Home Assignment 2: Simulations in Petri Nets (with some solutions)

To hand in before or on February 15, 2012.
The penalty for delays is 2 points per day.

	23	24	25	26	27	28	29
	30	31					
February			1	2	3	4	5
	6	7	8	9	10	11	12
	13	14	15	16	17	18	19

Electronic versions (PDF only) can be sent by email to ⟨schmitz@lsv.ens-cachan.fr⟩, paper versions should be handed in on the 15th or put in my mailbox at LSV, ENS Cachan.

Recall that a marked *Petri net* is a tuple $\mathcal{N} = \langle P, T, \Sigma, W, m_0\rangle$ where P is a finite set of *places*, T a finite set of *transitions*, Σ a finite alphabet, $W : (P \times T) \cup (T \times P) \to \mathbb{N}$ the *arc weight mapping*, and $m_0 : P \to \mathbb{N}$ is the *initial marking*.

A transition t in T is *firable* in a marking m in $\mathbb{N}^P$ if $m(p) \geq W(p, t)$ for all $p \in P$, and results in a new marking m' defined by $m'(p) = m(p) - W(p, t) + W(t, p)$ for all p in P; we note $m \xrightarrow{t} m'$ in this case.

Let us define some set AP of atomic propositions, which will always verify $\mathrm{AP} \subseteq P$. A Petri net $\mathcal{N}$ defines a (generally infinite) Kripke structure $\mathfrak{M}(\mathcal{N}) \stackrel{\text{def}}{=} \langle S, T', I, \mathrm{AP}, \ell\rangle$ with state set $S = \mathbb{N}^P$, initial state set $I = \{m_0\}$, and transition relation $T' = \{m \to m' \in \mathbb{N}^P \times \mathbb{N}^P \mid \exists t \in T.m \xrightarrow{t} m'\}$. The set $\ell(m)$ of atomic propositions holding at a state m in $\mathbb{N}^P$ is $\{p \in \mathrm{AP} \mid m(p) > 0\}$.

These definitions lead to a "state-based" view of model-checking on Petri nets: a Petri net $\mathcal{N}$ satisfies a CTL* formula φ in a marking m, written $\mathcal{N}, m \models \varphi$, if $\mathfrak{M}(\mathcal{N}), m \models \varphi$.

1 Simulations and Existential CTL

The idea behind the simulation preorder between two systems $\mathfrak{M}_1$ and $\mathfrak{M}_2$ is that any behaviour of the simulated system $\mathfrak{M}_1$ can be exhibited by the simulating system $\mathfrak{M}_2$.

Definition 1 (Simulation)**.** Let $\mathfrak{M}_1 = \langle S_1, T_1, I_1, \mathrm{AP}, \ell_1\rangle$ and $\mathfrak{M}_2 = \langle S_2, T_2, I_2, \mathrm{AP}, \ell_2\rangle$ be two Kripke structures. A binary relation $Z \subseteq S_1 \times S_2$ is called a (positive) *simulation* from $\mathfrak{M}_1$ to $\mathfrak{M}_2$ if the following conditions are satisfied: for every $s_1 \mathrel{Z} s_2$,

1. $\ell_1(s_1) \subseteq \ell_2(s_2)$,
2. if $s_1 \to s_1'$ in T_1, then there exists s_2' in S_2 with $s_2 \to s_2'$ in T_2 and $s_1' \mathrel{Z} s_2'$.

We write $s_1 \preceq s_2$ if there exists a simulation Z between $\mathfrak{M}_1$ and $\mathfrak{M}_2$ s.t. $s_1 \mathrel{Z} s_2$. If, in addition,

3. for every s_1 in I_1, there exists s_2 in I_2 s.t. $s_1 \mathrel{Z} s_2$,

then we write $\mathfrak{M}_1 \preceq \mathfrak{M}_2$, and $\mathcal{N}_1 \preceq \mathcal{N}_2$ if $\mathfrak{M}(\mathcal{N}_1) \preceq \mathfrak{M}(\mathcal{N}_2)$.

Exercise 1 (Logical Characterization)**.** Let us define *positive existential CTL** as the fragment of CTL* defined by the following abstract syntax, where p ranges over the set of atomic propositions AP:

$$\varphi ::= \top \mid \bot \mid p \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \mathsf{E}\psi \qquad \text{(state formulæ)}$$
$$\psi ::= \varphi \mid \mathsf{X}\psi \mid \psi \wedge \psi \mid \psi \vee \psi \mid \psi \,\mathsf{U}\, \psi \mid \psi \,\mathsf{R}\, \psi \;. \qquad \text{(path formulæ)}$$

Positive existential CTL* includes *positive existential CTL* (hereafter noted E$^+$CTL), which is defined by the following abstract syntax:

$$\varphi ::= \top \mid \bot \mid p \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \mathsf{EX}\varphi \mid \mathsf{E}(\varphi \,\mathsf{U}\, \varphi) \mid \mathsf{E}(\varphi \,\mathsf{R}\, \varphi) \;. \qquad \text{(state formulæ)}$$

We also write E$^+$CTL(X) for the fragment of E$^+$CTL that only allows the "X" temporal modality.

Let us consider two (not necessarily different) Kripke structures $\mathfrak{M}_1 = \langle S_1, T_1, I_1, \mathrm{AP}, \ell_1\rangle$ and $\mathfrak{M}_2 = \langle S_2, T_2, I_2, \mathrm{AP}, \ell_2\rangle$.

[4] 1. Assume $\mathfrak{M}_1$ to be *total*, i.e. for any state s_1 there exists some state s_1' such that $s_1 \to s_1'$ is a transition in T_1. Prove the following two statements, for any two states s_1 and s_2, and any two infinite paths π_1 and π_2 in $\mathfrak{M}_1$ and $\mathfrak{M}_2$, resp.:
   (a) if $s_1 \preceq s_2$, then for any positive existential CTL* state formula φ, $s_1 \models \varphi$ implies $s_2 \models \varphi$,
   (b) if $\pi_1 = s_{0,1}s_{1,1}\cdots$ and $\pi_2 = s_{0,2}s_{1,2}\cdots$ are two infinite paths with $s_{i,1} \preceq s_{i,2}$ for all i in $\mathbb{N}$, then for any positive existential CTL* path formula ψ, $\pi_1 \models \psi$ implies $\pi_2 \models \psi$.

[2] 2. Assume $\mathfrak{M}_2$ to be *image-finite*, i.e. for any state s_2 the set $T_2(s_2)$ is finite. Let us consider the following relation on $S_1 \times S_2$:

$$\mathcal{F} = \{(s_1, s_2) \in S_1 \times S_2 \mid \forall \varphi \in \mathrm{E^+CTL}(\mathsf{X}), s_1 \models \varphi \text{ implies } s_2 \models \varphi\} \;.$$

   Show that $\mathcal{F}$ satisfies conditions 1 and 2 of Definition 1, i.e. that it is a simulation between $\mathfrak{M}_1$ and $\mathfrak{M}_2$.

[1] 3. Conclude by proving the following theorem:

Theorem 1 (Logical Characterization of Simulation)**.** *Let $\mathfrak{M}_1 = \langle S_1, T_1, I_1, \mathrm{AP}, \ell_1 \rangle$ be a total Kripke structure, $\mathfrak{M}_2 = \langle S_2, T_2, I_2, \mathrm{AP}, \ell_2 \rangle$ be an image-finite Kripke structure, and s_1 and s_2 be two states of S_1 and S_2 resp. The following three statements are equivalent:*

1. $s_1 \preceq s_2$,
2. *for all positive existential CTL* state formulæ* φ: $s_1 \models \varphi$ *implies* $s_2 \models \varphi$,
3. *for all* $\mathrm{E}^+\mathrm{CTL}(\mathsf{X})$ *formulæ* φ: $s_1 \models \varphi$ *implies* $s_2 \models \varphi$.

Theorem 1 has interesting implications for model-checking problems: consider two systems $\mathfrak{M}_1$ and $\mathfrak{M}_2$ with $s_1 \preceq s_2$ for some $(s_1, s_2) \in S_1 \times S_2$, and φ an $\mathrm{E}^+\mathrm{CTL}$ formula. Further assume that $\mathfrak{M}_1$ is a model with a small description, then $\mathfrak{M}_1, s_1 \models \varphi$ can be tested more efficiently and ensures $\mathfrak{M}_2, s_2 \models \varphi$.

2 Undecidability of Simulations

Consider now the case of Petri nets: $\mathrm{E}^+\mathrm{CTL}(\mathsf{U}, \mathsf{X})$ model-checking of a net $\mathcal{N}_2$ is in general ExpSpace-complete (the lower bound comes from the hardness of coverability; the upper bound from an extension of Rackoff's technique for small models seen in Exercise 8 of TD 6). Therefore, coming up with a suitably small $\mathcal{N}_1$ and testing for the existence of a simulation between $\mathcal{N}_1$ and $\mathcal{N}_2$ would seem like a nice way of avoiding some of that complexity. We are going to see that, unfortunately, the simulation problem, i.e. given $\langle \mathcal{N}_1, \mathcal{N}_2, \mathrm{AP} \rangle$ to check whether $\mathcal{N}_1 \preceq \mathcal{N}_2$, is undecidable.

The proof relies on a reduction from an instance $\langle \mathcal{M} \rangle$ of the halting problem of a Minsky machine to an instance $\langle \mathcal{N}_1, \mathcal{N}_2, \mathrm{AP} \rangle$ of the simulation problem, where $\mathcal{N}_1$ and $\mathcal{N}_2$ are two Petri nets with $\mathcal{N}_1 \preceq \mathcal{N}_2$ iff $\mathcal{M}$ does not halt.

Definition 2 (Minsky Machines)**.** A *2-counter Minsky machine* is a tuple $\mathcal{M} = \langle Q, C, \delta, q_0, q_f \rangle$ where Q is a finite set of states with distinguished initial state q_0 and halting state q_f, $C = \{c_1, c_2\}$ are two counter names, and δ associates to each state q except q_f a unique transition instruction, which is either

$$q \mapsto c\texttt{++; goto } q' \,, \tag{inc}$$

or

$$q \mapsto \texttt{if } (c \texttt{ == 0) \{ goto } q' \texttt{ \} else \{ } c\texttt{--; goto } q'' \texttt{ \}} \,, \tag{dec}$$

for some $c \in C$ and $q', q'' \in Q$; we can view the halting state q_f as associated to the instruction

$$q_f \mapsto \texttt{halt} \,. \tag{halt}$$

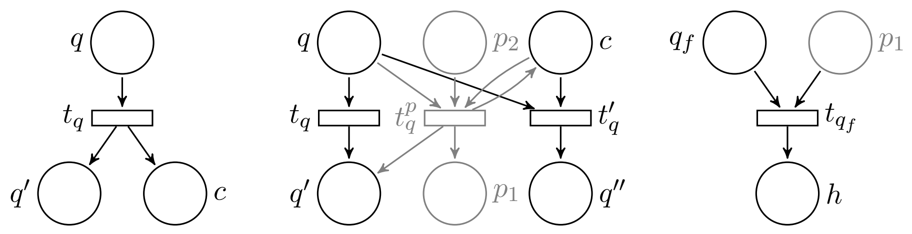
The (unique) *run* of a 2-counter Minsky machine is the finite or infinite sequence $\rho = ((q_i, c_{i,1}, c_{i,2}))_{i \geq 0}$ of configurations in $Q \times \mathbb{N}^2$ holding the current state and the current values of the two counters, where $(q_0, c_{0,1}, c_{0,2}) = (q_0, 0, 0)$, and respecting the transition instructions for all $i \geq 0$. The run ρ *halts* if $q_n = q_f$ for some $n \in \mathbb{N}$ (regardless of the counter values).[1] It is undecidable, given $\langle \mathcal{M} \rangle$, whether its run halts.

[1] As q_f does not allow any further transition, the run ρ is then finite.

Exercise 2 (Undecidability of the Simulation Problem)**.** Let us explain a possible reduction from the halting problem to the simulation problem. Given an instance $\langle \mathcal{M} \rangle$, we define

$$\begin{aligned} \mathrm{AP} &\stackrel{\text{def}}{=} C \uplus Q \uplus \{h\} , \\ P &\stackrel{\text{def}}{=} \mathrm{AP} \uplus \{p_1, p_2\} , \\ T &\stackrel{\text{def}}{=} \{t_q \mid q \in Q \setminus \{q_f\} \wedge \delta(q) \text{ of form (inc)}\} \\ &\quad \uplus \{t_q, t_q^p, t'_q \mid q \in Q \setminus \{q_f\} \wedge \delta(q) \text{ of form (dec)}\} \\ &\quad \uplus \{t_{q_f}\} , \end{aligned}$$

and the weights W defined by the following:



(inc) (dec) (halt)

Note that t_q^p witnesses an incorrect simulation of a transition of type (dec) (indeed, it checks the presence of at least one token in c but goes to q' instead of q''), and furthermore moves a token from p_2 to p_1.

Define $\mu_1 : Q \times \mathbb{N}^2 \to \mathbb{N}^P$ and $\mu_2 : Q \times \mathbb{N}^2 \to \mathbb{N}^P$ by

$$\mu_1((q,c,c'))(p) \stackrel{\text{def}}{=} \begin{cases} 1 & \text{if } p = q, \\ c & \text{if } p = c_1, \\ c' & \text{if } p = c_2, \\ 1 & \text{if } p = p_1, \\ 0 & \text{otherwise} \end{cases} \qquad \mu_2((q,c,c'))(p) \stackrel{\text{def}}{=} \begin{cases} 1 & \text{if } p = q, \\ c & \text{if } p = c_1, \\ c' & \text{if } p = c_2, \\ 1 & \text{if } p = p_2, \\ 0 & \text{otherwise} \end{cases}$$

for all $p \in P$. We lift μ_1 and μ_2 to be homomorphisms from $(Q \times \mathbb{N}^2)^*$ to $(\mathbb{N}^P)^*$, i.e. mappings from runs of $\mathcal{M}$ to Petri nets executions.

[2] 1. Consider the Petri net $\mathcal{N}_1 \stackrel{\text{def}}{=} \langle P, T, W, \mu_1((q_0, 0, 0)) \rangle$. Show that, if ρ is the run of $\mathcal{M}$, then

   (a) $\mu_1(\rho)$ is a possible execution of $\mathcal{N}_1$, and

   (b) if $\mathcal{M}$ halts, then the last marking in $\mu_1(\rho)$ can fire t_{q_f}.

[2] 2. Let $\mathcal{N}_2 \stackrel{\text{def}}{=} \langle P, T, W, \mu_2((q_0, 0, 0)) \rangle$. Show that, if $\mathcal{M}$ halts, then $\mathcal{N}_1 \not\preceq \mathcal{N}_2$.

Hint: define an E$^+$CTL formula φ over AP s.t. $\mathcal{N}_1, \mu_1((q_0,0,0)) \models \varphi$ but $\mathcal{N}_2, \mu_2((q_0,0,0)) \not\models \varphi$ and conclude by Theorem 1. It can be helpful to assume wlog. that $q' \neq q''$ in (dec).

[3] 3. Show that, if $\mathcal{M}$ does not halt, then $\mathcal{N}_1 \preceq \mathcal{N}_2$.

3 Simulation of a Finite System

Back to the consequences of Theorem 1: if the system $\mathfrak{M}_1$ is *finite* of size n, then $\mathfrak{M}_1, s_1 \models \varphi$ can be tested in polynomial time $O(n \cdot |\varphi|)$. Unlike the case of simulations between Petri nets, the existence of a simulation between a given finite-state system and a given Petri net can be checked.

Exercise 3. We want to prove that, given $\mathfrak{M}_1 = \langle S_1, T_1, I_1, \mathrm{AP}, \ell_1\rangle$ a finite Kripke structure and $\mathcal{N} = \langle P, T, W, m_0\rangle$ a Petri net with $\mathrm{AP} \subseteq P$, one can decide whether $\mathfrak{M}_1 \preceq \mathfrak{M}(\mathcal{N})$, where $\mathfrak{M}(\mathcal{N}) = \langle \mathbb{N}^P, T', \{m_0\}, \mathrm{AP}, \ell\rangle$.

Suppose we want to decide whether $s_0 \preceq m_0$ for some s_0 in I_1 s.t. $\ell_1(s_0) \subseteq \ell(m_0)$ (otherwise there is no point trying!). We construct a tree $t(s_0, m_0)$ with labels of form $\wedge(s,m)$ ("universal nodes") or $\vee(s,m)$ ("existential nodes") where s and m range over S_1 and $\mathbb{N}^P$ resp. The tree root is labeled by $\wedge(s_0, m_0)$.

- A node labeled $\wedge(s,m)$
  - either is a leaf if $T_1(s) = \emptyset$ or if there exists an ancestor in the tree labeled $\wedge(s, m')$ for some $m' \leq m$,
  - or is an internal node with $r = |T_1(s)|$ children with labels $(\vee(s', m))_{s \to s'}$.
- A node labeled $\vee(s,m)$
  - either is a leaf if $T'(m) = \emptyset$, i.e. if no transition can be fired from m in $\mathcal{N}$,
  - or is an internal node with $r \leq |T'(m)|$ children labeled $(\wedge(s, m'))_{m \to m' \wedge \ell_1(s) \subseteq \ell(m')}$.

[2] 1. Show that $t(s_0, m_0)$ is always finite.

Assume $t(s_0,m_0)$ is infinite. As it is of finite branching degree (bounded by the cardinality of $T_1(s)$ for universal nodes $\wedge(s,m)$ and of $T(m)$ for existential nodes $\vee(s,m)$), it must contain an infinite branch by Kőnig's Lemma. Consider the sequence of universal nodes along this branch; as existential and universal nodes are alternating, this is an infinite sequence $\wedge(s_0,m_0)\wedge(s_1,m_1)\cdots$ of elements in $S_1 \times \mathbb{N}^P$.

Now, by the pigeon-hole principle, $(S_1, =)$ is a wqo, and by Dickson's Lemma, $(\mathbb{N}, \leq)$ is also a wqo, thus $(S_1 \times \mathbb{N}, \leq_\times)$ is a also wqo (again by Dickson's Lemma) for the product ordering defined by $(s,m) \leq_\times (s',m')$ iff $s = s'$ and $m \leq m'$. Thus there exist two indices $i < j$ s.t. $s_i = s_j$ and $m_i \leq m_j$. But by definition of $t(s_0,m_0)$, this entails that $\wedge(s_j, m_j)$ is a leaf, in contradiction with the branch being infinite.

[1] 2. Let $s \in S_1$ and $m, m' \in \mathbb{N}^P$. Show that, if $s \preceq m'$ and $m' \leq m$, then $s \preceq m$.

[4] 3. Define inductively the *interpretation* of a tree by

$$[\![\wedge(s,m)(t_1,\ldots,t_r)]\!] \stackrel{\text{def}}{=} \bigwedge_{i=1}^{r} [\![t_i]\!] \qquad [\![\vee(s,m)(t_1,\ldots,t_r)]\!] \stackrel{\text{def}}{=} \bigvee_{i=1}^{r} [\![t_i]\!] .$$

Prove that $s_0 \preceq m_0$ iff $[\![t(s_0,m_0)]\!] = \top$.

$\Rightarrow$ Let us show that, if $[\![\wedge(s,m)(t_1,\ldots,t_r)]\!] = \bot$, then there exists an $\mathrm{E}^+\mathrm{CTL}(\mathsf{X})$ formula φ s.t. $s \models \varphi$ but $m \not\models \varphi$, which by Theorem 1 entails $s \not\preceq m$. In game-theoretic terms, φ describes a winning strategy for Spoiler (i.e. the universal player) starting from (s,m).

We proceed by induction on the height of the tree rooted at $\wedge(s,m)$. By definition, if $[\![\wedge(s,m)(t_1,\ldots,t_r)]\!] = \bot$, then there exists a child labeled $\vee(s',m)$ with $s \to_{T_1} s'$ and $[\![t_i = \vee(s',m)(t'_1,\ldots,t'_r)]\!] = \bot$. For all m' with $m \to m'$, we are going to define a formula $\varphi_{m'}$ s.t. $s' \models \varphi_{m'}$ but $m' \not\models \varphi_{m'}$. By definition of $[\![\vee(s',m)(t'_1,\ldots,t'_r)]\!]$,

if $\ell_1(s') \subseteq \ell(m')$, then there is a child labeled $\wedge(s',m')$ with $[\![t'_j = \wedge(s',m')(t''_1,\ldots,t''_r)]\!] = \bot$, and thus $\varphi_{m'}$ is provided by the induction hypothesis, and otherwise,

if $\ell_1(s') \not\subseteq \ell(m')$, then choosing $\varphi_{m'} \stackrel{\text{def}}{=} p$ an atomic proposition in $\ell_1(s') \setminus \ell(m)$ fits (note that this encompasses the base case of $\vee(s',m)$ being a leaf).

Then, defining $\varphi \stackrel{\text{def}}{=} \mathsf{EX} \bigwedge_{m \to m'} \varphi_{m'}$ fits.

$\Leftarrow$ Assume $[\![t(s_0,m_0)]\!] = \top$. We define σ to be a tree rooted in $\wedge(s_0,m_0)$ obtained from $t(s_0,m_0)$ by removing subtrees: if a universal node $\wedge(s,m)$ is a node of σ then all its children in $t(s_0,m_0)$ are nodes of σ, and if an existential $\vee(s,m)$ is a node of σ, then exactly one of its children $\wedge(s,m')$ in $t(s_0,m_0)$, rooting a tree that evaluates to $\top$, i.e. $[\![\wedge(s,m')(t_1,\ldots,t_r)]\!] = \top$, is a node of σ. Thanks to the definition of $[\![\cdot]\!]$, at least one such σ exists. In game-theoretic terms, σ defines a winning strategy for Duplicator (i.e. the existential player) starting from (s_0,m_0).

Let us show that

$$Z \stackrel{\text{def}}{=} \{(s,m) \mid \exists m' \leq m, \wedge(s,m') \text{ is a node of } \sigma\}$$

is a simulation between $\mathfrak{M}_1$ and $\mathfrak{M}(\mathcal{N})$. Let $s \mathrel{Z} m$ and select some $m' \leq m$ with $\wedge(s,m')$ a node of σ:

Condition 1: by a trivial induction on $t(s_0,m_0)$, every universal node $\wedge(s,m')$ in $t(s_0,m_0)$ (and thus in σ) verifies $\ell_1(s) \subseteq \ell(m')$, and $\ell(m') \subseteq \ell(m)$ since $m' \leq m$.

Condition 2: Assume $s \to_{T_1} s'$. We can then assume that $\wedge(s, m')$ is not a leaf in σ (otherwise it would also be a leaf in $t(s_0, m_0)$ and we could instead select its ancestor $\wedge(s, m_1)$ with $m_1 \leq m' \leq m$ instead, which would still be in σ) and has an existential child $\vee(s', m')$, which is by definition in σ. Still by definition of σ, there exists a single universal child $\wedge(s', m'')$ in σ of $\vee(s', m')$. By definition of a child of an existential node, $m' \xrightarrow{t} m''$ for some $t \in T$ and $\ell(s') \subseteq \ell(m'')$. Consider now the marking m''' obtained by $m \xrightarrow{t} m'''$: by monotonicity of $\mathcal{N}$, $m'' \leq m'''$. Thus we have found a successor marking m''' of m with $s' \; Z \; m'''$.

To conclude, observe that Z contains (s_0, m_0) by definition, thus proving that $s_0 \preceq m_0$.

[1] 4. Conclude that the simulation of a given finite Kripke structure by a given Petri net is decidable.

We have that $\mathfrak{M}_1 \preceq \mathfrak{M}(\mathcal{N})$ iff, for every $s_0 \in I_1$, $\ell_1(s_0) \subseteq \ell(m_0)$ and $[\![t(s_0, m_0)]\!] = \top$, the latter being the decidable evaluation of a finite Boolean circuit. As I_1 is finite this is clearly decidable.