Complete Finite Prefixes of Symbolic Unfoldings of Safe Time Petri Nets

Thomas Chatain[1] and Claude Jard[2]

[1] IRISA/INRIA,
Campus de Beaulieu, F-35042 Rennes cedex, France
Thomas.Chatain@irisa.fr

[2] IRISA/ENS Cachan-Bretagne,
Campus de Ker Lann, F-35170 Bruz, France
Claude.Jard@bretagne.ens-cachan.fr

Abstract. Time Petri nets have proved their interest in modeling real-time concurrent systems. Their usual semantics is defined in term of firing sequences, which can be coded in a (symbolic and global) state graph, computable from a bounded net. An alternative is to consider a "partial order" semantics given in term of processes, which keep explicit the notions of causality and concurrency without computing arbitrary interleavings. In ordinary place/transition bounded nets, it has been shown for many years that the whole set of processes can be finitely represented by a prefix of what is called the "unfolding". This paper defines such a prefix for safe time Petri nets. It is based on a symbolic unfolding of the net, using a notion of "partial state".

1 Introduction and Related Work

Time Petri nets have proved their interest in modeling real-time concurrent systems. Their usual semantics is defined in term of firing sequences, which can be coded in a (symbolic and global) state graph, computable if the net is bounded. Although efficient for many verification problems, the main drawback of this approach is to mask the concurrent aspects of the model behind the explicit computation of the possible interleavings of actions, leading to the usual state explosion problem. This can be circumvented by the use of heuristics, named as "partial-order reductions". The idea is to explore only the subset of states and transitions that are relevant for properties that are not concerned with commutation of concurrent actions. The main difficulty is the identification of concurrency among the symbolic representation of states. Examples of this approach can be found in [1,2].

An alternative is to consider a "partial order" semantics given in term of processes, which keep explicit the notions of causality and concurrency without computing arbitrary interleavings. This is our framework. The goal is not only to avoid the cost of having in memory all the interleavings when performing verification, but also to have a graphical representation of the timed processes. This opens new perspectives to other applications like supervision and diagnosis [3].

The first definition of a (denotational) partial-order semantics for time Petri nets was given in 1996 by Aura and Lilius [4,5], who formally defined the timed processes of a net. The question of a finite representation of the whole set of timed processes was left open. To do that, two approaches have been explored. The first one is limited to the discrete time framework. It is based on a modeling of clock ticks, which defines an embedding of time Petri nets into ordinary Petri nets. In ordinary place/transition bounded nets, it has been shown for many years that the whole set of processes can be finitely represented by a prefix of what is called the "unfolding" [6,7]. The drawback is the explosive nature of the transformation. The advantage is to recover the unfolding technology and the existence of a complete finite prefix. This is the historical approach of [8,9], who defined for the first time the notion of finite prefix for time Petri nets.

We follow a second approach, which definitely uses a symbolic framework to code the time constraints associated with the timed processes. It can deal with dense time and is in the continuation of Berthomieu's works on symbolic representations of the global states of time Petri nets [10]. The first contribution in that direction was made in 1996 by Semenov [11], who has considered a restrictive subclass of safe time Petri nets, named "time independent choice nets". It is a very simple case where the timed aspects do not actually introduce so many constraints. The interest is that the whole set of timed processes can be simply represented as a subset of the unfolding of the underlying ordinary Petri net, by copying the interval constraints. The general case is much more complicated. We have shown in [3] that a new definition of unfoldings is required. These use symbolic constraints on the possible firing dates of transitions, and are based on a notion of "partial state", richer than the usual marking of the input places. This is required by the fact that firing a timed transition cannot be decided locally, and may depend on the dates of arrival of tokens in places feeding transitions that are in conflict (this situation is often called "confusion" in Petri nets). [3] presented this new notion of unfolding and its application for diagnosing timed distributed systems. In this paper, we show that there also exists a notion of complete and finite prefix of this unfolding. It opens new perspectives in the verification of timed systems, based on a time Petri net modeling.

The rest of the paper is organized as follows. Section 2 presents the safe time Petri net model, with their interleaving semantics and their partial order representation given in term of processes. The concurrent operational semantics and the merging of the induced extended processes into a symbolic unfolding is described in Section 3. Section 4 is dedicated to its finite representation using the notion of complete finite prefix, before conclusion.

2 Safe Time Petri Nets

2.1 Definition

Notations. We denote f^{-1} the inverse of a bijection f. We denote $f_{|A}$ the restriction of a mapping f to a set A. The restriction has higher priority than the inverse: $f_{|A}^{-1} = (f_{|A})^{-1}$. We denote $\circ$ the usual composition of functions. Q denotes the set of nonnegative rational numbers.

Time Petri nets were introduced in [12]. A *time Petri net* is a tuple $\langle P, T, pre, post, efd, lfd\rangle$ where P and T are finite sets of *places* and *transitions* respectively, *pre* and *post* map each transition $t \in T$ to its *preset* often denoted ${}^\bullet t \stackrel{\text{def}}{=} pre(t) \subseteq P$ (${}^\bullet t \neq \emptyset$) and its *postset* often denoted $t^\bullet \stackrel{\text{def}}{=} post(t) \subseteq P$; $efd : T \longrightarrow Q$ and $lfd : T \longrightarrow Q \cup \{\infty\}$ associate the *earliest firing delay* $efd(t)$ and *latest firing delay* $lfd(t)$ with each transition t. A time Petri net is represented as a graph with two types of nodes: places (circles) and transitions (rectangles). The closed interval $[efd(t), lfd(t)]$ is written near each transition (see Figure 1).

2.2 Interleaving Semantics

A *state* of a time Petri net is given by a triple $\langle M, dob, \theta\rangle$, where $M \subseteq P$ is a *marking* denoted with tokens (thick dots), $\theta \in Q$ is its date and $dob : M \longrightarrow Q$ associates a *date of birth* $dob(p) \leq \theta$ with each token (marked place) $p \in M$. A transition $t \in T$ is *enabled* in the state $\langle M, dob, \theta\rangle$ if all of its input places are marked: ${}^\bullet t \subseteq M$. Its *date of enabling* $doe(t)$ is the date of birth of the youngest token in its input places: $doe(t) \stackrel{\text{def}}{=} \max_{p \in {}^\bullet t} dob(p)$. All the time Petri nets we consider in this article are *safe*, i.e. in each reachable state $\langle M, dob, \theta\rangle$, if a transition t is enabled in $\langle M, dob, \theta\rangle$, then $t^\bullet \cap (M \setminus {}^\bullet t) = \emptyset$.

A time Petri net starts in an *initial state* $\langle M_0, dob_0, \theta_0\rangle$, which is given by the *initial marking* M_0 and the initial date θ_0. Initially, all the tokens carry the date θ_0 as date of birth: for all $p \in M_0$, $dob_0(p) \stackrel{\text{def}}{=} \theta_0$.

The transition t can fire at date $\theta' \geq \theta$ from state $\langle M, dob, \theta\rangle$, if:

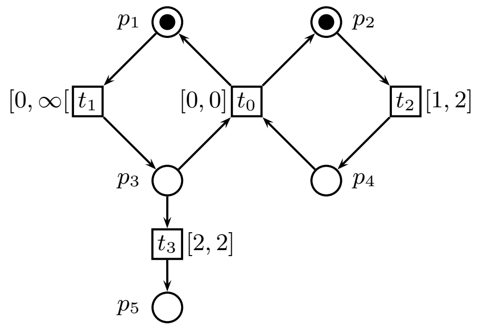
- t is enabled: ${}^\bullet t \subseteq M$;
- the minimum delay is reached: $\theta' \geq doe(t) + efd(t)$;
- the enabled transitions do not overtake the maximum delays:
  $\forall t' \in T \quad {}^\bullet t' \subseteq M \implies \theta' \leq doe(t') + lfd(t')$.

The firing of t at date θ' leads to the state $\langle (M \setminus {}^\bullet t) \cup t^\bullet, dob', \theta'\rangle$, where $dob'(p) \stackrel{\text{def}}{=} dob(p)$ if $p \in M \setminus {}^\bullet t$ and $dob'(p) \stackrel{\text{def}}{=} \theta'$ if $p \in t^\bullet$.

We call *firing sequence* starting from the initial state S_0 any sequence $((t_1, \theta_1), \ldots, (t_n, \theta_n))$ where there exist states $S_1, \ldots, S_n$ such that for all $i \in \{1, \ldots, n\}$, firing t_i from S_{i-1} at date θ_i is possible and leads to S_i. The empty firing sequence is denoted ϵ.

Finally we assume that time *diverges*: when infinitely many transitions fire, time necessarily diverges to infinity.

In the initial state of the net of Figure 1, p_1 and p_2 are marked and their date of birth is 0. t_1 and t_2 are enabled and their date of enabling is the initial date 0. t_2 can fire in the initial state at any time between 1 and 2. Choose time 1.3. After this firing, p_1 and p_4 are marked, t_1 is the only enabled transition and it has already waited 1.3 time unit. t_1 can fire at any time θ, provided it is greater than 1.3. Let t_1 fire at time 3. p_3 and p_4 are marked in the new state, and transitions t_3 and t_0 are enabled, and their date of enabling is 3 because they have just been enabled by the firing of t_1. To fire, t_3 would have to wait 2 time units. But transition t_0 cannot wait at all. So t_0 will necessarily fire (at time 3), and t_3 cannot fire.



$\sigma_1 \stackrel{\text{def}}{=} ((t_2, 1.3), (t_1, 3), (t_0, 3), (t_1, 3), (t_2, 5), (t_3, 5))$
$\sigma_2 \stackrel{\text{def}}{=} ((t_2, 1.3), (t_1, 3), (t_0, 3), (t_1, 3), (t_3, 5), (t_2, 5))$

$e_1 \stackrel{\text{def}}{=} (\{(\bot, p_1)\}, t_1)$ $\quad e_2 \stackrel{\text{def}}{=} (\{(\bot, p_2)\}, t_2)$
$e_3 \stackrel{\text{def}}{=} (\{(e_1, p_3), (e_2, p_4)\}, t_0)$ $\quad e_4 \stackrel{\text{def}}{=} (\{(e_3, p_1)\}, t_1)$
$e_5 \stackrel{\text{def}}{=} (\{(e_3, p_2)\}, t_2)$ $\quad e_6 \stackrel{\text{def}}{=} (\{(e_4, p_3)\}, t_3)$

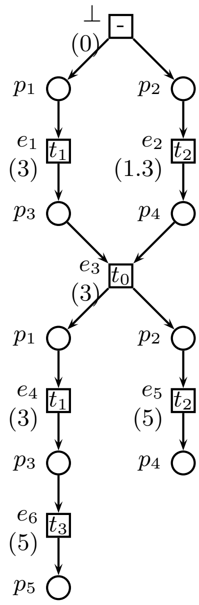


Fig. 1. A safe time Petri net and two of its firing sequences σ_1 and σ_2 starting at date 0 from the marking $M_0 \stackrel{\text{def}}{=} \{p_1, p_2\}$, that lead to the same process, represented on the right, with the date of the events in parentheses.

Remark. The semantics of time Petri nets are often defined in a slightly different way: the state of the net is given as a pair $\langle M, I \rangle$, where M is the marking, and I maps each enabled transition t to the delay that has elapsed since it was enabled, that is $\theta - doe(t)$ with our notations. It is more convenient for us to attach time information to the tokens of the marking than to the enabled transitions. We have chosen the date of birth of the tokens rather than their age, because we want to make the impact of the firing of transitions as local as possible. And the age of each token in the marking must be updated each time a transition t fires, whereas the date of birth has to be set only for the tokens that are created by t. Furthermore, usual semantics often deal with the delay between the firing of two consecutive transitions. In this paper we use the absolute firing date of the transitions instead. This fits better to our approach in which we are not interested in the total ordering of the events.

2.3 Partial Order Representation of the Runs: Processes

Processes are a way to represent an execution of a Petri net so that the actions (called events) are not totally ordered like in firing sequences: only causality orders the events. We will define the mapping Π from the firing sequences of a safe time Petri net to their partial order representation as processes. These processes are those described in [4]. We use a canonical coding like in [13].

Each process will be a pair $x \stackrel{\text{def}}{=} \langle E, \Theta \rangle$, where E is a set of *events*, and $\Theta : E \longrightarrow Q$ maps each event to its firing date. Θ is sometimes represented as a set of pairs $(e, \Theta(e))$. Each event e is a pair $({}^\bullet e, \tau(e))$ that codes an occurrence of the transition $\tau(e)$ in the process. ${}^\bullet e$ is a set of pairs $b \stackrel{\text{def}}{=} ({}^\bullet b, \mathit{place}(b)) \in E \times P$. Such a pair is called a *condition* and refers to the token that has been created by the event ${}^\bullet b$ in the place $\mathit{place}(b)$. We say that the event $e \stackrel{\text{def}}{=} ({}^\bullet e, \tau(e))$ *consumes* the conditions in ${}^\bullet e$. Symmetrically the set $\{(e, p) \mid p \in \tau(e)^\bullet\}$ of conditions that are *created* by e is denoted $e^\bullet$.

For all set B of conditions, we denote $\mathit{Place}(B) \stackrel{\text{def}}{=} \{\mathit{place}(b) \mid b \in B\}$, and when the restriction of *place* to B is injective, we denote $\mathit{place}_{|B}^{-1}$ its inverse, and for all $P \subseteq \mathit{Place}(B)$, $\mathit{Place}_{|B}^{-1}(P) \stackrel{\text{def}}{=} \{\mathit{place}_{|B}^{-1}(p) \mid p \in P\}$. The set of conditions that remain at the end of the process $\langle E, \Theta \rangle$ (meaning that they have been created by an event of E, and no event of E has consumed them) is $\uparrow(E) \stackrel{\text{def}}{=} \bigcup_{e \in E} e^\bullet \setminus \bigcup_{e \in E} {}^\bullet e$ (it does not depend on Θ).

The function Π that maps each firing sequence $((t_1, \theta_1), \ldots, (t_n, \theta_n))$ to a process is defined as follows:

- $\Pi(\epsilon) \stackrel{\text{def}}{=} \langle \{\bot\}, \{(\bot, \theta_0)\} \rangle$, where $\bot \stackrel{\text{def}}{=} (\emptyset, \text{-})$ represents the initial event and θ_0 the initial date. Notice that the initial event does not actually represent the firing of a transition, which explains the use of the special value - $\notin T$. For the same reason, the set of conditions that are created by $\bot$ is defined in a special way: $\bot^\bullet \stackrel{\text{def}}{=} \{(\bot, p) \mid p \in M_0\}$.
- $\Pi(((t_1, \theta_1), \ldots, (t_{n+1}, \theta_{n+1}))) \stackrel{\text{def}}{=} \langle E \cup \{e\}, \Theta \cup \{(e, \theta_{n+1})\} \rangle$, where $\langle E, \Theta \rangle \stackrel{\text{def}}{=} \Pi(((t_1, \theta_1), \ldots, (t_n, \theta_n)))$ and the event $e \stackrel{\text{def}}{=} (\mathit{Place}_{|\uparrow(E)}^{-1}({}^\bullet t_{n+1}), t_{n+1})$ represents the last firing of the sequence.

The set of all the processes obtained as the image by Π of the firing sequences is denoted X.

We define the relation $\rightarrow$ on the events as: $e \rightarrow e'$ iff $e^\bullet \cap {}^\bullet e' \neq \emptyset$. The reflexive transitive closure $\rightarrow^*$ of $\rightarrow$ is called the *causality* relation. Two events of a process that are not causally related are called *concurrent*. For all event e, we denote $\lceil e \rceil \stackrel{\text{def}}{=} \{f \in E \mid f \rightarrow^* e\}$, and for all set E of events, $\lceil E \rceil \stackrel{\text{def}}{=} \bigcup_{e \in E} \lceil e \rceil$.

Figure 1 shows two firing sequences that correspond to the same process. In the representation of the process, the rectangles represent the events, and the circles represent the conditions. An arrow from a condition b to an event e means that $b \in {}^\bullet e$. An arrow from an event e to a condition b means that $b \in e^\bullet$.

3 Symbolic Unfoldings of Safe Time Petri Nets

3.1 Introduction

Symbolic unfoldings have already been addressed in the context of high-level Petri nets [14] to reflect the genericity that appears in the model. In this section we define the symbolic unfolding of time Petri nets, i.e. a compact structure that contains all the processes and exhibits concurrency. When we build unfoldings, we would like to be able to unfold seperately two parts of the system when these two parts do not communicate, like the left part and the right part of the net of Figure 1 when t_1 and t_2 fire. As opposed to untimed Petri nets, in a timed context we accept that this may not yield proper processes but only what we will call *pre-processes*, in which the different parts of the system may not have reached the same date, provided the events that have been built are contained in a real execution. Let us define formally these *pre-process* as prefixes of the processes. Notice that in an untimed context pre-processes would simply be processes.

Definition 1 (pre-processes). *For all process $\langle E, \Theta \rangle$, and for all nonempty, causally closed set of events $E' \subseteq E$ ($\bot \in E'$ and $\lceil E' \rceil = E'$), $\langle E', \Theta_{|E'} \rangle$ is called a* pre-process. *We sometimes write $\langle E', \Theta \rangle$ instead of $\langle E', \Theta_{|E'} \rangle$ for short.*

Definition 2 (prefix relation on pre-processes). *We define the* prefix *relation $\leq$ on pre-processes as follows: $\langle E, \Theta \rangle \leq \langle E', \Theta' \rangle \quad \mathit{iff} \quad E \subseteq E' \wedge \Theta = \Theta'_{|E}$.*

In the case of untimed Petri nets, the unfolding can be defined as the superimposition of all the processes, that is the set of all the events that appear in the processes. This structure is quite compact since an event generally occurs in many different processes. However, it has to be easy to extract a process from the unfolding. Especially, given a causally closed set of events, it has to be easy to tell if there is a process that contains all these events, or containing at least these events. With untimed Petri nets, these two questions are the same and can be solved easily. In some special classes of time Petri nets, especially when the underlying untimed Petri net is extended free choice [15], we could simply define a symbolic unfolding of a time Petri net as in the untimed case. [11] defines such an unfolding for "time independent choice nets".

On the contrary, in the general timed case, a similar definition would not give good results. [4] explains how to know if there is a valid timed execution of a time Petri net that corresponds to a set of events taken from the unfolding of the underlying untimed Petri net. But this does not give a way to build an unfolding of a time Petri net and does not tell if there is a process that contains at least these events.

To be convinced that things are much more complicated than in the untimed case, it may be interesting to remark that in the timed case, the union of two pre-processes $\langle E, \Theta \rangle$ and $\langle E', \Theta' \rangle$ is not necessarily a pre-process, even if $E \cup E'$ is conflict free and $\Theta_{|E \cap E'} = \Theta'_{|E \cap E'}$. In the example of Figure 1, we observe this if $\langle E, \Theta \rangle$ is the process which contains a firing of t_1 at time 0 and a firing of t_2 at time 1, and $\langle E', \Theta' \rangle$ is the pre-process that we obtain by removing the firing of t_2 from the process made of t_1 at time 0, t_2 at time 2 and t_3 at time 2.

These difficulties come from the fact that the condition that allows us to extend a process $x \stackrel{\text{def}}{=} \langle E, \Theta \rangle$ with a new event e concerns all the state reached after the process x, and however the conditions in ${}^\bullet e$ refer only to the tokens in the input places of $\tau(e)$.

3.2 Concurrent Operational Semantics for Safe Time Petri Nets

Although the semantics of time Petri nets requires to check time conditions for all the enabled transitions in the net before firing a transition, there are cases when we know that a transition can fire at a given date θ, even if other transitions will fire before θ in other parts of the net. As an example consider the net of Figure 1 starting at time 0 in the marking $\{p_1, p_2\}$. The semantics forbids to fire t_1 at time 10 from the initial state because t_2 is enabled and must fire before time 2. However we are allowed to run the net until time 10 without firing t_1 (because its latest firing delay is infinite). Then, whatever has occurred until time 10, nothing can prevent t_1 from firing at date 10, because only t_1 can remove the token in place p_1. On the contrary, the firing of t_3 highly depends on the firing date of t_2 because when t_0 is enabled it fires immediately and disables t_3. So if we want to fire t_3 we have to check whether p_2 or p_4 is marked. This intuition leads us to define a **concurrent operational semantics** where it is possible to fire a transition without knowing the entire marking of the net, but only a partial marking made of the consumed tokens plus possibly some tokens which are only read (not consumed) in order to get enough information. Theorems 1 and 2 will validate our concurrent partial order semantics by establishing connections with the processes of Section 2.3.

Assumption. From now on we assume that we know a partition of the set P of places of the net in sets $P_i \subseteq P$ of mutually exclusive places[3]; more precisely we demand that for all reachable marking M, $P_i \cap M$ is a singleton. For all place $p \in P_i$, we denote $\bar{p} \stackrel{\text{def}}{=} P_i \setminus \{p\}$. In the example of Figure 1, we will use the partition $\{p_1, p_3, p_5\}$, $\{p_2, p_4\}$. In fact this partition will be used to test the absence of a token in a marking. For instance if we want to fire t_3, we have to check that t_0 will not fire before t_3 and remove the token in place p_3; if we know that p_2 is marked then we can deduce that p_4 is not, and that t_0 is disabled.

Definition 3 (partial state). *A* partial state *of a time Petri net is a triple* $\langle L, dob, lrd \rangle$ *where* $L \subseteq P$ *is a partial marking and* $dob, lrd : L \longrightarrow Q$ *associate a* date of birth $dob(p)$ *and a* latest reading date $lrd(p)$ *with each token* $p \in L$.

As opposed to global states, partial states may give only partial information on the state of the net since the partial marking L may not contain one place per set of mutually exclusive places. Notice also that the date θ that appears in global states is replaced by a function that gives the latest reading date of each token of the partial marking, since the global time of the system is not relevant any more in a concurrent semantics.

Definition 4 (maximal partial state). *A partial state* $\langle L, dob, lrd \rangle$ *is* maximal *if* L *contains one place per set of mutually exclusive places (see the assumption before). From now on the notion of* maximal partial state *or* maximal state *will replace the notion of global state.*

[3] If we do not know any such partition, a solution is to extend the structure of the net with one complementary place for each place of the net and to add these new places in the preset and in the postset of the transitions such that in any reachable marking each place $p \in P$ is marked iff its complementary place is not. This operation does not change the behavior of the time Petri net.

Definition 5 (age of a token in a maximal state). *Let $S \overset{\text{def}}{=} \langle M, dob, lrd \rangle$ be a maximal state and let $p \in M$ a token (marked place). The date that is reached by the system can be defined as* $\max_{p' \in M} lrd(p')$. *We define the* age $I_S(p)$ *of p in the state S as the difference:* $I_S(p) \overset{\text{def}}{=} \max_{p' \in M} lrd(p') - dob(p)$.

Definition 6 (temporally consistent maximal state (or consistent state)). *A maximal state $S \overset{\text{def}}{=} \langle M, dob, lrd \rangle$ is* temporally consistent *if for each transition $t \in T$ which is enabled in M ($^\bullet t \subseteq M$), $\min_{p \in {}^\bullet t} I_S(p) \leq lfd(t)$. A temporally consistent maximal state is also called a* consistent state *for short.*

We will construct a predicate that applies to tuples (L, dob, t, θ), where $L \subseteq P$ is a partial marking, $dob : L \longrightarrow Q$ associates a *date of birth* $dob(p)$ with each token (marked place) $p \in L$, t is a transition and $\theta \geq \max_{p \in L} dob(p)$ is a date.

Such a predicate is called a *local firing condition* and is supposed to tell if knowing that the net is in a state that contains a partial state $\langle L, dob, lrd \rangle$ with $lrd(p) \leq \theta$ for all $p \in L$ is enough to be sure that t can fire at date θ.

Several local firing conditions are possible; some possibilities are discussed in [3]. In this article we will only use a local firing condition *LFC* that will allow us to build a complete finite prefix of the symbolic unfolding of a time Petri net.

Definition 7 (local firing condition *LFC'*). *We first define a predicate LFC' as follows: $LFC'(L, dob, t, \theta)$ holds iff*

- *t is enabled: $^\bullet t \subseteq L$;*
- *the minimum delay is reached: $\theta \geq doe(t) + efd(t)$;*
- *the transitions that may consume tokens of L are disabled or do not overtake the maximum delays:*

$$\forall t' \in T \quad {}^\bullet t' \cap L \neq \emptyset \implies \begin{cases} \exists p \in {}^\bullet t' \quad \bar{p} \cap L \neq \emptyset \\ \vee\ \theta \leq \max\limits_{p \in {}^\bullet t' \cap L} dob(p) + lfd(t') \end{cases}$$

The predicate LFC' guarantees that a partial state $\langle L, dob, lrd \rangle$ with $lrd(p) \leq \theta$ for all $p \in L$ is enough to be sure that t can fire at date θ. We define a new local firing condition *LFC* by demanding that the partial marking L is minimal.

Definition 8 (local firing condition *LFC*). *LFC is defined as:*

$$LFC(L, dob, t, \theta) \quad \textit{iff} \quad \begin{cases} (LFC'(L, dob, t, \theta) \\ \nexists L' \subsetneq L \quad LFC'(L', dob_{|L'}, t, \theta). \end{cases}$$

Semantics of Local Firings. We will now define formally the concurrent operational semantics that we obtain when we allow transitions to fire from a partial state if the local firing condition *LFC* is satisfied.

The time Petri net starts in an *initial maximal state* $\langle M_0, dob_0, lrd_0 \rangle$, which is given by the *initial marking* M_0 and the initial date θ_0. Initially, all the tokens carry the date θ_0 as date of birth and latest reading date: for all $p \in M_0$, $dob_0(p) \overset{\text{def}}{=} lrd_0(p) \overset{\text{def}}{=} \theta_0$.

The transition t can fire at date θ using the partial marking $L \subseteq M$, from the maximal state $\langle M, dob, lrd\rangle$ if $(L, dob_{|L}, t, \theta)$ satisfies LFC and for all $p \in L$, $\theta \geq lrd(p)$.

This action leads to the maximal state $\langle (M \setminus {}^\bullet t) \cup t^\bullet, dob', lrd'\rangle$ with $dob'(p) \stackrel{\text{def}}{=} \begin{cases} dob(p) & \text{if } p \in M \setminus {}^\bullet t \\ \theta & \text{if } p \in t^\bullet \end{cases}$ and $lrd'(p) \stackrel{\text{def}}{=} \begin{cases} lrd(p) & \text{if } p \in M \setminus L \\ \theta & \text{if } p \in (L \setminus {}^\bullet t) \cup t^\bullet. \end{cases}$

We call *sequence of local firings* starting from the initial state S_0 any sequence $((t_1, L_1, \theta_1), \ldots, (t_n, L_n, \theta_n))$ where there exist states $S_1, \ldots, S_n$ such that for all $i \in \{1, \ldots, n\}$, firing t_i from S_{i-1} at date θ_i using the partial marking L_i is possible and leads to S_i. The empty sequence of local firings is denoted ϵ.

Extended Processes. We will define a notion of *extended process*, which is close to the notion of process, but the events are replaced by *extended events* which represent firings from partial states and keep track of all the conditions corresponding to the partial state, not only those that are consumed by the transition: the other conditions will be treated as context of the event. This uses classical techniques of *contextual nets* or nets with *read arcs* (see [16,17]). It would also be possible to consume and rewrite the conditions in the context of an event, but we feel that the notion of read arc or contextual net is a good way to capture the idea that we develop here.

For all extended event $\dot{e} \stackrel{\text{def}}{=} (B, t)$, denote $\tau(\dot{e}) \stackrel{\text{def}}{=} t$ and $\dot{e}^\bullet \stackrel{\text{def}}{=} \{(\dot{e}, p) \mid p \in t^\bullet\}$. In an extended event, not all the conditions of B are consumed, but only ${}^\bullet\dot{e} \stackrel{\text{def}}{=} Place^{-1}_{|B}({}^\bullet t)$; the conditions in $\underline{\dot{e}} \stackrel{\text{def}}{=} B \setminus {}^\bullet\dot{e}$ are only *read* by $\dot{e}$, which is represented by read arcs. Like for processes, we define the set of conditions that remain at the end of the extended process $\langle \dot{E}, \Theta\rangle$ as $\uparrow(\dot{E}) \stackrel{\text{def}}{=} \bigcup_{\dot{e} \in \dot{E}} \dot{e}^\bullet \setminus \bigcup_{\dot{e} \in \dot{E}} {}^\bullet\dot{e}$.

The function $\dot{\Pi}$ that maps each sequence of local firings $((t_1, L_1, \theta_1), \ldots, (t_n, L_n, \theta_n))$ to an extended process is defined as follows:

- Like for processes, $\dot{\Pi}(\epsilon) \stackrel{\text{def}}{=} \langle \{\bot\}, \{(\bot, \theta_0)\}\rangle$, where $\bot \stackrel{\text{def}}{=} (\emptyset, \text{-})$ represents the initial event. The set of conditions that are created by $\bot$ is defined as: $\bot^\bullet \stackrel{\text{def}}{=} \{(\bot, p) \mid p \in M_0\}$.
- $\dot{\Pi}(((t_1, L_1, \theta_1), \ldots, (t_{n+1}, L_{n+1}, \theta_{n+1}))) \stackrel{\text{def}}{=} \langle \dot{E} \cup \{\dot{e}\}, \Theta \cup \{(\dot{e}, \theta_{n+1})\}\rangle$, where $\langle \dot{E}, \Theta\rangle \stackrel{\text{def}}{=} \dot{\Pi}(((t_1, L_1, \theta_1), \ldots, (t_n, L_n, \theta_n)))$ and the extended event $\dot{e} \stackrel{\text{def}}{=} (Place^{-1}_{|\uparrow(\dot{E})}(L_{n+1}), t_{n+1})$ represents the last local firing of the sequence.

The set of all the extended processes obtained as the image by $\dot{\Pi}$ of the sequences of local firings is denoted $\dot{X}$.

As we use read arcs, the usual causality is not sufficient any more: we have to define an unconditional or strong causality $\rightarrow$ and a conditional or weak causality $\nearrow$ between extended events as:

- $\dot{e} \rightarrow \dot{f}$ iff $\dot{e}^\bullet \cap ({}^\bullet\dot{f} \cup \underline{\dot{f}}) \neq \emptyset$ and
- $\dot{e} \nearrow \dot{f}$ iff $(\dot{e} \rightarrow \dot{f}) \vee (\underline{\dot{e}} \cap {}^\bullet\dot{f} \neq \emptyset)$.

For all extended event $\dot{e}$, we denote $\lceil \dot{e} \rceil \stackrel{\text{def}}{=} \{\dot{f} \in \dot{E} \mid \dot{f} \rightarrow^* \dot{e}\}$ and for all set $\dot{E}$ of extended events, $\lceil \dot{E} \rceil \stackrel{\text{def}}{=} \bigcup_{\dot{e} \in \dot{E}} \lceil \dot{e} \rceil$.

Figure 2 shows several extended processes. An arrow from a condition b to an extended event $\dot{e}$ means that $b \in {}^\bullet\dot{e}$. An arrow from an extended event $\dot{e}$ to a condition b means that $b \in \dot{e}^\bullet$. When $b \in \underline{\dot{e}}$, the read arc is represented by a line without arrow between b and $\dot{e}$.

Definition 9 ($\boldsymbol{RS(\langle \dot{E}, \Theta \rangle)}$). *The maximal state that is reached after an extended process $\langle \dot{E}, \Theta \rangle$ is defined as $RS(\langle \dot{E}, \Theta \rangle) \stackrel{\text{def}}{=} \langle Place(\uparrow(\dot{E})), dob, lrd \rangle$ where for all $b = ({}^\bullet b, p) \in \uparrow(\dot{E})$, $dob(p) \stackrel{\text{def}}{=} \Theta({}^\bullet b)$ and $lrd(p) \stackrel{\text{def}}{=} \max_{\dot{e} \in \dot{E},\, b \in \dot{e}^\bullet \cup \underline{\dot{e}}} \Theta(\dot{e})$.*

Remark that all the sequences of local firings σ such that $\dot{\Pi}(\sigma) = \langle \dot{E}, \Theta \rangle$ lead to $RS(\langle \dot{E}, \Theta \rangle)$.

Definition 10 (temporally complete extended process, $\dot{\boldsymbol{Y}}$). *We say that $\langle \dot{E}, \Theta \rangle$ is* temporally complete *if $RS(\langle \dot{E}, \Theta \rangle)$ is temporally consistent. The set of all temporally complete extended processes is denoted $\dot{Y}$.*

Correctness and Completeness of *LFC*. Each extended event $\dot{e}$ can be mapped to the corresponding event

$$h(\dot{e}) \stackrel{\text{def}}{=} \Big(\big\{ (h(\dot{f}), p) \mid (\dot{f}, p) \in {}^\bullet\dot{e} \big\}, \tau(\dot{e}) \Big) .$$

Given an extended process $\langle \dot{E}, \Theta \rangle \in \dot{X}$, $\langle h(\dot{E}), \Theta \circ h^{-1}_{|\dot{E}} \rangle$ is intuitively what we obtain if we remove the read arcs from $\langle \dot{E}, \Theta \rangle$. For example the extended process $\dot{x}$ in Figure 2 would be mapped to the process of Figure 1.

Lemma 1. *For all $\langle \dot{E}, \Theta \rangle \in \dot{X}$, $\langle h(\dot{E}), \Theta \circ h^{-1}_{|\dot{E}} \rangle \in X$ iff $\langle \dot{E}, \Theta \rangle \in \dot{Y}$.*

Proof. Let $\langle \dot{E}, \Theta \rangle \in \dot{X}$ be an extended process and denote $\langle M, dob, lrd \rangle \stackrel{\text{def}}{=} RS(\langle \dot{E}, \Theta \rangle)$ and $\theta \stackrel{\text{def}}{=} \max_{p \in M} lrd(p) = \max_{\dot{e} \in \dot{E}} \Theta(\dot{e})$.

It follows from the definition of the processes that if $\langle h(\dot{E}), \Theta \circ h^{-1}_{|\dot{E}} \rangle \in X$, then $\langle \dot{E}, \Theta \rangle$ is temporally complete.

Conversely, assume that $\langle \dot{E}, \Theta \rangle$ is temporally complete. Choose $\dot{e} \in \dot{E}$ such that $\Theta(\dot{e}) = \theta$ and $\nexists \dot{f} \in \dot{E}$ such that $\dot{e} \nearrow \dot{f}$. Then denote $\langle M', dob', lrd' \rangle \stackrel{\text{def}}{=} RS(\langle \dot{E} \setminus \{\dot{e}\}, \Theta \rangle)$ and $\theta' \stackrel{\text{def}}{=} \max_{p \in M'} lrd'(p)$, and let $t \in T$ such that ${}^\bullet t \subseteq M'$. If ${}^\bullet t \cap {}^\bullet\tau(\dot{e}) = \emptyset$, then $doe'(t) = doe(t) \geq \theta - lfd(t) \geq \theta' - lfd(t)$. Otherwise let $L \stackrel{\text{def}}{=} {}^\bullet\dot{e} \cup \underline{\dot{e}}$. As $LFC(L, dob, \tau(\dot{e}), \Theta(\dot{e}))$ holds, then

$$\begin{cases} \quad \exists p \in {}^\bullet t \quad \bar{p} \cap L \neq \emptyset \\ \vee\, \theta \leq \displaystyle\max_{p \in {}^\bullet t \cap L} dob'(p) + lfd(t) \end{cases}$$

As ${}^\bullet t \subseteq M'$, then $\nexists p \in {}^\bullet t$ such that $\bar{p} \cap L \neq \emptyset$; thus $\theta \leq \displaystyle\max_{p \in {}^\bullet t \cap L} dob'(p) + lfd(t)$. Hence $doe'(t) = \displaystyle\max_{p \in {}^\bullet t} dob'(p) \geq \max_{p \in {}^\bullet t \cap L} dob'(p) \geq \theta - lfd(t) \geq \theta' - lfd(t)$. As a result $\langle \dot{E} \setminus \{\dot{e}\}, \Theta \rangle \in \dot{Y}$.

Assume now that $\langle E, \Theta' \rangle \stackrel{\text{def}}{=} \langle h(\dot{E} \setminus \{\dot{e}\}), \Theta \circ h^{-1}_{|\dot{E}} \rangle \in X$. It leads to the global state $\langle M', dob', \theta' \rangle$. As ${}^\bullet\tau(\dot{e}) \subseteq M'$ and $\theta \geq \theta'$ and $\theta \geq doe'(\tau(\dot{e})) + efd(\tau(\dot{e}))$ and for all $t \in T$, ${}^\bullet t \subseteq M' \implies \theta \leq doe'(t) + lfd(t)$, then $\tau(\dot{e})$ can fire at date θ from $\langle M', dob', \theta' \rangle$, which is coded by the event $(Place^{-1}_{|\uparrow(E)}(\tau(\dot{e})), \tau(\dot{e})) = h(\dot{e})$. Thus $\langle h(\dot{E}), \Theta \circ h^{-1}_{|\dot{E}} \rangle \in X$.

Theorem 1 (correctness of *LFC*). *For all extended process $\langle \dot{E}, \Theta \rangle \in \dot{X}$, $\langle h(\dot{E}), \Theta \circ h^{-1}_{|\dot{E}} \rangle$ is a pre-process (notice that $h_{|\dot{E}}$ is injective). In other terms there exists a process $\langle E', \Theta' \rangle \in X$ such that $\langle h(\dot{E}), \Theta \circ h^{-1}_{|\dot{E}} \rangle \leq \langle E', \Theta' \rangle$.*

Proof. To prove that *LFC* is correct, we will prove that for all $\langle \dot{E}, \Theta \rangle \in \dot{X}$, there exists $\langle \dot{E}', \Theta' \rangle \in \dot{Y}$ such that $\dot{E} \subseteq \dot{E}'$ and $\Theta = \Theta'_{|\dot{E}}$; as a consequence $\langle h(\dot{E}), \Theta \circ h^{-1}_{|\dot{E}} \rangle \leq \langle h(\dot{E}'), \Theta' \circ h^{-1}_{|\dot{E}'} \rangle \in X$.

Let $\langle \dot{E}, \Theta \rangle \in \dot{X}$. If $\langle \dot{E}, \Theta \rangle$ is temporally complete, then it is sufficient to take $\langle \dot{E}', \Theta' \rangle \stackrel{\text{def}}{=} \langle \dot{E}, \Theta \rangle$.

Otherwise, denote $\langle M, dob, lrd \rangle \stackrel{\text{def}}{=} RS(\langle \dot{E}, \Theta \rangle)$ and $\theta \stackrel{\text{def}}{=} \max_{p \in M} lrd(p)$, choose $t \in T$ such that ${}^\bullet t \subseteq M \wedge \theta > doe(t) + lfd(t)$ and such that t minimizes $\theta_t \stackrel{\text{def}}{=} doe(t) + lfd(t)$. Let $\dot{F} \stackrel{\text{def}}{=} \{\dot{f} \in \dot{E} \mid \Theta(\dot{f}) \leq \theta_t\}$. $\langle \dot{F}, \Theta_{|\dot{F}} \rangle$ is a temporally complete extended process. Denote $\langle M', dob', lrd' \rangle \stackrel{\text{def}}{=} RS(\langle \dot{F}, \Theta_{|\dot{F}} \rangle)$. $LFC'(M', dob', t, \theta_t)$ holds. Thus there exists $L \subseteq M'$ such that $LFC(L, dob'_{|L}, t, \theta_t)$ holds. Let $\dot{e} \stackrel{\text{def}}{=} (Place^{-1}_{|\uparrow(\dot{F})}(L), t)$. We will show that $\langle \dot{E} \cup \{\dot{e}\}, \Theta \cup \{(\dot{e}, \theta_t)\} \rangle \in \dot{X}$. $\Theta \cup \{(\dot{e}, \theta_t)\}$ is compatible with $\nearrow$: if an extended event $\dot{f} \in \dot{E}$ is such that $\underline{\dot{f}} \cap {}^\bullet\dot{e} \neq \emptyset$, then $\Theta(\dot{f}) \leq \theta_t$ and if ${}^\bullet\dot{f} \cap \underline{\dot{e}} \neq \emptyset$, then $\Theta(\dot{f}) > \theta_t$. The strict inequality in the second case also guarantees that $\nearrow$ is acyclic on $\dot{E} \cup \{\dot{e}\}$. As a result, we have built an extended process $\langle \dot{E} \cup \{\dot{e}\}, \Theta \cup \{(\dot{e}, \theta_t)\} \rangle \in \dot{X}$ by adding the event to $\langle \dot{E}, \Theta \rangle$.

Iterating this until $\langle \dot{E}, \Theta \rangle$ is temporally complete, terminates if we assume that time diverges: at each step $\langle \dot{F}, \Theta_{|\dot{F}} \rangle$ is temporally complete, so $\langle h(\dot{F}), \Theta \circ h^{-1}_{|\dot{F}} \rangle \in X$; moreover this process has strictly more events at each step and the dates remain below θ, which does not increase.

Theorem 2 (completeness of *LFC*). *For all process $\langle E, \Theta \rangle \in X$, there exists an extended process $\langle \dot{E}, \Theta' \rangle \in \dot{X}$ such that $\langle h(\dot{E}), \Theta' \circ h^{-1}_{|\dot{E}} \rangle = \langle E, \Theta \rangle$.*

Proof. Let $\langle E, \Theta \rangle \in X$ leading to the global state $\langle M, dob, \theta \rangle$, let $t \in T$ be a transition that can fire at date $\theta' \geq \theta$ from $\langle M, dob, \theta \rangle$, and assume that there exists an extended process $\langle \dot{E}, \Theta' \rangle \in \dot{X}$ such that $\langle h(\dot{E}), \Theta' \circ h^{-1}_{|\dot{E}} \rangle = \langle E, \Theta \rangle$. $LFC'(M, dob, t, \theta')$ holds. Thus there exists $L \subseteq M$ such that $LFC(L, dob_{|L}, t, \theta')$ holds. Define $\dot{e} \stackrel{\text{def}}{=} (Place^{-1}_{|\uparrow\dot{E}}(L), t)$. $\langle \dot{E} \cup \{\dot{e}\}, \Theta' \cup \{(\dot{e}, \theta')\} \rangle \in \dot{X}$ and the event $h(\dot{e})$ codes the firing of t at date θ' after $\langle E, \Theta \rangle$.

3.3 Symbolic Unfoldings of Safe Time Petri Nets

We have explained in Section 3.1 that the definition of the unfolding has to rely on a concurrent operational semantics. We will now show how the extended processes obtained from our concurrent operational semantics for time Petri nets can be superimposed to build a symbolic unfolding, and that it is easy to recover the extended processes from their superimposition and to build the unfolding. After the definition, we give two theorems: the first one gives a way to extract extended processes from the unfolding, while the second theorem gives a direct construction of the unfolding.

Definition 11 (symbolic unfolding). *We define the* symbolic unfolding U *of a time Petri net by collecting all the extended events that appear in its extended processes:* $U \stackrel{\text{def}}{=} \bigcup_{\langle \dot{E}, \Theta \rangle \in \dot{X}} \dot{E}$.

For all set B of conditions such that $place_{|B}$ is injective and for all mapping $\Theta : \bigcup_{b \in B} \lceil {}^\bullet b \rceil \longrightarrow Q$, we denote $dob_{B,\Theta}$ the mapping defined as:
for all $p \in Place(B)$, $dob_{B,\Theta}(p) \stackrel{\text{def}}{=} \Theta({}^\bullet(place_{|B}^{-1}(p)))$.

Theorem 3. *Let $\dot{E} \subseteq U$ be a nonempty finite set of extended events and $\Theta : \dot{E} \longrightarrow Q$ associate a firing date with each extended event of $\dot{E}$. $\langle \dot{E}, \Theta \rangle$ is an extended process iff:*

$$\begin{cases} \lceil \dot{E} \rceil = \dot{E} & (\dot{E} \text{ is causally closed}) \\ \nexists \dot{e}, \dot{e}' \in \dot{E} \quad \dot{e} \neq \dot{e}' \ \wedge\ {}^\bullet\dot{e} \cap {}^\bullet\dot{e}' \neq \emptyset & (\dot{E} \text{ is conflict free}) \\ \nexists \dot{e}_0, \dot{e}_1, \ldots, \dot{e}_n \in \dot{E} \quad \dot{e}_0 \nearrow \dot{e}_1 \nearrow \cdots \nearrow \dot{e}_n \nearrow \dot{e}_0 & (\nearrow \text{ is acyclic on } \dot{E}) \\ \forall \dot{e}, \dot{e}' \in \dot{E} \quad \dot{e} \nearrow \dot{e}' \implies \Theta(\dot{e}) \leq \Theta(\dot{e}') & (\Theta \text{ is compatible with } \nearrow) \\ \forall \dot{e} = (B,t) \in \dot{E} \setminus \{\bot\} \quad LFC\,(Place(B), dob_{B,\Theta}, t, \Theta(\dot{e})) & \\ & (\dot{e} \text{ corresponds to a local firing condition}) \end{cases}$$

Proof. Let $\langle \dot{E}, \Theta \rangle \in \dot{X}$ be an extended process that satisfies the conditions in the curly brace, let $\dot{e} \stackrel{\text{def}}{=} (B,t)$ with $B \subseteq \uparrow(\dot{E})$ and $t \in T$ and $\theta' \geq \max_{\dot{f} \in \dot{E},\ \dot{f} \nearrow \dot{e}} \Theta(\dot{f})$ such that $LFC(Place(B), dob_{B,\Theta}, t, \theta')$ holds. Then we will show that the extended process $\langle \dot{E}', \Theta' \rangle \stackrel{\text{def}}{=} \langle \dot{E} \cup \{\dot{e}\}, \Theta \cup \{(\dot{e}, \theta')\} \rangle$ also satisfies the conditions in the curly brace. By construction $\dot{E}'$ is causally closed. Moreover for each condition $b \in {}^\bullet\dot{e}$ that is consumed by $\dot{e}$, $b \in \uparrow(\dot{E})$, which implies that b has not been consumed by any event of $\dot{E}$. Thus for all $\dot{f} \in \dot{E}$, ${}^\bullet\dot{e} \cap {}^\bullet\dot{f} = \emptyset$ and $\neg(\dot{e} \nearrow \dot{f})$. So $\dot{E}'$ is conflict free and $\nearrow$ is acyclic on $\dot{E}'$. Θ' is compatible with $\nearrow$ because Θ is compatible with $\nearrow$ and $\Theta'(\dot{e}) = \theta' \geq \max_{\dot{f} \in \dot{E},\ \dot{f} \nearrow \dot{e}} \Theta(\dot{f})$.

Conversely let $\langle \dot{E}', \Theta' \rangle$ satisfy the conditions in the curly brace. If $\dot{E}' = \{\bot\}$, then $\langle \dot{E}', \Theta' \rangle \in \dot{X}$. Otherwise let $\dot{e} \in \dot{E}'$ be an extended event that has no successor by $\nearrow$ in $\dot{E}'$ (such an extended event exists since $\nearrow$ is acyclic on $\dot{E}'$). $\langle \dot{E}, \Theta \rangle \stackrel{\text{def}}{=} \langle \dot{E}' \setminus \{\dot{e}\}, \Theta'_{|\dot{E}' \setminus \{\dot{e}\}} \rangle$ satisfies the conditions in the curly brace. Assume that $\langle \dot{E}, \Theta \rangle \in \dot{X}$. As $\dot{E}$ is conflict free, ${}^\bullet\dot{e} \subseteq \uparrow(\dot{E})$. And as $\dot{e}$ has no successor by $\nearrow$ in $\dot{E}'$, $\underline{\dot{e}} \subseteq \uparrow(\dot{E})$. Furthermore $\Theta'(\dot{e}) \geq \max_{\dot{f} \in \dot{E},\ \dot{f} \nearrow \dot{e}} \Theta(\dot{f})$ and $LFC\left(Place({}^\bullet\dot{e} \cup \underline{\dot{e}}), dob_{{}^\bullet\dot{e} \cup \underline{\dot{e}}, \Theta}, \tau(\dot{e}), \Theta'(\dot{e})\right)$ holds. Thus $\langle \dot{E}', \Theta' \rangle = \langle \dot{E} \cup \{\dot{e}\}, \Theta \cup \{(\dot{e}, \Theta'(\dot{e}))\} \rangle \in \dot{X}$.

Theorem 4. *For all* $\dot{e} \stackrel{\text{def}}{=} (B,t) \in (\bigcup_{\dot{f} \in U} \dot{f}^\bullet) \times T, \quad \dot{e} \in U$ *iff*

$$\begin{cases} \nexists \dot{f}, \dot{f}' \in \lceil \dot{e} \rceil \quad \dot{f} \neq \dot{f}' \ \wedge \ {}^\bullet\dot{f} \cap {}^\bullet\dot{f}' \neq \emptyset & (1) \\ \nexists \dot{e}_0, \dot{e}_1, \ldots, \dot{e}_n \in \lceil \dot{e} \rceil \quad \dot{e}_0 \nearrow \dot{e}_1 \nearrow \cdots \nearrow \dot{e}_n \nearrow \dot{e}_0 & (2) \\ \exists \Theta : \lceil \dot{e} \rceil \longrightarrow Q \quad \begin{Bmatrix} \forall \dot{f}, \dot{f}' \in \lceil \dot{e} \rceil \quad \dot{f} \nearrow \dot{f}' \implies \Theta(\dot{f}) \leq \Theta(\dot{f}') \\ \forall \dot{f} = (B', t') \in \lceil \dot{e} \rceil \setminus \{\bot\} \\ \qquad LFC\big(Place(B'), dob_{B',\Theta}, t, \Theta(\dot{f})\big) \end{Bmatrix} & (3) \end{cases}$$

This theorem allows us to simply build the unfolding starting from the set $\{\bot\}$ and adding extended events one by one when they satisfy the condition.

Proof. Let $\dot{e} \in U$. There exists $\langle \dot{E}, \Theta' \rangle \in \dot{X}$ such that $\dot{e} \in \dot{E}$. $\langle \dot{E}, \Theta' \rangle$ satisfies the conditions in the curly brace of Theorem 3. As $\lceil \dot{E} \rceil \subseteq \dot{E}$, $\lceil \dot{e} \rceil$ also satisfies them. Then (1) and (2) hold. For (3) a possible Θ is $\Theta'_{|\lceil \dot{e} \rceil}$.

Conversely if $\dot{e} \stackrel{\text{def}}{=} (B,t)$ satisfies (1), (2) and (3), consider a possible Θ for (3). $\langle \lceil \dot{e} \rceil \setminus \{\dot{e}\}, \Theta \rangle$ satisfies the curly brace of Theorem 3. Then $\langle \lceil \dot{e} \rceil \setminus \{\dot{e}\}, \Theta \rangle \in \dot{X}$. Moreover (1) implies that $B \subseteq \uparrow(\lceil \dot{e} \rceil \setminus \{\dot{e}\})$. In addition $\Theta(\dot{e}) \geq \max_{\dot{f} \in \lceil \dot{e} \rceil,\, \dot{f} \nearrow \dot{e}} \Theta(\dot{f})$ and $LFC(Place(B), dob_{B,\Theta}, t, \Theta(\dot{e}))$ holds. Thus $\langle \lceil \dot{e} \rceil, \Theta \rangle \in \dot{X}$ and therefore $\dot{e} \in U$.

4 Complete Finite Prefixes

We have defined the symbolic unfolding of a time Petri net. In general this structure is infinite, as well as the unfoldings of untimed Petri nets. However in the untimed case it is possible to define a finite prefix of the unfolding, which contains complete information about the unfolding [6,7]. To construct this complete finite prefix one remarks that each untimed safe Petri net has finitely many markings, and that if two processes reach the same marking, then they have the same possible futures. With time Petri nets, the same is true with two temporally complete extended processes that reach the same consistent state. But in general there are infinitely many possible maximal states.

This is why we will try to group them as much as possible. The problem of the density of time has already been solved by the use of a symbolic representation of the dates. Another problem is that the time keeps progressing and never loops; this is why the age of the tokens will now be used instead of their date of birth. Recall that the date of birth was first preferred in order to define a concurrent semantics where the system is allowed to reach temporally inconsistent states, that is states where the different parts of the net have not reached the same date; from now we will work with temporally consistent states.

A last problem arises: even the age of a token may progress forever. But we will define a *reduced age* for each token in a marking, which gives enough information to know what actions are possible, and remains bounded.

4.1 Equivalence of Two Maximal States

It was already shown in [9] that the age of the tokens can be reduced to bounded values without losing information about the possible future actions.

Definition 12 (reduced age of a token). *The* reduced age $J_S(p)$ *of the token* $p \in M$ *in the maximal state* $S \stackrel{\text{def}}{=} \langle M, dob, lrd\rangle$ *as:*

$$J_S(p) \stackrel{\text{def}}{=} \min\{I_S(p), \max\{bound(t) \mid t \in T \wedge p \in {}^\bullet t\}\}$$

where $bound(t) \stackrel{\text{def}}{=} \begin{cases} efd(t) & \text{if} \quad lfd(t) = \infty \\ lfd(t) & \text{otherwise.} \end{cases}$

Definition 13 (equivalence of two maximal states). *Two maximal states* $S_1 \stackrel{\text{def}}{=} \langle M_1, dob_1, lrd_1\rangle$ *and* $S_2 \stackrel{\text{def}}{=} \langle M_2, dob_2, lrd_2\rangle$ *are* equivalent *(denoted* $S_1 \sim S_2$*) iff* $M_1 = M_2$ *and* $J_{S_1} = J_{S_2}$.

Theorem 5 (firing a transition from two equivalent consistent states). *Let* S_1 *and* S_2 *be two equivalent consistent states. Let* M *be their marking. A transition* t *can fire from* S_1 *at date* $\theta_1 \geq \max_{p\in M} lrd_1(p)$ *using the partial marking* $L \subseteq M$ *iff it can fire from* S_2 *at date* $\theta_1 - \max_{p\in M} lrd_1(p) + \max_{p\in M} lrd_2(p)$ *using the same partial marking* L.

Proof. Denote $\langle M, dob_i, lrd_i\rangle \stackrel{\text{def}}{=} S_i$ and $\theta'_i \stackrel{\text{def}}{=} \max_{p\in M} lrd_i(p)$ for $i \in \{1, 2\}$. Assume that t can fire from S_1 at date $\theta_1 \geq \max_{p\in M} lrd_1(p)$ using the partial marking $L \subseteq M$. To prove that t can fire from S_2 at date $\theta_2 \stackrel{\text{def}}{=} \theta_1 - \theta'_1 + \theta'_2$ using the same partial marking L, we will show that:

1. $\theta_2 \geq doe_2(t) + efd(t)$, with $doe_2(t) \stackrel{\text{def}}{=} \max_{p\in {}^\bullet t} dob_2(p)$,
2. $\forall t' \in T \quad \begin{Bmatrix} {}^\bullet t' \cap L \neq \emptyset \\ \nexists p \in {}^\bullet t' \quad \bar{p} \cap L \neq \emptyset \end{Bmatrix} \implies \theta_2 \leq \max\limits_{p\in {}^\bullet t' \cap L} dob_2(p) + lfd(t')$.

Here are the proofs for these two points:

1. If $\min_{p\in {}^\bullet t} J_{S_1}(p) \geq efd(t)$, then $\min_{p\in {}^\bullet t} I_{S_2}(p) \geq \min_{p\in {}^\bullet t} J_{S_2}(p) = \min_{p\in {}^\bullet t} J_{S_1}(p) \geq efd(t)$ and $\theta_1 \geq \theta'_1$ implies that $\theta_2 \geq \theta'_2$. Furthermore $\theta'_2 = doe_2(t) + \min_{p\in {}^\bullet t} I_{S_2}(p) \geq doe_2(t) + efd(t)$.
   Otherwise, (if $\min_{p\in {}^\bullet t} J_{S_1}(p) < efd(t)$), then $\theta_1 \geq doe_1(t) + efd(t) = \theta'_1 - \min_{p\in {}^\bullet t} I_{S_1}(p) + efd(t)$. And $\min_{p\in {}^\bullet t} I_{S_1}(p) = \min_{p\in {}^\bullet t} I_{S_2}(p)$ because for all p such that $I_{S_1}(p) < efd(t)$, $I_{S_1}(p) = J_{S_1}(p) = J_{S_2}(p) = I_{S_2}(p)$ (the equalities between $I_{S_i}(p)$ and $J_{S_i}(p)$ hold since one of them is strictly smaller than $efd(t)$), and for all p such that $I_{S_1}(p) \geq efd(t)$, $I_{S_2}(p) \geq J_{S_2}(p) = J_{S_1}(p) \geq efd(t)$. Thus $\theta_2 \geq \theta'_2 - \min_{p\in {}^\bullet t} I_{S_2}(p) + efd(t) = doe_2(t) + efd(t)$.
2. Let $t' \in T$ such that ${}^\bullet t' \cap L \neq \emptyset$ and ($\nexists p \in {}^\bullet t' \quad \bar{p} \cap L \neq \emptyset$). Then $\theta_1 \leq \max_{p\in {}^\bullet t' \cap L} dob_1(p) + lfd(t')$.
   If $lfd(t') = \infty$ then $\max_{p\in {}^\bullet t' \cap L} dob_2(p) + lfd(t') = \infty \geq \theta_2$.
   Otherwise for $i \in \{1, 2\}$, $\max_{p\in {}^\bullet t' \cap L} dob_i(p) = \theta'_i - \min_{p\in {}^\bullet t' \cap L} I_{S_i}(p)$. Then $\theta'_1 \leq \theta_1 \leq \theta'_1 - \min_{p\in {}^\bullet t' \cap L} I_{S_1}(p) + lfd(t')$, and consequently $\min_{p\in {}^\bullet t' \cap L} I_{S_1}(p) \leq lfd(t')$. So $\min_{p\in {}^\bullet t' \cap L} I_{S_2}(p) \geq \min_{p\in {}^\bullet t' \cap L} I_{S_1}(p)$ because for all p such that $I_{S_1}(p) \leq lfd(t')$, $I_{S_1}(p) = J_{S_1}(p) = J_{S_2}(p) \leq I_{S_2}(p)$, and for all p such that $I_{S_1}(p) > lfd(t')$, $I_{S_2}(p) \geq J_{S_2}(p) = J_{S_1}(p) \geq lfd(t')$. Thus $\theta_2 \leq \theta'_2 - \min_{p\in {}^\bullet t' \cap L} I_{S_2}(p) + lfd(t') = \max_{p\in {}^\bullet t' \cap L} dob_2(p) + lfd(t')$.

4.2 Substitution of Prefixes in Extended Processes

Knowing that the same actions are possible from equivalent consistent states, if we have two temporally complete extended processes that reach equivalent states, we can translate any continuation of one extended process to the other, providing we also translate the firing dates of the events. This operation is illustrated in Figure 2. It corresponds intuitively to merging the final conditions of the first extended process with the conditions from which the extension starts in the second process.

Definition 14 (substitution of prefixes in extended processes). *Let* $\dot{x}_1 \stackrel{\text{def}}{=} \langle \dot{E}_1, \Theta_1 \rangle$ *and* $\dot{x}_2 \stackrel{\text{def}}{=} \langle \dot{E}_2, \Theta_2 \rangle$ *be two extended processes, and* $\dot{E}'_2 \subseteq \dot{E}_2$ *such that* $\dot{x}_1$ *and* $\langle \dot{E}'_2, {\Theta_2}_{|\dot{E}'_2} \rangle$ *are temporally complete extended processes,* $RS(\langle \dot{E}'_2, {\Theta_2}_{|\dot{E}'_2} \rangle) \sim RS(\langle \dot{E}_1, \Theta_1 \rangle)$ *and for all* $\dot{e}' \in \dot{E}'_2$ *and* $\dot{e} \in \dot{E}_2 \setminus \dot{E}'_2$, $\Theta(\dot{e}'_2) \leq \Theta(\dot{e}_2)$ *and* $\neg(\dot{e}'_2 \nearrow \dot{e}_2)$*. We define the* substitution *which replaces* $\langle \dot{E}'_2, {\Theta_2}_{|\dot{E}'_2} \rangle$ *by* $\dot{x}_1$ *in* $\dot{x}_2$ *as:*

$$subst(\dot{x}_1, \dot{E}'_2, \dot{x}_2) \stackrel{\text{def}}{=} \langle \dot{E}, \Theta \rangle$$

where

$$\dot{E} \stackrel{\text{def}}{=} \dot{E}_1 \cup \phi(\dot{E}_2 \setminus \dot{E}'_2)$$

$$\Theta(\dot{e}) \stackrel{\text{def}}{=} \begin{cases} \Theta_1(\dot{e}) & \text{if } \dot{e} \in \dot{E}_1 \\ \Theta_2(\phi^{-1}(\dot{e})) - \max\limits_{\dot{f} \in \dot{E}'_2} \Theta_2(\dot{f}) + \max\limits_{\dot{f} \in \dot{E}_1} \Theta_1(\dot{f}) & \text{if } \dot{e} \in \phi(\dot{E}_2 \setminus \dot{E}'_2) \end{cases}$$

$$\forall \dot{e} \stackrel{\text{def}}{=} (B, t) \in \dot{E}_2 \setminus \dot{E}'_2 \quad \phi(\dot{e}) \stackrel{\text{def}}{=} (\psi(B), t)$$

$$\forall b \stackrel{\text{def}}{=} (\dot{e}, p) \in \textstyle\bigcup_{\dot{e} \in \dot{E}_2 \setminus \dot{E}'_2} {}^\bullet\dot{e} \cup \underline{\dot{e}} \quad \psi(b) \stackrel{\text{def}}{=} \begin{cases} (\phi(\dot{e}), p) & \text{if } \dot{e} \notin \dot{E}'_2 \\ place^{-1}_{|\uparrow(\dot{E}_1)}(p) & \text{if } \dot{e} \in \dot{E}'_2 \end{cases}$$

We generalize this notation to more than two extended processes as:

$$subst(\dot{x}_0, \dot{E}'_1, \dot{x}_1, \ldots, \dot{E}'_n, \dot{x}_n) \stackrel{\text{def}}{=} subst(subst(\dot{x}_0, \dot{E}'_1, \dot{x}_1, \ldots, \dot{E}'_{n-1}, \dot{x}_{n-1}), \dot{E}'_n, \dot{x}_n)$$

Theorem 6 ($\dot{X}$ is closed under substitution of prefixes). *Let* $\dot{x}_0, \ldots, \dot{x}_n \in \dot{X}$ *and* $\dot{E}'_1, \ldots, \dot{E}'_n$ *that satisfy the conditions required to define* $subst(\dot{x}_0, \dot{E}'_1, \dot{x}_1, \ldots, \dot{E}'_n, \dot{x}_n)$*. Then* $subst(\dot{x}_0, \dot{E}'_1, \dot{x}_1, \ldots, \dot{E}'_n, \dot{x}_n) \in \dot{X}$*.*

Proof. We detail the proof for the substitution $subst(\dot{x}_1, \dot{E}'_2, \dot{x}_2)$; the case of more than two extended processes follows immediately.
If $\dot{E}'_2 = \dot{E}_2$ then $subst(\dot{x}_1, \dot{E}'_2, \dot{x}_2) = \dot{x}_1 \in \dot{X}$. Now assume that the theorem is true when $\dot{E}_2 \setminus \dot{E}'_2$ has n elements and consider the case where there are $n+1$ elements. Choose an extended event $\dot{e}_2 \stackrel{\text{def}}{=} (B, t) \in \dot{E}_2 \setminus \dot{E}'_2$ that is minimal in $\dot{E}_2 \setminus \dot{E}'_2$ w.r.t. causality ($\nearrow$) and temporal ordering by Θ_2. Theorem 5 says that t can fire from $RS(\dot{x}_1)$ at date $\theta_1 \stackrel{\text{def}}{=} \Theta_2(\dot{e}_2) - \max_{\dot{e} \in \dot{E}'_2} \Theta_2(\dot{e}) + \max_{\dot{e} \in \dot{E}'_1} \Theta_1(\dot{e})$ using the same partial marking $L \stackrel{\text{def}}{=} Place(B)$. This firing can be coded by the extended event $\dot{e}_1 \stackrel{\text{def}}{=} (Place^{-1}_{|\uparrow(\dot{E}_1)}(L), t)$, and $\dot{x}'_1 \stackrel{\text{def}}{=} \langle \dot{E}_1 \cup \{\dot{e}_1\}, \Theta_1 \cup \{(\dot{e}_1, \theta_1)\} \rangle \in \dot{Y}$. Moreover $subst(\dot{x}_1, \dot{E}'_2, \dot{x}_2)$ equals $subst(\dot{x}'_1, \dot{E}'_2 \cup \{\dot{e}_2\}, \dot{x}_2)$, which belongs to $\dot{X}$ since $\dot{E}_2 \setminus (\dot{E}'_2 \cup \{\dot{e}_2\})$ has n elements.

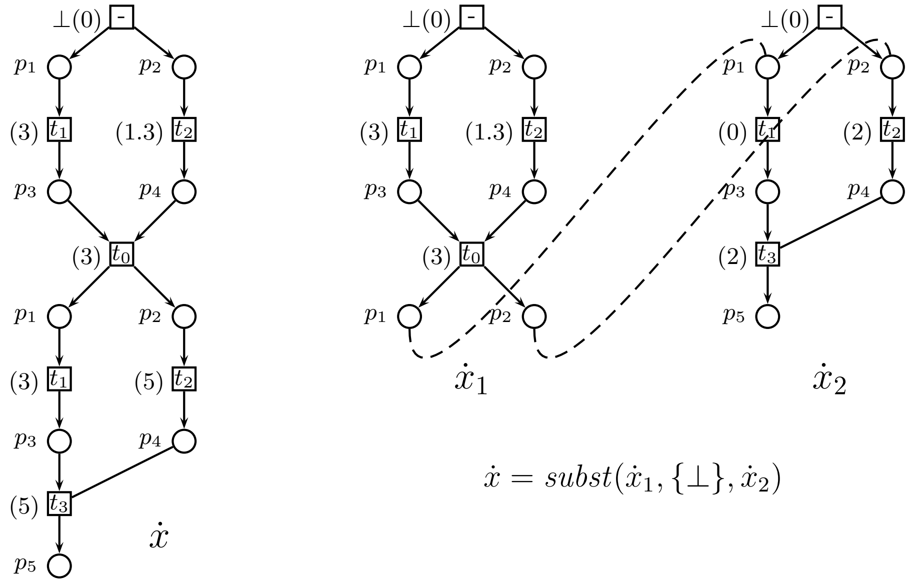


Fig. 2. Substitution of prefixes in extended processes. The dashed curves show how the final conditions of $\dot{x}_1$ are merged with the conditions of $\uparrow(\{\bot\})$ in $\dot{x}_2$.

4.3 Study of the Form of the Constraints

Now we have to deal with the fact that the unfolding we have defined is symbolic, and thus each event represents an action that may occur at several dates. We will show how to check that all the actions that are possible after a symbolic extended process are possible after another one. For this we have to take into account all the possible values for the date of the events of the symbolic extended processes. As well as Berthomieu defined a finite graph of symbolic state classes in [10] using the interleaving semantics, we show that the set of possible reduced ages after a symbolic extended process is taken in a finite set, which allows us to define a complete finite prefix of the symbolic unfolding of a time Petri net.

Definition 15 (constraints $\boldsymbol{predJ(\dot{E})}$). *Let $\dot{E}$ be a nonempty, causally closed, finite set of extended events and $M \stackrel{\text{def}}{=} Place(\uparrow(\dot{E}))$. We define the predicate $predJ(\dot{E})$ as follows: for all $J : M \longrightarrow Q$, $predJ(\dot{E})(J)$ holds iff there exists $\Theta : \dot{E} \to Q$ such that $\langle \dot{E}, \Theta \rangle \in \dot{Y}$ and $J = J_{RS(\langle \dot{E}, \Theta \rangle)}$.*

Theorem 7. *For each maximal marking M, the set of the $predJ(\dot{E})$ with $M \stackrel{\text{def}}{=} Place(\uparrow(\dot{E}))$ is finite.*

Proof. Recall that $predJ(\dot{E})$ is a predicate on the $J(p)$, $p \in M$. If we denote $\dot{e}_1, \ldots, \dot{e}_n$ the events of $\dot{E}$ and introduce a variable θ to represent $\max_{\dot{e} \in \dot{E}} \Theta(\dot{e})$, which plays a role in the definition of $J_{RS(\langle \dot{E}, \Theta \rangle)}$ and also in checking that $\langle \dot{E}, \Theta \rangle$ is temporally complete, we can write $predJ(\dot{E})(J)$ as:

$\exists \Theta(\dot{e}_1), \ldots, \Theta(\dot{e}_n), \theta \in Q$ such that

$$\begin{cases} \langle \dot{E}, \Theta \rangle \in \dot{X} \\ \theta = \max_{\dot{e} \in \dot{E}} \Theta(\dot{e}) \\ \forall t \in T \quad {}^\bullet t \subseteq M \implies \theta \leq \max_{p \in {}^\bullet t} \Theta({}^\bullet(place^{-1}_{|\uparrow(\dot{E})}(p))) + lfd(t) \\ \qquad\qquad\qquad\qquad \text{(to check that } \langle \dot{E}, \Theta \rangle \text{ is temporally complete)} \\ \forall p \in M \quad J(p) = \min\{I(p), \max\{bound(t) \mid t \in T \wedge p \in {}^\bullet t\}\} \\ \qquad\qquad\qquad\qquad \text{(with } I(p) \stackrel{\text{def}}{=} \theta - \Theta({}^\bullet(place^{-1}_{|\uparrow(\dot{E})}(p)))) \end{cases}$$

Consider the system in the curly brace and rewrite all the quantifiers that concern information about the structure of the time Petri net or the structure of $\dot{E}$ (including those coming from $(\langle \dot{E}, \Theta \rangle \in \dot{X})$) as disjunctions or conjunctions. For instance $(\exists p \in {}^\bullet t_0 \quad f(p))$ becomes $(f(p_3) \vee f(p_4))$. The result is a system of inequalities, some of which containing one "min" or one "max". These inequalities can be rewritten without "min" and "max", so that we obtain a boolean combination of inequalities of the following types:

$$\Theta(\dot{e}) \# \Theta(\dot{e}') + c \qquad \Theta(\dot{e}) \# \theta + c \qquad \Theta(\dot{e}) \# \theta - J(p)$$

where $\dot{e}$ and $\dot{e}'$ are events of $\dot{E}$, p is a place, c is a constant taken among the $efd(t)$ and $lfd(t)$ and $\#$ is an operator in $\{<, \leq, \geq, >\}$ ($=$ is not necessary).

Rewrite now this boolean combination of inequalities in normal disjunctive form. The quantifiers $(\exists \Theta(\dot{e}_1), \ldots, \Theta(\dot{e}_n), \theta \in Q)$ can be distributed in each term of the disjunction. $predJ(\dot{E})(J)$ becomes a disjunction of quantified conjunctions of inequalities of the types we have described before. We will now eliminate one by one the quantifiers $\exists \Theta(\dot{e}_i)$ in one quantified conjunction of inequalities: we show that there remains a quantified conjunction of inequalities of a slightly more general type than before:

$$\begin{array}{ll} \Theta(\dot{e}) \# \Theta(\dot{e}') + c & \\ \Theta(\dot{e}) \# \theta + c & J(p) \# c \\ \Theta(\dot{e}) \# \theta - J(p) + c & J(p) \# J(p') + c \end{array}$$

where the constants c may now be linear combinations of the $efd(t)$ and $lfd(t)$. To eliminate $\Theta(\dot{e}_i)$, we isolate it in each inequality when it appears, which leads to a conjunction C of $a < \Theta(\dot{e}_i)$, $b \leq \Theta(\dot{e}_i)$, $c \geq \Theta(\dot{e}_i)$ and $d > \Theta(\dot{e}_i)$, where a, b, c and d are terms of the form $(\Theta(\dot{e}) + c)$, $(\theta + c)$ or $(\theta - J(p) + c)$. Then $(\exists \Theta(\dot{e}_i) \quad C)$ is equivalent to the conjunction of all the inequalities $(a < c)$, $(a < d)$, $(b \leq c)$ and $(b < d)$, which all have one of the expected forms.

Once all the $\Theta(\dot{e}_i)$ have been eliminated, the remaining inequalities can be only of the form $J(p) \# c$ or $J(p) \# J(p') + c$. That is, θ does not appear any more. So the quantifier $\exists \theta$ can be removed.

Notice now that by definition $0 \leq J(p) \leq \max_p \stackrel{\text{def}}{=} \max\{bound(t) \mid t \in T \wedge p \in {}^\bullet t\}$ for all $p \in M$. Therefore all the inequalities of type $(J(p) \# c)$ with $|c| > \max_p$ can be immediately evaluated to **true** or **false**. The same happens for the inequalities of the form $(J(p) \# J(p') + c)$ with $|c| > \max\{\max_p, \max_{p'}\}$. The constants c that remain are bounded. Recall also that they are linear combinations of the $efd(t)$ and $lfd(t)$. Since the $efd(t)$ and $lfd(t)$ are rationals, there are finitely many acceptable values for the constants c.

As a consequence, there are finitely many interesting inequalities, and then finitely many conjunctions of such inequalities, and then finitely many disjunctions of such conjunctions. Finally there is a finite number of $predJ(\dot{E})$.

Let us take the example of $predJ(\{\bot, \dot{e}_1\})(J)$ using the extended events that are represented in Figure 3. It can be written, after some simplifications, as:

$$\exists \Theta(\bot), \Theta(\dot{e}_1), \theta \quad \begin{cases} \Theta(\dot{e}_1) \geq \Theta(\bot) \\ \theta = \max\{\Theta(\bot), \Theta(\dot{e}_1)\} \\ \theta - \Theta(\dot{e}_1) \leq 2 \\ \theta - \Theta(\bot) \leq 2 \\ J(p_2) = \min\{\theta - \Theta(\bot), 2\} \\ J(p_3) = \min\{\theta - \Theta(\dot{e}_1), 2\} \end{cases}$$

These inequalities can be rewritten without "min" and "max", so that we obtain a boolean combination of inequalities, which can be written in normal disjunctive form. Then the quantified variables can be eliminated one by one, and we obtain: $J(p_3) = 0 \ \wedge \ 0 \leq J(p_2) \leq 2$.

4.4 Complete Finite Prefix

Now we can define the complete finite prefix of the symbolic unfolding of a time Petri net, by keeping only a finite number of extended events, that contain all the information about the unfolding. More precisely, we show that every temporally complete extended process can be obtained by substitution of prefixes in extended processes that belong to the prefix. Figure 2 shows an example of such a decomposition. The complete finite prefix is represented in Figure 3. The idea behind the construction of the prefix is that a temporally complete extended process $\langle \dot{E}, \Theta \rangle$ will not be continued if the predicate $predJ(\dot{E})$ is equal to a $predJ(\dot{E}')$ with $|\dot{E}'| < |\dot{E}|$. As a possible improvement, the idea of adequate order, introduced by Esparza [7] seems to be usable in our framework.

Definition 16 ($\bar{X}$ and complete finite prefix $\bar{U}$). *We define the subset $\bar{X}$ of $\dot{X}$ as:*

$$\langle \dot{E}, \Theta \rangle \in \bar{X} \quad \textit{iff} \quad \exists \sigma \quad \begin{cases} \dot{\Pi}(\sigma) = \langle \dot{E}, \Theta \rangle \\ \nexists n', \sigma'' \quad |\sigma''| < n' < |\sigma| \ \wedge \ predJ(\dot{E}') = predJ(\dot{E}'') \end{cases}$$

where $\sigma \stackrel{\text{def}}{=} ((t_1, L_1, \theta_1), \ldots, (t_{|\sigma|}, L_{|\sigma|}, \theta_{|\sigma|}))$ and σ'' are sequences of local firings and $\dot{E}'$ (respectively $\dot{E}''$) is the set of events that appear in $\dot{\Pi}((t_1, L_1, \theta_1), \ldots, (t_{n'}, L_{n'}, \theta_{n'}))$ (respectively $\dot{\Pi}(\sigma'')$).

We define the finite complete prefix *$\bar{U}$ of the symbolic unfolding U of a time Petri net by collecting all the extended events that appear in the extended processes of $\bar{X}$: $\bar{U} \stackrel{\text{def}}{=} \bigcup_{\langle \dot{E}, \Theta \rangle \in \bar{X}} \dot{E}$.*

Denote N the cardinality of $\{predJ(\dot{E}) \mid \langle \dot{E}, \Theta \rangle \in \bar{X}\}$, which was proved finite in Section 4.3. The extended process $\dot{\Pi}(\sigma)$ may belong to $\bar{X}$ only if $|\sigma| < N$. Since there is a finite number of sequences of local firings that are shorter than N, there is a finite number of extended processes in $\bar{X}$ and each of them has less than N events (without $\bot$). Thus $\bar{U}$ is finite.

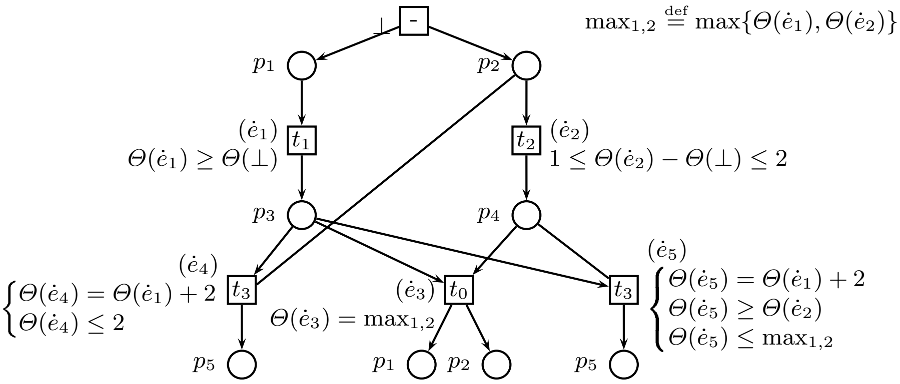


Fig. 3. The complete finite prefix of the symbolic unfolding of the time Petri net of Figure 1. The predicate $LFC(Place(B), dob_{B,\Theta}, t, \Theta(\dot{e}))$ is written near each extended event $\dot{e} \stackrel{\text{def}}{=} (B, t)$.

Theorem 8 (decomposition of an extended process in $\bar{U}$). *For all temporally complete extended process $\langle \dot{E}, \Theta \rangle \in \dot{Y}$, there exist extended processes $\dot{x}_0, \ldots, \dot{x}_n \in \bar{X}$ and $\dot{E}'_1, \ldots, \dot{E}'_m$ with $\dot{x}_i \stackrel{\text{def}}{=} \langle \dot{E}_i, \Theta_i \rangle$ for all $i \in \{0, \ldots, m\}$ and $\dot{E}'_i \subsetneq \dot{E}_i$ for all $i \in \{1, \ldots, m\}$, such that $\langle \dot{E}, \Theta \rangle = subst(\dot{x}_0, \dot{E}'_1, \dot{x}_1, \ldots, \dot{E}'_m, \dot{x}_m)$.*

Proof. To build the substitution we take the extended events in a total order that respects causality and temporal ordering. Each time we add an event, we try to add it at the end of the last extended process ($\dot{x}_m$) if it remains in $\bar{X}$. Otherwise we add an extended process $\dot{x}_{m+1}$ in the substitution. More formally, let $\langle \dot{E}, \Theta \rangle \in \dot{Y}$, $\dot{e} \stackrel{\text{def}}{=} (B, t) \in \dot{E}$ a maximal extended event in $\dot{E}$ w.r.t. causality ($\nearrow$) and temporal ordering by Θ, and assume that there exist $\dot{x}_0, \ldots, \dot{x}_n \in \bar{X}$ and $\dot{E}'_1, \ldots, \dot{E}'_m$ such that $\langle \dot{E} \setminus \{\dot{e}\}, \Theta \rangle = subst(\dot{x}_0, \dot{E}'_1, \dot{x}_1, \ldots, \dot{E}'_m, \dot{x}_m)$. Let $\langle \dot{E}_m, \Theta_m \rangle \stackrel{\text{def}}{=} \dot{x}_m$ and $\dot{x}'_m \stackrel{\text{def}}{=} \langle \dot{E}_m \cup \{\dot{e}'\}, \Theta'_m \rangle \stackrel{\text{def}}{=} subst(\dot{x}_m, \dot{E} \setminus \{\dot{e}\}, \langle \dot{E}, \Theta \rangle)$, where $\dot{e}' \stackrel{\text{def}}{=} \phi(\dot{e})$ in the substitution. If $\dot{x}'_m \in \bar{X}$ then $subst(\dot{x}_0, \dot{E}'_1, \dot{x}_1, \ldots, \dot{E}'_m, \dot{x}'_m)$ fits. Otherwise let $\dot{F} \stackrel{\text{def}}{=} \dot{E}_m \cup \{\dot{e}'\}$ and find a sequence of local firings $\sigma_n \stackrel{\text{def}}{=} ((t_1, L_1, \theta_1), \ldots, (t_n, L_n, \theta_n))$ such that $\dot{\Pi}(\sigma_n) = \dot{x}_m$. Let $t_{n+1} \stackrel{\text{def}}{=} t$, $L_{n+1} \stackrel{\text{def}}{=} B$, and $\theta_{n+1} \stackrel{\text{def}}{=} \Theta'_m(\dot{e}')$ so that $\dot{x}'_m = \dot{\Pi}((t_1, L_1, \theta_1), \ldots, (t_{n+1}, L_{n+1}, \theta_{n+1}))$. There exist σ'' and $n' < n+1$ such that $|\sigma''| < n'$ and $predJ(\dot{F}') = predJ(\dot{F}'')$, where $\dot{F}'$ (respectively $\dot{F}''$) is the set of events that appear in $\dot{\Pi}((t_1, L_1, \theta_1), \ldots, (t_{n'}, L_{n'}, \theta_{n'}))$ (respectively $\dot{\Pi}(\sigma'')$). Choose σ'' of minimal length so that $\dot{x}_{m+1} \stackrel{\text{def}}{=} \dot{\Pi}(\sigma'' \cdot (t_{n+1}, L_{n+1}, \theta_{n+1})) \in \bar{X}$. It holds that $n' = n$ since $\dot{x}_m \in \bar{X}$. There exists $\Theta'_{m+1} : \dot{F}'' \to Q$ such that $\langle \dot{F}'', \Theta_{m+1} \rangle$ is temporally complete and $RS(\langle \dot{F}'', \Theta_{m+1} \rangle) \sim RS(\langle \dot{F}', \Theta_m \rangle)$. And $\langle \dot{E}, \Theta \rangle = subst(\dot{x}_0, \dot{E}'_1, \dot{x}_1, \ldots, \dot{E}'_m, \dot{x}_m, \dot{F}'', \dot{x}_{m+1})$.

5 Conclusion

We have presented a new notion of complete finite prefix for safe time Petri nets. It is based on the construction of a symbolic unfolding, and on the study of the form of constraints associated with the transitions. This required to define a notion of partial state in order to equip time Petri nets with a concurrent operational semantics. A prototype has been implemented (a few thousands lines of Lisp code, and the help of a Simplex subroutine). Several improvements could be done. In particular, the idea of adequate order, introduced by Esparza [7] seems to be usable in our framework. Our next work on the subject will be to make some experiments to try to experimentally prove (or disprove) the interest of our technique in the context of model-checking or others.

References

1. Kitai, T., Oguro, Y., Yoneda, T., Mercer, E., Myers, C.: Partial order reduction for timed circuit verification based on a level oriented model. IEICE Trans. **E86-D**(12) (2001) 2601–2611
2. Penczek, W., Pólrola, A.: Abstractions and partial order reductions for checking branching properties of time Petri nets. In: ICATPN. Volume 2075 of LNCS. (2001) 323–342
3. Chatain, T., Jard, C.: Time supervision of concurrent systems using symbolic unfoldings of time Petri nets. In: FORMATS. Volume 3829 of LNCS. (2005) 193–207 Extended version available in INRIA Research Report RR-5706.
4. Aura, T., Lilius, J.: Time processes for time Petri nets. In: ICATPN. Volume 1248 of LNCS. (1997) 136–155
5. Lilius, J.: Efficient state space search for time Petri nets. In: MFCS Workshop on Concurrency '98. Volume 18 of ENTCS., Elsevier (1999)
6. McMillan, K.L.: A technique of state space search based on unfolding. Formal Methods in System Design **6**(1) (1995) 45–65
7. Esparza, J., Römer, S., Vogler, W.: An improvement of McMillan's unfolding algorithm. Formal Methods in System Design **20**(3) (2002) 285–310
8. Bieber, B., Fleischhack, H.: Model checking of time Petri nets based on partial order semantics. In: CONCUR. Volume 1664 of LNCS. (1999) 210–225
9. Fleischhack, H., Stehno, C.: Computing a finite prefix of a time Petri net. In: ICATPN. (2002) 163–181
10. Berthomieu, B., Diaz, M.: Modeling and verification of time dependent systems using time Petri nets. IEEE Trans. Software Eng. **17**(3) (1991) 259–273
11. Semenov, A.L., Yakovlev, A.: Verification of asynchronous circuits using time Petri net unfolding. In: DAC, ACM Press (1996) 59–62
12. Merlin, P., Farber, D.: Recoverability of communication protocols – implications of a theorical study. IEEE Transactions on Communications **24** (1976)
13. Engelfriet, J.: Branching processes of Petri nets. Acta Inf. **28**(6) (1991) 575–591
14. Chatain, T., Jard, C.: Symbolic diagnosis of partially observable concurrent systems. In: FORTE. Volume 3235 of LNCS. (2004) 326–342
15. Best, E.: Structure theory of Petri nets: the free choice hiatus. In: Proceedings of an Advanced Course on Petri Nets: Central Models and Their Properties, Advances in Petri Nets 1986-Part I, London, UK, Springer-Verlag (1987) 168–205
16. Baldan, P., Corradini, A., Montanari, U.: Contextual Petri nets, asymmetric event structures, and processes. Inf. Comput. **171**(1) (2001) 1–49
17. Vogler, W., Semenov, A.L., Yakovlev, A.: Unfolding and finite prefix for nets with read arcs. In: CONCUR. Volume 1466 of LNCS. (1998) 501–516