TD 8: Petri Nets

1 Modeling Using Petri Nets

Exercise 1 (Traffic Lights). Consider again the traffic lights example from the lecture notes:

1. How can you modify this Petri net so that it becomes 1-safe?

2. Extend your Petri net to model two traffic lights handling a street intersection.

Exercise 2 (Producer/Consumer). A producer/consumer system gathers two types of processes:

- **producers** who can make the actions *produce* \((p)\) or *deliver* \((d)\), and
- **consumers** with the actions *receive* \((r)\) and *consume* \((c)\).

All the producers and consumers communicate through a single unordered channel.

1. Model a producer/consumer system with two producers and three consumers. How can you modify this system to enforce a maximal capacity of ten simultaneous items in the channel?

2. An *inhibitor arc* between a place \(p\) and a transition \(t\) makes \(t\) firable only if the current marking at \(p\) is zero. In the following example, there is such an inhibitor arc between \(p_1\) and \(t\). A marking \((0, 2, 1)\) allows to fire \(t\) to reach \((0, 1, 2)\), but \((1, 1, 1)\) does not allow to fire \(t\).
Using inhibitor arcs, enforce a priority for the first producer and the first consumer on the channel: the other processes can use the channel only if it is empty it is not currently used by the first producer and the first consumer.

2 Model Checking Petri Nets

Exercise 3 (Upper Bounds). Let us fix a Petri net $\mathcal{N} = \langle P, T, F, W, m_0 \rangle$. We consider as usual propositional LTL, with a set of atomic propositions AP equal to $P$ the set of places of the Petri net. We define proposition $p$ to hold in a marking $m$ in $\mathbb{N}^P$ if $m(p) > 0$.

The models of our LTL formulae are computations $m_0 m_1 \cdots$ in $(\mathbb{N}^P)^\omega$ such that, for all $i \in \mathbb{N}$, $m_i \xrightarrow{T} \mathcal{N} m_{i+1}$ is a transition step of the Petri net $\mathcal{N}$.

1. We want to prove that state-based LTL model checking can be performed in polynomial space for 1-safe Petri nets. For this, prove that one can construct an exponential-sized Büchi automaton $\mathcal{B}_\mathcal{N}$ from a 1-safe Petri net that recognizes all the infinite computations of $\mathcal{N}$ starting in $m_0$.

2. In the general case, state-based LTL model checking is undecidable. Prove it for Petri nets with at least two unbounded places, by a reduction from the halting problem for 2-counter Minsky machines.

3. We consider now a different set of atomic propositions, such that $\Sigma = 2^\text{AP}$, and a labeled Petri net, with a labeling homomorphism $\lambda : T \to \Sigma$. The models of our LTL formulae are infinite words $a_0 a_1 \cdots$ in $\Sigma^\omega$ such that $m_0 \xrightarrow{t_0} \mathcal{N} m_1 \xrightarrow{t_1} \mathcal{N} m_2 \cdots$ is an execution of $\mathcal{N}$ and $\lambda(t_i) = a_i$ for all $i$.

Prove that action-based LTL model checking can be performed in polynomial space for labeled 1-safe Petri nets.

Exercise 4 (Lower Bounds for 1-Safe Petri Nets). A linear bounded automaton (LBA) $\mathcal{M} = \langle Q, \Sigma \cup \{\dashv, \vdash\}, \Gamma, \delta, q_0, #, F \rangle$ is a Turing machine with a left endmarker $\dashv$ and a right endmarker $\vdash$,

- that cannot move left from $\dashv$ nor right from $\vdash$,
- that cannot print over $\dashv$ or $\vdash$, and
that starts with input \( \vdash x \vdash \) for some \( x \) in \( \Sigma^* \).

A LBA is thus restricted to its initial tape contents. The membership problem for a LBA with input \( \vdash x \vdash \) is \( \text{PSPACE} \)-hard.

1. Show how to simulate a LBA with input \( \vdash x \vdash \) by a 1-safe Petri net of quadratic size.
2. Show that state-based LTL model checking is \( \text{PSPACE} \)-hard in the size of the Petri net for 1-safe Petri nets.
3. Show that action-based LTL model checking is \( \text{PSPACE} \)-hard in the size of the Petri net for labeled 1-safe Petri nets.

3 Coverability

The \textit{coverability problem} for Petri nets is the following decision problem:

\textbf{Instance:} A Petri net \( \mathcal{N} = \langle P, T, F, W, m_0 \rangle \) and a marking \( m_1 \) in \( \mathbb{N}^P \).

\textbf{Question:} Does there exist \( m_2 \) in \( \text{Reach}_{\mathcal{N}}(m_0) \) such that \( m_1 \leq m_2 \)?

For 1-safe Petri nets, coverability coincides with reachability, and is thus \( \text{PSPACE} \)-complete according to the previous exercises.

\textbf{Exercise 5} (Inhibitor Arcs). Prove that the coverability problem is undecidable for Petri nets having two inhibitor arcs.
(Hint: start by proving its undecidability for Petri nets with two places that are the sources of inhibitor arcs.)

\textbf{Exercise 6} (Coverability Graph). One way to decide the coverability problem is to use Karp and Miller’s coverability graph (see the lecture notes). Indeed, we have the equivalence between the two statements:

\( i. \) there exists \( m_2 \) in \( \text{Reach}_{\mathcal{N}}(m_0) \) such that \( m_1 \leq m_2 \), and
\( ii. \) there exists \( m_3 \) in \( \text{CoverabilityGraph}_{\mathcal{N}}(m_0) \) such that \( m_1 \leq m_3 \).

1. Prove that \( [i] \) implies \( [ii] \).
(Hint: prove that if \( m \xrightarrow{\mathcal{N}} m_2 \) in the Petri net \( \mathcal{N} \) for some \( m \) in \( \mathbb{N}^P \) and \( u \) in \( T^* \), then there exists \( m_3 \) in \( (\mathbb{N} \cup \{\omega\})^P \) such that \( m_2 \leq m_3 \) and \( m \xrightarrow{G} m_3 \) in the coverability graph.)
Let us prove that (ii) implies (i). The idea is that we can find reachable markings that agree with \( m_3 \) on its finite places, and that can be made arbitrarily high on its \( \omega \)-places. For this, we need to identify the graph nodes where new \( \omega \) values were introduced, which we call \( \omega \)-nodes. Moreover, for a marking \( m \) in \((\mathbb{N} \cup \{\omega\})^P\), we define \( \Omega(m) \) as the set of places \( p \) such that \( m(p) = \omega \).

(a) Recall that an \( \omega \) value is introduced in the coverability graph thanks to Algorithm 1.

```
1 repeat
2   saved ← \( m' \)
3 foreach \( m'' \in V \) s.t. \( \exists v \in T^+, m'' \xrightarrow{v} G m \) do
4     if \( m'' < m' \) then
5         \( m' \leftarrow m' + ((m' - m'') \cdot \omega) \)
6 end
7 until saved = \( m' \)
8 return \( m' \)
```

**Algorithm 1:** \textsc{AddOmegas}(\( m, t, m', V, E \))

Let \( \{v_1, \ldots, v_i\} \) be the set of \( v \) sequences found on line 3 of the algorithm that resulted in an \( \omega \) value for \( m' \) on line 5 during a call to \textsc{AddOmegas}(\( m, t, m', V, E \)). For each \( i \), let \( n_i \in \mathbb{N} \) be a value such that the sequence \( v_i \) can be fired from the marking \((n_i, n_i, \ldots, n_i)\).

Show that, for any \( j \in \mathbb{N} \), there exists a marking \( \nu_j \) such that \( \nu_j(p) = \frac{m(p) - W(p, t) + W(t, p)}{j \cdot \sum_{i=1}^{l} n_i} \) if \( p \in P \setminus \Omega(m) \) and \( \nu_j(p) = \frac{m(p)}{j} \) if \( p \in \Omega(m) \), that allows to fire the sequence \( v^1_j \cdots v^j_j \). How does the marking \( \nu^j_j \) with \( \nu_j(v^1_j \cdots v^j_j) \rightarrow_N \nu^j_j \) compare to \( \nu_j \)?

(b) Prove that, if \( m \xrightarrow{u} G m_3 \) for some \( u \) in \( T^* \) in the coverability graph and \( m' \) in \( \mathbb{N}^{\Omega(m_3)} \) is a partial marking on the places of \( \Omega(m_3) \), then there are

- a decomposition \( u = u_1 u_2 \cdots u_{n+1} \) with each \( u_i \) in \( T^* \) (where the markings \( \mu_i \) reached by \( m \xrightarrow{u_1 \cdots u_i} G \mu_i \) are \( \omega \)-nodes),
- sequences \( w_1, \ldots, w_n \) in \( T^+ \),
- numbers \( k_1, \ldots, k_n \) in \( \mathbb{N} \),

such that \( m \xrightarrow{u_1 u_2 \cdots u_n w_n} G m_2 \rightarrow_N m_2 \) with \( m_2(p) = m_3(p) \) for all \( p \) in \( P \setminus \Omega(m_3) \) and \( m_2(p) \geq m'(p) \) for all \( p \) in \( \Omega(m_3) \).
Exercise 7 (Rackoff’s Algorithm). A rather severe issue with the coverability graph construction (see Exercise 6) is that it can generate a graph of non primitive recursive size compared to that of the original Petri net. We show here a much more decent ExpSpace upper bound, which is matched by an ExpSpace hardness proof by Lipton.

Let us fix a Petri net $\mathcal{N} = \langle P, T, F, W, m_0 \rangle$. We consider *generalized markings* in $\mathbb{Z}^P$. A *generalized computation* is a sequence $\mu_1 \cdots \mu_n$ in $(\mathbb{Z}^P)^*$ such that, for all $1 \leq i < n$, there is a transition $t$ in $T$ with $\mu_{i+1}(p) = \mu_i(p) - W(p, t) + W(t, p)$ for all $p \in P$ (i.e. we do not enforce enabling conditions). For a subset $I$ of $P$, a generalized sequence is $I$-*admissible* if furthermore $\mu_i(p) \geq W(p, t)$ for all $p$ in $I$ at each step $1 \leq i < n$. For a value $B$ in $\mathbb{N}$, it is $I$–$B$-*bounded* if furthermore $\mu_i(p) < B$ for all $p$ in $I$ at each step $1 \leq i \leq n$. A generalized sequence is an $I$-*covering* for $m_1$ if $\mu_1 = m_0$ and $\mu_n(p) \geq m_1(p)$ for all $p$ in $I$.

Thus a computation is a $P$-admissible generalized computation, and a $P$-admissible $P$-covering for $m_1$ answers the coverability problem.

For a Petri net $\mathcal{N} = \langle P, T, F, W, m_0 \rangle$ and a marking $m_1$ in $\mathbb{N}^P$, let $\ell(\mathcal{N}, m_1)$ be the length of the shortest $P$-admissible $P$-covering for $m_1$ in $\mathcal{N}$ if one exists, and otherwise $\ell(\mathcal{N}, m_1) = 0$. For $L$, $k$ in $\mathbb{N}$, define

$$M_L(k) = \sup \{ \ell(\mathcal{N}, m_1) \mid |P| = k, \max\{W(p, t) \mid p \in P, t \in T\} + \max\{m_1(p) \mid p \in P\} \leq L \} .$$

1. Show that $M_L(0) \leq 1$.

2. We want to show that

$$M_L(k) \leq (L \cdot M_L(k-1))^k + M_L(k-1)$$

for all $k \geq 1$. To this end, we prove that, for every marking $m_1$ in $\mathbb{N}^P$ for a Petri net $\mathcal{N}$ with $|P| = k$,\n
$$\ell(\mathcal{N}, m_1) \leq (L \cdot M_L(k-1))^k + M_L(k-1) .$$

(\*)

Let

$$B = M_L(k-1) \cdot \max\{W(p, t) \mid p \in P, t \in T\} + \max\{m_1(p) \mid p \in P\} .$$

and suppose that there exists a $P$-admissible $P$-covering $w = \mu_1 \cdots \mu_n$ for $m_1$ in $\mathcal{N}$.

(a) Show that, if $w$ is $P$–$B$-bounded, then (\*) holds.

(b) Assume the contrary: we can split $w$ as $w_1w_2$ such that $w_1$ is $P$–$B$-bounded and $w_2$ starts with a marking $\mu_j$ with a place $p$ such that $\mu_j(p) \geq B$. Show that (\*) also holds.

3. Show that $M_L(|P|) \leq L^{(3(|P|)!}$ for $L = 2 + \max\{W(p, t) \mid p \in P, t \in T\} + \max\{m_1(p) \mid p \in P\}$.
4. Assuming that the size $n$ of the instance $(N, m_1)$ of the coverability problem is more than
\[ \max\{ \log L, |P|, \max \{ \log W(t, p) | t \in T, p \in P \} \} , \]
deduce that we can guess a $P$-admissible $P$-covering for $m_1$ of length at most $2^{c \cdot n \log n}$ for some constant $c$. Conclude.