Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science 239 (2009) 155–165
Electronic Notes in Theoretical Computer Science
www.elsevier.com/locate/entcs

Covering Steps Graphs of Time Petri Nets

Hanifa Boucheneb[1]

Laboratoire VeriForm, Department of Computer Engineering, École Polytechnique de Montréal
P.O. Box 6079, Station Centre-ville, Montréal, Québec,Canada, H3C 3A7

Kamel Barkaoui[2]

Laboratoire CEDRIC, Conservatoire National des Arts et Métiers,
292 rue Saint Martin, Paris Cedex 03, France

Abstract

We consider here time Petri nets and the covering steps graph technique proposed by Vernadat et al. for untimed Petri nets. In this technique, some transitions are put together to be fired in a single transition step. This paper investigates how this technique can be extended to be applied to time Petri nets.

Keywords: Time Petri nets, state class graph method, covering steps graph.

1 Introduction

The main obstacle for enumerative verification methods such as model checking is the state space explosion problem. Many techniques have been developed to alleviate this problem such as abstraction [2,3,4,7,11,16] and partial order techniques [5,6,8,9,10,12,13,14,15,16].

Abstraction techniques aim to construct by removing some irrelevant details, a contraction of the state space, which preserves properties of interest. For better performances, the contraction should also be the smallest possible and computed with minor resources too (time and space). The preserved properties can be verified using the standard techniques on the contraction [11].

Partial order techniques aim to construct a smaller state space by addressing a specific reason behind the state space explosion, namely the existence of many

[1] Email: hanifa.boucheneb@polymtl.ca

[2] Email: kamel.barkaoui@cnam.fr

doi:10.1016/j.entcs.2009.05.037

potentially equivalent firing sequences[3] which are not distinguishable by some properties. The idea is to represent some equivalent firing sequences by only one or group in one step the firing of some transitions (covering steps graphs).

This paper investigates how the covering steps graph technique can be applied to time Petri nets (TPN in short). In section 2, we present the TPN model and its semantics. Section 3 deals with the abstraction of the TPN state space. Section 4 is devoted to the covering steps graph technique and its application to TPN.

2 Time Petri Nets

Let $\mathbb{N}$ be the set of nonnegative integers, Q^+ the set of nonnegative rational numbers and INT the set of non empty intervals of the form: $[a, b]$ or $[a, \infty[$, where $a, b \in Q^+$. Formally, a TPN is a tuple $(P, T, Pre, Post, M_0, Is)$ where P and T are finite sets of places and transitions such that $(P \cap T = \emptyset)$, Pre and $Post$ are the backward and the forward incidence functions $(Pre, Post : P \times T \longrightarrow \mathbb{N})$, M_0 is the initial marking $(M_0 : P \longrightarrow \mathbb{N})$, and Is is the static firing interval function $(Is : T \rightarrow INT)$.

Let M be a marking and $t_i \in T$. t_i is enabled for M iff all required tokens for firing t_i are present in M, i.e.: $\forall p \in P, M(p) \geq Pre(p, t_i)$. Without loss of generality, for reasons of clarity in this paper, if a transition remains enabled after its firing, it is considered newly enabled. We denote by $En(M)$ the set of all transitions enabled for M, i.e.: $En(M) = \{t_i \in T \mid \forall p \in P, Pre(p, t_i) \leq M(p)\}$.

Let M be a marking, $t_i \in En(M)$ a transition enabled for M and M' the marking reached by firing t_i from M, i.e.: $\forall p \in P, M'(p) = M(p) - Pre(p, t_i) + Post(p, t_i)$. $Nw(M, t_i)$ denotes the set of all transitions enabled by firing t_i from M, i.e.: $Nw(M, t_i) = \{t_j \in En(M') \mid t_j = t_i \vee \exists p \in P, M(p) - Pre(p, t_i) < Pre(p, t_j)\}$. $CF(M, t_i)$ denotes the set of transitions enabled in M but in conflict with t_i, i.e.: $CF(M, t_i) = \{t_k \in En(M) \mid t_k = t_i \vee \exists p \in P, M(p) < Pre(p, t_k) + Pre(p, t_i)\}$.

The TPN state is defined as a pair $s = (M, I)$, where M is a marking and I is a firing interval function $(I : En(M) \rightarrow INT)$. For some t_i of $En(M)$, $\downarrow I(t_i)$ and $\uparrow I(t_i)$ denote respectively the lower and the upper bounds of the firing interval of t_i. The set of firing intervals $\{I(t_i) | t_i \in En(M)\}$ is called the firing domain of s. The initial state is $s_0 = (M_0, I_0)$ where $I_0(t_i) = Is(t_i)$, for all $t_i \in En(M_0)$.

The TPN state evolves either by time progressions or by firing transitions. When a transition t_i becomes enabled, its firing interval is set to its static firing interval. The bounds of this interval decrease synchronously with time, until t_i is fired or disabled by another firing. t_i can fire if the lower bound of its firing interval reaches 0 but must fire, without any additional delay, if the upper bound of its firing interval reaches 0. The firing of a transition takes no time but may lead to another marking. Let $s = (M, I)$ and $s' = (M', I')$ be two interval states of a TPN, $\theta \in \mathbb{R}^+$ and $t_f \in T$. We write $s \xrightarrow{\theta} s'$, also denoted $s + \theta$, iff s' is reachable from s after θ time units, i.e.: $\bigwedge\limits_{t_i \in En(M)} \theta \leq \uparrow I(t_i)$, $M' = M$, $\forall t_j \in En(M')$, $\downarrow I'(t_j) = Max(\downarrow I(t_j) - \theta, 0)$

[3] Two firing sequences are equivalent if one of them can be obtained from the other by successive permutations.

and $\downarrow I'(t_j) = \uparrow I(t_j) - \theta$.

We write $s \overset{t_f}{\rightarrow} s'$ iff s' is immediately reachable from s by firing transition t_f, i.e.: $t_f \in En(M)$, $\downarrow I(t_f) = 0, \forall p \in P, M'(p) = M(p) - Pre(p,t_f) + Post(p,t_f)$, and $\forall t_i \in En(M')$, $I'(t_i) = Is(t_i)$, if $\mathrm{t_i} \in \mathrm{Nw(M, t_f)}$ and $I'(t_i) = I(t_i)$ otherwise.

The TPN state space is the structure $(S, \rightarrow, s_0)$, where: s_0 is the initial state of the model and $S = \{s | s_0 \overset{*}{\rightarrow} s\}$ is the set of reachable states of the model ($\overset{*}{\rightarrow}$ being the reflexive and transitive closure of relation $\rightarrow$ defined above). A *run* in the TPN state space $(\mathcal{S}, \rightarrow, s_0)$, starting with some state s, is a maximal sequence $s_1 \overset{\theta_1}{\rightarrow} s_1 + \theta_1 \overset{t_1}{\rightarrow} s_2 \overset{\theta_2}{\rightarrow} s_2 + \theta_2.....$, such that $s_1 = s$. A marking M is reachable iff $\exists s \in \mathcal{S}$ s.t. its marking is M. Runs of the model are all runs starting with s_0.

3 State Class Graph

Among the TPN state space abstractions proposed in the literature [2,4,7,16], we consider here the state class graph (SCG). In the SCG, all states reachable from the initial state by firing the same sequence of transitions are agglomerated in the same set of states. These sets are then considered modulo the relation of equivalence defined by: Two sets of states are equivalent iff they have the same marking and the same firing domain[4]. All equivalent sets are agglomerated in the same node called a *state class* defined as a pair $\alpha = (M, F)$, where M is a marking and F is a formula which characterizes the firing domain of α. Each transition t_i which is enabled in M is a variable with the same name in F representing its firing delay. Moreover, F can be rewritten as a set of atomic constraints of the form[5]: $t_i - t_j \leq c$, $t_i \leq c$ or $-t_j \leq c$, where t_i, t_j are transitions, $c \in Q \cup \{\infty\}$ and Q is the set of rational numbers. F has a unique canonical form defined by: $\bigwedge_{x,y \in En(M) \cup \{o\}} x - y \leq Sup_F(x-y)$, where o is a symbol representing the value 0 and $Sup_F(x-y)$ is the supremum (i.e., the least upper bound) of the difference $x - y$ in the domain of F. Its computation is based on the shortest path *Floyd-Warshall*'s algorithm and is considered as the most costly operation (cubic in the number of variables of F).

Two state classes are said to be equal iff they share the same marking and their firing domains are equal (i.e., they have the same canonical form).

Starting from the initial state class $\alpha_0 = (M_0, F_0)$, where M_0 is the initial marking and $F_0 = (\bigwedge_{x,y \in En(M_0) \cup \{o\}} x - y \leq \uparrow Is(x) - \downarrow Is(y))$ with $\downarrow Is(o) = \uparrow Is(o) = 0$, successor state classes are computed using the following firing rule: Let $\alpha = (M, F)$ be a state class and t_f a transition. α has a successor by t_f (i.e., $succ(\alpha, t_f) \neq \emptyset$) iff t_f is enabled in M and can be fired before any other enabled transition (i.e.: $F \wedge (\bigwedge_{t_i \in En(M)} t_f - t_i \leq 0)$ is consistent).

If $succ(\alpha, t_f) \neq \emptyset$ then $succ(\alpha, t_f) = (M', F')$ can be computed as follows[6]:

(i) $\forall p \in P, M'(p) = M(p) - Pre(p, t_f) + Post(p, t_f)$;

[4] The firing domain of a set of states is the union of the firing domains of its states.

[5] For economy of notation, we use operator $\leq$ even if $c = \infty$.

[6] Variable t_k^f is associated with the instance of transition t_k that is newly enabled by t_f from α.

(ii) Set F' to $F \wedge \bigwedge_{t_i \in En(M)} t_f - t_i \leq 0 \;\wedge \bigwedge_{t_k \in Nw(M,t_f)} \downarrow Is(t_k) \leq t_k^f - t_f \leq \uparrow Is(t_k)$;

(iii) Put F' in canonical form, eliminate o and all transitions of $CF(M, t_f) - \{t_f\}$;

(iv) Rename t_f in o and each transition t_k^f in t_k.

Let α, α' be two state classes and t_f a transition. We write $\alpha \xrightarrow{t_f} \alpha'$ iff $\alpha' = succ(\alpha, t_f) \neq \emptyset$. The SCG of a *TPN* is the structure $(\mathcal{C}, \longrightarrow, \alpha_0)$ where α_0 is the initial state class and $\mathcal{C} = \{\alpha | \alpha_0 \xrightarrow{*} \alpha\}$ is the set of reachable state classes. The SCG is finite for bounded *TPN* [7] and preserves linear properties [2]. Moreover, it is, in general, more compact than other state space abstractions [2,3].

In [3], authors have proposed a bisimulation relation $\simeq$ over the SCG, which induces more compact graphs preserving linear properties: $\forall \alpha_1 = (M_1, F_1), \alpha_2 = (M_2, F_2) \in \mathcal{C}$, $\alpha_1 \simeq \alpha_2$ iff (i) $M_1 = M_2$ and (ii) $\forall t_i, t_j \in En(M_1)$,

$$\begin{cases} Min(0, Sup_{F_1}(t_i - t_j)) = Min(0, Sup_{F_2}(t_i - t_j)) & \text{if } \mathrm{t_j \in CF(M_1, t_i)} \\ Sup_{F_1}(t_i - t_j) = Sup_{F_2}(t_i - t_j) & \text{otherwise} \end{cases}$$

Intuitively, the basic idea behind this relation is to eliminate information which are not needed to compute successor state classes. According with the firing rule given of the SCG, simple constraints [8] are not relevant for computing successor classes. Moreover, since the firing of a transition will disable all transitions conflicting with it, some time constraints between conflicting transitions are not relevant for computing successor state classes.

We propose, here, to define a class of equivalence of $\simeq$ as an over-approximation of its state classes. Let $\alpha = (M, F)$ be a state class, in canonical form, its class of equivalence is the state class $\widetilde{\alpha} = (M, \widetilde{F})$, where $\widetilde{F}$ is the formula obtained from F by eliminating o and all constraints $t_i - t_j \leq c$ such that $t_j \in CF(M, t_i) \wedge c \geq 0$, i.e.: Let $E(\alpha) = \{(t_i, t_j) \mid t_i, t_j \in En(M) \wedge (t_j \in CF(M, t_i) \Rightarrow Sup_F(t_i - t_j) < 0)\}$. $\widetilde{F} = \bigwedge_{(t_i,t_j) \in E(\alpha)} t_i - t_j \leq Sup_F(t_i - t_j)$. Note that $\alpha \subseteq \widetilde{\alpha}$.

Lemma 3.1 *α and $\widetilde{\alpha}$ have the same firing sequences.*

Proof. The proof is immediate from the fact that $\simeq$ is a bisimulation relation over the SCG [3] and $\alpha \simeq \widetilde{\alpha}$.□

Note that the successor function *succ*, defined before, adds only constraints of the form $t_i - t_j \leq c$, where t_i, $t_j \in T$ and $c \in \{0, - \downarrow Is(t_j), \uparrow Is(t_i)\}$. Therefore, it can be used to compute successors of classes of equivalence. Let α, α' be two state classes and t_i a transition such that $\alpha' = succ(\alpha, t_i) \neq \emptyset$. $\widetilde{succ}(\alpha, t_i)$ denotes the over-approximation of $succ(\alpha, t_i)$ (i.e.: $\widetilde{\alpha}' = \widetilde{succ}(\alpha, t_i)$).

In the rest of the paper, we consider the quotient graph of the *SCG* w.r.t. $\simeq$, where equivalent state classes w.r.t. $\simeq$ are represented by their over-approximations defined above. This graph, called Contracted State Class Graph (*CSCG*), is defined as a structure $(\mathcal{B}, \rightsquigarrow, \beta_0)$ where: (i) $\beta_0 = \widetilde{\alpha}_0$ is the equivalence class w.r.t. $\simeq$ of the initial state class of the SCG, (ii) $\rightsquigarrow$ is the transition relation between classes of equivalence defined by: $\beta \overset{t_i}{\rightsquigarrow} \beta'$ iff $succ(\beta, t_i) \neq \emptyset \;\wedge\; \beta' = \widetilde{succ}(\beta, t_i)$, and (iii)

[7] A TPN is bounded iff it has a finite number of reachable markings.

[8] Simple constraints are of the form: $-t_i \leq c$ or $t_i \leq c$ where $t_i \in T$ and $c \in Q \cup \{\infty\}$, Q being the set of rational numbers.

$\mathcal{B} = \{\beta | \beta_0 \overset{*}{\rightsquigarrow} \beta\}$, $\overset{*}{\rightsquigarrow}$ is the set of reachable classes of equivalence w.r.t. $\simeq$.

A *run* in the CSCG starting from a state class β, is a maximal sequence $\rho = \beta_1 \overset{t_1}{\rightsquigarrow} \beta_2 \overset{t_2}{\rightsquigarrow} \beta_3 \overset{t_3}{\rightsquigarrow}$ ....., such that $\beta_1 = \beta$. Let β, β' be two state classes and ω a sequence of transitions ($\omega \in T^+$). $\beta \overset{\omega}{\rightsquigarrow} \beta'$ (with $\beta' = \widetilde{succ}(\beta, \omega)$) means that the sequence ω is firable from β (i.e.: $succ(\beta, \omega) \neq \emptyset$) and its firing leads to β' in the CSCG.

Let β and β' be two state classes in canonical form having the same marking M. β is included β' iff $\forall t_i, t_j \in En(M), Sup_F(t_i - t_j) \leq Sup_{F'}(t_i - t_j)$.
The union of state classes may be not convex. The convex hull of the union of β and β', denoted $\beta \sqcup \beta'$, is the state class $\beta" = (M, F")$ defined by: $\forall t_i, t_j \in En(M), Sup_{F"}(t_i - t_j) = Max(Sup_F(t_i - t_j), Sup_{F'}(t_i - t_j))$. In case $\beta \cup \beta'$ is not convex, its convex hull contains some extra states which do not belong neither to β nor to β'. Otherwise, we have: $\beta \cup \beta' = \beta \sqcup \beta'$.

4 Covering steps graphs for time Petri nets

Commonly, partial order techniques are shown to be very useful for specially a system composed of several concurrent processes. The construction of the global state space of such a system is mainly based on the interleaving semantics that may cause a blow-up of the state space. Partial order techniques aim to counter this problem, by considering only some representative firing sequences of concurrent transitions (reduced graphs) [8,10,14,12,16], or grouping into atomic firing steps some concurrent transitions (covering steps graphs) [15]. In [13], the authors have shown how to combine the persistent set method [8] with the covering steps method [15] to verify LTL_{-X} properties of untimed Petri nets[9]. Their approach consists of two steps: 1) computing, for each marking, the subset of enabled transitions to explore (persistent set) and then 2) computing groups of transitions within the persistent set to be fired together in an atomic step. We interest here to extend the covering steps method, proposed in [13,15] for Petri nets, to time Petri nets.

In general, partial order reduction techniques are based on the concept of *stuttering-equivalent sequences*. In the context of the CSCG, this concept can be defined as follows: Let ϕ be an LTL_{-X} formula whose atomic propositions are interpreted on markings and L_ϕ the label function which associates with each state class the set of atomic propositions of ϕ that are satisfied for its marking. Let ρ be run of the CSCG. The label set sequence of ρ w.r.t. ϕ is obtained by replacing each state class of ρ with its label set, and collapsing to a single set any maximal sequence of identical label sets. Two runs are stuttering-equivalent if they have identical label set sequences. It has been shown in [10,12,14] that for any LTL_{-X} formula ϕ, the truth values of ϕ for stuttering-equivalent runs are the same. Therefore, to verify ϕ for all runs of a state class, it suffices to consider only runs which are not stuttering-equivalent (representative runs).

The selection of representative runs must be made by selecting, from each state class, transitions and/or firing steps to be considered, without exploring beforehand

[9] LTL_{-X} is a subclass of linear time logic where the next operator X is not allowed.

all runs. This selection is mainly based on two notions: visibility and independence of transitions. A transition t_i is said to be invisible w.r.t. ϕ if its input and output places [10] do not appear in ϕ. We denote $vis(\phi)$ the set of transitions visible w.r.t. ϕ. The firing order of visible transitions may be relevant for the evaluation of ϕ. Intuitively, two transitions t_1 and t_2 are independent iff whenever t_1 and t_2 are firable, we can fire them in any order and the resulting state classes are equal.

The relation of independence is however less appropriate for time Petri nets. Indeed, in the TPN state space abstractions, a node represents, in fact, a finite/infinite set of states (state class) and two interleavings of concurrent transitions may lead to two different state classes. We show, by means of two examples, up to which level state classes, resulting from the interleaving of concurrent transitions, may be different.

The TPN in Fig.1 (left) shows that the different interleavings of the same set of transitions may lead to state classes which have different sets of firing sequences. From the initial state $\beta_0 = (p_0 + p_1, -3 \leq t_1 - t_2 \leq 1)$, sequences $t_1 t_2$ and $t_2 t_1$ lead respectively to state classes $\beta_1 = (p_3 + p_4, -2 \leq t_3 - t_4 \leq -1)$ and $\beta_2 = (p_3 + p_4, -1 \leq t_3 - t_4 \leq 0)$. Transition t_4 is firable from β_2 (since $-1 \leq t_3 - t_4 \leq 0 \wedge t_4 - t_3 \leq 0$ is consistent) but not firable from β_1 (since $-2 \leq t_3 - t_4 \leq -1 \wedge t_4 - t_3 \leq 0$ is not consistent).

The TPN in Fig.1 (right) shows that the union of state classes resulting from the interleaving of concurrent transitions is not necessarily convex. From the initial state $\beta_0 = (p_1 + p_2, -3 \leq t_1 - t_2 \leq 1)$, the firings of sequences $t_1 t_2$ and $t_2 t_1$ lead respectively to state classes:
$\beta_1 = (p_3 + p_4 + p_5, -2 \leq t_3 - t_4 \leq 0 \wedge -2 \leq t_3 - t_5 \leq 2 \wedge 0 \leq t_4 - t_5 \leq 2)$ and
$\beta_2 = (p_3 + p_4 + p_5, -1 \leq t_3 - t_4 \leq 1 \wedge -1 \leq t_3 - t_5 \leq 2 \wedge -1 \leq t_4 - t_5 \leq 2)$.
These state classes are not equal and none of them is included in the other: $\beta_1 \nsubseteq \beta_2$ and $\beta_2 \nsubseteq \beta_1$. In addition, their union $\beta_1 \cup \beta_2$ is not convex because $\beta_1 \cup \beta_2 \neq \beta_1 \sqcup \beta_2$. Indeed, $\beta_1 \sqcup \beta_2 = (p_3 + p_4 + p_5, -2 \leq t_3 - t_4 \leq 1 \wedge -2 \leq t_3 - t_5 \leq 2 \wedge -1 \leq t_4 - t_5 \leq 2)$ and the subdomain of $\beta_1 \sqcup \beta_2$ defined by: $t_3 - t_4 = -1 \wedge t_3 - t_5 = -2 \wedge t_4 - t_5 = -1$ is neither included in the domain of β_1 nor in the domain of β_2. For instance, the valuation $(t_3 = 0, t_4 = 1, t_5 = 2)$ belongs to the convex hull of the union of β_1 and β_2 but does not belong neither to β_1 nor to β_2.

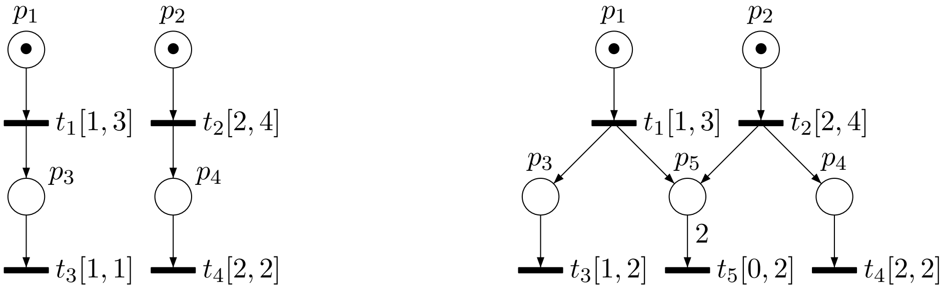

Fig. 1. Time Petri nets used to illustrate features of the interleaving

[10] Input and output places of some transition t_i are sets defined respectively by: ${}^\circ t_i = \{p \in P | Pre(p, t_i) > 0\}$ and $t_i{}^\circ = \{p \in P | Post(p, t_i) > 0\}$.

To introduce the principle of the covering steps method we propose here for time Petri nets, we consider a state class β of some system composed of n concurrent processes (TPN's). Suppose that each process has exactly one firable transition from β and the property, to be verified, relates only to the state class β and state classes resulting from the different firing orders (without depending on the intermediate state classes). These firable transitions can be ordered in $n!$ possible ways, which may lead to different state classes. In case the union of the resulting state classes is convex, it is much more efficient to represent the different firing orders by a single firing step and the resulting state classes by their union. In this way, intermediate state classes and different firing orders are not explored and the truth value of the property is preserved. To apply this reduction principle, we define the notion of weak-commutative over sets of transitions as follows:

Definition 4.1 Let β be a state class of $\mathcal{B}$, ϕ an LTL_{-X} formula, $T_f = \{t_{f_1}, t_{f_2}, ..., t_{f_n}\} \subseteq T$ (with $n > 1$) and $\Omega(T_f)$ the set of sequences equivalent to the sequence $t_{f_1} t_{f_2} ... t_{f_n}$. T_f is weak-commutative, denoted $\wr T_f$, in β w.r.t. ϕ iff:

(i) The number of visible transitions w.r.t. ϕ in T_f does not exceed one (i.e.: $|vis(\phi) \cap T_f| \leq 1$);

(ii) $\forall p \in P, M(p) \geq \sum\limits_{t_{f_i} \in T_f} Pre(p, t_{f_i})$ and $\forall t_{f_i} \in T_f, succ(\beta, t_{f_i}) \neq \emptyset$;

(iii) $\bigcup\limits_{\omega \in \Omega(T_f)} \widetilde{succ}(\beta, \omega)$ is convex.

Note that condition (ii) implies that transitions of T_f can be fired in any order from β.

The covering steps graphs of the CSCG is defined in a similar way as in [15], except that the classical independence relation is replaced by the weak-commutative relation defined above.

Definition 4.2 [15] Let $(\mathcal{B}, \rightsquigarrow, \beta_0)$ be the CSCG of some TPN. A covering steps graph of the CSCG w.r.t. an LTL_{-X} formula ϕ, is a transition system $(\mathcal{B}_R, \rightsquigarrow_R, \beta_{0_R})$ where:

- $\beta_{0_R} = \beta_0$. The initial class of the covering steps graph is exactly the initial state class of the CSCG.
- $\mathcal{B}_R$ is the set of reachable state classes of the covering steps graph s.t. $\forall \beta_R \in \mathcal{B}_R, \exists \beta_1, ..., \beta_n \in \mathcal{B}, \beta_R = \bigcup\limits_{i=1,n} \beta_i$. Each state class of the covering steps graph is the union of some state classes of the CSCG.
- $\rightsquigarrow_R \in \mathcal{B}_R \times (2^T - \{\emptyset\}) \times \mathcal{B}_\mathcal{R}$ is a transition relation which satisfies the following conditions:

(i) $\forall \beta_R, \beta'_R \in \mathcal{B}_\mathcal{R}, \forall T_f \subseteq T,$

$$\beta_R \overset{T_f}{\rightsquigarrow}_R \beta'_R \Rightarrow \wr T_f \text{ in } \beta_\mathrm{R} \text{ w.r.t. } \phi \wedge \beta'_\mathrm{R} = \bigcup_{\omega \in \Omega(\mathrm{T_f})} \widetilde{\mathrm{succ}}(\beta_\mathrm{R}, \omega)$$

(ii) $\forall \beta_R \in \mathcal{B}_\mathcal{R}, \forall \omega \in T^+, \;\; succ(\beta_R, \omega) \neq \emptyset \;\;\Rightarrow$

$$\exists \beta'_R \in \mathcal{B}_\mathcal{R}, \exists T1_f, ..., Tn_f \subseteq T, \; \exists \omega_1 \in \Omega(T1_f), ..., \omega_n \in \Omega(Tn_f), \; \exists \omega' \in T^* \;\text{ s.t.}$$

$$\widetilde{succ}(\beta_R, \omega\omega') \subseteq \beta'_R \;\;\wedge\;\; \omega\omega' = \omega_1\omega_2...\omega_n \;\;\wedge\;\; \beta_R \overset{T1_fT2_f...Tn_f}{\rightsquigarrow_R} \beta'_R$$

Intuitively, condition (i) means that each firing step in the covering steps graph corresponds to the fusion of some firing sequences in the CSCG. Condition (ii) ensures that each firing sequence of the CSCG is represented in some sequence of steps in the covering graph.

Lemma 4.3 *The covering steps graph of the CSCG w.r.t. ϕ preserves ϕ.*

Proof. Each firing sequence ω in the CSCG is covered by a sequence of firing steps. Each sequence of firing steps in the covering graph is exactly the fusion of some firing sequences of the CSCG and in each firing step there is at most one visible transition w.r.t. ϕ. It follows that for each run ρ in the CSCG, there is a run ρ', in the covering graph, stuttering-equivalent to ρ w.r.t. ϕ, and for each run ρ' in the covering graph, there is a run ρ, in the CSCG, stuttering-equivalent to ρ' w.r.t. ϕ. □

Concretely, the construction of the covering steps graph needs to establish two main procedures:

(i) A procedure to compute, for a given LTL_{-X} formula ϕ and a state class β, sets of transitions to be fired together, in an atomic step, and those to be fired alone. Transitions to be fired in an atomic step must be weak-commutative in β w.r.t. ϕ. As different interleavings of the same set of transitions may lead to state classes whose union is not convex, we need, at this level, simple conditions which ensure convexity.

(ii) A procedure to calculate the successor state class by firing, in a single step, two or more transitions. This successor state class is the union of state classes resulting from the different firing orders.

Theorem 4.4 and Lemma 4.5 below establish two sufficient conditions which ensure convexity for the union of state classes reached by different interleavings of the same set of transitions. They also show how to compute this union without computing beforehand intermediate state classes.

Let $\beta = (M, F)$ be a state class and $T_f = \{t_{f_1}, t_{f_2}, ..., t_{f_n}\} \subseteq T$ be a subset of transitions such that:

(i) $\forall p \in P, M(p) \geq \sum_{t_{f_i} \in T_f} Pre(p, t_{f_i})$ and $\forall t_{f_i} \in T_f, \; succ(\beta, t_{f_i}) \neq \emptyset$;

(ii) $\forall t_{f_i} \in T_f, \forall \omega_1 \in T^+, \forall \omega_2 \in T^*$ s.t. $\omega_1 \mathrm{t_{f_i}} \omega_2 \in \Omega(\mathrm{T_f})$,
$CF(M_{\omega_1}, t_{f_i}) = CF(M, t_{f_i})$ and $Nw(M_{\omega_1}, t_{f_i}) = Nw(M, t_{f_i})$;

(iii) $\forall t_{f_i}, t_{f_j} \in T_f$ s.t. $\mathrm{t_{f_i} \neq t_{f_j}, CF(M, t_{f_i}) \cap CF(M, t_{f_j}) = \emptyset}$

Intuitively, condition (ii) states that the firing of any transition t_{f_i} of T_f will disable and enable the same sets of transitions, independently of the firing order (M_{ω_1} is the marking reached from M by ω_1). Condition (iii) means that each transition of

T_f has its own conflicting transitions in M. We denote $sc1(\beta, T_f)$ the conjunction of conditions (i), (ii) and (iii) above.

Theorem 4.4 *$sc1(\beta, T_f) \Rightarrow$ the domain of $\beta' = \bigcup_{\omega \in \Omega(T_f)} \widetilde{succ}(\beta, \omega)$ is convex and $\beta' = (M', F')$ where $\forall p \in P, M'(p) = M(p) + \sum_{t_{f_i} \in T_f} Post(p, t_{f_i}) - Pre(p, t_{f_i})$ and F' is computed as follows: Let $Old(M, T_f) = En(M) - \bigcup_{t_{f_i} \in T_f} CF(M, t_{f_i})$.*

(i) Set F' to[11]:

$$F \;\wedge \bigwedge_{t_{f_i} \in T_f} [\bigwedge_{t_j \in Old(M,T_f) \cup CF(M,t_{f_i})} t_{f_i} - t_j \leq 0 \;\wedge$$

$$\bigwedge_{t_k \in Nw(M,t_{f_i})} \downarrow Is(t_k) \leq t_k^{f_i} - t_{f_i} \leq \uparrow Is(t_k) \;\wedge \bigwedge_{t_{f_j} \in T_f, t_k \in Nw(M,t_{f_j})} t_{f_i} - t_k^{f_j} \leq 0]$$

(ii) Put F' in canonical form and eliminate all transitions of $\bigcup_{t_{f_i} \in T_f} CF(M, t_{f_i})$.

(iii) Rename each variable t_k^i in t_k and compute its equivalence class.

Proof. (sketch of proof) Let $FC(\beta, T_f)$ be the formula given in step (i). Since $FC(\beta, T_f)$ is a conjunction of atomic constraints (i.e.: its domain is convex), we have to show that: $\forall \omega = t_{f_1} t_{f_2} ... t_{f_n} \in \Omega(T_f)$, $FC(\beta, T_f) \wedge t_{f_1} \leq t_{f_2} \leq ... \leq t_{f_n}$ is equivalent to the firing condition of ω from β. We give here the proof for $n = 3$ (the proof is similar for $n \neq 3$). $FC(\beta, T_f) \wedge t_{f_1} \leq t_{f_2} \leq t_{f_3}$ is equivalent to:

$$F \;\wedge\; t_{f_1} \leq t_{f_2} \leq t_{f_3} \;\wedge \bigwedge_{t_j \in Old(M,T_f)+CF(M,t_{f_1})} t_{f_1} - t_j \leq 0 \;\wedge$$

$$\bigwedge_{t_j \in Old(M,T_f)+CF(M,t_{f_2})} t_{f_2} - t_j \leq 0 \;\wedge \bigwedge_{t_j \in Old(M,T_f)+CF(M,t_{f_3})} t_{f_3} - t_j \leq 0 \;\wedge$$

$$\bigwedge_{t_{f_i} \in T_f, t_k \in Nw(M,t_{f_i})} \downarrow Is(t_k) \leq t_k^{f_i} - t_{f_i} \leq \uparrow Is(t_k) \;\wedge$$

$$\bigwedge_{t_{f_i} \in T_f, t_k \in Nw(M,t_{f_1})} t_{f_i} - t_k^{f_1} \leq 0 \;\wedge \bigwedge_{t_{f_i} \in T_f, t_k \in Nw(M,t_{f_2})} t_{f_i} - t_k^{f_2} \leq 0 \;\wedge \bigwedge_{t_{f_i} \in T_f, t_k \in Nw(M,t_{f_3})} t_{f_i} - t_k^{f_3} \leq 0$$

Using $sc1(\beta, T_f)$, $t_{f_1} \leq t_{f_2} \leq t_{f_3}$, $En(M) = Old(M, T_f) + CF(M, t_{f_1}) + CF(M, t_{f_2}) + CF(M, t_{f_3})$, and $\forall t_{f_i} \in T_f, t_k \in Nw(M, t_{f_i}), t_{f_i} \leq t_k^{f_i}$, we can show that the above formula is equivalent to the firing condition of $t_{f_1} t_{f_2} t_{f_3}$ from β (see Section 3):

$$F \wedge \bigwedge_{t_j \in En(M)} t_{f_1} - t_j \leq 0 \wedge \bigwedge_{t_j \in En(M) - CF(M,t_1)} t_{f_2} - t_j \leq 0 \wedge \bigwedge_{t_j \in En(M) - (CF(M,t_1) + CF(M,t_2))} t_{f_3} - t_j \leq 0 \wedge$$

$$\bigwedge_{t_k \in Mw(M,t_{f_1})} t_{f_2} - t_k^{f_1} \leq 0 \;\wedge \bigwedge_{t_k \in Nw(M,t_{f_1})} t_{f_3} - t_k^{f_1} \leq 0 \;\wedge \bigwedge_{t_k \in Nw(M,t_{f_2})} t_{f_3} - t_k^{f_2} \leq 0 \;\wedge$$

$$\bigwedge_{t_{f_i} \in T_f, t_k \in Nw(M,t_{f_i})} \downarrow Is(t_k) \leq t_k^{f_i} - t_{f_i} \leq \uparrow Is(t_k)$$

□

[11] Variable $t_k^{f_i}$ is associated with the instance of transition t_k that is newly enabled by firing transition t_{f_i} from M.

Note that for any LTL_{-X} formula ϕ s.t. $|vis(\phi) \cap T_f| \leq 1$, condition $sc1(\beta, T_f)$ implies that $\wr T_f$ in β w.r.t. ϕ. We now derive from the previous condition another sufficient condition based on the structure of the net. Let $sc2(\beta, T_f)$ be the conjunction of conditions: (i) $\forall t_{f_i} \in T_f$, $succ(\beta, t_{f_i}) \neq \emptyset$ and (ii) $\forall t_{f_i}, t_{f_j} \in T_f$ s.t. $t_{f_i} \neq t_{f_j}, \forall t_k \in T, ({}^\circ t_{f_i} \cup t_{f_i}^\circ) \cap {}^\circ t_k \neq \emptyset \Rightarrow ({}^\circ t_{f_j} \cup t_{f_j}^\circ) \cap {}^\circ t_k = \emptyset$. Intuitively, condition (ii) means that there is no transition which shares input or output places with more than one transition of T_f.

Lemma 4.5 *$sc2(\beta, T_f) \Rightarrow$ the domain of $\beta' = \bigcup_{\omega \in \Omega(T_f)} \widetilde{succ}(\beta, \omega)$ is convex and β' is computed as shown in Theorem 4.4.*

Proof. The proof is immediate from the fact that $sc2(\beta, T_f)$ implies $sc1(\beta, T_f)$. □

5 Conclusion

We proposed an extension to the covering steps graph technique [13] more appropriate to time Petri nets. The basic idea of this extension is to group, into an atomic step, the firing of some set of transitions such that the union of states reached by their different interleavings is convex. We proved however that this union is not necessarily convex. We then established two sufficient conditions $sc1$ and $sc2$ which ensure convexity for the contracted state class graph [3]. Moreover, we showed how to compute this union without computing beforehand intermediate state classes.

In [1], the authors showed that the union of state zones [12] reached by different interleavings of the same set of transitions is convex, for a CCS-like parallel composition of timed automata (with no shared variables). According to condition $sc2$, this result is also valid for the CSCG of any CCS-like parallel composition of time Petri nets and a set of transitions belonging to different nets. Note that this result is however not valid for the SCG of a CCS-like parallel composition of time Petri nets. Indeed, consider the TPN shown in Fig. 1. From the initial state class $\alpha_0 = (p_1 + p_2, 1 \leq t_1 \leq 3 \ \wedge \ 2 \leq t_2 \leq 4)$, sequences $t_1 t_2$ and $t_2 t_1$ lead to two state classes $\alpha_1 = (p_3 + p_4, 0 \leq t_3 \leq 1 \wedge t_4 = 2 \wedge -2 \leq t_3 - t_4 \leq -1)$ and $\alpha_2 = (p_3 + p_4, t_3 = 1 \wedge 1 \leq t_4 \leq 2 \wedge -1 \leq t_3 - t_4 \leq 0)$ such that their union is not convex.

References

[1] R. Ben Salah, M. Bozga, O. Maler, *On Interleaving in Timed Automata*, CONCUR' 06, 465-476, volume 4137 of LNCS, 2006.

[2] B. Berthomieu, F. Vernadat, *State class constructions for branching analysis of Time Petri nets*, volume 2619 of LNCS, 2003.

[3] H. Boucheneb, H. Rakkay, *A more efficient time Petri net state space abstraction useful to model checking timed linear properties* In Proc of the 7th International Conference on Application of Concurrency to System Design (ACSD). IEEE Computer Society Press, 2007 (extended version accepted for publication in a special issue of Fundamenta Informaticae journal).

[12] A zone is a convex clock domain defined by a conjunction of atomic constraints on clocks.

[4] H. Boucheneb, R. Hadjidj, *CTL* model checking for Time Petri Nets*, Journal of Theoretical Computer Science TCS, volume 353/1-3, 2006.

[5] C. Daws, R. Gerth, B. Knaack, and R. Kuiper, *Partial order reduction techniques for real-time model checking*, Formal Aspects of Computing,(10), Springer, 1998.

[6] S. Edelkamp, S. Leue, A. Lluch-Lafuente *Partial order reduction and trail improvement in directed model checking*, International Journal of Software Tools Technology Transfer (2004)6, Springer-Verlag, 2004.

[7] G. Gardey, O. H. Roux, and O. F. Roux. *Using zone graph method for computing the state space of a Time Petri Net*, Springer-Verlag, volume 2791 of LNCS, 2004.

[8] P. Godefroid. *Partial Order Methods for the Verification of Concurrent Systems*, Springer-Verlag, volume 1032 of LNCS, 1996.

[9] D. Peled. *All from one, one for all: on model checking using representatives*, Springer-Verlag, volume 697 of LNCS, Springer-Verlag, 1993.

[10] D. Peled and T. Wilke. *Stutter invariant temporal properties are expressible without the next-time operator.* Information Processing Letters, 63(5), 1997.

[11] W. Penczek and A. Pólrola, *Specification and Model Checking of Temporal Properties in Time Petri Nets and Timed Automata*, In Proc. of ICATPN, Springer-Verlag, volume 3099 of LNCS, pages 37-76, Springer–Verlag, 2004.

[12] W. Penczek, A. Pólrola, *Abstraction and partial order reductions for checking branching properties of time Petri nets*, In Proc. of ICATPN, Springer-Verlag, volume 2075 of LNCS, pages 323-342, 2001.

[13] P.O.Ribet, F.Vernadat, B.Berthomieu, *On combining the persitent sets method with the covering steps graph method*, Springer-Verlag, volume 2529 of LNCS, 2002.

[14] A. Valmari. *A stubborn attack on state explosion*, Springer-Verlag, volume 531 of LNCS, 1990.

[15] F. Vernadat, P. Azéma, F. Michel, *Covering step graph.* In proc. of ATPN'96, Springer Verlag, volume 1091 of LNCS, 1996.

[16] D.Pradubsuwun, T.Yoneda, C. Myers, *Partial order reduction for detecting safety and timing failures of timed circuits*, IEICE Trans. Inf. & Syst., volume E88-D, No. 7, 2005.