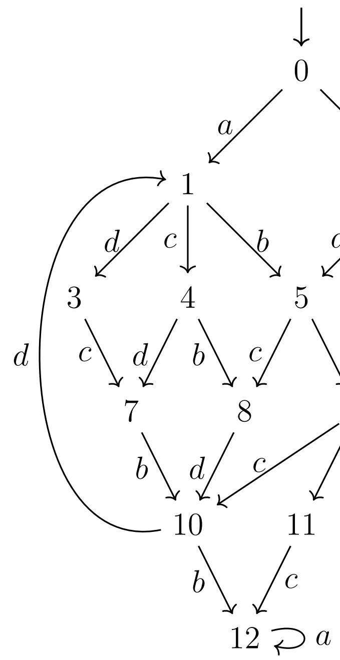
Technische Universität München (I7) **Summer Semester 2019**
J. Esparza / P. Ashok / T. Meggendorfer **06.06.2019**

Model Checking – Exercise sheet 6

Exercise 6.1
Consider the following Kripke structure $\mathcal{K} = (S, A, \rightarrow, 0, AP, \nu)$, where $A = \{a, b, c, d, e\}$, $AP = \{p\}$, $\nu(6) = \{p\}$, and $\nu(s) = \emptyset$ if $s \neq 6$.



(a) Write down the maximal independence relation $I \subseteq A \times A$.

(b) Write down the maximal invisibility set $U \subseteq A$.

(c) Compute a reduction function *red* that satisfies the ample set conditions C0–C3. Whenever possible, choose $red(s)$ such that it is a proper subset of $en(s)$, for each state s.

(d) Use *red* to construct a reduced Kripke structure $\mathcal{K}'$ that is stuttering equivalent to the original Kripke structure $\mathcal{K}$.

Exercise 6.2

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.

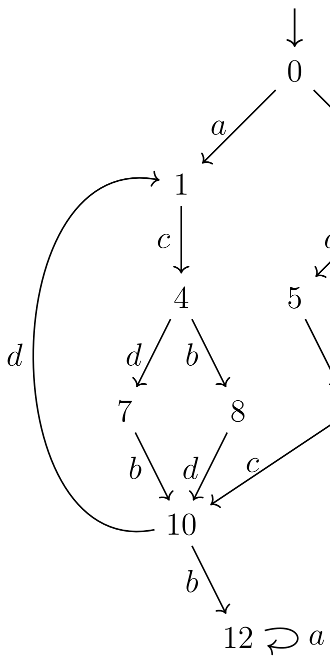
Solution 6.1

(a)
$$I = \{ \ (a,b),(a,c),(a,d),(b,c),(b,e),(c,d),(c,e),(d,e),$$
$$(b,a),(c,a),(d,a),(c,b),(e,b),(d,c),(e,c),(e,d) \ \}$$

(b) $U = \{b, c, d\}$

(c) $red(0) = \{a, b\}$, $red(1) = \{c\}$, $red(2) = \{a, e\}$, $red(5) = \{d\}$, $red(4) = \{b, d\}$, $red(6) = \{a\}$, $red(7) = \{b\}$, $red(8) = \{d\}$, $red(9) = \{c\}$, $red(10) = \{b\}$, $red(12) = \{a\}$,

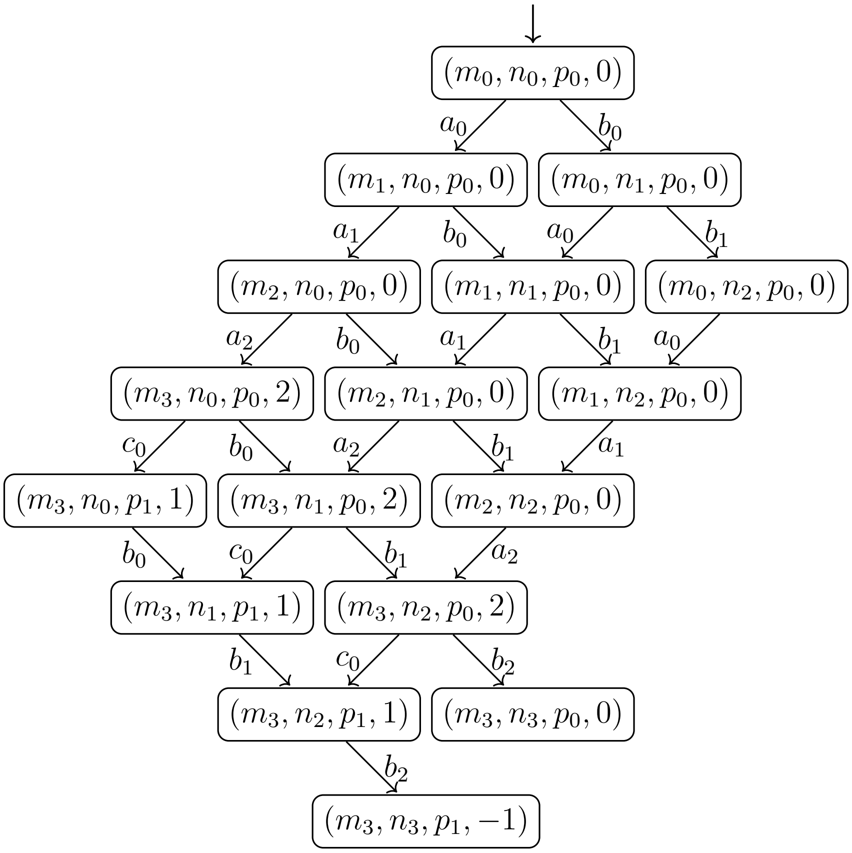
(d)



Solution 6.2

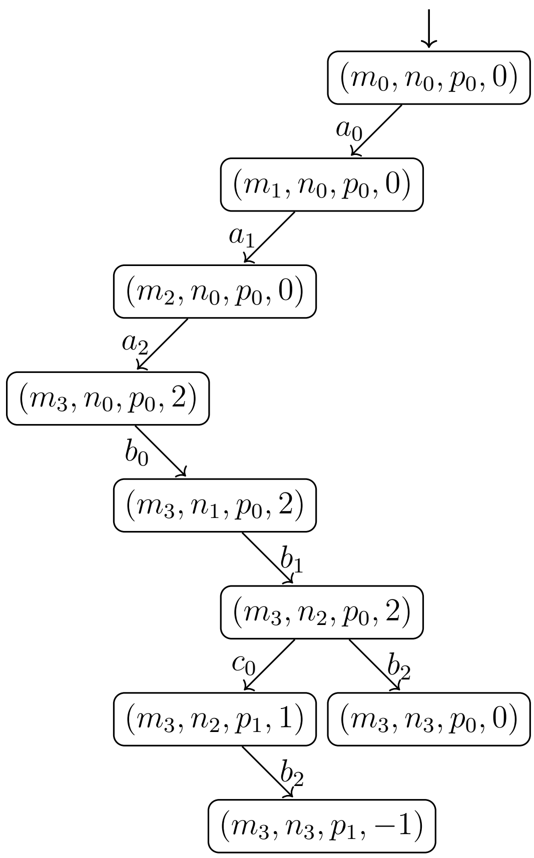
We define actions $a_0, a_1, a_2, b_0, b_1, b_2$, and c_0 for statements in `m`, `n`, and `p`, respectively. Each state in the Kripke structure is a tuple of program locations and a valuation of `g`. Notice that it is not necessary to explicitly models valuations of `x` and `y` as they are implicitly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