Aalto University, Department of Information and Computer Science Antti Siirtola

T-79.4302 Parallel and Distributed Systems
Examination, 20 May 2014

Write down on every answer sheet: the name of the course, the course code, the date, your name, your student id, and your signature.

Calculators are NOT allowed.

To pass the course, you also need to have passed the quizes and home assignments in Autumn 2013.

Assignment 1. Consider the following Promela model.

```
mtype = {msg,ack};
chan ch = [1] of {mtype,bit};

active proctype P1()
{
    bit i = 0;
    do
    :: ch!msg(i)
    :: atomic{ch?ack(0) -> i = 1}
    :: atomic{ch?ack(1) -> i = 0}
    od
}

active proctype P2()
{
    do
    :: ch?msg(0) -> ch!ack(0)
    :: ch?msg(0)
    :: ch?msg(1) -> ch!ack(1)
    :: ch?msg(1)
    od
}
```

(a) What pieces of data are needed to identify a single state of this model? Design a compact state vector representation for the states of the model. (2pt)

(b) Construct the reachability graph of the model and list all reachable deadlock states. (6pt)

(c) Present and describe an algorithm that inputs a Kripke structure $M = (S, s^0, R, L)$ and outputs "correct" if there is no reachable state $s \in S$ such that $err \in L(s)$. Otherwise, the algorithm outputs an execution of M that leads to a state $s \in S$ such that $err \in L(s)$. (4pt)

Assignment 2.

(a) Give a Kripke structure M such that the following holds:

(1) $M \models \mathbf{G}\,\mathbf{F}\,(a \land \mathbf{X}\,a)$ and $M \models (\mathbf{G}\,\mathbf{F}\,a) \rightarrow \mathbf{G}\,\mathbf{F}\,(\neg a)$ (2pt)

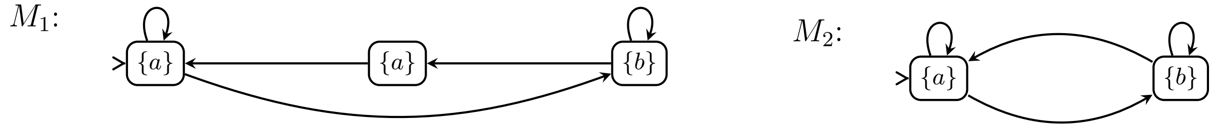
(2) $M \models \mathbf{G}\,(a \rightarrow \mathbf{Y}\,\mathbf{O}\,b)$ and $M \not\models \mathbf{G}\,\mathbf{H}\,(\neg a)$ (2pt)

(b) Formalise the following properties in LTL or as a past safety formula:

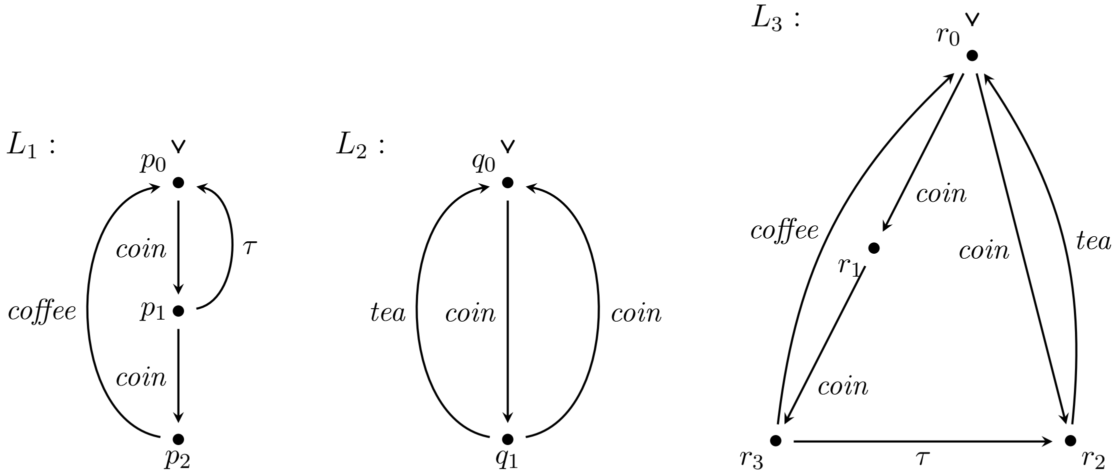
(1) "If a message is sent, then it is eventually acknowledged and no message is sent before the acknowledgement is received". (2pt)

(2) "If there is an acknowledgement, then a message has been sent in the past". (2pt)

(c) Devise an LTL formula that is satisfied by the Kripke structure M_1 but not by the Kripke structure M_2. Devise also a past safety formula that is satisfied by M_1 but not by M_2. (4pt)



Assignment 3. Consider the following LTSs L_1, L_2, L_3 over alphabets $\Sigma_1 = \{coin, coffee\}$, $\Sigma_2 = \{coin, tea\}$, $\Sigma_3 = \{coin, coffee, tea\}$, respectively.



(a) Construct the reachable part of the parallel composition (asynchronous product) $L_{12} := L_1 \parallel L_2$. (3pt)

(b) Construct a deterministic FSA A_3 that recognizes the language $traces(L_3)$. (3pt)

(c) By complementing A_3, construct a deterministic FSA $\overline{A}_3$ that recognizes the language $\Sigma^* \setminus traces(L_3)$ (3pt)

(d) Consider $\overline{A}_3$ as an LTS $\overline{L}_3$ and construct the parallel composition $\overline{L}_3 \parallel L_{12}$. By analysing the parallel composition $\overline{L}_3 \parallel L_{12}$, decide whether $(L_1 \parallel L_2) \leq_{tr} L_3$? Explain how you arrived at the answer. (3pt)

Assignment 4.

(a) Describe the flow of a verification process, i.e., what are the typical steps that you take to verify that, e.g., the design of a network protocol meets its specification. (4pt)

(b) Explain the reasons behind the state explosion problem? What can you do to tackle the state explosion problem? Name and describe at least two techniques. (4pt)

(c) What kinds of concurrency flaws there are? What are the major benefits of verification methods, e.g., model checking, over traditional testing-based approaches? (4pt)