Software Design, Modelling and Analysis in UML

Lecture 20: Inheritance I

2014-02-03

Prof. Dr. Andreas Podelski, **Dr. Bernd Westphal**

Albert-Ludwigs-Universität Freiburg, Germany

Contents & Goals

Last Lecture:

- Live Sequence Charts Semantics

This Lecture:

- **Educational Objectives:** Capabilities for following tasks/questions.
  - What's the Liskov Substitution Principle?
  - What is late/early binding?
  - What is the subset, what the uplink semantics of inheritance?
  - What's the effect of inheritance on LSCs, State Machines, System States?
  - What's the idea of Meta-Modelling?
- **Content:**
  - Quickly: Behavioural Features, Active vs. Passive
  - Inheritance in UML: concrete syntax
  - Liskov Substitution Principle — desired semantics
  - Two approaches to obtain desired semantics
  - The UML Meta Model

Active and Passive Objects [Harel and Gery, 1997]

What about non-Active Objects?

Recall:

- We're **still** working under the assumption that all classes in the class diagram (and thus all objects) are **active**.
- That is, each object has its own thread of control and is (if stable) at any time ready to process an event from the ether.

But the world doesn't consist of only active objects.

For instance, in the crossing controller from the exercises we could wish to have the whole system live in one thread of control.

So we have to address questions like:

- Can we send events to a non-active object?
- And if so, when are these events processed?
- etc.

Active and Passive Objects: Nomenclature

[Harel and Gery, 1997] propose the following (orthogonal!) notions:

- A class (and thus the instances of this class) is either **active** or **passive** as declared in the class diagram.
  - An **active** object has (in the operating system sense) an own thread: an own program counter, an own stack, etc.
  - A **passive** object doesn't.
- A class is either **reactive** or **non-reactive**.
  - A **reactive** class has a (non-trivial) state machine.
  - A **non-reactive** one hasn't.

Which combinations do we understand?

	active	passive
reactive	✓	?
non-reactive	(✓)	(✓)

Passive and Reactive

- So why don't we understand passive/reactive?
- Assume passive objects u_1 and u_2, and active object u, and that there are events in the ether for all three.

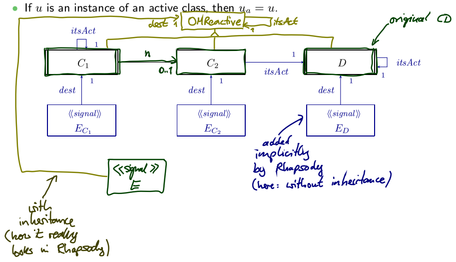
  Which of them (can) start a run-to-completion step...?
  Do run-to-completion steps still interleave...?

Reasonable Approaches:

- **Avoid** — for instance, by
  - require that **reactive implies active** for model well-formedness.
  - requiring for model well-formedness that events are **never sent** to instances of non-reactive classes.
- **Explain** — here: (following [Harel and Gery, 1997])
  - Delegate all dispatching of events to the active objects.

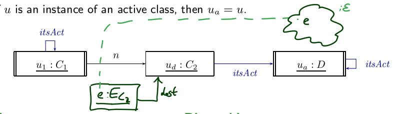
Passive Reactive Classes

- Firstly, establish that each object u knows, via (implicit) link $itsAct$, **the active object** u_{act} which is responsible for dispatching events to u.
- If u is an instance of an active class, then $u_a = u$.



Passive Reactive Classes

- Firstly, establish that each object u knows, via (implicit) link $itsAct$, **the active object** u_{act} which is responsible for dispatching events to u.
- If u is an instance of an active class, then $u_a = u$.



Sending an event:

- Establish that of each signal we have a version E_C with an association $dest : C_{0,1}$, $C \in \mathscr{C}$.
- Then $n!E$ in $u_1 : C_1$ becomes:
- Create an instance u_e of E_{C_2} and set u_e's $dest$ to $u_d := \sigma(u_1)(n)$.
- Send to $u_a := \sigma(\sigma(u_1)(n))(itsAct)$, i.e., $\varepsilon' = \varepsilon \oplus (u_a, u_e)$.

Dispatching an event:

- Observation: the ether only has events for active objects.
- Say u_e is ready in the ether for u_a.
- Then u_a asks $\sigma(u_e)(dest) = u_d$ to process u_e — and waits until completion of corresponding RTC.
- u_d may in particular discard event.

And What About Methods?

And What About Methods?

- In the current setting, the (local) state of objects is only modified by actions of transitions, which we abstract to transformers.
- In general, there are also **methods**.
- UML follows an approach to separate
  - the **interface declaration** from
  - the **implementation**.

  In C++ lingo: distinguish **declaration** and **definition** of method.
- In UML, the former is called **behavioural feature** and can (roughly) be
  - a **call interface** $f(\tau_{1_1}, \dots, \tau_{n_1}) : \tau_1$
  - a **signal name** E

C
$\xi_1\ f(\tau_{1,1}, \dots, \tau_{1,n_1}) : \tau_1\ P_1$ $\xi_2\ F(\tau_{2,1}, \dots, \tau_{2,n_2}) : \tau_2\ P_2$
$\langle\langle signal\rangle\rangle\ E$

Note: The signal list is redundant as it can be looked up in the state machine of the class. But: certainly useful for documentation.

Behavioural Features

C
$\xi_1\ f(\tau_{1,1}, \dots, \tau_{1,n_1}) : \tau_1\ P_1$ $\xi_2\ F(\tau_{2,1}, \dots, \tau_{2,n_2}) : \tau_2\ P_2$
$\langle\langle signal\rangle\rangle\ E$

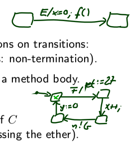
Semantics:

- The **implementation** of a behavioural feature can be provided by:
  - An **operation**.

    In our setting, we simply assume a transformer like T_f.

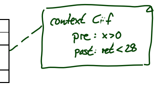
    It is then, e.g. clear how to admit method calls as actions on transitions: function composition of transformers (clear but tedious: non-termination).

    In a setting with Java as action language: operation is a method body.
  - The class' **state-machine** ("triggered operation").
    - Calling F with n_2 parameters for a stable instance of C creates an auxiliary event F and dispatches it (bypassing the ether).
    - Transition actions may fill in the return value.
    - On completion of the RTC step, the call returns.
    - For a non-stable instance, the caller blocks until stability is reached again.



Behavioural Features: Visibility and Properties

C
$\xi_1\ f(\tau_{1,1}, \dots, \tau_{1,n_1}) : \tau_1\ P_1$ $\xi_2\ F(\tau_{2,1}, \dots, \tau_{2,n_2}) : \tau_2\ P_2$
$\langle\langle signal\rangle\rangle\ E$



- **Visibility**:
  - Extend typing rules to sequences of actions such that a well-typed action sequence only calls visible methods.
- **Useful properties**:
  - **concurrency**
    - **concurrent** — is thread safe
    - **guarded** — some mechanism ensures/should ensure mutual exclusion
    - **sequential** — is not thread safe, users have to ensure mutual exclusion
  - **isQuery** — doesn't modify the state space (thus thread safe)
- For simplicity, we leave the notion of steps untouched, we construct our semantics around state machines.

  Yet we could explain pre/post in OCL (if we wanted to).

State Machines: Discussion.

Semantic Variation Points

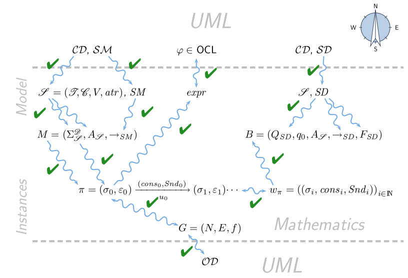
Pessimistic view: They are legion...

- **For instance,**
  - allow **absence of initial pseudo-states**
    can then "be" in enclosing state without being in any substate; or assume one of the children states non-deterministically
  - (implicitly) **enforce determinism**, e.g.
    by considering the order in which things have been added to the CASE tool's repository, or graphical order
  - allow **true concurrency**

  Exercise: Search the standard for "semantical variation point".
- [Crane and Dingel, 2007], e.g., provide an in-depth comparison of Statemate, UML, and Rhapsody state machines — the bottom line is:
  - **the intersection is not empty**
    (i.e. there are pictures that mean the same thing to all three communities)
  - **none is the subset of another**
    (i.e. for each pair of communities exist pictures meaning different things)

Optimistic view: tools exist with complete and consistent code generation.

Course Map



Inheritance: Syntax

~~Recall:~~ Abstract Syntax

Recall: a signature (with signals) is a tuple $\mathscr{S} = (\mathscr{T}, \mathscr{C}, V, atr, \mathscr{E})$.

Now (finally): extend to

$$\mathscr{S} = (\mathscr{T}, \mathscr{C}, V, atr, \mathscr{E}, F, mth, \lhd)$$

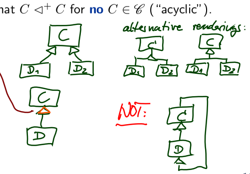
where F/mth are methods, analogously to attributes and

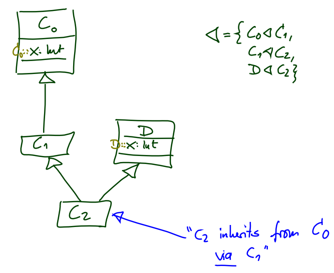
$$\lhd \subseteq (\mathscr{C} \times \mathscr{C}) \cup (\mathscr{E} \times \mathscr{E})$$

is a **generalisation** relation such that $C \lhd^+ C$ for **no** $C \in \mathscr{C}$ ("acyclic").

$C \lhd D$ reads as

- C is a generalisation of D,
- D is a specialisation of C,
- D inherits from C,
- D is a sub-class of C,
- C is a super-class of D,
- ...





Recall: Reflexive, Transitive Closure of Generalisation

Definition. Given classes $C_0, C_1, D \in \mathscr{C}$, we say D inherits from C_0 **via** C_1 if and only if there are $C_0^1, \dots C_0^n, C_1^1, \dots C_1^m \in \mathscr{C}$ such that

$$C_0 \lhd C_0^1 \lhd \dots C_0^n \lhd C_1 \lhd C_1^1 \lhd \dots C_1^m \lhd D.$$

We use '$\preceq$' to denote the reflexive, transitive closure of '$\lhd$'.

In the following, we assume

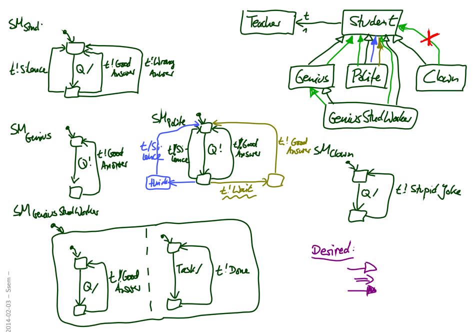
- that all attribute (method) names are of the form

$$C::v, \quad C \in \mathscr{C} \cup \mathscr{E} \qquad (C::f, \quad C \in \mathscr{C}),$$

- that we have $C::v \in atr(C)$ resp. $C::f \in mth(C)$ **if and only if** v (f) appears in an attribute (method) compartment of C in a class diagram.

We still want to accept "context C inv : $v < 0$", which v is meant? Later!

Inheritance: Desired Semantics



Desired Semantics of Specialisation: Subtyping

There is a classical description of what one **expects** from **sub-types**, which in the OO domain is closely related to inheritance:

The principle of type substitutability [Liskov, 1988, Liskov and Wing, 1994].
(**Liskov Substitution Principle** (LSP).)

"If for each object o_1 of type S there is an object o_2 of type T such that for all programs P defined in terms of T,
the behavior of P is unchanged when o_1 is substituted for o_2
then S is a **subtype** of T."

S sub-type of T $:\iff \forall o_1 \in S\ \exists o_2 \in T\ \forall P_T \bullet [\![P_T]\!](o_1) = [\![P_T]\!](o_2)$

Desired Semantics of Specialisation: Subtyping

There is a classical description of what one **expects** from **sub-types**, which in the OO domain is closely related to inheritance:

The principle of type substitutability [Liskov, 1988, Liskov and Wing, 1994].
(**Liskov Substitution Principle** (LSP).)

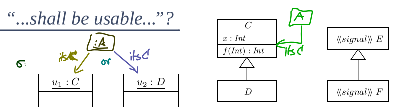
"If for each object o_1 of type S there is an object o_2 of type T such that for all programs P defined in terms of T,
the behavior of P is unchanged when o_1 is substituted for o_2
then S is a **subtype** of T."

In other words: [Fischer and Wehrheim, 2000]

"An instance of the **sub-type** shall be **usable** whenever an instance of the supertype was expected,
without a client being able to tell the difference."

So, what's "**usable**"? Who's a "**client**"? And what's a "**difference**"?

"...shall be usable..."?

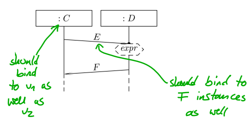


$I[\![\varphi]\!](\sigma, \{self \mapsto u_1\})$ vs. (*) $I[\![\varphi]\!](\sigma, \{self \mapsto u_2\})$ — value in σ may be different, but (*) must be defined!

- **OCL**:
  - context C inv : $x > 0$
- **Actions**:
  - $itsC.x = 0$
  - $itsC.f(0)$
  - $itsC\ !\ F$

  } must be defined
- **Triggers**:
  - $E[\dots]/\dots$

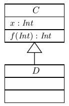
Sequence Diagrams:



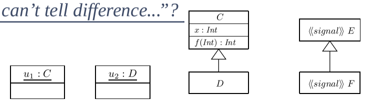
"...a client..."?

"An instance of the **sub-type** shall be **usable** whenever an instance of the supertype was expected, without **a client** being able to tell the **difference**."

- **Narrow** interpretation: another object in the model.
- **Wide** interpretation: another modeler.

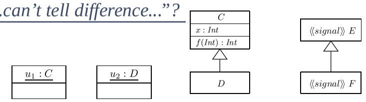


"...can't tell difference..."?



- **OCL**:
  - $I[\![\text{context } C \text{ inv} : x > 0]\!](\sigma_1, \emptyset)$ vs. $I[\![\text{context } C \text{ inv} : x > 0]\!](\sigma_2, \emptyset)$

"...can't tell difference..."?



- **Triggers**, **Actions**: if

$$(\sigma_0, \varepsilon_0) \xrightarrow[u_2]{(cons_0, Snd_0)} (\sigma_1, \varepsilon_1)$$

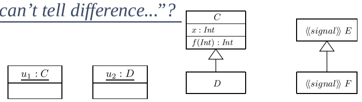
is possible, then

$$(\sigma_0, \varepsilon_0) \xrightarrow[u_1]{(cons_0, Snd_0)} (\sigma_1, \varepsilon_1)$$

should be possible – sub-type does less on inputs of super-type.

$[u_2/u_1]$, $u_2 \in \mathscr{D}(D)$, LSP, for some $u_1 \in \mathscr{D}(C)$ and a proper definition of $\cdot[\cdot/\cdot]$

"...can't tell difference..."?



- **Sequence Diagram**: $w \in \mathcal{L}(\mathcal{B}_L)$ implies $w \in \mathcal{L}(\mathcal{B}_L)$.

$[u_2/u_1]$, $\mathscr{D}(D)$, $\mathscr{D}(C)$

Motivations for Generalisation

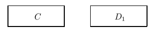
- **Re-use**,
- **Sharing**,
- **Avoiding Redundancy**,
- **Modularisation**,
- **Separation of Concerns**,
- **Abstraction**,
- **Extensibility**,
- ...

→ See textbooks on object-oriented analysis, development, programming.

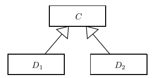
What Does [Fischer and Wehrheim, 2000] Mean for UML?

"An instance of the **sub-type** shall be **usable** whenever an instance of the supertype was expected, without **a client** being able to tell the **difference**."

- Wanted: sub-typing for UML.
- With



  we don't even have usability.
- It would be nice, if the well-formedness rules and semantics of

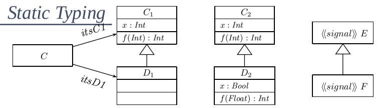


  would ensure D_1 **is a sub-type** of C:
  - that D_1 objects can be used interchangeably by everyone who is using C's,
  - is not able to tell the difference (i.e. see unexpected behaviour).

"...shall be usable..." for UML

Easy: Static Typing

Given:



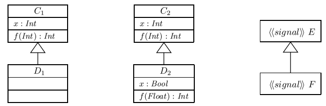
Wanted:

- $x > 0$ also **well-typed** for D_1
- assignment $itsC1 := itsD1$ being **well-typed**
- $itsC1.x = 0$, $itsC1.f(0)$, $itsC1 \,!\, F$
  being well-typed (and doing the right thing).

Approach:

- Simply define it as being well-typed,
  adjust system state definition to do the right thing.

Static Typing Cont'd



Notions (from category theory):

- **invariance**,
- **covariance**,
- **contravariance**.

We could call, e.g. a method, **sub-type preserving**, if and only if it

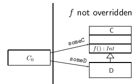
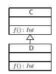
- accepts **more general** types as input (**contravariant**),
- provides a **more specialised** type as output (**covariant**).

This is a notion used by many programming languages — and easily type-checked.

Excursus: Late Binding of Behavioural Features

Late Binding

What transformer applies in what situation? (Early (compile time) binding.)

	f not overridden in D	f overridden in D	value of someC/ someD
			
someC -> f()			
someD -> f()			
someC -> f()			

What one could want is something different: (Late binding.)

someC -> f()			
someD -> f()			
someC -> f()			

Late Binding in the Standard and Programming Lang.

- In **the standard**, Section 11.3.10, "CallOperationAction":
  "**Semantic Variation Points**
  The mechanism for determining the method to be invoked as a result of a call operation is unspecified." [OMG, 2007b, 247]
- In C++,
  - methods are by default "(early) compile time binding",
  - can be declared to be "late binding" by keyword "`virtual`",
  - the declaration applies to all inheriting classes.
- In **Java**,
  - methods are "late binding";
  - there are patterns to imitate the effect of "early binding"

Exercise: What could have driven the designers of C++ to take that approach?

Late Binding in the Standard and Programming Lang.

- In **the standard**, Section 11.3.10, "CallOperationAction":
  "**Semantic Variation Points**
  The mechanism for determining the method to be invoked as a result of a call operation is unspecified." [OMG, 2007b, 247]
- In **C++**,
  - methods are by default "(early) compile time binding",
  - can be declared to be "late binding" by keyword "`virtual`",
  - the declaration applies to all inheriting classes.
- In **Java**,
  - methods are "late binding";
  - there are patterns to imitate the effect of "early binding"

Exercise: What could have driven the designers of C++ to take that approach?

Note: late binding typically applies only to **methods**, **not** to **attributes**.
(But: getter/setter methods have been invented recently.)

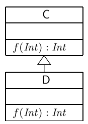
Back to the Main Track: "...tell the difference..." for UML

With Only Early Binding...

- ...we're **done** (if we realise it correctly in the framework).
- Then
  - if we're calling method f of an object u,
  - which is an instance of D with $C \preceq D$
  - via a C-link,
  - then we (by definition) only see and change the C-part.
  - We cannot tell whether u is a C or an D instance.

  So we immediately also have behavioural/dynamic subtyping.

Difficult: Dynamic Subtyping



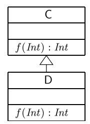
- $C::f$ and $D::f$ are **type compatible**, but D is **not necessarily** a **sub-type** of C.
- **Examples**: (C++)

```
int C::f(int) {
   return 0;
};
```

vs.

```
int D::f(int) {
   return 1;
};
```


Difficult: Dynamic Subtyping



- $C::f$ and $D::f$ are **type compatible**, but D is **not necessarily** a **sub-type** of C.
- **Examples**: (C++)

```
int C::f(int) {
   return 0;
};
```

vs.

```
int D::f(int) {
   return 1;
};
```

```
int C::f(int) {
   return (rand() % 2);
};
```

vs.

```
int D::f(int x) {
   return (x % 2);
};
```


Sub-Typing Principles Cont'd

- In the standard, Section 7.3.36, "**Operation**":
  "**Semantic Variation Points**
  [...] When operations are redefined in a specialization, rules regarding **invariance**, **covariance**, or **contravariance** of types and preconditions determine whether the specialized classifier is substitutable for its more general parent. Such rules constitute semantic variation points with respect to redefinition of operations." [OMG, 2007a, 106]

Sub-Typing Principles Cont'd

- In the standard, Section 7.3.36, "**Operation**":

  "**Semantic Variation Points**
  [...] When operations are redefined in a specialization, rules regarding **invariance**, **covariance**, or **contravariance** of types and preconditions determine whether the specialized classifier is substitutable for its more general parent. Such rules constitute semantic variation points with respect to redefinition of operations." [OMG, 2007a, 106]

- So, better: call a method **sub-type preserving**, if and only if it

  (i) accepts **more input values** (**contravariant**),

  (ii) on the **old values**, has **fewer behaviour** (**covariant**).

  Note: ~~This~~ (ii) is no longer a matter of simple type-checking!

Sub-Typing Principles Cont'd

- In the standard, Section 7.3.36, "**Operation**":

  "**Semantic Variation Points**
  [...] When operations are redefined in a specialization, rules regarding **invariance**, **covariance**, or **contravariance** of types and preconditions determine whether the specialized classifier is substitutable for its more general parent. Such rules constitute semantic variation points with respect to redefinition of operations." [OMG, 2007a, 106]

- So, better: call a method **sub-type preserving**, if and only if it

  (i) accepts **more input values** (**contravariant**),

  (ii) on the **old values**, has **fewer behaviour** (**covariant**).

  Note: ~~This~~ (ii) is no longer a matter of simple type-checking!

- And not necessarily the end of the story:
  - One could, e.g. want to consider execution time.
  - Or, like [Fischer and Wehrheim, 2000], relax to "fewer observable behaviour", thus admitting the sub-type to do more work on inputs.

  Note: "testing" differences depends on the **granularity** of the semantics.

Sub-Typing Principles Cont'd

- In the standard, Section 7.3.36, "**Operation**":

  "**Semantic Variation Points**
  [...] When operations are redefined in a specialization, rules regarding **invariance**, **covariance**, or **contravariance** of types and preconditions determine whether the specialized classifier is substitutable for its more general parent. Such rules constitute semantic variation points with respect to redefinition of operations." [OMG, 2007a, 106]

- So, better: call a method **sub-type preserving**, if and only if it

  (i) accepts **more input values** (**contravariant**),

  (ii) on the **old values**, has **fewer behaviour** (**covariant**).

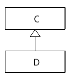
  Note: ~~This~~ (ii) is no longer a matter of simple type-checking!

- And not necessarily the end of the story:
  - One could, e.g. want to consider execution time.
  - Or, like [Fischer and Wehrheim, 2000], relax to "fewer observable behaviour", thus admitting the sub-type to do more work on inputs.

  Note: "testing" differences depends on the **granularity** of the semantics.

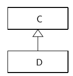
- **Related**: "has a weaker pre-condition," (**contravariant**),
  "has a stronger post-condition." (**covariant**).

Ensuring Sub-Typing for State Machines



- In the CASE tool we consider, multiple classes in an inheritance hierarchy can have state machines.

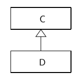
Ensuring Sub-Typing for State Machines



- In the CASE tool we consider, multiple classes in an inheritance hierarchy can have state machines.
- But the state machine of a sub-class **cannot** be drawn from scratch.
- Instead, the state machine of a sub-class can only be obtained by applying actions from a **restricted** set to a copy of the original one.

  Roughly (cf. User Guide, p. 760, for details),
  - add things into (hierarchical) states,
  - add more states,
  - attach a transition to a different target (limited).

Ensuring Sub-Typing for State Machines



- In the CASE tool we consider, multiple classes in an inheritance hierarchy can have state machines.
- But the state machine of a sub-class **cannot** be drawn from scratch.
- Instead, the state machine of a sub-class can only be obtained by applying actions from a **restricted** set to a copy of the original one.

  Roughly (cf. User Guide, p. 760, for details),
  - add things into (hierarchical) states,
  - add more states,
  - attach a transition to a different target (limited).

- They **ensure**, that the sub-class is a **behavioural sub-type** of the super class. (But method implementations can still destroy that property.)

- Technically, the idea is that (by late binding) only the state machine of the most specialised classes are running.

  By knowledge of the framework, the (code for) state machines of super-classes is still accessible — but using it is hardly a good idea...

Towards System States

Wanted: a formal representation of "if $C \preceq D$ then D **'is a'** C", that is,

(i) D has the same attributes and behavioural features as C, and

(ii) D objects (identities) can replace C objects.

Towards System States

Wanted: a formal representation of "if $C \preceq D$ then D **'is a'** C", that is,

(i) D has the same attributes and behavioural features as C, and

(ii) D objects (identities) can replace C objects.

We'll discuss **two approaches** to semantics:

- **Domain-inclusion** Semantics (more **theoretical**)
- **Uplink** Semantics (more **technical**)

Domain Inclusion Semantics

Domain Inclusion Structure

Let $\mathscr{S} = (\mathscr{T}, \mathscr{C}, V, atr, \mathscr{E}, F, mth, \lhd)$ be a signature.

Now a **structure** $\mathscr{D}$

- [**as before**] maps types, classes, associations to domains,
- [**for completeness**] methods to transformers,
- [**as before**] indentities of instances of classes not (transitively) related by generalisation are disjoint,
- [**changed**] the indentities of a super-class comprise all identities of sub-classes, i.e.

$$\forall C \in \mathscr{C} : \mathscr{D}(C) \supsetneq \bigcup_{C \lhd D} \mathscr{D}(D).$$

Note: the old setting coincides with the special case $\lhd\ = \emptyset$.

Domain Inclusion System States

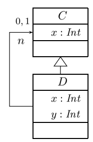
Now: a **system state** of $\mathscr{S}$ wrt. $\mathscr{D}$ is a **type-consistent** mapping

$$\sigma : \mathscr{D}(\mathscr{C}) \nrightarrow (V \nrightarrow (\mathscr{D}(\mathscr{T}) \cup \mathscr{D}(\mathscr{C}_{0,1}) \cup \mathscr{D}(\mathscr{C}_*)))$$

that is, for all $u \in \text{dom}(\sigma) \cap \mathscr{D}(C)$,

- [**as before**] $\sigma(u)(v) \in \mathscr{D}(\tau)$ if $v : \tau$, $\tau \in \mathscr{T}$ or $\tau \in \{C_*, C_{0,1}\}$.
- [**changed**] $\text{dom}(\sigma(u)) = \bigcup_{C_0 \preceq C} atr(C_0)$,

Example:



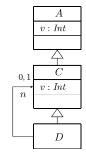
Note: the old setting still coincides with the special case $\lhd\ = \emptyset$.

Preliminaries: Expression Normalisation

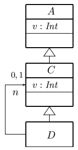
Recall:

- we want to allow, e.g., "context D inv : $v < 0$".
- we assume **fully qualified names**, e.g. $C::v$.

Intuitively, v shall denote the "**most special more general**" $C::v$ according to $\lhd$.



Preliminaries: Expression Normalisation



Recall:

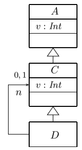
- we want to allow, e.g., "context D inv : $v < 0$".
- we assume **fully qualified names**, e.g. $C::v$.

Intuitively, v shall denote the "**most special more general**" $C::v$ according to $\lhd$.

To keep this out of typing rules, we assume that the following **normalisation** has been applied to all OCL expressions and all actions.

- Given expression v (or f) in **context** of class D, as determined by, e.g.
  - by the (type of the) navigation expression prefix, or
  - by the class, the state-machine where the action occcurs belongs to,
  - similar for method bodies,
- **normalise** v to (= replace by) $C::v$,
- where C is the **greatest** class wrt. "$\preceq$" such that
  - $C \preceq D$ and $C::v \in atr(C)$.

Preliminaries: Expression Normalisation



Recall:

- we want to allow, e.g., "context D inv : $v < 0$".
- we assume **fully qualified names**, e.g. $C::v$.

Intuitively, v shall denote the "**most special more general**" $C::v$ according to $\lhd$.

To keep this out of typing rules, we assume that the following **normalisation** has been applied to all OCL expressions and all actions.

- Given expression v (or f) in **context** of class D, as determined by, e.g.
  - by the (type of the) navigation expression prefix, or
  - by the class, the state-machine where the action occcurs belongs to,
  - similar for method bodies,
- **normalise** v to (= replace by) $C::v$,
- where C is the **greatest** class wrt. "$\preceq$" such that
  - $C \preceq D$ and $C::v \in atr(C)$.

If no (unique) such class exists, the model is considered **not well-formed**; the expression is ambiguous. Then: explicitly provide the **qualified name**.

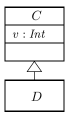
OCL Syntax and Typing

- Recall (part of the) OCL syntax and typing: $v, r \in V$; $C, D \in \mathscr{C}$

$$\begin{aligned} expr ::= \; & v(expr_1) && : \tau_C \to \tau(v), && \text{if } v : \tau \in \mathscr{T} \\ | \; & r(expr_1) && : \tau_C \to \tau_D, && \text{if } r : D_{0,1} \\ | \; & r(expr_1) && : \tau_C \to Set(\tau_D), && \text{if } r : D_* \end{aligned}$$

The definition of the semantics remains (textually) **the same**.

More Interesting: Well-Typed-ness



- We want

  context D inv : $v < 0$

  to be well-typed.

  Currently it isn't because

  $$v(expr_1) : \tau_C \to \tau(v)$$

  but $A \vdash self : \tau_D$.

  (Because τ_D and τ_C are still **different types**, although $\mathrm{dom}(\tau_D) \subset \mathrm{dom}(\tau_C)$.)

- So, add a (first) new typing rule

  $$\frac{A \vdash expr : \tau_D}{A \vdash expr : \tau_C}, \text{ if } C \preceq D. \qquad \text{(Inh)}$$

  Which is correct in the sense that, if '$expr$' is of type τ_D, then we can use it everywhere, where a τ_C is allowed.

  The system state is prepared for that.

Well-Typed-ness with Visibility Cont'd

$$\frac{A, D \vdash expr : \tau_C}{A, D \vdash C::v(expr) : \tau}, \quad \xi = + \qquad \text{(Pub)}$$

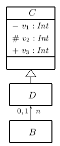
$$\frac{A, D \vdash expr : \tau_C}{A, D \vdash C::v(expr) : \tau}, \quad \xi = \#, \qquad \text{(Prot)}$$

$$\frac{A, D \vdash expr : \tau_C}{A, D \vdash C::v(expr) : \tau}, \quad \xi = -, \; C = D \qquad \text{(Priv)}$$

$\langle C::v : \tau, \xi, v_0, P \rangle \in atr(C)$.

Example:

context/ inv	$(n.)v_1 < 0$	$(n.)v_2 < 0$	$(n.)v_3 < 0$
C			
D			
B			

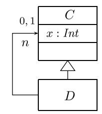


Satisfying OCL Constraints (Domain Inclusion)

- Let $\mathcal{M} = (\mathscr{CD}, \mathscr{OD}, \mathscr{SM}, \mathscr{I})$ be a UML model, and $\mathscr{D}$ a structure.
- We (**continue to**) say $\mathcal{M} \models expr$ for $\underbrace{\text{context } C \text{ inv} : expr_0}_{=expr} \in Inv(\mathcal{M})$ iff

  $$\forall \pi = (\sigma_i, \varepsilon_i)_{i \in \mathbb{N}} \in [\![\mathcal{M}]\!] \quad \forall i \in \mathbb{N} \quad \forall u \in \mathrm{dom}(\sigma_i) \cap \mathscr{D}(C) :$$
  $$I[\![expr_0]\!](\sigma_i, \{self \mapsto u\}) = 1.$$

- $\mathcal{M}$ is (still) consistent if and only if it satisfies all constraints in $Inv(\mathcal{M})$.
- **Example**:



Transformers (Domain Inclusion)

- Transformers also remain **the same**, e.g. [VL 12, p. 18]

$$update(expr_1, v, expr_2) : (\sigma, \varepsilon) \mapsto (\sigma', \varepsilon)$$

with

$$\sigma' = \sigma[u \mapsto \sigma(u)[v \mapsto I[\![expr_2]\!](\sigma)]]$$

where $u = I[\![expr_1]\!](\sigma)$.

Semantics of Method Calls

- **Non late-binding**: clear, by normalisation.
- **Late-binding**:
  Construct a **method call** transformer, which is applied to all method calls.

Inheritance and State Machines: Triggers

- **Wanted**: triggers shall also be sensitive for inherited events, sub-class shall execute super-class' state-machine (unless overridden).

$$(\sigma, \varepsilon) \xrightarrow[u]{(cons, Snd)} (\sigma', \varepsilon') \text{ if}$$

- $\exists\, u \in \mathrm{dom}(\sigma) \cap \mathscr{D}(C)\ \exists\, u_E \in \mathscr{D}(\mathscr{E}) : u_E \in ready(\varepsilon, u)$
- u is stable and in state machine state s, i.e. $\sigma(u)(stable) = 1$ and $\sigma(u)(st) = s$,
- a transition is enabled, i.e.

$$\exists\, (s, F, expr, act, s') \in \rightarrow (\mathcal{SM}_C) : F = E \wedge I[\![expr]\!](\tilde{\sigma}) = 1$$

  where $\tilde{\sigma} = \sigma[u.params_E \mapsto u_e]$.

and

- (σ', ε') results from applying t_{act} to (σ, ε) and removing u_E from the ether, i.e.

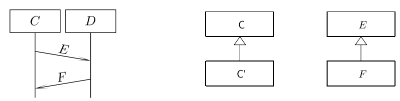
$$(\sigma'', \varepsilon') = t_{act}(\tilde{\sigma}, \varepsilon \ominus u_E),$$

$$\sigma' = (\sigma''[u.st \mapsto s', u.stable \mapsto b, u.params_E \mapsto \emptyset])|_{\mathscr{D}(\mathscr{C}) \setminus \{u_E\}}$$

  where b **depends**:
  - If u becomes stable in s', then $b = 1$. It **does** become stable if and only if there is no transition **without trigger** enabled for u in (σ', ε').
  - Otherwise $b = 0$.
- Consumption of u_E and the side effects of the action are observed, i.e.

$$cons = \{(u, (E, \sigma(u_E)))\}, Snd = Obs_{t_{act}}(\tilde{\sigma}, \varepsilon \ominus u_E).$$

Domain Inclusion and Interactions



- Similar to satisfaction of OCL expressions above:
  - An instance line stands for all instances of C (exact or inheriting).
  - Satisfaction of event observation has to take inheritance into account, too, so we have to **fix**, e.g.

$$\sigma, cons, Snd \models_\beta E^!_{x,y}$$

  if and only if

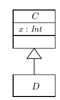
$$\beta(x) \text{ sends an } F\text{-event to } \beta y \text{ where } E \preceq F.$$

  - **Note**: C-instance line also binds to C'-objects.

Uplink Semantics

Uplink Semantics

- **Idea**:
  - Continue with the existing definition of **structure**, i.e. disjoint domains for identities.
  - Have an **implicit association** from the child to each parent part (similar to the implicit attribute for stability).



  - Apply (a different) pre-processing to make appropriate use of that association, e.g. rewrite (C++)

```
x = 0;
```

  in D to

```
uplink_C -> x = 0;
```

Pre-Processing for the Uplink Semantics

- For each pair $C \lhd D$, extend D by a (fresh) association

$$uplink_C : C \text{ with } \mu = [1,1],\ \xi = +$$

(**Exercise**: public necessary?)

- Given expression v (or f) in the **context** of class D,
  - let C be the **smallest** class wrt. "$\preceq$" such that
    - $C \preceq D$, and
    - $C{::}v \in atr(D)$
  - then there exists (by definition) $C \lhd C_1 \lhd \ldots \lhd C_n \lhd D$,
  - **normalise** v to (= replace by)

$$uplink_{C_n} \texttt{->} \cdots \texttt{->} uplink_{C_1}.C{::}v$$

- Again: if no (unique) smallest class exists, the model is considered **not well-formed**; the expression is ambiguous.

Uplink Structure, System State, Typing

- Definition of structure remains **unchanged**.
- Definition of system state remains **unchanged**.
- Typing and transformers remain **unchanged** — the preprocessing has put everything in shape.

Satisfying OCL Constraints (Uplink)

- Let $\mathcal{M} = (\mathscr{CD}, \mathscr{OD}, \mathscr{SM}, \mathscr{I})$ be a UML model, and $\mathscr{D}$ a structure.
- We (**continue to**) say

$$\mathcal{M} \models expr$$

for

$$\underbrace{\text{context } C \text{ inv} : expr_0}_{=expr} \in \mathit{Inv}(\mathcal{M})$$

if and only if

$$\forall\, \pi = (\sigma_i)_{i \in \mathbb{N}} \in [\![\mathcal{M}]\!]$$
$$\forall\, i \in \mathbb{N}$$
$$\forall\, u \in \mathrm{dom}(\sigma_i) \cap \mathscr{D}(C) :$$
$$I[\![expr_0]\!](\sigma_i, \{self \mapsto u\}) = 1.$$

- $\mathcal{M}$ is (still) consistent if and only if it satisfies all constraints in $\mathit{Inv}(\mathcal{M})$.

Transformers (Uplink)

- What **has to change** is the **create** transformer:

$$create(C, expr, v)$$

- Assume, C's inheritance relations are as follows.

$$C_{1,1} \lhd \ldots \lhd C_{1,n_1} \lhd C,$$
$$\ldots$$
$$C_{m,1} \lhd \ldots \lhd C_{m,n_m} \lhd C.$$

- Then, we have to
  - create one fresh object for each part, e.g.

$$u_{1,1}, \ldots, u_{1,n_1}, \ldots, u_{m,1}, \ldots, u_{m,n_m},$$

  - set up the uplinks recursively, e.g.

$$\sigma(u_{1,2})(uplink_{C_{1,1}}) = u_{1,1}.$$

  - And, if we had constructors, be careful with their order.

Late Binding (Uplink)

- Employ something similar to the "`mostspec`" trick (in a minute!). But the result is typically far from concise.

  (Related to OCL's `isKindOf`() function, and RTTI in C++.)

Domain Inclusion vs. Uplink Semantics

Cast-Transformers

- C c;
- D d;
- **Identity upcast** (C++):
  - C∗ cp = &d; // *assign address of 'd' to pointer 'cp'*
- **Identity downcast** (C++):
  - D∗ dp = (D∗)cp; // *assign address of 'd' to pointer 'dp'*
- **Value upcast** (C++):
  - ∗c = ∗d; // *copy attribute values of 'd' into 'c', or,* // *more precise, the values of the C-part of 'd'*

Casts in Domain Inclusion and Uplink Semantics

	Domain Inclusion	**Uplink**
C∗ cp = &d;	**easy**: immediately compatible (in underlying system state) because &d yields an identity from $\mathscr{D}(D) \subset \mathscr{D}(C)$.	**easy**: By pre-processing, C∗ cp = d.uplink$_C$;
D∗ dp = (D∗)cp;	**easy**: the value of cp is in $\mathscr{D}(D) \cap \mathscr{D}(C)$ because the pointed-to object is a D. Otherwise, error condition.	**difficult**: we need the identity of the D whose C-slice is denoted by cp. (See next slide.)
c = d;	**bit difficult**: set (for all $C \preceq D$) $(C)(\cdot,\cdot) : \tau_D \times \Sigma \to \Sigma\|_{atr(C)}$ $(u, \sigma) \mapsto \sigma(u)\|_{atr(C)}$ Note: $\sigma' = \sigma[u_C \mapsto \sigma(u_D)]$ is not type-compatible!	**easy**: By pre-processing, c = ∗(d.uplink$_C$);

Identity Downcast with Uplink Semantics

- **Recall** (C++): D d; C∗ cp = &d; D∗ dp = (D∗)cp;
- **Problem**: we need the identity of the D whose C-slice is denoted by cp.
- **One technical solution**:
  - Give up disjointness of domains for **one additional type** comprising all identities, i.e. have

$$\texttt{all} \in \mathscr{T}, \qquad \mathscr{D}(\texttt{all}) = \bigcup_{C \in \mathscr{C}} \mathscr{D}(C)$$

  - In each $\preceq$**-minimal class** have associations "mostspec" pointing to **most specialised** slices, plus information of which type that slice is.
  - Then **downcast** means, depending on the mostspec type (only finitely many possibilities), **going down and then up** as necessary, e.g.

```
switch(mostspec_type){
  case C :
    dp = cp -> mostspec -> uplink_Dn -> ... -> uplink_D1 -> uplink_D;
  ...
}
```


Domain Inclusion vs. Uplink Semantics: Differences

- **Note**: The uplink semantics views inheritance as an abbreviation:
  - We only need to touch transformers (create) — and if we had constructors, we didn't even needed that (we could encode the recursive construction of the upper slices by a transformation of the existing constructors.)
- **So**:
  - Inheritance **doesn't add** expressive power.
  - And it also **doesn't improve** conciseness **soo dramatically**.

As long as we're "**early binding**", that is...

Domain Inclusion vs. Uplink Semantics: Motives

- **Exercise**:

  What's the point of

  - having the **tedious** adjustments of the **theory** if it can be approached **technically**?
  - having the **tedious** technical **pre-processing** if it can be approached **cleanly** in the **theory**?

Meta-Modelling: Idea and Example

Meta-Modelling: Why and What

- **Meta-Modelling** is one major prerequisite for understanding
  - the standard documents [OMG, 2007a, OMG, 2007b], and
  - the MDA ideas of the OMG.
- The idea is **simple**:
  - if a **modelling language** is about modelling **things**,
  - and if UML models are and comprise **things**,
  - then why not **model** those in a modelling language?

Meta-Modelling: Why and What

- **Meta-Modelling** is one major prerequisite for understanding
  - the standard documents [OMG, 2007a, OMG, 2007b], and
  - the MDA ideas of the OMG.
- The idea is **simple**:
  - if a **modelling language** is about modelling **things**,
  - and if UML models are and comprise **things**,
  - then why not **model** those in a modelling language?
- In other words:

  Why not have a model $\mathcal{M}_U$ such that
  - the set of legal instances of $\mathcal{M}_U$

  is
  - the set of well-formed (!) UML models.

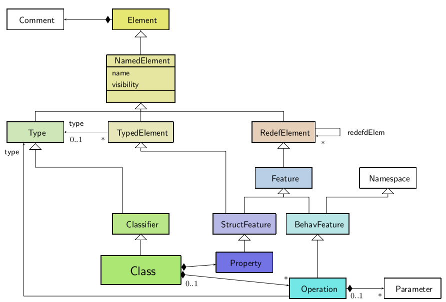
Meta-Modelling: Example

- For example, let's consider a class.
- A **class** has (on a superficial level)
  - a **name**,
  - any number of **attributes**,
  - any number of **behavioural features**.

  Each of the latter two has
  - a **name** and
  - a **visibility**.

  Behavioural features in addition have
  - a boolean attribute **isQuery**,
  - any number of parameters,
  - a return type.
- Can we model this (in UML, for a start)?

UML Meta-Model: Extract



Classes [OMG, 2007b, 32]

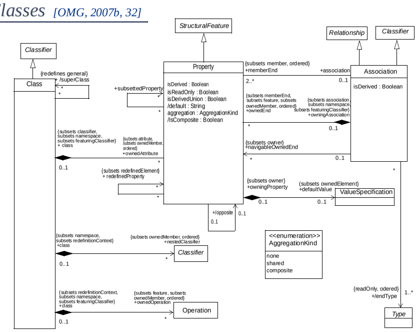


Figure 7.12 - Classes diagram of the Kernel package

Operations [OMG, 2007b, 31]

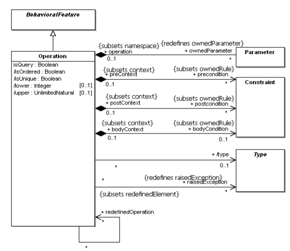


Figure 7.11 - Operations diagram of the Kernel package

Operations [OMG, 2007b, 30]

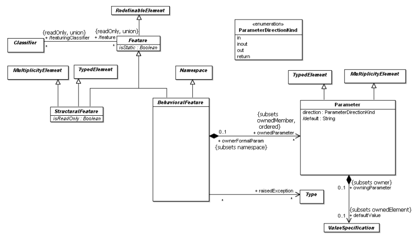


Figure 7.10 - Features diagram of the Kernel package

Classifiers [OMG, 2007b, 29]

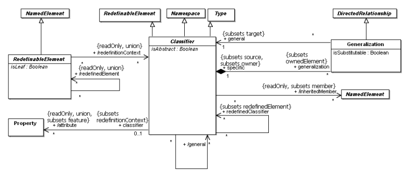


Figure 7.9 - Classifiers diagram of the Kernel package

Namespaces [OMG, 2007b, 26]

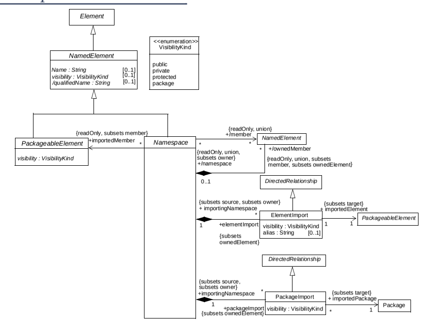


Figure 7.4 - Namespaces diagram of the Kernel package

Root Diagram [OMG, 2007b, 25]

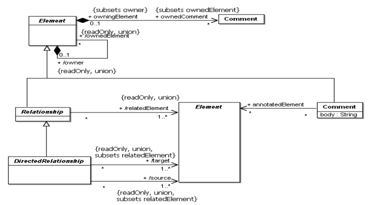


Figure 7.3 - Root diagram of the Kernel package

Interesting: Declaration/Definition [OMG, 2007b, 424]

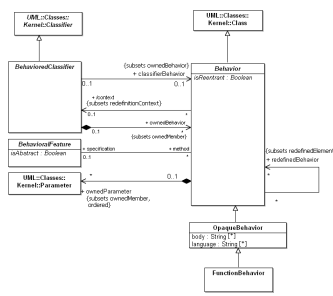


Figure 13.6 - Common Behavior

UML Architecture [OMG, 2003, 8]

- Meta-modelling has already been used for UML 1.x.
- For UML 2.0, the request for proposals (RFP) asked for a separation of concerns: **Infrastructure** and **Superstructure**.
- **One reason**: sharing with MOF (see later) and, e.g., CWM.

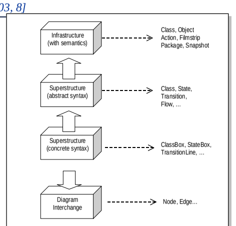
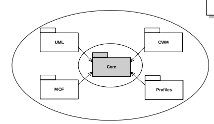


Figure 0-1 *Overview of architecture*



UML Superstructure Packages [OMG, 2007a, 15]

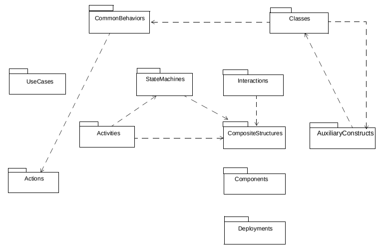
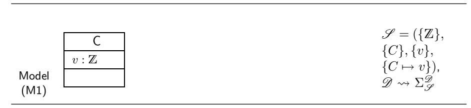


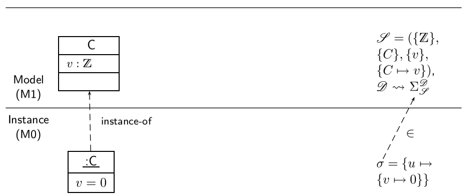
Figure 7.5 - The top-level package structure of the UML 2.1.1 Superstructure

Meta-Modelling: Principle

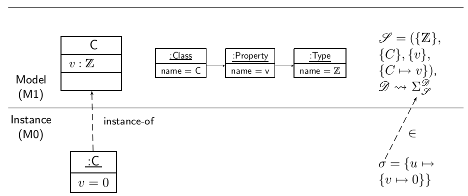
Modelling vs. Meta-Modelling



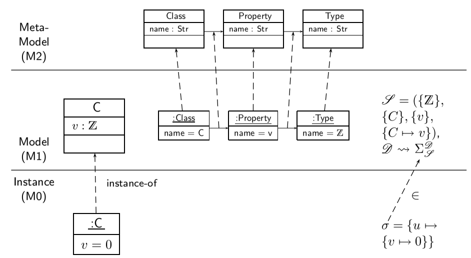
Modelling vs. Meta-Modelling



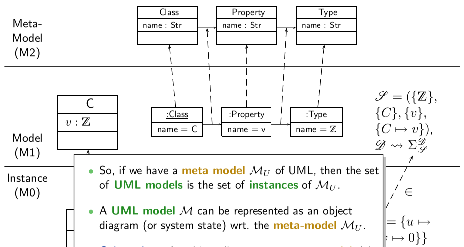
Modelling vs. Meta-Modelling



Modelling vs. Meta-Modelling



Modelling vs. Meta-Modelling



- So, if we have a **meta model** $\mathcal{M}_U$ of UML, then the set of **UML models** is the set of **instances** of $\mathcal{M}_U$.
- A **UML model** $\mathcal{M}$ can be represented as an object diagram (or system state) wrt. the **meta-model** $\mathcal{M}_U$.
- **Other view**: An object diagram wrt. **meta-model** $\mathcal{M}_U$ can (alternatively) be rendered as the **UML model** $\mathcal{M}$.

Well-Formedness as Constraints in the Meta-Model

- The set of **well-formed UML models** can be defined as the set of object diagrams satisfying all constraints of the **meta-model**.

  For example,

  > "[2] Generalization hierarchies must be directed and acyclical. A classifier cannot be both a transitively general and transitively specific classifier of the same classifier.
  >
  > not self . allParents() -> includes(self)" [OMG, 2007b, 53]

Well-Formedness as Constraints in the Meta-Model

- The set of **well-formed UML models** can be defined as the set of object diagrams satisfying all constraints of the **meta-model**.

  For example,

  > "[2] Generalization hierarchies must be directed and acyclical. A classifier cannot be both a transitively general and transitively specific classifier of the same classifier.
  >
  > not self . allParents() -> includes(self)" [OMG, 2007b, 53]

- The other way round:

  Given a **UML model** $\mathcal{M}$, unfold it into an object diagram O_1 wrt. $\mathcal{M}_U$.
  If O_1 is a **valid** object diagram of $\mathcal{M}_U$ (i.e. satisfies all invariants from *Inv*$(\mathcal{M}_U)$), then $\mathcal{M}$ is a well-formed UML model.

Well-Formedness as Constraints in the Meta-Model

- The set of **well-formed UML models** can be defined as the set of object diagrams satisfying all constraints of the **meta-model**.

  For example,

  > "[2] Generalization hierarchies must be directed and acyclical. A classifier cannot be both a transitively general and transitively specific classifier of the same classifier.
  >
  > not self . allParents() -> includes(self)" [OMG, 2007b, 53]

- The other way round:

  Given a **UML model** $\mathcal{M}$, unfold it into an object diagram O_1 wrt. $\mathcal{M}_U$.
  If O_1 is a **valid** object diagram of $\mathcal{M}_U$ (i.e. satisfies all invariants from *Inv*$(\mathcal{M}_U)$), then $\mathcal{M}$ is a well-formed UML model.

  That is, if we have an object diagram **validity checker** for of the meta-modelling language, then we have a **well-formedness checker** for UML models.

Reading the Standard

Table of Contents

UML Superstructure Specification, v2.1.2 i

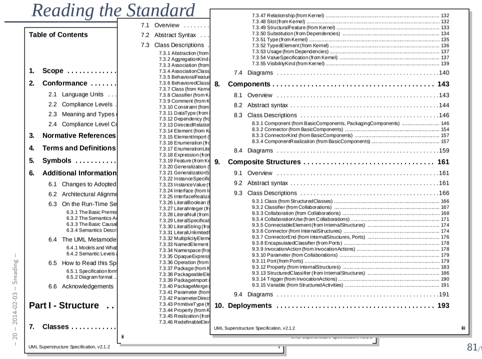
Reading the Standard

Table of Contents

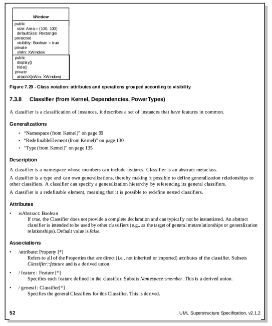
1. Scope
2. Conformance
  2.1 Language Units
  2.2 Compliance Levels
  2.3 Meaning and Types
  2.4 Compliance Level C
3. Normative References
4. Terms and Definitions
5. Symbols
6. Additional Information
  6.1 Changes to Adopted
  6.2 Architectural Alignme
  6.3 On the Run-Time Se
    6.3.1 The Basic Premis
    6.3.2 The Semantics Ar
    6.3.3 The Basic Causal
    6.3.4 Semantics Descri
  6.4 The UML Metamode
    6.4.1 Models and What
    6.4.2 Semantic Levels
  6.5 How to Read this Sp
    6.5.1 Specification form
    6.5.2 Diagram format
  6.6 Acknowledgements
Part I - Structure
7. Classes

ii UML Superstructure Specification, v2.1.2

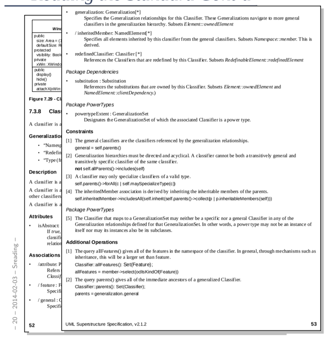
Reading the Standard



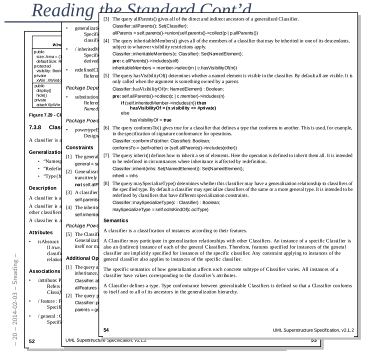
Reading the Standard Cont'd



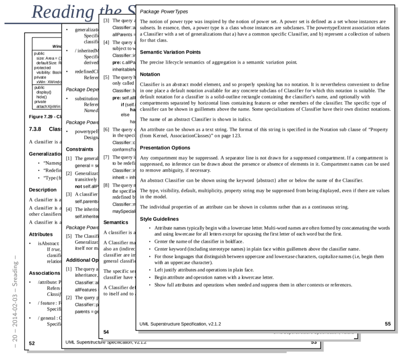
Reading the Standard Cont'd



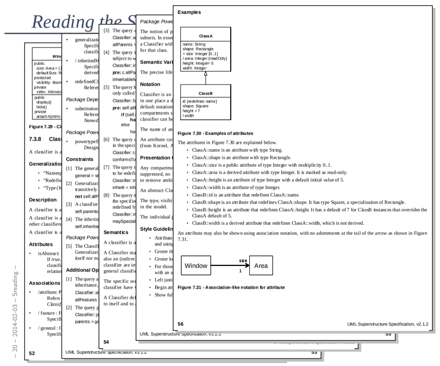
Reading the Standard Cont'd



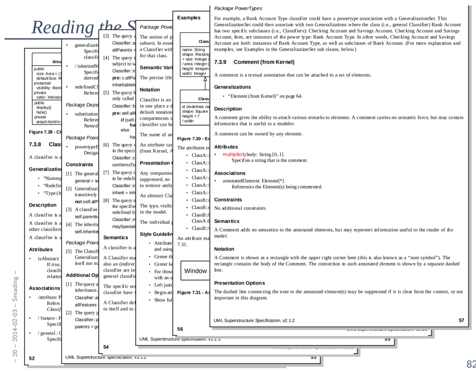
Reading the Standard Cont'd



Reading the Standard Cont'd



Reading the Standard



Meta Object Facility (MOF)

Open Questions...

- Now you've been "**tricked**" again. Twice.
  - We didn't tell what the **modelling language** for meta-modelling is.
  - We didn't tell what the **is-instance-of** relation of this language is.
- **Idea**: have a **minimal object-oriented core** comprising the notions of **class**, **association**, **inheritance**, **etc.** with "self-explaining" semantics.

- This is **Meta Object Facility** (MOF), which (more or less) coincides with UML Infrastructure [OMG, 2007a].
- So: things on meta level
  - M0 are object diagrams/system states
  - M1 are **words of the language UML**
  - M2 are **words of the language MOF**
  - M3 are **words of the language** ...

MOF Semantics

- One approach:
  - Treat it with **our signature-based theory**
  - This is (in effect) the right direction, but may require new (or extended) signatures for each level.
    (For instance, MOF doesn't have a notion of Signal, our signature has.)

– 20 – 2014-02-03 – Smof –

MOF Semantics

- One approach:
  - Treat it with **our signature-based theory**
  - This is (in effect) the right direction, but may require new (or extended) signatures for each level.
    (For instance, MOF doesn't have a notion of Signal, our signature has.)

- Other approach:
  - Define a **generic**, **graph based** "is-instance-of" relation.
  - Object diagrams (that **are** graphs) then **are** the system states — not **only graphical representations** of system states.

– 20 – 2014-02-03 – Smof –

MOF Semantics

- One approach:
  - Treat it with **our signature-based theory**
  - This is (in effect) the right direction, but may require new (or extended) signatures for each level.
    (For instance, MOF doesn't have a notion of Signal, our signature has.)

- Other approach:
  - Define a **generic**, **graph based** "is-instance-of" relation.
  - Object diagrams (that **are** graphs) then **are** the system states — not **only graphical representations** of system states.

  - If this works out, good: We can easily experiment with different language designs, e.g. different flavours of UML that immediately have a semantics.

MOF Semantics

- One approach:
  - Treat it with **our signature-based theory**
  - This is (in effect) the right direction, but may require new (or extended) signatures for each level.
    (For instance, MOF doesn't have a notion of Signal, our signature has.)
- Other approach:
  - Define a **generic**, **graph based** "is-instance-of" relation.
  - Object diagrams (that **are** graphs) then **are** the system states — not **only graphical representations** of system states.
  - If this works out, good: We can easily experiment with different language designs, e.g. different flavours of UML that immediately have a semantics.
  - Most interesting: also do generic definition of behaviour within a closed modelling setting, but this is clearly still research, e.g. [Buschermöhle and Oelerink, 2008]

Meta-Modelling: (Anticipated) Benefits

Benefits: Overview

- We'll (superficially) look at three aspects:
  - Benefits for **Modelling Tools**.
  - Benefits for **Language Design**.
  - Benefits for **Code Generation and MDA**.

Benefits for Modelling Tools

- The meta-model $\mathcal{M}_U$ of UML **immediately** provides a **data-structure** representation for the abstract syntax ($\sim$ for our signatures).

  If we have code generation for UML models, e.g. into Java, then we can immediately represent UML models **in memory** for Java.

  (Because each MOF model is in particular a UML model.)
- There exist tools and libraries called **MOF-repositories**, which can generically represent instances of MOF instances (in particular UML models).

  And which can often generate specific code to manipulate instances of MOF instances in terms of the MOF instance.

Benefits for Modelling Tools Cont'd

- And not only **in memory**, if we can represent MOF instances in files, we obtain a canonical representation of UML models **in files**, e.g. in XML.
  → XML Metadata Interchange (XMI)

Benefits for Modelling Tools Cont'd

- And not only **in memory**, if we can represent MOF instances in files, we obtain a canonical representation of UML models **in files**, e.g. in XML.
  → XML Metadata Interchange (XMI)
- **Note**: A priori, there is no graphical information in XMI (it is only abstract syntax like our signatures) → OMG Diagram Interchange.

Benefits for Modelling Tools Cont'd

- And not only **in memory**, if we can represent MOF instances in files, we obtain a canonical representation of UML models **in files**, e.g. in XML.
  → XML Metadata Interchange (XMI)
- **Note**: A priori, there is no graphical information in XMI (it is only abstract syntax like our signatures) → OMG Diagram Interchange.
- **Note**: There are slight ambiguities in the XMI standard.
  And different tools by different vendors often seem to lie at opposite ends on the scale of interpretation. Which is surely a coincidence.
  In some cases, it's possible to fix things with, e.g., XSLT scripts, but full vendor independence is today not given.
  Plus XMI compatibility doesn't necessarily refer to Diagram Interchange.

Benefits for Modelling Tools Cont'd

- And not only **in memory**, if we can represent MOF instances in files, we obtain a canonical representation of UML models **in files**, e.g. in XML.
  → XML Metadata Interchange (XMI)
- **Note**: A priori, there is no graphical information in XMI (it is only abstract syntax like our signatures) → OMG Diagram Interchange.
- **Note**: There are slight ambiguities in the XMI standard.
  And different tools by different vendors often seem to lie at opposite ends on the scale of interpretation. Which is surely a coincidence.
  In some cases, it's possible to fix things with, e.g., XSLT scripts, but full vendor independence is today not given.
  Plus XMI compatibility doesn't necessarily refer to Diagram Interchange.
- **To re-iterate**: this is **generic for all** MOF-based modelling languages such as UML, CWM, etc.
  And also for **Domain Specific Languages** which don't even exit yet.

Benefits: Overview

- We'll (superficially) look at three aspects:
  - Benefits for **Modelling Tools**. ✔
  - Benefits for **Language Design**.
  - Benefits for **Code Generation and MDA**.

Benefits for Language Design

- Recall: we said that code-generators are possible "readers" of stereotypes.
- For example, (heavily simplifying) we could
  - introduce the stereotypes **Button**, **Toolbar**, ...
  - for convenience, instruct the modelling tool to use special pictures for stereotypes — in the meta-data (the abstract syntax), the stereotypes are clearly present.
  - instruct the code-generator to automatically add inheritance from Gtk::Button, Gtk::Toolbar, etc. **corresponding** to the stereotype.

One mechanism to define DSLs (based on UML, and "within" UML): **Profiles**.

Benefits for Language Design

- Recall: we said that code-generators are possible "readers" of stereotypes.
- For example, (heavily simplifying) we could
  - introduce the stereotypes **Button**, **Toolbar**, ...
  - for convenience, instruct the modelling tool to use special pictures for stereotypes — in the meta-data (the abstract syntax), the stereotypes are clearly present.
  - instruct the code-generator to automatically add inheritance from Gtk::Button, Gtk::Toolbar, etc. **corresponding** to the stereotype.

  Et voilà: we can model Gtk-GUIs and generate code for them.

One mechanism to define DSLs (based on UML, and "within" UML): **Profiles**.

Benefits for Language Design

- Recall: we said that code-generators are possible "readers" of stereotypes.
- For example, (heavily simplifying) we could
  - introduce the stereotypes **Button**, **Toolbar**, ...
  - for convenience, instruct the modelling tool to use special pictures for stereotypes — in the meta-data (the abstract syntax), the stereotypes are clearly present.
  - instruct the code-generator to automatically add inheritance from Gtk::Button, Gtk::Toolbar, etc. **corresponding** to the stereotype.

  Et voilà: we can model Gtk-GUIs and generate code for them.
- Another view:
  - UML with these stereotypes **is a new modelling language**: Gtk-UML.
  - Which lives on the same meta-level as UML (M2).
  - It's a **Domain Specific** Modelling **Language** (DSL).

One mechanism to define DSLs (based on UML, and "within" UML): **Profiles**.

Benefits for Language Design Cont'd

- For each DSL defined by a Profile, we immediately have
  - in memory representations,
  - modelling tools,
  - file representations.
- **Note**: here, the **semantics** of the stereotypes (and thus the language of Gtk-UML) **lies in the code-generator**.

  That's the first "reader" that understands these special stereotypes.
  (And that's what's meant in the standard when they're talking about giving stereotypes semantics).
- One can also impose additional well-formedness rules, for instance that certain components shall all implement a certain interface (and thus have certain methods available). (Cf. [Stahl and Völter, 2005].)

Benefits for Language Design Cont'd

- One step further:
  - Nobody hinders us to obtain a model of UML (written in MOF),
  - throw out parts unnecessary for our purposes,
  - add (= integrate into the existing hierarchy) more adequat new constructs, for instance, **contracts** or something more close to hardware as **interrupt** or **sensor** or **driver**,
  - and maybe also stereotypes.

  → a new language standing next to UML, CWM, etc.
- Drawback: the resulting language is not necessarily UML any more, so we **can't use** proven UML modelling tools.
- But we can use all tools for MOF (or MOF-like things).
  For instance, Eclipse EMF/GMF/GEF.

Benefits: Overview

- We'll (superficially) look at three aspects:
  - Benefits for **Modelling Tools**. ✔
  - Benefits for **Language Design**. ✔
  - Benefits for **Code Generation and MDA**.

Benefits for Model (to Model) Transformation

- There are manifold applications for model-to-model transformations:
  - For instance, tool support for **re-factorings**, like moving common attributes upwards the inheritance hierarchy.

    This can now be defined as **graph-rewriting** rules on the level of MOF.
    The graph to be rewritten is the UML model

Benefits for Model (to Model) Transformation

- There are manifold applications for model-to-model transformations:
  - For instance, tool support for **re-factorings**, like moving common attributes upwards the inheritance hierarchy.

    This can now be defined as **graph-rewriting** rules on the level of MOF.
    The graph to be rewritten is the UML model
  - Similarly, one could transform a **Gtk-UML** model into a **UML model**, where the inheritance from classes like Gtk::Button is made explicit:

    The transformation would add this class Gtk::Button and the inheritance relation and remove the stereotype.

Benefits for Model (to Model) Transformation

- There are manifold applications for model-to-model transformations:
  - For instance, tool support for **re-factorings**, like moving common attributes upwards the inheritance hierarchy.

    This can now be defined as **graph-rewriting** rules on the level of MOF.
    The graph to be rewritten is the UML model
  - Similarly, one could transform a **Gtk-UML** model into a **UML model**, where the inheritance from classes like Gtk::Button is made explicit:

    The transformation would add this class Gtk::Button and the inheritance relation and remove the stereotype.
  - Similarly, one could have a **GUI-UML** model transformed into a **Gtk-UML** model, or a Qt-UML model.

    The former a PIM (Platform Independent Model), the latter a PSM (Platform Specific Model) — cf. MDA.

Special Case: Code Generation

- Recall that we said that, e.g. Java code, can also be seen as a model.

  So code-generation is a **special case** of model-to-model transformation; only the destination looks quite different.

Special Case: Code Generation

- Recall that we said that, e.g. Java code, can also be seen as a model.

  So code-generation is a **special case** of model-to-model transformation; only the destination looks quite different.

- **Note**: Code generation needn't be as expensive as buying a modelling tool with full fledged code generation.

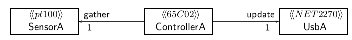
  - If we have the UML model (or the DSL model) given as an XML file, code generation can be **as simple as** an XSLT script.

  "Can be" in the sense of

  > *"There may be situation where a graphical and abstract representation of something is desired which has a clear and direct mapping to some textual representation."*

  In general, code generation can (in colloquial terms) become **arbitrarily difficult**.

Example: Model and XMI




```
<?xml version = '1.0' encoding = 'UTF-8' ?>
<XMI xmi.version = '1.2' xmlns:UML = 'org.omg.xmi.namespace.UML' timestamp = 'Mon Feb 02 18:23:12 CET 2009'>
  <XMI.content>
    <UML:Model xmi.id = '...'>
      <UML:Namespace.ownedElement>
        <UML:Class xmi.id = '...' name = 'SensorA'>
          <UML:ModelElement.stereotype>
            <UML:Stereotype name = 'pt100'/>
          </UML:ModelElement.stereotype>
        </UML:Class>
        <UML:Class xmi.id = '...' name = 'ControllerA'>
          <UML:ModelElement.stereotype>
            <UML:Stereotype name = '65C02'/>
          </UML:ModelElement.stereotype>
        </UML:Class>
        <UML:Class xmi.id = '...' name = 'UsbA'>
          <UML:ModelElement.stereotype>
            <UML:Stereotype name = 'NET2270'/>
          </UML:ModelElement.stereotype>
        </UML:Class>
        <UML:Association xmi.id = '...' name = 'in' >...</UML:Association>
        <UML:Association xmi.id = '...' name = 'out' >...</UML:Association>
      </UML:Namespace.ownedElement>
    </UML:Model>
  </XMI.content>
</XMI>
```


References

References

[Buschermöhle and Oelerink, 2008] Buschermöhle, R. and Oelerink, J. (2008). Rich meta object facility. In Proc. 1st IEEE Int'l workshop UML and Formal Methods.

[Crane and Dingel, 2007] Crane, M. L. and Dingel, J. (2007). UML vs. classical vs. rhapsody statecharts: not all models are created equal. Software and Systems Modeling, 6(4):415–435.

[Fischer and Wehrheim, 2000] Fischer, C. and Wehrheim, H. (2000). Behavioural subtyping relations for object-oriented formalisms. In Rus, T., editor, AMAST, number 1816 in Lecture Notes in Computer Science. Springer-Verlag.

[Harel and Gery, 1997] Harel, D. and Gery, E. (1997). Executable object modeling with statecharts. IEEE Computer, 30(7):31–42.

[Liskov, 1988] Liskov, B. (1988). Data abstraction and hierarchy. SIGPLAN Not., 23(5):17–34.

[Liskov and Wing, 1994] Liskov, B. H. and Wing, J. M. (1994). A behavioral notion of subtyping. ACM Transactions on Programming Languages and Systems (TOPLAS), 16(6):1811–1841.

[OMG, 2003] OMG (2003). Uml 2.0 proposal of the 2U group, version 0.2, http://www.2uworks.org/uml2submission.

[OMG, 2007a] OMG (2007a). Unified modeling language: Infrastructure, version 2.1.2. Technical Report formal/07-11-04.

[OMG, 2007b] OMG (2007b). Unified modeling language: Superstructure, version 2.1.2. Technical Report formal/07-11-02.

[Stahl and Völter, 2005] Stahl, T. and Völter, M. (2005). Modellgetriebene Softwareentwicklung. dpunkt.verlag, Heidelberg.