# Model Checking - Exercise Sheet 1

1. We did modeling of the experiment in which there were two jars, where big jar has capacity 5 and small jar has capacity 3. Initially, jars were both empty. It was possible to either (i) empty a jar (ii) fill a jar, or (iii) transfer liquid from one jar to another until either the former one is empty or the latter one is full. You had defined an FDS for this system in which the set of variables is $\{big, small\}$ where $big$ takes values from $\{0..5\}$ and small takes values from $\{0..3\}$. Answer the following with respect to this FDS.

   - What is the state space (that is, the set of states) of this system? List down three different states of this system, where $big \neq 0 \neq small$ and $big \neq 5$ and $small \neq 3$.
   - What is the initial state of this system? List down three distinct states which are reachable in one step from the initial state. List down all states which are reachable in at most two steps from the initial state.
   - Consider the logic formula that you wrote corresponding to the action "empty the big jar". Give three different state transitions of the underlying transition system which satisfies this formula. How many different state transitions are possible corresponding to this formula?

2. Consider your modeling for Peterson's algorithm for two asynchronous processes. The variables used were the program counters of the two processes $s_0$ and $s_1$, the shared variables turn, intr0 and intr1.

   - What is the state space of the (joint) system?
   - Give two states of the system such that there is no one step transition from the former to the latter, but there is a two step transition from the former to the latter. Justify your answer.

3. In this question, we will redo modeling of Perterson's algorithm more abstractly, where the individual system's program counters $s_0$ and $s_1$ takes values from the set $\{ready, interested, attempting, inCrit\}$ only and the shared variables are as before. You have to do this without changing the underlying meaning of the transitions allowed and disallowed. You may assume that initially, both systems are in ready state, and values of all the three shared variables are 0. Consider the joint system obtained by asynchronous composition of the two systems.

   - Give the state space of the new joint system.
   - For this system, give the formula corresponding to the initial state.
   - Give the formula corresponding to the transition relation of the individual systems.
   - Give the formula corresponding to the transition relation of the joint system.
   - Suppose Crit0 represents the atomic proposition that $s0 = inCrit$ and Crit1 represents the atomic proposition that $s1 = inCrit$. Let $\pi$ be any run of the system. Give an LTL formula $\phi$ (using atomic propositions Crit0 and Crit1 and operators allowed in LTL) which represents the property that $\pi \models \phi$ precisely means that both processes cannot be in their critical section simultaneously in any state of $\pi$.

- Suppose Intrested0 represents the atomic proposition that represents $s0 = \mathit{interested}$ and Crit0 is as in the previous part. Give an LTL formula $\psi$ (using atomic propositions Crit0 and Interested0 and operators allowed in LTL) which represents the property that a run $\pi \models \phi$ precisely means that if $\pi$ has a state where Intrested0 holds, then there is a later state in $\pi$ where Crit0 holds.

4. For the modeling of solving critical section problem using semaphores that we did in class, do a state space reduction as we did in previous question.

5. Let $\phi = (p \to q) \to r$. Give two different models $\tau_1$ and $\tau_2$ for $\phi$ in such a way that $\tau_1 \models \phi$ and $\tau_2 \not\models \phi$. Compute $\mathcal{M}(\phi)$ (restricting the variable set to $\{p, q, r\}$).

6. For each of the following pairs of formula, check whether (a) $\phi_2$ is a semantic consequence of $\phi_1$ not (b) $\phi_1$ is a semantic consequence of $\phi_2$ or not (c) $\phi_1$ and $\phi_2$ are semantically equivalent or not. Justify your answers.

   - $\phi_1 = (p \to q) \wedge q$, $\phi_2 = q$
   - $\phi_1 = (p \to q) \wedge q$, $\phi_2 = p$
   - $\phi_1 = (p \to q) \wedge p$, $\phi_2 = q$
   - $\phi_1 = p \to q$, $\phi_2 = q \to p$
   - $\phi_1 = p \to q$, $\phi_2 = \neg q \to \neg p$

7. Let $\psi_1 = \phi_1 \vee p$ and $\psi_2 = \phi_2 \vee \neg p$ be two propositional formulas where $p$ is a proposition. Let $\psi = \phi_1 \vee \phi_2$. Let $M$ be an arbitrary model that satisfies both $\psi_1$ and $\psi_2$. Then, using the semantics of propositional logic we defined, show that $M$ also satisfies $\psi$.

8. Consider a predicate logic vocabulary consisting of ($\mathcal{F} = \{f\}$, $\mathcal{P} = \{P\}$) where $f$ is a unary function symbol, and $P$ is a binary predicate symbol. Consider the formula $\phi := \exists x \forall y P(x, f(y))$. Give two models $M_1$ and $M_2$ such that $M_1 \models \phi$ and $M_2 \not\models \phi$. In each case, take the underlying world of values $A = \{1, 2\}$.

9. Let $\phi = G(p \to q)$ and $\psi = FG(p \to q)$. Define a model $\mathcal{K}$ (which will be a Kripke structure, with appropriate transitions and labeling function) which satisfies one of these formulas and not the other. Justify your answer.

10. Give an LTL formula $\phi$ such that for an arbitrary Kripke structure $K$ whose set of atomic propositions includes $p$, $K \models \phi$ if and only if in every run of $K$, there is exactly one state which satisfies $p$.