Technische Universität München **Summer Term 2019**
I7
Prof. J. Esparza / Ch. Weil-Kennedy / P. Meyer **11.06.2019**

Petri nets — Exercise Sheet 4

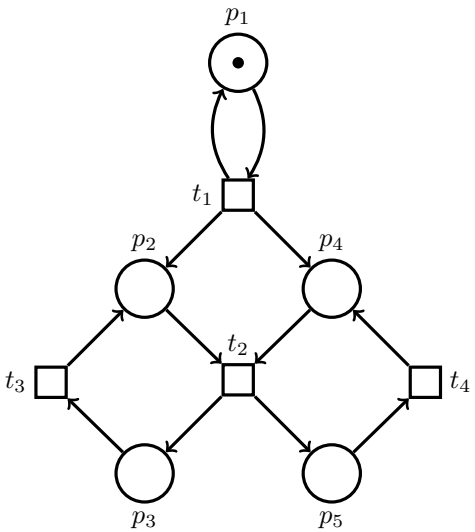
Exercise 4.1

(a) Show that

$$X = \{(x_1, x_2, x_3) \in \mathbb{N}^3 : (x_1 + 3 \leq x_2 \leq x_3 + 1) \vee (x_2 = 2x_1 + x_3 + 5)\}$$

is semilinear by giving its representation as a finite set of roots and periods.

(b) Consider the following Petri net, and define its set of reachable markings. Show that the number of tokens per place of these markings is describable by a semi-linear set.



Exercise 4.2

(a) Reduce the coverability problem to the reachability problem.

For that, describe an algorithm that, given a Petri net $(\mathcal{N}, M_0)$ and a marking M, constructs a Petri net $(\mathcal{N}', M_0')$ and a marking M' such that M' is reachable in $\mathcal{N}'$ from M_0' **if and only if** M is coverable in $\mathcal{N}$ from M_0. The algorithm should run in polynomial time.

(b) Consider problem **P**:

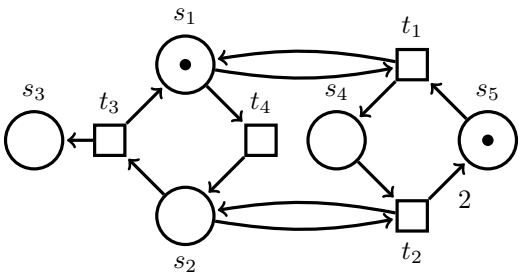
INPUT: A Petri net $(\mathcal{N}, M_0)$ and a transition t of $\mathcal{N}$.
QUESTION: Is there an infinite run σ in $(\mathcal{N}, M_0)$ such that t occurs infinitely many times in σ ?

You are given an algorithm that, given a Petri net, returns its coverability graph. Using this algorithm, devise an algorithm to solve problem **P**.

Then prove this algorithm correct : prove that there exists an infinite run σ in $(\mathcal{N}, M_0)$ such that t occurs infinitely many times in σ **if and only if** the algorithm gives the correct answer.

Exercise 4.3

We want to show that the following Petri net with weighted arcs has a non-semilinear reachability set.



Consider the following sets of markings, given as $M = (s_1, s_2, s_3, s_4, s_5)$:

$$\mathcal{M}_1 = \{(1, 0, x_1, x_2, x_3) \mid 0 < x_2 + x_3 \leq 2^{x_1}\}$$
$$\mathcal{M}_2 = \{(0, 1, x_1, x_2, x_3) \mid 0 < 2x_2 + x_3 \leq 2^{x_1+1}\}$$
$$\mathcal{M} = \mathcal{M}_1 \cup \mathcal{M}_2$$

The set $\mathcal{M}$ is non-semilinear. We are going to show that $\mathcal{M}$ is equal to the set of reachable markings for the above Petri net.

1. Show that if $M_0 \xrightarrow{*} M$, then $M \in \mathcal{M}$. For this, show that $M_0 \in \mathcal{M}$ and if $M \in \mathcal{M}$ and $M \xrightarrow{t} M'$ for some transition t, then also $M' \in \mathcal{M}$.
2. Show that if $M \in \mathcal{M}$, then $M_0 \xrightarrow{*} M$.

   Note: This is a rather hard exercise. *Hint*: Do this by induction on $x_1 = M(s_3)$ for $M \in \mathcal{M}$. In the induction step at x_1, do a case distinction between $M \in \mathcal{M}_1$ and $M \in \mathcal{M}_2$. In each case, find an M' for which you can apply the induction hypothesis and from which M is reachable.

Exercise 4.4

(a) Show that the upward closed sets ($\subseteq \mathbb{N}^k$ for some positive constant k) are semi-linear.

(b) The dual notion of an upward closed set is called a downward closed set. Downward closed sets ($\subseteq \mathbb{N}^k$ for some positive constant k) are sets $\mathcal{M}$ such that $\forall M, M' \in \mathbb{N}^k$, if $M \in \mathcal{M}$ and $M' \leq M$ then $M' \in \mathcal{M}$.

- Show that the complement of a downward closed set is upward closed.
- Show that downward closed sets are also semi-linear, using the fact that a finite intersection of semi-linear sets is semi-linear.

Solution 4.1

(a)

$$X = (0,3,2) + \mathbb{N} \cdot (1,1,1) + \mathbb{N} \cdot (0,1,1) + \mathbb{N} \cdot (0,0,1) \cup \\ (0,5,0) + \mathbb{N} \cdot (1,2,0) + \mathbb{N} \cdot (0,1,1)$$

(b) The markings reachable from $(1,0,0,0,0)$ are the markings M such that $M(p_1) = 1$ and $M(p_2) + M(p_3) = M(p_4) + M(p_5)$. So the reachability set of the Petri net is

$$(1,0,0,0,0) + \mathbb{N} \cdot (0,1,0,1,0) \\ + \mathbb{N} \cdot (0,1,0,0,1) \\ + \mathbb{N} \cdot (0,0,1,1,0) \\ + \mathbb{N} \cdot (0,0,1,0,1)$$

Solution 4.2

(a) Let $\mathcal{N}'$ be a copy of $\mathcal{N}$ and for each place of $\mathcal{N}$, add a transition to $\mathcal{N}'$ with that place as its only input place and no output places. Let the initial marking and target marking for $\mathcal{N}'$ be the same as for $\mathcal{N}$, i.e. $M_0' = M_0$ and $M' = M$.

If M is coverable in $\mathcal{N}$ by some marking $M_1 \geq M$, then we can also reach M_1 in $\mathcal{N}'$, and fire the additional transitions to reduce tokens until we reach $M = M'$ in $\mathcal{N}'$.

On the other hand, if M' is reachable in $\mathcal{N}'$, then we can execute the sequence to reach M' without firing the additional transitions. That sequence is also enabled in $\mathcal{N}$ at M_0 and leads to a marking $M_1 \geq M' = M$, so M is coverable in $\mathcal{N}$.

Formal answer (given for clarity):

Define the net $\mathcal{N}' = (S', T', F')$ with $S' = S$, $T' = T \uplus \{t_s \mid s \in S\}$ and $F' = F \cup \{(s, t_s) \mid s \in S\}$ and the markings $M_0' = M_0$ and $M' = M$.

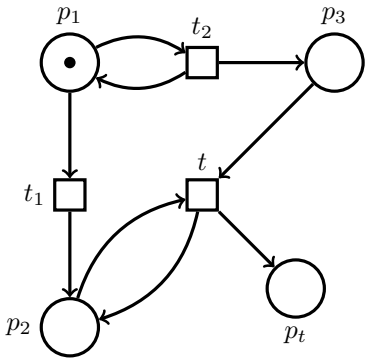
If M is coverable in $\mathcal{N}$ from M_0, then there is a marking M_1 and an occurrence sequence σ with $M_0 \xrightarrow{\sigma} M_1$ in $\mathcal{N}$ and $M_1 \geq M$. Then also $M_0' \xrightarrow{\sigma} M_1$ in $\mathcal{N}'$. From M_1, for each $s \in S$, we can fire t_s exactly $M_1(s) - M(s)$ times. This yields our target marking $M = M'$, so M' is reachable in $\mathcal{N}'$ from M_0'.

On the other hand, if M' is reachable in $\mathcal{N}'$ from M_0', then there is an occurrence sequence σ with $M_0' \xrightarrow{\sigma} M'$ in $\mathcal{N}'$. Let τ be the occurrence sequence obtained from σ by removing all occurrences of t_s for $s \in S$. As every t_s only removes tokens in $\mathcal{N}'$, by the monotonicity property of Petri nets, τ is also enabled at M_0' in $\mathcal{N}'$ and as τ only contains transitions from T, it is also enabled at M_0 in $\mathcal{N}$. This yields $M_0 \xrightarrow{\tau} M_1$ in $\mathcal{N}$ for some marking M_1 with $M_1 \geq M' = M$, so M is coverable in $\mathcal{N}$ from M_0.

(b) In the tutorial, the following solution was presented, but it was incorrect:

Given a Petri net $(\mathcal{N}, M_0)$ and a transition t, we give a procedure that answers if there exists an infinite run σ such that t occurs infinitely many times in σ. Let $\mathcal{N}'$ be a copy of $\mathcal{N} = (S, T, F)$. We add a new place p_t and an arc from transition t to place p_t. Let M_0' be equal to M_0 over S and equal to 0 on p_t. We run the given algorithm on $(\mathcal{N}', M_0')$ to obtain its coverability graph. If there exists a marking of the coverability graph that contains an ω in place p_t then we answer yes, and otherwise no.

This was incorrect because it is possible to exhibit a Petri net with place p_t for some t whose coverability graph contains an ω in p_t, but in which there is no infinite run with an infinite number of t. Here is such a Petri net courtesy of Philipp Czerner.



To fire t from the initial marking, transition t_2 must be fired at least once, then t_1 must be fired, and then t can be fired as many times as t_2 was fired. Transitions t_2 and t can be fired an unbounded number of times, so the coverability graph contains an ω in p_t, but there is no infinite sequence that fires t infinitely often (in fact, once t_1 has been fired there can be no infinite sequence at all).

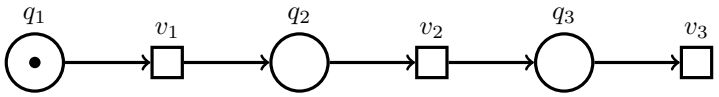
So this algorithm was too simplistic. It is still possible to reduce problem **P** to an EXPSPACE problem (like coverability, but unlike reachability), but the proof is quite complicated. For those who are interested, links to such a reduction can be found at the end of this solution. As an alternative reduction, we present here a reduction of problem **P** to reachability.

Reduction to reachability: Let $(\mathcal{N}, M_0)$ be the net in which we want to solve whether there exists a run with an infinite number of occurrences of transition t. We are going to construct another Petri net $(\mathcal{N}', M_0')$ such that M_0' reaches the empty marking $\mathbf{0}$ in this new net if and only if there exists $M_1, M_2, \sigma_1, \sigma_2$ such that $M_0 \xrightarrow{\sigma_1} M_1 \xrightarrow{\sigma_2} M_2$ and $M_1 \leq M_2$ and σ_2 contains at least one occurence of t. This will be an algorithm for problem **P** because the existence of such $M_1, M_2, \sigma_1, \sigma_2$ is equivalent to the existence of a run with an infinite number of occurrences of transition t. Indeed:

- If there exists such a run in $(\mathcal{N}, M_0)$, then by Dickson's Lemma, there exists an infinite sequence of markings $C_1, C_2, C_3 \ldots$ such that $M_0 \xrightarrow{*} C_1 \xrightarrow{*} C_2 \xrightarrow{*} C_3 \ldots$ and $C_1 \leq C_2 \leq C_3 \leq \ldots$. Since the run admits an infinite number of occurrences of t, we can choose $M_1 = C_i, M_2 = C_j$ and σ_1, σ_2 fulfilling our condition.
- If there exists $M_1, M_2, \sigma_1, \sigma_2$ such that $M_0 \xrightarrow{\sigma_1} M_1 \xrightarrow{\sigma_2} M_2$ and $M_1 \leq M_2$ and σ_2 contains at least one occurence of t then the run $\sigma_1\sigma_2\sigma_2\sigma_2 \ldots$ is a run verifying our condition.

Our new net is going to be constituted of two copies of net $(\mathcal{N}, M_0)$ plus some additional control places. Intuitively, there are three "phases": in the first phase, both copies of the net start in M_0 and reach some marking M_1. In the second phase, the second copy goes from M_1 to some M_2. Finally in the third phase, all the tokens are emptied out from the places, checking on the way that $M_1 \leq M_2$ and that t occurred in the second phase in the second copy.

Let our new net $(\mathcal{N}', M_0')$ be two copies of the original net $\mathcal{N}$ plus some new places and transitions. We note the first copy's places and transitions just as in $\mathcal{N}$, and we note the second copy's places and transitions with a prime: that is if p is a place of the original net $\mathcal{N}$, we note it p in the first copy and p' in the second copy. Both copies are initially marked with M_0. To the second copy we add a place p_t and an arc from transition t' to place p_t. Outside of the two copies we add control places q_1, q_2, q_3 and transitions v_1, v_2, v_3 initially marked in q_1 such that



The new initial marking M_0' is thus a marking of M_0 on both copies and a token in q_1. Morally, a token in place $q_i \in \{q_1, q_2, q_3\}$ means that we are in "phase i".

For each transition u of the first copy, we draw arcs from q_1 to u and from u to q_1 as well as arcs from the places of ${}^\bullet u$ to u and from u to $u^\bullet$ in the first copy, and from ${}^\bullet u'$ to u and from u to $u'^\bullet$ in the second copy,. In this way, while q_1 is marked, the transitions are taken in the first copy but consume and produce tokens on both copies at the same time.

For each transition u' of the second copy, we draw arcs from q_2 to u' and from u' to q_2. In this way, while q_2 is marked, the transitions are taken only in the second copy.

For each place p in the original net $\mathcal{N}$, we create a transition in our new net $\mathcal{N}'$ with incoming arcs from p, p' and q_3 and an outgoing arc to q_3. We also create a new transition with incoming arcs from p' and q_3 and an outgoing arc to q_3 for every place p' of the second net including p_t. In this way, while q_3 is marked, places of the first copy can be emptied "at the same time" as the corresponding places in the second copy, and extra tokens in the second copy can be emptied "on their own".

Finally, we add an arc from p_t to v_3. In this way, a token in q_3 can be consumed only if p_t was marked, i.e. if t' was fired at least once in the second copy.

This reduction from **P** to reachability of the empty marking is correct (sketch):

- If there exists $M_1, M_2, \sigma_1, \sigma_2$ such that $M_0 \xrightarrow{\sigma_1} M_1 \xrightarrow{\sigma_2} M_2$ and $M_1 \leq M_2$ and σ_2 contains at least one occurence of t then we can reach the empty marking in the following way: first execute σ_1 on

the transitions of the first copy which results in having marking M_1 on both copies. Then fire v_1, and execute σ_2 on the second copy (using primed transitions), marking p_t when t' is taken. Then fire v_2, and remove all tokens from M_1 on both copies, thus leaving the first copy empty and the second copy with the tokens of $M_2 - M_1$ and tokens on p_t. Then remove these tokens from the second copy, leaving only 1 token in p_t. Finally, fire v_3 by consuming the token in p_t and the token in q_3.

- If there is a run σ from M_0' to the empty marking in $\mathcal{N}'$ then there exists $M_1, M_2, \sigma_1, \sigma_2$ as described above. By construction, σ is of the form $\sigma_1' v_1 \sigma_2' v_2 \sigma_3' v_3$. We can take M_1 to be the marking on the first copy after σ_1', σ_1 to be σ_1' on the corresponding places of $\mathcal{N}$, M_2 to be the marking on the second copy (not counting p_t) after σ_2' and σ_2 to be σ_2' on the corresponding places of $\mathcal{N}$. This is correct by construction, as described above.

Here are references to a reduction of **P** to EXPSPACE:
[1] `https://www.sciencedirect.com/science/article/pii/089054019290059O`
[2] `https://link.springer.com/chapter/10.1007/978-3-642-04420-5_7`

The paper in [1] shows that deciding the existence of sequences and markings

$$M_0 \xrightarrow{\sigma_1} M_1 \xrightarrow{\sigma_2} M_2 \xrightarrow{\sigma_3} \dots \xrightarrow{\sigma_k} M_k$$

satisfying some predicate F on $M_1, \dots, M_k, \sigma_1, \dots, \sigma_k$ is EXPSPACE-complete. F can contain terms of the form $M_i \geq M_j$ or $|\sigma_i|_t > 0$ (among others). The proof is done by adapting Rackoff's result to show there is always a sequence $\sigma_1 \dots \sigma_k$ bounded by double exponential length, if any such sequence exists.

In [2], they show there is a small mistake in [1], and that in general, for any path formulas, the problem is actually as hard as reachability, however when the formula implies $M_k \geq M_1$, it is still EXPSPACE-complete. This then includes the "Fair Nontermination Problems" and the problem **P**.

[2] also uses the idea of simulating k copies of the net to guess the markings $M_1, \dots, M_k$ in phases and verify the path formula by reducing the final marking to the empty marking, thus giving a reduction to reachability.

Solution 4.3

1. We have $M_0 \in \mathcal{M}_1$. Now assume $M \in \mathcal{M}$ and $M \xrightarrow{t} M'$ for some transition t. We show that $M' \in \mathcal{M}$.

   - $M \xrightarrow{t_1} M'$: Then $M = (1, 0, x_1, x_2, x_3)$ with $x_3 \geq 1$ and $M' = (1, 0, x_1, x_2 + 1, x_3 - 1)$. We have $0 < x_2 + 1 + x_3 - 1 = x_2 + x_3 \leq 2^{x_1}$, therefore $M' \in \mathcal{M}_1$.
   - $M \xrightarrow{t_2} M'$: Then $M = (0, 1, x_1, x_2, x_3)$ with $x_2 \geq 1$ and $M' = (0, 1, x_1, x_2 - 1, x_3 + 2)$. We have $0 < 2(x_2 - 1) + x_3 + 2 = 2x_2 + x_3 \leq 2^{x_1+1}$, therefore $M' \in \mathcal{M}_2$.
   - $M \xrightarrow{t_3} M'$: Then $M = (0, 1, x_1, x_2, x_3)$ and $M' = (1, 0, x_1 + 1, x_2, x_3)$. We have $0 < 2x_2 + x_3 \leq 2^{x_1+1}$ and so $0 < x_2 + x_3 \leq 2^{x_1+1}$, therefore $M' \in \mathcal{M}_1$.
   - $M \xrightarrow{t_4} M'$: Then $M = (1, 0, x_1, x_2, x_3)$ and $M' = (0, 1, x_1, x_2, x_3)$. We have $0 < x_2 + x_3 \leq 2^{x_1}$ and so $0 < 2x_2 + x_3 \leq 2^{x_1+1}$, therefore $M' \in \mathcal{M}_2$.

2. We show for all M, if $M \in \mathcal{M}$, then $M_0 \xrightarrow{*} M$, by induction on $x_1 = M(s_3)$.

   Induction base: $x_1 = 0$. Then M is one of the following and can be reached from M_0:

   - $M = (1, 0, 0, 0, 1)$: $M_0 \xrightarrow{\epsilon} M$.
   - $M = (1, 0, 0, 1, 0)$: $M_0 \xrightarrow{t_1} M$.
   - $M = (0, 1, 0, 0, 1)$: $M_0 \xrightarrow{t_4} M$.
   - $M = (0, 1, 0, 1, 0)$: $M_0 \xrightarrow{t_1 t_4} M$.
   - $M = (0, 1, 0, 0, 2)$: $M_0 \xrightarrow{t_1 t_4 t_2} M$.

   Induction hypothesis: Let $x_1 > 0$ and assume that for all M' with $M'(s_3) < x_1$, if $M' \in \mathcal{M}$, then $M_0 \xrightarrow{*} M'$.

   - *Case 1*: $M \in \mathcal{M}_1$. Then $M = (1, 0, x_1, x_2, x_3)$ with $0 < x_2 + x_3 \leq 2^{x_1}$. With $M' := (0, 1, x_1 - 1, 0, x_2 + x_3)$, we have $M' \in \mathcal{M}_2$, so it is reachable by the induction hypothesis. M is then reachable from M' with $\sigma = t_3 t_1^{x_2}$.

- *Case 2*: $M \in \mathcal{M}_2$. Then $M = (0, 1, x_1, x_2, x_3)$ with $0 < 2x_2 + x_3 \leq 2^{x_1+1}$. With $M' := (0, 1, x_1 - 1, 0, x_2 + \lfloor \frac{x_3}{2} \rfloor + x_3 \bmod 2)$, we have $M' \in \mathcal{M}_2$, so it is reachable by the induction hypothesis. M is then reachable from M' with $\sigma = t_3 t_1^{(x_2 + \lfloor \frac{x_3}{2} \rfloor)} t_4 t_2^{\lfloor \frac{x_3}{2} \rfloor}$, as $x_3 = 2\lfloor \frac{x_3}{2} \rfloor + x_3 \bmod 2$.

Solution 4.4

(a) The finite union of semi-linear sets is semi-linear. An upward closed set of minimal elements $\{m_1, ..., m_n\}$ is the union of the upward closed sets of single minimal element m_i. So we just need to show that for any element $m \in \mathbb{N}^k$, the upward closed set $\{m' \mid m \leq m'\}$ is semi-linear. This set is actually even linear, with root $r = m$ and set of periods P the vectors $p_i \in \mathbb{N}^k$ such that $p_i(j) = 1$ if $i = j$ and 0 otherwise, for $i, j \in \{1, \ldots, k\}$.

(b)
- Let $\mathcal{D}$ be a downward closed set, let us show its complement is upward closed. Let $M \in \overline{\mathcal{D}}$ and M' such that $M' \geq M$. We reason by contradiction and suppose $M' \notin \overline{\mathcal{D}}$. Then $M' \in \mathcal{D}$. Since $\mathcal{D}$ is downward closed, M must be in $\mathcal{D}$, contradiction.
- Let $\mathcal{D}$ be a downward closed set. Its complement $\overline{\mathcal{D}}$ is upward closed, so there are a finite number of minimal elements $m_1, \ldots, m_n$ such that $\overline{\mathcal{D}}$ is the union of the upward closed sets of unique minimal element m_i. So $\mathcal{D}$ is the finite intersection of the $\overline{m_i \uparrow}$. We just need to show that for any element $m \in \mathbb{N}^k$, the set $\overline{m \uparrow}$ is semi-linear.

  Let $M \in \mathbb{N}^k$. We have $M \in \overline{m \uparrow}$ if and only if $\exists j \in \{1, \ldots, k\}$ such that $M(j) < m(j)$. For a certain j, this condition can be described as the semi-linear set

$$\bigcup_{i=0}^{m(j)-1} r_{j,i} + P_j$$

  where $r_{j,i}$ is the vector of $\mathbb{N}^k$ with $r_{j,i}(j) = i$ and 0 elsewhere, and P_j is the set of periods p_i such that $p_i(l) = 1$ if $i = l$ and 0 otherwise, for $i \in \{1, \ldots, k\} - \{j\}$. Therefore the set $\overline{m \uparrow}$ is semi-linear as a finite union of these semi-linear unions for each $j \in \{1, \ldots, k\}$