Universal Safety for Timed Petri Nets is PSPACE-complete

Citation for published version:

Digital Object Identifier (DOI):
10.4230/LIPIcs.CONCUR.2018.6

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:
29th International Conference on Concurrency Theory (CONCUR 2018)

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.
Universal Safety for Timed Petri Nets is PSPACE-complete

Parosh Aziz Abdulla
Uppsala University, Sweden

Mohamed Faouzi Atig
Uppsala University, Sweden

Radu Ciobanu
University of Edinburgh, UK

Richard Mayr
University of Edinburgh, UK

Patrick Totzke
University of Edinburgh, UK

Abstract

A timed network consists of an arbitrary number of initially identical 1-clock timed automata, interacting via hand-shake communication. In this setting there is no unique central controller, since all automata are initially identical. We consider the universal safety problem for such controller-less timed networks, i.e., verifying that a bad event (enabling some given transition) is impossible regardless of the size of the network.

This universal safety problem is dual to the existential coverability problem for timed-arc Petri nets, i.e., does there exist a number \( m \) of tokens, such that starting with \( m \) tokens in a given place, and none in the other places, some given transition is eventually enabled.

We show that these problems are PSPACE-complete.

2012 ACM Subject Classification Theory of computation → Timed and hybrid models

Keywords and phrases timed networks, safety checking, Petri nets, coverability

Digital Object Identifier 10.4230/LIPIcs.CONCUR.2018.6

Funding This work was supported by the EPSRC, grant EP/M027651/1.

1 Introduction

Background. Timed-arc Petri nets (TPN) [4, 16, 3, 8, 13] are an extension of Petri nets where each token carries one real-valued clock and transitions are guarded by inequality constraints where the clock values are compared to integer bounds (via strict or non-strict inequalities). The known models differ slightly in what clock values newly created tokens can have, i.e., whether newly created tokens can inherit the clock value of some input token, or whether newly created tokens always have clock value zero. We consider the former, more general, case.

Decision problems associated with the reachability analysis of (extended) Petri nets include Reachability (can a given marking reach another given marking?) and Coverability (can a given marking ultimately enable a given transition?).

While Reachability is undecidable for all these TPN models [15], Coverability is decidable using the well-quasi ordering approach of [1, 10] and complete for the hyper-Ackermannian
complexity class $F_{\omega \omega}$ [12]. With respect to Coverability, TPN are equivalent [7] to (linearly ordered) data nets [14].

The Existential Coverability problem for TPN asks, for a given place $p$ and transition $t$, whether there exists a number $m$ such that the marking $M(m) = m \cdot \{(p,0)\}$ ultimately enables $t$. Here, $M(m)$ contains exactly $m$ tokens on place $p$ with all clocks set to zero and no other tokens. This problem corresponds to checking safety properties in distributed networks of arbitrarily many (namely $m$) initially identical timed processes that communicate by handshake. A negative answer certifies that the ‘bad event’ of transition $t$ can never happen regardless of the number $m$ of processes, i.e., the network is safe for any size. Thus by checking existential coverability, one solves the dual problem of Universal Safety. (Note that the $m$ timed tokens/processes are only initially identical. They can develop differently due to non-determinacy in the transitions.)

The corresponding problem for timed networks studied in [2] does not allow the dynamic creation of new timed processes (unlike the TPN model which can increase the number of timed tokens), but considers multiple clocks per process (unlike our TPN with one clock per token).

The TPN model above corresponds to a distributed network without a central controller, since initially there are no tokens on other places that could be used to simulate one. Adding a central controller would make Existential Coverability polynomially inter-reducible with normal Coverability and thus complete for $F_{\omega \omega}$ [12] (and even undecidable for $> 1$ clocks per token [2]).

Aminof et. al. [6] study the model checking problem of $\omega$-regular properties for the controller-less model and in particular claim an EXPSPACE upper bound for checking universal safety. However, their result only holds for discrete time (integer-valued clocks) and they do not provide a matching lower bound.

Our contribution. We show that Existential Coverability (and thus universal safety) is decidable and PSPACE-complete. This positively resolves an open question from [2] regarding the decidability of universal safety in the controller-less networks. Moreover, a symbolic representation of the set of coverable configurations can be computed (using exponential space).

The PSPACE lower bound is shown by a reduction from the iterated monotone Boolean circuit problem. (It does not follow directly from the PSPACE-completeness of the reachability problem in timed automata of [5], due to the lack of a central controller.)

The main ideas for the PSPACE upper bound are as follows. First we provide a logspace reduction of the Existential Coverability problem for TPN to the corresponding problem for a syntactic subclass, non-consuming TPN. Then we perform an abstraction of the real-valued clocks, similar to the one used in [3]. Clock values are split into integer parts and fractional parts. The integer parts of the clocks can be abstracted into a finite domain, since the transition guards cannot distinguish between values above the maximal constant that appears in the system. The fractional parts of the clock values that occur in a marking are ordered sequentially. Then every marking can be abstracted into a string where all the tokens with the $i$-th fractional clock value are encoded in the $i$-th symbol in the string. Since token multiplicities do not matter for existential coverability, the alphabet from which these strings are built is finite. The primary difficulty is that the length of these strings can grow dynamically as the system evolves, i.e., the space of these strings is still infinite for a given TPN. We perform a forward exploration of the space of reachable strings. By using an acceleration technique, we can effectively construct a symbolic representation of the
set of reachable strings in terms of finitely many regular expressions. Finally, we can check existential coverability by using this symbolic representation.

2 Timed Petri Nets

We use $\mathbb{N}$ and $\mathbb{R}_{\geq 0}$ to denote the sets of nonnegative integers and reals, respectively. For $n \in \mathbb{N}$ we write $[n]$ for the set $\{0, \ldots, n\}$.

For a set $A$, we use $A^*$ to denote the set of words, i.e. finite sequences, over $A$, and write $\varepsilon$ for the empty word. If $R$ is a regular expression over $A$ then $L(R) \subseteq A^*$ denotes its language.

A multiset over a set $X$ is a function $M : X \to \mathbb{N}$. The set $X^{\oplus}$ of all (finitely supported) multisets over $X$ is partially ordered pointwise ($\preceq$). The multiset union of $M, M' \in X^{\oplus}$ is $(M \oplus M')(\alpha) \overset{\text{def}}{=} M(\alpha) + M'(\alpha)$ for all $\alpha \in X$. If $M \geq M'$ then the multiset difference $(M \ominus M')$ is the unique $M'' \in X^{\oplus}$ with $M = M' \oplus M''$. We will use a monomial representation and write for example $(\alpha + \beta^3)$ for the multiset $(\alpha \mapsto 1, \beta \mapsto 3)$. For a multiset $M$ and a number $m \in \mathbb{N}$ we let $m \cdot M$ denote the $m$-fold multiset sum of $M$. We further lift this to sets of numbers and multisets on the obvious fashion, so that in particular $\mathbb{N} \cdot S \overset{\text{def}}{=} \{n \cdot M \mid n \in \mathbb{N}, M \in S\}$.

Timed Petri nets are place/transition nets where each token carries a real value, sometimes called its clock value or age. Transition firing depends on there being sufficiently many tokens whose value is in a specified interval. All tokens produced by a transition either have age 0, or inherit the age of an input-token of the transition. To model time passing, all token ages can advance simultaneously by the same (real-valued) amount.

\begin{definition}[TPN] A timed Petri net (TPN) $\mathcal{N} = (P, T, \text{Var}, G, \text{Pre}, \text{Post})$ consists of finite sets of places $P$, transitions $T$ and variables $\text{Var}$, as well as functions $G, \text{Pre}, \text{Post}$ defining transition guards, pre- and postconditions, as follows.

For every transition $t \in T$, the guard $G(t)$ maps variables to (open, half-open or closed) intervals with endpoints in $\mathbb{N} \cup \{\infty\}$, restricting which values variables may take. All numbers are encoded in unary. The precondition $\text{Pre}(t)$ is a finite multiset over $(P \times \text{Var})$. Let $\text{Var}(t) \subseteq \text{Var}$ be the subset of variables appearing positively in $\text{Pre}(t)$. The postcondition $\text{Post}(t)$ is then a finite multiset over $(P \times (\{0\} \cup \text{Var}(t)))$, specifying the locations and clock values of produced tokens. Here, the symbolic clock value is either 0 (demanding a reset to age 0), or a variable that appeared already in the precondition. 

A marking is a finite multiset over $P \times \mathbb{R}_{\geq 0}$.
\end{definition}

\begin{example} The picture below shows a place/transition representation of an TPN with four places and one transition. $\text{Var}(t) = \{x, y\}$, $\text{Pre}(t) = (p, x^2 + (q, y), G(t)(x) = [0, 5], G(t)(y) = ]1, 2]$ and $\text{Post}(t) = (r, y^3 + (s, 0))$.

The transition $t$ consumes two tokens from place $p$, both of which have the same clock value $x$ (where $0 \leq x \leq 5$) and one token from place $q$ with clock value $y$ (where $1 < y \leq 2$). It produces three tokens on place $r$ who all have the same clock value $y$ (where $y$ comes from the clock value of the token read from $q$), and another token with value 0 on place $s$. 
\end{example}
There are two different binary step relations on markings: discrete steps $\rightarrow_t$ which fire a transition $t$ as specified by the relations $G$, $Pre$, and $Post$, and time passing steps $\rightarrow_d$ for durations $d \in \mathbb{R}_{\geq 0}$, which simply increment all clocks by $d$.

**Definition 3 (Discrete Steps).** For a transition $t \in T$ and a variable evaluation $\pi : Var \rightarrow \mathbb{R}_{\geq 0}$, we say that $\pi$ satisfies $G(t)$ if $\pi(x) \in G(t)(x)$ holds for all $x \in Var$. By lifting $\pi$ to multisets over $(P \times Var)$ (respectively, to multisets over $(P \times \{(0) \cup Var\})$ with $\pi(0) = 0$) in the canonical way, such an evaluation translates preconditions $Pre(t)$ and $Post(t)$ into markings $\pi(Pre(t))$ and $\pi(Post(t))$, where for all $p \in P$ and $c \in \mathbb{R}_{\geq 0}$,

$$\pi(Pre(t))(p,c) \overset{\text{def}}{=} \sum_{\pi(v)=c} Pre(t)(p,v) \quad \text{and} \quad \pi(Post(t))(p,c) \overset{\text{def}}{=} \sum_{\pi(v)=c} Post(t)(p,v).$$

A transition $t \in T$ is called enabled in marking $M$, if there exists an evaluation $\pi$ that satisfies $G(t)$ and such that $\pi(Pre(t)) \leq M$. In this case, there is a discrete step $M \rightarrow_t M'$ from marking $M$ to $M'$, defined as $M' = M \oplus \pi(Pre(t)) \oplus \pi(Post(t))$.

**Definition 4 (Time Steps).** Let $M$ be a marking and $d \in \mathbb{R}_{\geq 0}$. There is a time step $M \rightarrow_d M'$ to the marking $M'$ with $M'(p,c) \overset{\text{def}}{=} M(p,c-d)$ for $c \geq d$, and $M'(p,c) \overset{\text{def}}{=} 0$, otherwise. We also refer to $M'$ as $(M + d)$.

We write $\rightarrow_{\text{time}}$ for the union of all timed steps, $\rightarrow_{\text{Disc}}$ for the union of all discrete steps and simply $\rightarrow$ for $\rightarrow_{\text{Disc}} \cup \rightarrow_{\text{time}}$. The transitive and reflexive closure of $\rightarrow$ is $\rightarrow^*$. $\text{Cover}(M)$ denotes the set of markings $M'$ for which there is an $M'' \geq M'$ with $M \rightarrow^* M''$.

We are interested in the existential coverability problem ($\exists \text{COVER}$ for short), as follows.

**Input:** A TPN, an initial place $p$ and a transition $t$.

**Question:** Does there exist $M \in \text{Cover}(\mathbb{N} \cdot \{(p,0)\})$ that enables $t$?

We show that this problem is PSPACE-complete. Both lower and upper bound will be shown (w.l.o.g., see Lemma 8) for the syntactic subclass of non-consuming TPN, defined as follows.

**Definition 5.** A timed Petri net $(P, T, Var, G, Pre, Post)$ is non-consuming if for all $t \in T$, $p \in P$ and $x \in Var$ it holds that both 1) $Pre(t)(p,x) \leq 1$, and 2) $Pre(t) \leq Post(t)$.

In a non-consuming TPN, token multiplicities are irrelevant for discrete transitions. Intuitively, having one token $(p,c)$ is equivalent to having an inexhaustible supply of such tokens.

The first condition is merely syntactic convenience. It asks that each transition takes at most one token from each place. The second condition in Definition 5 implies that for each discrete step $M \rightarrow_t M'$ we have $M' \geq M$. Therefore, once a token $(p,c)$ is present on a place $p$, it will stay there unchanged (unless time passes), and it will enable transitions with $(p,c)$ in their precondition.

Wherever possible, we will from now on therefore allow ourselves to use the set notation for markings, that is simply treat markings $M \in (P \times \mathbb{R}_{\geq 0})^\oplus$ as sets $M \subseteq (P \times \mathbb{R}_{\geq 0})$.

### 3 Lower Bound

PSPACE-hardness of $\exists \text{COVER}$ does not follow directly from the PSPACE-completeness of the reachability problem in timed automata of [5]. The non-consuming property of our TPN makes it impossible to fully implement the control-state of a timed automaton. Instead our
where there exists a number analogous). There are two cases depending on constraint of $M$. For every bitpass by one unit to enter the next round.

Proof. Let $F(v) = 0\iff v'_j = j \land k$. All transitions demand that incoming tokens are of age exactly 1 and only tokens of age 0 are produced.

For the first part, we construct a sequence $(M_0 \rightarrow_{\text{Disc}} M_1 \rightarrow_{\text{Disc}} \cdots \rightarrow_{\text{Disc}} M_n-1$ where $M_0 \not\equiv_\omega (M_v + 1)$ and every step $M_{i-1} \rightarrow_{\text{Disc}} M_i$ adds tokens simulating the $i$th constraint of $F$. Since the TPN is non-consuming, we will have that $M_i \geq (M_v + 1)$, for all $i < n$. Consider now constraint $i'$, and assume w.l.o.g. that $i' = j \land k$ (the other case is analogous). There are two cases depending on $v'[i]$.

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{figure1.png}
\caption{The transitions $i.B$, $i.R$ and $i.L$ that simulate the update of bit $i$ according to constraint $i' = j \land k$. All transitions demand that incoming tokens are of age exactly 1 and only tokens of age 0 are produced.}
\end{figure}

A depth-1 monotone Boolean circuit is a function $F : \{0,1\}^n \rightarrow \{0,1\}^n$ represented by $n$ constraints: For every $0 \leq i < n$ there is a constraint of the form $i' = j \land k$, where $0 \leq j, k < n$ and $\otimes \in \{\land, \lor\}$, which expresses how the next value of bit $i$ depends on the current values of bits $j$ and $k$. For every bitvector $v \in \{0,1\}^n$, the function $F$ then satisfies $F(v)[i] \defeq v[j] \otimes v[k]$. It is $\text{PSPACE}$-complete to check whether for a given vector $v \in \{0,1\}^n$ there exists a number $m \in \mathbb{N}$ such that $F^m(v)[0] = 1$.

Towards a lower bound for $\exists \text{COVER}$ (Theorem 7) we construct a non-consuming TPN as follows, for a given circuit. The main idea is to simulate circuit constraints by transitions that reset tokens of age 1 (encoding $v$) to fresh ones of age 0 (encoding $F(v)$), and let time pass by one unit to enter the next round.

For every bit $0 \leq i < n$, the net contains two places $T$ and $F$. A marking $M_v \leq P \times \mathbb{R}_{\geq 0}$ is an encoding of a vector $v \in \{0,1\}^n$ if for every $0 \leq i < n$ the following hold.

1. $(T,v_0) \in M_v \iff v[i] = 1$.
2. $(F,v_0) \in M_v \iff v[i] = 0$.
3. If $(p,c) \in M_v$ then $c = 0$ or $c \geq 1$.

Note that in particular one cannot have both $(T,v_0)$ and $(F,v_0)$ in $M_v$. For every constraint $i' = j \land k$ we introduce three transitions, $i.L$, $i.R$, and $i.B$, where

\begin{align*}
Pre(i.B) &\defeq (T,v_x) + (T,v_y) & Post(i.B) &\defeq Pre(i.B) + (T,v_0) \\
Pre(i.L) &\defeq (F,v_x) & Post(i.L) &\defeq Pre(i.L) + (F,v_0) \\
Pre(i.R) &\defeq (F,v_x) & Post(i.R) &\defeq Pre(i.R) + (F,v_0)
\end{align*}

and the guard for all transitions is $G(x) = G(y) = 1$. See Figure 1 for an illustration. For disjunctions $i' = j \lor k$ the transitions are defined analogously, with $T$ and $F$ inverted. The correctness proof of our construction rests on the following simple observation.

\begin{lemma}
If $F(v) = v'$ then for every encoding $M_v$ of $v$, there exists an encoding $M_{v'}$ of $v'$ such that $M_v \rightarrow_{\text{Disc}} M_{v'}$. Conversely, if $M_v \rightarrow_{\text{Disc}} M_{v'}$ for encodings $M_v$ and $M_{v'}$ of $v$ and $v'$ respectively, then $F(v) = v'$.
\end{lemma}

Proof. For the first part, we construct a sequence $M_0 \rightarrow_{\text{Disc}} M_1 \rightarrow_{\text{Disc}} \cdots \rightarrow_{\text{Disc}} M_{n-1}$ where $M_0 \not\equiv_\omega (M_v + 1)$ and every step $M_{i-1} \rightarrow_{\text{Disc}} M_i$ adds tokens simulating the $i$th constraint of $F$. Since the TPN is non-consuming, we will have that $M_i \geq (M_v + 1)$, for all $i < n$. Consider now constraint $i'$, and assume w.l.o.g. that $i' = j \land k$ (the other case is analogous). There are two cases depending on $v'[i]$.
1. Case \( v'[i] = 1 \). By our assumption that \( F(v) = v' \) we know that \( v[j] = 1 \) and \( v[k] = 1 \).
So \( (\text{True}_j, 1) \in (M_v + 1) \leq M_{i-1} \) and \( (\text{True}_k, 1) \in (M_v + 1) \leq M_{i-1} \).
By construction of the net, there is a transition \( i.B \) with \( \text{Pre}(i.B) = (\text{True}_j, 1) + (\text{True}_k, 1) \) and \( \text{Post}(i.B) = \text{Pre}(i.B) + (\text{True}_i, 0) \).
This justifies step \( M_{i-1} \xrightarrow{i.B} M_i \) and therefore that \( (\text{True}_i, 0) \in M_i \leq M_{n-1} \).
Also notice that no marking reachable from \( M_0 \) using only discrete steps can contain the token \( (\text{False}_i, 0) \). This is because these can only be produced by transitions requiring either \( (\text{False}_j, 1) \) or \( (\text{False}_k, 1) \), which are not contained in \( M_0 \) by assumption that \( M_0 \) encodes \( v \). Therefore \( (\text{False}_i, 0) \not\in M_{n-1} \).

2. Case \( v'[i] = 0 \). W.l.o.g., \( v[j] = 0 \). Therefore, \( (\text{False}_j, 1) \in (M_v + 1) \leq M_{i-1} \).
By construction of the net, there exists transition \( i.L \) with \( \text{Pre}(i.L) = (\text{False}_j, 1) \) and \( \text{Post}(i.L) = \text{Pre}(i.L) + (\text{False}_i, 0) \).
This justifies the step \( M_{i-1} \xrightarrow{i.L} M_i \), with \( (\text{False}_i, 0) \in M_i \leq M_{n-1} \).
Moreover, if there is a marking \( v \) such that \( \exists i.B \), there is a transition \( \xrightarrow{i.B} M_i \) and therefore that \( (\text{True}_i, 0) \in M_i \leq M_{n-1} \).
Notice again that no marking reachable from \( M_0 \) using only discrete steps can contain the token \( (\text{True}_i, 0) \). This is because these can only be produced by transitions \( i.B \), requiring both \( (\text{True}_j, 1), (\text{True}_k, 1) \in M_0 \), contradicting our assumptions. Hence, \( (\text{True}_i, 0) \not\in M_{n-1} \).

We conclude that the constructed marking \( M_{n-1} \) is an encoding of \( v' \).

For the other part of the claim, assume that there exist markings \( M_v \) and \( M_{v'} \) which are encodings of vectors \( v \) and \( v' \), respectively, with \( M_v \rightarrow \xrightarrow{\text{Disc}} M_{v'} \). We will show that \( F(v) = v' \).
Recall that \( F(v)[i] \overset{df}{=} v[j] \otimes v[k], \) where \( 0 \leq j, k < n \) and \( \otimes \in \{\wedge, \vee\} \).
We will show for each \( i < n \) that \( v'[i] = v[j] \otimes v[k] \).
Again, consider the constraint \( i' \), and assume w.l.o.g. that \( i' = j \land k \) (the other case is analogous).
There are two cases.

1. Case \( v'[i] = 1 \). By definition of a marking encoding, we have that \( (\text{True}_i, 0) \in M_v \).
By construction, there is a transition \( i.B \) with \( \text{Pre}(i.B) = (\text{True}_i, 1) + (\text{True}_k, 1) \) and \( \text{Post}(i.B) = \text{Pre}(i.B) + (\text{True}_i, 0) \).
By assumption, it holds that \( (M_v + 1) \rightarrow \text{Disc} M_v' \), where \( M_v \rightarrow \text{Disc} M_v' \), with \( (M_v + 1) \in M_v \).
Note that \( (\text{True}_i, 1) \in (M_v + 1) \) and \( (\text{True}_k, 1) \in (M_v + 1) \).
Hence, we have that \( v[j] = 1 \) and \( v[k] = 1 \), and therefore that \( F(v)[i] = v'[i] = v[j] \land v[k] \).

2. Case \( v'[i] = 0 \). Then \( (\text{False}_i, 0) \in M_v \) and, since this token can only be produced by transitions \( i.L \) or \( i.R \), either \( (\text{False}_j, 1) \in (M_v + 1) \) or \( (\text{False}_k, 1) \in (M_v + 1) \).
Therefore \( (\text{False}_j, 0) \in (M_v) \) or \( (\text{False}_k, 0) \in (M_v) \) and because \( M_v \) is an encoding of \( v \), this means that either \( v[j] = 0 \) or \( v[k] = 0 \). Therefore, \( F(v')[i] = v[j] \land v[k] = 0 \).

\[ \blacktriangleleft \]

Theorem 7. \( \exists \text{COVER} \) is PSPACE-hard for non-consuming TPN.

Proof. For a given monotone Boolean circuit, define a non-consuming TPN as above. By induction on \( m \in \mathbb{N} \) using Lemma 6, we derive that there exists \( m \in \mathbb{N} \) with \( F^m(v) = v' \) and \( v'[0] = 1 \) if, and only if, there exists encodings \( M_v \) of \( v \) and \( M_{v'} \) of \( v' \), with \( M_v \rightarrow M_{v'} \).
Moreover, if there is a marking \( M \) such that \( M_v \rightarrow M \) and \( 0 \in \text{frac}(M) \), where \( M \) contains a token of age 0, then \( M \leq M_{v'} \) for some encoding \( M_{v'} \) of a vector \( v'' = F^m(v) \). This means that it suffices to add one transition \( t \) with \( \text{Pre}(t) = (\text{True}_0, 0) \) whose enabledness witnesses the existence of a reachable encoding \( M_{v'} \) containing a token \( (\text{True}_0, 0) \). By the properties above, there exists \( m \in \mathbb{N} \) with \( F^m(v) = v' \) and \( v'[0] = 1 \) if, and only if, \( M_v \rightarrow M_{v'} \).

This lower bound holds even for discrete time TPN, e.g. [9], because the proof uses only timed steps with duration \( d = 1 \).

4 Upper Bound

We start by observing that we can restrict ourselves, without loss of generality, to non-consuming TPN (Definition 5) for showing the upper bound. Intuitively, since we start with
an arbitrarily high number of tokens anyway, it does not matter how many of them are consumed by transitions during the computation, since some always remain.

**Lemma 8.** The \( \exists \text{COVER} \) problem for TPN logspace-reduces to the \( \exists \text{COVER} \) problem for non-consuming TPN. That is, for every TPN \( N \) and for every place \( p \) and transition \( t \) of \( N \), one can construct, using logarithmic space, a non-consuming TPN \( N' \) together with a place \( p' \) and transition \( t' \) of \( N' \), so that there exists \( M \in \text{Cover}_N(\mathbb{N} \cdot \{(p,0)\}) \) enabling \( t \) in \( N \) if and only if there exists \( M' \in \text{Cover}_{N'}(\mathbb{N} \cdot \{(p',0)\}) \) that enables \( t' \) in \( N' \).

### 4.1 Region Abstraction

We recall a constraint system called regions defined for timed automata [5]. The version for TPN used here is similar to the one in [3].

Consider a fixed, nonconsuming TPN \( N = (P,T,\text{Var},G,\text{Pre},\text{Post}) \). Let \( c_{\text{max}} \) be the largest finite value appearing in transition guards \( G \). Since different tokens with age \( > c_{\text{max}} \) cannot be distinguished by transition guards, we consider only token ages below or equal to \( c_{\text{max}} \) and treat the integer parts of older tokens as equal to \( c_{\text{max}} + 1 \). Let \( \text{int}(c) \stackrel{\text{def}}{=} \min\{c_{\text{max}} + 1, |c|\} \) and \( \text{frac}(c) \stackrel{\text{def}}{=} c - |c| \) for a real value \( c \in \mathbb{R}_{\geq 0} \). We will work with an abstraction of TPN markings as words over the alphabet \( \Sigma \stackrel{\text{def}}{=} 2^{P \times [c_{\text{max}}+1]} \). Each symbol \( X \in \Sigma \) represents the places and integer ages of tokens for a particular fractional value.

**Definition 9.** Let \( M \subseteq P \times \mathbb{R}_{\geq 0} \) be a marking and let \( \text{frac}(M) \stackrel{\text{def}}{=} \{\text{frac}(c) \mid (p, c) \in M\} \) be the set of fractional clock values that appear in \( M \).

Let \( S \subset [0,1] \) be a finite set of real numbers with \( 0 \in S \) and \( \text{frac}(M) \subseteq S \) and let \( f_0, f_1, \ldots, f_n \), be an enumeration of \( S \) so that \( f_i < f_i \) for all \( i \leq n \). The \( S \)-abstraction of \( M \) is

\[
\text{abs}_S(M) \stackrel{\text{def}}{=} x_0 x_1 \ldots x_n \in \Sigma^*
\]

where \( x_i \stackrel{\text{def}}{=} \{(p, \text{int}(c)) \mid (p, c) \in M \land \text{frac}(c) = f_i\} \) for all \( i \leq n \). We simply write \( \text{abs}(M) \) for the shortest abstraction, i.e. with respect to \( S = \{0\} \cup \text{frac}(M) \).

**Example 10.** The abstraction of marking \( M = \{(p,2.1),(q,2.2),(p,5.1),(q,5.1)\} \) is \( \text{abs}(M) = \emptyset \{(p,2),(p,5),(q,5)\} \{(q,2)\} \). The first symbol is \( \emptyset \), because \( M \) contains no token with an integer age (i.e., no token whose age has fractional part 0). The second and third symbols represent sets of tokens with fractional values 0.1 and 0.2, respectively.

Clocks with integer values play a special role in the behavior of TPN, because the constants in the transition guards are integers. Thus we always include the fractional part 0 in the set \( S \) in Definition 9.

We use a special kind of regular expressions over \( \Sigma \) to represent coverable sets of TPN markings as follows.

**Definition 11.** A regular expression \( E \) over \( \Sigma \) represents the downward-closed set of TPN markings covered by one that has an abstraction in the language of \( E \):

\[
[E] \stackrel{\text{def}}{=} \{M \mid \exists S . M \geq N \land \text{abs}_S(M) \in \mathcal{L}(E)\}.
\]

An expression is *simple* if it is of the form \( E = x_0 x_1 \ldots x_k \) where for all \( i \leq k \) either \( x_i \in \Sigma \) or \( x_i = y^* \) for some \( y \in \Sigma \). In the latter case we say that \( x_i \) carries a star. That is, a simple expression is free of Boolean combinators and uses only concatenation and Kleene star. We will write \( \hat{x}_i \) to denote the symbol in \( \Sigma \) at position \( i \): it is \( x_i \) if \( x_i \in \Sigma \) and \( y_i \) otherwise.
Universal Safety for Timed Petri Nets is PSPACE-complete

Remark 12. Notice that for all simple expressions \( \alpha, \beta \) so that \( |\alpha| > 0 \), we have that \( [\alpha \beta] = [\alpha \beta] \). However, unless \( \alpha \) has length 0 or is of the form \( \alpha = 0 \alpha' \), we have \( [\emptyset \alpha] \neq [\alpha] \). This is because a marking \( M \) that contains a token \((p, c)\) with \( \text{frac}(c) = 0 \) has the property that all abstractions \( \text{abs}_S(M) = x_0 \ldots x_k \) of \( M \) have \( x_0 \neq \emptyset \).

The following lemmas express the effect of TPN transitions at the level of the region abstraction. Lemmas 13 and 15 state that maximally firing of discrete transitions (the relation \( \rightarrow_{\text{Disc}} \)) is computable and monotone. Lemmas 16 and 17 state how to represent timed-step successor markings.

Lemma 13. For every non-consuming TPN \( \mathcal{N} \) there are polynomial time computable functions \( f : \Sigma \times \Sigma \times \Sigma \to \Sigma \) and \( g : \Sigma \times \Sigma \times \Sigma \to \Sigma \) with the following properties.

1. \( f(\alpha, \beta, x) \supseteq x \) and \( g(\alpha, \beta, x) \supseteq x \) for all \( \alpha, \beta, x \in \Sigma \).
2. Suppose that \( E = x_0 x_1 \ldots x_k \) is a simple expression, \( \alpha \defeq x_0 \) and \( \beta \defeq \bigcup_{i>0} \hat{x}_i \), and \( E' = x'_0 x'_1 \ldots x'_k \) is the derived expression defined by conditions:
   a. \( x'_0 \defeq f(\alpha, \beta, x_0) \)
   b. \( x'_i \defeq g(\alpha, \beta, \hat{x}_i)^* \) for \( i > 0 \)
   c. \( x'_i \) carries a star iff \( x_i \) does.

Then \( [E'] = \{ M'' \mid \exists M \in [E] \wedge M \twoheadrightarrow_{\text{Disc}} M' \supseteq M'' \} \).

Definition 14. We will write \( \text{SAT}(E) \defeq E' \) for the successor expression \( E' \) of \( E \) guaranteed by Lemma 13. I.e., \( \text{SAT}(E) \) is the saturation of \( E \) by maximally firing discrete transitions.

Notice that by definition it holds that \( [E] \subseteq [\text{SAT}(E)] \subseteq \text{Cover}([E]) \), and consequently also that \( \text{Cover}([\text{SAT}(E)]) = \text{Cover}([E]) \).

Lemma 15. Suppose that \( X = x_0 x_1 \ldots x_k \) is a simple expression of length \( k + 1 \) with \( \text{SAT}(X) = x'_0 x'_1 \ldots x'_k \) and \( x_0, x'_0 \in \Sigma \). Let \( Y = y_0 \alpha_1 y_1 \alpha_2 \ldots \alpha_k y_k \) be a simple expression with \( \text{SAT}(Y) = y'_0 \alpha'_1 y'_1 \alpha'_2 \ldots \alpha'_k y'_k \) and \( y_0, y_0' \in \Sigma \).

If \( \hat{x}_i \subseteq \hat{y}_i \) for all \( i \leq k \) then \( \hat{x}'_i \subseteq \hat{y}'_i \) for all \( i \leq k \).

Proof. The assumption of the lemma provides that \( \alpha_x \defeq x_0 \subseteq \alpha_y \defeq y_0 \) and \( \beta_x \defeq \bigcup_{k \geq 1} \hat{x}_i \subseteq \beta_y \defeq \bigcup_{k \geq 1} \hat{y}_i \). Therefore, by Item 1 of Lemma 13, we get that
\[
x_0 = f(\alpha_x, \beta_x, x_0) \subseteq f(\alpha_y, \beta_y, y_0) = y_0
\]
and similarly, for all \( k \geq i \geq 0 \), that \( \hat{x}'_i = g(\alpha_x, \beta_x, \hat{x}_i) \subseteq g(\alpha_y, \beta_y, \hat{y}_i) = \hat{y}'_i \).

For \( x \in \Sigma \) we write \( (x + 1) \defeq \{(p, \text{int}(n+1)) \mid (p, n) \in x\} \) for the symbol where token ages are incremented by 1.

Lemma 16. \( [\emptyset E] = \{ M' \mid \exists M \in [E] \wedge M \twoheadrightarrow_d M' \wedge d < 1 - \max(\text{frac}(M)) \} \).

Lemma 17. Let \( \alpha z \) be a simple expression where \( \hat{z} = z \in \Sigma \) (the rightmost symbol is not starred). Then, \( [[(z + 1)\alpha] \) contains a marking \( N \) if, and only if, there exists markings \( N' \geq N \) and \( M \), and a set \( S \subseteq [0, 1] \) so that

1. \( |S| = |\alpha z| \)
2. \( \text{abs}_S(M) \in L(\alpha z) \)
3. \( M \twoheadrightarrow_d N' \) for \( d = 1 - \max(S) \).
Proof. Suppose markings $N, N', M$, a set $S \subseteq [0, 1]$ and $d \in \mathbb{R}_{\geq 0}$ so that the conditions 1 to 3 are satisfied. Let $S' \triangleq \{0\} \cup \{s + d \mid s \in S \setminus \{d\}\}$. Then, $|S'| = |S|$ and $\text{abs}(N') \in \mathcal{L}((z + 1)\alpha)$, which witnesses that $N \in [(z + 1)\alpha]$. Conversely, let $N \in [(z + 1)\alpha]$ be a non-empty marking. If $|\alpha| = 0$, then $N \in [(z + 1)]$ and so $\text{abs}(N) \in \mathcal{L}((z + 1))$ for $S \triangleq \frac{N}{z} = \{0\}$. This means that $M \xrightarrow{\cdot 1} N = (M + 1)$ for a marking $M$ with $\text{abs}(M) \in \mathcal{L}(z) = \mathcal{L}(\alpha)$. If $|\alpha| > 0$, pick some marking $N' \geq N$ and set $S'$ so that $\text{abs}(N') = (z + 1)w$, for some word $w \in \mathcal{L}(\alpha)$. Then we must have that $|S'| = |(z + 1)\alpha| > 1$ and so $d \triangleq \min(S' \setminus \{0\})$ exists. Let $S' \triangleq \{s - d \mid s \in S'\} \cup \{1 - d\}$ and $M$ be the unique marking with $M \xrightarrow{\cdot d} N'$. Notice that $1 - d = \max(S)$. It follows that $\text{abs}(M) = wz \in \mathcal{L}(\alpha)$.

We will often use the following simple fact, which is a direct consequence of Lemma 17.

\begin{corollary}
\[(z + 1)\alpha \subseteq \text{Cover}([\alpha z]).\]
\end{corollary}

Finally, the following lemma will be the basis for our exploration algorithm.

\begin{lemma}
Let $\alpha x_0^\ast$ be a simple expression with $\text{SAT}(\alpha x_0^\ast) = \alpha x_0^\ast$. Then $\text{Cover}([\alpha x_0^\ast]) = \text{Cover}([\alpha x_0^\ast]) \cup \text{Cover}([\{0\} + 1\alpha x_0^\ast])$.
\end{lemma}

\begin{proof}
For the right to left inclusion notice that $[\alpha x_0^\ast] \subseteq \text{Cover}([\alpha x_0^\ast])$ trivially holds. For the rest, we have $[(x_0 + 1)\alpha x_0^\ast] \subseteq \text{Cover}([\alpha x_0^\ast])$ by Corollary 18, and therefore $\text{Cover}([x_0 + 1\alpha x_0^\ast]) \subseteq \text{Cover}([\alpha x_0^\ast]) = \text{Cover}([\alpha x_0^\ast])$. For the left to right inclusion, we equivalently show that

\[
\text{Cover}([\alpha x_0^\ast]) \setminus [\alpha x_0^\ast] \subseteq \text{Cover}([x_0 + 1\alpha x_0^\ast]).
\]

Using the assumption that $\text{SAT}(\alpha x_0^\ast) = \alpha x_0^\ast$, the set on the left contains everything coverable from $[\alpha x_0^\ast]$ by a sequence that starts with a (short) time step. It can therefore be written as

\[
\text{Cover}([\{N_1 \mid \exists N_0 \in [\alpha x_0^\ast] \wedge N_0 \xrightarrow{\cdot d} N_1 \wedge 0 < d < 1 - \max(frac(N_0))}]\}
\]

By Lemma 16 and because $[\emptyset \alpha] \subseteq [X \alpha]$ for all $X \in \Sigma$ and $\alpha \in \Sigma^*$, we conclude that indeed, $\text{Cover}([\alpha x_0^\ast]) \setminus [\alpha x_0^\ast] \subseteq \text{Cover}([\emptyset \alpha x_0^\ast]) \subseteq \text{Cover}([\{0\} + 1\alpha x_0^\ast])$.

\end{proof}

4.2 Acceleration

We propose an acceleration procedure based on unfolding expressions according to Lemma 19 (interleaved with saturation steps to guarantee its premise) and introducing new Kleene stars to keep the length of intermediate expressions bounded. This procedure (depicted in Algorithm 1), is used to characterize an initial subset of the coverability set.
Algorithm 1: Accelerate

**Input:** a simple expression $S_0 = x_1 x_0^*$ (of length 2 and with last symbol starred)

**Output:** simple expressions $S_1, S_i$ and $R$, of lengths 2, 4, and 2, respectively.

1. $S_1 \equiv x_1(x_0^*)^* = SAT(x_1 x_0^*)$
2. $S_2 \equiv x_1^2 x_1^2(x_0^*)^* = SAT((x_0^*) + 1)S_1$
3. $S_3 \equiv x_3 x_3 x_3(x_0^*)^* = SAT((x_0^*) + 1)S_2$
4. $i \leftarrow 3$
5. repeat
   6. $x_i^{i+1} x_i^{i+1} x_i^{i+1} x_i^{i+1} x_i^{i+1} x_i^{i+1} \equiv SAT((x_0^*) + 1)S_i$
   7. $S_i+1 \equiv x_i^{i+1} x_i^{i+1} x_i^{i+1} x_i^{i+1} x_i^{i+1} x_i^{i+1} S_i$
   8. $i \leftarrow i + 1$
9. until $S_i = S_{i-1}$
10. $R \equiv (x_1 + 1)(x_{i-1}^*)$
11. return $S_1, S_i, R$

---

**Figure 2** A Run of Algorithm 1 (initial steps). The column on the left indicates the line of code, the middle depicts the current expression and the column on the right recalls its origin. Gray bars indicate that the respective symbols are equal. Arrows denote (set) inclusion between symbols. The gray vertical arrows indicate inclusions due to saturation (Lemma 13), as claimed in item 1 of Lemma 20. Red and blue arrows indicate derived inclusions (as stated in Lemma 20).
Given a length-2 simple expression \( S_0 \) where the rightmost symbol is starred, the algorithm will first saturate (Definition 14, in line 1), and then alternately rotate a copy of the rightmost symbol (Lemma 17), and saturate the result (see lines 2, 3, 6). Since each such round extends the length of the expression by one, we additionally collapse them (in line 7) by adding an extra Kleene star to the symbol at the second position. The crucial observation for the correctness of this procedure is that the subsumption step in line 7 does not change the cover sets of the respective expressions.

Observe that Algorithm 1 is well defined because the \( SAT(S_i) \) are computable by Lemma 13. Termination is guaranteed by the following simple observation.

**Lemma 20.** Let \( x_i^j \in \Sigma \) be the symbols computed by Algorithm 1. Then

1. \( x_i^{j+1} \geq x_i^j \), for all \( i > j \geq 0 \).
2. \( x_i^{j} \geq x_i^{j-1} \) and \( x_i^{j+1} \geq x_i^{j-1} \), for all \( i \geq 3 \).

**Proof.** The first item is guaranteed by Point 2 of Lemma 13. In particular this means that \( x_i^{j+1} \geq x_i^j \) and therefore that \( (x_i^{j+1} + 1) \geq (x_i^j + 1) \) for all \( i \geq 0 \) (indicated as red arrows in Figure 2). The second item now follows from this observation by Lemma 15.

**Lemma 21 (Termination).** Algorithm 1 terminates with \( i \leq 4 \cdot |P| \cdot (c_{\text{max}} + 1) \).

**Proof.** From Lemma 20 we deduce that for all \( i \geq 2 \), the expression \( S_{i+1} \) is point-wise larger than or equal to \( S_i \) with respect to the subset ordering on symbols. The claim now follows from the observation that all expressions \( S_{i+1} \geq S_i \) have length 4 and that every symbol \( x_i \in \Sigma \) can only increase at most \( |P| \cdot (c_{\text{max}} + 1) \) times.

**Lemma 22 (Correctness).** Suppose that \( S_1, S_i, R \) be the expressions computed by Algorithm 1 applied to the simple expression \( x_1x_0^i \). Then \( \text{Cover}(\{x_1x_0^i\}) = \{ S_1 \} \cup \{ S_i \} \cup \text{Cover}(\{ R \}) \).

**Proof.** Let \( S_1, \ldots, S_i \) denote the expressions defined in lines 1,2,3, and 7 of the algorithm. That is, \( i \) is the least index such that \( S_{i+1} = S_i \). We define a sequence \( E_i \) of expressions inductively, starting with \( E_1 \equiv S_1 \) and if \( E_i = e_1^i \cdot e_{i-1} \ldots e_0 \), we let \( E_{i+1} \equiv e_i^i \cdot e_{i-1} \ldots e_0 \equiv SAT(e_0 + 1)E_i \). Here, the superscript indicates the position of a symbol and not iteration. This is the sequence of expressions resulting from unfolding Lemma 19, interleaved with saturation steps, just in line 6 of the algorithm. That is, the expressions \( E_i \) are not collapsed (line 7) and instead grow in length with \( i \). Still, \( E_1 = S_1, E_2 = S_2 \) and \( E_3 = S_3 \), but \( E_4 \not\equiv S_4 \), because the latter is the result of applying the subsumption step of line 7 in our algorithm.

Notice that \( \text{Cover}(\{x_1x_0^i\}) = \left( \bigcup_{i \geq 2}[E_i] \right) \bigcup \text{Cover}([R]) \) holds for all \( k \in \mathbb{N} \). We will use that

\[
\bigcup_{i \geq 2}[E_i] = \bigcup_{i \geq 2}[S_i] = [S_i].
\]  

(2)

We start by observing that for all \( i, j \in \mathbb{N} \) it holds that \( e_j^i = x_j^i \). For \( i \leq 3 \) this holds trivially by definition of \( E_i \equiv S_i \). For larger \( i \), this can be seen by induction using Lemma 13. Towards the first equality in Equation (2), let \( S_i^j \) be the expression resulting from \( S_i = x_i^j(x_i^{j-1})^* \) by unfolding the first star \( j \) times. That is, \( S_i^j \equiv x_i^j(x_i^{j-1})^*) \equiv x_i^j(x_i^{j-1})^* \), where the superscript \( (j) \) denotes \( j \)-fold concatenation. Clearly, \( [S_i] = \bigcup_{j \geq 0}[S_i^j] \) and so the \( \geq \)-direction of the first equality in Equation (2) follows by

\[
[S_i^j] = [x_i^j(x_i^{j-1})^* x_i^j] \subseteq [x_i^{j+i}(x_i^{j+i-1})^* x_i^{j+i}] \\
\subseteq [x_i^{j+i}(x_i^{j+i-1})^* x_i^{j+i} x_i^{j+i-1}] \\
= [E_{i+j}].
\]
where the first inclusion is due to Lemma 20. The same helps for the other direction:
\[
\lbrack E_i \rbrack = \lbrack x_i'_{t-1} x_i'_{t-2} \ldots x_i^0 \rbrack \subseteq \lbrack x_i'(x'_i)_{i-1}^{(i-2)} x_i^0 \rbrack = [S_i^{t-2}] = [S_t],
\]
which completes the proof of the first equality in Equation (2). The second equality holds because \([S_i] \subseteq [S_{i+1}]\) for all \(i \geq 2\), by Lemma 20, and by definition of \(S_t = S_{t+1}\). As a next step we show that
\[
Cover([S_t]) = [S_t] \cup Cover([R])
\]
First observe that \([R] = \lbrack (x_i' + 1)(x_i'_{t-1})^* \rbrack = \lbrack (x_i'_{t-1})^* \rbrack\) and consequently,
\[
Cover([R]) = Cover(\{(x_i'_{t-1})^*\}) \subseteq Cover(\{(x_i'_{t-1})^* x_i^0\}) = Cover([S_t])
\]
where the first equation follows by Corollary 18 and the second because \(L(x_i'_{t-1})^* x_i^0 \subseteq L(x_i'_{t-1})^* x_i^0\). For the left to right inclusion in Equation (4), consider a marking \(M \in Cover([S_t]) \setminus [S_t]\). We show that \(Cover([S_t])\) consists of all those markings \(M\) so that there exists a finite path
\[
M_0 \xrightarrow{d_0} Disc M'_{0} \xrightarrow{t_1} Time M_1 \xrightarrow{d_1} Disc M'_{1} \xrightarrow{t_2} Time M_2 \ldots M'_{k-1} \xrightarrow{d_k} Disc M_k
\]
alternating between timed and (sequences of) discrete transition steps, with \(M_0 \in [S_t]\), \(M_k \geq M\) and all \(d_i \leq \max(frac(M'_i))\).

By our choice of \(M\), there must be a first expression in the sequence which is not a member of \([S_t]\). Since \([SAT(S_t)] = [S_t]\), we can assume an index \(i > 0\) so that \(M_i \notin [S_t]\) but \(M'_{i-1} \in [S_t]\) that is, the step that takes us out of \([S_t]\) is a timed step.

Because \([S_t] = \bigcup_{j \geq 2} [S_j]\), it must hold that \(M'_{i-1} \in [S_j] = \lbrack x_i'(x_j'_{t-1})^* x_i^0\rbrack\) for some index \(j \geq 2\). We claim that it already holds that
\[
M'_{i-1} \in \lbrack x_i'(x_j'_{t-1})^* x_i^0\rbrack.
\]
Suppose not. If \(d_i < \max(frac(M'_{i-1}))\) then \(M_i \notin [S_j] \subseteq [S_t]\) by Lemma 16, contradiction. Otherwise, if \(d_i = \max(frac(M'_{i-1}))\), notice that every abstraction \(abs_S(M'_{i-1}) \in L(S_j)\) must have \(|S| = 4\). So by Lemma 17, \(M_i \in \lbrack x_i^0 + 1\rbrack S_j\). But then again
\[
\lbrack (x_i^0 + 1)S_j \rbrack \subseteq [SAT((x_i^0 + 1)S_j)] \subseteq [S_{j+1}],
\]
contradicting our assumption that \(M_i \notin [S_t]\). Therefore Equation (5) holds. By Lemma 17 we derive that \(M_i \in \lbrack (x_i^0 + 1)(x_j'_{t-1})^* \rbrack = \lbrack (x_i^0 + 1)(x_j'_{t-1})^* \rbrack \subseteq \lbrack (x_i^0 + 1)(x_i'_{t-1})^* \rbrack = [R]\). This concludes the proof of Equation (4).

Notice that by Lemma 19 we have that
\[
Cover([x_i x_j^0]) = [SAT(x_i x_j^0)] \cup Cover([SAT(x_i x_j^0)]) = [S_i] \cup Cover([S_i]).
\]
Analogously, we get for every \(i \geq 1\) that
\[
Cover([E_i]) = [SAT(E_i)] \cup Cover([SAT((x_i^0 + 1)E_i)]) = [E_i] \cup Cover([E_{i+1}]).
\]
This used Lemma 19 and the fact that $\text{SAT}(E_i) = E_i$ by construction. Using Equation (8) and that $[E_i] \subseteq [E_{i+1}]$ for $i \geq 2$, we deduce

\[
\text{Cover}([S_i]) = \text{Cover}([E_i]) = [E_i] \cup \left( \bigcup_{i \geq 2} \text{Cover}([E_i]) \right).
\]

Finally we can conclude the desired result as follows.

\[
\text{Cover}([x_1 x_0]) \overset{(\ast)}{=} [S_1] \cup \text{Cover}([S_1]) \overset{(\ast)}{=} [S_1] \cup \text{Cover} \left( \bigcup_{i \geq 2} [E_i] \right) \\
\overset{(\ast)}{=} [S_1] \cup \text{Cover}([S_i]) \\
\overset{(\ast)}{=} [S_1] \cup [S_2] \cup \text{Cover}([R])
\]

4.3 Main Result

The following theorem summarizes our main claims regarding the \texttt{\exists COVER} problem.

\textbf{Theorem 23.} Consider an instance of \texttt{\exists COVER} with $N = (P,T,\text{Var},G,\text{Pre},\text{Post})$ a non-consuming TPN where $c_{\text{max}}$ is the largest constant appearing in the transition guards $G$ encoded in unary, and let $p$ be an initial place and $t$ be a transition.

1. The number of different simple expressions of length $m$ is $B(m) \overset{\text{def}}{=} 2^{\min_P (c_{\text{max}} + 2) m + m}$.

2. It is possible to compute a symbolic representation of the set of markings coverable from some marking in the initial set $N \cdot \{(p,0)\}$, as a finite set of simple expressions. I.e., one can compute simple expressions $S_1,\ldots,S_\ell$ s.t. $\bigcup_{1 \leq i \leq \ell} [S_i] = \text{Cover}(N \cdot \{(p,0)\})$ and where $\ell \leq 3 \cdot B(2)$. Each of the $S_i$ has length either 2 or 4.

3. Checking if there exists $M \in \text{Cover}(N \cdot \{(p,0)\})$ with $M \xrightarrow{t} \cdot$, can be done in $O(|P| \cdot c_{\text{max}})$ deterministic space.

\textbf{Proof.} For Item 1 note that a simple expression is described by a word where some symbols have a Kleene star. There are $|\Sigma|^m$ different words of length $m$ and $2^m$ possibilities to attach stars to symbols. Since the alphabet is $\Sigma \overset{\text{def}}{=} 2^{P \times (c_{\text{max}} + 1)}$ and $|c_{\text{max}} + 1| = c_{\text{max}} + 2$, the result follows.

Towards Item 2, we can assume w.l.o.g. that our TPN is non-consuming by Lemma 8, and thus the region abstraction introduced in Section 4.1 applies. In particular, the initial set of markings $N \cdot \{(p,0)\}$ is represented exactly by the expression $S_0 \overset{\text{def}}{=} \{(p,0)\}0^*$ where $0 \in \Sigma$ is the symbol corresponding to the empty set. That is, we have $[S_0] = N \cdot \{(p,0)\}$ and thus $\text{Cover}([S_0]) = \text{Cover}(N \cdot \{(p,0)\})$.

The claimed expressions $S_i$ are the result of iterating Algorithm 1 until a previously seen expression is revisited. Starting at $i = 0$ and $S_0 \overset{\text{def}}{=} \{(p,0)\}0^*$, each round will set $S_{1+i},S_{i+2}$ and $S_{i+3}$ to the result of applying Algorithm 1 to $S_i$, and increment $i$ to $i + 3$.

Notice that then all $S_i$ are simple expressions of length 2 or 4 and that in particular, all expressions with index divisible by 3 are of the form $ab^*$ for $a,b \in \Sigma$. Therefore after at most $B(2)$ iterations, an expression $S_\ell$ is revisited (with $\ell \leq 3B(2)$). Finally, an induction using Lemma 22 provides that $\bigcup_{1 \leq i \leq \ell} [S_i] = \text{Cover}(N \cdot \{(p,0)\})$.

Towards Item 3, we modify the above algorithm for the \texttt{\exists COVER} problem with the sliding window technique. The algorithm is the same as above where instead of recording all the expressions $S_1,\ldots,S_\ell$, we only store the most recent ones and uses them to decide
whether the transition $t$ is enabled. If the index $i$ reaches the maximal value of $3 \cdot B(2)$ we return unsuccessfully.

The bounded index counter uses $O(\log(B(2)))$ space; Algorithm 1 uses space $O(\log(B(5)))$ because it stores only simple expressions of length $\leq 5$. The space required to store the three expressions resulting from each application of Algorithm 1 is $O(3 \cdot \log(B(4)))$. For every encountered simple expression we can check in logarithmic space whether the transition $t$ is enabled by some marking in its denotation. Altogether the space used by our new algorithm is bounded by $O(\log(B(5)))$. By Item 1, this is $O(|P| \cdot (c_{max} + 2)) = O(|P| \cdot c_{max})$. ▶

\begin{corollary}
The $\exists$\textsc{Cover} problem for TPN is \textsc{PSPACE}-complete.
\end{corollary}

\textbf{Proof.} The \textsc{PSPACE} lower bound was shown in Theorem 7. The upper bound follows from Lemma 8 and Item 3 of Theorem 23. ▶

\section{Conclusion and Future Work}

We have shown that \textsc{Existential Coverability} (and its dual of universal safety) is \textsc{PSPACE}-complete for TPN with one real-valued clock per token. This implies the same complexity for checking safety of arbitrarily large timed networks without a central controller. The absence of a central controller makes a big difference, since the corresponding problem with a central controller is complete for $F_{\omega\omega}$ [12].

It remains an open question whether these positive results for the controller-less case can be generalized to multiple real-valued clocks per token. In the case with a controller, safety becomes undecidable already for two clocks per token [2].

Another question is whether our results can be extended to more general versions of timed Petri nets. In our version, clock values are either inherited, advanced as time passes, or reset to zero. However, other versions of TPN allow the creation of output-tokens with new non-deterministically chosen non-zero clock values, e.g., the timed Petri nets of [3, 4] and the read-arc timed Petri nets of [8].

\begin{thebibliography}{10}
\end{thebibliography}


