Complete Finite Prefixes of Symbolic Unfoldings of 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 Beaulieu, F-35042 Rennes cedex, France
Claude.Jard@bretagne.ens-cachan.fr

Abstract. Monitoring real-time concurrent systems is a challenging task. In this paper we formulate (model-based) supervision by means of hidden state history reconstruction, from event (e.g. alarm) observations. We follow a so-called true concurrency approach using time Petri nets: the model defines explicitly the causal and concurrency relations between the observable events, produced by the system under supervision on different points of observation, and constrained by time aspects. The problem is to compute on-the-fly the different partial order histories, which are the possible explanations of the observable events. We do not impose that time is observable: the aim of supervision is to infer the partial ordering of the events and their possible firing dates. This is achieved by considering a model of the system under supervision, given as a time Petri net, and the on-the-fly construction of an unfolding, guided by the observations. Using a symbolic representation, this paper presents a new definition of the unfolding of time Petri nets with dense time.

1 Introduction and Related Work

Monitoring real-time concurrent systems is a challenging task. In this paper we formulate model-based supervision by means of hidden state history reconstruction, from event (e.g. alarm) observations. We follow a so-called true concurrency approach using time Petri nets: the model defines explicitly the causality and concurrency relations between the observable events, produced by the system under supervision on different points of observation, and constrained by time aspects. The problem is to compute on-the-fly the different partial order histories, which are the possible explanations of the observable events. An important application is the supervision of telecommunications networks, which motivated this work.

Without considering time, a natural candidate to formalize the problem are safe Petri nets with branching processes and unfoldings. The previous work of our group used this framework to define the histories and a distributed algorithm to build them as a collection of consistent local views [3]. The approach defines

the possible explanations as the underlying event structure of the unfolding of the product of the Petri net model and of an acyclic Petri net representing the partial order of the observed alarms.

In this paper we extend our method to time Petri nets, allowing the designer to model time constraints, restricting by this way the set of possible explanations, We do not impose that time is observable: the aim of supervision is to infer the partial ordering of the events and their possible firing dates. Using a symbolic representation, this paper presents a new definition of the unfolding of time Petri nets with dense time.

Model-based diagnosis using time Petri nets and partial orders has already been addressed in [12]. In this work, temporal reasoning is based on (linear) logic. The first reference to time Petri net unfolding seems to be in 1996, by A. Semenov, A. Yakovlev and A. Koelmans [13] in the context of hardware verification. They deal only with a quite restricted class of nets, called *time independent choice time Petri net*, in which any choice is resolved independently of time. In [1], T. Aura and J. Lilius give a partial order semantics to time Petri nets, based on the nonsequential processes semantics for untimed net systems. A time process of a time Petri net is defined as a traditionally constructed causal process that has a valid timing. An algorithm for checking validness of a given timing is presented. It is proved that the interleavings of the time processes are in bijection with the firing schedules. But unfortunately, they do not provide a way to represent all the valid processes using the notion of unfolding of time Petri net, as usual in the untimed case. A few years later (in 2002), H. Fleischhack and C. Stehno in [10] give the first notion of a finite prefix of the unfolding of a time Petri net. Their method relies on a translation towards an ordinary place/transition net. This requires to consider only discrete time and to enumerate all the situations. This also relies on the introduction of new transitions, which represent the clock ticks. Although relevant for model-checking, it is not clear that it allows us to recover causalities and concurrencies, as required in the diagnosis application. Furthermore, we are convinced that time constraints must be treated in a symbolic way, using the analog of state class constructions of B. Berthomieu [4,5].

The rest of the paper is organized as follows. Section 2 defines the different ingredients of our model-based supervision, namely the diagnosis setup, the time Petri net model and its partial order semantics. Section 3 describes the symbolic unfolding technique used to compute the symbolic processes, which serve as explanations. Before entering the general case, we consider the simplest case of extended free-choice time Petri nets [6]. We conclude in Section 5.

2 Time Petri nets and Partial Order Semantics

2.1 Time Petri nets: 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

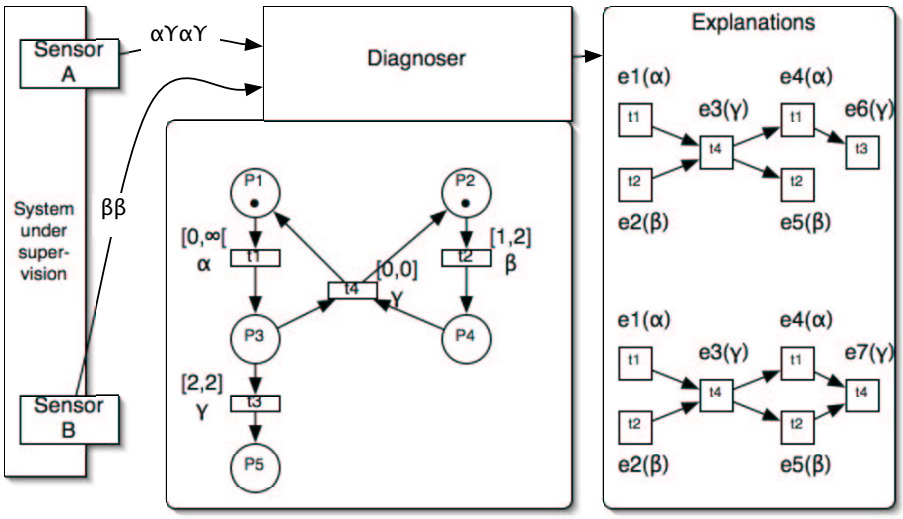

Fig. 1. A time Petri net.

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 [11].

A *time Petri net* is a tuple $N = \langle P, T, pre, post, efd, lfd \rangle$ 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 (bars). The closed interval $[efd(t), lfd(t)]$ is written near each transition.

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 $i \geq 1$, firing t_i from S_i at date θ_i is possible and leads to S_{i+1}. 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. After this firing p_1 and p_4 are marked, t_1 is the only enabled transition and it has already waited 1 time unit. t_1 can fire at any time θ, provided it is greater than 1. Consider t_1 fires at time 3. p_3 and p_4 are marked in the new state, and transitions t_3 and t_4 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_4 cannot wait at all. So t_4 will necessarily fire (at time 3), and t_3 cannot fire.

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 on the tokens of the marking than on 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 Semantics

Processes. 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 [1]. We use a canonical coding like in [8].

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 $\mathit{place}^{-1}_{|B}$ its inverse, and for all $P \subseteq \mathit{Place}(B)$, $\mathit{Place}^{-1}_{|B}(P) \stackrel{\text{def}}{=} \{\mathit{place}^{-1}_{|B}(p) \mid b \in P\}$. We also denote dob_B the mapping defined as: for all $p \in \mathit{Place}(B)$, $\mathit{dob}_B(p) \stackrel{\text{def}}{=} \Theta({}^\bullet(\mathit{place}^{-1}_{|B}(p)))$.

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. 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 $e \stackrel{\text{def}}{=} (\mathit{Place}^{-1}_{|\uparrow(E)}({}^\bullet t_{n+1}), t_{n+1})$ represents the last firing of the sequence.

The set of all the processes obtained as the image by Π of a firing sequence 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. 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, $\lceil E \rceil \stackrel{\text{def}}{=} \bigcup_{e \in E} \lceil e \rceil$. We also define $\mathit{cnds}(E) \stackrel{\text{def}}{=} \bigcup_{e \in E} e^\bullet$ the set of *conditions* created by the events of E.

Two events of a process that are not causally related are called *concurrent*.

Symbolic Processes. We choose to group the processes that differ only by their firing dates to obtain what we call a *symbolic process*.

A symbolic process of a time Petri net is a pair $\langle E, \mathit{pred} \rangle$ with $\mathit{pred} : (E \longrightarrow Q) \longrightarrow \mathbf{bool}$, such that for all mapping $\Theta : E \longrightarrow Q$, if $\mathit{pred}(\Theta)$, then $\langle E, \Theta \rangle \in X$.

In practice, *pred* is described by linear inequalities. Examples of symbolic processes are given in Figure 1. The first explanation groups all the processes formally defined as $\langle E, \Theta \rangle$ where E contains the six following events, with the

associated firing dates (the initial event $\bot$ is not represented):

$$\begin{array}{ll} 1 = (\{(\bot, P_1)\}, t_1) & \Theta(1) \geq \Theta(\bot) \\ 2 = (\{(\bot, P_2)\}, t_2) & 1 \leq \Theta(2) - \Theta(\bot) \leq 2 \\ 3 = (\{(1, P_3), (2, P_4)\}, t_4) & \Theta(3) = \max\{\Theta(1), \Theta(2)\} \\ 4 = (\{(3, P_1)\}, t_1) & \Theta(4) = \Theta(3) \\ 5 = (\{(3, P_2)\}, t_2) & \Theta(5) = \Theta(3) + 2 \\ 6 = (\{(4, P_3)\}, t_3) & \Theta(6) = \Theta(4) + 2 \end{array}$$

3 Symbolic Unfoldings of Time Petri nets

Symbolic unfoldings have already been addressed in the context of high-level Petri nets [7]. In this section we define the symbolic unfolding of time Petri nets, i.e. a quite compact structure that contains all the possible processes and exhibits concurrency.

3.1 Pre-processes

For the construction of symbolic unfoldings of time Petri nets, we need the notion of *pre-process*, that extends the notion of process.

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 often write $\langle E', \Theta \rangle$ instead of $\langle E', \Theta_{|E'} \rangle$ for short. The definition of the state that is reached after a process is also used for pre-processes. We define the *prefix* relation $\leq$ on pre-processes as follows:

$$\langle E, \Theta \rangle \leq \langle E', \Theta' \rangle \quad \text{iff} \quad E \subseteq E' \ \wedge \ \Theta = \Theta'_{|E}$$

3.2 Symbolic Unfoldings of Extended Free Choice Time Petri nets

An *extended free choice* time Petri net is a time Petri net such that:

$$\forall t, t' \in T \quad {}^\bullet t \cap {}^\bullet t' \neq \emptyset \implies {}^\bullet t = {}^\bullet t'.$$

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

This unfolding has two important properties in the case of extended free choice time Petri nets.

We first remark that:

Theorem 1. $\{\tau(e) \mid e \in U\} \subseteq T'$ *where*

$$T' \stackrel{\text{def}}{=} \{t \in T \mid \forall t' \in T \quad {}^\bullet t' = {}^\bullet t \implies efd(t) \leq lfd(t')\}.$$

Then we have:

Theorem 2. *Let $E \subseteq U$ be a nonempty finite set of events and $\Theta : E \longrightarrow Q$ associate a firing date with each event of E. $\langle E, \Theta \rangle$ is a pre-process iff:*

$$\begin{cases} \lceil E \rceil = E & \textit{(E is causally closed)} \\ \nexists e, e' \in E \quad e \neq e' \ \wedge \ {}^\bullet e \cap {}^\bullet e' \neq \emptyset & \textit{(E is conflict free)} \\ \forall e \in E \setminus \{\bot\} \quad efd(\tau(e)) \leq \Theta(e) - \max\limits_{b \in {}^\bullet e} \Theta({}^\bullet b) \leq \max\limits_{\substack{t' \in T \\ {}^\bullet t' = {}^\bullet \tau(e)}} lfd(t') & \\ & \textit{(all the events respect the firing delays)} \end{cases}$$

Theorem 3. *For all $e \stackrel{\text{def}}{=} (B, t) \in cnds(U) \times T$,*

$$e \in U \textit{ iff } \begin{cases} Place(B) = {}^\bullet t \\ \nexists f, f' \in \lceil e \rceil \quad f \neq f' \ \wedge \ {}^\bullet f \cap {}^\bullet f' \neq \emptyset \\ t \in T' \end{cases}$$

The first theorem gives a way to extract processes from the unfolding, while the second theorem gives a direct construction of the unfolding. The unfolding we define for extended free choice time Petri nets is exactly the unfolding of the underlying Petri net without time constraints, from which the transitions that are not in T' are removed.

We do not give proofs for the theorems 2 and 3 as they are particular cases of the theorems 4 and 5: the symbolic unfolding of extended free choice time Petri nets as defined in this section is the same as the symbolic unfolding we obtain if we use the general definition of the next section.

3.3 Symbolic Unfoldings of Time Petri nets: General Case

Introduction. If we define the symbolic unfolding of a time Petri net in the general case as we have done for extended free choice time Petri nets, none of the two previous theorems hold: extracting a process from the unfolding becomes complex (see [1]); and especially we do not know any direct way to build the unfolding. It is also interesting to notice that the union of two pre-processes $\langle E, \Theta \rangle$ and $\langle E', \Theta' \rangle$ is not necessarily a pre-process, even if $\Theta_{|E \cap E'} = \Theta'_{|E \cap E'}$ and $E \cup E'$ is conflict free. In the example of Figure 1, we observe this if $\langle E, \Theta \rangle$ is the process which contains a firing of $t1$ at time 0 and a firing of $t2$ at time 1, and $\langle E', \Theta' \rangle$ is the pre-process that we obtain by removing the firing of $t2$ from the process made of $t1$ at time 0, $t2$ at time 2 and $t3$ 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 $\tau(e)$.

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 date 0 with the marking $\{p_1, p_2\}$. Although the

semantics forbids to fire t_1 at date 10 before firing t_2, we feel that nothing can prevent t_1 from firing at date 10, because only t_1 can remove the token in place p_1. By contrast, the firing of t_3 highly depends on the firing date of t_2 because when t_4 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.

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 $\{p_1, p_3, p_5\}$, $\{p_2, p_4\}$.

Definition 1 (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 (marked place)* $p \in L$.

Definition 2 (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 assumtion before). From now on the notion of* maximal partial state *or* maximal state *will replace the notion of global state.*

Definition 3 (age of an enabled transition in a maximal state). *Let* $S \stackrel{\text{def}}{=} \langle M, dob, lrd\rangle$ *be a maximal state and let* $t \in T$ *a transition that is enabled in the marking* M *(*$^\bullet t \subseteq M$*). The date of enabling of* t *is* $\max_{p \in {}^\bullet t} dob(p)$*, and the date that is reached by the system can be defined as* $\max_{p \in P} lrd(p)$*. We define the* age $I_S(t)$ *of* t *in the state* S *as the difference:*

$$I_S(t) \stackrel{\text{def}}{=} \max_{p \in P} lrd(p) - \max_{p \in {}^\bullet t} dob(p).$$

Definition 4 (temporally complete maximal state (or complete state)). *A maximal state* $S \stackrel{\text{def}}{=} \langle M, dob, lrd\rangle$ *is* temporally complete *if for all transition* $t \in T$ *which is enabled in the marking* M *(*$^\bullet t \subseteq M$*),* $I_S(t) \leq lfd(t)$*. A temporally complete maximal state is also called a* complete state *for short.*

Definition 5 (local firing condition). *A* local firing condition *is a triple* (L, dob, t, θ) *where* $L \subseteq P$ *is a partial marking,* $dob : L \longrightarrow Q$ *associate a* date of birth $dob(p)$ *with each token (marked place)* $p \in L$*,* t *is a transition such that* $^\bullet t \subseteq L$ *and* $\theta \geq \max_{p \in L} dob(p)$ *is a date.*

[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 behaviour of the time Petri net.

We expect that each local firing condition (L, dob, t, θ) is chosen such that knowing that the net is in a state that contains a local 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.

It will be crucial in the following to know how to select local firing conditions. However several choices are possible. If we are given a predicate LFC on local firing conditions, we can build extended processes by using only the local firing conditions that satisfy LFC. Then we will try to map these extended processes into pre-processes. If LFC is valid, then all the pre-processes we obtain are correct.

Semantics of Local Firings. We will define formally the semantics that we obtain when we allow only local firing conditions that satisy a given predicate LFC on local firing conditions.

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 $p \in M_0$, $dob_0(p) \stackrel{\text{def}}{=} lrd_0(p) \stackrel{\text{def}}{=} \theta_0$.

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

$$dob'(p) \stackrel{\text{def}}{=} \begin{cases} dob(p) & \text{if } p \in M \setminus {}^\bullet t \\ \theta & \text{if } p \in t^\bullet \end{cases} \quad \text{and} \quad lrd'(p) \stackrel{\text{def}}{=} \begin{cases} lrd(p) & \text{if } p \in M \setminus L \\ \theta & \text{if } p \in (L \setminus {}^\bullet t) \cup t^\bullet. \end{cases}$$

We call *sequence of local firings* (w.r.t. LFC) 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 $i \geq 1$, t_i can fire from S_i at date θ_i using the partial marking L_i and this leads to S_{i+1}. The empty firing sequence is denoted ϵ.

Extended Processes. Let LFC be a predicate on local firing conditions.

We will define a notion of *extended process* (parameterized by LFC), 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 [2,14]). 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 $\dot{e} \stackrel{\text{def}}{=} (B, t)$, we use the notations $\tau(\dot{e}) \stackrel{\text{def}}{=} t$, ${}^\bullet\dot{e} \stackrel{\text{def}}{=} Place_{|B}^{-1}({}^\bullet t)$, $\underline{\dot{e}} \stackrel{\text{def}}{=} B \setminus {}^\bullet e$ and $\dot{e}^\bullet \stackrel{\text{def}}{=} \{(\dot{e}, p) \mid p \in t^\bullet\}$. We define the relations $\rightarrow$ and $\nearrow$ 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 $(\dot{e} \rightarrow \dot{f}) \vee (\underline{\dot{e}} \cap {}^\bullet\dot{f} \neq \emptyset)$.

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 a sequence of local firings (w.r.t. *LFC*) is denoted $\dot{X}_{LFC}$. The maximal state that is reaches after an extended process $\langle \dot{E}, \Theta \rangle$ is denoted $RS(\langle \dot{E}, \Theta \rangle)$. We say that $\langle \dot{E}, \Theta \rangle$ is *temporally complete* if $RS(\langle \dot{E}, \Theta \rangle)$ is temporally complete. The set of all temporally complete extended processes is denoted $\dot{Y}_{LFC}$.

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

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

We say that *LFC* is a *valid predicate on local firing conditions* iff for all extended process $\langle \dot{E}, \Theta \rangle \in \dot{X}_{LFC}$, $\langle h(\dot{E}), \Theta \circ h^{-1}_{|\dot{E}} \rangle$ 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 $\langle h(\dot{E}), \Theta \circ h^{-1}_{|\dot{E}} \rangle \leq \langle E', \Theta' \rangle$.

Symbolic Unfolding. As we did for extended free choice time Petri nets with events in Section 3.2, we define the *symbolic unfolding* U_{LFC} of a time Petri net by collecting all the extended events that appear in its extended processes: $U_{LFC} \stackrel{\text{def}}{=} \bigcup_{\langle \dot{E}, \Theta \rangle \in \dot{X}_{LFC}} \dot{E}$.

We have equivalents of the two theorems we had with symbolic unfoldings of extended free choice time Petri nets.

Theorem 4. *Let $\dot{E} \subseteq U_{LFC}$ 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:*

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

Proof. Let $\langle \dot{E}, \Theta \rangle \in \dot{X}_{LFC}$ 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 $LFC(RS_\Theta(B), t, \theta')$ 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 $\langle \dot{E}', \Theta' \rangle \in \dot{X}_{LFC}$. 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 $\langle \dot{E}, \Theta \rangle \in \dot{X}_{LFC}$. 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 $LFC\left(RS_{\Theta'}({}^\bullet\dot{e} \cup \underline{\dot{e}}), \tau(\dot{e}), \Theta'(\dot{e})\right)$ holds. Thus $\langle \dot{E}', \Theta' \rangle = \langle \dot{E} \cup \{\dot{e}\}, \Theta \cup \{(\dot{e}, \Theta'(\dot{e}))\} \rangle \in \dot{X}_{LFC}$.

Theorem 5. *For all* $\dot{e} \stackrel{\text{def}}{=} (B, t) \in cnds(U_{LFC}) \times T, \quad \dot{e} \in U_{LFC}$ *iff*

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

Proof. Let $\dot{e} \in U_{LFC}$. There exists $\langle \dot{E}, \Theta' \rangle \in \dot{X}_{LFC}$ such that $\dot{e} \in \dot{E}$. $\langle \dot{E}, \Theta' \rangle$ satisfies the conditions in the curly brace of Theorem 4. 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 4. Then $\langle \lceil \dot{e} \rceil \setminus \{\dot{e}\}, \Theta \rangle \in \dot{X}_{LFC}$. 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 $LFC(RS_\Theta(B), t, \Theta(\dot{e}))$ holds. Thus $\langle \lceil \dot{e} \rceil, \Theta \rangle \in \dot{X}_{LFC}$ and therefore $\dot{e} \in U_{LFC}$.

Selecting Local Firing Conditions. The definition of extended processes is parameterized by a predicate *LFC* on local firing conditions: each extended event must correspond to a local firing condition that satisfies *LFC*, the others are forbidden. A good choice for *LFC* takes three notions into account: completeness, redundancy and preservation of concurrency.

Completeness. A predicate *LFC* on local firing conditions is *complete* if for all process $\langle E, \Theta \rangle \in X$, there exists an extended process $\langle \dot{E}, \Theta' \rangle \in \dot{X}_{LFC}$ such that $\langle h(\dot{E}), \Theta' \circ h^{-1}_{|\dot{E}} \rangle = \langle E, \Theta \rangle$.

Redundancy. Given a predicate LFC on local firing conditions and a process $\langle E, \Theta\rangle \in X$, there may exist *several* extended processes $\langle \dot{E}, \Theta'\rangle \in \dot{X}_{LFC}$ such that $\langle h(\dot{E}), \Theta' \circ h^{-1}_{|\dot{E}}\rangle = \langle E, \Theta\rangle$. This is called *redundancy*. In particular, if LFC contains two local firing conditions (L, dob, t, θ) and (L', dob', t, θ) with $L' \subsetneq L$ and $dob' = dob_{|L'}$, then all the extended processes involving (L, dob, t, θ') are redundant.

A trivial choice for LFC which does not preserve any concurrency. A trivial complete predicate LFC is the predicate that demands that the state S is a maximal partial state, and then check that t can fire at date θ from S. In addition, this choice gives little redundancy. But the extended events of the extended processes that we obtain in this case are totally ordered by causality. In other words, these extended processes do not exhibit any concurrency at all. Actually we retrieve here all the firing sequences of the interleaving semantics.

A proposition for LFC. What we want is a complete predicate on local firing conditions that generates as little redundancy as possible and that exhibits as much concurrency as possible.

We first define a predicate LFC' on local firing conditions as follows:
$LFC'(L, dob, t, \theta)$ 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:

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

Now we define LFC by eliminating some redundancy in LFC':
$LFC(L, dob, t, \theta)$ holds iff $LFC'(L, dob, t, \theta)$ holds and there exists no $L' \subsetneq L$ such that $LFC'(L', dob_{|L'}, t, \theta)$.

It is important that the constraints (see Theorems 4 and 5) can be solved automatically: with the definition of LFC we have proposed here, the quantifiers ($\forall$ and $\exists$) on places and transitions expand into disjunctions and conjunctions. The result is a disjunction of conjunctions of linear inequalities on the $\Theta(\dot{e})$. When a "max" appears in an inequality, this inequality can be rewritten into the desired form. These systems are shown near the events in Figure 2.

Theorem 6. *Let $\langle \dot{E}, \Theta\rangle \in \dot{X}_{LFC}$. $\langle h(\dot{E}), \Theta \circ h^{-1}_{|\dot{E}}\rangle \in X$ iff $RS(\langle \dot{E}, \Theta\rangle)$ is temporally complete.*

Theorem 7. *LFC is a valid, complete predicate on local firing conditions.*

Proof. The proof of the validity is done in two parts:

1. For all $\langle \dot{E}, \Theta\rangle \in \dot{X}_{LFC}$, denote $\langle M, dob, \theta\rangle$ the global state reached after $\langle \dot{E}, \Theta\rangle$. $\langle h(\dot{E}), \Theta \circ h^{-1}_{|\dot{E}}\rangle \in X$ iff

$$\forall t \in T \quad {}^\bullet t \subseteq M \implies \theta \leq doe(t) + lfd(t). \tag{1}$$

2. For all $\langle \dot{E}, \Theta \rangle \in \dot{X}_{LFC}$, there exists $\langle \dot{E}', \Theta' \rangle \in \dot{X}_{LFC}$ which satisfies (1) and such that $\langle \dot{E}, \Theta \rangle \leq \langle \dot{E}', \Theta' \rangle$.
Consequently $\langle h(\dot{E}), \Theta \circ h^{-1}_{|\dot{E}} \rangle \leq \langle h(\dot{E}'), \Theta' \circ h^{-1}_{|\dot{E}'} \rangle \in \dot{X}$.

Here are the proofs for these two points:

1. Let $\langle \dot{E}, \Theta \rangle \in \dot{X}_{LFC}$ and denote $\langle M, dob, \theta \rangle$ the global state reached after $\langle \dot{E}, \Theta \rangle$.
It follows from the definition of the processes that if $\langle h(\dot{E}), \Theta \circ h^{-1}_{|\dot{E}} \rangle \in X$, then (1) holds.
Conversely, assume that $\langle \dot{E}, \Theta \rangle$ satisfies (1); 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 $\langle M', dob', \theta' \rangle$ the global state reached after $\langle \dot{E} \setminus \{\dot{e}\}, \Theta \rangle$ 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 $LFC(RS_\Theta(L), \tau(\dot{e}), \Theta(\dot{e}))$ holds, then

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

As ${}^\bullet t \subseteq M'$, then $\nexists p \in {}^\bullet t$ such that $\bar{p} \cap L \neq \emptyset$; thus $\theta \leq \max\limits_{p \in {}^\bullet t \cap L} dob'(p) + lfd(t)$. Hence $doe'(t) = \max\limits_{p \in {}^\bullet t} dob'(p) \geq \max\limits_{p \in {}^\bullet t \cap L} dob'(p) \geq \theta - lfd(t) \geq \theta' - lfd(t)$. As a result $\langle \dot{E} \setminus \{\dot{e}\}, \Theta \rangle \in \dot{X}_{LFC}$ and satisfies (1).
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 $\langle M', dob', \theta' \rangle$. 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 $\langle h(\dot{E}), \Theta \circ h^{-1}_{|\dot{E}} \rangle \in X$.
2. Let $\langle \dot{E}, \Theta \rangle \in \dot{X}_{LFC}$. If $\langle \dot{E}, \Theta \rangle$ satifies (1), then $\langle \dot{E}', \Theta' \rangle \stackrel{\text{def}}{=} \langle \dot{E}, \Theta \rangle$ fits.
Otherwise, 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 $\dot{F} \stackrel{\text{def}}{=} \{\dot{f} \in \dot{E} \mid \Theta(\dot{f}) \leq \theta_t\}$. $\langle \dot{F}, \Theta_{|\dot{F}} \rangle \in \dot{X}_{LFC}$. Denote $\langle M', dob', \theta' \rangle$ the global state reached after $\langle \dot{F}, \Theta_{|\dot{F}} \rangle$. $LFC'(\langle M', dob', \theta' \rangle, t, \theta_t)$ holds. Thus there exists $L \subseteq M'$ such that $LFC(\langle L, dob'_{|L}, \theta' \rangle, t, \theta_t)$ holds. Let $\dot{e} \stackrel{\text{def}}{=} (Place^{-1}_{|\uparrow(\dot{F})}(L), t)$. We will show that $\langle \dot{E} \cup \{\dot{e}\}, \Theta \cup \{(\dot{e}, \theta_t)\} \rangle \in \dot{X}_{LFC}$. $\Theta \cup \{(\dot{e}, \theta_t)\}$ 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 $\langle \dot{E} \cup \{\dot{e}\}, \Theta \cup \{(\dot{e}, \theta_t)\} \rangle \in \dot{X}_{LFC}$ by adding the event to $\langle \dot{E}, \Theta \rangle$.
Iterating this until $\langle \dot{E}, \Theta \rangle$ satisfies (1) terminates if we assume that time diverges: at each step $\langle \dot{F}, \Theta_{|\dot{F}} \rangle$ satisfies (1), 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.

This ends the proof of the validity of LFC. Now we have to prove that LFC is complete. 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 $\langle \dot{E}, \Theta'\rangle \in \dot{X}_{LFC}$ such that $\langle h(\dot{E}), \Theta' \circ h^{-1}_{|\dot{E}}\rangle = \langle E, \Theta\rangle$. $LFC'(\langle M, dob, \theta\rangle, t, \theta')$ holds. Thus there exists $L \subseteq M$ such that $LFC(\langle L, dob_{|L}, \theta\rangle, t, \theta')$ holds. Define $\dot{e} \stackrel{\text{def}}{=} (Place^{-1}_{|\uparrow \dot{E}}(L), t)$. $\langle \dot{E} \cup \{\dot{e}\}, \Theta' \cup \{(\dot{e}, \theta')\}\rangle \in \dot{X}_{LFC}$ and the event $h(\dot{e})$ codes the firing of t at date θ' after $\langle E, \Theta\rangle$.

3.4 Example of Unfolding

We come back to our simple example of time Petri net given in Figure 1. Figure 2 shows a prefix of its symbolic unfolding. In this figure the rectangles represent the extended events, and the circles represent the conditions. 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 $b \in \dot{e}^\bullet$. A line without arrow between a condition b and an extended event $\dot{e}$ means that $b \in \underline{\dot{e}}$.

The constraint $LFC\,(Place(B), dob_B, t, \Theta(\dot{e}))$ is represented near each extended event $\dot{e} = (B, t)$ of Figure 2. While extracting an extending process from this unfolding, we can solve the conjunction of the constraints appearing on the extended events of the extended process, plus the constraints that ensure that Θ is compatible with $\nearrow$. This gives all the possible values for the dates of the extended events. For example, considering the extended events $\dot{E} \stackrel{\text{def}}{=} \{e1, e2, e3, e4, e5, e6\}$, $\langle \dot{E}, \Theta\rangle$ is an extended process iff Θ satisfies:

$$\left\{\begin{array}{l}
\left.\begin{array}{l}
0 \leq \Theta(e1) - \Theta(\bot) \\
1 \leq \Theta(e2) - \Theta(\bot) \leq 2 \\
\Theta(e3) = \max\{\Theta(e1), \Theta(e2)\} \\
\Theta(e3) - \Theta(e1) \leq 2 \quad (t3 \text{ has not consumed} \\
\qquad \text{the token in } p3 \text{ before } t4 \text{ fires.}) \\
0 \leq \Theta(e4) - \Theta(e3) \\
1 \leq \Theta(e5) - \Theta(e3) \leq 2 \\
\Theta(e6) - \Theta(e4) = 2 \\
\Theta(e6) - \Theta(e3) \leq 2 \quad (t2 \text{ has not consumed} \\
\qquad \text{the token in } p2 \text{ before } t3 \text{ fires.})
\end{array}\right\} \forall \dot{e} = (B, t) \in \dot{E} \setminus \{\bot\} \\
\qquad LFC\,(Place(B), dob_B, t, \Theta(\dot{e})) \\
\\
\left.\begin{array}{l}
\Theta(\bot) \leq \Theta(e1) \\
\Theta(\bot) \leq \Theta(e2) \\
\Theta(e1) \leq \Theta(e3) \\
\Theta(e2) \leq \Theta(e3) \\
\Theta(e3) \leq \Theta(e4) \\
\Theta(e3) \leq \Theta(e6) \\
\Theta(e4) \leq \Theta(e6) \\
\Theta(e3) \leq \Theta(e5) \\
\Theta(e6) \leq \Theta(e5)
\end{array}\right\} \forall \dot{e}, \dot{e}' \quad \dot{e} \nearrow \dot{e}' \implies \Theta(\dot{e}) \leq \Theta(\dot{e}'). \\
\text{Notice that } e6 \nearrow e5.
\end{array}\right.$$

These constraints can be simplified into:

$$\begin{cases} \Theta(\bot) \leq \Theta(e1) \\ 1 \leq \Theta(e2) - \Theta(\bot) \leq 2 \\ \Theta(e3) = \max\{\Theta(e1), \Theta(e2)\} \\ \Theta(e4) = \Theta(e3) \\ \Theta(e6) = \Theta(e4) + 2 \\ \Theta(e5) = \Theta(e3) + 2 \end{cases}$$

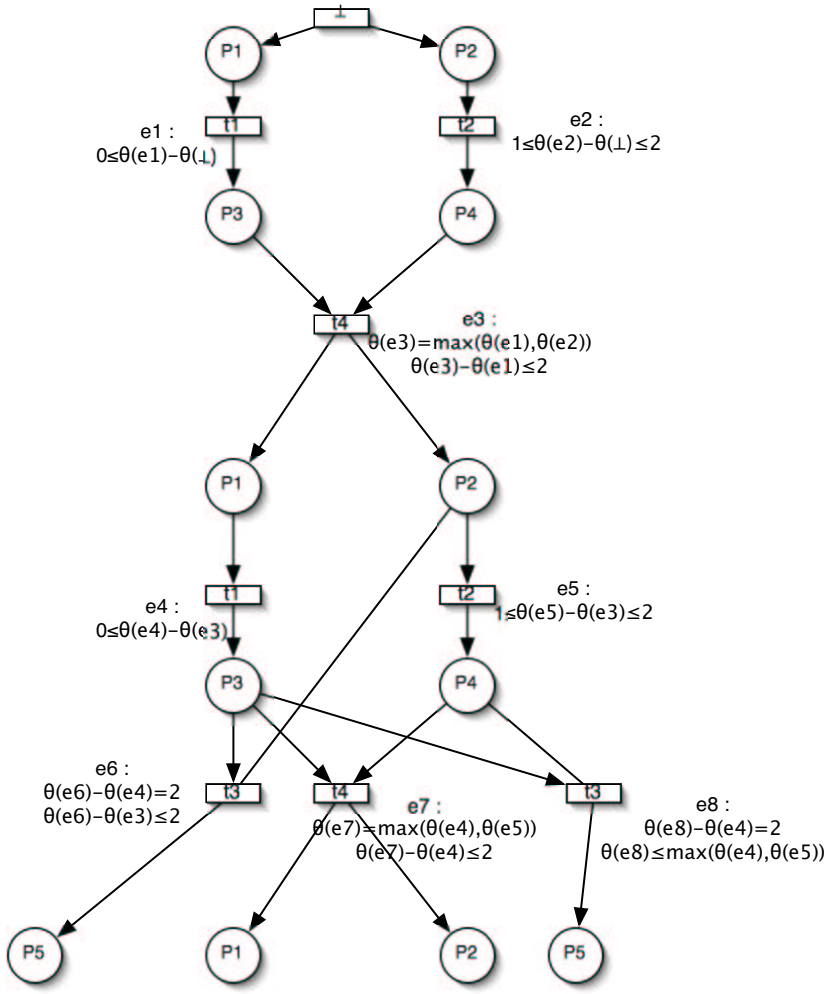

Fig. 2. A prefix of the symbolic unfolding of the time Petri net of Figure 1.

The three maximal extended processes of Figure 2 share the prefix $\{e1, e2, e3, e4, e5\}$. The first extended process contains also $e7$. It corresponds to the second explanation of Figure 1. The second extended process contains the prefix, plus $e6$ and the third contains the prefix, plus $e8$. These two extended processes correspond to the same explanation: the first of Figure 1. This is what we have called redundancy. After solving the linear constraints we see that the second occurrence of $t1$ must have occured immediately after $t4$ has fired and the second occurrence of $t2$ must have fired 2 time units later. Actually the extended process with $e6$ and the one with $e8$ only differ by the fact that transition $t3$ has fired *before* $t2$ in the first one, whereas $t3$ has fired *after* $t2$ in the second one. Because of transition $t4$, the firing of $t2$ has a strong influence on the firing of $t3$. This is the reason why there are too distinct cases in the unfolding.

4 Complete Finite Prefixes

4.1 Equivalence of Two Maximal States

Definition 6 (bound for the age of a transition). *For all transition $t \in T$, we define*

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

Definition 7 (reduced age of an enabled transition). *Let $S \stackrel{\text{def}}{=} \langle M, dob, lrd \rangle$ be a complete state and $t \in T$ a transition that is enabled in the marking M ($^\bullet t \subseteq M$). We define the* reduced age $J_S(t)$ *of t in the state S as:*

$$J_S(t) \stackrel{\text{def}}{=} \max\{I_S(t), bound(t)\}.$$

Definition 8 (equivalence of two maximal states). *Two complete 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:*

$$\begin{cases} M_1 = M_2 \stackrel{\text{def}}{=} M \\ \forall t \in T \quad ^\bullet t \subseteq M \implies J_{S_1}(t) = J_{S_2}(t). \end{cases}$$

Theorem 8 (firing a transition from two equivalent maximal states). *Let S_1 and S_2 be two equivalent complete states. Let M be their marking. A transition t can fire from S_1 at date $\theta_1 \geq \max_{p \in P} lrd_1(p)$ using the partial marking $L \subseteq M$ iff it can fire from S_2 at date $\theta_1 - \max_{p \in P} lrd_1(p) + \max_{p \in P} lrd_2(p)$ using the same partial marking L.*

4.2 Composition of Extended Processes

Definition 9 (composition of extended processes).
Let $\dot{x}_1 \stackrel{\text{def}}{=} \langle \dot{E}_1, \Theta_1 \rangle, \dot{x}_2 \stackrel{\text{def}}{=} \langle \dot{E}_2, \Theta_2 \rangle \in \dot{X}_{LFC}$ be two extended processes, and

$\dot{E}'_2 \subseteq \dot{E}_2$ *such that* $\langle \dot{E}_1, \Theta_1 \rangle$ *and* $\langle \dot{E}'_2, \Theta_{2_{|\dot{E}'_2}} \rangle$ *are complete extended processes and* $RS(\langle \dot{E}'_2, \Theta_{2_{|\dot{E}'_2}} \rangle) \sim RS(\langle \dot{E}_1, \Theta_1 \rangle)$.

We define the composition *which replaces* $\langle \dot{E}'_2, \Theta_{2_{|\dot{E}'_2}} \rangle$ *by* $\dot{x}_1$ *in* $\dot{x}_2$ *as:*

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

where $\dot{E} \stackrel{\text{def}}{=} \dot{E}_1 \cup f(\dot{E}_2 \setminus \dot{E}'_2)$ *and*

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

and $\forall \dot{e} \stackrel{\text{def}}{=} (B, t) \in \dot{E}_2 \setminus \dot{E}'_2 \quad f(\dot{e}) \stackrel{\text{def}}{=} (g(B), t)$ *and*

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

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

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

Theorem 9 (composition of extended processes).
$tr(\dot{x}_0, \dot{E}'_1, \dot{x}_1, \ldots, \dot{E}'_n, \dot{x}_n) \in \dot{X}_{LFC}$.

4.3 Study of the Form of the Constraints

define *pred* (and find a better name).
Let $M \stackrel{\text{def}}{=} Place(\dot{E})$. For all $j : \{t \in T \mid {}^\bullet t \subseteq M\} \longrightarrow Q$,

$$pred(\dot{E})(j) \stackrel{\text{def}}{=} (\exists \Theta : \dot{E} \to Q \quad \langle \dot{E}, \Theta \rangle \in \dot{Y}_{LFC} \wedge j = J_{RS(\langle \dot{E}, \Theta \rangle)}).$$

We show that there is a finite set of $pred(\dot{E})$.

4.4 Definition of the Complete Finite Prefixes

Definition 10 (equivalence of two configurations). *Two configurations* $\dot{E}_1$ *and* $\dot{E}_2$ *are equivalent if* $Place(\dot{E}_1) = Place(\dot{E}_2)$ *and* $pred(\dot{E}_1) = pred(\dot{E}_2)$.

Theorem 10. *Let* $\dot{E}_1$ *and* $\dot{E}_2$ *be two equivalent configurations, and* $\langle \dot{E}, \Theta \rangle \in \dot{X}_{LFC}$ *such that* $\dot{E}_1 \subseteq \dot{E}$ *and* $\langle \dot{E}_1, \Theta_{|\dot{E}_1} \rangle \in \dot{Y}_{LFC}$. *Then there exists* $\Theta_2 : \dot{E}_2 \longrightarrow Q$ *such that* $tr(\langle \dot{E}_2, \Theta_2 \rangle, \dot{E}_1, \langle \dot{E}, \Theta \rangle) \in \dot{X}_{LFC}$.

Definition 11 (complete finite prefix). *The complete finite prefix is denoted* $\bar{U}_{LFC}$.
The set of processes $\langle \dot{E}, \Theta \rangle$ *with* $\dot{E} \subseteq \bar{U}_{LFC}$ *is denoted* $\bar{X}_{LFC}$.

Theorem 11 (decomposition of an extended process in $\bar{U}$). *Let* $\langle \dot{E}, \Theta \rangle \in \dot{X}_{LFC}$. *There exists* n *extended processes in* $\bar{X}_{LFC}$ *such that their composition is* $\langle \dot{E}, \Theta \rangle$.

4.5 Example

5 Conclusion

We have presented a possible approach to the supervision/diagnosis of timed systems, using safe time Petri nets. In such nets, time constraints are given by interval of nonnegative rationals and are used to restrict the set of behaviours. The diagnosis problem is to recover the possible behaviours from a set of observations. We consider that the observations are given as a partial order (without any timing information) from the activity of several sensors. The goal of the supervisor is to select the possible timed behaviours of the model, which do not contradict the observations: i.e. presents the same set of events labelled by the alarms and orders the events in the same direction that the sensors do. This goal is achevied by considering a symbolic unfolding of time Petri nets, which is restricted by the observations. The result is a set of explanations, which explicit the causalities (both structural and temporal) between the observations. At the same time, our algorithm infers the possible delays before the firing of the transitions associated with them. Up to our knowledge, our symbolic unfolding for safe time Petri nets is original, and its application to compute symbolic explanations too.

A prototype implementation exists (a few thousands lines of Lisp code) and we plan to use it on real case studies. Another project is to define an algorithm to produce a complete finite prefix of the unfolding [9], which could be used for other applications than diagnosis (for which we do not need this notion since the observations are finite sets).

At longer term, the notion of temporal diagnosis could be refined and revisited when considering timed distributed systems, in which alarms could bring a time information.

References

1. Tuomas Aura and Johan Lilius. Time processes for time Petri nets. In *ICATPN*, volume 1248 of *LNCS*, pages 136–155, 1997.
2. Paolo Baldan, Andrea Corradini, and Ugo Montanari. Contextual petri nets, asymmetric event structures, and processes. *Inf. Comput.*, 171(1):1–49, 2001.
3. A. Benveniste, E. Fabre, C. Jard, and S. Haar. Diagnosis of asynchronous discrete event systems, a net unfolding approach. *IEEE Transactions on Automatic Control*, 48(5):714–727, May 2003.
4. Bernard Berthomieu and Michel Diaz. Modeling and verification of time dependent systems using time Petri nets. *IEEE Trans. Software Eng.*, 17(3):259–273, 1991.
5. Bernard Berthomieu and François Vernadat. State class constructions for branching analysis of time Petri nets. In *TACAS*, pages 442–457, 2003.
6. Eike Best. 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*, pages 168–205, London, UK, 1987. Springer-Verlag.
7. Thomas Chatain and Claude Jard. Symbolic diagnosis of partially observable concurrent systems. In *FORTE*, pages 326–342, 2004.

8. Joost Engelfriet. Branching processes of Petri nets. *Acta Inf.*, 28(6):575–591, 1991.
9. Javier Esparza, Stefan Römer, and Walter Vogler. An improvement of McMillan's unfolding algorithm. In *TACAS*, pages 87–106, 1996.
10. Hans Fleischhack and Christian Stehno. Computing a finite prefix of a time Petri net. In *ICATPN*, pages 163–181, 2002.
11. P.M. Merlin and D.J. Farber. Recoverability of communication protocols – implications of a theorical study. *IEEE Transactions on Communications*, 24, 1976.
12. B. Pradin-Chézalviel, R. Valette, and L.A. Künzle. Scenario duration characterization of t-timed Petri nets using linear logic. In *IEEE PNPM*, pages 208–217, 1999.
13. Alexei Semenov and Alexandre Yakovlev. Verification of asynchronous circuits using time Petri net unfolding. In *DAC'96: Proceedings of the 33rd annual conference on Design automation*, pages 59–62, New York, NY, USA, 1996. ACM Press.
14. Walter Vogler, Alexei L. Semenov, and Alexandre Yakovlev. Unfolding and finite prefix for nets with read arcs. In *International Conference on Concurrency Theory*, pages 501–516, 1998.