Petri Nets Coverability

Answer sketches for Home Assignment 2

To hand in before or on February 12, 2014.

February

27	28	29	30	31		
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16

Electronic versions (PDF only) can be sent by email to ⟨schmitz@lsv.ens-cachan.fr⟩, paper versions should be handed in on the 12th or put in my mailbox at LSV, ENS Cachan. **No delays**.

The numbers in the margins next to exercises are indications of time and difficulty.

This assignment is concerned with the *coverability* problem in Petri nets. Formally, given a Petri net $\mathcal{N}$ with set of places P, a source marking m_s in $\mathbb{N}^P$, and a target marking m_t in $\mathbb{N}^P$, the problem asks whether there exists m in $\mathbb{N}^P$ such that $m_s \to_{\mathcal{N}}^* m$ and $m \geq m_t$.

Here (and in the remainder of this assignment), the ordering is the *product ordering* over $\mathbb{N}^P$, defined by $m \leq m'$ if and only if $m(p) \leq m'(p)$ for all p in P.

The main application in verification is to check safety properties in concurrent systems, where the target marking represents an undesired state that we wish to avoid.

1 Large Coverability Graphs

We start by demonstrating that the algorithm studied in class for coverability, which first constructs the coverability graph of the Petri net, and then checks whether the target marking is covered in the coverability graph, has a non-elementary complexity:

Exercise 1 (A Non-Elementary Coverability Graph)**.** Consider the Petri net depicted in Figure 1. We fix a linear ordering $q_0, q_1, q_2, p_0, p'_0, p_1, p_2$ over its places, so that markings in $\mathbb{N}^P$ can be seen as vectors in $\mathbb{N}^7$.

[0] 1. Show that $m(q_0) + m(q_1) + m(q_2) = 1$ in any reachable marking m.

[1] 2. Assume that $n = 0$. Show that a marking m with $m(q_0) = 1$ and $m(p_0) = 2^k$ is reachable.

We show by induction that, for all $i \leq k$, the marking $\langle 1, 0, 0, 2^i, 0, k-i, 0\rangle$ is reachable. For the base case $i = 0$, this is the initial marking. For the induction step, assuming $i < k$, by induction hypothesis we reach $\langle 1, 0, 0, 2^i, 0, k-i, 0\rangle$. Then the sequence of transitions $u_i \stackrel{\text{def}}{=} b^{2^i} dc^{2^{i+1}} a$ yields the marking $\langle 1, 0, 0, 2^{i+1}, 0, k-i-1, 0\rangle$ as desired. □

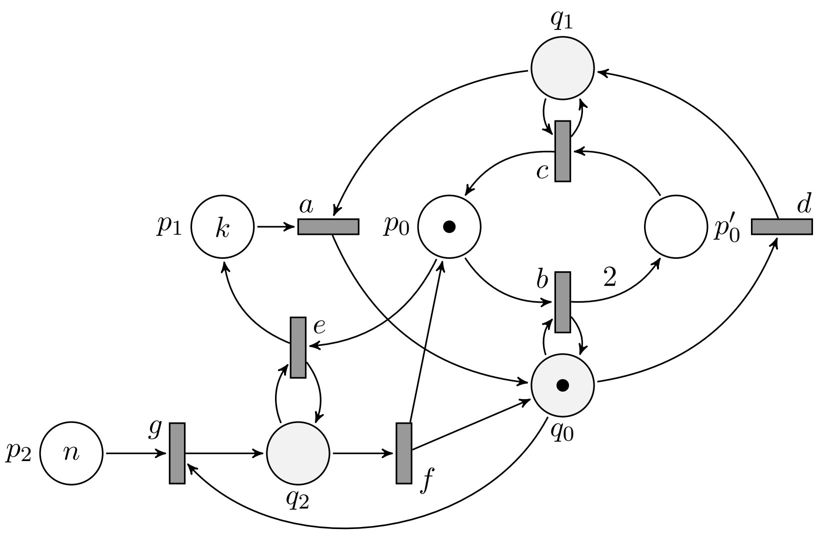

Figure 1: A Petri net.

[1] 3. Assume $k = 0$ and define $\text{tower}(0) \stackrel{\text{def}}{=} 1$ and $\text{tower}(n+1) \stackrel{\text{def}}{=} 2^{\text{tower}(n)}$. Show that a marking m with $m(q_0) = 1$ and $m(p_0) = \text{tower}(n)$ is reachable.

We show by induction that, for all $j \leq n$, the marking $\langle 1, 0, 0, \text{tower}(j), 0, 0, n - j\rangle$ is reachable. For the base case $j = 0$, this is indeed the initial marking. For the induction step, assuming $j < n$, by induction hypothesis we can reach $\langle 1, 0, 0, \text{tower}(j), 0, 0, n - j\rangle$. Then the sequence $v_j \stackrel{\text{def}}{=} ge^{\text{tower}(j)}f$ yields the marking

$$\langle 1, 0, 0, 1, 0, \text{tower}(j), n - j - 1\rangle ,$$

from which the sequence $u_0 \cdots u_{\text{tower}(j)-1}$ yields the desired marking

$$\langle 1, 0, 0, \text{tower}(j + 1), 0, 0, n - j - 1\rangle$$

according to the previous question. □

[2] 4. Show that any sequence of markings $m_0, m_1, \ldots$ with $m_i \to m_{i+1}$ for all i is *bad*, i.e. satisfies $m_i \not\leq m_j$ for all $i < j$. Deduce that the coverability graph for this Petri net has non-elementary size.

It suffices to show that $m_j(p) < m_i(p)$ for some place p:

- If transition g is fired at least once between steps i and j, then $m_j(p_2) < m_i(p_2)$.
- Otherwise, if g is never fired and f is fired at least once, then $m_j(q_2) < m_i(q_2)$.
- Otherwise, if g, f are never fired, and e is fired at least once, then $m_i(q_1) = m_j(q_1) = m_i(q_1) = m_j(q_1) = 0$, i.e. only e can be fired, thus $m_j(p_0) < m_i(p_0)$.

- Otherwise, if g, f, e are never fired, then we can ignore p_2 and q_2. If a is fired at least once, then $m_j(p_1) < m_i(p_1)$.
- Otherwise, if g, f, e, a are never fired, and d is fired at least once, then $m_j(q_0) < m_i(q_0)$.
- Otherwise, if g, f, e, a, d are never fired, then either b is fired at least once and $m_j(p_0) < m_i(p_0)$, or c is fired at least once and $m_j(p'_0) < m_i(p'_0)$.

Then, the coverability graph for this Petri net does not have any ω-value, hence it has to explicitly contain all the markings leading to tower(n). □

In fact, by extending the construction of the exercise, one can show that the coverability graph can be of non primitive-recursive size.

2 Backward Chaining

Let us recall that a well-quasi-order (wqo) is a quasi-order $(A, \leq)$ with the additional property that, if $x_0, x_1, \ldots$ is an infinite sequence of elements of A, then there exist two indices $i < j$ such that $x_i \leq x_j$. In particular, $(\mathbb{N}^P, \leq)$ for P finite is a wqo.

Exercise 2 (Ascending Chains Condition)**.** Let $(A, \leq)$ be a quasi-order. The *upward-closure* of a subset X of A is $\uparrow X \stackrel{\text{def}}{=} \{y \in A \mid \exists x \in X. x \leq y\}$. A subset U of A is *upward-closed* if $U = \uparrow U$.

[2] Show that a quasi-order $(A, \leq)$ is a well-quasi-order (wqo) if and only if any increasing sequence $U_0 \subseteq U_1 \subseteq U_2 \subseteq \cdots$ of upward-closed subsets of A eventually *stabilizes*, i.e., $\exists i \in \mathbb{N}$ s.t. $U_i = U_{i+1} = \cdots = U_{i+k}$ for all k.

Assume that the ascending chains condition holds. Consider an infinite sequence $x_0, x_1, \ldots$ over A, and build the sequence $\uparrow\{x_0\} \subseteq \uparrow\{x_0, x_1\} \subseteq \cdots$ of upward-closed subsets of A. Then the latter sequence stabilizes at rank j, i.e. $\uparrow\{x_0, \ldots, x_{j-1}, x_j\} \subseteq \uparrow\{x_0, \ldots, x_{j-1}\}$, which means $x_j \in \uparrow\{x_0, \ldots, x_{j-1}\}$. Thus $\exists 0 \leq i < j$ such that $x_i \leq x_j$.

Conversely, assume that $(A, \leq)$ is a wqo, and consider an increasing sequence $U_0 \subseteq U_1 \subseteq U_2 \subseteq \cdots$ of upward-closed subsets of A. Whenever $U_{i_j+1} \not\subseteq U_{i_j}$, extract an element x_{i_j} from $U_{i_j+1} \setminus U_{i_j}$, and observe that $j < k$ implies $x_{i_j} \not\leq x_{i_k}$ since the U_i's are upward-closed. If the sequence $U_0 \subseteq U_1 \subseteq U_2 \subseteq \cdots$ does not stabilize, then we have exhibited an infinite bad sequence $x_{i_0}, x_{i_1}, \ldots$ over A, a contradiction. □

Exercise 3 (Finite Basis Property)**.** Let $(A, \leq)$ a wqo.

[1] 1. For a subset X of A, we say that x is a *minimal* element of X if x is in X and for all y in X, $y \not< x$, and write $\min(X) \stackrel{\text{def}}{=} \{x \in X \mid \forall y \in X. y \not< x\}$, where $< \stackrel{\text{def}}{=} \leq \setminus \geq$. Show that every element of X is larger or equal to a minimal element of X.

   Assume for the sake of contradiction that there exists x_0 in X such that, for all $y \in \min(X)$, $y \not\leq x_0$. In particular, x_0 does not belong to $\min(X)$, hence there exists x_1 in X with $x_1 < x_0$. Now, $x_1 \leq x_0$ thus x_1 cannot belong to $\min(X)$, and we can find $x_2 < x_1$. Pursuing this construction, we obtain an infinite bad sequence $x_0 > x_1 > \cdots$ over $(A, \leq)$, a contradiction.

[1] 2. Let us write $\equiv \stackrel{\text{def}}{=} \leq \cap \geq$ for the equivalence generated by $\leq$. For a subset U of A, write $U/\equiv$ for its quotient by $\equiv$. Note that $\leq$ becomes a partial ordering over the equivalence classes in $U/\equiv$. Show that $\min(U/\equiv)$ is finite.

It suffices to show that $\min(U/\equiv)$ is an antichain, since any antichain is necessarily finite over a wpo. Let $[x]$ and $[y]$ be two elements of $U/\equiv$, and assume $[x] \leq [y]$. Since $[x] \not< [y]$ and $\leq$ is a partial ordering over $U/\equiv$, this entails $[x] = [y]$.

[1] 3. Show that any upward-closed $U \subseteq A$ can be written as $U = \uparrow B$ for some finite $B \subseteq A$: B is then called a *finite basis* for U.

For each equivalence class $[x]$ in $U/\equiv$, we pick a representative $r([x])$ in $[x]$. Define

$$B \stackrel{\text{def}}{=} r(\min(U/\equiv)) .$$

Since $(A, \leq)$ is a wqo, B is finite. Furthermore, if y is in U, then there exists $[x]$ in $\min(U/\equiv)$ s.t. $[x] \leq [y]$, i.e. there exists $r([x])$ in B s.t. $r([x]) \leq r([y]) \leq y$ by transitivity of $\leq$, hence $U \subseteq \uparrow B$.

For the converse inclusion, consider some $y \in A$ with $r([x]) \leq y$ for some $[x]$ in $\min(U/\equiv)$. Then $x \leq r([x]) \leq y$ and $x \in U$, hence $y \in U$ since U is upward-closed, i.e. $\uparrow B \subseteq U$. □

Exercise 4 (Backward Chaining Algorithm)**.** Fix a coverability instance $\langle \mathcal{N}, m_s, m_t \rangle$ where $\mathcal{N} = \langle P, T, W, m_s \rangle$ is a Petri net with a finite set of places P, a finite set of transitions T, transition weights $W \colon (P \times T) \cup (T \times P) \to \mathbb{N}$, and initial marking m_s in $\mathbb{N}^P$, and m_t is a target marking in $\mathbb{N}^P$.

[1] 1. Let U be an upward-closed set included in $\mathbb{N}^P$. Show that

$$\mathrm{Pre}(U) \stackrel{\text{def}}{=} \{m \in \mathbb{N}^P \mid \exists m' \in U . m \to_{\mathcal{N}} m'\}$$

is upward-closed.

Assume $m_1 \in \mathrm{Pre}(U)$ and $m_1' \geq m_1$. Then there exists $m_2 \in U$ with $m_1 \xrightarrow{t}_{\mathcal{N}} m_2$ for some $t \in T$, which also yields $m_1' \xrightarrow{t}_{\mathcal{N}} m_2'$ for some $m_2' \geq m_2$. Since U is upward-closed, this entails $m_1' \in \mathrm{Pre}(U)$. □

[1] 2. For a marking m in $\mathbb{N}^S$ for some finite S, define its *norm* $\|m\|$ as $\max_{s \in S} m(s)$. For a finite set B of markings in $\mathbb{N}^S$, define its norm as $\|B\| \stackrel{\text{def}}{=} \max_{m \in B} \|m\|$ and write $|B|$ for its cardinality. We also write $\|T\|$ for $\max(\|W_{\restriction P \times T}\|, \|W_{\restriction T \times P}\|)$.

Let B be a finite set included in $\mathbb{N}^P$. Show that we can compute a finite basis B' for $\uparrow B \cup \mathrm{Pre}(\uparrow B)$ in time $O(|B| \cdot |T| \cdot |P| \cdot \log(\|B\| + \|T\|))$ and satisfying $\|B'\| \leq \|B\| + \|W_{\restriction_{P\times T}}\|$.

Let

$$B'' \stackrel{\text{def}}{=} \{(0^P \sqcup (m - W(t, P))) + W(P, t) \mid m \in B\}$$

where $\sqcup$ denotes the lub operation in $\mathbb{Z}^P$, i.e. the componentwise maximum. Then $B'' \subseteq \mathbb{N}^P$ can be computed in time $O(|B| \cdot |T| \cdot |P| \cdot \log(\|B\| + \|T\|))$ by computing the effect of every transition in T on every marking in B. It satisfies $\|B''\| \leq \|B\| + \|W_{\restriction_{P\times T}}\|$. The answer then follows by setting $B' \stackrel{\text{def}}{=} B \cup B''$. □

[0] 3. Deduce that $B_{\min} \stackrel{\text{def}}{=} \min(\uparrow B \cup \mathrm{Pre}(\uparrow B))$ can be computed in time $O(|B|^2 \cdot |T|^2 \cdot |P| \cdot \log(\|B\| + \|T\|))$ and satisfies $\|B_{\min}\| \leq \|B\| + \|W_{\restriction_{P\times T}}\|$.

[2] 4. Consider the following sequence of sets of markings $(C_i)_i$:

$$C_0 \stackrel{\text{def}}{=} \uparrow\{m_t\}\ , \qquad C_{i+1} \stackrel{\text{def}}{=} C_i \cup \mathrm{Pre}(C_i)\ .$$

Show that $(C_i)_i$ stabilizes to some set C_ℓ for some $\ell \in \mathbb{N}$. Show that

$$C_i = \{m \in \mathbb{N}^P \mid \exists m' \in \mathbb{N}^P. \exists j \leq i. m' \geq m_t \wedge m \to^j_{\mathcal{N}} m'\}\ ,$$

i.e. that C_i is exactly the set of markings that cover m_t in i or less steps.

For the first point, each C_i is upward-closed by induction over i, and $C_i \subseteq C_{i+1}$ for every i, thus by the ascending chain condition the family $(C_i)_i$ stabilizes.

For the second point, we proceed by induction over i. The base case holds trivially, and for the induction step, we have that m belongs to $C_{i+1} \setminus C_i$ iff there exists m' in C_i such that $m \to_{\mathcal{N}} m'$. By induction hypothesis, m' belongs to C_i iff there exists $j \leq i$ and $m'' \geq m_t$ s.t. $m' \to^j_{\mathcal{N}} m''$, hence $m \to^{j+1}_{\mathcal{N}} m''$, but $j + 1 > i$ since $m \notin C_i$, hence $i = j$. □

[1] 5. Let $B_i \stackrel{\text{def}}{=} \min C_i$ for all i. Deduce an algorithm for coverability that employs the $(B_i)_i$ sequence.

We construct the sequence of sets $(B_i)_i$ by

$$B_0 = \{m_t\}\ , \qquad B_{i+1} = \min(\uparrow B_i \cup \mathrm{Pre}(\uparrow B_i))\ .$$

Then by induction over i, we can check that $B_i = \min(C_i)$ and $C_i = \uparrow B_i$.

Since $(C_i)_i$ eventually stabilizes and since we are working over a wpo, so does $(B_i)_i$. Each step of the computation of the B_i's is effective, and checking whether $B_i = B_{i+1}$ can be undertaken in

$$O(|P| \cdot |B_i| \cdot |B_{i+1}| \cdot \log(\|B_i\| + \|B_{i+1}\|))\ .$$

Thus we can effectively compute $(B_i)_{0\leq i\leq \ell}$. It only remains to check whether $m_s \in \uparrow B_\ell$, in time

$$O(|P| \cdot |B_\ell| \cdot \log(\|B_\ell\| + \|m_s\|)) .$$

□

[1] 6. Let $b \stackrel{\text{def}}{=} \max_{0\leq i\leq \ell} \|B_i\|$ and $c \stackrel{\text{def}}{=} \max_{0\leq i\leq \ell} |B_i|$. Give bounds on b and c in terms of ℓ, $\|m_t\|$, $\|W_{\restriction_{P\times T}}\|$, and $|P|$. Deduce that the algorithm works in time

$$2^{O(|P|\cdot\log(\|m_t\|+\ell\cdot\|T\|))} \cdot |T|^2 \cdot \log(\|m_s\|) .$$

By Question 3, $b \leq \|m_t\| + \ell \cdot \|W_{\restriction_{P\times T}}\|$. Thus $c \leq (b+1)^{|P|}$. The overall complexity should take into account ℓ steps of computation, each with complexity

$$O(c^2 \cdot |T|^2 \cdot |P| \cdot \log(b + \|T\|))$$

plus ℓ checks for stabilization in

$$O(c^2 \cdot |P| \cdot \log b)$$

and a final membership test for m_s in

$$O(c \cdot |P| \cdot \log(b + \|m_s\|)) .$$

Note that the stabilization check is basically for free in a concrete algorithm where the elements of B'' are checked against $\uparrow B$ as they are constructed.

The overall complexity is thus in

$$O(\ell \cdot c^2 \cdot |T|^2 \cdot |P| \cdot \log(b + \|T\| + \|m_s\|)) \subseteq 2^{O(|P|\cdot\log(\|m_t\|+\ell\cdot\|T\|))} \cdot |T|^2 \cdot \log(\|m_s\|)$$ □

3 Complexity Upper Bounds

The missing information in order to bound the complexity of the backward chaining algorithm for coverability is an upper bound on ℓ, the stabilization rank. One could extract upper bounds on ℓ from so-called length function theorems for Dickson's Lemma, but they will be too high for our problem here.

Instead, assume that we can cover m_t from m_s. We are going to prove an upper bound on the minimal rank i such that m_s belongs to C_i, working for this by induction over P the set of places. This is actually pretty simple, but requires quite a bit of notation.

We consider for this the *projected net* $\mathcal{N}_{\restriction_I}$ for $I \subseteq P$: it has place set I, transition set T, weights $W_{\restriction_{I\times T\cup T\times I}}$, and initial marking $m_{s\restriction_I}$ in $\mathbb{N}^I$. Note that $\|m_{\restriction_I}\| \leq \|m\|$ for all m in $\mathbb{N}^P$, and similarly $\|W_{\restriction_{I\times T}}\| \leq \|W_{\restriction_{P\times T}}\|$. We call an *$I$-witness from m_1* a sequence $m_1, \ldots, m_n$ of markings in $\mathbb{N}^I$ with $m_n \geq m_{t\restriction_I}$ and $m_i \rightarrow_{\mathcal{N}_{\restriction_I}} m_{i+1}$ for all $1 \leq i < n$. A *coverability witness* is a P-witness from m_s.

Exercise 5 (Upper Bound on Coverability Witnesses)**.** For $I \subseteq P$ and m in $\mathbb{N}^I$, let us define $\ell(I, m)$ as the minimal length of an I-coverability witness from m, and set $\ell(I, m) = 0$ if no such witness exists. We further define

$$M(I) \stackrel{\text{def}}{=} \sup_{m \in \mathbb{N}^I} \ell(I, m) \ .$$

[0] 1. Show that $M(\emptyset) = 1$ for the base case.

A Petri net with no places has the zero-dimensional marking for initial marking, which equals the also zero-dimensional $m_{t{\restriction_\emptyset}}$. □

2. For the induction step, let $I \neq \emptyset$. We want to bound $M(I)$ using $M \stackrel{\text{def}}{=} \max_{I' \subsetneq I} M(I')$. To this end, we define

$$L \stackrel{\text{def}}{=} M \cdot \|W_{\restriction_{P \times T}}\| + \|m_t\|$$

and prove that, for every marking m_1 in $\mathbb{N}^I$, if there exists an I-witness $w = m_1, \ldots, m_n$ of minimal length from m_1, then

$$n \leq L^{|I|} + M \ . \qquad (*)$$

[1] (a) Let us call w *L-bounded* if $m_i(p) < L$ for all $1 \leq i \leq n$ and p in I. Show that, if w is L-bounded, then $(*)$ holds.

We can assume all the markings in w to be distinct, otherwise we could avoid a loop in the sequence and obtain a shorter one, contradicting the minimality of w. There are at most $L^{|I|}$ distinct markings bounded by L, hence $(*)$ holds in this case. □

[1] (b) Assume the contrary: we can split w as w_1, w_2 such that w_1 is L-bounded and w_2 starts with a marking m_j such that $m_j(p) \geq L$ for some (maybe several) p in I. Show that $(*)$ also holds.

By the same reasoning as in Question (a), w_1 can be chosen of length bounded by $L^{|I|}$. Because w_2 starts with a place p where $m_j(p) \geq L$, we can consider the places in $I' = I \setminus \{p \mid m_j(p) \geq L\}$ and project w_2 on I': by definition of M, $w_{2{\restriction_{I'}}}$ can be chosen of length at most M. Looking at the corresponding unprojected witness, we still manage to end with a marking $m_n(p) \geq m_t(p)$ for all p in $I \setminus I$ since it can only decrease by $\|W_{\restriction_{P \times T}}\|$ at each of its M steps. □

[1] 3. Let $N \stackrel{\text{def}}{=} \|W_{\restriction_{P \times T}}\| + \|m_t\| + 2$. Show that $M(P) \leq N^{(3 \cdot |P|)!}$.

By induction over P: for $\emptyset$, $M(\emptyset) \leq 1 < N = N^{0!}$. For the induction step, by $(*)$,

$$\begin{aligned} M(I) &\leq (N \cdot M)^{|I|} + M \\ &\leq (N \cdot M)^{|I|+1} && \text{(since } N \geq 2) \\ &\leq N^{((3(|I|-1))!+1)(|I|+1)} && \text{(by ind. hyp.)} \\ &\leq L^{(3|I|)!} \ . \end{aligned}$$

□

Exercise 6 (Complexity of Coverability Algorithms)**.** Given a Petri net $\mathcal{N} = \langle P, T, W, m_s\rangle$ and a marking m_t, set $N \stackrel{\text{def}}{=} 2 + \|W_{\restriction P\times T}\| + \|m_t\|$.

[1] 1. Assuming that the size n of the instance $\langle \mathcal{N}, m_s, m_t\rangle$ of the coverability problem is at least

$$\max(\log N, |P|, \log \|W_{\restriction T\times P}\|, \log \|m_s\|)\ ,$$

deduce that, if m_t is coverable from m_s, then there is a coverability witness of length at most $2^{2^{c\cdot n\log n}}$ for some constant c.

If $\mathcal{N}$ covers m_t, then there is a coverability witness of length at most $M(P)$. By Exercise 5 $M(P) \leq N^{(3|P|)!} \leq (2^n)^{(3n)!} \leq 2^{2^{cn\log n}}$ for some constant c.

[3] 2. Let us exploit this bond for the backward chaining algorithm. Show that we can adapt the backward chaining algorithm to work in 2-ExpTime.

Let us first show that, if we can cover m_t from m_s, then m_s belongs to $C_{\ell(P,m_s)}$: by definition of $\ell(P, m_s)$, there is a coverability witness of length $\ell(P, m_s)$, hence by Exercise 4.4, $m_s \in C_{\ell(P,m_s)}$. Remember that $\ell(P, m_s) \leq M(P) \leq 2^{2^{cn\log n}}$ for some constant c.

Thus a new version of the backward chaining algorithm terminates at the minimal rank ℓ such that at least one of the three conditions is fulfilled:

(a) saturation: $B_\ell = B_{\ell+1}$ (and then accept iff $m_s \in \uparrow B_\ell$),

(b) witness: $m_s \in \uparrow B_\ell$ (and then accept),

(c) timeout: $\ell > 2^{2^{cn\log n}}$ for the same constant c (and then reject).

Since the only new check for (c) can rely on an exponential time pre-computation, it does not modify the complexity of the algorithm, which is by Exercise 4.6 in

$$2^{O(|P|\cdot n\cdot 2^{cn\log n+n})} \cdot n^3 \subseteq 2^{2^{O(n\log n)}}$$

A closer look at the bound computed in Exercise 5.3 allows to avoid the new termination checks: more generally, for any marking m, if m can cover m_t in the Petri net, then there is a witness of length at most $\ell = N^{3\cdot|P|!}$, where N does not depend on m (but depends on $\|W_{\restriction P\times T}\| + \|m_t\|$). This entails that the saturation length is at most ℓ. Indeed, assume for the sake of contradiction that there exists a marking m in $C_{\ell+1} \setminus C_\ell$. By Exercise 4.4, this means that there does not exist any marking $m' \geq m_t$ and $j \leq \ell$ such that $m \rightarrow^j_{\mathcal{N}} m'$, contradicting the bound ℓ. □

[2] 3. Another way of exploiting this bound is to use a *combinatorial algorithm*, which searches for a coverability witness of length at most $2^{2^{c \cdot n \log n}}$ for some constant c, and concludes that none exists if none can be found. Show that this is an ExpSpace algorithm.

A nondeterministic algorithm in NExpSpace can proceed to find this witness: it requires a counter for the current length, which uses space at most $2^{cn \log n}$, and counters for each of the P places, which can each hold values of at most $2^{2^{cn \log n}} \cdot \|W_{\restriction_{T \times P}}\| + \|m_s\| \leq 2^{2^{cn \log n}+n} + 2^n$, thus each using space at most $2^{dn \log n}$ for some constant d.

By Savitch's Theorem, NExpSpace = ExpSpace.