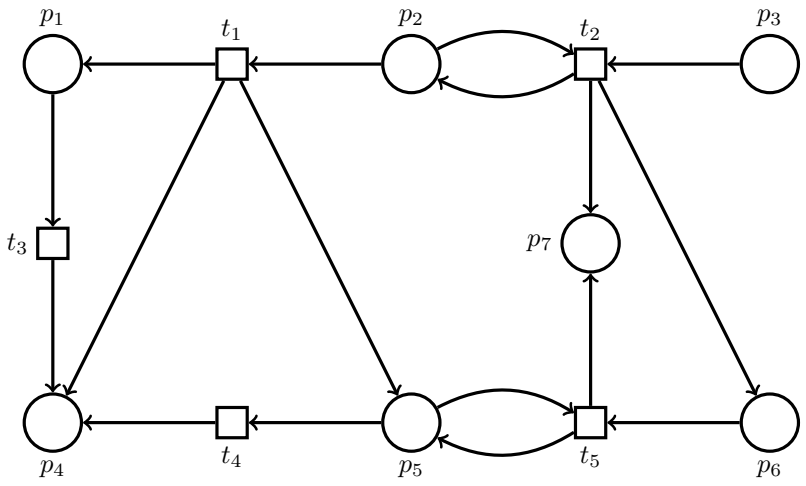
Petri nets — Exercise sheet 6

Solution to be published on 07.07.2020

Exercise 6.1
Consider the following Petri net $\mathcal{N} = (P, T, F)$ with the markings $M = \{p_1, p_2, p_4, p_4\}$ and $M' = \{p_1, p_3\}$:



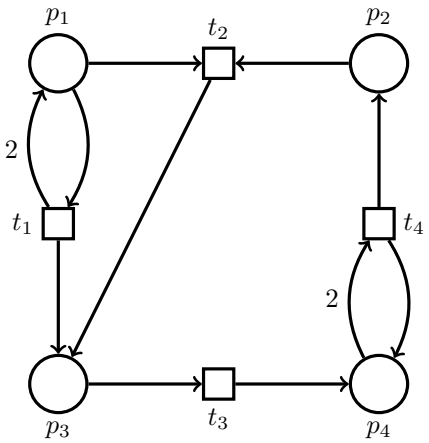
(a) Give a basis of the vector space of S-invariants of $\mathcal{N}$. *Hint: use a characterization of S-invariants.*

(b) Using (a), can you tell whether $(\mathcal{N}, M)$ and $(\mathcal{N}, M')$ are bounded? Can you tell whether they are live?

(c) Give a basis of the vector space of T-invariants of $\mathcal{N}$. *Hint: use a characterization of T-invariants.*

(d) Using (a) and (c), can you tell whether $(\mathcal{N}, M)$ and $(\mathcal{N}, M')$ are live?

Exercise 6.2
Consider the following Petri net (with weights) $\mathcal{N}$:



(a) Find all minimal proper siphons of the net.

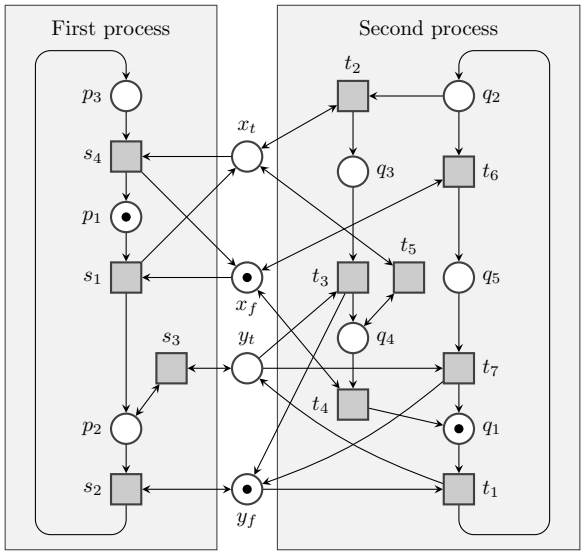
(b) Use (a) to to prove or disprove that $\mathcal{N}$ is live from $M_0 = \{p_2, 3 \cdot p_4\}$,

Exercise 6.3

Lamport's algorithm for mutual exclusion is an algorithm to ensure that two processes never enter their critical section simultaneously, similarly to Peterson's algorithm which you have seen in the lecture.

Below you find pseudocode for the algorithm and a model of it as a Petri net. We want to show that it ensures mutual exclusion, using invariants and traps instead of state-space exploration by e.g. the reachability graph.

First process		Second process	
	`x = False`		`y = False`
	`while True:`		`while True:`
p_1:	`x = True`	q_1:	`y = True`
p_2:	`while y: pass`	q_2:	`if x:`
p_3:	`# critical section`	q_3:	`y = False`
	`x = False`	q_4:	`while x: pass`
			`goto` q_1
		q_5:	`# critical section`
			`y = False`



The goal is to show that there is no reachable marking M such that $M(p_3) \geq 1$ and $M(q_5) \geq 1$.

(a) The net has the following S-invariants $I_1, \ldots, I_6$, which form a basis of the space of all S-invariants:

		p_1	p_2	p_3	x_t	x_f	q_1	q_2	q_3	q_4	q_5	y_t	y_f
I_1	=	1	1	1	0	0	0	0	0	0	0	0	0
I_2	=	0	1	1	0	1	0	0	0	0	0	0	0
I_3	=	0	0	0	1	1	0	0	0	0	0	0	0
I_4	=	0	0	0	0	0	1	1	1	1	1	0	0
I_5	=	0	0	0	0	0	0	1	1	0	1	0	1
I_6	=	0	0	0	0	0	0	0	0	0	0	1	1

Use these invariants to show that there is a unique marking M where $M \sim M_0$, $M(p_3) \geq 1$ and $M(q_5) \geq 1$.

(b) Use traps to show that the marking M derived in (a) is not reachable from M_0. For this, find the largest unmarked trap at M using the algorithm for the largest siphon.

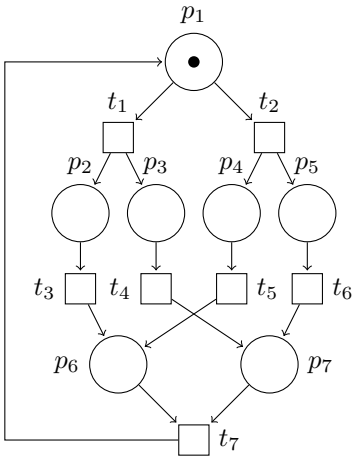
The algorithm can be adapted to find a trap instead of a siphon by switching $Q^\bullet$ to ${}^\bullet Q$ and ${}^\bullet s$ to $s^\bullet$, and finds the largest unmarked trap by initializing R with the set of places unmarked at M.

Exercise 6.4

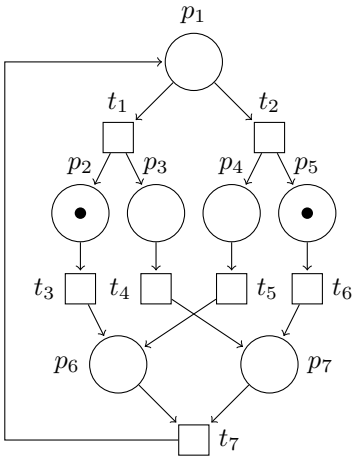
For this exercise, we will use the `Z3` SMT solver as a tool. An SMT solver can solve systems of constraints over different theories, among them propositional logic, i.e. solve boolean formulas, and linear integer arithmetic, i.e. solve systems of linear equations and inequations over the integers. `Z3` can be downloaded from source or with precompiled binaries for Ubuntu, Windows and macOS from `https://github.com/Z3Prover/z3/releases` (z3-4.8.8). After installing it, you should be able to invoke `z3` from the command line.

Consider the following net $\mathcal{N}$ with the two markings M_0 and M shown on the left and right:

Marking M_0



Marking M



(a) Download the file `pn_6-4_marking_equation.smt` and have a look at it. This file contains constraints for the marking equation $M = M_0 + \boldsymbol{N} \cdot X$ applied to above net $\mathcal{N}$ with the markings M, M_0, and declares integer variables `x_t` for each entry $X(t)$, then restricted to the natural numbers.

Check satisfiability of the constraints by invoking `Z3` as follows: `z3 pn_6-4_marking_equation.smt`

`Z3` should then answer either with `unsat` if there is no solution or with `sat` and a model giving a solution. Can you infer from this result whether M is reachable from M_0 in $\mathcal{N}$?

(b) Download the file `pn_6-4_traps_partial.smt`. This file is partially completed with variable definitions `r_p` for each $p \in S$, for now referred to as r_p.

Add a set of boolean constraints to the file, representing conjuncts of a boolean formula φ over the variables r_p, satisfying the following properties:

- if φ is satisfiable, then $\mathcal{N}$ has a trap,
- if φ is not satisfiable, then $\mathcal{N}$ has no trap,
- and additionally, if A is a model of φ, then the set given by $R = \{p \in S \mid A(r_p)\}$ is a trap of $\mathcal{N}$.

Instructions about the SMT syntax are given in the file. After entering the constraints, check that `Z3` accepts the file and outputs a solution, which should be some trap of the net (possibly the empty one).

(c) Add further constraints to your partially completed file from (b) to further ensure that any trap R obtained as a solution by the constraints is marked at M_0 and unmarked at M. The constraints should be satisfiable iff a trap marked at M_0 and unmarked at M exists.

Invoke `Z3` on the file and check if there is a solution. Can you use this result to decide if M is reachable from M_0 in $\mathcal{N}$?

Solution 6.1

(a) Recall that I is an S-invariant if and only if $\sum_{p \in {}^\bullet t} I(p) = \sum_{p \in t^\bullet} I(p)$ for every $t \in T$. This gives rise to the following system of equations:

$$\begin{aligned} I(p_2) &= I(p_1) + I(p_4) + I(p_5), \\ I(p_2) + I(p_3) &= I(p_2) + I(p_6) + I(p_7), \\ I(p_1) &= I(p_4), \\ I(p_5) &= I(p_4), \\ I(p_5) + I(p_6) &= I(p_5) + I(p_7), \end{aligned}$$

which is equivalent to:

$$\begin{aligned} I(p_2) &= 3 \cdot I(p_1), \\ I(p_3) &= 2 \cdot I(p_6), \\ I(p_4) &= I(p_1), \\ I(p_5) &= I(p_1), \\ I(p_7) &= I(p_6). \end{aligned}$$

Therefore, each S-invariant I is fully determined by $I(p_1)$ and $I(p_6)$, and hence the vector space of S-invariants is given by:

$$x \cdot \begin{pmatrix} 1 & 3 & 0 & 1 & 1 & 0 & 0 \end{pmatrix} + y \cdot \begin{pmatrix} 0 & 0 & 2 & 0 & 0 & 1 & 1 \end{pmatrix} \quad \text{for } x, y \in \mathbb{Q}.$$

★ This can be verified using `PIPE` by loading the Petri net and clicking on "Invariant Analysis" in the left menu.

(b) If a Petri net has a positive S-invariant, then it is bounded from any initial marking. By (a), taking $x, y > 0$ yields a positive S-invariants, e.g. $\begin{pmatrix} 1 & 3 & 2 & 1 & 1 & 1 & 1 \end{pmatrix}$ obtained by taking $x = y = 1$. Therefore, $\mathcal{N}$ is bounded both from M and M'.

Assume that $(\mathcal{N}, M)$ is live, then $I \cdot M > 0$ for every semi-positive S-invariant I. By (a), semi-positive S-invariants of $\mathcal{N}$ are obtained by taking $x, y \geq 0$ and $x + y > 0$. Therefore, we have

$$\begin{pmatrix} x \\ 3x \\ 2y \\ x \\ x \\ y \\ y \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 & 2 & 0 & 0 & 0 \end{pmatrix} = 6x$$

When $x = 0$, we have $6x = 0$ which contradicts the fact that $(\mathcal{N}, M)$ is live. Therefore, it is not live.

Let us do the same calculations for M':

$$\begin{pmatrix} x \\ 3x \\ 2y \\ x \\ x \\ y \\ y \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix} = 2x + 2y$$

Since $x + y > 0$, we have $2x + 2y = 2(x + y) > 0$. This implies that $I \cdot M' > 0$ for every semi-positive S-invariant I. Therefore, we cannot conclude whether $(\mathcal{N}, M')$ is live or not.

(c) Recall that J is a T-invariant if and only if $\sum_{t\in{}^\bullet p} I(t) = \sum_{t\in p^\bullet} I(t)$ for every $p \in S$. This gives rise to the following system of equations:

$$\begin{aligned} J(t_1) &= J(t_3), \\ J(t_2) &= J(t_1) + J(t_2), \\ 0 &= J(t_2), \\ J(t_1) + J(t_3) + J(t_4) &= 0, \\ J(t_1) + J(t_5) &= J(t_4) + J(t_5), \\ J(t_2) &= J(t_5), \\ J(t_2) + J(t_5) &= 0. \end{aligned}$$

This system of equations is equivalent to $J(t_1) = J(t_2) = J(t_3) = J(t_4) = J(t_5) = 0$. Therefore, the vector space of T-invariants of $\mathcal{N}$ is trivial, i.e. it only contains the null vector.

★ This can be verified using `PIPE` by loading the Petri net and clicking on "Invariant Analysis" in the left menu.

(d) In addition to the results from (b), we can now show that $\mathcal{N}$ is not live from any initial marking M_0. Assume $(\mathcal{N}, M_0)$ is live. Since $(\mathcal{N}, M_0)$ is also bounded by (b), it is well-formed. We have seen that every well-formed net has a positive T-invariant. This is a contradiction since the only T-invariant of $\mathcal{N}$ is the trivial invariant which is not positive. Therefore, $(\mathcal{N}, M_0)$ is not live. In particular, this implies that both $(\mathcal{N}, M)$ and $(\mathcal{N}, M')$ are not live.

Solution 6.2

(a) A set $Q \subseteq P$ is a siphon iff ${}^\bullet Q \subseteq Q^\bullet$. This is the case if for all transitions $t \in T$, if for some $p \in t^\bullet$ we have $p \in Q$, then for some $p' \in {}^\bullet t$ we have $p' \in Q$. This condition, applied to the four transitions t_1, t_2, t_3, t_4 of $\mathcal{N}$, results in the following conditions for any siphon Q:

$$\begin{aligned} (p_1 \in Q \vee p_3 \in Q) &\Rightarrow p_1 \in Q \\ p_3 \in Q &\Rightarrow (p_1 \in Q \vee p_2 \in Q) \\ p_4 \in Q &\Rightarrow p_3 \in Q \\ (p_2 \in R \vee p_4 \in Q) &\Rightarrow p_4 \in Q \end{aligned}$$

We are looking for minimal proper siphons, so siphons of size at least one. It is easy to that $Q = \{p_1\}$ is the only siphon of size one, and it is our first minimal proper siphon. Then no other minimal siphon can contain p_1, and actually there is no other minimal proper siphon: if either $p_2 \in Q$, $p_3 \in Q$ or $p_4 \in Q$, then the constraints imply $p_1 \in Q$.

(b) From (a) we have that $Q = \{p_1\}$ is a proper siphon. Since Q is not marked by M_0, we conclude that $(\mathcal{N}, M_0)$ is not live. □

Solution 6.3

(a) Assume $M \sim M_0$, $M(p_3) \geq 1$ and $M(q_5) \geq 1$. We then need to have $I_k \cdot M = I_k \cdot M_0$ for $k \in \{1, 2, 3, 4, 5, 6\}$. We can then derive

$$\dfrac{\dfrac{\dfrac{I_1 \cdot M = I_1 \cdot M_0}{\sum_{i=1}^{3} M(p_i) = 1} \quad M(p_3) \geq 1}{M(p_1) = 0,\, M(p_2) = 0,\, M(p_3) = 1} \quad \dfrac{I_2 \cdot M = I_2 \cdot M_0}{M(p_2) + M(p_3) + M(x_f) = 1}}{M(x_f) = 0} \quad \dfrac{I_3 \cdot M = I_3 \cdot M_0}{M(x_t) + M(x_f) = 1}}{M(x_t) = 1}$$

and

$$\dfrac{\dfrac{\dfrac{I_4 \cdot M = I_4 \cdot M_0}{\sum_{i=1}^{5} M(q_i) = 1} \quad M(q_5) \geq 1}{M(\{q_1, q_2, q_3, q_4\}) = 0,\, M(q_5) = 1} \quad \dfrac{I_5 \cdot M = I_5 \cdot M_0}{M(q_2) + M(q_3) + M(q_5) + M(y_f) = 1}}{M(y_f) = 0} \quad \dfrac{I_6 \cdot M = I_6 \cdot M_0}{M(y_t) + M(y_f) = 1}}{M(y_t) = 1}$$

from which it follows that $M = \{p_3, x_t, q_5, y_t\}$. We have that M agrees with M_0 on $I_1, \ldots, I_6$, and as these are a basis, also on all invariants. Therefore we have $M \sim M_0$. This means using only invariants (or the marking equation over the rationals), we can not conclude that M is not reachable from M_0.

(b) As the invariants in (a) were inconclusive in determining if a marking M with $M(p_3) \geq 1$ and $M(q_5)$ is reachable, we now use traps to show that the M of (a) is not reachable. We want to find a trap R such that $M_0(R) > 0$ and $M(R) = 0$, therefore violating the fundamental property of traps for reachable markings.

It suffices to look at the largest unmarked trap in M, derived with the fixed-point algorithm for siphons from the lecture, adapted to traps by switching pre- and postsets. Initially, we set $R = \{s \in S \mid M(s) = 0\}$. We then obtain:

$$\begin{aligned} R &= \{p_1, p_2, x_f, q_1, q_2, q_3, q_4, y_f\} = S \setminus \{p_3, x_t, q_5, y_t\} \\ {}^\bullet R &= \{s_1, s_2, s_3, s_4, t_1, t_2, t_3, t_4, t_5, t_6, t_7\} = T \\ R^\bullet &= \{s_1, s_2, s_3, t_1, t_2, t_3, t_4, t_5, t_6\} = T \setminus \{s_4, t_7\} \end{aligned}$$

We have $R^\bullet \subseteq {}^\bullet R$, so R is already a trap and our solution to the largest unmarked trap at M.

With $M_0 = \{p_1, x_f, q_1, y_f\}$ we have $M_0(R) = 4 > 0$. As $M(R) = 0$, by the fundamental property of traps, we then obtain that M is not reachable from M_0. We showed in (a) that this M is the only M with $M(p_3) \geq 1$ and $M(q_5) \geq 1$ satisfying $M \sim M_0$, and thus also the only M for which the marking equation has a solution. With our trap R it then follows that there is no such M where both $M \sim M_0$ and $M(R) > 0$ hold, so no such M is reachable. This shows that the algorithm satisfies mutual exclusion.

★ The minimal trap $R' = \{p_2, q_2, q_3, x_f, y_f\} \subseteq R$ would also be sufficient to show this property.

Solution 6.4

(a) The answer of `Z3` is `sat`, so the marking equation has a solution. Therefore we can not infer whether M is reachable from M_0 or not from this information alone.

(b) Any trap R satisfies $R^\bullet \subseteq {}^\bullet R$ and therefore $\forall t \in T : \exists s \in {}^\bullet t : s \in R \implies \exists s' \in t^\bullet : s' \in R$. This can be encoded with the following formula:

$$\bigwedge_{t \in T} \left(\left(\bigvee_{p \in {}^\bullet t} r_p \right) \implies \left(\bigvee_{p' \in t^\bullet} r'_p \right) \right)$$

Any assignment satisfying the formula gives rise to a set R which satisfies the trap condition and is therefore a trap.

For the given net, the constraints are as follows:

$$\begin{aligned} r_{p_1} &\implies r_{p_2} \vee r_{p_3} \\ r_{p_1} &\implies r_{p_4} \vee r_{p_5} \\ r_{p_2} &\implies r_{p_6} \\ r_{p_3} &\implies r_{p_7} \\ r_{p_4} &\implies r_{p_6} \\ r_{p_5} &\implies r_{p_7} \\ r_{p_6} \vee r_{p_7} &\implies r_{p_1} \end{aligned}$$

The constraints in SMT format are given in the file `pn_6-4_traps_completed_b.smt`. When `Z3` is invoked on it, the answer is `sat` and the model which assigns `false` to every variable, so the model corresponds to the empty trap $R = \{\}$.

Note: As `Z3` can return any solution, the output and trap found might differ on other systems.

(c) To ensure that the trap is marked at M_0 and unmarked at M, we can add the following constraint:

$$\left(\bigvee_{p \in S : M_0(p) > 0} r_p \right) \wedge \left(\bigwedge_{p \in S : M(p) > 0} \neg r_p \right)$$

For the given markings M_0 and M, the constraint is as follows:

$$r_{p_1} \wedge (\neg r_{p_2} \wedge \neg r_{p_5})$$

The constraints in SMT format are given in the file `pn_6-4_traps_completed_c.smt`.

When `Z3` is invoked on it, the answer is `sat` and the model which assigns `true` to p_1, p_3, p_4, p_6, p_7 and `false` to p_2 and p_5. This corresponds to the trap $R = \{p_1, p_3, p_4, p_6, p_7\}$ As the trap is marked at M_0, it needs to stay marked in any reachable marking, therefore the marking M is not reachable.