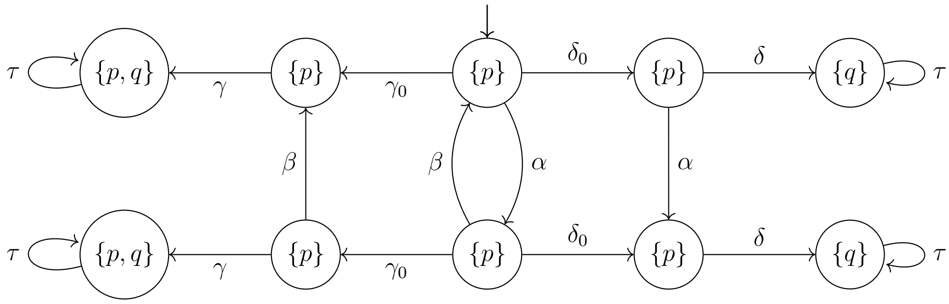
Technische Universität München (I7)
J. Křetínský / M. Azeem / K. Grover

Summer Semester 2022
21.06.2022

Model Checking – Exercise sheet 7

Exercise 7.1

Consider the transition system TS depicted below. Show that the ample set conditions (C0)-(C3) do not allow for any state reduction, although there is a smaller subsystem $\hat{TS}$ that is stutter equivalent to TS.



Exercise 7.2

Consider the following Promela model

```
byte g;

active proctype m() {
byte x;
m0: x++;
m1: x++;
m2: g = x;
}

active proctype n() {
byte y;
n0: y++;
n1: y++;
n2: atomic { (g>0) -> g = g-y }
}

active proctype p() {
p0: atomic { (g>0) -> g-- }
}
```

and the following properties:

a) The value of g will eventually become one.

b) The process `n` cannot finish before the process `m` reaches `m1`.

For each property, define a labeled Kripke structure with actions extracted from program statements. Determine the independence relation and the invisibility set, and construct a reduced Kripke structure using the ample sets method.

Exercise 7.3

Which of the following equivalences for CTL^* are correct? Provide a proof or a counterexample.

(a) $\mathbf{AXAG}\ \phi \equiv \mathbf{AXG}\ \phi$

(b) $\mathbf{EXEG}\ \phi \equiv \mathbf{EXG}\ \phi$

(c) $\mathbf{A}\ (\phi \wedge \psi) \equiv \mathbf{A}\ \phi \wedge \mathbf{A}\ \psi$

(d) $\mathbf{E}\ (\phi \wedge \psi) \equiv \mathbf{E}\ \phi \wedge \mathbf{E}\ \psi$

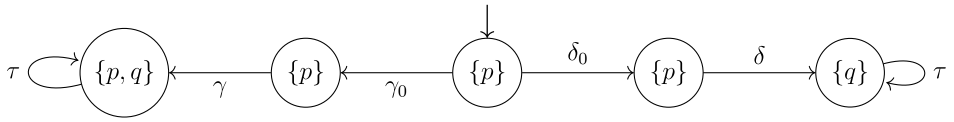
Solution 7.1

Dependent set: $\{(\alpha,\gamma_0),(\gamma_0,\alpha),(\beta,\delta_0),(\delta_0,\alpha),(\gamma_0,\delta_0),(\delta_0,\gamma_0),(\beta,\gamma),(\gamma,\beta),(\alpha,\delta),(\delta,\alpha)\}$
Invisible set: $\{\alpha,\beta,\gamma_0,\delta_0\}$

We shall show that it's not possible to reduce any actions for the initial state, similar arguments can be given for the other states.

Since all actions are invisible, condition (C2) does not impose any restrictions. But since γ_0 and δ_0 are independent, (C1) says that either both of them would be the $red()$ set or neither of them. Similarly, either both α and γ_0 would be in the $red()$ set or neither of them. This combined with $C0$ conditions gives us that all three of them would have to be included in the $red()$ set.

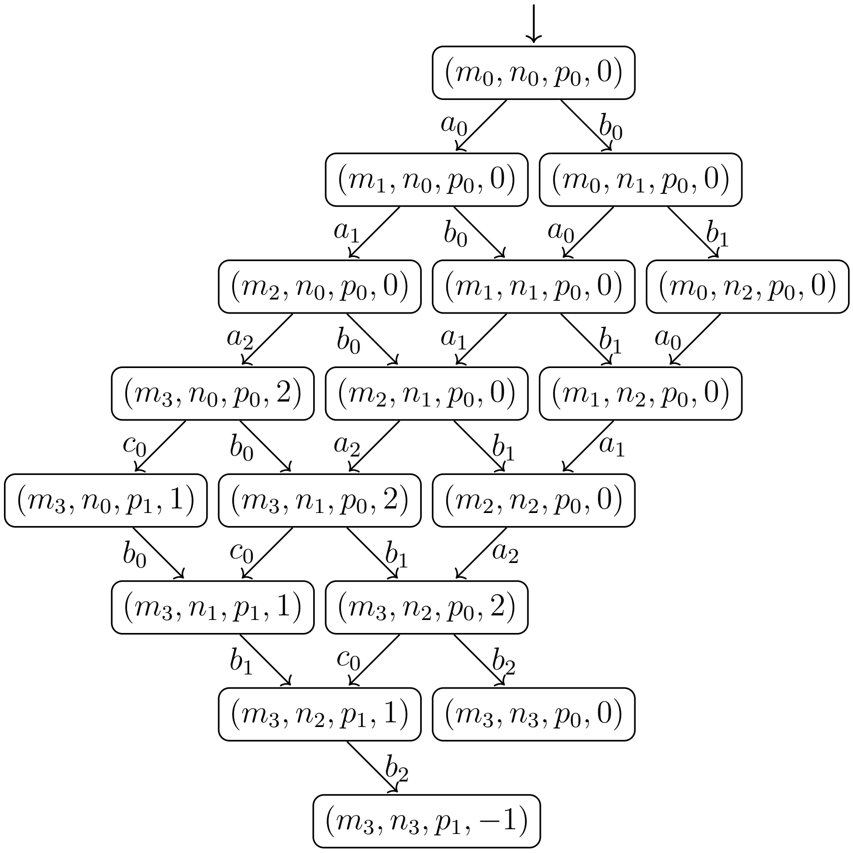
Smaller subsystem that is stutter equivalent to the TS:



Solution 7.2

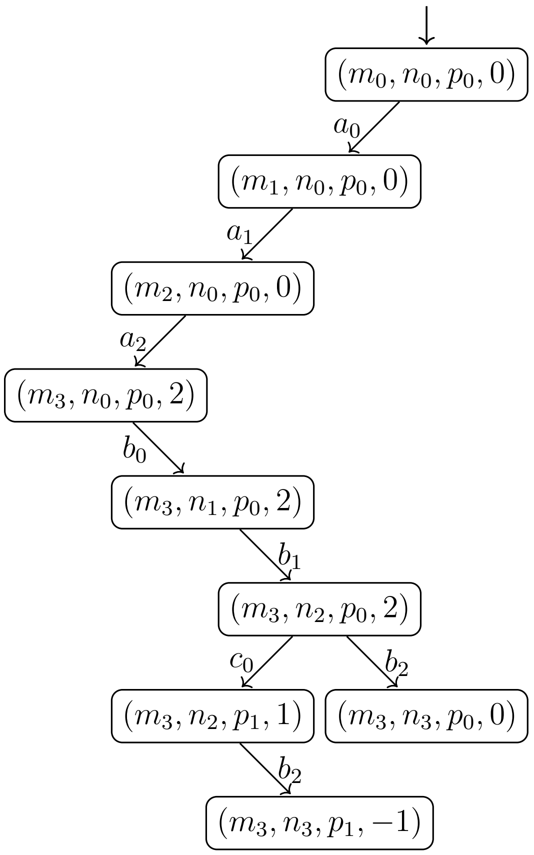
We define actions $a_0, a_1, a_2, b_0, b_1, b_2$, and c_0 for statements in `m`, `n`, and `p`, respectively. Each state in the Kripke structure is a tuple of program locations and a valuation of `g`. Notice that it is not necessary to explicitly models valuations of `x` and `y` as they are implicitly defined by program locations of `m` and `n`.

For each property, we construct a labeled Kripke structure $\mathcal{K} = (S, A, \rightarrow, r, AP, \nu)$, where and S, A, $\rightarrow$, and r are as follows:

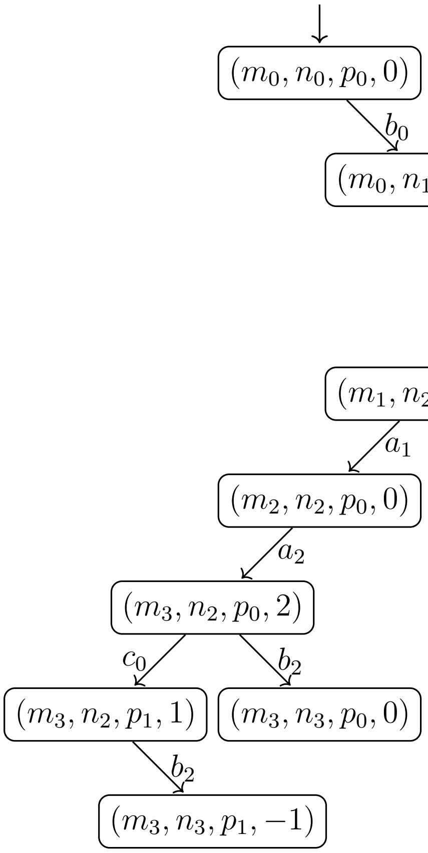

$(m_0, n_0, p_0, 0)$
a_0
b_0
$(m_1, n_0, p_0, 0)$
$(m_0, n_1, p_0, 0)$
a_1
b_0
a_0
b_1
$(m_2, n_0, p_0, 0)$
$(m_1, n_1, p_0, 0)$
$(m_0, n_2, p_0, 0)$
a_2
b_0
a_1
b_1
a_0
$(m_3, n_0, p_0, 2)$
$(m_2, n_1, p_0, 0)$
$(m_1, n_2, p_0, 0)$
c_0
b_0
a_2
b_1
a_1
$(m_3, n_0, p_1, 1)$
$(m_3, n_1, p_0, 2)$
$(m_2, n_2, p_0, 0)$
b_0
c_0
b_1
a_2
$(m_3, n_1, p_1, 1)$
$(m_3, n_2, p_0, 2)$
b_1
c_0
b_2
$(m_3, n_2, p_1, 1)$
$(m_3, n_3, p_0, 0)$
b_2
$(m_3, n_3, p_1, -1)$

The independence relation $I = (A \times A \setminus Id) \setminus \{(b_2, c_0), (c_0, b_2)\}$.
Next, we consider each property individually.

a) The corresponding LTL formula is $\mathbf{F}(\mathtt{g} == 1)$, where $AP_a = \{\mathtt{g} == 1\}$. So, $\nu_a(s) = \{\mathtt{g} == 1\}$ iff the valuation of $\mathtt{g}$ in the state s is 1, and as a result, $U = A \setminus \{b_2, c_0\}$. A possible reduced Kripke structure is as follows:



b) The corresponding LTL formula is $m_1 \; \mathbf{R} \; \neg n_3$, where $AP_b = \{m_1, n_3\}$. $\nu_b(s) = \{m_1\}$ (resp. $\{n_3\}$) iff the s contains m_1 (resp. $\{n_3\}$). As a result, $U = A \setminus \{a_0, a_1, b_2\}$. A possible reduced Kripke structure is as follows:



Solution 7.3

Note that the solutions discussed during the tutorial for this exercise are wrong.

(a) Yes, if a tree T satisfies $\mathbf{AXAG}\phi$ then, every path in the tree is of the form $\pi = a_1, a_2, a_3 \ldots$ where everything from a_2 onwards satisfies ϕ which is equivalent to saying that π also satisfies the formula $\mathbf{XG}\phi$. Now, since all paths satisfies $\mathbf{XG}\phi$, then T satisfies $\mathbf{AXG}\phi$.

(b) Yes, if a tree T satisfies $\mathbf{EXEG}\phi$ then there exists a path in the tree $a_1, a_2, a_3 \ldots$ such that starting from a_2 there exist another path, let's say $a_2, a_3', a_4' \ldots$ on which ϕ is true everywhere. This means that the path $a_1, a_2, a_3', a_4' \ldots$ satisfies the formula $\mathbf{XG}\phi$ which means that T satisfies $\mathbf{EXG}\phi$.

(c) Yes, since ϕ and ψ both are true in all paths of a tree satisfying the formula, this means that ϕ is true in all paths of the tree and ψ is also true in all paths of the tree.

(d) No, consider this tree which satisfies $\mathbf{EX}p \wedge \mathbf{EX}q$ but does not satisfy $\mathbf{E}(\mathbf{X}p \wedge \mathbf{X}q)$: