsKindOf_{OclAny}$-$OclAny$:
$(X::OclAny)$ $.oclIsKindOf(OclAny) \equiv$
$(\lambda\tau.$ $case\ X\ \tau\ of$
$\perp \Rightarrow invalid\ \tau$
$|\ \text{-} \Rightarrow true\ \tau)$

defs (**overloaded**) $OclIsKindOf_{OclAny}$-$Person$:
$(X::Person)$ $.oclIsKindOf(OclAny) \equiv$
$(\lambda\tau.$ $case\ X\ \tau\ of$
$\perp \Rightarrow invalid\ \tau$
$|\ \text{-}\Rightarrow true\ \tau)$

defs (**overloaded**) $OclIsKindOf_{Person}$-$OclAny$:
$(X::OclAny)$ $.oclIsKindOf(Person) \equiv$
$(\lambda\tau.$ $case\ X\ \tau\ of$
$\perp\ \ \Rightarrow invalid\ \tau$
$|\ \lfloor\perp\rfloor \Rightarrow true\ \tau$
$|\ \lfloor\lfloor mk_{OclAny}\ oid\ \perp\ \rfloor\rfloor \Rightarrow false\ \tau$
$|\ \lfloor\lfloor mk_{OclAny}\ oid\ \lfloor\text{-}\rfloor\ \rfloor\rfloor \Rightarrow true\ \tau)$

defs (**overloaded**) $OclIsKindOf_{Person}$-$Person$:
$(X::Person)$ $.oclIsKindOf(Person) \equiv$
$(\lambda\tau.$ $case\ X\ \tau\ of$
$\perp \Rightarrow invalid\ \tau$
$|\ \text{-} \Rightarrow true\ \tau)$

Context Passing

lemma cp-$OclIsKindOf_{OclAny}$-$Person$-$Person$: $cp\ P \Longrightarrow cp(\lambda X.(P(X::Person)::Person).oclIsKindOf(OclAny))$
$\langle proof \rangle$
lemma cp-$OclIsKindOf_{OclAny}$-$OclAny$-$OclAny$: $cp\ P \Longrightarrow cp(\lambda X.(P(X::OclAny)::OclAny).oclIsKindOf(OclAny))$
$\langle proof \rangle$
lemma cp-$OclIsKindOf_{Person}$-$Person$-$Person$: $cp\ P \Longrightarrow cp(\lambda X.(P(X::Person)::Person).oclIsKindOf(Person))$
$\langle proof \rangle$
lemma cp-$OclIsKindOf_{Person}$-$OclAny$-$OclAny$: $cp\ P \Longrightarrow cp(\lambda X.(P(X::OclAny)::OclAny).oclIsKindOf(Person))$
$\langle proof \rangle$

lemma *cp-OclIsKindOf$_{OclAny}$-Person-OclAny*: $cp\ P \Longrightarrow cp(\lambda X.(P(X::Person)::OclAny).oclIsKindOf(OclAny))$
⟨*proof*⟩
lemma *cp-OclIsKindOf$_{OclAny}$-OclAny-Person*: $cp\ P \Longrightarrow cp(\lambda X.(P(X::OclAny)::Person).oclIsKindOf(OclAny))$
⟨*proof*⟩
lemma *cp-OclIsKindOf$_{Person}$-Person-OclAny*: $cp\ P \Longrightarrow cp(\lambda X.(P(X::Person)::OclAny).oclIsKindOf(Person))$
⟨*proof*⟩
lemma *cp-OclIsKindOf$_{Person}$-OclAny-Person*: $cp\ P \Longrightarrow cp(\lambda X.(P(X::OclAny)::Person).oclIsKindOf(Person))$
⟨*proof*⟩

lemmas [*simp*] =
cp-OclIsKindOf$_{OclAny}$-Person-Person
cp-OclIsKindOf$_{OclAny}$-OclAny-OclAny
cp-OclIsKindOf$_{Person}$-Person-Person
cp-OclIsKindOf$_{Person}$-OclAny-OclAny

cp-OclIsKindOf$_{OclAny}$-Person-OclAny
cp-OclIsKindOf$_{OclAny}$-OclAny-Person
cp-OclIsKindOf$_{Person}$-Person-OclAny
cp-OclIsKindOf$_{Person}$-OclAny-Person

Execution with Invalid or Null as Argument

lemma *OclIsKindOf$_{OclAny}$-OclAny-strict1*[*simp*] : $(invalid::OclAny)\ .oclIsKindOf(OclAny) = invalid$
⟨*proof*⟩

lemma *OclIsKindOf$_{OclAny}$-OclAny-strict2*[*simp*] : $(null::OclAny)\ .oclIsKindOf(OclAny) = true$
⟨*proof*⟩

lemma *OclIsKindOf$_{OclAny}$-Person-strict1*[*simp*] : $(invalid::Person)\ .oclIsKindOf(OclAny) = invalid$
⟨*proof*⟩

lemma *OclIsKindOf$_{OclAny}$-Person-strict2*[*simp*] : $(null::Person)\ .oclIsKindOf(OclAny) = true$
⟨*proof*⟩

lemma *OclIsKindOf$_{Person}$-OclAny-strict1*[*simp*]: $(invalid::OclAny)\ .oclIsKindOf(Person) = invalid$
⟨*proof*⟩

lemma *OclIsKindOf$_{Person}$-OclAny-strict2*[*simp*]: $(null::OclAny)\ .oclIsKindOf(Person) = true$
⟨*proof*⟩

lemma *OclIsKindOf$_{Person}$-Person-strict1*[*simp*]: $(invalid::Person)\ .oclIsKindOf(Person) =$

invalid
⟨*proof*⟩

lemma $\mathit{OclIsKindOf}_{\mathit{Person}}$*-Person-strict2*[*simp*]: (*null*::*Person*) .*oclIsKindOf*(*Person*) = *true*
⟨*proof*⟩

Up Down Casting

lemma *actualKind-larger-staticKind*:
assumes *isdef*: $\tau \models (\delta\ X)$
shows $\tau \models (X::\mathit{Person})\ .\mathit{oclIsKindOf}(\mathit{OclAny}) \triangleq \mathit{true}$
⟨*proof*⟩

lemma *down-cast-kind*:
assumes *isOclAny*: $\neg\ \tau \models (X::\mathit{OclAny})\ .\mathit{oclIsKindOf}(\mathit{Person})$
and *non-null*: $\tau \models (\delta\ X)$
shows $\tau \models (X\ .\mathit{oclAsType}(\mathit{Person})) \triangleq \mathit{invalid}$
⟨*proof*⟩

7.1.7. OclAllInstances

To denote OCL-types occuring 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* ≡ $\mathit{OclAsType}_{\mathit{Person}}$-$\mathfrak{A}$
definition *OclAny* ≡ $\mathit{OclAsType}_{\mathit{OclAny}}$-$\mathfrak{A}$
lemmas [*simp*] = *Person-def OclAny-def*

lemma $\mathit{OclAllInstances\text{-}generic}_{\mathit{OclAny}}$*-exec*: *OclAllInstances-generic pre-post OclAny* =
$(\lambda\tau.\ \ \mathit{Abs\text{-}Set\text{-}0}\ \ \lfloor\lfloor\ \mathit{Some}\ `\ \mathit{OclAny}\ `\ \mathit{ran}\ (\mathit{heap}\ (\mathit{pre\text{-}post}\ \tau))\ \rfloor\rfloor)$
⟨*proof*⟩

lemma $\mathit{OclAllInstances\text{-}at\text{-}post}_{\mathit{OclAny}}$*-exec*: *OclAny* .*allInstances*() =
$(\lambda\tau.\ \ \mathit{Abs\text{-}Set\text{-}0}\ \ \lfloor\lfloor\ \mathit{Some}\ `\ \mathit{OclAny}\ `\ \mathit{ran}\ (\mathit{heap}\ (\mathit{snd}\ \tau))\ \rfloor\rfloor)$
⟨*proof*⟩

lemma $\mathit{OclAllInstances\text{-}at\text{-}pre}_{\mathit{OclAny}}$*-exec*: *OclAny* .*allInstances@pre*() =
$(\lambda\tau.\ \ \mathit{Abs\text{-}Set\text{-}0}\ \ \lfloor\lfloor\ \mathit{Some}\ `\ \mathit{OclAny}\ `\ \mathit{ran}\ (\mathit{heap}\ (\mathit{fst}\ \tau))\ \rfloor\rfloor)$
⟨*proof*⟩

OclIsTypeOf

lemma *OclAny-allInstances-generic-oclIsTypeOf*$_{\mathit{OclAny}}$*1*:
assumes [*simp*]: $\bigwedge x.\ \mathit{pre\text{-}post}\ (x,\ x) = x$
shows $\exists\tau.\ \ (\tau\ \models\ ((\mathit{OclAllInstances\text{-}generic}\ \ \mathit{pre\text{-}post}\ \ \mathit{OclAny}){-}{>}\mathit{forAll}(X|X\ .\mathit{oclIsTypeOf}(\mathit{OclAny}))))$
⟨*proof*⟩

lemma *OclAny-allInstances-at-post-oclIsTypeOf*$_{\mathit{OclAny}}$*1*:

$\exists \tau. (\tau \models (OclAny\ .allInstances() {-}{>} forAll(X|X\ .oclIsTypeOf(OclAny))))$
⟨proof⟩

lemma *OclAny-allInstances-at-pre-oclIsTypeOf*$_{OclAny}$*1*:
$\exists \tau. (\tau \models (OclAny\ .allInstances@pre() {-}{>} forAll(X|X\ .oclIsTypeOf(OclAny))))$
⟨proof⟩

lemma *OclAny-allInstances-generic-oclIsTypeOf*$_{OclAny}$*2*:
assumes [*simp*]: $\bigwedge x.\ pre\text{-}post\ (x, x) = x$
shows $\exists \tau. (\tau \models not\ ((OclAllInstances\text{-}generic\ pre\text{-}post\ OclAny) {-}{>} forAll(X|X\ .oclIsTypeOf(OclAny))))$
⟨proof⟩

lemma *OclAny-allInstances-at-post-oclIsTypeOf*$_{OclAny}$*2*:
$\exists \tau. (\tau \models not\ (OclAny\ .allInstances() {-}{>} forAll(X|X\ .oclIsTypeOf(OclAny))))$
⟨proof⟩

lemma *OclAny-allInstances-at-pre-oclIsTypeOf*$_{OclAny}$*2*:
$\exists \tau. (\tau \models not\ (OclAny\ .allInstances@pre() {-}{>} forAll(X|X\ .oclIsTypeOf(OclAny))))$
⟨proof⟩

lemma *Person-allInstances-generic-oclIsTypeOf*$_{Person}$:
$\tau \models ((OclAllInstances\text{-}generic\ pre\text{-}post\ Person) {-}{>} forAll(X|X\ .oclIsTypeOf(Person)))$
⟨proof⟩

lemma *Person-allInstances-at-post-oclIsTypeOf*$_{Person}$:
$\tau \models (Person\ .allInstances() {-}{>} forAll(X|X\ .oclIsTypeOf(Person)))$
⟨proof⟩

lemma *Person-allInstances-at-pre-oclIsTypeOf*$_{Person}$:
$\tau \models (Person\ .allInstances@pre() {-}{>} forAll(X|X\ .oclIsTypeOf(Person)))$
⟨proof⟩

OclIsKindOf

lemma *OclAny-allInstances-generic-oclIsKindOf*$_{OclAny}$:
$\tau \models ((OclAllInstances\text{-}generic\ pre\text{-}post\ OclAny) {-}{>} forAll(X|X\ .oclIsKindOf(OclAny)))$
⟨proof⟩

lemma *OclAny-allInstances-at-post-oclIsKindOf*$_{OclAny}$:
$\tau \models (OclAny\ .allInstances() {-}{>} forAll(X|X\ .oclIsKindOf(OclAny)))$
⟨proof⟩

lemma *OclAny-allInstances-at-pre-oclIsKindOf*$_{OclAny}$:
$\tau \models (OclAny\ .allInstances@pre() {-}{>} forAll(X|X\ .oclIsKindOf(OclAny)))$
⟨proof⟩

lemma *Person-allInstances-generic-oclIsKindOf*$_{OclAny}$:
$\tau \models ((OclAllInstances\text{-}generic\ pre\text{-}post\ Person) {-}{>} forAll(X|X\ .oclIsKindOf(OclAny)))$

⟨*proof*⟩

lemma *Person-allInstances-at-post-oclIsKindOf*$_{OclAny}$:
$\tau \models (Person\ .allInstances()\text{->}forAll(X|X\ .oclIsKindOf(OclAny)))$
⟨*proof*⟩

lemma *Person-allInstances-at-pre-oclIsKindOf*$_{OclAny}$:
$\tau \models (Person\ .allInstances@pre()\text{->}forAll(X|X\ .oclIsKindOf(OclAny)))$
⟨*proof*⟩

lemma *Person-allInstances-generic-oclIsKindOf*$_{Person}$:
$\tau \models ((OclAllInstances\text{-}generic\ pre\text{-}post\ Person)\text{->}forAll(X|X\ .oclIsKindOf(Person)))$
⟨*proof*⟩

lemma *Person-allInstances-at-post-oclIsKindOf*$_{Person}$:
$\tau \models (Person\ .allInstances()\text{->}forAll(X|X\ .oclIsKindOf(Person)))$
⟨*proof*⟩

lemma *Person-allInstances-at-pre-oclIsKindOf*$_{Person}$:
$\tau \models (Person\ .allInstances@pre()\text{->}forAll(X|X\ .oclIsKindOf(Person)))$
⟨*proof*⟩

7.1.8. The Accessors (any, boss, salary)

Should be generated entirely from a class-diagram.

Definition

definition *eval-extract* :: $('\mathfrak{A},('a::object)\ option\ option)\ val$
$\Rightarrow (oid \Rightarrow ('\mathfrak{A},'c::null)\ val)$
$\Rightarrow ('\mathfrak{A},'c::null)\ val$
where $eval\text{-}extract\ X\ f = (\lambda\ \tau.\ case\ X\ \tau\ of$
$\bot \Rightarrow invalid\ \tau\quad (*\ exception\ propagation\ *)$
$|\ \lfloor\ \bot\ \rfloor \Rightarrow invalid\ \tau\ (*\ dereferencing\ null\ pointer\ *)$
$|\ \lfloor\lfloor\ obj\ \rfloor\rfloor \Rightarrow f\ (oid\text{-}of\ obj)\ \tau)$

definition *deref-oid*$_{Person}$ :: $(\mathfrak{A}\ state \times \mathfrak{A}\ state \Rightarrow \mathfrak{A}\ state)$
$\Rightarrow (type_{Person} \Rightarrow (\mathfrak{A},\ 'c::null)val)$
$\Rightarrow oid$
$\Rightarrow (\mathfrak{A},\ 'c::null)val$
where $deref\text{-}oid_{Person}\ fst\text{-}snd\ f\ oid = (\lambda\tau.\ case\ (heap\ (fst\text{-}snd\ \tau))\ oid\ of$
$\lfloor\ in_{Person}\ obj\ \rfloor \Rightarrow f\ obj\ \tau$
$|\ \text{-}\quad \Rightarrow invalid\ \tau)$

definition *deref-oid*$_{OclAny}$ :: $(\mathfrak{A}\ state \times \mathfrak{A}\ state \Rightarrow \mathfrak{A}\ state)$

$\Rightarrow (type_{OclAny} \Rightarrow (\mathfrak{A},\ 'c{::}null)val)$
$\Rightarrow oid$
$\Rightarrow (\mathfrak{A},\ 'c{::}null)val$

where $\textit{deref-oid}_{OclAny}\ \textit{fst-snd}\ f\ oid = (\lambda\tau.\ case\ (heap\ (\textit{fst-snd}\ \tau))\ oid\ of$
$\lfloor\ in_{OclAny}\ obj\ \rfloor \Rightarrow f\ obj\ \tau$
$\mid -\quad \Rightarrow invalid\ \tau)$

pointer undefined in state or not referencing a type conform object representation

definition $select_{OclAny}\mathcal{ANY}\ f = (\lambda\ X.\ case\ X\ of$
$(mk_{OclAny}\ \text{-}\ \bot) \Rightarrow null$
$\mid (mk_{OclAny}\ \text{-}\ \lfloor any\rfloor) \Rightarrow f\ (\lambda x\ \text{-}.\ \lfloor\lfloor x\rfloor\rfloor)\ any)$

definition $select_{Person}\mathcal{BOSS}\ f = (\lambda\ X.\ case\ X\ of$
$(mk_{Person}\ \text{-}\ \text{-}\ \bot) \Rightarrow null\ \ (*\ object\ contains\ null\ pointer\ *)$
$\mid (mk_{Person}\ \text{-}\ \text{-}\ \lfloor boss\rfloor) \Rightarrow f\ (\lambda x\ \text{-}.\ \lfloor\lfloor x\rfloor\rfloor)\ boss)$

definition $select_{Person}\mathcal{SALARY}\ f = (\lambda\ X.\ case\ X\ of$
$(mk_{Person}\ \text{-}\ \bot\ \text{-}) \Rightarrow null$
$\mid (mk_{Person}\ \text{-}\ \lfloor salary\rfloor\ \text{-}) \Rightarrow f\ (\lambda x\ \text{-}.\ \lfloor\lfloor x\rfloor\rfloor)\ salary)$

definition $\textit{in-pre-state} = fst$
definition $\textit{in-post-state} = snd$

definition $\textit{reconst-basetype} = (\lambda\ convert\ x.\ convert\ x)$

definition $dot_{OclAny}\mathcal{ANY} :: OclAny \Rightarrow \text{-}\ \ ((1(\text{-}).any)\ 50)$
where $(X).any = \textit{eval-extract}\ X$
$(\textit{deref-oid}_{OclAny}\ \textit{in-post-state}$
$(select_{OclAny}\mathcal{ANY}$
$\textit{reconst-basetype}))$

definition $dot_{Person}\mathcal{BOSS} :: Person \Rightarrow Person\ \ ((1(\text{-}).boss)\ 50)$
where $(X).boss = \textit{eval-extract}\ X$
$(\textit{deref-oid}_{Person}\ \textit{in-post-state}$
$(select_{Person}\mathcal{BOSS}$
$(\textit{deref-oid}_{Person}\ \textit{in-post-state})))$

definition $dot_{Person}\mathcal{SALARY} :: Person \Rightarrow Integer\ \ ((1(\text{-}).salary)\ 50)$
where $(X).salary = \textit{eval-extract}\ X$
$(\textit{deref-oid}_{Person}\ \textit{in-post-state}$
$(select_{Person}\mathcal{SALARY}$
$\textit{reconst-basetype}))$

definition $dot_{OclAny}\mathcal{ANY}\textit{-at-pre} :: OclAny \Rightarrow \text{-}\ \ ((1(\text{-}).any@pre)\ 50)$
where $(X).any@pre = \textit{eval-extract}\ X$
$(\textit{deref-oid}_{OclAny}\ \textit{in-pre-state}$

$(select_{OclAny}\mathcal{ANY}$
$reconst\text{-}basetype))$

definition $dot_{Person}\mathcal{BOSS}$*-at-pre*:: *Person* $\Rightarrow$ *Person* $((1(\text{-}).boss@pre)\ 50)$
where $(X).boss@pre = eval\text{-}extract\ X$
$(deref\text{-}oid_{Person}\ in\text{-}pre\text{-}state$
$(select_{Person}\mathcal{BOSS}$
$(deref\text{-}oid_{Person}\ in\text{-}pre\text{-}state)))$

definition $dot_{Person}\mathcal{SALARY}$*-at-pre*:: *Person* $\Rightarrow$ *Integer* $((1(\text{-}).salary@pre)\ 50)$
where $(X).salary@pre = eval\text{-}extract\ X$
$(deref\text{-}oid_{Person}\ in\text{-}pre\text{-}state$
$(select_{Person}\mathcal{SALARY}$
$reconst\text{-}basetype))$

lemmas [*simp*] =
$dot_{OclAny}\mathcal{ANY}\text{-}def$
$dot_{Person}\mathcal{BOSS}\text{-}def$
$dot_{Person}\mathcal{SALARY}\text{-}def$
$dot_{OclAny}\mathcal{ANY}\text{-}at\text{-}pre\text{-}def$
$dot_{Person}\mathcal{BOSS}\text{-}at\text{-}pre\text{-}def$
$dot_{Person}\mathcal{SALARY}\text{-}at\text{-}pre\text{-}def$

Context Passing

lemmas [*simp*] = *eval-extract-def*

lemma $cp\text{-}dot_{OclAny}\mathcal{ANY}$: $((X).any)\ \tau = ((\lambda\text{-}.\ X\ \tau).any)\ \tau$ ⟨*proof*⟩
lemma $cp\text{-}dot_{Person}\mathcal{BOSS}$: $((X).boss)\ \tau = ((\lambda\text{-}.\ X\ \tau).boss)\ \tau$ ⟨*proof*⟩
lemma $cp\text{-}dot_{Person}\mathcal{SALARY}$: $((X).salary)\ \tau = ((\lambda\text{-}.\ X\ \tau).salary)\ \tau$ ⟨*proof*⟩

lemma $cp\text{-}dot_{OclAny}\mathcal{ANY}\text{-}at\text{-}pre$: $((X).any@pre)\ \tau = ((\lambda\text{-}.\ X\ \tau).any@pre)\ \tau$ ⟨*proof*⟩
lemma $cp\text{-}dot_{Person}\mathcal{BOSS}\text{-}at\text{-}pre$: $((X).boss@pre)\ \tau = ((\lambda\text{-}.\ X\ \tau).boss@pre)\ \tau$ ⟨*proof*⟩
lemma $cp\text{-}dot_{Person}\mathcal{SALARY}\text{-}at\text{-}pre$: $((X).salary@pre)\ \tau = ((\lambda\text{-}.\ X\ \tau).salary@pre)\ \tau$ ⟨*proof*⟩

lemmas $cp\text{-}dot_{OclAny}\mathcal{ANY}\text{-}I$ [*simp*, *intro*!]=
$cp\text{-}dot_{OclAny}\mathcal{ANY}[THEN\ allI[THEN\ allI],$
$of\ \lambda\ X\ \text{-}.\ X\ \lambda\ \text{-}\ \tau.\ \tau,\ THEN\ cpI1]$
lemmas $cp\text{-}dot_{OclAny}\mathcal{ANY}\text{-}at\text{-}pre\text{-}I$ [*simp*, *intro*!]=
$cp\text{-}dot_{OclAny}\mathcal{ANY}\text{-}at\text{-}pre[THEN\ allI[THEN\ allI],$
$of\ \lambda\ X\ \text{-}.\ X\ \lambda\ \text{-}\ \tau.\ \tau,\ THEN\ cpI1]$

lemmas $cp\text{-}dot_{Person}\mathcal{BOSS}\text{-}I$ [*simp*, *intro*!]=
$cp\text{-}dot_{Person}\mathcal{BOSS}[THEN\ allI[THEN\ allI],$
$of\ \lambda\ X\ \text{-}.\ X\ \lambda\ \text{-}\ \tau.\ \tau,\ THEN\ cpI1]$
lemmas $cp\text{-}dot_{Person}\mathcal{BOSS}\text{-}at\text{-}pre\text{-}I$ [*simp*, *intro*!]=
$cp\text{-}dot_{Person}\mathcal{BOSS}\text{-}at\text{-}pre[THEN\ allI[THEN\ allI],$
$of\ \lambda\ X\ \text{-}.\ X\ \lambda\ \text{-}\ \tau.\ \tau,\ THEN\ cpI1]$

lemmas $cp\text{-}dot_{Person}\mathcal{SALARY}\text{-}I$ [$simp$, $intro!$]=
$cp\text{-}dot_{Person}\mathcal{SALARY}[THEN\ allI[THEN\ allI],$
$of\ \lambda\ X\ \text{-}.\ X\ \lambda\ \text{-}\ \tau.\ \tau,\ THEN\ cpI1]$
lemmas $cp\text{-}dot_{Person}\mathcal{SALARY}\text{-}at\text{-}pre\text{-}I$ [$simp$, $intro!$]=
$cp\text{-}dot_{Person}\mathcal{SALARY}\text{-}at\text{-}pre[THEN\ allI[THEN\ allI],$
$of\ \lambda\ X\ \text{-}.\ X\ \lambda\ \text{-}\ \tau.\ \tau,\ THEN\ cpI1]$

Execution with Invalid or Null as Argument

lemma $dot_{OclAny}\mathcal{ANY}\text{-}nullstrict$ [$simp$]: $(null).any = invalid$
$\langle proof \rangle$
lemma $dot_{OclAny}\mathcal{ANY}\text{-}at\text{-}pre\text{-}nullstrict$ [$simp$] : $(null).any@pre = invalid$
$\langle proof \rangle$
lemma $dot_{OclAny}\mathcal{ANY}\text{-}strict$ [$simp$] : $(invalid).any = invalid$
$\langle proof \rangle$
lemma $dot_{OclAny}\mathcal{ANY}\text{-}at\text{-}pre\text{-}strict$ [$simp$] : $(invalid).any@pre = invalid$
$\langle proof \rangle$

lemma $dot_{Person}\mathcal{BOSS}\text{-}nullstrict$ [$simp$]: $(null).boss = invalid$
$\langle proof \rangle$
lemma $dot_{Person}\mathcal{BOSS}\text{-}at\text{-}pre\text{-}nullstrict$ [$simp$] : $(null).boss@pre = invalid$
$\langle proof \rangle$
lemma $dot_{Person}\mathcal{BOSS}\text{-}strict$ [$simp$] : $(invalid).boss = invalid$
$\langle proof \rangle$
lemma $dot_{Person}\mathcal{BOSS}\text{-}at\text{-}pre\text{-}strict$ [$simp$] : $(invalid).boss@pre = invalid$
$\langle proof \rangle$

lemma $dot_{Person}\mathcal{SALARY}\text{-}nullstrict$ [$simp$]: $(null).salary = invalid$
$\langle proof \rangle$
lemma $dot_{Person}\mathcal{SALARY}\text{-}at\text{-}pre\text{-}nullstrict$ [$simp$] : $(null).salary@pre = invalid$
$\langle proof \rangle$
lemma $dot_{Person}\mathcal{SALARY}\text{-}strict$ [$simp$] : $(invalid).salary = invalid$
$\langle proof \rangle$
lemma $dot_{Person}\mathcal{SALARY}\text{-}at\text{-}pre\text{-}strict$ [$simp$] : $(invalid).salary@pre = invalid$
$\langle proof \rangle$

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** $OclInt1000 = (\lambda\ \text{-}\ .\ \lfloor\lfloor 1000 \rfloor\rfloor)$
definition $OclInt1200$ (**1200**) **where** $OclInt1200 = (\lambda\ \text{-}\ .\ \lfloor\lfloor 1200 \rfloor\rfloor)$
definition $OclInt1300$ (**1300**) **where** $OclInt1300 = (\lambda\ \text{-}\ .\ \lfloor\lfloor 1300 \rfloor\rfloor)$
definition $OclInt1800$ (**1800**) **where** $OclInt1800 = (\lambda\ \text{-}\ .\ \lfloor\lfloor 1800 \rfloor\rfloor)$
definition $OclInt2600$ (**2600**) **where** $OclInt2600 = (\lambda\ \text{-}\ .\ \lfloor\lfloor 2600 \rfloor\rfloor)$
definition $OclInt2900$ (**2900**) **where** $OclInt2900 = (\lambda\ \text{-}\ .\ \lfloor\lfloor 2900 \rfloor\rfloor)$
definition $OclInt3200$ (**3200**) **where** $OclInt3200 = (\lambda\ \text{-}\ .\ \lfloor\lfloor 3200 \rfloor\rfloor)$
definition $OclInt3500$ (**3500**) **where** $OclInt3500 = (\lambda\ \text{-}\ .\ \lfloor\lfloor 3500 \rfloor\rfloor)$

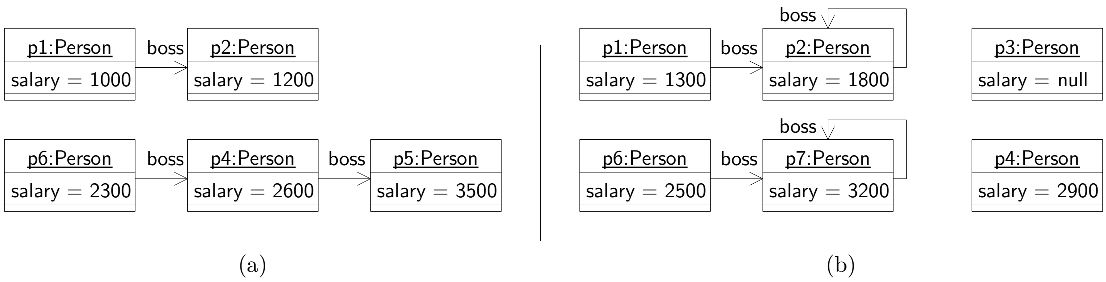


Figure 7.2.: (a) pre-state σ_1 and (b) post-state σ_1'.

definition $oid0 \equiv 0$
definition $oid1 \equiv 1$
definition $oid2 \equiv 2$
definition $oid3 \equiv 3$
definition $oid4 \equiv 4$
definition $oid5 \equiv 5$
definition $oid6 \equiv 6$
definition $oid7 \equiv 7$
definition $oid8 \equiv 8$

definition $person1 \equiv mk_{Person}\ oid0\ \lfloor 1300 \rfloor\ \lfloor oid1 \rfloor$
definition $person2 \equiv mk_{Person}\ oid1\ \lfloor 1800 \rfloor\ \lfloor oid1 \rfloor$
definition $person3 \equiv mk_{Person}\ oid2\ None\ None$
definition $person4 \equiv mk_{Person}\ oid3\ \lfloor 2900 \rfloor\ None$
definition $person5 \equiv mk_{Person}\ oid4\ \lfloor 3500 \rfloor\ None$
definition $person6 \equiv mk_{Person}\ oid5\ \lfloor 2500 \rfloor\ \lfloor oid6 \rfloor$
definition $person7 \equiv mk_{OclAny}\ oid6\ \lfloor (\lfloor 3200 \rfloor, \lfloor oid6 \rfloor) \rfloor$
definition $person8 \equiv mk_{OclAny}\ oid7\ None$
definition $person9 \equiv mk_{Person}\ oid8\ \lfloor 0 \rfloor\ None$

definition

$$
\begin{aligned}
\sigma_1 \equiv (\!|\ heap = empty(&oid0 \mapsto in_{Person}\ (mk_{Person}\ oid0\ \lfloor 1000 \rfloor\ \lfloor oid1 \rfloor))\\
&(oid1 \mapsto in_{Person}\ (mk_{Person}\ oid1\ \lfloor 1200 \rfloor\ \ None))\\
&(*oid2*)\\
&(oid3 \mapsto in_{Person}\ (mk_{Person}\ oid3\ \lfloor 2600 \rfloor\ \lfloor oid4 \rfloor))\\
&(oid4 \mapsto in_{Person}\ person5)\\
&(oid5 \mapsto in_{Person}\ (mk_{Person}\ oid5\ \lfloor 2300 \rfloor\ \lfloor oid3 \rfloor))\\
&(*oid6*)\\
&(*oid7*)\\
&(oid8 \mapsto in_{Person}\ person9),\\
assocs_2 = empty&,\\
assocs_3 = empty&\ |\!)
\end{aligned}
$$

definition

$$\sigma_1{}' \equiv (\!|\ heap = empty(oid0 \mapsto in_{Person}\ person1)$$

$(oid1 \mapsto in_{Person}\ person2)$
$(oid2 \mapsto in_{Person}\ person3)$
$(oid3 \mapsto in_{Person}\ person4)$
$(*oid4*)$
$(oid5 \mapsto in_{Person}\ person6)$
$(oid6 \mapsto in_{OclAny}\ person7)$
$(oid7 \mapsto in_{OclAny}\ person8)$
$(oid8 \mapsto in_{Person}\ person9)$,
$assocs_2 = empty$,
$assocs_3 = empty$ ⦈

definition $\sigma_0 \equiv$ ⦇ $heap = empty,\ assocs_2 = empty,\ assocs_3 = empty$ ⦈

lemma *basic-τ-wff*: $WFF(\sigma_1,\sigma_1{}')$
⟨*proof*⟩

lemma [*simp,code-unfold*]: $dom\ (heap\ \sigma_1) = \{oid0,oid1,(*,oid2*)oid3,oid4,oid5(*,oid6,oid7*),oid8\}$
⟨*proof*⟩

lemma [*simp,code-unfold*]: $dom\ (heap\ \sigma_1{}') = \{oid0,oid1,oid2,oid3,(*,oid4*)oid5,oid6,oid7,oid8\}$
⟨*proof*⟩

definition $X_{Person}1 :: Person \equiv \lambda\ \text{-}\ .\lfloor\lfloor\ person1\ \rfloor\rfloor$
definition $X_{Person}2 :: Person \equiv \lambda\ \text{-}\ .\lfloor\lfloor\ person2\ \rfloor\rfloor$
definition $X_{Person}3 :: Person \equiv \lambda\ \text{-}\ .\lfloor\lfloor\ person3\ \rfloor\rfloor$
definition $X_{Person}4 :: Person \equiv \lambda\ \text{-}\ .\lfloor\lfloor\ person4\ \rfloor\rfloor$
definition $X_{Person}5 :: Person \equiv \lambda\ \text{-}\ .\lfloor\lfloor\ person5\ \rfloor\rfloor$
definition $X_{Person}6 :: Person \equiv \lambda\ \text{-}\ .\lfloor\lfloor\ person6\ \rfloor\rfloor$
definition $X_{Person}7 :: OclAny \equiv \lambda\ \text{-}\ .\lfloor\lfloor\ person7\ \rfloor\rfloor$
definition $X_{Person}8 :: OclAny \equiv \lambda\ \text{-}\ .\lfloor\lfloor\ person8\ \rfloor\rfloor$
definition $X_{Person}9 :: Person \equiv \lambda\ \text{-}\ .\lfloor\lfloor\ person9\ \rfloor\rfloor$

lemma [*code-unfold*]: $((x::Person) \doteq y) = StrictRefEq_{Object}\ x\ y$ ⟨*proof*⟩
lemma [*code-unfold*]: $((x::OclAny) \doteq y) = StrictRefEq_{Object}\ x\ y$ ⟨*proof*⟩

lemmas [*simp,code-unfold*] =
$OclAsType_{OclAny}$-*OclAny*
$OclAsType_{OclAny}$-*Person*
$OclAsType_{Person}$-*OclAny*
$OclAsType_{Person}$-*Person*

$OclIsTypeOf_{OclAny}$-*OclAny*
$OclIsTypeOf_{OclAny}$-*Person*
$OclIsTypeOf_{Person}$-*OclAny*
$OclIsTypeOf_{Person}$-*Person*

$OclIsKindOf_{OclAny}$-*OclAny*
$OclIsKindOf_{OclAny}$-*Person*

OclIsKindOf$_{Person}$-*OclAny*
OclIsKindOf$_{Person}$-*Person*

value $\bigwedge s_{pre} \;.\; (s_{pre},\sigma_1{}') \models (X_{Person}1\ .salary\ <>\ \mathbf{1000})$
value $\bigwedge s_{pre} \;.\; (s_{pre},\sigma_1{}') \models (X_{Person}1\ .salary\ \doteq\ \mathbf{1300})$
value $\bigwedge s_{post} .\; (\sigma_1,s_{post}) \models (X_{Person}1\ .salary@pre\ \doteq\ \mathbf{1000})$
value $\bigwedge s_{post} .\; (\sigma_1,s_{post}) \models (X_{Person}1\ .salary@pre\ <>\ \mathbf{1300})$
value $\bigwedge s_{pre} \;.\; (s_{pre},\sigma_1{}') \models (X_{Person}1\ .boss\ <>\ X_{Person}1)$
value $\bigwedge s_{pre} \;.\; (s_{pre},\sigma_1{}') \models (X_{Person}1\ .boss\ .salary\ \doteq\ \mathbf{1800})$
value $\bigwedge s_{pre} \;.\; (s_{pre},\sigma_1{}') \models (X_{Person}1\ .boss\ .boss\ <>\ X_{Person}1)$
value $\bigwedge s_{pre} \;.\; (s_{pre},\sigma_1{}') \models (X_{Person}1\ .boss\ .boss\ \doteq\ X_{Person}2)$
value $(\sigma_1,\sigma_1{}') \models (X_{Person}1\ .boss@pre\ .salary\ \doteq\ \mathbf{1800})$
value $\bigwedge s_{post} .\; (\sigma_1,s_{post}) \models (X_{Person}1\ .boss@pre\ .salary@pre\ \doteq\ \mathbf{1200})$
value $\bigwedge s_{post} .\; (\sigma_1,s_{post}) \models (X_{Person}1\ .boss@pre\ .salary@pre\ <>\ \mathbf{1800})$
value $\bigwedge s_{post} .\; (\sigma_1,s_{post}) \models (X_{Person}1\ .boss@pre\ \doteq\ X_{Person}2)$
value $(\sigma_1,\sigma_1{}') \models (X_{Person}1\ .boss@pre\ .boss\ \doteq\ X_{Person}2)$
value $\bigwedge s_{post} .\; (\sigma_1,s_{post}) \models (X_{Person}1\ .boss@pre\ .boss@pre\ \doteq\ null)$
value $\bigwedge s_{post} .\; (\sigma_1,s_{post}) \models not(\upsilon(X_{Person}1\ .boss@pre\ .boss@pre\ .boss@pre))$

lemma $(\sigma_1,\sigma_1{}') \models (X_{Person}1\ .oclIsMaintained())$
⟨*proof*⟩

lemma $\bigwedge s_{pre}\ s_{post} .\; (s_{pre},s_{post}) \models ((X_{Person}1\ .oclAsType(OclAny)\ .oclAsType(Person))$
$\doteq X_{Person}1)$
⟨*proof*⟩
value $\bigwedge s_{pre}\ s_{post} .\; (s_{pre},s_{post}) \models (X_{Person}1\ .oclIsTypeOf(Person))$
value $\bigwedge s_{pre}\ s_{post} .\; (s_{pre},s_{post}) \models not(X_{Person}1\ .oclIsTypeOf(OclAny))$
value $\bigwedge s_{pre}\ s_{post} .\; (s_{pre},s_{post}) \models (X_{Person}1\ .oclIsKindOf(Person))$
value $\bigwedge s_{pre}\ s_{post} .\; (s_{pre},s_{post}) \models (X_{Person}1\ .oclIsKindOf(OclAny))$
value $\bigwedge s_{pre}\ s_{post} .\; (s_{pre},s_{post}) \models not(X_{Person}1\ .oclAsType(OclAny)\ .oclIsTypeOf(OclAny))$

value $\bigwedge s_{pre} \;.\; (s_{pre},\sigma_1{}') \models (X_{Person}2\ .salary\ \doteq\ \mathbf{1800})$
value $\bigwedge s_{post} .\; (\sigma_1,s_{post}) \models (X_{Person}2\ .salary@pre\ \doteq\ \mathbf{1200})$
value $\bigwedge s_{pre} \;.\; (s_{pre},\sigma_1{}') \models (X_{Person}2\ .boss\ \doteq\ X_{Person}2)$
value $(\sigma_1,\sigma_1{}') \models (X_{Person}2\ .boss\ .salary@pre\ \doteq\ \mathbf{1200})$
value $(\sigma_1,\sigma_1{}') \models (X_{Person}2\ .boss\ .boss@pre\ \doteq\ null)$
value $\bigwedge s_{post} .\; (\sigma_1,s_{post}) \models (X_{Person}2\ .boss@pre\ \doteq\ null)$
value $\bigwedge s_{post} .\; (\sigma_1,s_{post}) \models (X_{Person}2\ .boss@pre\ <>\ X_{Person}2)$
value $(\sigma_1,\sigma_1{}') \models (X_{Person}2\ .boss@pre\ <>\ (X_{Person}2\ .boss))$
value $\bigwedge s_{post} .\; (\sigma_1,s_{post}) \models not(\upsilon(X_{Person}2\ .boss@pre\ .boss))$
value $\bigwedge s_{post} .\; (\sigma_1,s_{post}) \models not(\upsilon(X_{Person}2\ .boss@pre\ .salary@pre))$
lemma $(\sigma_1,\sigma_1{}') \models (X_{Person}2\ .oclIsMaintained())$
⟨*proof*⟩

value $\bigwedge s_{pre} \;.\; (s_{pre},\sigma_1{}') \models (X_{Person}3\ .salary\ \doteq\ null)$
value $\bigwedge s_{post} .\; (\sigma_1,s_{post}) \models not(\upsilon(X_{Person}3\ .salary@pre))$

value $\bigwedge s_{pre} \quad . \quad (s_{pre},\sigma_1{}') \models \quad (X_{Person}\mathit{3}\ .\mathit{boss} \quad \doteq \mathit{null})$
value $\bigwedge s_{pre} \quad . \quad (s_{pre},\sigma_1{}') \models \mathit{not}(\upsilon(X_{Person}\mathit{3}\ .\mathit{boss}\ .\mathit{salary}))$
value $\bigwedge \quad s_{post}. \quad (\sigma_1,s_{post}) \models \mathit{not}(\upsilon(X_{Person}\mathit{3}\ .\mathit{boss@pre}))$
lemma $(\sigma_1,\sigma_1{}') \models \quad (X_{Person}\mathit{3}\ .\mathit{oclIsNew}())$
$\langle \mathit{proof} \rangle$

value $\bigwedge \quad s_{post}. \quad (\sigma_1,s_{post}) \models \quad (X_{Person}\mathit{4}\ .\mathit{boss@pre} \quad \doteq X_{Person}\mathit{5})$
value $(\sigma_1,\sigma_1{}') \models \mathit{not}(\upsilon(X_{Person}\mathit{4}\ .\mathit{boss@pre}\ .\mathit{salary}))$
value $\bigwedge \quad s_{post}. \quad (\sigma_1,s_{post}) \models \quad (X_{Person}\mathit{4}\ .\mathit{boss@pre}\ .\mathit{salary@pre} \quad \doteq \mathbf{3500})$
lemma $(\sigma_1,\sigma_1{}') \models \quad (X_{Person}\mathit{4}\ .\mathit{oclIsMaintained}())$
$\langle \mathit{proof} \rangle$

value $\bigwedge s_{pre} \quad . \quad (s_{pre},\sigma_1{}') \models \mathit{not}(\upsilon(X_{Person}\mathit{5}\ .\mathit{salary}))$
value $\bigwedge \quad s_{post}. \quad (\sigma_1,s_{post}) \models \quad (X_{Person}\mathit{5}\ .\mathit{salary@pre} \quad \doteq \mathbf{3500})$
value $\bigwedge s_{pre} \quad . \quad (s_{pre},\sigma_1{}') \models \mathit{not}(\upsilon(X_{Person}\mathit{5}\ .\mathit{boss}))$
lemma $(\sigma_1,\sigma_1{}') \models \quad (X_{Person}\mathit{5}\ .\mathit{oclIsDeleted}())$
$\langle \mathit{proof} \rangle$

value $\bigwedge s_{pre} \quad . \quad (s_{pre},\sigma_1{}') \models \mathit{not}(\upsilon(X_{Person}\mathit{6}\ .\mathit{boss}\ .\mathit{salary@pre}))$
value $\bigwedge \quad s_{post}. \quad (\sigma_1,s_{post}) \models \quad (X_{Person}\mathit{6}\ .\mathit{boss@pre} \quad \doteq X_{Person}\mathit{4})$
value $(\sigma_1,\sigma_1{}') \models \quad (X_{Person}\mathit{6}\ .\mathit{boss@pre}\ .\mathit{salary} \quad \doteq \mathbf{2900})$
value $\bigwedge \quad s_{post}. \quad (\sigma_1,s_{post}) \models \quad (X_{Person}\mathit{6}\ .\mathit{boss@pre}\ .\mathit{salary@pre} \quad \doteq \mathbf{2600})$
value $\bigwedge \quad s_{post}. \quad (\sigma_1,s_{post}) \models \quad (X_{Person}\mathit{6}\ .\mathit{boss@pre}\ .\mathit{boss@pre} \ \doteq X_{Person}\mathit{5})$
lemma $(\sigma_1,\sigma_1{}') \models \quad (X_{Person}\mathit{6}\ .\mathit{oclIsMaintained}())$
$\langle \mathit{proof} \rangle$

value $\bigwedge s_{pre}\ s_{post}. \quad (s_{pre},s_{post}) \models \quad \upsilon(X_{Person}\mathit{7}\ .\mathit{oclAsType}(\mathit{Person}))$
value $\bigwedge \quad s_{post}. \quad (\sigma_1,s_{post}) \models \mathit{not}(\upsilon(X_{Person}\mathit{7}\ .\mathit{oclAsType}(\mathit{Person})\ .\mathit{boss@pre}))$
lemma $\bigwedge s_{pre}\ s_{post}. \quad (s_{pre},s_{post}) \models \quad ((X_{Person}\mathit{7}\ .\mathit{oclAsType}(\mathit{Person})\ .\mathit{oclAsType}(\mathit{OclAny})$
$.\mathit{oclAsType}(\mathit{Person}))$
$\doteq (X_{Person}\mathit{7}\ .\mathit{oclAsType}(\mathit{Person})))$
$\langle \mathit{proof} \rangle$
lemma $(\sigma_1,\sigma_1{}') \models \quad (X_{Person}\mathit{7}\ .\mathit{oclIsNew}())$
$\langle \mathit{proof} \rangle$

value $\bigwedge s_{pre}\ s_{post}. \quad (s_{pre},s_{post}) \models \quad (X_{Person}\mathit{8} \ <> X_{Person}\mathit{7})$
value $\bigwedge s_{pre}\ s_{post}. \quad (s_{pre},s_{post}) \models \mathit{not}(\upsilon(X_{Person}\mathit{8}\ .\mathit{oclAsType}(\mathit{Person})))$
value $\bigwedge s_{pre}\ s_{post}. \quad (s_{pre},s_{post}) \models \quad (X_{Person}\mathit{8}\ .\mathit{oclIsTypeOf}(\mathit{OclAny}))$
value $\bigwedge s_{pre}\ s_{post}. \quad (s_{pre},s_{post}) \models \quad \mathit{not}(X_{Person}\mathit{8}\ .\mathit{oclIsTypeOf}(\mathit{Person}))$
value $\bigwedge s_{pre}\ s_{post}. \quad (s_{pre},s_{post}) \models \quad \mathit{not}(X_{Person}\mathit{8}\ .\mathit{oclIsKindOf}(\mathit{Person}))$

value $\bigwedge s_{pre}\ s_{post}.\quad (s_{pre},s_{post}) \models \quad (X_{Person}8\ .oclIsKindOf(OclAny))$

lemma *σ-modifiedonly*: $(\sigma_1,\sigma_1{}') \models (Set\{\ X_{Person}1\ .oclAsType(OclAny)$
$\quad ,\ X_{Person}2\ .oclAsType(OclAny)$
$\quad (*,\ X_{Person}3\ .oclAsType(OclAny)*)$
$\quad ,\ X_{Person}4\ .oclAsType(OclAny)$
$\quad (*,\ X_{Person}5\ .oclAsType(OclAny)*)$
$\quad ,\ X_{Person}6\ .oclAsType(OclAny)$
$\quad (*,\ X_{Person}7\ .oclAsType(OclAny)*)$
$\quad (*,\ X_{Person}8\ .oclAsType(OclAny)*)$
$\quad (*,\ X_{Person}9\ .oclAsType(OclAny)*)\}{-}{>}oclIsModifiedOnly())$
⟨*proof*⟩

lemma $(\sigma_1,\sigma_1{}') \models ((X_{Person}9\ @pre\ (\lambda x.\ \lfloor OclAsType_{Person}\text{-}\mathfrak{A}\ x\rfloor))\ \triangleq X_{Person}9)$
⟨*proof*⟩

lemma $(\sigma_1,\sigma_1{}') \models ((X_{Person}9\ @post\ (\lambda x.\ \lfloor OclAsType_{Person}\text{-}\mathfrak{A}\ x\rfloor))\ \triangleq X_{Person}9)$
⟨*proof*⟩

lemma $(\sigma_1,\sigma_1{}') \models (((X_{Person}9\ .oclAsType(OclAny))\ @pre\ (\lambda x.\ \lfloor OclAsType_{OclAny}\text{-}\mathfrak{A}\ x\rfloor)) \triangleq$
$\quad ((X_{Person}9\ .oclAsType(OclAny))\ @post\ (\lambda x.\ \lfloor OclAsType_{OclAny}\text{-}\mathfrak{A}\ x\rfloor)))$
⟨*proof*⟩

lemma *perm-σ₁′* : $\sigma_1{}' = (\!|\ heap = empty$
$\quad (oid8 \mapsto in_{Person}\ person9)$
$\quad (oid7 \mapsto in_{OclAny}\ person8)$
$\quad (oid6 \mapsto in_{OclAny}\ person7)$
$\quad (oid5 \mapsto in_{Person}\ person6)$
$\quad (*oid4*)$
$\quad (oid3 \mapsto in_{Person}\ person4)$
$\quad (oid2 \mapsto in_{Person}\ person3)$
$\quad (oid1 \mapsto in_{Person}\ person2)$
$\quad (oid0 \mapsto in_{Person}\ person1)$
$\quad ,\ assocs_2 = assocs_2\ \sigma_1{}'$
$\quad ,\ assocs_3 = assocs_3\ \sigma_1{}'\ |\!)$
⟨*proof*⟩

declare *const-ss* [*simp*]

lemma $\bigwedge\sigma_1.$
$(\sigma_1,\sigma_1{}') \models (Person\ .allInstances() \doteq Set\{\ X_{Person}1,\ X_{Person}2,\ X_{Person}3,\ X_{Person}4(*,\ X_{Person}5*),\ X_{Person}6,$
$X_{Person}7\ .oclAsType(Person)(*,\ X_{Person}8*),\ X_{Person}9\ \})$
⟨*proof*⟩

lemma $\bigwedge\sigma_1.$
$(\sigma_1,\sigma_1{}') \models (OclAny\ .allInstances() \doteq Set\{\ X_{Person}1\ .oclAsType(OclAny),\ X_{Person}2\ .oclAsType(OclAny),$

$X_{Person}3$ .oclAsType(OclAny), $X_{Person}4$ .oclAsType(OclAny)
(*, $X_{Person}5$*), $X_{Person}6$ .oclAsType(OclAny),
$X_{Person}7$, $X_{Person}8$, $X_{Person}9$ .oclAsType(OclAny) })

⟨*proof*⟩

end

7.2. The Employee Design Model (OCL)

theory
Employee-DesignModel-OCLPart
imports
Employee-DesignModel-UMLPart
begin

7.2.1. Standard State Infrastructure

Ideally, these definitions are automatically generated from the class model.

7.2.2. Invariant

These recursive predicates can be defined conservatively by greatest fix-point constructions—automatically. See [4, 6] for details. For the purpose of this example, we state them as axioms here.

axiomatization *inv-Person* :: *Person* ⇒ *Boolean*
where $A : (\tau \models (\delta\ self)) \longrightarrow$
$(\tau \models inv\text{-}Person(self)) =$
$((\tau \models (self\ .boss \doteq null)) \vee$
$(\ \tau \models (self\ .boss <> null) \wedge (\tau \models ((self\ .salary)\ \ `\leq\ \ (self\ .boss\ .salary)))\ \wedge$
$(\tau \models (inv\text{-}Person(self\ .boss)))))$

axiomatization *inv-Person-at-pre* :: *Person* ⇒ *Boolean*
where $B : (\tau \models (\delta\ self)) \longrightarrow$
$(\tau \models inv\text{-}Person\text{-}at\text{-}pre(self)) =$
$((\tau \models (self\ .boss@pre \doteq null)) \vee$
$(\ \tau \models (self\ .boss@pre <> null) \wedge$
$(\tau \models (self\ .boss@pre\ .salary@pre\ `\leq\ self\ .salary@pre))\ \wedge$
$(\tau \models (inv\text{-}Person\text{-}at\text{-}pre(self\ .boss@pre)))))$

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* ⇒ $(\mathfrak{A})st$ ⇒ *bool* **where**
$(\tau \models (\delta\ self)) \Longrightarrow ((\tau \models (self\ .boss \doteq null)) \vee$
$(\tau \models (self\ .boss <> null) \wedge (\tau \models (self\ .boss\ .salary\ `\leq\ self\ .salary))\ \wedge$

$(\; (inv(self \; .boss))\tau \;)))$
$\Longrightarrow (\; inv \; self \; \tau)$

7.2.3. The Contract of a Recursive Query

The original specification of a recursive query :

```
context Person::contents():Set(Integer)
post:  result = if self.boss = null
                 then Set{i}
                 else self.boss.contents()->including(i)
                 endif
```

consts $\mathit{dot\text{-}contents} :: \mathit{Person} \Rightarrow \mathit{Set\text{-}Integer} \;\; ((\mathit{1}(\text{-}).\mathit{contents}'(')) \; \mathit{50})$

axiomatization where $\mathit{dot\text{-}contents\text{-}def}$:
$(\tau \models ((\mathit{self}).\mathit{contents}() \triangleq \mathit{result})) =$
$\;(\mathit{if} \; (\delta \; \mathit{self}) \; \tau = \mathit{true} \; \tau$
$\;\;\mathit{then} \; ((\tau \models \mathit{true}) \wedge$
$\quad\quad (\tau \models (\mathit{result} \triangleq \mathit{if} \; (\mathit{self} \; .\mathit{boss} \doteq \mathit{null})$
$\quad\quad\quad\quad \mathit{then} \; (\mathit{Set}\{\mathit{self} \; .\mathit{salary}\})$
$\quad\quad\quad\quad \mathit{else} \; (\mathit{self} \; .\mathit{boss} \; .\mathit{contents}() {-}{>} \mathit{including}(\mathit{self} \; .\mathit{salary}))$
$\quad\quad\quad\quad \mathit{endif})))$
$\;\;\mathit{else} \; \tau \models \mathit{result} \triangleq \mathit{invalid})$

consts $\mathit{dot\text{-}contents\text{-}AT\text{-}pre} :: \mathit{Person} \Rightarrow \mathit{Set\text{-}Integer} \;\; ((\mathit{1}(\text{-}).\mathit{contents@pre}'(')) \; \mathit{50})$

axiomatization where $\mathit{dot\text{-}contents\text{-}AT\text{-}pre\text{-}def}$:
$(\tau \models (\mathit{self}).\mathit{contents@pre}() \triangleq \mathit{result}) =$
$\;(\mathit{if} \; (\delta \; \mathit{self}) \; \tau = \mathit{true} \; \tau$
$\;\;\mathit{then} \; \tau \models \mathit{true} \wedge \quad\quad\quad\quad\quad\quad\quad\quad (* \; \mathit{pre} \; *)$
$\quad\quad \tau \models (\mathit{result} \triangleq \mathit{if} \; (\mathit{self}).\mathit{boss@pre} \doteq \mathit{null} \;\; (* \; \mathit{post} \; *)$
$\quad\quad\quad\quad \mathit{then} \; \mathit{Set}\{(\mathit{self}).\mathit{salary@pre}\}$
$\quad\quad\quad\quad \mathit{else} \; (\mathit{self}).\mathit{boss@pre} \; .\mathit{contents@pre}() {-}{>} \mathit{including}(\mathit{self} \; .\mathit{salary@pre})$
$\quad\quad\quad\quad \mathit{endif})$
$\;\;\mathit{else} \; \tau \models \mathit{result} \triangleq \mathit{invalid})$

These `@pre` variants on methods are only available on queries, i. e., operations without side-effect.

7.2.4. The Contract of a Method

The specification in high-level OCL input syntax reads as follows:

```
context Person::insert(x:Integer)
post: contents():Set(Integer)
contents() = contents@pre()->including(x)
```

consts $\mathit{dot\text{-}insert} :: \mathit{Person} \Rightarrow \mathit{Integer} \Rightarrow \mathit{Void} \;\; ((\mathit{1}(\text{-}).\mathit{insert}'(\text{-}')) \; \mathit{50})$

axiomatization where *dot-insert-def*:

$$
\begin{array}{l}
(\tau \models ((\mathit{self}).\mathit{insert}(x) \triangleq \mathit{result})) = \\
\;(\mathit{if}\ \ (\delta\ \mathit{self})\ \tau = \mathit{true}\ \tau \land (\upsilon\ x)\ \tau = \mathit{true}\ \tau \\
\;\;\mathit{then}\ \tau \models \mathit{true} \land \\
\;\;\;\;\;\;\tau \models ((\mathit{self}).\mathit{contents}() \triangleq (\mathit{self}).\mathit{contents}@\mathit{pre}(){-}{>}\mathit{including}(x)) \\
\;\;\mathit{else}\ \tau \models ((\mathit{self}).\mathit{insert}(x) \triangleq \mathit{invalid}))
\end{array}
$$

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.[1] Moreover, all derived execution rules are by construction type-safe (which would be an issue, if we had chosen to use an object universe construction in Zermelo-Fraenkel set theory as an alternative approach to subtyping.). In more detail, our theory gives answers and concrete solutions to a number of open major issues for the UML/OCL standardization:

1. the role of the two exception elements invalid and null, the former usually assuming strict evaluation while the latter ruled by non-strict evaluation.

2. the functioning of the resulting four-valued logic, together with safe rules (for example foundation9 – foundation12 in Section 3.5.2) that allow a reduction to two-valued reasoning as required for many automated provers. The resulting logic still enjoys the rules of a strong Kleene Logic in the spirit of the Amsterdam Manifesto [19].

3. the complicated life resulting from the two necessary equalities: the standard's "strict weak referential equality" as default (written $\_ \doteq \_$ throughout this document) and the strong equality (written $\_ \triangleq \_$), which follows the logical Leibniz principle that "equals can be replaced by equals." Which is not necessarily the case if invalid or objects of different states are involved.

4. a type-safe representation of objects and a clarification of the old idea of a one-to-one correspondence between object representations and object-id's, which became a state invariant.

5. a simple concept of state-framing via the novel operator `_->oclIsModifiedOnly()` and its consequences for strong and weak equality.

[1] Our two examples of Employee_DesignModel (see Chapter 7) sketch how this construction can be captured by an automated process.

6. a semantic view on subtyping clarifying the role of static and dynamic type (aka *apparent* and *actual* type in Java terminology), and its consequences for casts, dynamic type-tests, and static types.

7. a semantic view on path expressions, that clarify the role of invalid and null as well as the tricky issues related to de-referentiation in pre- and post state.

8. an optional extension of the OCL semantics by *infinite* sets that provide means to represent "the set of potential objects or values" to state properties over them (this will be an important feature if OCL is intended to become a full-blown code annotation language in the spirit of JML [25] for semi-automated code verification, and has been considered desirable in the Aachen Meeting [15]).

Moreover, we managed to make our theory in large parts executable, which allowed us to include mechanically checked value-statements that capture numerous corner-cases relevant for OCL implementors. Among many minor issues, we thus pin-pointed the behavior of `null` in collections as well as in casts and the desired `isKindOf`-semantics of `allInstances()`.

8.2. Lessons Learned

While our paper and pencil arguments, given in [13], turned out to be essentially correct, there had also been a lesson to be learned: If the logic is not defined as a Kleene-Logic, having a structure similar to a complete partial order (CPO), reasoning becomes complicated: several important algebraic laws break down which makes reasoning in OCL inherent messy and a semantically clean compilation of OCL formulae to a two-valued presentation, that is amenable to animators like KodKod [36] or SMT-solvers like Z3 [20] completely impractical. Concretely, if the expression `not(null)` is defined `invalid` (as is the case in the present standard [33]), 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

[1] P. B. Andrews. *Introduction to Mathematical Logic and Type Theory: To Truth through Proof.* Kluwer Academic Publishers, Dordrecht, 2nd edition, 2002. ISBN 1-402-00763-9.

[2] C. Barrett and C. Tinelli. Cvc3. In W. Damm and H. Hermanns, editors, *CAV*, volume 4590 of *Lecture Notes in Computer Science*, pages 298–302. Springer-Verlag, 2007. ISBN 978-3-540-73367-6. doi: 10.1007/978-3-540-73368-3_34.

[3] J. C. Blanchette and T. Nipkow. Nitpick: A counterexample generator for higher-order logic based on a relational model finder. In M. Kaufmann and L. C. Paulson, editors, *ITP*, volume 6172 of *Lecture Notes in Computer Science*, pages 131–146. Springer-Verlag, 2010. ISBN 978-3-642-14051-8. doi: 10.1007/978-3-642-14052-5_11.

[4] A. D. Brucker. *An Interactive Proof Environment for Object-oriented Specifications.* PhD thesis, ETH Zurich, Mar. 2007. URL http://www.brucker.ch/bibliography/abstract/brucker-interactive-2007. ETH Dissertation No. 17097.

[5] A. D. Brucker and B. Wolff. A proposal for a formal OCL semantics in Isabelle/HOL. In V. A. Carreño, C. A. Muñoz, and S. Tahar, editors, *Theorem Proving in Higher Order Logics (TPHOLs)*, number 2410 in Lecture Notes in Computer Science, pages 99–114. Springer-Verlag, Heidelberg, 2002. ISBN 3-540-44039-9. doi: 10.1007/3-540-45685-6_8. URL http://www.brucker.ch/bibliography/abstract/brucker.ea-proposal-2002.

[6] A. D. Brucker and B. Wolff. The HOL-OCL book. Technical Report 525, ETH Zurich, 2006. URL http://www.brucker.ch/bibliography/abstract/brucker.ea-hol-ocl-book-2006.

[7] A. D. Brucker and B. Wolff. An extensible encoding of object-oriented data models in hol. *Journal of Automated Reasoning*, 41:219–249, 2008. ISSN 0168-7433. doi: 10.1007/s10817-008-9108-3. URL http://www.brucker.ch/bibliography/abstract/brucker.ea-extensible-2008-b.

[8] A. D. Brucker and B. Wolff. HOL-OCL – A Formal Proof Environment for UML/OCL. In J. Fiadeiro and P. Inverardi, editors, *Fundamental Approaches to Software Engineering (FASE08)*, number 4961 in Lecture Notes in Computer Science, pages 97–100. Springer-Verlag, Heidelberg, 2008. doi: 10.1007/978-3-540-78743-3_8. URL http://www.brucker.ch/bibliography/abstract/brucker.ea-hol-ocl-2008.

[9] A. D. Brucker and B. Wolff. HOL-TestGen: An interactive test-case generation framework. In M. Chechik and M. Wirsing, editors, *Fundamental Approaches to Software Engineering (FASE09)*, number 5503 in Lecture Notes in Computer Science, pages 417–420. Springer-Verlag, Heidelberg, 2009. doi: 10.1007/978-3-642-00593-0_28. URL http://www.brucker.ch/bibliography/abstract/brucker.ea-hol-testgen-2009.

[10] A. D. Brucker and B. Wolff. Semantics, calculi, and analysis for object-oriented specifications. *Acta Informatica*, 46(4):255–284, July 2009. ISSN 0001-5903. doi: 10.1007/s00236-009-0093-8. URL http://www.brucker.ch/bibliography/abstract/brucker.ea-semantics-2009.

[11] A. D. Brucker, J. Doser, and B. Wolff. Semantic issues of OCL: Past, present, and future. *Electronic Communications of the EASST*, 5, 2006. ISSN 1863-2122. URL http://www.brucker.ch/bibliography/abstract/brucker.ea-semantic-2006-b.

[12] A. D. Brucker, J. Doser, and B. Wolff. A model transformation semantics and analysis methodology for SecureUML. In O. Nierstrasz, J. Whittle, D. Harel, and G. Reggio, editors, *MoDELS 2006: Model Driven Engineering Languages and Systems*, number 4199 in Lecture Notes in Computer Science, pages 306–320. Springer-Verlag, Heidelberg, 2006. doi: 10.1007/11880240_22. URL http://www.brucker.ch/bibliography/abstract/brucker.ea-transformation-2006. An extended version of this paper is available as ETH Technical Report, no. 524.

[13] A. D. Brucker, M. P. Krieger, and B. Wolff. Extending OCL with null-references. In S. Gosh, editor, *Models in Software Engineering*, number 6002 in Lecture Notes in Computer Science, pages 261–275. Springer-Verlag, Heidelberg, 2009. doi: 10.1007/978-3-642-12261-3_25. URL http://www.brucker.ch/bibliography/abstract/brucker.ea-ocl-null-2009. Selected best papers from all satellite events of the MoDELS 2009 conference.

[14] A. D. Brucker, M. P. Krieger, D. Longuet, and B. Wolff. A specification-based test case generation method for UML/OCL. In J. Dingel and A. Solberg, editors, *MoDELS Workshops*, number 6627 in Lecture Notes in Computer Science, pages 334–348. Springer-Verlag, Heidelberg, 2010. ISBN 978-3-642-21209-3. doi: 10.1007/978-3-642-21210-9_33. URL http://www.brucker.ch/bibliography/abstract/brucker.ea-ocl-testing-2010. Selected best papers from all satellite events of the MoDELS 2010 conference. Workshop on OCL and Textual Modelling.

[15] A. D. Brucker, D. Chiorean, T. Clark, B. Demuth, M. Gogolla, D. Plotnikov, B. Rumpe, E. D. Willink, and B. Wolff. Report on the Aachen OCL meeting. In J. Cabot, M. Gogolla, I. Rath, and E. Willink, editors, *Proceedings of the MODELS 2013 OCL Workshop (OCL 2013)*, volume 1092 of *CEUR Workshop Proceedings*, pages 103–111. CEUR-WS.org, 2013. URL http://www.brucker.ch/bibliography/abstract/brucker.ea-summary-aachen-2013.

[16] A. D. Brucker, D. Longuet, F. Tuong, and B. Wolff. On the semantics of object-oriented data structures and path expressions. In *OCL@MoDELS*, pages 23–32, 2013.

[17] A. Church. A formulation of the simple theory of types. *Journal of Symbolic Logic*, 5(2):56–68, June 1940.

[18] T. Clark and J. Warmer, editors. *Object Modeling with the OCL: The Rationale behind the Object Constraint Language*, volume 2263 of *Lecture Notes in Computer Science*, Heidelberg, 2002. Springer-Verlag. ISBN 3-540-43169-1.

[19] S. Cook, A. Kleppe, R. Mitchell, B. Rumpe, J. Warmer, and A. Wills. The amsterdam manifesto on OCL. In Clark and Warmer [18], pages 115–149. ISBN 3-540-43169-1.

[20] L. M. de Moura and N. Bjørner. Z3: An efficient SMT solver. In C. R. Ramakrishnan and J. Rehof, editors, *TACAS*, volume 4963 of *Lecture Notes in Computer Science*, pages 337–340, Heidelberg, 2008. Springer-Verlag. ISBN 978-3-540-78799-0. doi: 10.1007/978-3-540-78800-3_24.

[21] M. Gogolla and M. Richters. Expressing UML class diagrams properties with OCL. In Clark and Warmer [18], pages 85–114. ISBN 3-540-43169-1.

[22] A. Hamie, F. Civello, J. Howse, S. Kent, and R. Mitchell. Reflections on the Object Constraint Language. In J. Bézivin and P.-A. Muller, editors, *The Unified Modeling Language. «UML»'98: Beyond the Notation*, volume 1618 of *Lecture Notes in Computer Science*, pages 162–172, Heidelberg, 1998. Springer-Verlag. ISBN 3-540-66252-9. doi: 10.1007/b72309.

[23] P. Kosiuczenko. Specification of invariability in OCL. In O. Nierstrasz, J. Whittle, D. Harel, and G. Reggio, editors, *Model Driven Engineering Languages and Systems (MoDELS)*, volume 4199 of *Lecture Notes in Computer Science*, pages 676–691, Heidelberg, 2006. Springer-Verlag. ISBN 978-3-540-45772-5. doi: 10.1007/11880240_47.

[24] M. P. Krieger, A. Knapp, and B. Wolff. Generative programming and component engineering. In E. Visser and J. Järvi, editors, *International Conference on Generative Programming and Component Engineering (GPCE 2010)*, pages 53–62. ACM, Oct. 2010. ISBN 978-1-4503-0154-1.

[25] G. T. Leavens, E. Poll, C. Clifton, Y. Cheon, C. Ruby, D. R. Cok, P. Müller, J. Kiniry, and P. Chalin. JML reference manual (revision 1.2), Feb. 2007. Available from http://www.jmlspecs.org.

[26] L. Mandel and M. V. Cengarle. On the expressive power of OCL. In J. M. Wing, J. Woodcock, and J. Davies, editors, *World Congress on Formal Methods in the Development of Computing Systems (FM)*, volume 1708 of *Lecture Notes in*

Computer Science, pages 854–874, Heidelberg, 1999. Springer-Verlag. ISBN 3-540-66587-0.

[27] T. Nipkow, L. C. Paulson, and M. Wenzel. *Isabelle/HOL—A Proof Assistant for Higher-Order Logic*, volume 2283 of *Lecture Notes in Computer Science*. Springer-Verlag, Heidelberg, 2002. doi: 10.1007/3-540-45949-9.

[28] Object Management Group. Object constraint language specification (version 1.1), Sept. 1997. Available as OMG document ad/97-08-08.

[29] Object Management Group. UML 2.0 OCL specification, Oct. 2003. Available as OMG document ptc/03-10-14.

[30] Object Management Group. UML 2.0 OCL specification, Apr. 2006. Available as OMG document formal/06-05-01.

[31] Object Management Group. UML 2.4.1: Infrastructure specification, Aug. 2011. Available as OMG document formal/2011-08-05.

[32] Object Management Group. UML 2.4.1: Superstructure specification, Aug. 2011. Available as OMG document formal/2011-08-06.

[33] Object Management Group. UML 2.3.1 OCL specification, Feb. 2012. Available as OMG document formal/2012-01-01.

[34] A. Riazanov and A. Voronkov. Vampire. In H. Ganzinger, editor, *CADE*, volume 1632 of *Lecture Notes in Computer Science*, pages 292–296. Springer-Verlag, 1999. ISBN 3-540-66222-7. doi: 10.1007/3-540-48660-7_26.

[35] M. Richters. *A Precise Approach to Validating UML Models and OCL Constraints*. PhD thesis, Universität Bremen, Logos Verlag, Berlin, BISS Monographs, No. 14, 2002.

[36] E. Torlak and D. Jackson. Kodkod: A relational model finder. In O. Grumberg and M. Huth, editors, *TACAS*, volume 4424 of *Lecture Notes in Computer Science*, pages 632–647, Heidelberg, 2007. Springer-Verlag. ISBN 978-3-540-71208-4. doi: 10.1007/978-3-540-71209-1_49.

[37] M. Wenzel and B. Wolff. Building formal method tools in the Isabelle/Isar framework. In K. Schneider and J. Brandt, editors, *TPHOLs 2007*, number 4732 in Lecture Notes in Computer Science, pages 352–367. Springer-Verlag, Heidelberg, 2007. doi: 10.1007/978-3-540-74591-4_26.

[38] M. M. Wenzel. *Isabelle/Isar — a versatile environment for human-readable formal proof documents*. PhD thesis, TU München, München, Feb. 2002. URL http://tumb1.biblio.tu-muenchen.de/publ/diss/in/2002/wenzel.html.