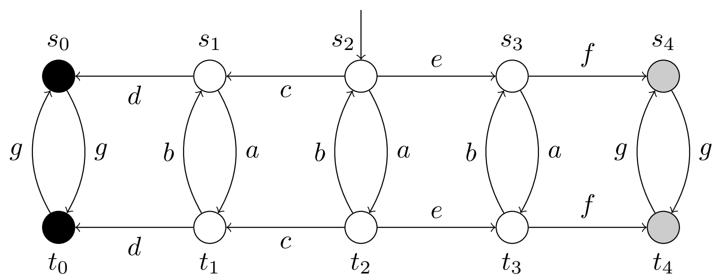
Second Exam – Introduction to Verification

January 13, 2023

Answers can be given in either French or English. Justify all your answers.

1 Partial-order reduction

Consider the structure shown below, where states with identical shades (white, grey, black) indicate that they satisfy the same atomic properties.



(a) Which pairs of actions are independent of each other? (It suffices to examine those that actually appear together at some state.) Which actions are visible and invisible?

(b) According to the rules of reduction C0–C3, which transitions (and states) can be eliminated from the system?

(c) Ignoring C0–C3, propose a maximal set of transitions that can be removed while maintaining stuttering equivalence.

Reminder: **C0** = no additional deadlocks may be introduced; **C1** = for every state s, every path starting at s in the original system satisfies the following: no action that depends on some action in $red(s)$ occurs before an action from $red(s)$; **C2** = when reducing, only invisible actions can be kept; **C3** = for all cycles in the reduced system: if $a \in en(s)$ for some state s in the cycle, then $a \in red(s')$ for some state s' in the cycle.

2 Petri nets

Let $N = \langle P, T, F, W, m_0 \rangle$ be a Petri net, and let $R := reach(m_0)$, i.e. the set of markings reachable from m_0 in N. With $N(m)$ we denote the net that is like N but with m as the intitial marking. We write $m \geq m'$ if $m(p) \geq m(p')$ for all $p \in P$. An *invariant* of N is a vector I with one entry for each place such that $C^T I = 0$, where C is the incidence matrix of N. An invariant is called *positive* if $I(p) > 0$ for every place $p \in P$.

We define the following properties of nets:

- N is *bounded* if there is some K such that for all $p \in P$ and $m \in R$, $m(p) \leq K$.

- N is *live* if for every marking $m \in R$ and every transition $t \in T$, m can reach a marking m' such that m' enables t (intuitively, every transition t can always occur again).
- N is *cyclic* if every marking $m \in R$ can reach m_0.

(a) Consider the eight different combinations of these three properties and their negations:

(i) not bounded, not live, not cyclic	(v) bounded, not live, not cyclic
(ii) not bounded, not live, cyclic	(vi) bounded, not live, cyclic
(iii) not bounded, live, not cyclic	(vii) bounded, live, not cyclic
(iv) not bounded, live, cyclic	(viii) bounded, live, cyclic

For each case, either give an example of a Petri net *with one single place* that exhibits these properties or explain why it is not possible to construct such a net.

(b) Prove or refute the following properties:

(i) If N has a positive invariant, then N is bounded.

(ii) If N is live and $m \geq m_0$, then $N(m)$ is live.

3 Coverability graphs

The following algorith for computing coverability graphs was presented in the course:

```
COVERABILITY-GRAPH(⟨P, T, F, W, M0⟩)
⟨V, E, v0⟩ := ⟨{M0}, ∅, M0⟩;
Work : set := {M0};
while Work ≠ ∅
   do remove some M from Work;
      for t ∈ enabled(M)
         do M' := fire(M, t);
            M' := AddOmegas(M, M', V);
            if M' ∉ V
              then V := V ∪ {M'}
                   Work := Work ∪ {M'};
            E := E ∪ {⟨M, t, M'⟩};
return ⟨V, E, v0⟩;
```

```
ADDOMEGAS(M, M', V)
repeat saved := M';
       for all M'' ∈ V s.t. M'' →* M
          do if M'' < M'
               then M' := M' + ((M' − M'') · ω);
until saved = M';
return M';
```

(a) The algorithm above is partially non-deterministic: e.g., the order in which nodes are removed from the worklist is undefined. Find an example of a net N for which the algorithm could produce two different, non-isomorphic coverability graphs. For both coverability graphs, indicate the order in which nodes were treated in the worklist.

(b) A marking of a net N is said to be a *deadlock* if no transition can fire in it. Clearly, N contains a reachable deadlock if and only if the reachability graph of N contains a node with no outgoing edges. Is the same true of N and any of its coverability graphs?

4 Bisimulation

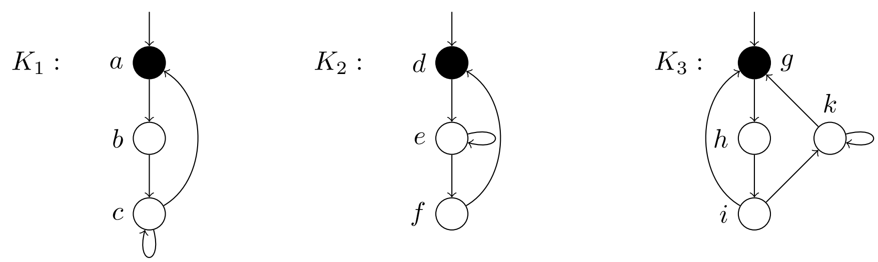
Recall: Let $\mathcal{K}_1 = \langle S, \to_1, s_0, AP, \nu \rangle$ and $\mathcal{K}_2 = \langle T, \to_2, t_0, AP, \mu \rangle$ be two Kripke structures. $H \subseteq S \times T$ is a *bisimulation* between $\mathcal{K}_1$ and $\mathcal{K}_2$ if $\langle s_0, t_0 \rangle \in H$ and for all $\langle s, t \rangle \in H$ the following hold:

(i) $\nu(s) = \mu(t)$;

(ii) for every s' with $s \to_1 s'$, there exists t' such that $t \to_2 t'$ and $\langle s', t' \rangle \in H$;

(iii) for every t' with $t \to_2 t'$, there exists s' such that $s \to_1 s'$ and $\langle s', t' \rangle \in H$.

(a) In the figure below, black nodes satisfy p while white nodes do not. Determine for each pair of Kripke structures K_i, K_j whether $K_i \equiv K_j$. If $K_i \equiv K_j$, give a bisimulation. If $K_i \not\equiv K_j$, give a CTL formula using only the modalities AX and EX that distinguishes the two.



(b) Prove or refute (by a counterexample) the following claim:

- Let H be a bisimulation between structures K_1 and K_2 and J a bisimulation between K_2 and K_3. Is $H \circ J$ a bisimulation between K_1 and K_3?