Softwaretechnik / Software-Engineering

Lecture 12: Structural Software Modelling II

2018-06-18

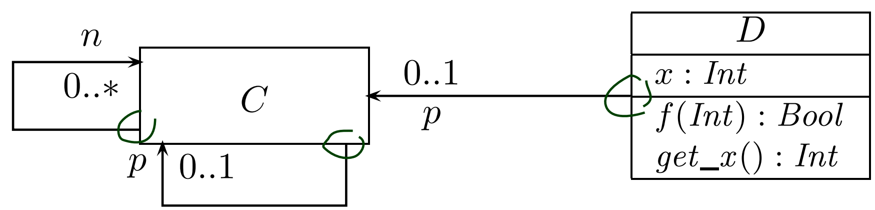
Prof. Dr. Andreas Podelski, **Dr. Bernd Westphal**

Albert-Ludwigs-Universität Freiburg, Germany

Topic Area Architecture & Design: Content

VL 11	• **Introduction and Vocabulary**
	• **Software Modelling**
⋮	– • model; views / viewpoints; 4+1 view
	• **Modelling structure**
	– • (simplified) class & object diagrams
VL 12	– • (simplified) object constraint logic (OCL)
	• **Principles of Design**
⋮	– • modularity, separation of concerns
	– • information hiding and data encapsulation
	– • abstract data types, object orientation
VL 13	• **Design Patterns**
	• **Modelling behaviour**
⋮	– • communicating finite automata (CFA)
	– • Uppaal query language
VL 14	– • CFA vs. Software
	– • Unified Modelling Language (UML)
⋮	– – • basic state-machines
	– – • an outlook on hierarchical state-machines
	• **Model-driven/-based Software Engineering**

From Abstract to Concrete Syntax



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

- $\mathscr{T} = \{Int, Bool\}$
- $\mathscr{C} = \{C, D\}$
- $V = \{x : Int, p : C_{0,1}, n : C_*\}$
- $atr = \{C \mapsto \{p, n\}, D \mapsto \{x, p\}\}$
- $F =$
  similar
- $mth =$

Content

- **Class Diagrams**
  - semantics: system states.
- **Object Diagrams**
  - concrete syntax,
  - dangling references,
  - partial vs. complete,
  - object diagrams at work.
- **Proto-OCL**
  - syntax, semantics,
  - Proto-OCL vs. OCL.
  - Putting It All Together: Proto-OCL vs. Software

A More Abstract Class Diagram Semantics

Object System Structure

Definition. An Object System **Structure** of signature

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

is a domain function $\mathscr{D}$ which assigns to each type a domain, i.e.

- $\tau \in \mathscr{T}$ is mapped to $\mathscr{D}(\tau)$,
- $C \in \mathscr{C}$ is mapped to an infinite set $\mathscr{D}(C)$ of **(object) identities**.
  - object identities of different classes are disjoint, i.e.
    $\forall C, D \in \mathscr{C} : C \neq D \rightarrow \mathscr{D}(C) \cap \mathscr{D}(D) = \emptyset$,
  - on object identities, (only) comparison for equality "$=$" is defined.
- C_* **and** $C_{0,1}$ for $C \in \mathscr{C}$ are mapped to $2^{\mathscr{D}(C)}$.

We use $\mathscr{D}(\mathscr{C})$ to denote $\bigcup_{C \in \mathscr{C}} \mathscr{D}(C)$; analogously $\mathscr{D}(\mathscr{C}_*)$.

Note: We identify **objects** and **object identities**,
because both uniquely determine each other (cf. OCL 2.0 standard).

Basic Object System Structure Example

Wanted: a structure for signature

Abc,

$$\mathscr{S}_0 = (\{Int, Bool\}, \{C, D\}, \{x : Int, p : C_{0,1}, n : C_*\}, \{C \mapsto \{p, n\}, D \mapsto \{p, x\}\},$$
$$\{f : Int \to Bool, get\_x : Int\}, \{C \mapsto \emptyset, D \mapsto \{f, get\_x\}\})$$

A structure $\mathscr{D}$ maps

- $\tau \in \mathscr{T}$ to **some** $\mathscr{D}(\tau)$, $C \in \mathscr{C}$ to **some** identities $\mathscr{D}(C)$ (infinite, pairwise disjoint),
- C_* and $C_{0,1}$ for $C \in \mathscr{C}$ to $\mathscr{D}(C_{0,1}) = \mathscr{D}(C_*) = 2^{\mathscr{D}(C)}$.

$\mathscr{D}(Bool) = \{true, false\}$

$$\begin{aligned}
\mathscr{D}(Abc) &= \{red, green\} && = \{✿, ♡, ☆\} \\
\mathscr{D}(Int) &= \mathbb{Z} && = \{one, two, three\} \\
\mathscr{D}(C) &= \mathbb{N}^+ \times \{C\} \cong \{1_C, 2_C, 3_C, \ldots\} && = \{a, aa, aaa, \ldots\} \\
\mathscr{D}(D) &= \mathbb{N}^+ \times \{D\} \cong \{1_D, 2_D, \ldots\} && = \{\cdot, /, \triangle, \square, ⬠, \ldots\} \\
\mathscr{D}(C_{0,1}) = \mathscr{D}(C_*) &= 2^{\mathscr{D}(C)} \\
\mathscr{D}(D_{0,1}) = \mathscr{D}(D_*) &= 2^{\mathscr{D}(D)}
\end{aligned}$$

$\mathscr{D}(Bool) = \{-1, 0, 1\}$

System State

object identities — attributes in $\mathscr{S}$ — values of basic types — sets of object identities

Definition. Let $\mathscr{D}$ be a structure of $\mathscr{S} = (\mathscr{T}, \mathscr{C}, V, atr, F, mth)$.
A system state of $\mathscr{S}$ wrt. $\mathscr{D}$ is a type-consistent mapping

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

partial function

That is, for each $u \in \mathscr{D}(C)$, $C \in \mathscr{C}$, if $u \in \mathrm{dom}(\sigma)$

- $\mathrm{dom}(\sigma(u)) = atr(C)$
- $(\sigma(u))(v) \in \mathscr{D}(\tau)$ if $v : \tau, \tau \in \mathscr{T}$
- $(\sigma(u))(v) \in \underbrace{\mathscr{D}(D_*)}_{= 2^{\mathscr{D}(D)}}$ if $v : D_{0,1}$ or $v : D_*$ with $D \in \mathscr{C}$

We call $u \in \mathscr{D}(\mathscr{C})$ alive in σ if and only if $u \in \mathrm{dom}(\sigma)$.

We use $\Sigma_{\mathscr{S}}^{\mathscr{D}}$ to denote the set of all system states of $\mathscr{S}$ wrt. $\mathscr{D}$.

System State Examples

$$\mathscr{S}_0 = (\{Int, Bool\}, \{C, D\}, \{x : Int, p : C_{0,1}, n : C_*\}, \{C \mapsto \{p, n\}, D \mapsto \{p, x\}\},$$
$$\{f : Int \to Bool, get\_x : Int\}, \{C \mapsto \emptyset, D \mapsto \{f, get\_x\}\})$$

$\mathscr{D}(Bool) = \{true, false\}$

$$\mathscr{D}(Int) = \mathbb{Z}, \quad \mathscr{D}(C) = \{1_C, 2_C, 3_C, ...\}, \quad \mathscr{D}(D) = \{1_D, 2_D, 3_D, ...\}$$

A system state is a partial function $\sigma : \mathscr{D}(\mathscr{C}) \nrightarrow (V \nrightarrow (\mathscr{D}(\mathscr{T}) \cup \mathscr{D}(\mathscr{C}_*)))$ such that

- $\mathrm{dom}(\sigma(u)) = atr(C)$,
- $\sigma(u)(v) \in \mathscr{D}(\tau)$ if $v : \tau, \tau \in \mathscr{T}$,
- $\sigma(u)(v) \in \mathscr{D}(C_*)$ if $v : D_*$ or $v : D_{0,1}$ with $D \in \mathscr{C}$.

mapsto ($\sigma_1(2_C) = \dots$)

$$\sigma_1 = \{ \underset{\mathscr{D}(\mathscr{C})}{2_C} \mapsto \underbrace{\{ p \mapsto \{2_C\}, n \mapsto \emptyset \}}_{V \nrightarrow (\mathscr{D}(\mathscr{T}) \cup \mathscr{D}(\mathscr{C}_*))}, 1_D \mapsto \{ p \mapsto \{2_C\}, x \mapsto 27 \} \}$$

$$\sigma_2 = \emptyset$$

$$\sigma_3 = \{ 5_C \mapsto \{ p \mapsto \underline{\{13_C\}}, n \mapsto \emptyset \} \} \checkmark$$

Content

- **Class Diagrams**
  - semantics: system states.
- **Object Diagrams**
  - concrete syntax,
  - dangling references,
  - partial vs. complete,
  - object diagrams at work.
- **Proto-OCL**
  - syntax, semantics,
  - Proto-OCL vs. OCL.
  - Putting It All Together: Proto-OCL vs. Software

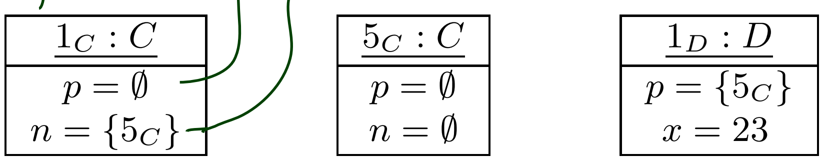
Object Diagrams

Object Diagrams

$$\mathscr{S}_0 = (\{Int, Bool\}, \{C, D\}, \{x : Int, p : C_{0,1}, n : C_*\}, \{C \mapsto \{p, n\}, D \mapsto \{p, x\}\},$$
$$\{f : Int \to Bool, get\_x : Int\}, \{C \mapsto \emptyset, D \mapsto \{f, get\_x\}\}), \qquad \mathscr{D}(Int) = \mathbb{Z}$$

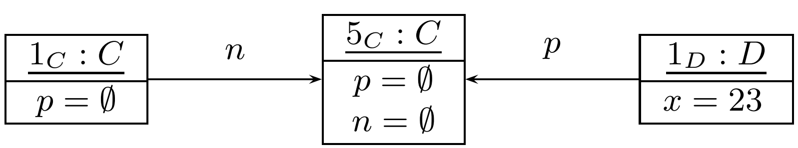
$$\sigma = \{1_C \mapsto \{p \mapsto \emptyset, n \mapsto \{5_C\}\}\cancel{\}}, 5_C \mapsto \{p \mapsto \emptyset, n \mapsto \emptyset\}, 1_D \mapsto \{p \mapsto \{5_C\}, x \mapsto 23\}\}$$

- We may **represent** σ graphically as follows:

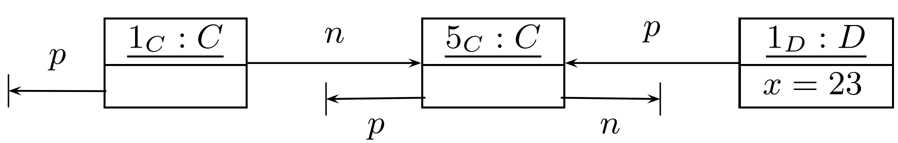


  This is an **object diagram**.

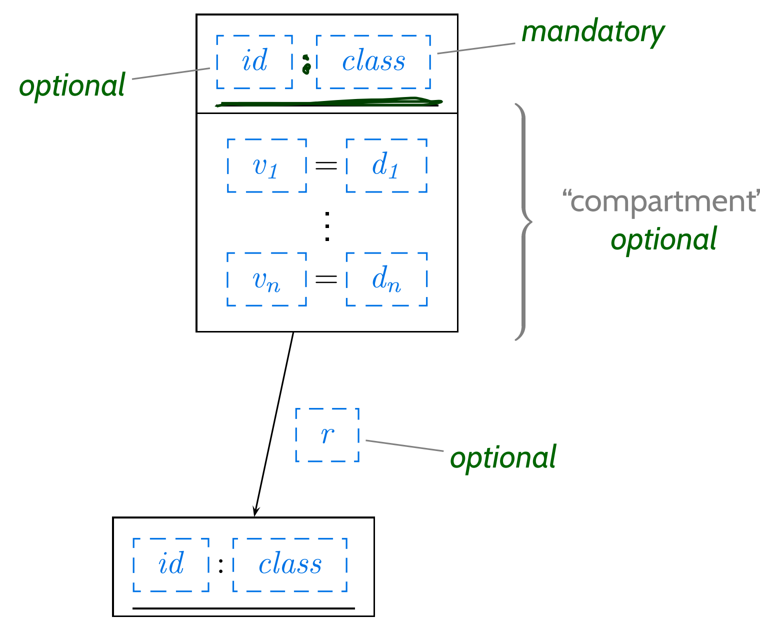
- Alternative notation:



- Alternative **non-standard** notation:



Concrete Syntax:



Special Case: Dangling Reference

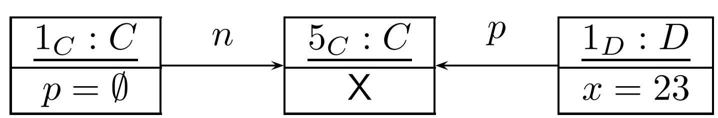
Definition.
Let $\sigma \in \Sigma_{\mathscr{S}}^{\mathscr{D}}$ be a system state and $u \in \mathrm{dom}(\sigma)$ an alive object of class C in σ.

We say $r \in atr(C)$ **is a dangling reference in** u if and only if
$r : C_{0,1}$ or $r : C_*$ and u refers to a **non-alive** object via v, i.e.

$$\big(\sigma(u)\big)(r) \not\subseteq \mathrm{dom}(\sigma).$$

Example:

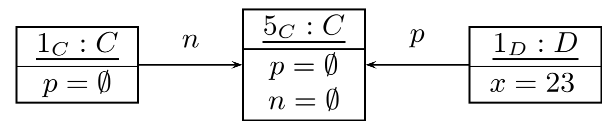
- $\sigma = \{1_C \mapsto \{p \mapsto \emptyset, n \mapsto \underline{\{5_C\}}\}\cancel{\}}, 1_D \mapsto \{p \mapsto \{5_C\}, x \mapsto 23\}\}$
- Object diagram representation:



Partial vs. Complete Object Diagrams

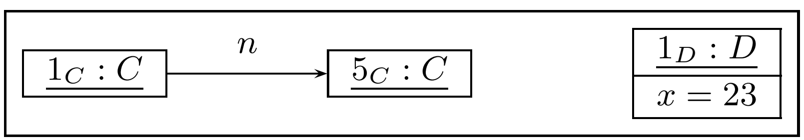
- By now we discussed "**object diagram represents system state**":

$$\{1_C \mapsto \{p \mapsto \emptyset, n \mapsto \{5_C\}\},\ 5_C \mapsto \{p \mapsto \emptyset, n \mapsto \emptyset\},\ 1_D \mapsto \{p \mapsto \{5_C\}, x \mapsto 23\}\} \quad \rightsquigarrow$$

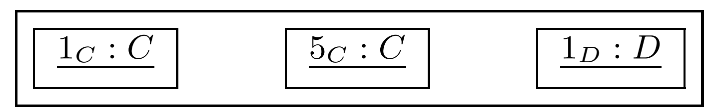


What about the other way round...?

- **Object diagrams** can be **partial**, e.g.

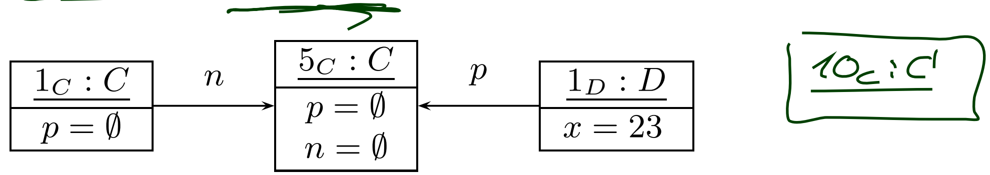


or



$\rightarrow$ we may omit information.

- Is the following object diagram **partial** or **complete**?

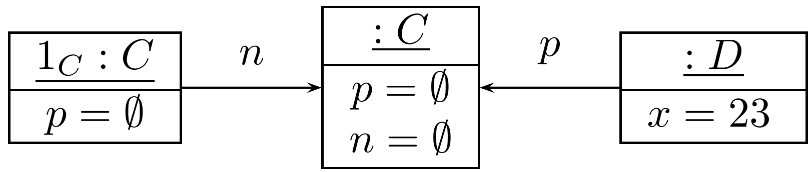


- If an object diagram
  - has values for **all** attributes of **all** objects in the diagram, and
  - if we **say that** it is meant to be complete

then we can **uniquely** reconstruct a system state σ.

Special Case: Anonymous Objects

If the object diagram



is considered as **complete**, then it denotes the set of all system states

$$\{1_C \mapsto \{p \mapsto \emptyset, n \mapsto \{c\}\}\cancel{\}}, c \mapsto \{p \mapsto \emptyset, n \mapsto \emptyset\}, d \mapsto \{p \mapsto \{c\}, x \mapsto 23\}\}$$

where $\quad c \in \mathscr{D}(C), \quad d \in \mathscr{D}(D), \quad \underline{c \neq 1_C}.$

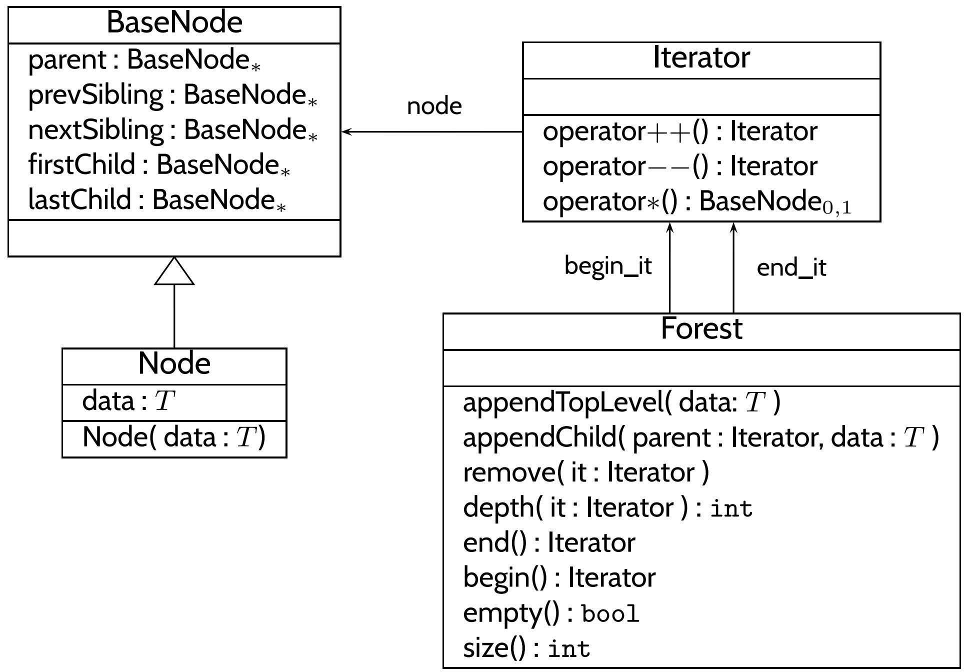
Intuition: different boxes represent different objects.

Content

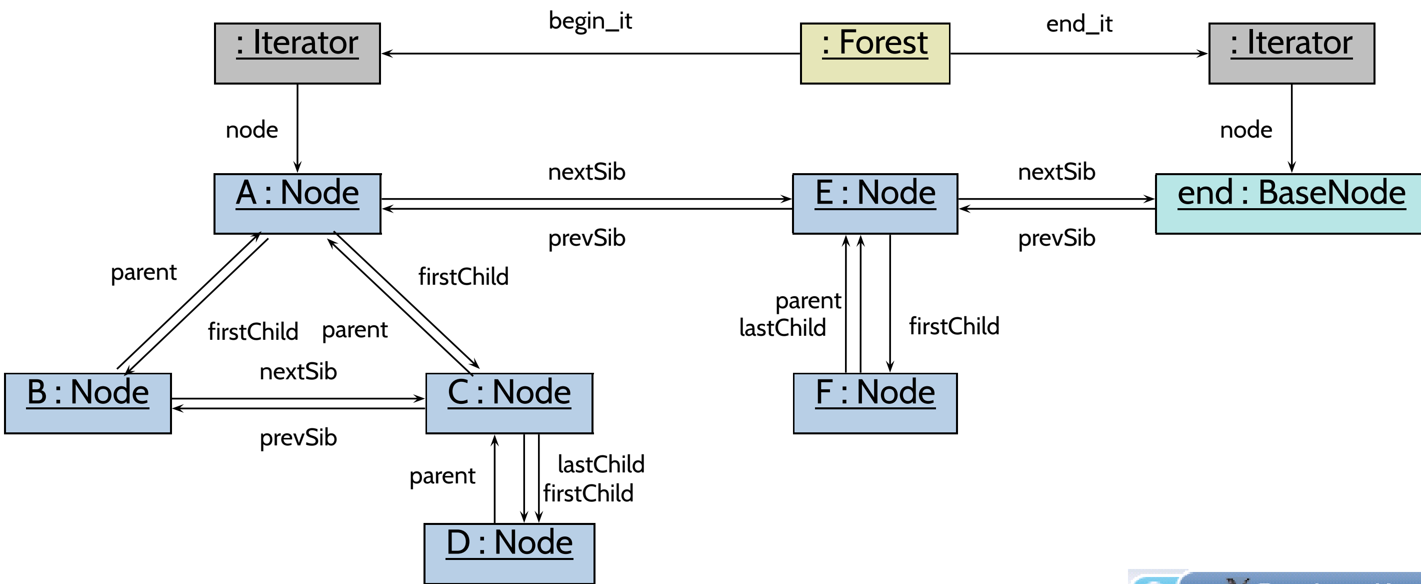
- **Class Diagrams**
  - semantics: system states.
- **Object Diagrams**
  - concrete syntax,
  - dangling references,
  - partial vs. complete,
  - object diagrams at work.
- **Proto-OCL**
  - syntax, semantics,
  - Proto-OCL vs. OCL.
  - Putting It All Together: Proto-OCL vs. Software

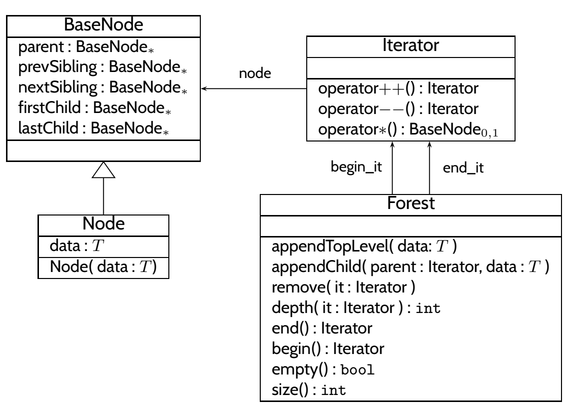
Object Diagrams at Work

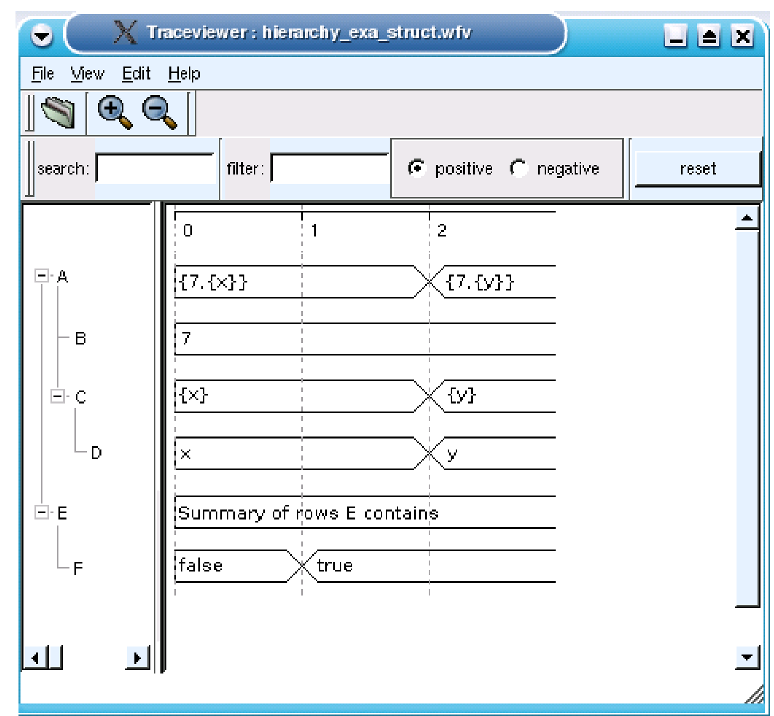
Example: Data Structure (Schumann et al., 2008)



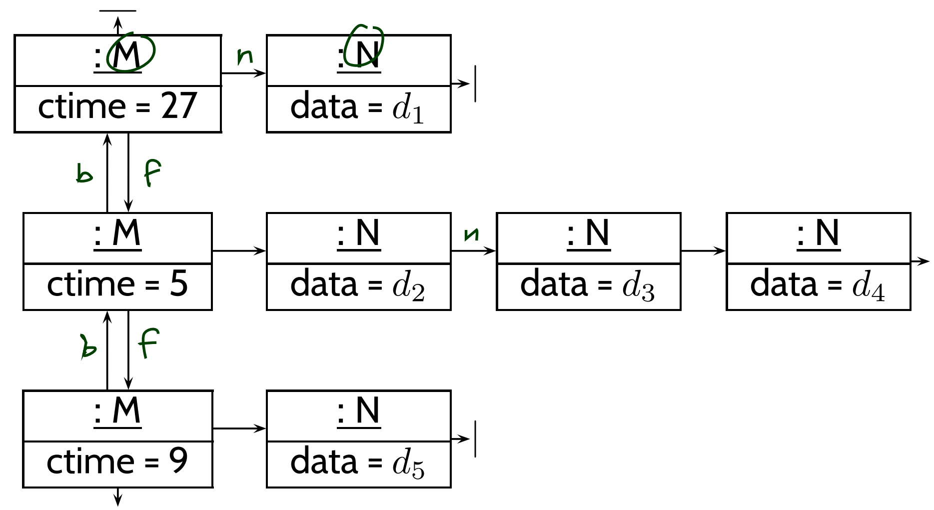
Example: Illustrative Object Diagram (Schumann et al., 2008)

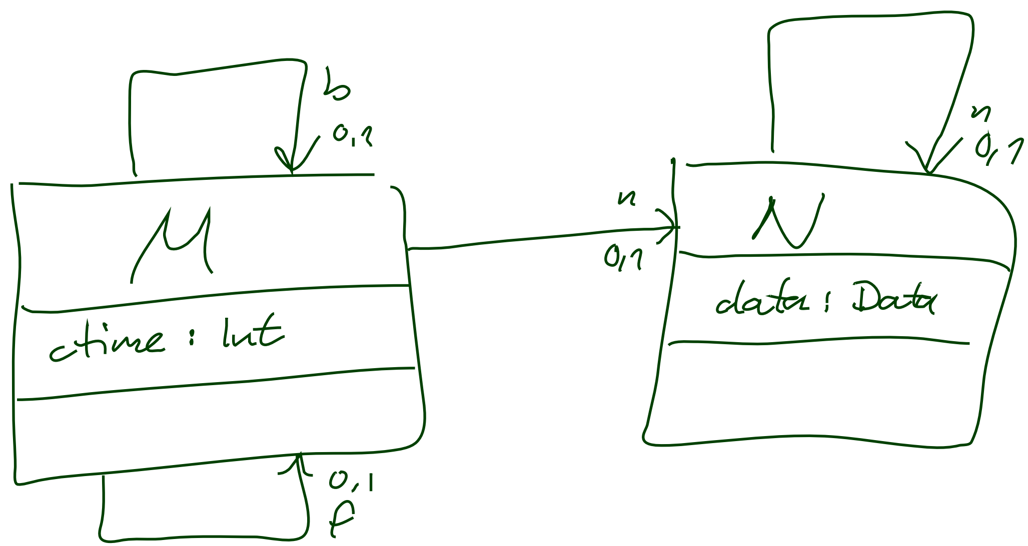






Object Diagrams for Analysis





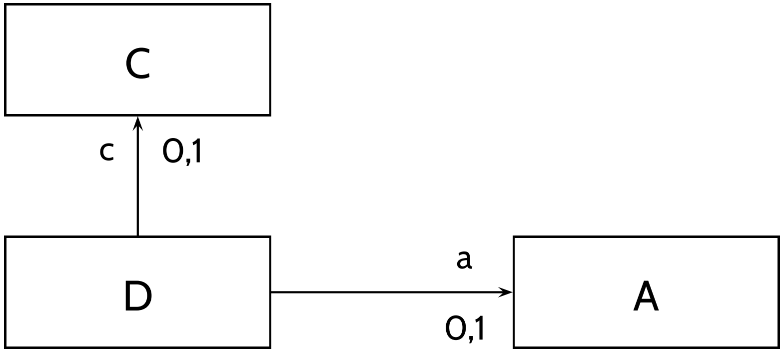
Content

- **Class Diagrams**
  - semantics: system states.
- **Object Diagrams**
  - concrete syntax,
  - dangling references,
  - partial vs. complete,
  - object diagrams at work.
- **Proto-OCL**
  - syntax, semantics,
  - Proto-OCL vs. OCL.
  - Putting It All Together: Proto-OCL vs. Software

Towards Object Constraint Logic (OCL)

— "Proto-OCL" —

Motivation

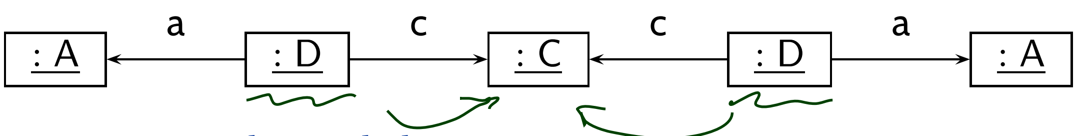


- How do I **precisely, formally** tell **my developers** that

  All D-instances having a link to the same C object
  must ~~should~~ have links to the same A.

  $\Longrightarrow$

- That is, the following system state is **forbidden** in the software:

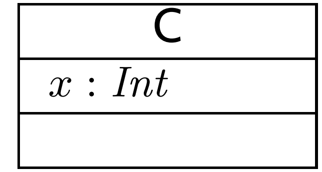


  Note: formally, it is a **proper system state**.

- Use **(Proto-)OCL**: "Dear developers, please only use system states which satisfy:"

$$\forall\, d_1 \in allInstances_D \bullet \forall\, d_2 \in allInstances_D \bullet c(d_1) = c(d_2) \implies a(d_1) = a(d_2)$$

Constraints on System States



- **Example**: for all C-instances, x should never have the value 27. $\neq(x(c), 27)$

$$\forall\, c \in \underbrace{allInstances_C}_{F_1} \bullet \underbrace{x(c) \neq 27}_{F_2}$$

- **Proto-OCL Syntax** wrt. signature $(\mathscr{T}, \mathscr{C}, V, atr, F, mth)$, c is a **logical variable**, $C \in \mathscr{C}$:

$$\begin{array}{rlll}
F ::= & c & : \tau_C & \\
| & allInstances_C & : 2^{\tau_C} & \\
| & v(F) & : \tau_C \to \tau_\perp, & \text{if } v : \tau \in atr(C), \tau \in \mathscr{T} \\
| & v(F) & : \tau_C \to \tau_D, & \text{if } v : D_{0,1} \in atr(C) \\
| & v(F) & : \tau_C \to 2^{\tau_D}, & \text{if } v : D_* \in atr(C) \\
| & f(F_1, \dots, F_n) & : \tau_1 \times \dots \times \tau_n \to \tau, & \text{if } f : \tau_1 \times \dots \times \tau_n \to \tau \\
| & \forall\, c \in F_1 \bullet F_2 & : \tau_C \times 2^{\tau_C} \times \mathbb{B}_\perp \to \mathbb{B}_\perp &
\end{array}$$

- The formula above in **prefix normal form**: $\forall\, c \in allInstances_C \bullet \neq (x(c), 27)$

Semantics

- **Proto-OCL Types:**
  - $\mathcal{I}[\![\tau_C]\!] = \mathscr{D}(C) \,\dot\cup\, \{\bot\}$, $\quad \mathcal{I}[\![\tau_\bot]\!] = \mathscr{D}(\tau) \,\dot\cup\, \{\bot\}$, $\quad \mathcal{I}[\![2^{\tau_C}]\!] = \mathscr{D}(C_*) \,\dot\cup\, \{\bot\}$
  - $\mathcal{I}[\![\mathbb{B}_\bot]\!] = \{\textit{true}, \textit{false}\} \,\dot\cup\, \{\bot\}$, $\quad \mathcal{I}[\![\mathbb{Z}_\bot]\!] = \mathbb{Z} \,\dot\cup\, \{\bot\}$

- **Functions:**
  - We assume $f_\mathcal{I}$ given for each function symbol f ($\rightarrow$ in a minute).

- **Proto-OCL Semantics** (interpretation function):
  - $\mathcal{I}[\![c]\!](\sigma, \beta) = \beta(c)$ (assuming β is a type-consistent valuation of the logical variables),
  - $\mathcal{I}[\![allInstances_C]\!](\sigma, \beta) = \mathrm{dom}(\sigma) \cap \mathscr{D}(C)$,
  - $\mathcal{I}[\![v(F)]\!](\sigma, \beta) = \begin{cases} \sigma\,(\mathcal{I}[\![F]\!](\sigma, \beta))(v) & \text{, if } \mathcal{I}[\![F]\!](\sigma, \beta) \in \mathrm{dom}(\sigma) \\ \bot & \text{, otherwise} \end{cases}$ (if not $v : C_{0,1}$)
  - $\mathcal{I}[\![v(F)]\!](\sigma, \beta) = \begin{cases} u' & \text{, if } \mathcal{I}[\![F]\!](\sigma, \beta) \in \mathrm{dom}(\sigma) \text{ and } \sigma(\mathcal{I}[\![F]\!](\sigma, \beta))(v) = \{u'\} \\ \bot & \text{, otherwise} \end{cases}$ (if $v : C_{0,1}$)
  - $\mathcal{I}[\![f(F_1, \dots, F_n)]\!](\sigma, \beta) = f_\mathcal{I}(\mathcal{I}[\![F_1]\!](\sigma, \beta), \dots, \mathcal{I}[\![F_n]\!](\sigma, \beta))$,
  - $\mathcal{I}[\![\forall\, c \in F_1 \bullet F_2]\!](\sigma, \beta) = \begin{cases} \textit{true} & \text{, if } \mathcal{I}[\![F_2]\!](\sigma, \beta[c := u]) = \textit{true} \text{ for all } u \in \mathcal{I}[\![F_1]\!](\sigma, \beta) \\ \textit{false} & \text{, if } \mathcal{I}[\![F_2]\!](\sigma, \beta[c := u]) = \textit{false} \text{ for some } u \in \mathcal{I}[\![F_1]\!](\sigma, \beta) \\ \bot & \text{, otherwise} \end{cases}$

Semantics Cont'd

- Proto-OCL is a **three-valued** logic: a formula evaluates to *true*, *false*, or $\bot$.
- **Example**: $\wedge_\mathcal{I}(\cdot,\cdot) : \{$*true*, *false*, $\bot\} \times \{$*true*, *false*, $\bot\} \to \{$*true*, *false*, $\bot\}$ is defined as follows:

x_1	*true*	*true*	*true*	*false*	*false*	*false*	$\bot$	$\bot$	$\bot$
x_2	*true*	*false*	$\bot$	*true*	*false*	$\bot$	*true*	*false*	$\bot$
$\wedge_\mathcal{I}(x_1, x_2)$	*true*	*false*	$\bot$	*false*	*false*	*false*	$\bot$	*false*	$\bot$

We assume common logical connectives $\neg, \wedge, \vee, \dots$ with canonical 3-valued interpretation.

- **Example**: $+_\mathcal{I}(\cdot,\cdot) : (\mathbb{Z} \dot\cup \{\bot\}) \times (\mathbb{Z} \dot\cup \{\bot\}) \to \mathbb{Z} \dot\cup \{\bot\}$

$$+_\mathcal{I}(x_1, x_2) = \begin{cases} x_1 + x_2 & \text{, if } x_1 \neq \bot \text{ and } x_2 \neq \bot \\ \bot & \text{, otherwise} \end{cases}$$

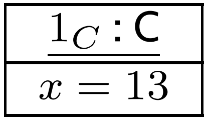
We assume common arithmetic operations $-, /, *, \dots$
and relation symbols $>, <, \leq, \dots$ with **monotone** 3-valued interpretation.

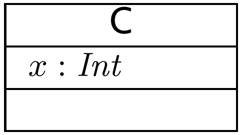
- And we assume the special unary function symbol $isUndefined$:

$$isUndefined_\mathcal{I}(x) = \begin{cases} \textit{true} & \text{, if } x = \bot, \\ \textit{false} & \text{, otherwise} \end{cases}$$

$isUndefined_\mathcal{I}$ is **definite**: it never yields $\bot$.

Example: Evaluate Formula for System State

σ :


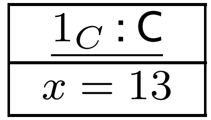


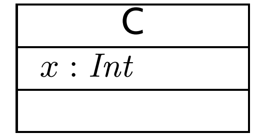
$$\forall\, c \in allInstances_C \bullet x(c) \neq 27$$

- Recall **prefix notation**: $\forall\, c \in allInstances_C \bullet \neq(x(c), 27)$

  Note: $\neq$ is a binary function symbol, 27 is a 0-ary function symbol.

Example: Evaluate Formula for System State

σ : 



$$\forall\, c \in allInstances_C \bullet x(c) \neq 27$$

- Recall **prefix notation**: $\forall\, c \in allInstances_C \bullet \neq(x(c), 27)$

  Note: $\neq$ is a binary function symbol, 27 is a 0-ary function symbol.

- **Example**:

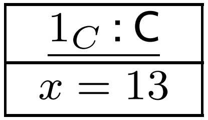
  $\{1_C\}$

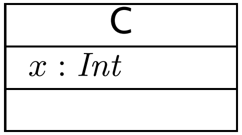
  $\mathcal{I}[\![\forall\, c \in allInstances_C \bullet \neq(x(c), 27)]\!](\sigma, \emptyset) =$ *true*, because…

  $\mathcal{I}[\![\neq(x(c), 27)]\!](\sigma, \beta)$, $\quad \beta := \emptyset[c := 1_C] = \{c \mapsto 1_C\}$

  $=$

Example: Evaluate Formula for System State

σ : 



$$\forall\, c \in allInstances_C \bullet x(c) \neq 27$$

- Recall **prefix notation**: $\forall\, c \in allInstances_C \bullet \neq(x(c), 27)$

  Note: $\neq$ is a binary function symbol, 27 is a 0-ary function symbol.

- **Example**:

  $\mathcal{I}[\![\forall\, c \in allInstances_C \bullet \neq(x(c), 27)]\!](\sigma, \emptyset) =$ *true*, because...

  $\mathcal{I}[\![\neq(x(c), 27)]\!](\sigma, \beta)$, $\quad \beta := \emptyset[c := 1_C] = \{c \mapsto 1_C\}$

  $= \neq_{\mathcal{I}}(\, \underbrace{\mathcal{I}[\![x(c)]\!](\sigma, \beta)}_{},\ \underbrace{\mathcal{I}[\![27]\!](\sigma, \beta)}_{}\,)$

  $=$

Example: Evaluate Formula for System State

σ : | $\underline{1_C : \mathsf{C}}$ |
|---|
| $x = 13$ |

C
$x : \mathit{Int}$

$$\forall\, c \in \mathit{allInstances}_C \bullet x(c) \neq 27$$

- Recall **prefix notation**: $\forall\, c \in \mathit{allInstances}_C \bullet \neq(x(c), 27)$

  Note: $\neq$ is a binary function symbol, 27 is a 0-ary function symbol.

- **Example**:

  $\mathcal{I}[\![\forall\, c \in \mathit{allInstances}_C \bullet \neq(x(c), 27)]\!](\sigma, \emptyset) =$ *true*, because...

  $\mathcal{I}[\![\neq(x(c), 27)]\!](\sigma, \beta), \quad \beta := \emptyset[c := 1_C] = \{c \mapsto 1_C\}$

  $= \neq_{\mathcal{I}}(\ \mathcal{I}[\![x(c)]\!](\sigma, \beta),\ \mathcal{I}[\![27]\!](\sigma, \beta)\ )$

  $= \neq_{\mathcal{I}}((\sigma(\ \underline{\mathcal{I}[\![c]\!](\sigma, \beta)}\ ))(\underline{x}),\ 27_{\mathcal{I}}\ )$

  $=$

Example: Evaluate Formula for System State

σ :

$\underline{1_C : \mathsf{C}}$
$x = 13$

C
$x : \mathit{Int}$

$$\forall\, c \in allInstances_C \bullet x(c) \neq 27$$

- Recall **prefix notation**: $\forall\, c \in allInstances_C \bullet \neq(x(c), 27)$

  Note: $\neq$ is a binary function symbol, 27 is a 0-ary function symbol.

- **Example**:

  $\mathcal{I}[\![\forall\, c \in allInstances_C \bullet \neq(x(c), 27)]\!](\sigma, \emptyset) =$ *true*, because…

  $\mathcal{I}[\![\neq(x(c), 27)]\!](\sigma, \beta)$, $\quad \beta := \emptyset[c := 1_C] = \{c \mapsto 1_C\}$

  $= \neq_\mathcal{I}(\ \mathcal{I}[\![x(c)]\!](\sigma, \beta),\ \mathcal{I}[\![27]\!](\sigma, \beta)\ )$

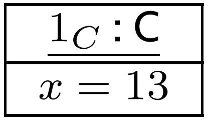
  $= \neq_\mathcal{I}(\ \sigma(\ \mathcal{I}[\![c]\!](\sigma, \beta)\ )(x),\ 27_\mathcal{I}\ )$

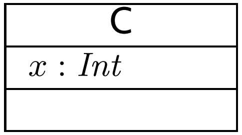
  $= \neq_\mathcal{I}(\ \sigma(\ \beta(c)\ )(x),\ 27_\mathcal{I}\ )$

  $= \neq_\mathcal{I}((\sigma(\ 1_C\ ))(x),\ 27_\mathcal{I}\ )$

  $=$

Example: Evaluate Formula for System State

σ : 



$$\forall\, c \in allInstances_C \bullet x(c) \neq 27$$

- Recall **prefix notation**: $\forall\, c \in allInstances_C \bullet \neq(x(c), 27)$

  Note: $\neq$ is a binary function symbol, 27 is a 0-ary function symbol.

- **Example**:

  $\mathcal{I}[\![\forall\, c \in allInstances_C \bullet \neq(x(c), 27)]\!](\sigma, \emptyset) =$ *true*, because…

  $\mathcal{I}[\![\neq(x(c), 27)]\!](\sigma, \beta)$, $\quad \beta := \emptyset[c := 1_C] = \{c \mapsto 1_C\}$

  $= \neq_{\mathcal{I}}(\ \mathcal{I}[\![x(c)]\!](\sigma, \beta),\ \mathcal{I}[\![27]\!](\sigma, \beta)\ )$

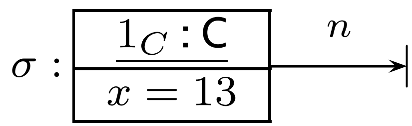
  $= \neq_{\mathcal{I}}(\ \sigma(\ \mathcal{I}[\![c]\!](\sigma, \beta)\ )(x),\ 27_{\mathcal{I}}\ )$

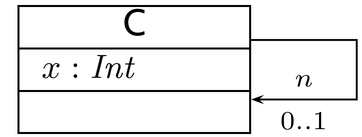
  $= \neq_{\mathcal{I}}(\ \sigma(\ \beta(c)\ )(x),\ 27_{\mathcal{I}}\ )$

  $= \neq_{\mathcal{I}}(\ \sigma(\ 1_C\ )(x),\ 27_{\mathcal{I}}\ )$

  $= \neq_{\mathcal{I}}(\ 13,\ 27\ ) =$ *true* …and 1_C is the only C-object in σ: $\mathcal{I}[\![allInstances_C]\!](\sigma, \emptyset) = \{1_C\}$.

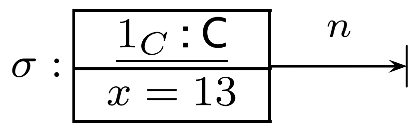
More Interesting Example

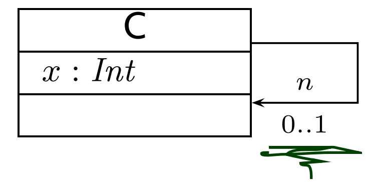




$$\forall\, c : allInstances_C \bullet x(n(c)) \neq 27$$

More Interesting Example





$$\forall\, c : allInstances_C \bullet x(n(c)) \neq 27$$

- Similar to the previous slide, we need the value of

$$\mathcal{I}[\![x(n(c))]\!](\sigma, \beta),\, \beta = \{c \mapsto 1_C\}$$

  - $\mathcal{I}[\![c]\!](\sigma, \beta) =$ $\beta(c) = 1_C$

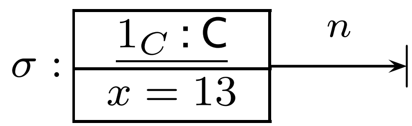
  - $\mathcal{I}[\![n(c)]\!](\sigma, \beta) = \bot$ since $\sigma(\, \mathcal{I}[\![c]\!](\sigma, \beta)\,)(n) = \emptyset \neq \{u'\}$ by rule

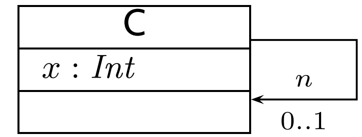
$$\mathcal{I}[\![v(F)]\!](\sigma, \beta) = \begin{cases} u' & \text{, if } \mathcal{I}[\![F]\!](\sigma, \beta) \in \mathrm{dom}(\sigma) \text{ and } \sigma(\mathcal{I}[\![F]\!](\sigma, \beta))(v) = \{u'\} \\ \bot & \text{, otherwise} \end{cases} \quad \text{(if } v : C_{0,1}\text{)}$$

  - $\mathcal{I}[\![x(n(c))]\!](\sigma, \beta) = \bot$ since $\mathcal{I}[\![n(c)]\!](\sigma, \beta) = \bot$ by rule

$$\mathcal{I}[\![v(F)]\!](\sigma, \beta) = \begin{cases} \sigma\,(\mathcal{I}[\![F]\!](\sigma, \beta))\,(v) & \text{, if } \mathcal{I}[\![F]\!](\sigma, \beta) \in \mathrm{dom}(\sigma) \\ \bot & \text{, otherwise} \end{cases} \quad \text{(if not } v : C_{0,1}\text{)}$$

More Interesting Example





$$\forall\, c : allInstances_C \bullet x(n(c)) \neq 27$$

- Similar to the previous slide, we need the value of

$$\mathcal{I}[\![x(n(c))]\!](\sigma, \beta), \beta = \{c \mapsto 1_C\}$$

- $\mathcal{I}[\![c]\!](\sigma, \beta) = \beta(c) = 1_C$
- $\mathcal{I}[\![n(c)]\!](\sigma, \beta) = \bot$ since $\sigma(\, \mathcal{I}[\![c]\!](\sigma, \beta)\,)(n) = \emptyset \neq \{u'\}$ by rule

$$\mathcal{I}[\![v(F)]\!](\sigma, \beta) = \begin{cases} u' & \text{, if } \mathcal{I}[\![F]\!](\sigma, \beta) \in \mathrm{dom}(\sigma) \text{ and } \sigma(\mathcal{I}[\![F]\!](\sigma, \beta))(v) = \{u'\} \\ \bot & \text{, otherwise} \end{cases} \quad \text{(if } v : C_{0,1}\text{)}$$

- $\mathcal{I}[\![x(n(c))]\!](\sigma, \beta) = \bot$ since $\mathcal{I}[\![n(c)]\!](\sigma, \beta) = \bot$ by rule

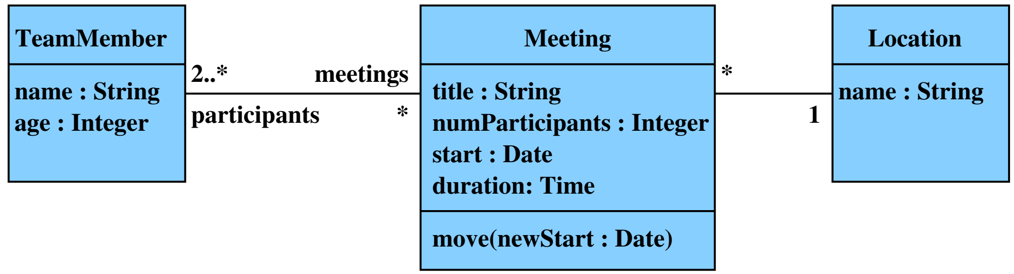
$$\mathcal{I}[\![v(F)]\!](\sigma, \beta) = \begin{cases} \sigma\,(\mathcal{I}[\![F]\!](\sigma, \beta))\,(v) & \text{, if } \mathcal{I}[\![F]\!](\sigma, \beta) \in \mathrm{dom}(\sigma) \\ \bot & \text{, otherwise} \end{cases} \quad \text{(if not } v : C_{0,1}\text{)}$$

Object Constraint Language (OCL)

OCL is the same — just with less readable (?) syntax.

Literature: (OMG, 2006; Warmer and Kleppe, 1999).

Examples *(from lecture “Softwaretechnik 2008”)*

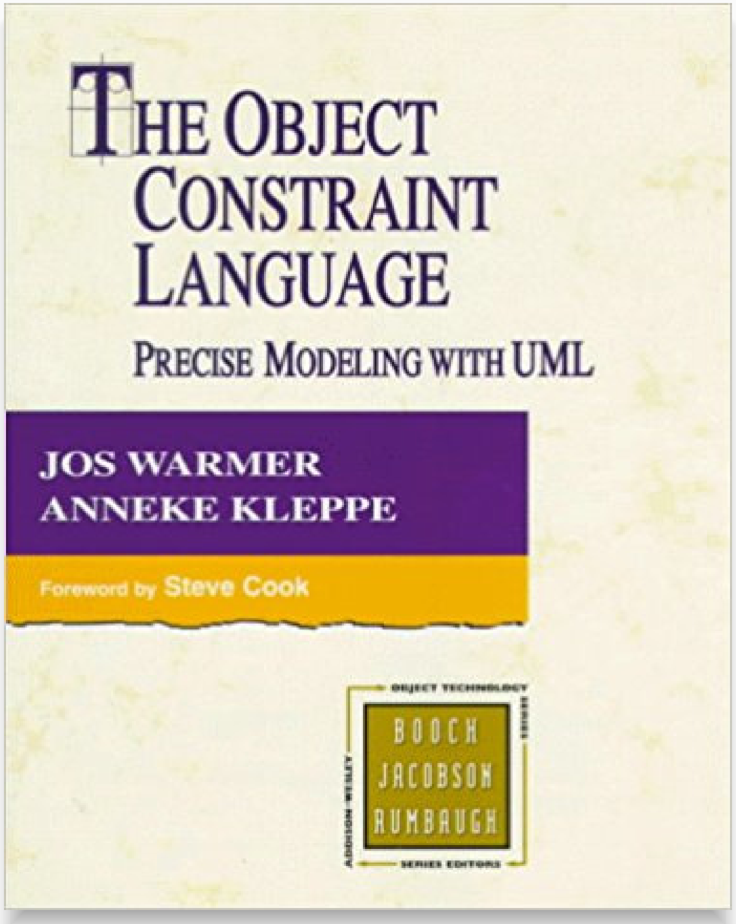


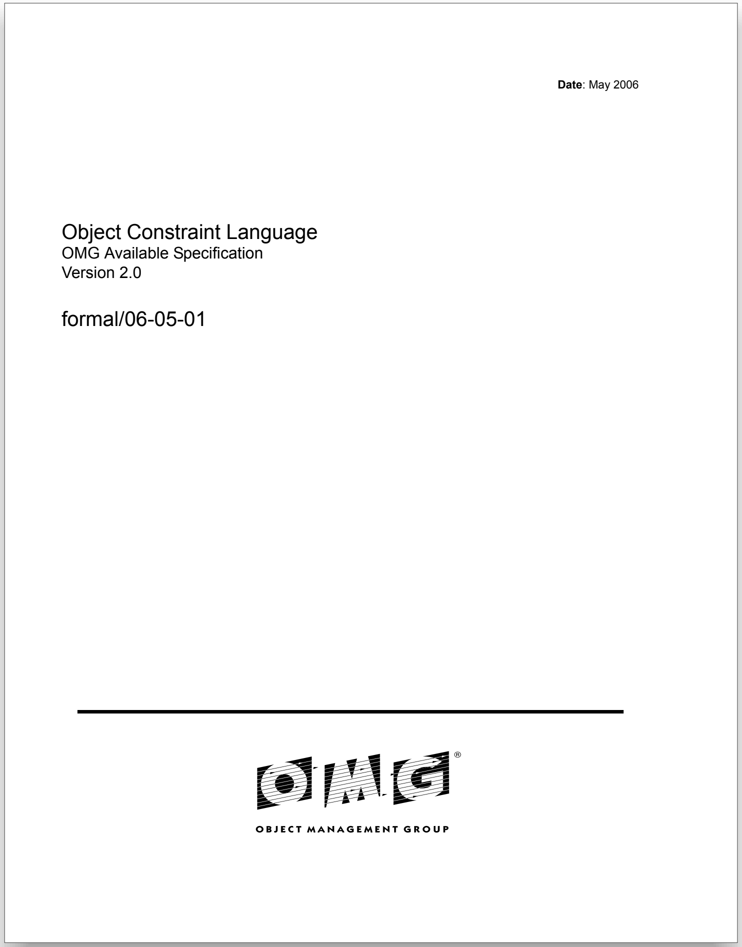
- **context** Meeting
  - **inv:** self.participants->size() = numParticipants
- **context** Location
  - **inv:** name="Lobby" **implies** meeting->isEmpty()

$\forall\, self : allInstances_{Meeting} \bullet$
$size(participants(self)) = numParticipants(self)$

Prof. Dr. P. Thiemann, http://proglang.informatik.uni-freiburg.de/teaching/swt/2008/

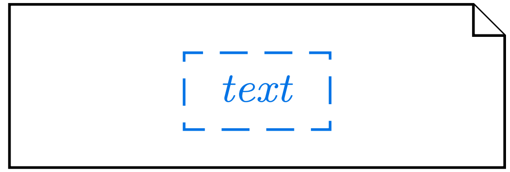
Literature


THE OBJECT CONSTRAINT LANGUAGE
PRECISE MODELING WITH UML
JOS WARMER
ANNEKE KLEPPE
Foreword by Steve Cook
BOOCH
JACOBSON
RUMBAUGH


Date: May 2006
Object Constraint Language
OMG Available Specification
Version 2.0
formal/06-05-01
OBJECT MANAGEMENT GROUP

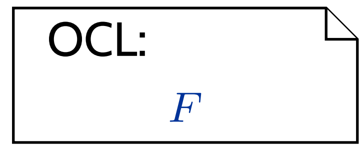
Where To Put OCL Constraints?

- **Notes**: A UML **note** is a diagram element of the form

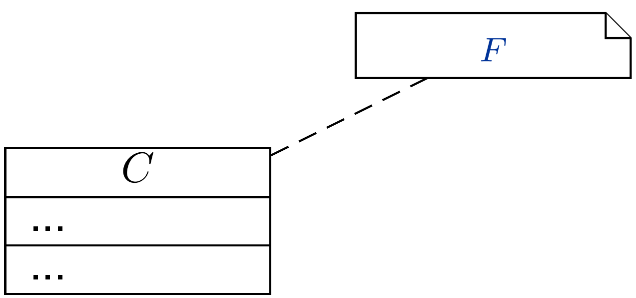


$text$ can principally be **everything**, in particular **comments** and **constraints**.

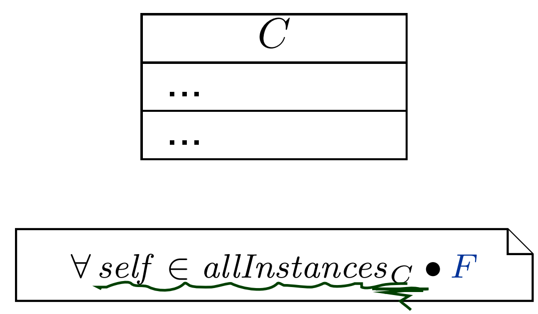
Sometimes, content is **explicitly classified** for clarity:



- Conventions:



stands for



Content

- **Class Diagrams**
  - semantics: system states.
- **Object Diagrams**
  - concrete syntax,
  - dangling references,
  - partial vs. complete,
  - object diagrams at work.
- **Proto-OCL**
  - syntax, semantics,
  - Proto-OCL vs. OCL.
  - Putting It All Together: Proto-OCL vs. Software

Putting It All Together

Modelling Structure with Class Diagrams

Definition. **Software** is a finite description S of a (possibly infinite) set $[\![S]\!]$ of (finite or infinite) computation paths of the form $\sigma_0 \xrightarrow{\alpha_1} \sigma_1 \xrightarrow{\alpha_2} \sigma_2 \cdots$ where

- $\sigma_i \in \Sigma$, $i \in \mathbb{N}_0$, is called **state** (or **configuration**), and
- $\alpha_i \in A$, $i \in \mathbb{N}_0$, is called **action** (or **event**).

The (possibly partial) function $[\![\,\cdot\,]\!] : S \mapsto [\![S]\!]$ is called **interpretation** of S.

- The set of **states** Σ could be the set of **system states** as defined by a class diagram, e.g.

$$\Sigma := \Sigma_{\mathscr{S}}^{\mathscr{D}} \qquad\qquad \mathscr{S} : \begin{array}{|c|}\hline \mathsf{C} \\ \hline x : \mathit{Int} \\ \hline \\ \hline\end{array}$$

- A corresponding **computation path** of a software S could be

$$\begin{array}{|c|}\hline \underline{27_C : \mathsf{C}} \\ \hline x = 0 \\ \hline\end{array} \xrightarrow{\tau} \begin{array}{|c|}\hline \underline{27_C : \mathsf{C}} \\ \hline x = 1 \\ \hline\end{array} \xrightarrow{\tau} \begin{array}{|c|}\hline \underline{27_C : \mathsf{C}} \\ \hline x = 3 \\ \hline\end{array} \xrightarrow{\tau} \begin{array}{|c|}\hline \underline{27_C : \mathsf{C}} \\ \hline x = 4 \\ \hline\end{array} \xrightarrow{\tau} \ldots$$

- If a requirement is formalised by the Proto-OCL constraint

$$F = \forall\, c \in allInstances_C \bullet x(c) < 4$$

then S **does not** satisfy the requirement.

More General: Software vs. Proto-OCL

- Let $\mathscr{S}$ be an **object system signature** and $\mathscr{D}$ a **structure**.
- Let S be a **software** with
  - states $\Sigma \subseteq \Sigma_{\mathscr{S}}^{\mathscr{D}}$, and
  - **computation paths** $[\![S]\!]$.
- Let F be a Proto-OCL constraint over $\mathscr{S}$.
- We say $[\![S]\!]$ **satisfies** F, denoted by $[\![S]\!] \models F$, if and only if for all

$$\sigma_0 \xrightarrow{\alpha_1} \sigma_1 \xrightarrow{\alpha_2} \sigma_2 \cdots \in [\![S]\!]$$

  and all $i \in \mathbb{N}_0$,

$$\mathcal{I}[\![F]\!](\sigma_i, \emptyset) = \textit{true}.$$

- We say $[\![S]\!]$ **does not satisfy** F, denoted by $[\![S]\!] \not\models F$, if and only if there exists $\sigma_0 \xrightarrow{\alpha_1} \sigma_1 \xrightarrow{\alpha_2} \sigma_2 \cdots \in [\![S]\!]$ and $i \in \mathbb{N}_0$, such that $\mathcal{I}[\![F]\!](\sigma_i, \emptyset) = \textit{false}$.
- **Note**: $\neg([\![S]\!] \not\models F)$ does not imply $[\![S]\!] \models F$.

Tell Them What You've Told Them...

- **Class Diagrams** can be used to **graphically**
  - visualise code,
  - define an **object system structure** $\mathscr{S}$.
- An **Object System Structure** $\mathscr{S}$ (together with a structure $\mathscr{D}$)
  - defines a set of **system states** $\Sigma_\mathscr{S}^\mathscr{D}$.
- A **System State** $\sigma \in \Sigma_\mathscr{S}^\mathscr{D}$
  - can be **visualised** by an **object diagram**.
- **Proto-OCL** constraints can be evaluated on **system states**.
- A **software** over $\Sigma_\mathscr{S}^\mathscr{D}$ satisfies a Proto-OCL constraint F if and only if F evaluates to *true* in all system states of all the software's computation paths.

References

References

Ludewig, J. and Lichter, H. (2013). *Software Engineering*. dpunkt.verlag, 3. edition.

OMG (2006). Object Constraint Language, version 2.0. Technical Report formal/06-05-01.

Schumann, M., Steinke, J., Deck, A., and Westphal, B. (2008). Traceviewer technical documentation, version 1.0. Technical report, Carl von Ossietzky Universität Oldenburg und OFFIS.

Warmer, J. and Kleppe, A. (1999). *The Object Constraint Language*. Addison-Wesley.