1

FOUNDATIONS OF THE UML

lecture 5 :

Realizability

Joost-Pieter Katoen

MOVES@RWTH

moves.rwth-aachen.de/i2/192

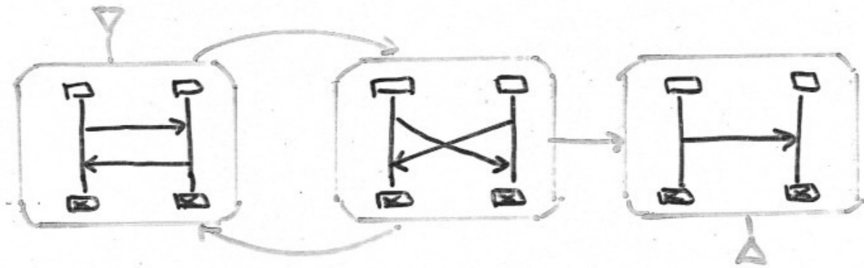
WS 2007/2008

November 26, 2007

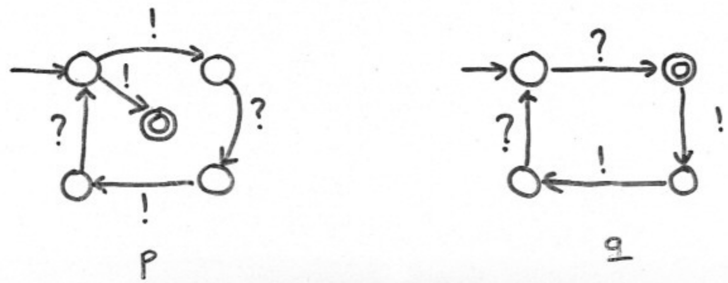
2

REALIZABILITY

- MSCs = example scenarios
  - impose a global system view
- MPA = implementation model
  - set of communicating finite-state machines
  - collection of local system views



FROM HIGH-LEVEL SPECIFICATION TO IMPLEMENTATION MODEL



MESSAGE PASSING AUTOMATA

An MPA over set of processes $\mathbb{P}$ and set of messages $\mathbb{C}$ is a structure

$$A = \left((S_p, \Delta_p)_{p \in \mathbb{P}}, \mathbb{D}, s_{init}, F \right)$$

where:

- $\mathbb{D}$ is a nonempty finite set of sync messages
- for each $p \in \mathbb{P}$:
  - S_p is a nonempty finite set of local states with $S_p \cap S_q = \emptyset$, $p \neq q$
  - $\Delta_p \subseteq S_p \times Act_p \times \mathbb{D} \times S_p$ local transition
- let $S_A := \prod_{p \in \mathbb{P}} S_p$ set of global satates
- $s_{init} \in S_A$ is global initial state
- $F \subseteq S_A$ set of global finil states

SEMANTICS OF MPA

Interpretation of MPA A is given in terms of a (possibly infinite-state) automaton

$$(Conf_A, \Longrightarrow_A, \gamma_{init})$$

with:

- $Conf_A$ is set of configurations

$$\gamma = (\underbrace{(s_1, s_2, \ldots, s_n)}_{\text{local state of each automaton } (S_p, \Delta_p)}, \eta)$$

  η = channel valuation = content of each channel

- $\Longrightarrow_A \subseteq Conf_A \times Act \times \mathbb{D} \times Conf_A$ is the global transition relation

  e.g., if $s_p \xrightarrow{p!q(a),m} s_p'$ is automaton p

  then:

$$((s_p, s_q), \eta) \overset{p!q(a),m}{\Longrightarrow_A} ((s_p', s_q), \eta')$$

  with $\eta'((q,p)) = \eta((q,p))$

  $\eta'((p,q)) = (a,m) \cdot \eta((p,q))$

- $\gamma_{init} \in Conf_A$ is initial configuration $(s_{init}, \eta_\varepsilon)$

LANGUAGE OF MPA

Let MPA $A = \left((S_p, \Delta_p)_{p \in P}, \mathbb{D}, s_{init}, F \right)$.

- A <u>run</u> of A on $\alpha_1 \ldots \alpha_n \in Act^*$ is a sequence $t_0 \, m_1 \, t_1 \, m_2 \ldots t_{n-1} \, m_n \, t_n$ such that:

  t_0 is initial configuration

  $t_i \xRightarrow[A]{\alpha_{i+1}, m_{i+1}} t_{i+1}$ for $0 \le i < n$

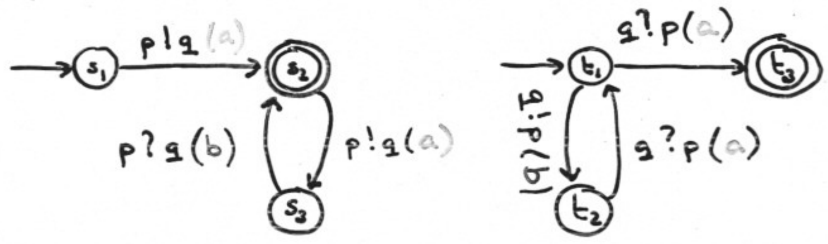
- Run ρ is <u>accepting</u> if $t_n \in F \times \underbrace{\{ \eta_\varepsilon \}}_{\text{all channels empty}}$

- $Lin(A) = \{ w \in Act^* \mid$ there is an accepting run of A on $w \}$

- $L(A)$ = set of <u>MSCs</u> defined by A

EXAMPLE

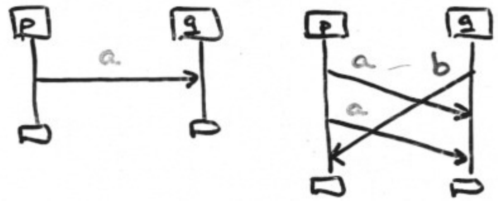
A :



process p   process q

- Some members of $Lin(A)$:
  - $p!q(a) \; q?p(a)$,
  - $p!q(a) \; q!p(b) \; p!q(a) \; p?q(b) \; q?p(a) \; q?p(a$
  - etc.

- Some MSCs defined by A :



etc.

AiM

Obtain a characterization of MSCs, or equivalently, their linearizations, for which an equivalent MPA exist.

For simplicity, we consider first the case **without** synchronization messages

$$|\mathbb{D}| = 1$$

(also known as **simple** realizability)

TRACES

$Act = \bigcup_{p \in P} Act_p$ with

$Act_p = Act_p^! \cup Act_p^?$

$Act_p^! = \{ p!q(a) \mid q \in P, q \neq p, a \in \mathbb{C} \}$

$Act_p^? = \{ p?q(a) \mid q \in P, q \neq p, a \in \mathbb{C} \}$

Sequence $w \in Act^*$ is well-formed if for every pair $(p,q) \in Ch$ it holds:

(1) for any $v \in pref(w)$:

$$\underbrace{\sum_{a \in \mathbb{C}} |v|_{p!q(a)}}_{\#\text{ sends } p \to q} - \underbrace{\sum_{a \in \mathbb{C}} |v|_{q?p(a)}}_{\#\text{ receipts } q \leftarrow p} \geq 0$$

(2) all messages sent from p to q are received by q (in w), and in the same order as they were sent.

TRACES

Let $e_1 e_2 \ldots e_n \in Lin(M)$ for MSC M.

We call $\underbrace{\ell(e_1)\,\ell(e_2) \ldots \ell(e_n)}_{\in Act^*}$ a <u>trace</u> of M

<u>Lemma:</u> $w \in Traces(M)$ iff w is well-formed

<u>Proof:</u> "$\Longrightarrow$": let $w \in Traces(M)$. Then in every prefix v of w, $\sum_a |v|_{p!q(a)} \geq \sum_a |v|_{\cancel{p?q}\,q?p(a)}$ for every $(p,q) \in Ch$. As M is FIFO, w is FIFO.

"$\Longleftarrow$": let w be well-formed. Then construct a (canonical) MSC M with trace w, starting with empty M and $w = \varepsilon$, by inductively inserting sends and receipts. For prefix $u\, p?q(a)$ of w, match $p?q(a)$ with first $q!p(a)$ in u that has not been matched yet. Since w is well-formed, all sends will be matched and messages cannot overtake each other. $\boxtimes$

REALIZABILITY

- MSC M is <u>realizable</u> whenever $M = L(A)$ for some MPA A
- Set $\{M_1, \ldots, M_k\}$ of MSCs is <u>realizable</u> whenever $\{M_1, \ldots, M_k\} = L(A)$ for some MPA A
- MSG G is <u>realizable</u> whenever $L(G) = L(A)$ for some MPA A.

<u>Equivalently:</u>

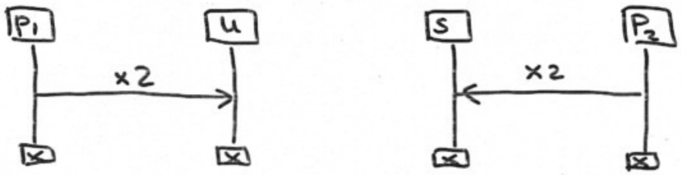
- MSC M is realizable if $Lin(M) = Lin(A)$ for some MPA A
- $\{M_1, \ldots, M_k\}$ is realizable if $\bigcup_i Lin(M_i) = Lin(A)$ for some MPA A
- MSG G is realizable if $Lin(G) = Lin(A)$ for some MPA A.

IMPOSSIBLE TO REALIZE

Consider the <u>set</u> of MSCs:

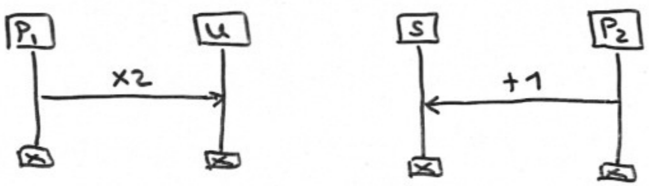
M_1:

M_2:



increase volume of U and S by one entity or double their volume (last 2 MSCs)

This implies (in absence of global control) the following scenario:



So: $\{M_1, M_2\}$ is <u>not</u> realizable

CLOSURE PROPERTY

Language $L \subseteq Act^*$ has property AB if:

for every well-formed word $w \in Act^*$

$\left(\forall p \in P.\ \exists v \in L.\ w{\upharpoonright}p = v{\upharpoonright}p\right)$ implies $w \in L$

Here $\upharpoonright p$ means <u>projection</u> on process p:

$$\varepsilon{\upharpoonright}p = \varepsilon$$

$$(r!s(a)\,u){\upharpoonright}p = \begin{cases} r!s(a)\,(u{\upharpoonright}p) & \text{if } r = p \\ u{\upharpoonright}p & \text{otherwise} \end{cases}$$

and similarly for receive actions

Intuition AB property: if w can be decomposed such that for each process its contribution to w is in L (i.e., is a possible system behavior), then w is in L.

Example: $w = p_1!u(x2)\ u?p_1(x2)\ p_2!s(+1)\ s?p_2(+1)$

$\notin Lin(\{M_1, M_2\})$ but:

$w{\upharpoonright}p_1 = p_1!u(x2)$ and $w{\upharpoonright}u = u?p_1(x2)$ are consistent with $Lin(M_2)$

$w{\upharpoonright}p_2$ and $w{\upharpoonright}s$ are consistent with $Lin(M_1)$

CHARACTERIZING REALIZABILITY

Theorem [Alur, Etessami, Yannakakis '00]

$L \subseteq Ack^*$ is realizable iff

L only contains well-formed words and L fulfills AB.

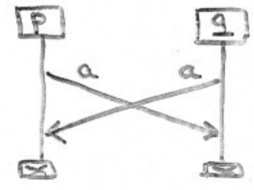
Proof : on black board

Theorem

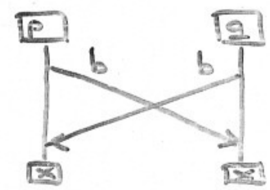
The decision problem "is a given set of MSCs realizable" is coNP-complete.

SAFE REALIZABILITY

It is possible that a set of MSCs is realizable but only by an MPA that may deadlock



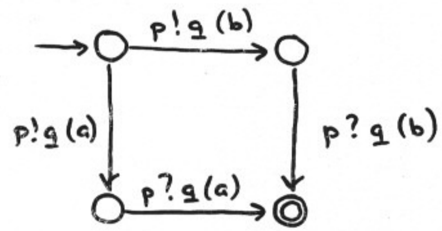
M_1



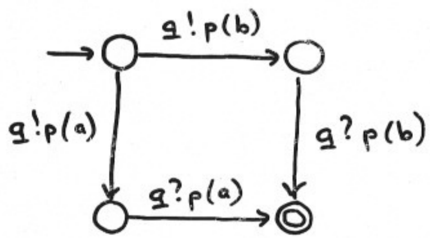
M_2

"processes p and q have to agree on a orb"

Realization:



process p

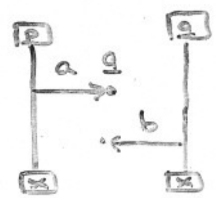


process q

Possible behavior:

$p!q(a) \quad q!p(b) \quad ↯$

deadlock !



SAFE REALIZABILITY

MPA A is <u>deadlock free</u> if from every configuration γ reachable from γ_0, a <u>final</u> configuration $\gamma' \in F \times \{\eta_\varepsilon\}$ is reachable.

- MSC M is <u>safely</u> <u>realizable</u> whenever $M = L(A)$ for some <u>deadlock free</u> MPA A

- set of MSCs $\{M_1, \dots, M_k\}$ is <u>safely</u> realizable if $\{M_1, \dots, M_k\} = L(A)$ for some deadlock free MPA A.

- MSG G is <u>safely</u> realizable if $L(G) = L(A)$ for some <u>deadlock free</u> MPA A.

Consider:

$L \subseteq Act^*$ is safely realizable if $Lin(A) = L$ for some deadlock free MPA A

Note: realizability $\not\Longrightarrow$ safe realizability (see example previous slide)

CLOSURE PROPERTY

$pref(L) = \{w \mid \exists u.\ wu \in L\}$ set of prefixes of L

<u>Recall:</u>

$L \subseteq Act^*$ has property AB if for every well-formed $w \in Act^*$:

$$\left(\forall p \in P.\ \exists v \in L.\ w\restriction_p = v\restriction_p\right) \longrightarrow w \in L.$$

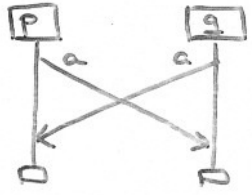
<u>Now:</u>

$L \subseteq Act^*$ has property <u>ABS</u> if for every prefix $w \in Act^*$ of a well-formed word:

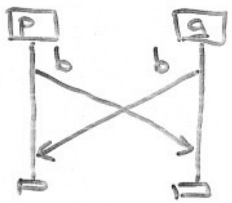
$$\left(\forall p \in P.\ \exists v \in pref(L).\ w\restriction_p = v\restriction_p\right) \longrightarrow w \in pref(L)$$

EXAMPLE

Reconsider :



M_1



M_2

$L = Lin(\{M_1, M_2\})$ fulfills AB , but <u>not</u> ABS

$L = \{$ $p!q(a)\ q!p(a)\ p?q(a)\ q?p(a)$,

$p!q(a)\ q!p(a)\ q?p(a)\ p?q(a)$,

$q!p(a)\ p!q(a)\ p?q(a)\ q?p(a)$,

$q!p(a)\ p!q(a)\ q?p(a)\ p?q(a)$,

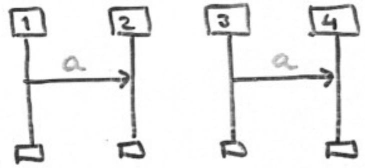
.... dito for M_2 .... $\}$

Take $w = p!q(a)\ q!p(b)$

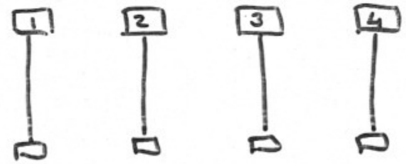
w is a prefix of a well-formed word,

$\left.\begin{array}{l} \text{and } p!q(a) \in pref(L) \\ \quad (p!q(a))\restriction p = w\restriction p \\ \text{and } q!p(b) \in pref(L) \\ \quad (q!p(b))\restriction q = w\restriction q \end{array}\right\}$ but $w \notin pref(L)$

ABS is INSUFFICIENT



M_4



M_5 (= empty)

$Lin(\{M_4, M_5\}) =$

$\{$ $1!2(a)\ 2?1(a)\ 3!4(a)\ 4?3(a)$,

$1!2(a), 3!4(a), 2?1(a)\ 4?3(a)$, ...,

$3!4(a)\ 4?3(a), 1!2(a)\ 2?1(a)$,

ε $\}$

$Lin(\{M_4, M_5\})$ possesses property ABS

but a safe realization should allow to

accept $1!2(a)\ 2?1(a)$ only — 3,4 decide to behave as M_5

or $3!4(a)\ 4?3(a)$ only — 1,2 decide to behave as M_4

So: ABS is insufficient to characterize safe realizability

ANOTHER CLOSURE PROPERTY

<u>Recall</u>:

$L \subseteq Act^*$ has property AB if for every well-formed $w \in Act^*$:

$$\left(\forall p \in P.\ \exists v \in L.\ w\restriction_p = v\restriction_p\right) \longrightarrow w \in L. \qquad (*)$$

<u>Now, in addition to ABS adapt AB as follows:</u>

$L \subseteq Act^*$ has property AB$'$ if for every well-formed $w \in pref(L)$:

$$\left(\forall p \in P.\ \exists v \in L.\ w\restriction_p = v\restriction_p\right) \longrightarrow w \in L. \qquad (*)$$

So: $(*)$ is only imposed on prefixes of L, not on arbitrary action sequences.

EXAMPLE

M_4 M_5

$Lin(\{M_4, M_5\}) =$

$\{\ 1!2(a),\ 2?1(a)\ 3!4(a)\ 4?3(a),$
$1!2(a)\ 3!4(a)\ 2?1(a)\ 4?3(a), \ldots, \varepsilon\}$

$Lin(\{M_4, M_5\})$ does <u>not</u> fulfill AB$'$, e.g.,

$1!2(a)\ 2?1(a) \in pref(Lin(\ldots))$ and is well-formed and

$(1!2(a)\ 2?1(a))\restriction 1 = 1!2(a)$ M_4

$(1!2(a)\ 2?1(a))\restriction 2 = 2?1(a)$ M_4

$(1!2(a)\ 2?1(a))\restriction 3 = \varepsilon$ M_5

$(1!2(a)\ 2?1(a))\restriction 4 = \varepsilon$ M_5

but $1!2(a)\ 2?1(a) \notin Lin(\{M_4, M_5\})$

CHARACTERIZING SAFE REALIZABILITY

<u>Theorem</u> [Alur, Etessami & Yannakakis '00]

$L \subseteq Act^*$ is safely realizable iff

L only contains well-formed words and

L fulfills AB' and ABS.

<u>Proof</u> : on black board

<u>Theorem</u>

The decision problem " is a given set of MSCs safely realizable " is in PTIME

For $\{M_1, \dots, M_k\}$ over $|P| = n$ and $|E| = m$:

- checking ABS takes $\mathcal{O}(k^2 n + mn)$ time
- checking AB' takes $\mathcal{O}(k^2 n + m)$ time

<u>Recall</u> : checking realizability is coNP-complete