Exam solution – Introduction to Verification

January 13, 2023

1 Partial-order reduction

(a) The following states have multiple enabled actions:

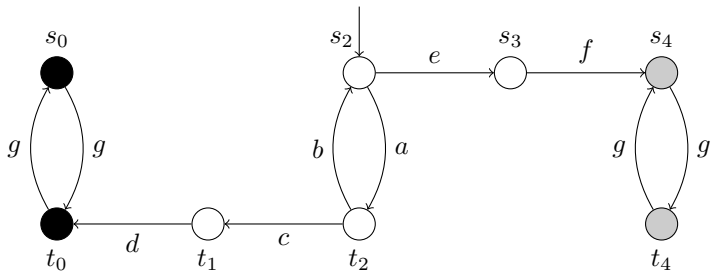
- s_2 with $\{a, c, e\}$: $\langle a, c\rangle$ and $\langle a, e\rangle$ form a 'diamond', but $\langle c, e\rangle$ do not.
- s_1 with $\{a, d\}$: we conclude that $\langle a, d\rangle$ are not independent.
- s_3 with $\{a, f\}$: ditto for $\langle a, f\rangle$.
- t_1, t_2, t_3: analogous, with b taking the role of a.

Thus, the only relevant dependent pairs are $\{a, b\} \times \{d, f\}$ and $\langle c, e\rangle$.

Obviously, only d and f are visible, the other actions are invisible.

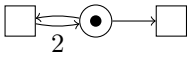
(b) In s_2, the outgoing a-transition can be removed (which eliminates t_2 altogether). No other transition (or state) can be eliminated, it suffices to apply rules C0 and C1, due to the dependencies found in (a).

(c) There are three classes for stutter equivalence to preserve: a run (i) either remains in the white states, (ii) or eventually reaches the black states, (iii) or eventually reaches the grey states. A possible result is shown below.



2 Petri nets

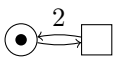
(a) (i) not bounded, not live, not cyclic



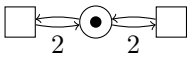
(ii) not bounded, not live, cyclic: impossible

Suppose that a net (with place p) is cyclic and unbounded but not live, i.e. there exists a transition t and a marking $m \in R$ such that m cannot reach any m' with $m'(p) \geq W(p,t)$.
But due to cyclicity, one can reach m_0 from any $m \in R$, and due to unboundedness, $R = \mathit{reach}(m_0)$ contains a marking m' with $m'(p) \geq W(p,t)$, a contradiction.

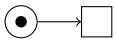
(iii) not bounded, live, not cyclic



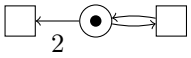
(iv) not bounded, live, cyclic



(v) bounded, not live, not cyclic



(vi) bounded, not live, cyclic



(vii) bounded, live, not cyclic: impossible

Let p be the single place. Call a transition t *increasing* if $W(p,t) < W(t,p)$, *preserving* if $W(p,t) = W(t,p)$, and *decreasing* if $W(p,t) > W(t,p)$.
Suppose that the net is bounded but not cyclic. Boundedness implies that no transition can be increasing. If the net had preserving transitions only, then only the initial marking is reachable, and the net would be cyclic. Thus the net must have at least one decreasing transition t. Consider the run where we repeat t until the number of tokens is less than $W(p,t)$. After this, t can never fire again, hence the net is not live.

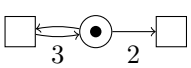
(viii) bounded, live, cyclic

(b) (i) Let I be a positive invariant, m some reachable marking and q some place. From the definition it follows that any multiple of an invariant is also an invariant, so w.l.o.g. assume that all entries of I are at least 1. We then have

$$m(q) \leq m(q) \cdot I(q) \leq \sum_{p \in P} I(p) \cdot m(p) = \sum_{p \in P} I(p) \cdot m_0(p).$$

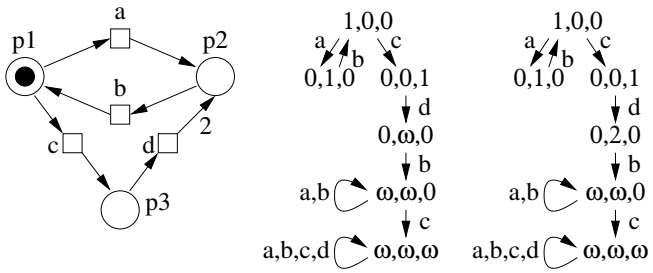
The first two steps are justified by the fact that I is positive and $m(p) \geq 0$ for all p. The last step follows from the fact that I is an invariant. The latter expression is a constant and provides a bound for q (and in fact for all places).

(ii) The statement is false. The net shown below is live and can reach any odd number of tokens. However, if $m(p) = 2$, the net can reach 0 tokens and is unable to continue afterwards.

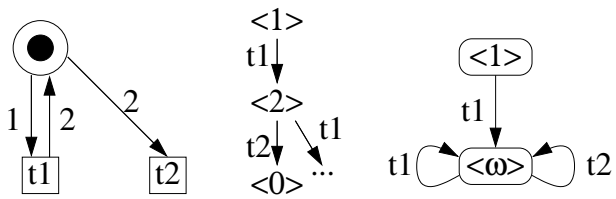


3 Coverability graphs

(a) An example is shown in the figure below. The left-hand side shows a simple net. The centre shows the coverability graph obtained if the marking $m_1 := \langle 0, 1, 0\rangle$ is treated before $m_2 := \langle 0, 0, 1\rangle$. This makes m_1 a predecessor of m_2, so when m_2 is treated, firing d leads to $\langle 0, \omega, 0\rangle$ rather than simply $\langle 0, 2, 0\rangle$. The right-hand side shows the coverability graph when m_2 is treated before m_1.



(b) The statement is not true. Indeed, it suffices to use the net from Question 2(b), the example below shows a modified version. It has a deadlock (by firing t_1, t_2), but its (unique) coverability graph has two nodes, both with outgoing edges (left figure: net; centre: excerpt of reachability graph; right: coverability graph).



4 Bisimulation

1. K_2 satisfies **EX EX AX** p, but K_1 and K_3 do not. Thus, K_2 is not bisimilar to either of them. K_1 and K_3 are bisimilar as witnessed by the relation $\{(a, g), (b, h), (c, i), (c, k)\}$.

2. The definition is equivalent to saying that H is a bisimulation iff both H and H^{-1} are. Therefore, it suffices to show that if H and J are simulations, then so is $H \circ J$; the rest follows from $(H \circ J)^{-1} = J^{-1} \circ H^{-1}$.

   Points (i) and (ii) are trivial. For (iii), suppose that $\langle s, t\rangle \in H \circ J$ and $s \to s'$. Then there exists u such that $\langle s, u\rangle \in H$ and $\langle u, t\rangle \in J$; since H is a simulation, then there is u' with $u \to u'$ and $\langle s', u'\rangle \in H$. Likewise, from $\langle u, t\rangle \in J$ we can deduce the existence of t' with $t \to t'$ and $\langle u', t'\rangle \in J$. But then $\langle s', t'\rangle \in H \circ J$, and we are done.