A Graph of Classes Preserving Quantitative Temporal Constraints considering unbounded transitions

Janette Cardoso
IRIT-UT1
21 allées de Brienne, F-31042 Toulouse
jcardoso@univ-tlse1.fr

Xiaoyu Mao
IRIT-UT1/LAAS
Toulouse France
xmao@laas.fr

Robert Valette
LAAS-CNRS
31077 Toulouse France
robert@laas.fr

Abstract

The objective of this paper is to extend the tool GraphC that generates a new graph of classes for t-time Petri nets, taking into account unbounded transitions. In this graph, a sequence of transitions effectively firable in the net is associated with each path between two nodes (classes). The constraints which have to be verified by the occurrence dates for any event sequence in the real system are directly derived by concatenating the constraints associated with the arcs covered by the corresponding sequence in the graph of classes.

1. Introduction

For checking some properties of critical embedded systems such as the timeliness property for correct environment interaction, it is frequently necessary to consider specific scenarios of operations and to analyze the temporal constraints which have to be verified by the events composing them [Ri 01].

Other properties (related for example to the fact that a state is not reachable) imply the exhaustive search for all the states of a system. When temporal constraints exist, the states, in an infinite number, can be covered by a finite set of state classes for bounded Petri nets. In this case, a graph of state classes can be built in order to study the system, where nodes are state classes and the arc from a class $\mathcal{C}$ to a class $\mathcal{C}'$ is labeled by the transition t (leading from $\mathcal{C}$ to $\mathcal{C}'$).

Several kinds of classes have been proposed according to the kind of properties to be proven (properties expressed in LTL or in CTL for instance) [Yo 98, Be 04, Ca 05].

In order to correctly delimit the domains of the variables attached to the firing dates in a transition firing sequence, it is necessary, in the case of a t-time Petri net [Be 04] with strong semantics, to know the transition enabling dates. This implies that, for each transition, the date of the firing which has produced the last token is known. In consequence, it is necessary to proceed in the context of interleaving semantics and therefore to explicitly consider states and firing sequences.

In this paper, the proposed approach is to construct a graph of classes with sets of constraints attached to its arcs, such that the constraints which have to be verified by the firing dates for any sequence in the net, are directly derived by concatenating the constraints attached to the arcs covered by the corresponding sequence in the graph of classes.

2. Basic notions

2.1. Simple temporal network (STN)

A STN N is composed of a finite set V of variables v_i and a finite set C of **binary** constraints $C_{ij}(v_i, v_j)$ defined as convex intervals $[c_{mij}, c_{Mij}]$ delimiting the possible distance between two variables v_i and v_j of V.

A STN $N = (V, C)$ is *complete* iff a constraint C_{ij} is associated with each pair of variables. A complete STN is *minimal* iff $\forall v_i, v_j \in V$ and $\forall c \in C_{ij}$, $c \in [c_{mij}, c_{Mij}]$, is such that $v_j - v_i = c$. The Floyd-Warshall algorithm derives from any consistent (having at least one solution) STN [De 91] a new complete and minimal STN.

2.2. t-time Petri nets

Definition 1 *A t-time Petri Net is a 3-tuple* $< \mathcal{N}, M_0, I >$*:*

- $\mathcal{N} =< P, T, Pre, Post >$ *is a Petri net,*
- M_0 *: is the initial marking,*
- $I : T \rightarrow (Q^+ \cup 0) * (Q^+ \cup \infty)$.

The static interval function I associates with each transition t_i a temporal interval $[a_i, b_i]$ (see fig. 3.a) that represents the set of its possible firing dates. When the upper bound of $I(t)$ is ∞ t is said to be unbounded. Otherwise it is bounded.

In this paper, the operational semantics for t-time Petri nets, includes the *strong semantics* (which enforces the firing of one of the enabled transitions before the earliest of all the latest firing dates for the enabled transitions) and the *interleaving semantics* (transitions may be enabled concurrently but are fired sequentially). It is assumed that there is no memory of the enabling time of a transition in the past.

In a t-time Petri Net, the following events associated with a transition must be taken into account: the *enabling date*, *begin/end of the firing interval* and *firing date*. The following constraints must be verified between these events:

- the enabling date of a transition t is equal to the firing date of the last transition t' contributing to its enabling,
- the transition firing date should be included in its firing interval I.

3. The graph of classes

3.1. States and state classes

Let us consider the execution of a firing sequence $\sigma = t_1\,;\,\cdots;\,t_i\,;\,t_j\,;\cdots;\,t_n$ in a t-time Petri net with unbounded transitions. A transition can be fired several times in a sequence. The oi^{th} firing in σ of transition t_i is denoted by x_i^{oi} (if o_i=1, we note x_i instead of x_i^1).

Given a specific execution of σ, the *state* after the firing of t_i is the obtained marking associated with the current value of the clock and the firing dates of all the transitions preceding t_i in σ in order to compute the remaining firing intervals for each enabled transition.

A *class* is composed of all the states which are reachable by an execution of σ after the firing of t_i and before that of t_j. Aiming to have all the constraints which must be verified by the firing date of t_j, it is necessary to be able to derive not only the distance of x_i^{oi} and x_j^{oj}, but also the distance of x_j^{oj} with all the preceding firing dates in σ. In order to have a finite number of classes, it is necessary to *forget* a part of the past, keeping only a fragment of the STN made by these variables and their constraints.

The initial state class $\mathcal{C}_0 = (M_0, Nc_0, T_\infty^0)$, is given by: the initial marking M_0, the STN $Nc_0 : x_0$, where x_0 represents the time origin (*the beginning of the world*) and the set of unbouded transitions $T_\infty^0 = \{t \mid I(t) = [0\ \infty)\}$.

Let σ be a firing sequence $t_1\,;\cdots;\ t_i$ of a t-time Petri net, t_i the last fired transition in σ and $t_{s(k)}$ the transition that has enabled a transition t_k.

Definition 2 *The* **state class** $\mathcal{C}$*, obtained after the firing of transition* t_i*, is defined by* $\{M, Nc, T_\infty^c\}$ *where:*

- M *is the current marking of the net; it is assumed that* n *transitions are enabled by* M*,*
- T_∞^c *is the set of unbouded transitions not constrained by the firing of* t_i*,*
- Nc *is the minimal and complete STN composed of the following variables and constraints:*
  1. *the variable* x_i^{oi} *associated with the last transition firing (*t_i *firing),*
  2. *for each enabled transition* t_k *from* M*,* $t_k \notin T_\infty^c$*, the variable* $x_{s(k)}^{osk}$ *(*$k = 1, \ldots, n$*) associated with the firing of transition* $t_{s(k)}$*,*
  3. *the temporal constraints between these variables (minimal and complete network).*

The complete definition of the temporal network Nc requires the initial constraints in point 3. These values are taken from the STN defined in the section 3.2.

When t_k is enabled by a transition $t_{s(k)}$ at some class before $\mathcal{C}$ (def. 2), its initial enabling time is the static interval $I(t_k)$. If t_k remains enabled at $\mathcal{C}$ (after t_i firing), the possible fing dates of t_k are no longer delimited by possible firing dates of t_k are no longer delimited by $I(t_k)$ but by the dynamic interval $I_d^c(t_k)$. In order to take the same time origin $x_{s(k)}$ than $I(t_k)$, $D(t_i) = C_{s(k),i}$ and (time has non negative values):

$$I_d^c(t_k) = (I(t_k) - C_{s(k),i}(x_{s(k)}, x_i)) \cap [0\ \infty) \qquad (1)$$

3.2. The arc associated with the firing of t_j

In our approach, the arc $(\mathcal{C}, \mathcal{C}')$, leading the system from class $\mathcal{C}$ to $\mathcal{C}'$ with the firing of transition t_j, is labelled by t_j and is associated with:

- a set of unbounded transitions not constrained by the firing of transitions leading to $\mathcal{C}$, $T_\infty^{j,c} = T_\infty^c \setminus \{t_j\}$,
- a STN $Nt_{j,c}$ delimiting the firing date of t_j from $\mathcal{C}$. It reflects the memory of the past necessary to characterize the dates of the future events.

Let t_j be a transition among the n enabled transitions at class $\mathcal{C} = \{M, Nc, T_\infty^c\}$, with $Nc = (Vc, Cc)$, and let t_l, $l \neq j$, be the other $n-1$ enabled transitions at $\mathcal{C}$.

Definition 3 *The STN* $Nt_{j,c} = (Vt, Ct)$ *delimiting the firing of* t_j *from class* $\mathcal{C}$ *is composed of:*

1. *all* Nc *variables and constraints,* $Vt = Vc, Ct = Cc$*;*
2. *the variable* x_j^{oj} *(firing date of* t_j*) and the static interval* $I(t_j)$ *as a constraint between* $x_{s(j)}^{osj}$ *and* x_j^{oj}*,*
3. *the variable* y_l^{ol} *corresponding to each bounded transition* t_l*, with the constraint* $C_{s(l),l}(x_{s(l)}^{osl}, y_l^{ol}) = [d_{Ml}, d_{Ml}]$*, the upper bound of static interval* $I(t_l)$*,*
4. *the variable* z_l^{ol}*,* $l \neq j, l \notin T_\infty^{j,c}$*, corresponding to each enabled unbouded transition* t_l*, with the constraint* $C_{s(l),l}(x_{s(l)}^{osl}, y_l^{ol}) = [d_{ml}, d_{ml}]$*, the lower bound of static interval* $I(t_l)$ *(*$|\{z_l\}| + |\{y_l\}| = n-1$*). If* $c_{mlj}(x_l^{ol}, x_j^{oj}) \geq 0$*,* $T_\infty^{j,c} = T_\infty^{j,c} \cup \{t_l\}$*,*
5. $C_{i,j}(x_i^{oi}, x_j^{oj}) = [0, \infty)$ *to express the fact that* t_j *must be fired* after t_i *(interleaving semantics),*
6. $C_{j,l}(x_j^{oj}, y_l^{ol}) = [0, \infty)$*,* $l \neq j$*, to express the fact that* t_j *must be fired* before *the upper bound of the firing interval of bounded transitions* t_l *(strong semantics).*

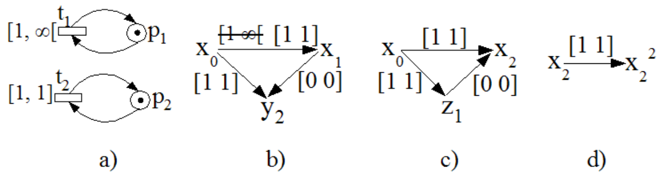

Figure 1. Petri net and some $Nt_{j,c}$

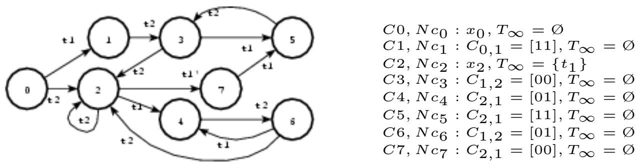

Figure 2. Graph of Petri net of fig. 1.a

If after applying Floyd-Warshall algorithm, $Nt_{j,c}$ is consistent, t_j can be fired. The final $Nt_{j,c}$ is obtained deleting all nodes y_l^{ol}, z_l^{ol} and $x_{s(l)}$ (if all the other transitions enabled by $x_{s(l)}$ are in $T_\infty^{j,c}$). All constraints directly connected to the deleted variables are also deleted [Ma 05].

Let us considerer the Petri net of fig. 1.a, with initial class $\mathcal{C}_0 = \{p_1p_2, x_0, \emptyset\}$. The firing of t_1 from $\mathcal{C}_0$ leads to class $\mathcal{C}_1$; this arc has $Nt_{1,0}$ (fig. 1.b) and $T_\infty^{1,0} = \emptyset$. The final $Nt_{1,0}$ is given by $V = \{x_0, x_1\}$ with $C_{0,1} = [1\ 1]$. Class $\mathcal{C}_1$ has $M_1 = p_1p_2$, $T_\infty^1 = \emptyset$ and Nc_1 given by $V = \{x_0, x_1\}$ with $C_{0,1} = [1\ 1]$.

The firing of t_2 from $\mathcal{C}_0$ leads to class $\mathcal{C}_2$ and is associated with $Nt_{2,0}$ (fig. 1.c). The final $Nt_{2,0}$ is only given by node x_2 and $T_\infty^{2,0} = \{t_1\}$. Class $\mathcal{C}_2$ with $M_2 = p_1p_2$, set $T_\infty^2 = \{t_1\}$ has Nc_2 given only by node x_2.

3.3. Restricted class

Some constraint $C_{k,l}$ between two nodes x_k and x_l in the $Nt_{j,c}$ from the class $\mathcal{C}$, can become more restricted than in the network Nc of $\mathcal{C}$. This means that transition t_j can only be fired from the states of $\mathcal{C}$ for which variables x_k and x_l verify this new, more restricted constraint $C_{k,l}$. This defines a sub-class $\mathcal{C}r^j$ restricted in order to permit the firing of t_j.

Let t_j be a transition which can be fired from $\mathcal{C} = (M, Nc)$ whose firing date is delimited by the $Nt_{j,c}$.

Definition 4 *The* ***restricted class*** $\mathcal{C}r^j = (M_r, Nc_r)$ *of class* $\mathcal{C}$ *is created if* $Nt_{j,c} \cap Nc \neq Nc$*, and is defined by: i)* $M_r = M$*, ii)* $T_\infty^{\mathcal{C}_r} = T_\infty^{\mathcal{C}}$*, iii)* $Nc_r = Nt_{j,c} \cap Nc$.

After a new application of Floyd-Warshall new restricted classes can appear in the past.

3.4. Equivalent classes

Definition 5 *Two classes* $\mathcal{C} = (M, Nc)$ *and* $\mathcal{C}' = (M', Nc')$*, differing from the initial class* $\mathcal{C}_0$*, with* $Nc = (X, C)$ *and* $Nc' = (X', C')$ *are* ***equivalent*** *if:*

1. *they have the same marking,* $M = M'$ *and the same set* T_∞, $T_\infty^c = T_\infty^{c'}$,
2. *there exists a bijection* τ *between the elements of* X *and* X' *such that:* i) $x_k'^{ok} = \tau(x_i^{oi})$ *implies* $k = i$ *(they are firing dates of the same transition);* ii) *if* $x_i' = \tau(x_i)$ *and* $x_j' = \tau(x_j)$ *then* $C_{ij}'(x_i', x_j') = C_{ij}(x_i, x_j)$.

Definition 6 *A class* $\mathcal{C} = (M, Nc)$ *is equivalent to the initial class* $\mathcal{C}_0 = (M_0, x_0)$ *if: 1)* $M = M_0$ *and* $T_\infty^c = T_\infty^0$*, 2) the set of variables* X *of* Nc *is a singleton,* $X = \{x_k\}$ *(no past memory).*

In fact, the firing of t_k leads the system back to the initial marking M_0 and enables all transitions at this marking.

The firing of t_2 in fig. 1 from $\mathcal{C}_2$ leads to a class $\mathcal{C}'$; $T_\infty^{2,2} = \{t_1\}$ with $Nt_{2,2}$ represented in fig. 1.d. Class $\mathcal{C}'$ has $M' = M_2$ and Nc' given by x_2^2, so it is equivalent to $\mathcal{C}_2$ (def. 5). The classes and the graph are represented in fig. 2 ($\mathcal{C}_7$ is a restricted class of $\mathcal{C}_4$). All classes have $M = p_1p_2$.

3.5. Sequence characterization

The temporal network of a sequence $\sigma = t_1; ...; t_i; t_j; ...; t_n$ from a class $\mathcal{C}$ is given by $Nt_\sigma = Nt_{1,c} \cup \ldots Nt_{i,ci} \cup Nt_{j,cj} \cup \ldots \cup Nt_{n,cn}$ [Ma 05].

A particular case appear when $\sigma = t_1; ...; t_i$ and the firing of last transition t_i leads to a class $\mathcal{C}$ and also to its restricted class $\mathcal{C}r$. Two networks are obtained, N_σ^1 leading to $\mathcal{C}$ and N_σ^2 leading to $\mathcal{C}r$, but $N_\sigma^1 \supseteq N_\sigma^2$ and so the network characterizing σ is N_σ^1 (see an example in the sequel).

4. Example

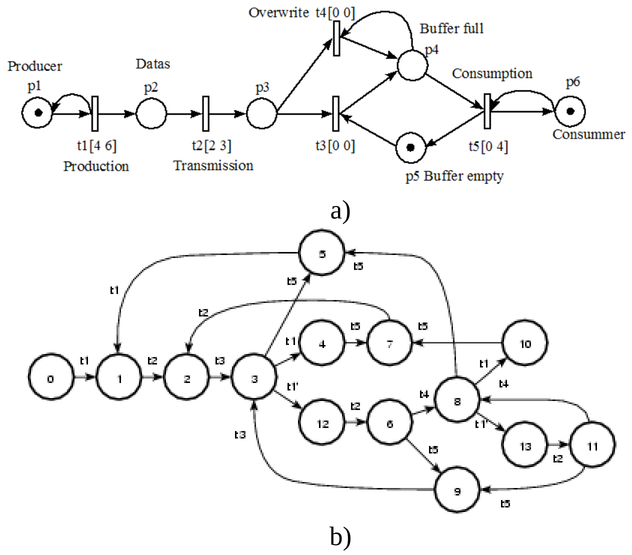

Figure 3. a) Petri net; b) Graph of classes

Let us consider an unidirectional protocol of data transfer [Ca 05] modeled by the Petri net in fig. 3.a presenting infinite sequences. We want to know if an overwrite, due to the earlier arriving of a new message whereas the precedent was not yet consumed, can occur in this system (represented by transition $t4$). The underlying Petri net (the structure without time specifications) is unbounded and so it is not possible to know if the overwrite is done. The graph is represented in fig. 3.b and the classes are given below:

Class	Marking	Constraints Nc	Class	Marking	Constraints Nc
$\mathcal{C}_0$	$p_1p_5p_6$	x_0	$\mathcal{C}_7$	$p_1p_2p_5p_6$	$C_{1,5}=[0\ 3]$
$\mathcal{C}_1$	$p_1p_2p_5p_6$	x_1	$\mathcal{C}_8$	$p_1p_4p_6$	$C_{1,4}=[2\ 3]$
$\mathcal{C}_2$	$p_1p_3p_5p_6$	$C_{1,2}=[2\ 3]$	$\mathcal{C}_9$	$p_1p_3p_5p_6$	$C_{1,5}=[2\ 3]$
$\mathcal{C}_3$	$p_1p_4p_6$	$C_{1,3}=[2\ 3]$	$\mathcal{C}_{10}$	$p_1p_2p_4p_6$	$C_{4,1}=[1\ 4]$
$\mathcal{C}_4$	$p_1p_2p_4p_6$	$C_{3,1}=[1\ 4]$	$\mathcal{C}_{11}$	$p_1p_3p_4p_6$	$C_{4,1}=[1\ 2]$
$\mathcal{C}_5$	$p_1p_5p_6$	$C_{1,5}=[2\ 6]$		$C_{1,2}=[2\ 3]$	$C_{4,2}=[3\ 4]$
$\mathcal{C}_6$	$p_1p_3p_4p_6$	$C_{3,1}=[1\ 2]$	$\mathcal{C}_{12}$	$p_1p_2p_4p_6$	$C_{3,1}=[1\ 2]$
	$C_{1,2}=[2\ 3]$,	$C_{3,2}=[3\ 4]$	$\mathcal{C}_{13}$	$p_1p_2p_4p_6$	$C_{4,1}=[1\ 2]$

We present here only some temporal network Nt attached to the arcs:

$Nt_{1,0}$,(x_0, x_1)=[4 6], $Nt_{2,1}$,(x_1, x_2)=[2 3]
$Nt_{3,2}$,(x_1, x_2)=(x_1, x_3)=[2 3], (x_2, x_3)=[0 0]
$Nt_{1,3}$,(x_1, x_3)=[2 3],(x_1, x_1^2)=[4 6],(x_3, x_1^2)=[1 4]
$Nt'_{1,3}$,(x_1, x_3)=[2 3],(x_1, x_1^2)=[4 5],(x_3, x_1^2)=[1 2]

Which constraints must be met in order to fire t_4 (overwriting)? Let us consider a sequence including the firing of t_4 in the graph of fig. 3.b, for example, $\sigma = t_1; t_2; t_3; t_1; t_2; t_4$. The network delimiting σ is given by $N_\sigma = Nt_{1,0} \cup Nt_{2,1} \cup Nt_{3,2} \cup Nt_{1,3} \cup Nt_{2,12} \cup Nt_{4,6}$, represented in fig. 4 (x_1^2 is the second firing of t_1 in σ). Two constraints are redundant in N_σ since we can obtain them from other constraints, $(x_1, x_3) = [2\ 3]$ and $(x_3, x_4) = [3\ 4]$. The occurrence of overwriting depends on the firing interval of $t1$ from $\mathcal{C}_3$; when $t1$ is fired between $[1\ 2]$ after $t3$ firing (rapid production), it can occurs.

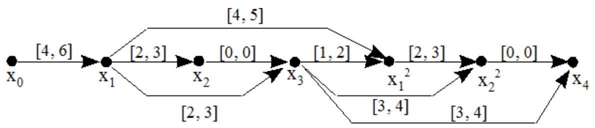

Figure 4. Temporal network of sequence σ

Let us consider now the sequence $\sigma_1 = t_1; t_2; t_3; t_1$ in figure 3.b. Two paths in the class graph can be associated with σ_1 and in consequence two networks are obtained: $N^1_{\sigma_1} = Nt_{1,0} \cup Nt_{2,1} \cup Nt_{3,2} \cup Nt_{1,3}$ (leading to $\mathcal{C}_4$) and $N^2_{\sigma_1} = Nt_{1,0} \cup Nt_{2,1} \cup Nt_{3,2} \cup Nt'_{1,3}$ (leading to $\mathcal{C}_{12}$). As $\mathcal{C}_{12}$ is a restriction of $\mathcal{C}_4$ (section 3.5) $N^1_{\sigma_1} \supseteq N^2_{\sigma_1}$, so the network characterizing σ_1 is given by $N^1_{\sigma_1}$ in fig. 5.

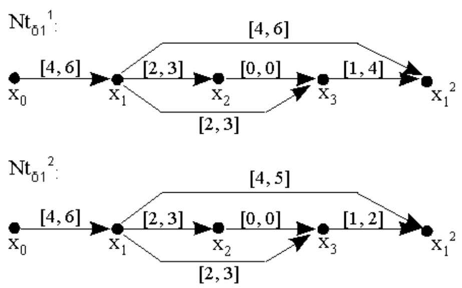

Figure 5. Temporal networks $N^1_{\sigma_1}$ and $N^2_{\sigma_1}$

5. Conclusion

The presented approach presents a graph of classes that allows obtaining the exact temporal constraints that have to be verified by each transition firing with respect to a given firing sequence. It extended the graph presented in [Ma 05] considering unbounded transitions. A state class reached by the firing of t in the graph is defined by a marking, a temporal network and a set of transitions not constrained by the firing of t. An arc between two classes is labeled by a temporal network Nt_i delimiting the firing date of a t_i, t_i itself and a set of transitions not constrained by the firing of transitions leading to the source class. The temporal constraints verified by a firing sequence are obtained by the union of the temporal constraints Nt_i attached to each arc along the corresponding path on the class graph.

There are two main differences with the graphs proposed in [Yo 98, Be 04]. The first one is that we use simple temporal networks instead of geometrical regions to deal with temporal information. The second one appears in the way the past is memorized. In relation to [Yo 98], our class does not keep all the constraints in the past, but only the ones that are necessary to characterize it, as proven in [Ma 05], and consider unbounded transitions. In relation to [Be 04],we can directly obtain the set of constraints of a sequence instead of obtaining it by transformations and calculations.

Further research should consider to extend the graph of classes to deal with time fuzzy Petri nets, where the interval of firing is fuzzy, allowing to evaluate a possibility and necessity degree of transition firing.

References

[Be 04] B.Berthomieu, P.O.Ribet, F.Vernadat: The tool TINA: construction of abstract state spaces for Petri nets and time Petri nets, IJPR, Vol.42, N^{o}14, pp.2741-2756, 15 Juillet 2004.

[Ca 05] J.Cardoso, S.Cousy, G.Juanole: A Graph of State Classes for fuzzy time Petri nets, 16th IFAC World Congress, Juillet 2005, Prague.

[Gui 04] G. Gardey, O.H. Roux, O.F. Roux : A zone-based method for computing the state space of a time Petri net. In FORMATS'03, LNCS 2791, pages 246-259, Marseille, France, Sep. 2003. Springer.

[Ma 05] X.Mao, J.Cardoso, R.Valette: A new graph of classes for the preservation of quantitative temporal constraints, ATVA 2005, LNCS 3707, pp. 278-292.

[De 91] R.Dechter, I.Meiri, J.Pearl: Temporal constraint networks, AI, Vol 49, p.61-91, 1991.

[Ri 01] N.Rivière, B.Pradin-Chézalviel, R.Valette: Reachability and temporal conflicts in t-time Petri nets, PNPM'01, Aachen, pp.229-238, 11-14 Sep 2001.

[Yo 98] T.Yoneda, H.Ryuba: CTL Model checking of time Petri nets using geometric regions, *IEICE Trans. inf. & Syst.*, Vol E81-D, No. 3, pp.297-396, 1998.