Software Modeling and Verification
Lehrstuhl für Informatik 2
RWTH Aachen University

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

Foundations of the UML

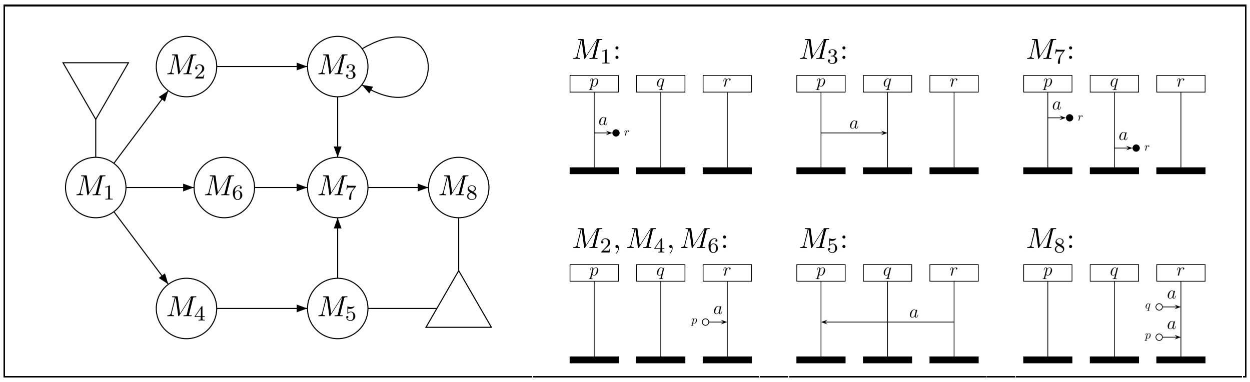
Winter Term 07/08

– Assignment 3 –

Hand in until December 5th before the exercise class.

Exercise 1 (10 points)

a) Given the definition of *locally safe* (cf. Definition 1): is the following CMSG locally safe? Justify your answer in detail by calculating the sets $V^1, V^2, \prod$ and arguing about $M(\pi)$, $\pi \in \prod$.



b) Prove the following statement:

If a CMSG $\mathcal{G}$ is *locally safe* then $\mathcal{G}$ is finitely generated (cf. Definition 2) and there exists an MSG $\mathcal{G}'$, such that $L(\mathcal{G}') = L(\mathcal{G})$.

c) Can the statement from b) be used to create an MSG $\mathcal{G}'$ for the CMSG from a)? If the answer is `yes`, write down $\mathcal{G}'$, if the answer is `no` justify your answer.

Exercise 2 (10 points)

Consider the following decision problem $\overline{\textbf{\textit{FIFO}}}$:

Input: a CMSG $\mathcal{G}$
Output: Yes, if $\mathcal{G}$ is not FIFO and no, otherwise

Prove that $\overline{\textbf{\textit{FIFO}}}$ is undecidable (do a PCP reduction similar to the proof in the lecture and try to ensure that the constructed CMSG fulfills a local-choice property).

Exercise 3 (10 points)

Given the following specification $\mathcal{S}$ where a producer p and a consumer c are the acting units:

- The producer p starts sending messages with content 0 (one bit) to the consumer c until he receives an acknowledgement message a from the consumer. In that case the bit is swapped to 1 and p starts sending messages with content 1 to c until the next a is received. Then again the bit is inverted and the procedure can continue as before.

- The consumer process c, however, starts by receiving at least one 0. After that he may receive more 0s until finally he sends an a to p. After this acknowledgement the remaining 0s in the buffer (p, c) have to be received. Then process c starts receiving 1s (if p sent at least one). Having received at least one message with content 1, c may send an a after any of the successing 1s. Having sent the a, the remaining 1s have to be processed before another round of receiving 0s may start.
- The system may accept directly after any a that is received by process p (as long as the empty-buffer condition is fulfilled).

Question: Find an MPA implementation for $\mathcal{S}$.

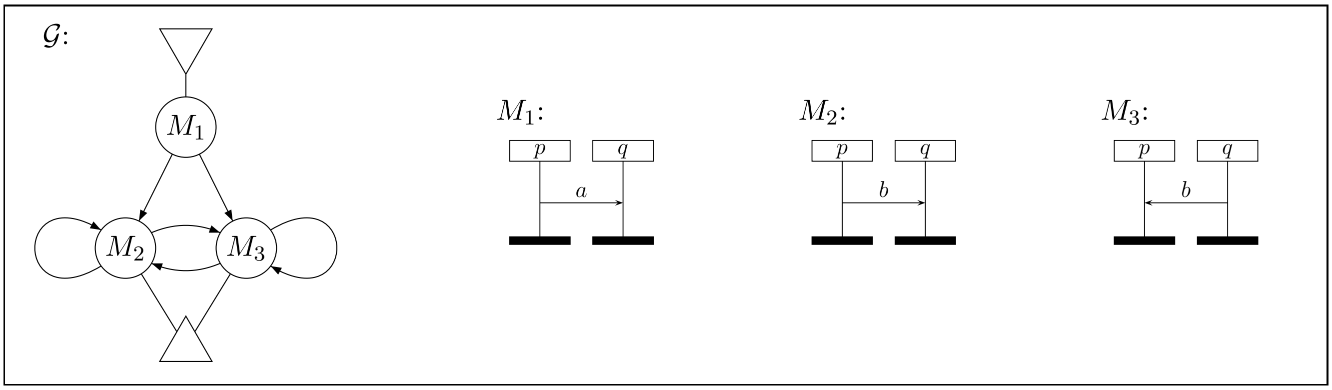
Exercise 4 (10 points)

Show that the following problem is decidable:

Input: safe MPA $\mathcal{A}$ and $B \geq 1$. Question: Is $\mathcal{A}$ $\forall B$-bounded?

Exercise 5 (10 points)

Consider the following MSG $\mathcal{G}$.



Construct an MPA $\mathcal{A}$ which exactly recognizes $L(\mathcal{G})$ (i.e., where $L(\mathcal{A}) = L(\mathcal{G})$).

Note: Pay attention to avoid non-local-choice which would result in unwanted behavior such as deadlocks.

Definition 1: Let the following sets be given for a CMSG $\mathcal{G} = \langle V, \rightarrow, v_0, F, \lambda \rangle$

- $V^1 := \{v_0\} \cup \{v \in V \mid |Succ_{\mathcal{G}}(v)| > 1\} \cup \{v \in F \mid |Succ_{\mathcal{G}}(v)| > 0\}$
- $V^2 := Pred_{\mathcal{G}}(V^1 \setminus \{v_0\}) \cup F$
- $\prod := \{\pi \text{ is path in } \mathcal{G} \mid \pi = v_1, \ldots, v_n, n \in \mathbb{N}, v_1 \in V^1, v_n \in V^2 \setminus V^1, v_i \notin V^2 \text{ for } 1 < i < n\} \cup \{v \mid v \in V^1 \cap V^2\}$

A compositional Message Sequence Graph $\mathcal{G}$ is called *locally safe* if for every path $\pi \in \prod$: $M(\pi) \in \mathbb{M}$ (i.e., if $M(\pi)$ is an MSC).

For a graph $\mathcal{G} = \langle V, \rightarrow \rangle$ and a node $v \in V$:

- $Succ_{\mathcal{G}}(v) := \{(v, w) \in \rightarrow \mid w \in V\}$
- $Pred_{\mathcal{G}}(v) := \{(w, v) \in \rightarrow \mid w \in V\}$ and $Pred_{\mathcal{G}}(V) = \bigcup_{v \in V} Pred_{\mathcal{G}}(v)$

Definition 2: A CMSG $\mathcal{G}$ is called *finitely generated* if there is a finite set $\mathcal{B} = \{M_1, \ldots, M_k\}$ of MSCs such that for any $M \in L(\mathcal{G})$ there are $n \in \mathbb{N}$ and indices $i_1, \ldots, i_n \in \{1, \ldots, k\}$ such that $M = \prod_{j=1}^{n} M_{i_j}$.