Contents & Goals

Last Lecture:
- State Machine semantics completed
- Inheritance in UML: concrete syntax

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:
  - Liskov Substitution Principle — desired semantics
  - Two approaches to obtain desired semantics
Inheritance: Syntax

Recall: Abstract Syntax

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

Now (finally): extend to

$\mathcal{S} = (\mathcal{T}, \mathcal{E}, V, atr, \ell, \mathcal{M}, mth, \triangleleft)$

where $F/mth$ are methods, analogously to attributes and

$\triangleleft \subseteq (\mathcal{E} \times \mathcal{E}) \cup (\ell \times \ell)$

is a generalisation relation such that $C \triangleleft^+ C$ for no $C \in \mathcal{E}$ (“acyclic”).

$C \triangleleft D$ 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 $C_0, C_1, D \in \mathcal{C}$, we say $D$ inherits from $C_0$ via $C_1$ if and only if there are $C_0, \ldots, C_n, C_1, \ldots, C_m \in \mathcal{C}$ such that

$$C_0 \prec C_0 \prec \ldots \prec C_n \prec C_1 \prec C_1 \prec \ldots \prec C_m \prec D.$$  

We use ‘≤’ to denote the reflexive, transitive closure of ‘≺’.

In the following, we assume

- that all attribute (method) names are of the form
  $$C::v, \quad C \in \mathcal{C} \cup \mathcal{S} \quad (C::f, \quad C \in \mathcal{C}),$$
- 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 \( T \).”

\[
\forall o_1 \in S \exists o_2 \in T \cdot \forall \pi \in \mathcal{P}(s) \cdot \pi \circ \mathcal{P}(o_1) = \pi \circ \mathcal{P}(o_2)
\]

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...”?

· OCL:
  · context C inv : x > 0

· Actions:
  · itsC.x = 0
  · itsC.f(0)
  · itsC ! F

· Triggers:
  · E[...] / ...

“...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.
- Wider interpretation: another modeler.
"...can’t tell difference..."?

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
C \xrightarrow{f} \text{Int} \\
\end{array}
\]

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
D \xrightarrow{\text{Int}} \text{Int} \\
\end{array}
\]

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
\{\text{signal}\} \xrightarrow{E} E \\
\end{array}
\]

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
\{\text{signal}\} \xrightarrow{F} F \\
\end{array}
\]

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
\text{Int} \xrightarrow{\text{Int}} \text{Int} \\
\end{array}
\]

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
\text{Int} \xrightarrow{\text{Int}} \text{Int} \\
\end{array}
\]

**OCL:**

- \[I[\text{context } C \text{ inv : } x > 0][\sigma_0, \emptyset] \text{ vs. } I[\text{context } C \text{ inv : } x > 0][\sigma_1, \emptyset]\]

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
\text{Int} \xrightarrow{\text{Int}} \text{Int} \\
\end{array}
\]

**Triggers, Actions:** if

\[
(\sigma_0, \xi_0, \epsilon_0) \xrightarrow{(\text{cons}_{\text{Int}}, \text{Snd}_{\text{Int}})} u_2 \xrightarrow{u_2} (\sigma_1, \xi_1, \epsilon_1)
\]

is possible, then

\[
(\sigma_0, \xi_0, \epsilon_0) \xrightarrow{(\text{cons}_{\text{Int}}, \text{Snd}_{\text{Int}})} (\sigma_1, \xi_1, \epsilon_1)
\]

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


"...can’t tell difference..."?

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
C \xrightarrow{f} \text{Int} \\
\end{array}
\]

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
D \xrightarrow{\text{Int}} \text{Int} \\
\end{array}
\]

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
\{\text{signal}\} \xrightarrow{E} E \\
\end{array}
\]

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
\{\text{signal}\} \xrightarrow{F} F \\
\end{array}
\]

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
\text{Int} \xrightarrow{\text{Int}} \text{Int} \\
\end{array}
\]

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
\text{Int} \xrightarrow{\text{Int}} \text{Int} \\
\end{array}
\]

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
\text{Int} \xrightarrow{\text{Int}} \text{Int} \\
\end{array}
\]

**OCL:**

- \[I[\text{context } C \text{ inv : } x > 0][\sigma_0, \emptyset] \text{ vs. } I[\text{context } C \text{ inv : } x > 0][\sigma_1, \emptyset]\]

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
\text{Int} \xrightarrow{\text{Int}} \text{Int} \\
\end{array}
\]

**Triggers, Actions:** if

\[
(\sigma_0, \xi_0, \epsilon_0) \xrightarrow{(\text{cons}_{\text{Int}}, \text{Snd}_{\text{Int}})} u_2 \xrightarrow{u_2} (\sigma_1, \xi_1, \epsilon_1)
\]

is possible, then

\[
(\sigma_0, \xi_0, \epsilon_0) \xrightarrow{(\text{cons}_{\text{Int}}, \text{Snd}_{\text{Int}})} (\sigma_1, \xi_1, \epsilon_1)
\]

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


"...can’t tell difference..."?

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
C \xrightarrow{f} \text{Int} \\
\end{array}
\]

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
D \xrightarrow{\text{Int}} \text{Int} \\
\end{array}
\]

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
\{\text{signal}\} \xrightarrow{E} E \\
\end{array}
\]

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
\{\text{signal}\} \xrightarrow{F} F \\
\end{array}
\]

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
\text{Int} \xrightarrow{\text{Int}} \text{Int} \\
\end{array}
\]

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
\text{Int} \xrightarrow{\text{Int}} \text{Int} \\
\end{array}
\]

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
\text{Int} \xrightarrow{\text{Int}} \text{Int} \\
\end{array}
\]

**OCL:**

- \[I[\text{context } C \text{ inv : } x > 0][\sigma_0, \emptyset] \text{ vs. } I[\text{context } C \text{ inv : } x > 0][\sigma_1, \emptyset]\]

\[
\begin{array}{c}
\text{Input} \to \text{Output} \\
\text{Int} \xrightarrow{\text{Int}} \text{Int} \\
\end{array}
\]

**Triggers, Actions:** if

\[
(\sigma_0, \xi_0, \epsilon_0) \xrightarrow{(\text{cons}_{\text{Int}}, \text{Snd}_{\text{Int}})} u_2 \xrightarrow{u_2} (\sigma_1, \xi_1, \epsilon_1)
\]

is possible, then

\[
(\sigma_0, \xi_0, \epsilon_0) \xrightarrow{(\text{cons}_{\text{Int}}, \text{Snd}_{\text{Int}})} (\sigma_1, \xi_1, \epsilon_1)
\]

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


"...can’t tell difference..."?
“...can’t tell difference...”?

![Sequence Diagram]

- **Sequence Diagram**: $w[u_1/u_2] \in \mathcal{L}(B_L)$ implies $w \in \mathcal{L}(B_L)$.

### Motivations for Generalisation

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

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

\[
\begin{array}{c}
D_1 \\
\end{array}
\begin{array}{c}
D_2 \\
\end{array}
\begin{array}{c}
C \\
\end{array}
\]

we don’t even have usability.

- It would be nice, if the well-formedness rules and semantics of

\[
\begin{array}{c}
D_1 \\
\end{array}
\begin{array}{c}
D_2 \\
\end{array}
\begin{array}{c}
C \\
\end{array}
\]

would ensure \textit{D}_1 \textit{ is a sub-type of } C: 
- that \textit{D}_1 objects can be used interchangeably by everyone who is using \textit{C}'s,
- is not able to tell the difference (i.e. see unexpected behaviour).

"...shall be usable..." for UML
Easy: Static Typing

Given:

\[ C_1 \xrightarrow{x : \text{Int}} f(\text{Int}) : \text{Int} \]
\[ D_1 \xrightarrow{\text{itsC1}} \]
\[ C_2 \xrightarrow{x : \text{Int}} f(\text{Int}) : \text{Int} \]
\[ D_2 \xrightarrow{\text{itsC2}} \]
\[ \langle \langle \text{signal} \rangle \rangle E \]
\[ \langle \langle \text{signal} \rangle \rangle F \]

Wanted:

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

Approach:

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

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.)

Where the type of the object determines which implementation is used (not caring for what an object really is):

- `someC -> f()`
  - `C::f()`
  - `C::f()`

- `someD -> f()`
  - `C::f()`
  - `D::f()`

- `someC -> f()`
  - `C::f()`
  - `C::f()`

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

Where the type of object determines which implementation is used:

- `someC -> f()`
  - `C::f()`
  - `C::f()`

- `someD -> f()`
  - `C::f()`
  - `D::f()`

- `someC -> f()`
  - `C::f()`
  - `D::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?

**Note**: late binding typically applies only to methods, not to attributes.

(But: getter/setter methods have been invented recently.)
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++)

\[
\begin{align*}
\text{int } C::f(\text{int}) & \{ \\
& \text{ return } 0; \\
& \}\;
\end{align*}
\]
\[
\begin{align*}
\text{int } D::f(\text{int}) & \{ \\
& \text{ return } 1; \\
& \}\;
\end{align*}
\]
\[
\begin{align*}
\text{int } C::f(\text{int}) & \{ \\
& \text{ return } (\text{rand()} \mod 2); \\
& \}\;
\end{align*}
\]
\[
\begin{align*}
\text{int } D::f(\text{int } x) & \{ \\
& \text{ return } (x \mod 2); \\
& \}\;
\end{align*}
\]
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.

- 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 $C \subseteq D$ 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 $\mathcal{S} = (\mathcal{T}, \mathcal{C}, V, atr, \mathcal{E}, F, mth, \triangleright)$ be a signature.

Now a structure $\mathcal{D}$

- [as before] maps types, classes, associations to domains,
- [for completeness] methods to transformers,
- [as before] identities of instances of classes not (transitively) related by generalisation are disjoint,
- [changed] the identities of a super-class comprise all identities of sub-classes, i.e.
  \[ \forall C \in \mathcal{C} : \mathcal{D}(C) \supseteq \bigcup_{C \triangleright D} \mathcal{D}(D). \]

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

Domain Inclusion System States

Now: a system state of $\mathcal{S}$ wrt. $\mathcal{D}$ is a type-consistent mapping
\[ \sigma : \mathcal{D}(\mathcal{C}) \rightarrow (V \rightarrow (\mathcal{D}(\mathcal{T}) \cup \mathcal{D}(\ell_{0,1}) \cup \mathcal{D}(\ell_*))) \]
that is, for all $u \in \text{dom}(\sigma) \cap \mathcal{D}(C),$

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

Example:

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


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 <.

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 occurs belongs to,
  - similar for method bodies,
- normalise v to (= replace by) C::v,
- where C is the greatest class wrt. “≤” such that
  - C ≤ D and C::v ∈ 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 $\prec$.

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 occurs belongs to,
  - similar for method bodies,
- normalise $v$ to ($= \text{replace by}$) $C::v$,
- where $C$ is the greatest class wrt. “$\preceq$” such that
  - $C \preceq D$ and $C::v \in \text{atr}(C)$.

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: $v, r \in V; C, D \in \mathcal{C}$

\[
expr ::= \begin{array}{ll}
  v(expr_1) & : \tau_C \rightarrow \tau(v), \quad \text{if } v : \tau \in \mathcal{F} \\
  r(expr_1) & : \tau_C \rightarrow \tau_D, \quad \text{if } r : D_{0,1} \\
  r(expr_1) & : \tau_C \rightarrow \text{Set}(\tau_D), \quad \text{if } r : D_*
\end{array}
\]

The definition of the semantics remains (textually) the same.
More Interesting: Well-Typed-ness

- We want
  \[
  \text{context } D \ \text{inv} : v < 0
  \]
  to be well-typed.

Currently it isn’t because
  \[
  v(e^{pr_1}) : \tau_C \to \tau(v)
  \]
  but \( A \vdash \text{self} : \tau_D \).

(Because \( \tau_D \) and \( \tau_C \) are still different types, although \( \text{dom}(\tau_D) \subset \text{dom}(\tau_C) \).)

- So, add a (first) new typing rule
  \[
  \frac{A \vdash e^{pr} : \tau_D}{A \vdash e^{pr} : \tau_C}, \text{ if } C \preceq D. \tag{Inh}
  \]
  Which is correct in the sense that, if \( \text{‘expr’} \) is of type \( \tau_D \), then we can use it everywhere, where a \( \tau_C \) is allowed.

The system state is prepared for that.

Well-Typed-ness with Visibility Cont’d

\[
\frac{A, D \vdash e^{pr} : \tau_C}{A, D \vdash C::v(e^{pr}) : \tau}, \ \xi = + \tag{Pub}
\]

\[
\frac{A, D \vdash e^{pr} : \tau_C}{A, D \vdash C::v(e^{pr}) : \tau}, \ \xi = #, \ C \preceq D \tag{Prot}
\]

\[
\frac{A, D \vdash e^{pr} : \tau_C}{A, D \vdash C::v(e^{pr}) : \tau}, \ \xi = -, \ C = D \tag{Priv}
\]

\( \langle C::\tau, \xi, v_0, P \rangle \in \text{atr}(C) \).

Example:

<table>
<thead>
<tr>
<th>context/inv</th>
<th>( (n.)v_1 &lt; 0 )</th>
<th>( (n.)v_2 &lt; 0 )</th>
<th>( (n.)v_3 &lt; 0 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( C )</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( D )</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( B )</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Satisfying OCL Constraints (Domain Inclusion)

- Let $\mathcal{M} = (\mathcal{C}, \mathcal{D}, \mathcal{M}, \mathcal{I})$ be a UML model, and $\mathcal{D}$ a structure.
- We (continue to) say $\mathcal{M} \models expr$ for context $C$ inv $: expr_0 \in \text{Inv}(\mathcal{M})$ iff
  \[
  \forall \pi = (\sigma_i, \varepsilon_i) \in [\mathcal{M}] \quad \forall i \in \mathbb{N} \quad \forall u \in \text{dom}(\sigma_i) \cap \mathcal{D}(C) : \\
  I[expr_0](\sigma_i, \{\text{self} \mapsto u\}) = 1.
  \]
- $\mathcal{M}$ is (still) consistent if and only if it satisfies all constraints in $\text{Inv}(\mathcal{M})$.

Example:

Transformers (Domain Inclusion)

- Transformers also remain the same, e.g. [VL 12, p. 18]
  \[
  \text{update}(expr_1, v, expr_2) : (\sigma, \varepsilon) \mapsto (\sigma', \varepsilon)
  \]
  with
  \[
  \sigma' = \sigma[u \mapsto \sigma(u)[v \mapsto I[expr_2](\sigma)]]
  \]
  where $u = I[expr_1](\sigma)$. 

\[
\begin{array}{c}
\text{0, 1} \\
\text{n} \\
\text{n} \\
\text{C} \\
\text{x : Int} \\
\text{D} \\
\end{array}
\]
**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).

\[
\begin{align*}
& (\sigma, \varepsilon) \xrightarrow{\text{cons, Snd}} (\sigma', \varepsilon') \quad \text{if} \\
& \exists u \in \text{dom}(\sigma) \cap \mathcal{D}(C) \exists u_E \in \mathcal{D}(\delta) : u_E \in \text{ready}(\varepsilon, u) \\
& u \text{ is stable and in state machine state } s, \ i.e. \sigma(u)(\text{stable}) = 1 \text{ and } \sigma(u)(\text{st}) = s, \\
& \text{a transition is enabled, i.e.} \\
& \exists (s, F, expr, act, s') \in \text{→}(SM_C) : F = E \land I[expr[\delta]] = 1 \\
& \text{where } \delta = \sigma[u.\text{params}_E \mapsto u].
\end{align*}
\]

and

- \((\sigma', \varepsilon')\) results from applying \(t_{\text{act}}\) to \((\sigma, \varepsilon)\) and removing \(u_E\) from the ether, i.e.

\[
\begin{align*}
& (\sigma'', \varepsilon'') = t_{\text{act}}(\delta, \varepsilon \oplus u_E), \\
& \sigma' = (\sigma''[u.\text{st} \mapsto s', u.\text{stable} \mapsto b, u.\text{params}_E \mapsto \emptyset])|_{\mathcal{D}(\delta) \setminus \{u_E\}}
\end{align*}
\]

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

\[
\begin{align*}
& \text{cons} = \{u, (E, \sigma(u_E))\}, \text{Snd} = \text{Obs}_{\text{act}}(\delta, \varepsilon \oplus u_E).
\end{align*}
\]
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.
    \[
    \sigma, \text{cons}, \text{Snd} \models_{\beta} E^I_{x,y}
    \]
    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).

```
C
  x : Int
  uplink

D
```

- 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 $C \triangleleft D$, extend $D$ by a (fresh) association

```
uplink_C : C 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) $C \triangleleft C_1 \triangleleft \ldots \triangleleft C_n \triangleleft D$,
  - normalise $v$ to (= replace by)

```
uplink_{C_n} -> \ldots -> 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 \( \mathcal{M} = (\mathcal{C}, \mathcal{D}, \mathcal{I}, \mathcal{S}, \mathcal{F}) \) be a UML model, and \( \mathcal{D} \) a structure.
- We (continue to) say

\[
\mathcal{M} \models \text{expr}
\]

for

\[
\text{context } C \quad \text{inv : expr} \_0 \in \text{Inv}(\mathcal{M}) = \text{expr}
\]

if and only if

\[
\forall \pi = (\sigma_i)_{i \in \mathbb{N}} \in [\mathcal{M}]
\]

\[
\forall i \in \mathbb{N}
\]

\[
\forall u \in \text{dom}(\sigma_i) \cap \mathcal{D}(C) :
\]

\[
I[, \{ \text{self } \mapsto u \}] = 1.
\]

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

- What has to change is the create transformer:
  
  \[ create(C, expr, v) \]

- Assume, C’s inheritance relations are as follows.
  
  \[
  C_{1,1} \triangleleft \ldots \triangleleft C_{1,n_1} \triangleleft C, \\
  \ldots \\
  C_{m,1} \triangleleft \ldots \triangleleft C_{m,n_m} \triangleleft C.
  \]

- 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

<table>
<thead>
<tr>
<th></th>
<th>Domain Inclusion</th>
<th>Uplink</th>
</tr>
</thead>
<tbody>
<tr>
<td>C* cp = &amp;d;</td>
<td><strong>easy:</strong> immediately compatible (in underlying system state) because &amp;d yields</td>
<td><strong>easy:</strong> By pre-processing, C* cp = d.uplink_C;</td>
</tr>
<tr>
<td></td>
<td>an identity from ( D(D) \subseteq D(C) ).</td>
<td></td>
</tr>
<tr>
<td>D* dp = (D*)cp;</td>
<td><strong>easy:</strong> the value of cp is in ( D(D) \cap D(C) ) because the pointed-to object</td>
<td><strong>difficult:</strong> we need the identity of the D whose C-slice is denoted by cp.</td>
</tr>
<tr>
<td></td>
<td>is a D. Otherwise, error condition.</td>
<td>(See next slide.)</td>
</tr>
<tr>
<td>c = d;</td>
<td><strong>bit difficult:</strong> set (for all ( C \preceq D )) ( (C)(\cdot, \cdot) : \tau D \times \Sigma \rightarrow \Sigma</td>
<td><strong>easy:</strong> By pre-processing, c = ( \ast d.uplink_C );</td>
</tr>
<tr>
<td></td>
<td>[ {u, \sigma} \mapsto \sigma(u</td>
<td>_{\text{atr}(C)}) ). Note: ( \sigma' = \sigma[u_C \mapsto \sigma(u_D)] ) is not type-compatible!</td>
</tr>
</tbody>
</table>

### 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
    \[
    \text{all} \in \mathcal{T}, \quad \mathcal{D}(\text{all}) = \bigcup_{C \in \mathcal{C}} \mathcal{D}(C)
    \]
  - 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*?
References


