Software Modeling and Verification
Lehrstuhl für Informatik 2
RWTH Aachen University

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

Foundations of the UML

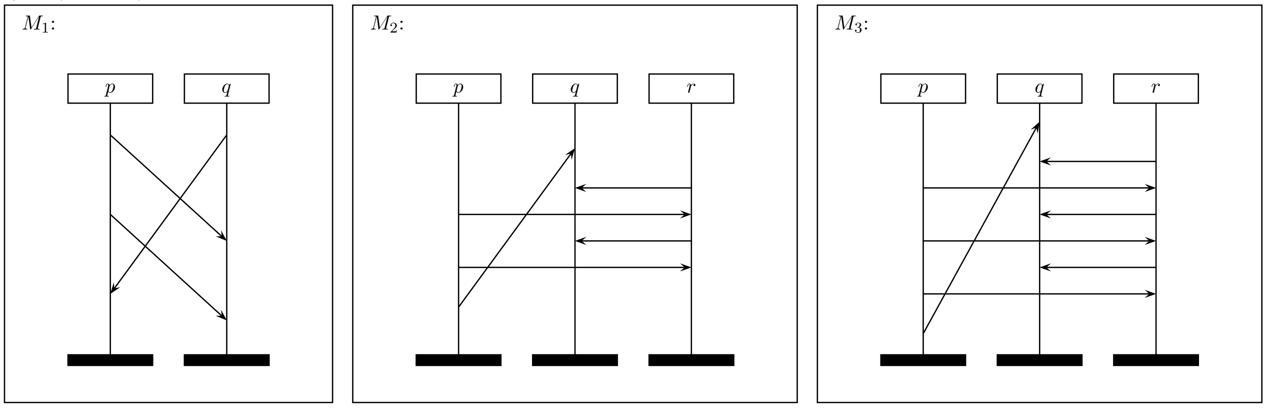
Winter Term 07/08

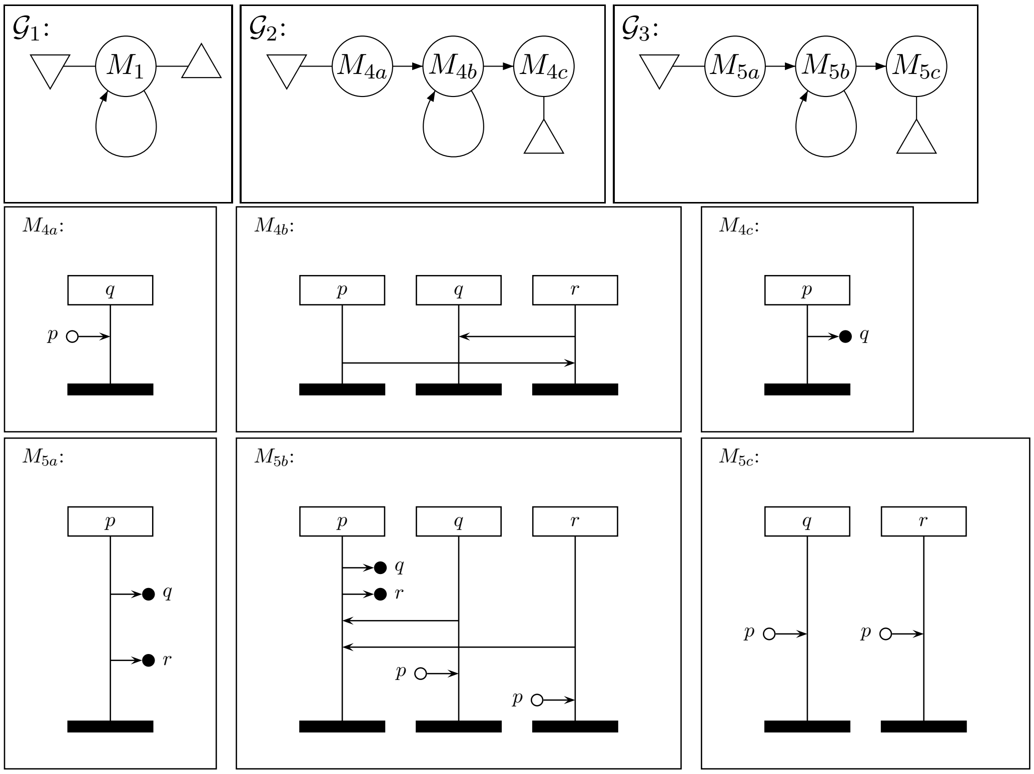
– Assignment 4 –

Hand in until December 19th before the exercise class.

Exercise 1 (10 points)

Determine for each of the following MSCs (M_1, M_2, M_3) and MSGs ($\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3$), respectively, if they are existentially ($\exists$-) or universally ($\forall$-) bounded. In case an MSC or MSG is $\exists/\forall$-bounded, determine the smallest B such that the MSC or MSG, respectively, is $\exists/\forall$-B-bounded and argue why it cannot be $\exists/\forall$-$(B-1)$-bounded.

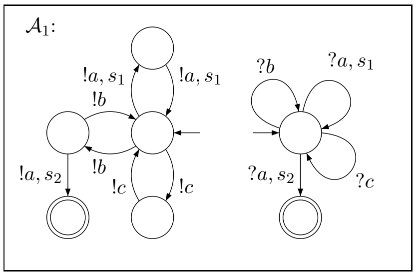


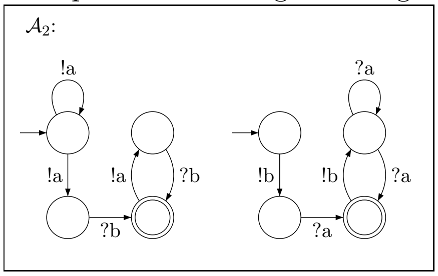


Note that, in contrast to the definition in the lecture, in $\mathcal{G}_2$ we allow a node containing a receive event to occur before the node of the corresponding send event.

Exercise 2 (10 points)

Let the following two MPA $\mathcal{A}_1$ and $\mathcal{A}_2$ be given: (The two MPA only contain 2 local automata, each. For readability purposes the sending and receiving processes were omitted. Thus, for example, executing action $!a$ in one local automaton corresponds to sending a message a to the other local automaton)





Answer the following questions for $i \in \{1, 2\}$ and give a detailed justification.

a) Is the MPA $\mathcal{A}_i$ is strongly-B-bounded? (if the answer is *yes* find the smallest such B)

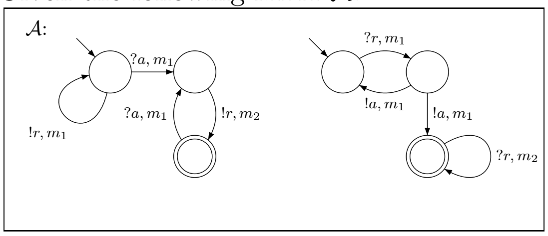
b) Is the MPA $\mathcal{A}_i$ a product MPA?

c) Is the MPA $\mathcal{A}_i$ deterministic?

d) Is the MPA $\mathcal{A}_i$ deadlock-free?

Exercise 3 (10 points)

Given the following MPA $\mathcal{A}$:



Show that $\mathcal{A}$ is not safe by finding a configuration that is reachable from the initial configuration γ_0 of $\mathcal{A}$ and from which a final configuration γ_e cannot be obtained. Justify your answer by indicating the sequence of configurations leading from the initial configuration γ_0 to the deadlock configuration γ_d and arguing why a final configuration is not reachable from γ_d.

Exercise 4 (10 points)

Let ABS' be the following property of a language L:

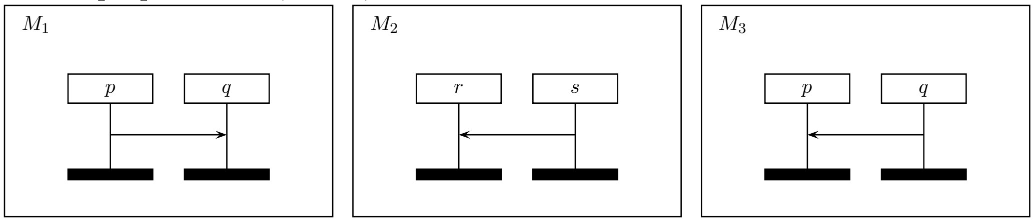
A language $L \subseteq Act^*$ fulfills property ABS' if for all $v, w \in pref(L)$ and all processes $p \in \mathcal{P}$: if $\big[v \upharpoonright p = w \upharpoonright p$ and $vx \in pref(L)$ for $x \in Act_p$ and wx is prefix of a well-formed word$\big]$ then $wx \in pref(L)$.

Prove the following statement:

A language L fulfills property $ABS \iff L$ fulfills property ABS'.

Exercise 5 (10 points)

Check (i.e., by using the definitions) for language L_1 whether or not property AB and for L_2 whether or not the properties AB, ABS, AB' and ABS' hold:



- $L_1 = \{w \mid w \in Traces(\{M_1, M_2\})\}$
- $L_2 = \{w \mid w \in Traces(\{M_1, M_3\})\}$

Which of the languages is realizable or even safely realizable? Justify your answers.