Software Modeling and Verification
Lehrstuhl für Informatik 2
RWTH Aachen University

Prof. Dr. Ir. J.-P. Katoen
C. Kern

Foundations of the UML

Winter Term 07/08

– Lecture number 5 Realizability –

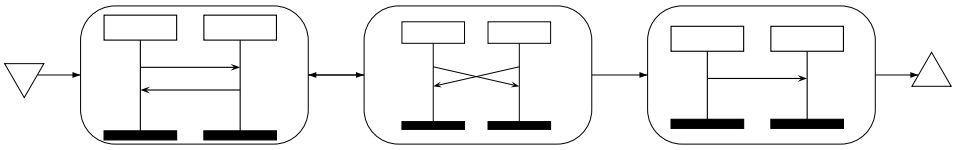
(Date (26.11.2007))
summarized by *Andrea Hutter* and *Peter Schumacher*

1 Aim

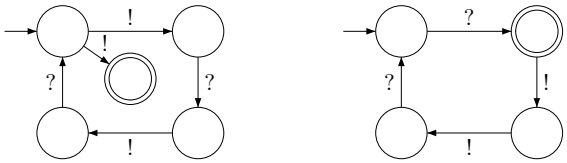
We already know that

- MSCs impose a global view of a system and
- MPA is a set of finite-state machines and a collection of local system views.

The aim of this lecture is to get from a high-level specification (MSC)



to an implementation model (MPA).



So we want to obtain a characterization of MSCs or equivalently, their linearizations for which an equivalent MPA exist. For simplificity, we consider the first case without synchronization messages, i.e. $\mid \mathbb{D} \mid = 1$. This is known as simple realizability.

First we introduce a new perception.

2 Traces

2.1 Definition "well-formed"‘

$Act = \bigcup_{p \in P} Act_p$ 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 $v \in pref(w)$:
$$\underbrace{\sum_{a \in \mathbb{C}} |v|_{p!q(a)}}_{\#send:p \to q} - \underbrace{\sum_{a \in \mathbb{C}} |v|_{q?p(a)}}_{\#receipts:q \leftarrow p} \geq 0$$

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

2.2 Definition Traces

Let $e_1, e_2, ..., e_n \in Lin(M)$ for MSC M
we call $l(e_1)\, l(e_2) ... \, l(e_n)$ a *trace* of M

Lemma 2.1 *$w \in Traces(M)$ iff w is well-formed*

Proof 2.1

"⇒": *let $w \in Traces(M)$. Then in every prefix v of w, $\sum_a |v|_{p!q(a)} \geq \sum_a |v|_{q?p(a)}$ for every $(p, q) \in Ch$. As M is FiFo, w is FiFo.*

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

3 Realizability

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

Equivalently

- MSC *M* is realizable if $Lin(M) = Lin(A)$ for some MPA A
- $\{M_1, ..., M_k\}$ is realizable if $\bigcup_{i=1}^{k} Lin(M_i) = Lin(A)$ for some MPA A
- MSG *G* is realizable if $Lin(G) = Lin(A)$ for some MPA A

3.1 Impossible to realize

Consider the following two MSCs :
M1:

M2:

They increase the volume of U and S by one entry (M1) or double their volume (M2).
The following scenario is implied by the ability of the process instances (*p1* and *p2*) to independently act as M1 or M2.

So: $\{M_1, M_2\}$ is **not** realizable

3.2 Closure property (AB)

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

for every well-formed word $w \in Act^*$. $(\forall p \in P \,.\exists v \in L \,.w \restriction_p = v \restriction_p)$ implies $w \in L$

Here $\restriction_p$ means *projection* on process p:

$\varepsilon \restriction_p = \varepsilon$

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

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:

$w = p_1!u(*2)u?p_1(*2)p_2!s(+1)s?p_2(+1) \notin Lin(\{M_1, M_2\})$ but:

$w \restriction_{p_1} = p_1!u(*2)$ and $w \restriction_u = u?p_1(*2)$ are consistent with $Lin(M_2)$

$w \restriction_{p_2}$ and $w \restriction_s$ are consistent with $Lin(M_1)$

Thus $Lin(M1, M2)$ does not fulfill property AB.

3.3 Characterizing realizability

Theorem 3.1 (Alur, Etessami, Yannakakis '00) *$L \subseteq Act^*$ is realizable iff L only contains well-formed words and L fulfills AB.*

Proof 3.1

"⇒": Assume L is realizable. Then there exists an MPA A with $L = Lin(A)$. Take $w \in Lin(A)$. Since $w \in Lin(A)$, w ends in a configuration in which all channels are empty. In addition for any $v \in pref(w)$, for any channel (p, q), the numbers of sends $(p, q) \geq$ the numbers of receives (q, p). As all channels in A are FIFO, it follows w is FIFO, thus w is well-formed. Remains to prove L satisfies AB. Let $w \in Act^*$, well-formed and assume for any $p \in P$, there exists $v^P \in L$ such that $w \restriction_p = v^P \restriction_p$. We show that $w \in L$. Consider an accepting run of A on v^P, in particular consider the local state of p in this run, as well as local transition in Δ_p. Since $w \restriction_p = v^P \restriction_p$, these local transitions are also possible in $w \restriction_p$. It is not difficult to see that the runs of the local automata can be combined into an accepting run of MPA A on w. So L satisfies AB.

"⇐": Assume L satisfies AB and L only contains well-formed words. Let A_p be an automaton that accepts $\{w \restriction_p | \ w \in L\}$. We show that for MPA $A = ((A_p)_{p \in P}, s_{init}, F)$ we have $Lin(A) = L$.

"⊇" Let $w \in L$. By construction of MPA A, $Lin(A) = \{w \restriction_p | \ w \in L\}$. But then $w \in Lin(A)$.

"⊆" Let $w \in Lin(A)$. Then $w \restriction_p \in Lin(A)$ for any $p \in P$. Since L satisfies AB, it follows $w \in L$.

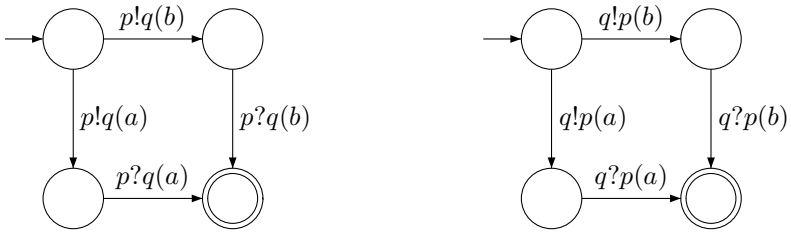
Theorem 3.2 *The decision problem "is a given set of MSCs realizable" is CoNP-complete.*

4 Safe Realizability

It is possible that a set of MSCs is realizable but only by an MPA that may have deadlocks.

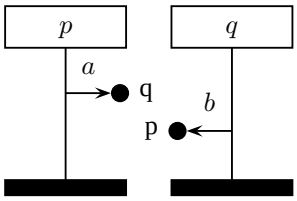
"processes p and q have to agree on a or b"

Realization:



process p process q

Possible behavior:



p!q(a) q!p(b) $\lightning$ $deadlock$!

4.1 Definition "deadlockfree"

An MPA A is deadlockfree if from every configuration γ reachable from γ_0, a final configuration $\gamma' \in \{\eta_\varepsilon\}$ is reachable.

4.2 Definition Safe Realizability

- An MSC M is safely realizable whenever M = L(A) for some deadlockfree MPA A.
- A set of MSCs $\{M_1, \ldots, M_k\}$ is safely realizable if $\{M_1, \ldots, M_k\} = L(A)$ for some deadlockfree MPA A.
- MSG G is safely realizable if $L(G) = L(A)$ for some deadlockfree MPA A.

Consider: $L \subseteq Act^*$ is safely realizable if $Lin(G) = L$ for some deadlockfree MPA A.
Note:$realizability \not\Rightarrow safe realizability$

4.3 Closure Property: ABS-Property part 1

Consider $pref(L) = \{w \mid \exists u : wu \in L\}$ is the set of prefixes of *L*.
$L \subseteq Act^*$ has a ABS property if for every prefix $w \in Act^*$ of a well-formed word:
($\forall p \in P : \exists v \in pref(L) : w \restriction_p = v \restriction_p) \longrightarrow w \in pref(L)$

Example:

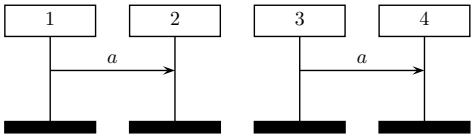
M_1 M_2

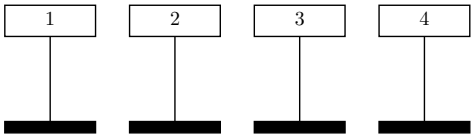
$L = (Lin\{M_1, M_2\})$ fullfills AB, but <u>not</u> ABS

$L = \{p!q(a)\ q!p(a)\ p?q(a)\ q?p(a),$
$p!q(a)\ q!p(a)\ q?p(a)\ p?q(a),$
$q!p(a)\ p!q(a)\ p?q(a)\ q?p(a),$
$q!p(a)\ p!q(a)\ q?p(a)\ p?q(a),$
$\ldots$dito for $M_2 \ldots$ }

Take $w = p!q(a)\ q!p(b)$
w is a prefix of a well-formed word,
and p!q(a) $\in$ pref(L), (p!q(a)) $\restriction p$ = w $\restriction p$
and q!p(b) $\in$ pref(L), (q!p(b)) $\restriction p$ = w $\restriction p$
} w $\notin$ pref(L)

ABS is insufficent to characterize safe realizability





M$_4$ M_5 (= empty)

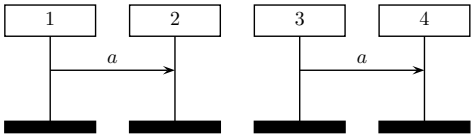
$Lin(\{M_4, M_5\}) = \{1!2(a)\ 2?1(a)\ 3!4(a)\ 4?3(a),$
$1!2(a)\ 3!4(a)\ 2?1(a)\ 4?3(a), \ldots$
$3!4(a)\ 4?3(a)\ 1!2(a)\ 2?1(a), \varepsilon\}$

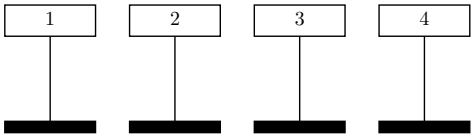
$Lin(\{M_4, M_5\})$ possesses property ABS but a safe realization should allow to accept
1!2(a) 2?1(a) only (3,4 decides to behave as M_5)
or 3!4(a) 4?3(a) only (1,2 decides to behave as M_5)

So: ABS is insufficient to characterize safe realizability

4.4 Closure Poperty: ABS-Property part 2

Now, in addition to ABS adapt AB as follows: $L \subseteq Act^*$ has property AB' if for every well-formed $w \in pref(L)$:
$(\forall p \in P : \exists v \in L : w \restriction_p = v \restriction_p) \longrightarrow w \in L$
(the last formula is only imposed on prefixes of L, not on arbitrary action sequences.)





M$_4$ M_5

$Lin(\{M_4, M_5\}) = \{1!2(a)\ 3!4(a)\ 2?1(a)\ 4?3(a),$
$3!4(a)\ 1!2(a)\ 4?3(a)\ 2?1(a), \varepsilon\}$

$Lin(\{M_4, M_5\})$ does not fulfill AB', e.g., $1!2(a)\ 2?1(a) \in$ ***pref(Lin(. . .))*** and is well-formed and

$(1!2(a)\ 2?1(a)) \restriction 1 = 1!2\ (a)$ $\quad M_4$
$(1!2(a)\ 2?1(a)) \restriction 2 = 2?1\ (a)$ $\quad M_4$
$(1!2(a)\ 2?1(a)) \restriction 3 = \varepsilon$ $\quad M_5$
$(1!2(a)\ 2?1(a)) \restriction 3 = \varepsilon$ $\quad M_5$

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

4.5 Characterizing Safe Realizability

Realizability can be characterized by two theorems:

(1) **Theorem 4.1 (Alur, Etessami, Yannakakis '00)** *$L \subseteq Act^*$ is safely realizable iff L only contains well-formed words and L fulfills AB' and ABS.*

Proof 4.1 *skipped, is simply like the proof of "Characterizing Realizability".*

(2) **Theorem 4.2** *The decision problem "'is given set of MSCs safely realizable"' is in PTIME. For $\{M_1, \ldots, M_k\}$ over $\mid P \mid = n$ and $\mid E \mid = m$:*

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