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.

Recall that a marked Petri net is a tuple \( N = (P, T, \Sigma, W, m_0) \) where \( P \) is a finite set of places, \( T \) a finite set of transitions, \( \Sigma \) a finite alphabet, \( W : (P \times T) \cup (T \times P) \rightarrow \mathbb{N} \) the arc weight mapping, and \( m_0 : P \rightarrow \mathbb{N} \) 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 \( AP \subseteq P \). A Petri net \( N \) defines a (generally infinite) Kripke structure \( \mathcal{M}(N) \) with state set \( S = \mathbb{N}^P \), initial state set \( I = \{ m_0 \} \), and transition relation \( T' = \{ m \xrightarrow{t} m' \mid \exists \tau \in T. m \xrightarrow{\tau} m' \} \). The set \( \ell(m) \) of atomic propositions holding at a state \( m \) in \( \mathbb{N}^P \) is \( \{ p \in AP \mid m(p) > 0 \} \).

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

1 Simulations and Existential CTL

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

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

Electronic versions (PDF only) can be sent by email to [schmitz@lsv.ens-cachan.fr](mailto:schmitz@lsv.ens-cachan.fr), paper versions should be handed in on the 15th or put in my mailbox at LSV, ENS Cachan.
1. \( \ell_1(s_1) \subseteq \ell_2(s_2) \),

2. if \( s_1 \rightarrow s'_1 \) in \( T_1 \), then there exists \( s'_2 \) in \( S_2 \) with \( s_2 \rightarrow s'_2 \) in \( T_2 \) and \( s'_1 \nsim s'_2 \).

We write \( s_1 \preceq s_2 \) if there exists a simulation \( Z \) between \( \mathcal{M}_1 \) and \( \mathcal{M}_2 \) s.t. \( s_1 \sim s_2 \). If, in addition,

3. for every \( s_1 \) in \( I_1 \), there exists \( s_2 \) in \( I_2 \) s.t. \( s_1 \sim s_2 \),

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

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

\[
\varphi ::= T \mid \bot \mid p \mid \varphi \land \varphi \mid \varphi \lor \varphi \mid \text{E}\psi \quad \quad \text{(state formulæ)}
\]

\[
\psi ::= \varphi \mid \text{X}\psi \mid \psi \land \psi \mid \psi \lor \psi \mid \psi \text{U}\psi \mid \psi \text{R}\psi . \quad \quad \text{(path formulæ)}
\]

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

\[
\varphi ::= T \mid \bot \mid p \mid \varphi \land \varphi \mid \varphi \lor \varphi \mid \text{EX}\varphi \mid \text{E}(\varphi \text{U} \varphi) \mid \text{E}(\varphi \text{R} \varphi) . \quad \quad \text{(state formulæ)}
\]

We also write \( \text{E}^+\text{CTL}(X) \) for the fragment of \( \text{E}^+\text{CTL} \) that only allows the “X” temporal modality.

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

[4] 1. Assume \( \mathcal{M}_1 \) to be total, i.e. for any state \( s_1 \) there exists some state \( s'_1 \) such that \( s_1 \rightarrow s'_1 \) 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 \( \pi_1 \) and \( \pi_2 \) in \( \mathcal{M}_1 \) and \( \mathcal{M}_2 \), resp.:

(a) if \( s_1 \preceq s_2 \), then for any positive existential \( \text{CTL}^* \) state formula \( \varphi \), \( s_1 \models \varphi \) 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 \( \text{CTL}^* \) path formula \( \psi \), \( \pi_1 \models \psi \) implies \( \pi_2 \models \psi \).

[2] 2. Assume \( \mathcal{M}_2 \) 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 \( S_1 \times S_2 \):

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

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

[1] 3. Conclude by proving the following theorem:
Theorem 1 (Logical Characterization of Simulation). Let $\mathcal{M}_1 = \langle S_1, T_1, I_1, AP, \ell_1 \rangle$ be a total Kripke structure, $\mathcal{M}_2 = \langle S_2, T_2, I_2, AP, \ell_2 \rangle$ 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 formula $\varphi$: $s_1 \models \varphi$ implies $s_2 \models \varphi$,

3. for all $E^+\text{CTL}(X)$ formula $\varphi$: $s_1 \models \varphi$ implies $s_2 \models \varphi$.

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

2 Undecidability of Simulations

Consider now the case of Petri nets: $E^+\text{CTL}(U, X)$ 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 $(\mathcal{N}_1, \mathcal{N}_2, AP)$ 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 $\langle \mathcal{N}_1, \mathcal{N}_2, AP \rangle$ 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 $\delta$ associates to each state $q$ except $q_f$ a unique transition instruction, which is either

$$q \mapsto c++; \text{ goto } q', \quad \text{(inc)}$$

or

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

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

$$q_f \mapsto \text{ halt}.$$  

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 $\rho$ halts if $q_n = q_f$ for some $n \in \mathbb{N}$ (regardless of the counter values). It is undecidable, given $\langle \mathcal{M} \rangle$, whether its run halts.

As $q_f$ does not allow any further transition, the run $\rho$ 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 \( (\mathcal{M}) \), we define

\[
\begin{align*}
AP & \overset{\text{def}}{=} C \uplus Q \uplus \{ h \}, \\
P & \overset{\text{def}}{=} AP \uplus \{ p_1, p_2 \}, \\
T & \overset{\text{def}}{=} \{ t_q \mid q \in Q \setminus \{ q_f \} \land \delta(q) \text{ of form } \text{(inc)} \} \\
& \quad \uplus \{ t_q, t^p_q, t'_q \mid q \in Q \setminus \{ q_f \} \land \delta(q) \text{ of form } \text{(dec)} \} \\
& \quad \uplus \{ t_{q_f} \}, \\
\end{align*}
\]

and the weights \( W \) defined by the following:

\[
\begin{align*}
\mu_1((q,c,c'))(p) & \overset{\text{def}}{=} \begin{cases} 
1 & \text{if } p = q, \\
c & \text{if } p = c_1, \\
c' & \text{if } p = c_2, \\
1 & \text{if } p = p_1, \\
0 & \text{otherwise}
\end{cases} \\
\mu_2((q,c,c'))(p) & \overset{\text{def}}{=} \begin{cases} 
1 & \text{if } p = q, \\
c & \text{if } p = c_1, \\
c' & \text{if } p = c_2, \\
1 & \text{if } p = p_2, \\
0 & \text{otherwise}
\end{cases}
\end{align*}
\]

for all \( p \in P \). We lift \( \mu_1 \) and \( \mu_2 \) 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.

1. Consider the Petri net \( \mathcal{N}_1 \overset{\text{def}}{=} (P, T, W, \mu_1((q_0,0,0))) \). Show that, if \( \rho \) 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. Let \( \mathcal{N}_2 \overset{\text{def}}{=} (P, T, W, \mu_2((q_0,0,0))) \). Show that, if \( \mathcal{M} \) halts, then \( \mathcal{N}_1 \not\preceq \mathcal{N}_2 \).
Hint: define an $E^c$-CTL formula $\varphi$ over $AP$ s.t. $N_1, \mu_1((q_0, 0, 0)) \models \varphi$ but $N_2, \mu_2((q_0, 0, 0)) \not\models \varphi$ and conclude by Theorem 1. It can be helpful to assume wlog. that $q' \neq q''$ in $t$.

3. Show that, if $M$ does not halt, then $N_1 \preceq N_2$.

3 Simulation of a Finite System

Back to the consequences of Theorem 1, if the system $M_1$ is finite of size $n$, then $M_1, s_1 \models \varphi$ 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 $M_1 = \langle S_1, T_1, I_1, AP, \ell_1 \rangle$ a finite Kripke structure and $N = \langle P, T, W, m_0 \rangle$ a Petri net with $AP \subseteq P$, one can decide whether $M_1 \preceq M(N)$, where $M(N) = \langle \mathbb{N}^P, T', \{m_0\}, AP, \ell \rangle$.

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 $\land(s, m)$ (“universal nodes”) or $\lor(s, m)$ (“existential nodes”) where $s$ and $m$ range over $S_1$ and $\mathbb{N}^P$ resp. The tree root is labeled by $\land(s_0, m_0)$.

- A node labeled $\land(s, m)$
  - either is a leaf if $T_1(s) = \emptyset$ or if there exists an ancestor in the tree labeled $\land(s, m')$ for some $m' \leq m$,
  - or is an internal node with $r = |T_1(s)|$ children with labels $(\lor(s', m))_{s \rightarrow s'}$.

- A node labeled $\lor(s, m)$
  - either is a leaf if $T'(m) = \emptyset$, i.e. if no transition can be fired from $m$ in $N$,
  - or is an internal node with $r \leq |T'(m)|$ children labeled $(\land(s, m'))_{m \rightarrow m' \land \ell_1(s) \subseteq \ell(m')}$. 

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 $\land(s, m)$ and of $T(m)$ for existential nodes $\lor(s, m)$), it must contain an infinite branch by König’s Lemma. Consider the sequence of universal nodes along this branch; as existential and universal nodes are alternating, this is an infinite sequence $\land(s_0, m_0) \land (s_1, m_1) \cdots$ 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 $\land(s_j, m_j)$ is a leaf, in contradiction with the branch being infinite.
2. Let \( s \in S_1 \) and \( m, m' \in N^P \). Show that, if \( s \preceq m' \) and \( m' \preceq m \), then \( s \preceq m \).

3. Define inductively the interpretation of a tree by

\[
\begin{align*}
[\land(s, m)(t_1, \ldots, t_r)] & \overset{\text{def}}{=} \bigwedge_{i=1}^r [t_i] \\
[\lor(s, m)(t_1, \ldots, t_r)] & \overset{\text{def}}{=} \bigvee_{i=1}^r [t_i].
\end{align*}
\]

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

\(\Rightarrow\) Let us show that, if \([\land(s, m)(t_1, \ldots, t_r)] = \bot\), then there exists an \( E^+\text{CTL}(X) \) formula \( \varphi \) s.t. \( s \models \varphi \) but \( m \not\models \varphi \), which by Theorem 1 entails \( s \not\preceq m \). In game-theoretic terms, \( \varphi \) 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 \( \land(s, m) \). By definition, if \([\land(s, m)(t_1, \ldots, t_r)] = \bot\), then there exists a child labeled \( \lor(s', m) \) with \( s \rightarrow_T s' \) and \([t_i = \lor(s', m)(t'_1, \ldots, t'_r)] = \bot\). For all \( m' \) with \( m \rightarrow m' \), we are going to define a formula \( \varphi_{m'} \) s.t. \( s' \models \varphi_{m'} \) but \( m' \not\models \varphi_{m'} \). By definition of \([\lor(s', m)(t'_1, \ldots, t'_r)]\):

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

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

Then, defining \( \varphi \overset{\text{def}}{=} \text{EX} \land_{m \rightarrow m'} \varphi_{m'} \) fits.

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

Let us show that

\[
Z \overset{\text{def}}{=} \{ (s, m) \mid \exists m' \leq m, \land(s, m') \text{ is a node of } \sigma \}
\]

is a simulation between \( \mathcal{W}_1 \) and \( \mathcal{W}(\land) \). Let \( s \in Z \) and select some \( m' \leq m \) with \( \land(s, m') \) a node of \( \sigma \):

**Condition** by a trivial induction on \( t(s_0, m_0) \), every universal node \( \land(s, m') \) in \( t(s_0, m_0) \) (and thus in \( \sigma \)) verifies \( \ell_1(s) \subseteq \ell(m') \), and \( \ell(m') \subseteq \ell(m) \) since \( m' \leq m \).
Condition 2. Assume $s \rightarrow T_1 s'$. We can then assume that $\land(s, m')$ is not a leaf in $\sigma$ (otherwise it would also be a leaf in $t(s_0, m_0)$ and we could instead select its ancestor $\land(s, m_1)$ with $m_1 \leq m' \leq m$ instead, which would still be in $\sigma$) and has an existential child $\lor(s', m')$, which is by definition in $\sigma$. Still by definition of $\sigma$, there exists a single universal child $\land(s', m'')$ in $\sigma$ of $\lor(s', m')$. By definition of a child of an existential node, $m' \not\rightarrow m''$ for some $t \in T$ and $\ell(s') \subseteq \ell(m'')$. Consider now the marking $m'''$ obtained by $m \not\rightarrow m'''$: by monotonicity of $N$, $m'' \leq m'''$. Thus we have found a successor marking $m'''$ of $m$ with $s' \not\rightarrow Z m'''$.

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

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

We have that $\forall_1 \preceq \forall(N)$ 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.