FOUNDATIONS OF THE UML

Lecture 1: Introduction

Joost-Pieter Katoen

Sofware Modeling & Verification
(MOVES)

moves.rwth-aachen.de/i2/1g2

WS 2007/2008

October 29, 2007

TARGET AUDIENCE

Diploma Programme "Informatik"
+ Master "Systems Software Engineering"

- elective course Theor. Computer Science
- spezialization MOVES

In general:

- interest in system software engineering
- interest in formal methods for software
- interest in semantics + verification
- application of mathematical reasoning

Prerequisites basic knowledge in:

- mathematical Logic,
- formal languages and automata theory
- algorithms and data structures
- complexity theory (a bit)

ORGANIZATION

Schedule

Lecture	Mon	$16^{00} - 17^{30}$	AH 4	(except 12.11 and 4.2)
	Wed	$10^{00} - 11^{30}$	AH 2	(14.11 + 16.1)
Exercises	Wed	$10^{00} - 11^{30}$	AH 2	

(7.11, 21.11, 5.12, 19.12, 9.1, 23.1, 6.2)

Keep track of website for single dates!

People involved

Lecture	Joost-Pieter	Katoen
Exercises	Carsten	Kern
Student-assistant	Denise	Nimmerichter

Mail

katoen@cs.rwth-aachen.de

kern@cs.rwth-aachen.de

denise.nimmerrichter@post.rwth-aachen.de

ORGANIZATION

Assignments

- bi-weekly assignments
- hand in solution at next exercise class
- first assignment: handed out *today*
- groups of two students

Examination (4 ECTS credit points)

written / oral exam (depending on # students)

in February 2008

Admission

1. at least 50 % of exercise points
2. a summary (7-12 pp. in LaTeX)
   on one of the lectures
   (except this one!)
   - delivery: $\leq$ 1 week after lecture
   - will be checked by me.

MOTIVATION

Goal: formal description and analysis of (concurrent) software systems

Focus: the Unified Modeling Language

More specifically:

- Sequence Diagrams
  used for requirements analysis
- Hierarchical State Machines
  behavioural description of systems
- The Object Constraint Language (OCL)
  property specification of UML diagram

Aims:

- clarify and make precise the semantics of treated UML fragments
- formal reasoning about basic properties of UML models
- algorithms to verify such properties

WHAT IS IT ** NOT ** ABOUT ?

- the use of the UML in the SW development cycle
- other notations of the UML (e.g. class diagrams, activity diagrams)
- what is precisely in the UML, and what is not
  - Liberal interpretation of which constructs belong to the UML
- applying the UML to concrete cases
- empirical results on usage UML
- drawing pictures

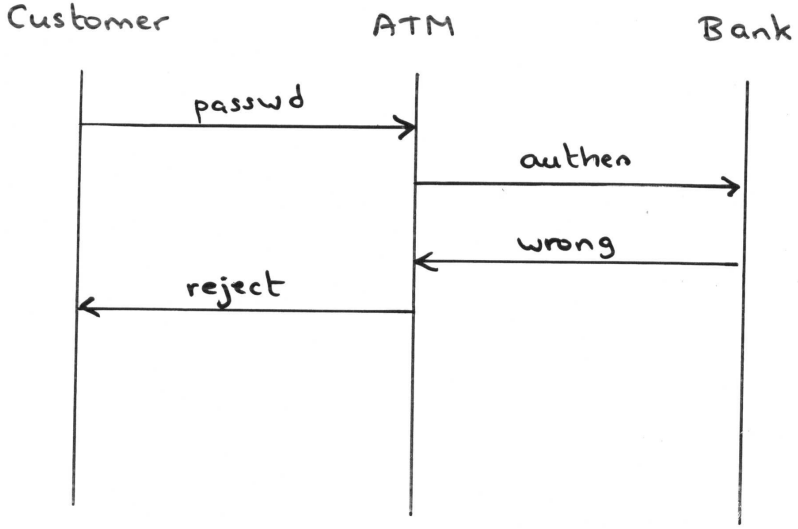
.....

SEQUENCE DIAGRAMS

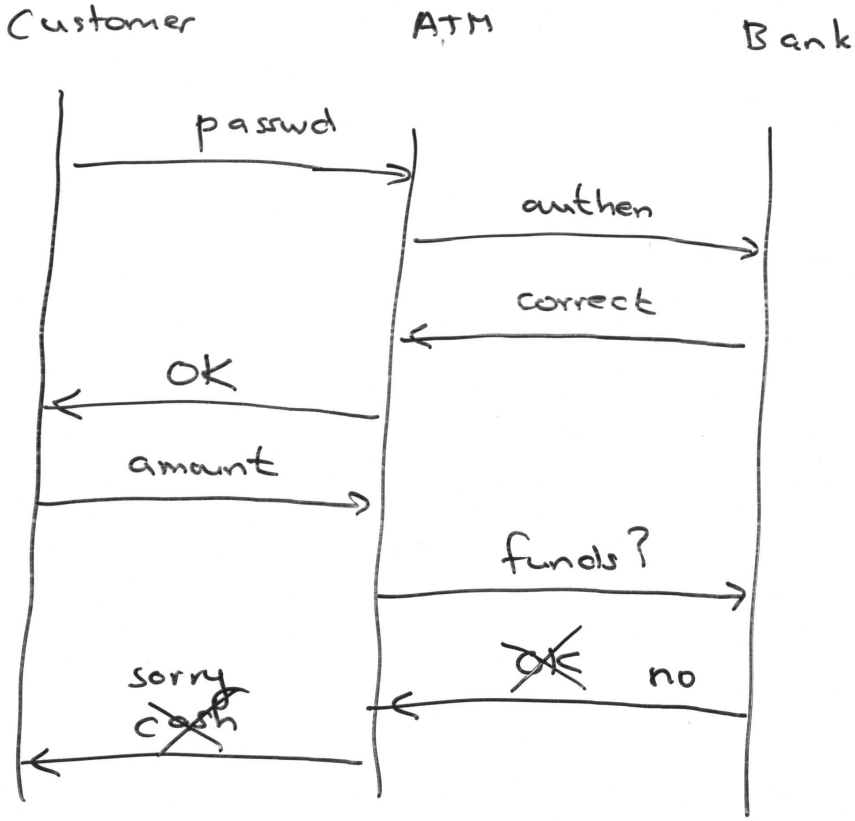
- origin: telecommunications

  "Message Sequence Charts" (MSCs)

- describe interactions between processes (or: objects)
- attractive visual formalism



- describes a possible scenario
- standardized by the ITU (Z.120)
- adopted by OMG for UML

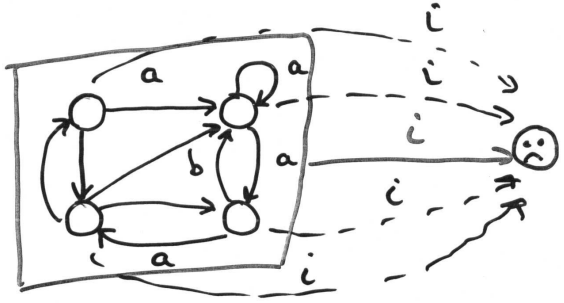


MESSAGE SEQUENCE CHARTS

- MSCs
  (syntax, semantics, linearizations, races)
- Message sequence graphs
  (composition, expressiveness, compositional MSGs)
- Realizability
  (∞ comm. finite state machines, reachability in CFSMs, MSCs vs. CFSMs, boundedness)
- Regularity
  (regular MSCs and MSGs, realizability)
- Verification
  (positive + negative model checking, complexity results, basic properties: MSCAN)

HIERARCHICAL STATE MACHINES

- finite state machines
  - no strategy for top-down or bottom-up development
    ("states have no structure")
  - no natural notion of hierarchy
  - uneconomical concerning transitions
    (e.g. high-level interrupt)

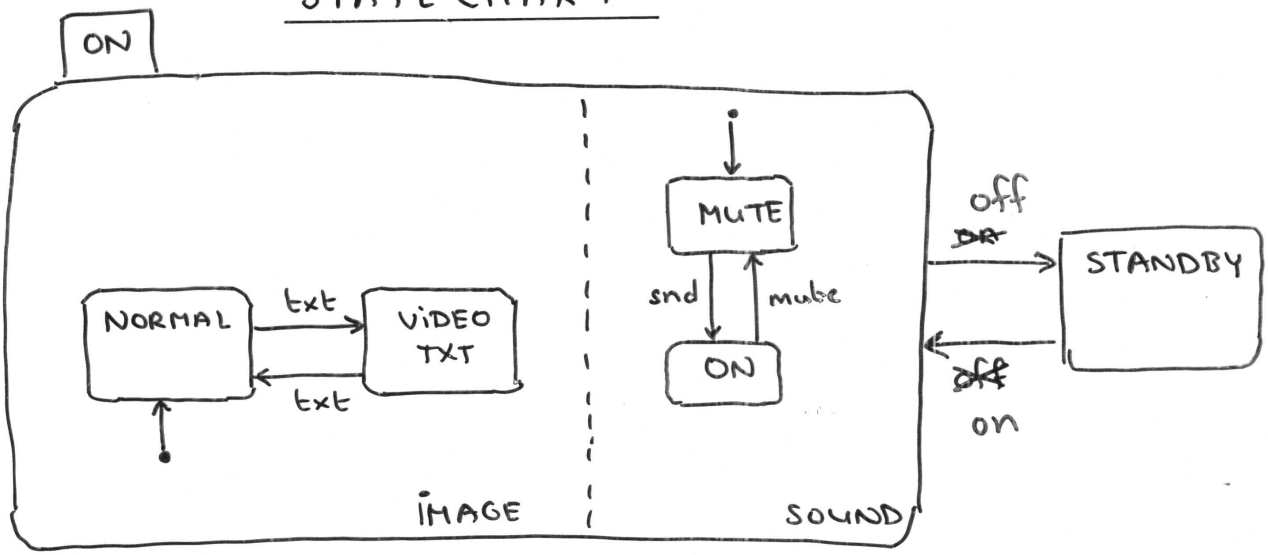


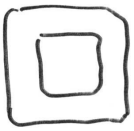
  - uneconomical w.r.t. parallel composition
    (exponential growth in # states)

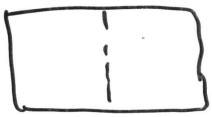
Statecharts = Mealy machines
+ depth
+ orthogonality
+ broadcast
+ data

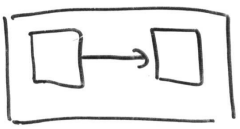
[Harel '86]

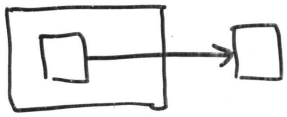
STATE CHART



 = hierarchical state

 = AND state

 = inter-level transition

 = intra-level transition

STATE CHARTS

- Harel's State charts
  (basic features, syntax, state hierarchy, orthogonality, intra- and inter-level transitions)
- Semantics
  (main issues, formal semantics, flattening, succinctness)
- Verification
  (expressiveness, reachability, LTL model checking)

OBJECT CONSTRAINT LANGUAGE

- allows specification of basic propeties on objects

```
context  Room  invariant
    guests → size  ≤  numOfBeds

context  Hotel :: checkIn (g: Guest)
pre   not  guests → includes(g)
post  guests → size = (guests@pre → size) + 1
      and  guests → includes (g)
```

- not related to particular diagram of UML
- often: annotations to different types of UML diagrams

  (e.g. class diagrams,
  activity diagrams,
  statecharts ....)

OBJECT CONSTRAINT LANGUAGE

Topics:

- OCL basics

  (types, operations, navigation, class diagr.)

- Semantics of the OCL

  (operational model, logic, types + values)

- Embedding into temporal logic

  (LTL/CTL, from OCL to temporal)

PART I

SEQUENCE DIAGRAMS

HISTORY

- 70s - 80s : often used informally
- 1992 : first version of MSCs standardized by CCITT (currently ITU) Z.120
- 1992 - 1996 : many extensions, e.g. high-level + formal semantics (using process algebras)
- 1996 : MSC '96 standard
- 2000 : MSC 2000 : time, data, o-o features

..... MSC 2004 .....

VARIANTS

UML sequence diagrams, (instantiations of) use cases, triggered MSCs, netcharts (= Petri net + MSC), STAIRS, live sequence charts

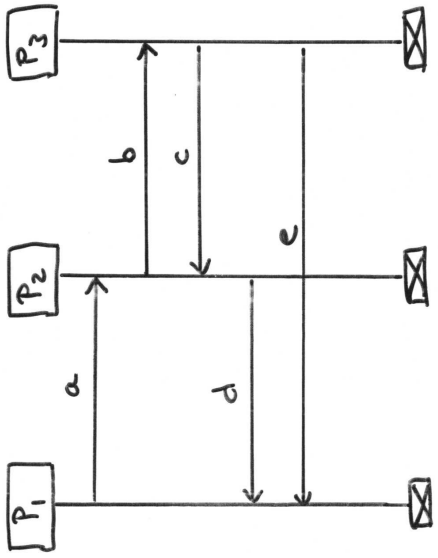
.....

APPLICATIONS

- requirements specification
  (positive, negative scenarios, e.g. CREWS)
- system design and software engineering
- visualization of test cases
  (graphical extension to TTCN)
- feature interaction detection
- workflow management systems

.....

EXAMPLE



PRELIMINARIES (1)

- Let $\mathcal{P}$: finite set of ≥ 2 sequential processes

  $\mathbb{C}$: a finite set of message contents

  $a, b, c, \ldots \in \mathbb{C}$

- Communication action: $p, q \in \mathcal{P}$, $p \neq q$, $a \in \mathbb{C}$

  $p\,!\,q\,(a)$ " p sends message a to q "

  $p\,?\,q\,(a)$ " p receives message a sent by q

- For E a set of events, a partial order over E is a relation $< \subseteq E \times E$ such that:

  1. $<$ is irreflexive, i.e., $\neg(e < e)$ $\forall e \in E$
  2. $<$ is transitive:

     $e < e' \wedge e' < e''$ implies $e < e''$
  3. $<$ is acyclic

     $e < e' \wedge e' < e$ is forbidden

- Let $(E, <)$ be a poset. The Hasse diagram $(E, <\cdot)$ is defined by: $e <\cdot e'$ iff $e < e'$ and $\neg(\exists e''.\ e < e'' < e')$

PRELIMINARIES (2)

- Let $(E, <)$ be a poset. A linearization of $(E, <)$ is a total order $\sqsubset$ such that

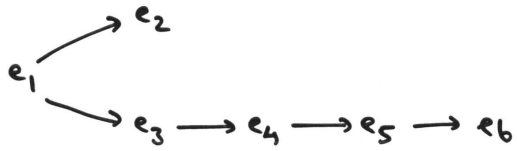
  $e < e'$ implies $e \sqsubset e'$

- A linearization is a topological sort of the Hasse diagram of $(E, <)$.

Example $E = \{e_1, \ldots, e_6\}$

$< = \{ (e_1, e_2), (e_1, e_3), (e_3, e_4), (e_4, e_5), (e_5, e_6), (e_1, e_4), (e_3, e_5), (e_1, e_5), (e_1, e_6), (e_3, e_6), (e_4, e_6) \}$

Hasse diagram:



Linearizations:

$e_1\ e_2\ e_3\ e_4\ e_5\ e_6$, $e_1\ e_3\ e_2\ e_4\ e_5\ e_6$, $e_1\ e_3\ e_4\ e_2\ e_5\ e_6$

$e_1\ e_3\ e_4\ e_5\ e_2\ e_6$, $e_1\ e_3\ e_4\ e_5\ e_6\ e_2$, ~~$e_2\ e_1\ e_3 \ldots$~~

DEFINITION

An MSC $M = (P, E, \mathbb{C}, \ell, m, <)$ with:

- P, a finite set of processes $\{p_1, p_2, \ldots, p_n\}$
- E, a finite set of events

$$E = \biguplus_{p \in P} E_p = \underbrace{E_? \uplus E_! \uplus E_{loc}}_{\text{partitioning of } E}$$

- $\mathbb{C}$, finite set of message content
- $\ell : E \to Act$, a labelling function

$$\ell(e) = \begin{cases} p\,!\,q\,(a) & \text{if } e \in E_p \cap E_! \\ p\,?\,q\,(a) & \text{if } e \in E_p \cap E_? \\ p(a) & \text{if } e \in E_p \cap E_{loc} \end{cases} \quad \left.\begin{array}{l} p \neq q \\ a \in \mathbb{C} \end{array}\right\}$$

- $m : E_! \to E_?$ a bijection ("matching function")

satisfying: $m(e) = e' \wedge \ell(e) = p\,!\,q\,(a)$ implies $\ell(e') = q\,?\,p\,(a)$

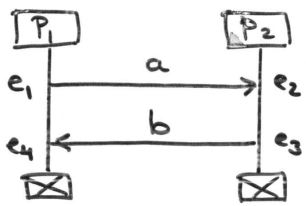
$(p \neq q,\ a \in \mathbb{C})$

- $< \subseteq E \times E$ is a partial order ("visual order")

$$< = \underbrace{\bigcup_{p \in P} <_p}_{<_p \text{ is total order}} \cup \underbrace{\{(e, m(e)) \mid e \in E_!\}}_{\text{communication order } <_c}$$

$<_p$ = "top-to-bottom" order on process p

EXAMPLE



MSC M

$M = (P, E, \mathbb{C}, \ell, m, <)$ with

$P = \{p_1, p_2\}$ $\quad E_{p_1} = \{e_1, e_4\}$

$E = \{e_1, e_2, e_3, e_4\}$

$\mathbb{C} = \{a, b\}$ $\quad E_! = \{e_1, e_3\}$

$\ell(e_1) = p_1\,!\,p_2\,(a)$ $\quad m(e_1) = e_2$

$\ell(e_2) = p_2\,?\,p_1\,(a)$

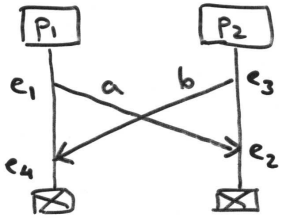
$\ell(e_3) = p_2\,!\,p_1\,(b)$ $\quad m(e_3) = e_4$

$\ell(e_4) = p_1\,?\,p_2\,(b)$

Hasse diagram of $(E, <)$:

$e_1 \longrightarrow e_2 \longrightarrow e_3 \longrightarrow e_4$ (agrees with $<_c$)

Linearizations?



MSC M'

$M' = (\underbrace{P, E, \mathbb{C}, \ell, m}_{\text{as above}}, <')$ with

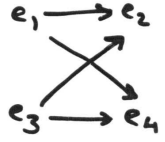
$<'_c$: $e_1 \longrightarrow e_2$

$e_3 \longrightarrow e_4$

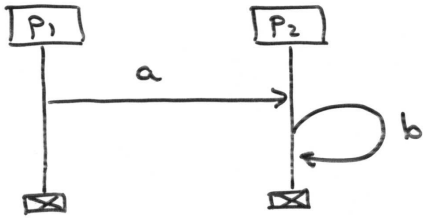
$<'_{p_1}$: $e_1 \longrightarrow e_4$

$<'_{p_2}$: $e_3 \longrightarrow e_2$

$<'$:



EXAMPLE (2)



not an MSC

FiFO Property

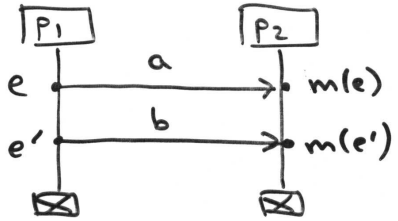
MSC $M = (P, E, \mathbb{C}, \ell, m, <)$ has the First-In First-Out (FiFO) property whenever:

for all $e, e' \in E_!$ we have

$$e < e' \wedge \ell(e) = p!q(a) \wedge \ell(e') = p!q(b)$$

implies $m(e) < m(e')$

"no message overtaking"



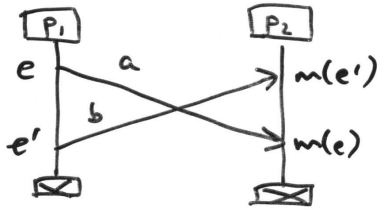
FiFO

$\ell(e) = P_1 ! P_2(a)$

$\ell(e') = P_1 ! P_2(b)$

$e < e'$

$\Rightarrow$ $m(e) < m(e')$



non-FiFO

Note: we assume an MSC to possess the FiFO property, unless stated otherwise

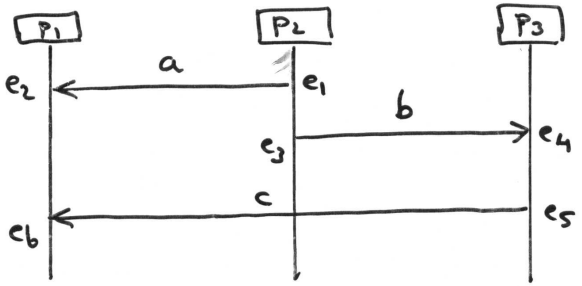
LINEARIZATIONS

Lin (M) = set of linearizations of MSC M

Lemma: there is a one-to-one correspondence between MSCs and their sets of linearizations

so: Lin (M) uniquely characterizes M!

VISUAL ORDER VS. POSSIBLE ORDER



$e_2 < e_6$?

if b takes much shorter than a,
then c might arrive at p_1 before a!

formally: $<_{p_1} = \{ (e_6, e_2) \}$ is possible

$\neq$ visual order

when are such situations possible?

RACES

- Let $M = (P, E, \mathbb{C}, t, m, <)$ be an MSC.
- Let $\ll \subseteq E \times E$ defined by:

$e \ll e'$ iff $e' = m(e)$

or $e <_p e'$ and either e or $e' \in E_!$

or $e, e' \in E_p \cap E_?$ and $m^{-1}(e) <_q m^{-1}e$

$\ll$ is the "interpreted / possible order"

- Example (cf. previous slide)

$e_1 \ll e_2$, $e_3 \ll e_4$, $e_5 \ll e_6$, $e_1 \ll e_3$

- MSC M contains a race if for some $e, e' \in E$.

$e <_p e'$ but $\neg(e \ll^* e')$

↓

reflexive and transitive closure of $\ll$

- How to check whether MSC M has a race?

compute $\ll^*$ and compare to $<_p$

(Floyd-Warshall $O(|E|^3)$, but here $O(|E|^2)$.