

# On minimal elements of upward-closed sets <sup>★</sup>

Hsu-Chun Yen <sup>\*</sup>

*Dept. of Electrical Engineering, National Taiwan University,  
Dept. of Computer Science, Kainan University, Taiwan, R.O.C.*

Chien-Liang Chen

*Dept. of Electrical Engineering, National Taiwan University, Taiwan, R.O.C.*

---

## Abstract

*Upward-closed sets* of integer vectors enjoy the merit of having a finite number of *minimal elements*, which is behind the decidability of a number of Petri net related problems. In general, however, such a finite set of minimal elements may not be effectively computable. In this paper, we develop a unified strategy for computing the sizes of the minimal elements of certain upward-closed sets associated with Petri nets. Our approach can be regarded as a refinement of a previous work by Valk and Jantzen (in which a necessary and sufficient condition for effective computability of the set was given), in the sense that complexity bounds now become available provided that a bound can be placed on the size of a witness for a key query. The sizes of several upward-closed sets that arise in the theory of Petri nets as well as in backward-reachability analysis in automated verification are derived in this paper, improving upon previous decidability results shown in the literature.

*Key words:* Minimal element, Petri net, upward-closed set, vector addition system.

---

## 1. Introduction

A set  $U$  over  $k$ -dimensional vectors of natural numbers is called *upward-closed* (or *right-closed*) if  $\forall x \in U, y \geq x \implies y \in U$ . It is well known that an upward-closed set is completely characterized by its *minimal* elements, which always

---

<sup>\*</sup> A preliminary version of this work was presented at ICATPN 2007, the 28th International Conference on Applications and Theory of Petri Nets and Other Models of Concurrency.

<sup>\*</sup> Corresponding author; Partially supported by NSC Grant 92-2213-E-002-018.  
*Email address:* yen@cc.ee.ntu.edu.tw (Hsu-Chun Yen).

form a finite set. Aside from being of interest mathematically, evidence has suggested that upward-closed sets play a key role in a number of decidability results in automated verification of *infinite state systems*. In the analysis of Petri nets, the notion of upward-closed sets is closely related to the so-called *property of monotonicity* which serves as the foundation for many decision procedures for Petri net problems. What the monotonicity property says is that if a sequence  $\sigma$  of transitions of a Petri net is executable from a marking (i.e., configuration)  $\mu \in \mathbb{N}^k$ , then the same sequence is legitimate at any marking greater than or equal to  $\mu$ . That is, all the markings enabling  $\sigma$  form an upward-closed set.

In spite of the fact that the set of all the minimal elements of an upward-closed set is always finite, such a set may not be effectively computable in general. Given the importance of upward-closed sets, it is of interest theoretically and practically to be able to characterize the class of upward-closed sets for which their minimal elements are computable. Along this line of research, Valk and Jantzen ([8]) presented a sufficient and necessary condition under which the set of minimal elements of an upward-closed set is guaranteed to be effectively computable. Supposed  $U$  is an upward-closed set over  $\mathbb{N}^k$  and  $\omega$  is a symbol representing something being arbitrarily large. In [8], it was shown that the set of minimal elements of  $U$  is effectively computable iff the question ‘ $reg(v) \cap U \neq \emptyset$ ?’ is decidable for every  $v \in (\mathbb{N} \cup \{\omega\})^k$ , where  $reg(v) = \{x \mid x \in \mathbb{N}^k, x \leq v\}$ . Such a strategy has been successfully applied to showing computability of a number of upward-closed sets associated with Petri nets ([8]). Note, however, that [8] reveals no complexity bounds for the sizes of the minimal elements. As knowing the size of minimal elements might turn out to be handy in many cases, the following question arises naturally. If more is known about the query ‘ $reg(v) \cap U \neq \emptyset$ ?’ (other than just being decidable), could the size of the minimal elements be measured? In fact, answering the question in the affirmative is the main contribution of this work.

Given a vector  $v \in (\mathbb{N} \cup \omega)^k$ , suppose  $\|v\|$  is defined to be the maximum component (excluding  $\omega$ ) in  $v$ . We demonstrate that for every  $v$ , if a bound on the size of a witness for  $reg(v) \cap U \neq \emptyset$ ? (if one exists) is available, then such a bound can be applied inductively to obtain a bound for *all* the minimal elements of  $U$ . In a recent article [9], such a strategy was first used for characterizing the solution space of a restricted class of *parametric timed automata*. In this paper, we move a step further by formulating a general strategy as well as applying our unified framework to a wide variety of Petri net problems with upward-closed solution sets.

Given a  $k$ -place  $m$ -transition Petri net  $\mathcal{P}$  with its transition set  $T = \{t_1, \dots, t_m\}$ , an  $d \times m$  integer matrix  $A$ , and an  $d \times 1$  integer column vector  $b$ , consider the set

$$\mathbb{S} = \{\mu \mid \mu \xrightarrow{\sigma_0} \mu_1 \xrightarrow{\sigma_1} \mu_2, \mu_2 \geq \mu_1; A \times \#\sigma_1 \geq b\}$$

where  $\mu_1, \mu_2 \in \mathbb{N}^k$ ,  $\sigma_1 \in T^*$ ,  $\sigma_2 \in T^+$ , and  $\#\sigma_1 (\in \mathbb{N}^m)$  is a vector whose  $i$ -th coordinate represents the number of times transition  $t_i$  appears in  $\sigma_1$ . What  $\mathcal{S}$  means is that it consists of all the markings  $\mu$  from which a "repeatable" path  $\mu_1 \xrightarrow{\sigma_1} \mu_2$  can be reached such that the transition count along  $\sigma_1$  meets a system of linear constraints  $A \times \#\sigma_1 \geq b$ . Following the monotonic property of Petri nets,  $\mathcal{S}$  is clearly upward-closed. In this paper, we first apply the inductive strategy developed by Rackoff in [6] (for deriving complexities of the boundedness and covering problems for vector addition systems) to obtain a bound for the minimal elements of  $\mathcal{S}$ . We then show the solutions to a wide variety of Petri net problems found in the literature to be characterizable by paths of form defined in  $\mathcal{S}$ , and therefore, a bound for the minimal elements of  $\mathcal{S}$  immediately yields bounds for the minimal elements of upward-closed sets associated with those problems.

In addition to those upward-closed sets investigated in [8] for general Petri nets, we illustrate the usefulness of our approach in performing *backward-reachability* analysis, which is a useful technique in automated verification. We show that for certain classes of Petri nets and state set  $Q$ , the backward-reachability set of  $Q$  is not only upward-closed but falls into the category to which our unified approach can be applied. Such Petri nets include several well known subclasses for which reachability is characterizable by *integer linear programming*. Our analysis can also be applied to the model of *lossy* vector addition systems with states (VASSs) [3] to derive bounds for the backward-reachability sets. For (conventional or lossy) VASSs, we further enhance the work of [3] by providing complexity bounds for the so-called *global model checking problem* with respect to a certain class of formulas. (In [3], such a problem was only shown to be decidable, yet no complexity was available there.) Upward-closed sets associated with a kind of *parametric clocked Petri nets* are also investigated in this paper, serving as yet another application of our unified approach.

## 2. Preliminaries

Let  $\mathbb{Z}$  ( $\mathbb{N}$ , resp.) be the set of all integers (nonnegative integers, resp.), and  $\mathbb{Z}^k$  ( $\mathbb{N}^k$ , resp.) be the set of  $k$ -dimensional vectors of integers (nonnegative integers, resp.). We define the *max-value* of  $v$ , denoted by  $\|v\|$ , to be  $\max\{|v(i)| \mid 1 \leq i \leq k\}$ , i.e., the absolute value of the largest component in  $v$ . For a set of vectors  $V = \{v_1, \dots, v_m\}$ , the *max-value* of  $V$  (also written as  $\|V\|$ ) is defined to be  $\max\{\|v_i\| \mid 1 \leq i \leq m\}$ . In our subsequent discussion, we let  $\mathbb{N}_\omega = \mathbb{N} \cup \{\omega\}$  ( $\omega$  is a new element capturing the notion of something being 'arbitrarily

large')<sup>1</sup>. We also let  $\mathbb{N}_\omega^k = (\mathbb{N} \cup \{\omega\})^k = \{(v_1, \dots, v_k) \mid v_i \in (\mathbb{N} \cup \{\omega\}), 1 \leq i \leq k\}$ . For a  $v \in \mathbb{N}_\omega^k$ , we also write  $\|v\|$  to denote  $\max\{v(i) \mid v(i) \neq \omega\}$  (i.e., the largest component in  $v$  excluding  $\omega$ ) if  $v \neq (\omega, \dots, \omega)$ ;  $\|(\omega, \dots, \omega)\| = 1$ . For an element  $v \in \mathbb{N}_\omega^k$ , let  $\text{reg}(v) = \{w \in \mathbb{N}^k \mid w \leq v\}$ .

A set  $U(\subseteq \mathbb{N}^k)$  is called *upward-closed* (or *right-closed* in some literature) if  $\forall x \in U, \forall y, y \geq x \implies y \in U$ . An element  $x (\in U)$  is said to be *minimal* if there is no  $y (\neq x) \in U$  such that  $y < x$ . We write  $\text{min}(U)$  to denote the set of minimal elements of  $U$ . From Dicksons lemma, it is well-known that for each upward-closed set  $U(\subseteq \mathbb{N}^k)$ ,  $\text{min}(U)$  is finite. Even so,  $\text{min}(U)$  might not be effectively computable in general. Given a function  $f$ , we write the  $k$ -fold

composition of  $f$  as  $f^{(k)}$  (i.e.,  $f^{(k)}(x) = \overbrace{f \circ \dots \circ f}^k(x)$ ).

A *Petri net* (PN, for short) is a 3-tuple  $\mathcal{P} = (P, T, \varphi)$ , where  $P$  is a finite set of *places*,  $T$  is a finite set of *transitions*, and  $\varphi$  is a *flow function*  $\varphi : (P \times T) \cup (T \times P) \rightarrow \mathbb{N}$ . Let  $k$  and  $m$  denote  $|P|$  (the number of places) and  $|T|$  (the number of transitions), respectively. The  $k$  is also called the *dimension* of the PN. A *marking* is a mapping  $\mu : P \rightarrow \mathbb{N}$ . The *transition vector* of a transition  $t$ , denoted by  $\bar{t}$ , is a  $k$ -dimensional column vector in  $\mathbb{Z}^k$ , such that  $\bar{t}(i) = \varphi(t, p_i) - \varphi(p_i, t)$ , and the set of transition vectors, denoted by  $\bar{T}$ , to be  $\{\bar{t} \mid t \in T\}$ . For a sequence of transition  $\sigma = t_1 t_2 \dots t_j$ , we define  $\Delta(\sigma) = \sum_{i=1}^j \bar{t}_i (\in \mathbb{Z}^k)$ , i.e., a vector corresponding to the changes of place values if  $\sigma$  is executed.

A transition  $t \in T$  is *enabled* at a marking  $\mu$  iff  $\forall p \in P, \varphi(p, t) \leq \mu(p)$ . If a transition  $t$  is enabled, it may *fire* and yields marking  $\mu'$  (written as  $\mu \xrightarrow{t} \mu'$ ) with  $\mu'(p) = \mu(p) - \varphi(p, t) + \varphi(t, p), \forall p \in P$ . By establishing an ordering on the elements of  $P$  and  $T$  (i.e.,  $P = \{p_1, \dots, p_k\}$  and  $T = \{r_1, \dots, r_m\}$ ), we can view a marking  $\mu$  as a  $k$ -dimensional column vector with its  $i$ -th component being  $\mu(p_i)$ , and  $\#_\sigma$  as an  $m$ -dimensional column vector with its  $j$ th entry denoting the number of occurrences of transition  $r_j$  in  $\sigma$ . The *reachability set* of  $\mathcal{P}$  with respect to  $\mu_0$  is the set  $R(\mathcal{P}, \mu_0) = \{\mu \mid \exists \sigma \in T^*, \mu_0 \xrightarrow{\sigma} \mu\}$ .  $F(\mathcal{P}, \mu_0) (= \{\sigma \in T^* \mid \mu_0 \xrightarrow{\sigma}\})$  denotes the set of all fireable sequences of transitions in PN  $(\mathcal{P}, \mu_0)$ . Given a  $\sigma \in T^\omega$ ,  $\text{In}(\sigma)$  denotes the set of all elements in  $T$  that occur infinitely many times in  $\sigma$ .

A *k-dimensional vector addition system with states* (VASSs) is a 5-tuple  $(v_0, V, s_1, S, \delta)$ , where  $v_0 \in \mathbb{N}^k$  is called the *start vector*,  $V (\subseteq \mathbb{Z}^k)$  is called the set of *addition rules*,  $S$  is a finite set of *states*,  $\delta (\subseteq S \times S \times V)$  is the transition relation, and  $s_1 (\in S)$  is the *initial state*. Elements  $(p, q, v)$  of  $\delta$  are called *transitions* and are usually written as  $p \rightarrow (q, v)$ . A configuration of a VASS is a pair

<sup>1</sup> We assume the following arithmetics for  $\omega$ : (1)  $\forall n \in \mathbb{N}, n < \omega$ , (2)  $\forall n \in \mathbb{N}_\omega, n + \omega = \omega - n = \omega, (n + 1) \times \omega = \omega, 0 \times \omega = \omega \times 0 = 0$ .

$(p, x)$  where  $p \in S$  and  $x \in \mathbb{N}^k$ . The transition  $p \rightarrow (q, v)$  can be applied to the configuration  $(p, x)$  and yields the configuration  $(q, x + v)$ , provided that  $x + v \geq \mathbf{0}$ .

### 3. A strategy for computing the sizes of minimal elements

In an article [8] by Valk and Jantzen, the following result was proven which suggests a sufficient and necessary condition under which the set of minimal elements of an upward-closed set is effectively computable:

**Theorem 1.** ([8]) *For each upward-closed set  $K(\subseteq \mathbb{N}^k)$ ,  $\min(K)$  is effectively computable iff for every  $v \in \mathbb{N}_\omega^k$ , the problem ‘ $\text{reg}(v) \cap K \neq \emptyset$ ?’ is decidable. (Recall that  $\text{reg}(v) = \{w \in \mathbb{N}^k \mid w \leq v\}$ .)*

What follows can be thought of as a refinement of Theorem 1.

**Theorem 2.** *Given an upward-closed set  $U(\subseteq \mathbb{N}^k)$ , if for every  $v \in \mathbb{N}_\omega^k$ , a witness  $\hat{w} \in \mathbb{N}^k$  for ‘ $\text{reg}(v) \cap U \neq \emptyset$ ’ (if one exists) can be computed with*

- (i)  $\|\hat{w}\| \leq b$ , for some  $b \in \mathbb{N}$  when  $v = (\omega, \dots, \omega)$ ,
- (ii)  $\|\hat{w}\| \leq f(\|v\|)$  when  $v \neq (\omega, \dots, \omega)$ , for some monotone function  $f$ ,

then  $\|\min(U)\| \leq f^{(k-1)}(b)$ .

**PROOF.** Given an arbitrary  $h, 1 \leq h \leq k$ , we show inductively that for each  $m \in \min(U)$ , there exist  $h$  indices  $i_{m_1}, \dots, i_{m_h}$  such that  $\forall l, 1 \leq l \leq h$ ,  $m(i_{m_l}) \leq f^{(h-1)}(b)$ .

- (*Induction Basis*) Consider the case when  $h = 1$ . We begin with  $v_0 = (\omega, \dots, \omega)$ . Assume that  $w_0$  is a witness for  $\text{reg}(v_0) \cap U \neq \emptyset$ , which, according to the assumption of the theorem, satisfies  $\|w_0\| \leq b = f^{(0)}(b)$ . Let  $\min_1(U) = \min(U) \setminus \text{reg}((b, \dots, b))$ , i.e., those in  $\min(U)$  that have at least one component larger than  $b$ . If  $\min_1(U) = \emptyset$ , then the theorem follows since  $f^{(0)}(b)$  becomes a bound for  $\|\min(U)\|$ . Otherwise,  $\forall m \in \min_1(U)$ , it must be the case that  $\exists i, 1 \leq i \leq k, m(i) < b$ ; otherwise,  $m$  would not have been minimal since  $w_0 \leq (b, \dots, b)$ . Hence, the assertion holds for  $h = 1$ , i.e.,  $f^{(0)}(b)$  is a bound for at least one component for all the elements in  $\min(U)$ .

See Figure 1.

- (*Induction Step*) Assume that the assertion holds for  $h (< k)$ , we now show the case for  $h + 1$ . Consider  $\min_h(U) = \min(U) \setminus \bigcup_{v \in \mathbb{N}^k, \|v\| \leq f^{(h-1)}(b)} \{\text{reg}(v)\}$ , i.e., the set of minimal elements that have at least one coordinate exceeding  $f^{(h-1)}(b)$ . If  $\min_h(U) = \emptyset$ , the assertion holds; otherwise, take an arbitrary  $m \in \min_h(U)$ , and let  $i_{m_1}, \dots, i_{m_h}$  be the indices of those components satisfying

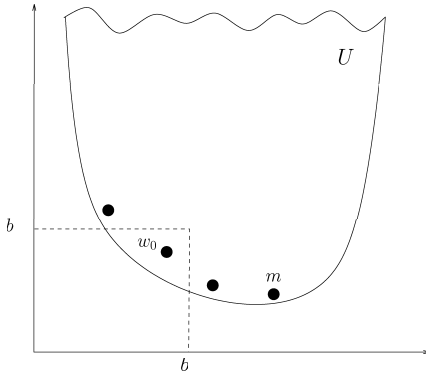


Fig. 1. Induction Basis.

the assertion, i.e.,  $\forall 1 \leq j \leq h, m(i_{m_j}) \leq f^{(h-1)}(b)$ . Let  $v_h^m$  be such that  $v_h^m(l) = m(i_{m_j})$ , if  $l = i_{m_j}$ ;  $=\omega$  otherwise. That is,  $v_h^m$  agrees with  $m$  on coordinates  $i_{m_1}, \dots, i_{m_h}$ , and carries the value  $\omega$  for the remaining coordinates. Notice that  $\|v_h^m\| \leq f^{(h-1)}(b)$ . According to the assumption of the theorem, a witness  $w_h^m$  for  $\text{reg}(v_h^m) \cap U \neq \emptyset$  with  $\|w_h^m\|$  bounded by  $f(\|v_h^m\|)$  ( $\leq f(f^{(h-1)}(b))$ ) can be obtained. Furthermore,  $w_h^m(i_{m_j}) \leq m(i_{m_j})$ ,  $1 \leq j \leq h$ . (Notice that  $m \in \text{min}_h(U)$  implies the existence of such a witness.) It must be the case that there exists an index  $i_{m_{h+1}} (\notin \{i_{m_1}, \dots, i_{m_h}\})$  such that  $m(i_{m_{h+1}}) \leq w_h^m(i_{m_{h+1}})$  ( $\leq f(f^{(h-1)}(b)) = f^{(h)}(b)$ ), since otherwise,  $w_h^m < m$  – contradicting that  $m$  being minimal. The induction step is therefore proven. ■

## 4. Some applications

### 4.1. Petri nets

Given a  $k$ -place  $m$ -transition PN  $(P, T, \varphi)$ , an  $d \times m$  integer matrix  $A$ , and an  $d \times 1$  integer column vector  $b$ , consider the set

$$\mathbb{S} = \{\mu \mid \mu \xrightarrow{\sigma_0} \mu_1 \xrightarrow{\sigma_1} \mu_2, \mu_2 \geq \mu_1; A \times \#\sigma_1 \geq b\}$$

where  $\mu_1, \mu_2 \in \mathbb{N}^k$ , and  $\sigma_1 \in T^*$ ,  $\sigma_2 \in T^+$ . (Here  $A \times \#\sigma_1 \geq b$  represents a system of  $d$  inequalities with their variables corresponding to the frequency counts of the  $m$  transitions along the path  $\sigma_1$ .) Clearly the set  $\mathbb{S}$  is an upward-closed set. In what follows, we first use Theorem 2 to find a bound for the sizes of the minimal elements of  $\mathbb{S}$ . We then show a wide variety of PN problems reported in the literature to be characterizable by the above set  $\mathbb{S}$  as special cases, which in turn yields upper bounds for the sizes of their minimal elements.

Our analysis makes use of the inductive strategy developed by Rackoff in [6], in which the complexities of the boundedness and covering problems for vector addition systems (equivalently, PNs) were developed. Intuitively speaking, Rackoff's strategy relies on showing that if a path exhibiting unboundedness or coverability exists, then there is a 'short' witness. Before going into details, we require the following definitions, most of which can be found in [6].

A *generalized marking* is a mapping  $\mu : P \rightarrow \mathbb{Z}$  (i.e., negative coordinates are allowed). A  $w \in \mathbb{Z}^k$  is called *i-bounded* (resp., *i-r bounded*) if  $0 \leq w(j), \forall 1 \leq j \leq i$  (resp.  $0 \leq w(j) \leq r, \forall 1 \leq j \leq i$ ). Given a  $k$ -place PN  $\mathcal{P} = (P, T, \varphi)$ , suppose  $p = w_1 w_2 \cdots w_l$  ( $l > 1$ ) is a sequence of vectors (generalized markings) in  $\mathbb{Z}^k$  such that  $\forall j, 1 \leq j < l, z_{j+1} - z_j \in T$  (the set of transition vectors). Sequence  $p$  is said to be

- *i-bounded* (resp., *i-r bounded*) if every member of  $p$  is *i-bounded* (resp., *i-r bounded*).
- *self-covering* if there is a  $j, 1 \leq j < l$  such that  $w_j \leq w_l$ .
- an *i-loop* if  $w_l(j) = w_1(j), \forall 1 \leq j \leq i$ . The *i-loop* is called *simple* if it does not contain any *i-loop* as its proper subsequence.  $w_l - w_1 \in \mathbb{Z}^k$  is called the *loop value* of the *i-loop*.

With respect to matrices  $[A]_{d \times m}$  and  $[b]_{d \times 1}$ , let  $s(i, \mu, A, b)$  be the length of the shortest *i-bounded* path  $\mu \xrightarrow{\sigma_0} \mu_1 \xrightarrow{\sigma_1} \mu_2$  (for some  $\sigma_0 \in T^*$  and  $\sigma_1 \in T^+$ ), such that  $\mu_2 \geq \mu_1$  and  $A \times \#_{\sigma_1} \geq b$ , i.e., a self-covering path with the transition count vector  $\#_{\sigma_1}$  satisfying  $A \times \#_{\sigma_1} \geq b$ . For convenience, we call such a path "self-covering  $(A, b)$ -path". If no such paths exist, then  $s(i, \mu, A, b) = 0$ . We define  $h(i, A, b) = \max\{s(i, \mu, A, b) \mid \mu \in \mathbb{Z}^k\}$ . In what follows, we argue that  $h(i, A, b) \in \mathbb{N}$ . To see this, first note that the function  $s$  is *monotonic* with respect to  $\mu$  in the sense that if an *i-bounded* self-covering  $(A, b)$ -path  $p$  exists for a marking  $\mu$ , then  $p$  is guaranteed to be an *i-bounded* self-covering  $(A, b)$ -path with respect to  $\mu + \Delta$ , for any  $\Delta \geq 0$ . This implies  $s(i, \mu + \Delta, A, b) \leq s(i, \mu, A, b)$ , for any  $\Delta \geq 0$ . As a result, if we let  $E(i, A, b) = \{\mu \mid s(i, \mu, A, b) > 0\}$ , i.e., the set of all generalized markings from which *i-bounded* self-covering  $(A, b)$ -paths exist, then  $E(i, A, b)$  is upward-closed. Let  $E'(i, A, b)$  be the set of minimal elements of  $E(i, A, b)$ . Then  $h(i, A, b) = \max\{s(i, \mu, A, b) \mid \mu \in \mathbb{Z}^k\} = \max\{s(i, \mu, A, b) \mid \mu \in E'(i, A, b)\}$  is finite, which does not depend on the starting marking.

Before deriving our result, we need the following concerning the size of the solutions of *integer linear programming* (ILP) instances.

**Lemma 3.** (From [4]) *Let  $d_1, d_2 \in \mathbb{N}^+$ , let  $B$  be a  $d_1 \times d_2$  integer matrix and let  $h$  be a  $d_1 \times 1$  integer matrix. Let  $e \geq d_2$  be an upper bound on the absolute values the integers in  $B$  and  $h$ . If there exists a vector  $v \in \mathbb{N}^{d_2}$  which is a solution to  $Bv \geq h$ , then for some constant  $c$  independent of  $e, d_1, d_2$ , there*

exists a vector  $v$  such that  $Bv \geq h$  and  $\|v\| \leq e^{cd_1}$ .

The following lemma bounds the length of the shortest  $i$ - $r$  bounded self-covering  $(A, b)$ -path in a  $k$ -place  $m$ -transition PN  $\mathcal{P}=(P, T, \varphi)$ . In the remainder of this section, we let  $n=\max\{d, k, m, \|T\|, \|A\|, \|b\|\}$ , where  $A$  is of dimension  $d \times m$ .

**Lemma 4.** *If there is an  $i$ - $r$  bounded self-covering  $(A, b)$ -path in PN  $\mathcal{P}$  with initial marking  $\mu$ , then there exists such a path of length  $\leq r^{nc}$ , for some constant  $c$  independent of  $r$  and  $n$ .*

**PROOF.** The proof is similar to (but more involved) than the corresponding one in [6]. For the sake of completeness, a proof sketch is given below.

Let  $\mu \xrightarrow{\sigma_0} \mu_1 \xrightarrow{\sigma_1} \mu_2$  be an  $i$ - $r$ -bounded self-covering  $(A, b)$ -path. First note that  $\mu \xrightarrow{\sigma_0} \mu_1$  need not be longer than  $r^k$ ; otherwise, there must exist an  $i$  loop which can be removed without affecting the requirement of being a self-covering  $(A, b)$ -path. (Recall that the condition  $A \times \#_{\sigma_1} \geq b$  is independent of the prefix  $\sigma_0$ .) We now decompose  $\mu_1 \xrightarrow{\sigma_1} \mu_2$  into a possibly shorter path  $\mu_1 \xrightarrow{\sigma'} \mu_2$  and a multiset of simple  $i$ -loops  $\{Q_1, Q_2, \dots, Q_j\}$  (for some  $j$ ) such that

- the length of  $\mu_1 \xrightarrow{\sigma'} \mu_2$  is  $\leq (r^k + 1)^2$ ,
- the length of each  $Q_i$  is  $\leq r^k$ ,
- each coordinate of the loop value of  $Q_i$  ( $1 \leq i \leq j$ ) has its absolute value  $\leq n * r^k$ ,
- the number of distinct  $m$ -dimensional vectors  $\#_{Q_1}, \#_{Q_2}, \dots, \#_{Q_j}$  is  $\leq (r^k + 1)^m$ .

The reason that such a decomposition exists can be found in [6]. Note that the total number of distinct loop values is  $\leq (r^k + 1)^m$ , as the same vector count yields the same loop value.

Let  $v_1, \dots, v_g$  ( $g \leq ((r^k + 1)^m)$ ) be the distinct vectors of transition counts of those simple  $i$ -loops, and let  $l_1, \dots, l_g$  be the respective loop values. Recall that each of  $v_i, 1 \leq i \leq g$ , is an  $m \times 1$  column vector. Now the path  $\mu_1 \xrightarrow{\sigma_1} \mu_2$  can be characterized by the following system of linear inequalities:

$$\begin{cases} \Delta(\sigma') + a_1 * l_1 + \dots + a_g * l_g \geq 0 & \text{--- (1)} \\ A \times (\#_{\sigma'} + a_1 * v_1 + \dots + a_g * v_g) \geq b & \text{--- (2)} \end{cases}$$

where  $a_i, 1 \leq i \leq g$ , corresponds to the number of times that simple  $i$ -loops with vector count  $v_i$  occurs.

(1) and (2) together can be regarded as a system of  $k+d$  inequalities with  $g$  unknown variables and the max-value of the system is bounded by  $n * (r^k + 1)^2$  (corresponding to the maximum increase/decrease of tokens in a place w.r.t. the firing of  $\sigma'$ ). Note that  $r^{3n^2} \geq \max\{n * (r^k + 1)^2, (r^k + 1)^m\}$ . By letting  $d_1 = k + d$  and  $e = r^{3n^2}$  and according to Lemma 4, there exists a solution  $u \in \mathbb{N}^g$  such that  $\|u\| \leq (r^{3n^2})^{c'(k+d)}$ , for some constant  $c'$ . As a result, there exists a "short"  $i$ - $r$  bounded self-covering  $(A,b)$ -path whose length is no more than  $r^{n^c}$ , for some constant  $c$  independent of  $r$  and  $n$ . ■

We are now ready to bound the max-value of the minimal elements of the set  $\mathbb{S} = \{\mu \mid \mu \in \mathbb{N}^k, \mu \xrightarrow{\sigma_0} \mu_1 \xrightarrow{\sigma_1} \mu_2, \mu_2 \geq \mu_1, A \times \#\sigma_1 \geq b\}$ .

**Lemma 5.** *Given PN  $\mathcal{P}$  and a  $z \in \mathbb{N}_\omega^k$ ,  $\text{reg}(z) \cap \mathbb{S} \neq \emptyset$  iff there is a witness  $z'$  with  $\|z'\| \leq n^{2^{c_1 \times k \times \log k}}$ . where  $c_1$  is a constant. (Note that the bound is independent of  $z$ .)*

## PROOF.

Recall that  $h(i, A, b) = \max\{s(i, \mu, A, b) \mid \mu \in \mathbb{Z}^k\}$ , where  $s(i, \mu, A, b)$  is the length of the shortest  $i$ -bounded self-covering  $(A, b)$ -path from  $\mu$ . We first show  $h(0, A, b) \leq 2^{n^c}$  and  $h(i + 1) \leq (n \times h(i))^{i+1} + h(i)$ , for  $1 \leq i < k$ .

$h(0, A, b) \leq 2^{n^c}$  can be proven along the same line as Lemma 4.6 of [6]. To show  $h(i + 1) \leq (n \times h(i))^{i+1} + h(i)$ , consider any  $(i + 1)$ -bounded self-covering  $(A, b)$ -path  $p : v_1 \cdots v_r$ . We have two cases:

- Case 1: Path  $p$  is  $(i + 1) - (n \times h(i))$ -bounded. Then according to Lemma 4, there exists a short one with length  $\leq (n \times h(i))^{n^c}$ .
- Case 2: Otherwise, let  $v_g$  be the first vector along  $p$  that is not  $(n \times h(i))$  bounded. By chopping off  $(i + 1)$ -loops, the prefix  $v_1 \dots v_g$  can be shortened if necessary to make the length  $\leq (n \times h(i))^{i+1}$ . Let  $p'$  the shortened prefix path. With no loss of generality, we assume the  $(i + 1)$ st position to be the coordinate whose value exceeds  $n \times h(i)$  at  $v_g$ . Recalling the definition of  $h(i, A, b)$ , there is an  $i$ -bounded self-covering  $(A, b)$ -path, say  $l$ , of length  $\leq h(i, A, b)$  from  $v_g$ . By appending  $l$  to the shortened prefix  $p'$  (i.e., replacing the original suffix path  $v_g \dots v_r$  by  $l$ ), the new path is an  $(i + 1)$ -bounded self-covering  $(A, b)$ -path, because the value of the  $(i + 1)$ st coordinate exceeds  $n \times h(i)$  and the path  $l$  (of length bounded by  $\leq h(i)$ ) can at most subtract  $n \times h(i)$  from coordinate  $i + 1$ , since the application of a PN transition can subtract at most  $n$  from a given coordinate. Note that the length of the new path is bounded by  $(n \times h(i))^{i+1} + h(i)$ .

By solving the recurrence relation  $h(0, A, b) \leq 2^{n^c}$  and  $h(i + 1, A, b) \leq (n \times$

$h(i)^{i+1} + h(i)$ , for  $1 \leq i < k$ , we have  $h(k, A, b) \leq 2^{n^{c_*} * 2^k * \log k} \leq 2^{2^{c_*} * k \log n}$ , for some constant  $c'$ . What this bound means is that regardless of the initial vector, if a self-covering  $(A, b)$ -path exists, then there is a short one whose length is bounded by  $2^{2^{c_*} * k \log n}$ . Since a path of length  $\leq 2^{2^{c_*} * k \log n}$  can at most subtract  $\|\bar{T}\| \times 2^{2^{c_*} * k \log n}$  from any component,  $\|z'\|$  is therefore bounded by  $n * 2^{2^{c_*} * k \log n} \leq 2^{2^{c_1} * k \log n}$ , for some constant  $c_1$ . ■

**Theorem 6.**  $\| \min(\mathbb{S}) \| \leq 2^{2^{c_1} * k * \log n}$ , where  $c_1$  is a constant.

**PROOF.** Given a  $z \in \mathbb{N}_\omega^k$ , define  $f(\|z\|) = 2^{2^{c_1} * k * \log n}$  (where  $c_1$  a constant stated in Lemma 5), which provides an upper bound for a witness certifying  $\text{reg}(z) \cap \min(\mathbb{S}) \neq \emptyset$ , if one exists. Notice that the value of  $f$  is independent of  $z$ . Our result follows immediately from Theorem 2. ■

In what follows, we show that a wide variety of PN problems studied in the literature are actually special cases of finding paths satisfying  $\mu \xrightarrow{\sigma_0} \mu_1 \xrightarrow{\sigma_1} \mu_2$ ;  $\mu_2 \geq \mu_1$ ;  $A \times \#_{\sigma_1} \geq b$ , for some matrices  $A$  and  $b$ . As a result, Theorem 6 can immediately be applied to deriving the max-value of the minimal elements of the upward-closed sets associated with those PN problems.

We first examine some upward-closed sets defined and discussed in [8]. Some definitions from [8] are recalled first. Given a PN  $(P, T, \varphi)$ , a vector  $\mu \in \mathbb{N}^k$  is said to be

- $\hat{T}$ -blocked, for  $\hat{T} \subseteq T$ , if  $\forall \mu' \in R(\mathcal{P}, \mu)$ ,  $\neg(\exists t \in \hat{T}, \mu' \xrightarrow{t})$ . For the case when  $\hat{T} = T$ ,  $\mu$  is said to be a *total deadlock*.
- *dead* if  $F(\mathcal{P}, \mu)$  is finite.
- *bounded* if  $R(\mathcal{P}, \mu)$  is finite; otherwise, it is called *unbounded*.
- $\hat{T}$ -continual, for  $\hat{T} \subseteq T$ , if there exists a  $\sigma \in T^\omega$ ,  $\mu \xrightarrow{\sigma}$  and  $\hat{T} \subseteq \text{In}(\sigma)$ .

Consider the following four sets defined in [8]:

- $\text{NOTBLOCKED}(\hat{T}) = \{\mu \in \mathbb{N}^k \mid \mu \text{ is not } \hat{T}\text{-blocked}\}$ .
- $\text{NOTDEAD} = \{\mu \in \mathbb{N}^k \mid \mu \text{ is not } \text{dead}\}$ .
- $\text{UNBOUNDED} = \{\mu \in \mathbb{N}^k \mid \mu \text{ is } \text{unbounded}\}$ .
- $\text{CONTINUAL}(\hat{T}) = \{\mu \in \mathbb{N}^k \mid \mu \text{ is } \hat{T}\text{-continual}\}$ .

It has been shown in [8] that for each of the above four upward-closed sets, the ‘ $\text{reg}(v) \cap K \neq \emptyset$ ?’ query of Theorem 1 is decidable; as a consequence, the set of minimal elements is effectively computable. We now show how to use Theorem 6 to estimate the bound of the minimal elements for each of the four sets.

- $\text{NOTBLOCKED}(\hat{T})$ :

Consider a PN  $\mathcal{P}' = (P', T' \varphi')$  derived from  $\mathcal{P}$  such that  $P' = P \cup \{p'\}$ ,  $T' = T \cup$

$\{t'\}$ ,  $(\varphi'(p, t) = \varphi(p, t), \varphi'(t, p) = \varphi(t, p), \forall p \in P, t \in T)$ ,  $(\varphi(t, p') = 1, \forall t \in \hat{T})$ , and  $\varphi(t', p) = \varphi(p, t') = 1$ . Note that  $p'$  and  $t'$  form a self-loop that can be fired repeatedly, provided that  $p'$  is not empty. It is not difficult to see that  $NOTBLOCKED(\hat{T}) = \{\mu \mid \mu \xrightarrow{\sigma_0} \mu_1 \xrightarrow{\sigma_1} \mu_2, \mu_2 \geq \mu_1, \sigma_0 \in (T')^*, \sigma_1 = t'\}$ .

• *NOTDEAD*:

It is easy to see that  $NOTDEAD = \{\mu \mid \mu \xrightarrow{\sigma_0} \mu_1 \xrightarrow{\sigma_1} \mu_2, \mu_2 \geq \mu_1, \sigma_0 \in T^*, \sigma_1 \in T^+\}$ .

• *UNBOUNDED*:

Consider a PN  $\mathcal{P}' = (P', T' \varphi')$  derived from  $\mathcal{P}$  such that  $P' = P \cup \{p'\}$ ,  $T' = T \cup \{t'\} \cup \{t_p \mid p \in P\}$ ,  $(\varphi'(p, t) = \varphi(p, t), \varphi'(t, p) = \varphi(t, p), \forall p \in P, t \in T)$ ,  $(\varphi(p, t_p) = \varphi(t_p, p') = 1, \forall p \in P)$ , and  $\varphi(p', t') = 1$ . Clearly  $UNBOUNDED = \{\mu \mid \mu \xrightarrow{\sigma_0} \mu_1 \xrightarrow{\sigma_1} \mu_2, \mu_2 \geq \mu_1, \sigma_0 \in (T')^*, \#\sigma_1(t') > 0\}$ .

• *CONTINUAL*( $\hat{T}$ ):

It is easy to see that  $CONTINUAL(\hat{T}) = \{\mu \mid \mu \xrightarrow{\sigma_0} \mu_1 \xrightarrow{\sigma_1} \mu_2, \mu_2 \geq \mu_1, \sigma_0 \in T^*, \#\sigma_1(t) > 0, \forall t \in \hat{T}\}$ .

We now consider a number of fairness-related problems defined in [8] (see Definition 6.9 of [8]), and see how they fall into our general framework discussed above.

Let  $\mathcal{A}$  be a finite set of nonempty subsets of transitions. Given an infinite sequence of transitions  $\sigma = t_1, t_2, \dots$ , let  $inf^{I'}(\sigma)$  be the set of transitions occurring infinitely often in  $\sigma$ . Consider the following 6 types of fairness notions [8]. The  $\sigma$  is said to be

- *T1-fair* iff  $\exists A \in \mathcal{A}, \exists i \geq 1, t_i \in A$
- *T1'-fair* iff  $\exists A \in \mathcal{A}, \forall i \geq 1, t_i \in A$
- *T2-fair* iff  $\exists A \in \mathcal{A}, inf^T(\sigma) \cap A \neq \emptyset$
- *T2'-fair* iff  $\exists A \in \mathcal{A}, inf^{I'}(\sigma) \subset A$
- *T3-fair* iff  $\exists A \in \mathcal{A}, inf^T(\sigma) = A$
- *T3'-fair* iff  $\exists A \in \mathcal{A}, A \subseteq inf^{I'}(\sigma)$

The *fair nontermination problem* (fair NTP, for short) with respect to *T1* (*T1'*, *T2*, *T2'*, *T3*, *T3'*, respectively) fairness is the problem of determining whether a PN  $\mathcal{P}$  has an infinite type *T1*- (*T1'*-, *T2*-, *T2'*-, *T3*-, *T3'*-, respectively) fair computation from its initial marking  $\mu$ .

Let  $X\text{-FAIR-NTP}(\mathcal{A})$  be the set  $\{\mu \mid \exists \sigma \in T^\omega, \mu \xrightarrow{\sigma}, \sigma \text{ is } X\text{-fair w.r.t. } \mathcal{A}\}$ , where  $X \in \{T1, T1', T2, T2', T3, T3'\}$ , which is clearly upward-closed. We now show for all six types of fairness notions,  $X\text{-FAIR-NTP}(\mathcal{A})$  can be dealt with in the framework discussed early in this section.

• *T1-FAIR-NTP*( $\mathcal{A}$ ):

Consider a PN  $\mathcal{P}' = ((P \cup \{p'\}), (T \cup \{t'\}), \varphi')$  derived from  $\mathcal{P}$  such that  $(\forall p \in P, t \in T, \varphi'(p, t) = \varphi(p, t), \varphi'(t, p) = \varphi(t, p))$ ,  $(\forall t \in \bigcup_{A \in \mathcal{A}} A, \varphi'(t, p') = 1)$ , and  $\varphi'(p', t') = \varphi(t', p') = 1$ . It is easy to see that  $\mu \in T1\text{-FAIR-NTP}(\mathcal{A})$  iff  $\mu \xrightarrow{\sigma_0} \mu_1 \xrightarrow{\sigma_1} \mu_2$ ,  $\mu_2 \geq \mu_1$ ,  $\#_{\sigma_1}(t') > 0$ ,  $\sum_{t \in T} \#_{\sigma_1}(t) > 0$ , for some  $\sigma_0 \in T^*$ ,  $\sigma_1 \in (T \cup \{t'\})^+$ .

•  $T1'\text{-FAIR-NTP}(\mathcal{A})$ :

$\mu \in T1'\text{-FAIR-NTP}(\mathcal{A})$  iff  $\exists A \in \mathcal{A}$  such that  $\mu \xrightarrow{\sigma_0} \mu_1 \xrightarrow{\sigma_1} \mu_2$ ,  $\mu_2 \geq \mu_1$ , for some  $\sigma_0 \in A^*$ ,  $\sigma_1 \in A^+$ .

•  $T2\text{-FAIR-NTP}(\mathcal{A})$ :

$\mu \in T2\text{-FAIR-NTP}(\mathcal{A})$  iff  $\mu \xrightarrow{\sigma_0} \mu_1 \xrightarrow{\sigma_1} \mu_2$ ,  $\mu_2 \geq \mu_1$ , and  $(\sum_{t \in (\bigcup_{A \in \mathcal{A}} A)} \#_{\sigma_1}(t)) > 0$ , for some  $\sigma_0 \in T^*$ ,  $\sigma_1 \in T^+$ .

•  $T2'\text{-FAIR-NTP}(\mathcal{A})$ :

$\mu \in T2'\text{-FAIR-NTP}(\mathcal{A})$  iff  $\exists A \in \mathcal{A}$  such that  $\mu \xrightarrow{\sigma_0} \mu_1 \xrightarrow{\sigma_1} \mu_2$ ,  $\mu_2 \geq \mu_1$ , and  $(\sum_{t \in A} \#_{\sigma_1}(t) \geq 0) \wedge (\sum_{t \notin A} \#_{\sigma_1}(t) = 0)$ , for some  $\sigma_0 \in T^*$ ,  $\sigma_1 \in T^+$ .

•  $T3\text{-FAIR-NTP}(\mathcal{A})$ :

$\mu \in T3\text{-FAIR-NTP}(\mathcal{A})$  iff  $\exists A \in \mathcal{A}$  such that  $\mu \xrightarrow{\sigma_0} \mu_1 \xrightarrow{\sigma_1} \mu_2$ ,  $\mu_2 \geq \mu_1$ , and  $(\forall t \in A, \#_{\sigma_1}(t) > 0) \wedge (\sum_{t \notin A} \#_{\sigma_1}(t) = 0)$ , for some  $\sigma_0 \in T^*$ ,  $\sigma_1 \in T^+$ .

•  $T3'\text{-FAIR-NTP}(\mathcal{A})$ :

$\mu \in T3'\text{-FAIR-NTP}(\mathcal{A})$  iff  $\exists A \in \mathcal{A}$  such that  $\mu \xrightarrow{\sigma_0} \mu_1 \xrightarrow{\sigma_1} \mu_2$ ,  $\mu_2 \geq \mu_1$ , and  $\sum_{t \in A} \#_{\sigma_1}(t) > 0$ , for some  $\sigma_0 \in T^*$ ,  $\sigma_1 \in T^+$ .

Now we consider a problem that arises frequently in *automated verification*. Given a system  $S$  with initial state  $q$ , and a designated set of states  $Q$ , it is often of interest and importance to ask whether some state in  $Q$  can be reached from  $q$ , which constitutes a question related to the analysis of a *safety property*. Instead of using the *forward-reachability analysis* (which computes all the states that can be reached from  $q$  to see whether the intersection with  $Q$  is non-empty or not), an equally useful approach is to use the so-called *backward-reachability analysis*. In the latter, we compute the set  $pre^*(S, Q)$  which consists of all the states from which some state in  $Q$  is reachable, and then decide whether  $q \in pre^*(S, Q)$ . In general,  $pre^*(S, Q)$  may not be computable for infinite state systems.

For PNs, we define the *backward-reachability* ( $BR$ , for short) problem as follows:

- **Input:** A PN  $\mathcal{P}$  and a set  $U$  of markings
- **Output:** The set  $pre^*(\mathcal{P}, U) = \{\mu \mid R(\mathcal{P}, \mu) \cap U \neq \emptyset\}$

Now suppose  $U$  is upward-closed, then  $\{\mu \mid R(\mathcal{P}, \mu) \cap U \neq \emptyset\}$  is upward-closed

as well, and is, in fact, equivalent to  $\bigcup_{\nu \in \min(U)} \{\mu \mid \exists \mu' \in R(\mathcal{P}, \mu), \mu' \geq \nu\}$ . The latter is basically asking about coverability issues of PNs. Hence, the max-value of the minimal elements can be derived along the same line as that for the set *NOTBLOCKED*.

#### 4.2. Parametric clocked Petri nets

*Clocked Petri nets* are Petri nets augmented by a finite set of real-value *clocks* and *clock constraints*. Clocks are used to measure the progress of real-time in the system. All the clocks are resettable and increase at a uniform rate. We can as well regard clocks as stop-watches which refer to the same global clock. The use of such clock structure was originally introduced in [1] for defining *timed automata*.

Given a set  $X = \{x_1, x_2, \dots, x_h\}$  of clock variables, the set  $\Phi(X)$  of clock constraints  $\delta$  is defined inductively by  $\delta := x \leq c \mid c \leq x \mid \neg\delta \mid \delta \wedge \delta$ , where  $x$  is a clock in  $X$  and  $c$  is a constant in  $\mathbb{Q}^+$  (i.e., the set of nonnegative rationals). A *clock reading* is a mapping  $\nu : X \rightarrow \mathbb{R}$  which assigns each clock a real value. For  $\eta \in \mathbb{R}$ , we write  $\nu + \eta$  to denote the clock reading which maps every clock  $x$  to the value  $\nu(x) + \eta$ . That is, after  $\eta$  time units added to the global clock, the value of every clock must increase by  $\eta$  units as well. A clock reading  $\nu$  for  $X$  *satisfies* a clock constraint  $\delta$  over  $X$ , denoted by  $\delta(\nu) \equiv \mathbf{true}$ , iff  $\delta$  evaluates to **true** using the values given by  $\nu$ .

A *clocked Petri net* is a 6-tuple  $\mathcal{N} = (P, T, \varphi, X, r, q)$ , where  $(P, T, \varphi)$  is a PN,  $X$  is a finite set of real-value clock variables,  $r : T \rightarrow 2^X$  is a labeling function assigning clocks to transitions, and  $q : T \rightarrow \Phi(X)$  is a labeling function assigning clock constraints to transitions. Intuitively,  $r(t)$  contains those clock variables which are reset when transition  $t$  is fired. A *configuration*  $(\mu, \eta, \nu)$  of a clocked Petri net consists of a *marking*  $\mu$ , the *global time*  $\eta$  and the present *clock reading*  $\nu$ . Note that the clock reading  $\nu$  is continuously being updated as  $\eta$ , the global time, advances. Hence,  $\nu$  and  $\eta$  are not completely independent. Given a configuration  $(\mu, \eta, \nu)$  of a clocked Petri net  $\mathcal{P}$ , a transition  $t$  is *enabled* iff  $\forall p \in P, \varphi(p, t) \leq \mu(p)$ , and  $\nu$  satisfies  $q(t)$ , the set of constraints associated with transition  $t$ , i.e.,  $q(t)(\nu) \equiv \mathbf{true}$ . Let  $\mu$  be the marking and  $\nu$  the clock reading at time  $\eta$ . Then  $t$  *may* fire at  $\eta$  if  $t$  is enabled in the marking  $\mu$  with the clock reading  $\nu$ . We then write  $(\mu, \nu) \xrightarrow{(t, \eta)} (\mu', \nu')$ , where  $\mu'(p) = \mu(p) - \varphi(p, t) + \varphi(t, p)$  (for all  $p \in P$ ), and  $\nu'(x) = 0$  (for all  $x \in r(t)$ ). Note that the global time remains unchanged as a result of firing  $t$ . That is, the firing of a transition is assumed to let no time elapse at all. The global clock will start moving immediately after the firing of a transition is completed. Initially, we assume the initial global time  $\eta_0$  and clock reading  $\nu_0$  to be  $\eta_0 = 0$  and  $\nu_0(x) = 0 (\forall x \in X)$ , respectively. It is important to point

out that, as opposed to timed PNs under *urgent firing semantics*, *enabledness* is necessary but not sufficient for transition firing in a clocked PN. In other words, it is not required to fire all the enabled transitions at any point in time during the course of the computation.

Now consider clocked PNs with parameterized constraints. That is, the ‘ $c$ ’ in the atomic constraints  $x \leq c$  and  $c \leq x$  is not a constant; instead, it is an unknown *parameter*. We are interested in the following question:

- *Input*: Given a clocked PN  $\mathcal{P}$  with unknown integer parameters  $\theta_1, \dots, \theta_n$  in its clock constraints, and a set  $Q$  of goal markings
- *Output*: find the values of  $\theta_1, \dots, \theta_n$  (if they exist) so that there exists a computation reaching a marking in  $Q$ . In what follows, we let  $S(\theta_1, \dots, \theta_n)$  denote such a set of solutions.

Even for timed automata, it is known that the emptiness problem (i.e., the problem of deciding whether there exists a parameter setting under which the associated timed language is empty or not) is undecidable when three or more clocks are compared with unknown parameters [2]. In what follows, we consider a special case in which the involved atomic clock constraints are only of the form  $x \leq \theta$  or  $x < \theta$ , and there are no negative signs immediately before inequalities. In this case, the set ‘ $\{(\theta_1, \dots, \theta_n) \mid \text{there exists a computation in } \mathcal{P} \text{ reaching a marking in } Q \text{ under } (\theta_1, \dots, \theta_n)\}$ ’ is clearly upward-closed, as  $x \leq \theta \implies x \leq \theta'$  and  $x < \theta \implies x < \theta'$ , if  $\theta \leq \theta'$ . That is, whatever enabled under  $\theta$  is also enabled under  $\theta'$ .

A technique known to be useful for reasoning about timed automata is based on the notion of ‘equivalence classes’ [1]. In spite of the differences in value, two different clock readings may induce identical system’s behaviors; in this case, they are said to be in the same clock region. For clock constraints falling into the types given in our setting, the number of distinct clock regions is always finite [1], meaning that a timed automaton (which is of infinite-state potentially) is equivalent behaviorally to a so-called *region automaton* (which is of finite-state). Furthermore, the number of clock regions of a timed automaton  $A$  is bounded by  $2|Q|(|X| \cdot (C_A + 2))^{|X|}$ , where  $|Q|$  is the number of states of  $A$ ,  $|X|$  is the number of clocks of  $A$ , and  $C_A$  is the maximum timing constant involved in  $A$  (see [1] for details). This, coupled with our earlier discussion of upward-closed sets and PNs, yields the following result:

**Theorem 7.** *Given a  $k$ -dimensional clocked PN  $\mathcal{P}$  with unknown integer parameters  $\theta_1, \dots, \theta_n$  in its clock constraints, and an upward-closed set  $Q$  of goal markings,  $|\min(S(\theta_1, \dots, \theta_n))|$  is bounded by  $O((D \cdot |X|)^{2^{d_2 \cdot n \cdot k \cdot \log k} \cdot |X|^n})$ , where  $|X|$  is the number of clocks,  $D$  is the absolute value of the maximum number involved in  $\mathcal{P}$  and  $\min(Q)$ , and  $d_2$  is a constant.*

**PROOF.** The proof is somewhat involved, and hence, only a proof sketch is

given here. Our derivation is based on the approach detailed in Theorem 2.

For the PN to reach  $Q$ , it suffices to consider whether a marking covering an element in  $\min(Q)$  is reachable or not. Recall from Theorem 2 that our approach for computing  $|\min(S(\theta_1, \dots, \theta_n))|$  begins by letting  $(\theta_1, \dots, \theta_n) = (\omega, \dots, \omega) = v_0$ . In this case, the associated clocked PN can be simplified by deleting all the clock constraints involving  $\theta_i$ , because  $x \leq (<) \omega$  always holds. Now the idea is to simulate clocked PNs by VASSs. To this end, we use the ‘state’ portion of the VASS to capture the structure of (finitely many) clock regions of a clocked PN as discussed earlier, and an ‘addition vector’ of the VASS to simulate a transition of the PN. Using the analysis of [1], it is not hard to see that the number of clock regions is bounded by  $O((|X| \cdot C_0)^{|X|})$ , where  $|X|$  is the number of clocks and  $C_0$  is the maximum timing constant (i.e., maximum value of constants involved in clock constraints), which corresponds to the number of states of the VASS.

It was shown in [7], using the technique of multi-parameter analysis, that for an  $m$ -state,  $k$ -dimensional VASS whose largest integer can be represented in  $l$  bits, the length of the shortest witnessing path covering a given marking is bounded by  $O((2^l \cdot m)^{2^{d_2 \cdot k \cdot \log k}})$ . Applying a similar analysis to our constructed VASS and the concept of clock regions, a witness for ‘ $\text{reg}(v_0) \cap S(\theta_1, \dots, \theta_n) \neq \emptyset$ ?’ (if it exists) of max-value bounded by  $d_1 \cdot (D \cdot (|X| \cdot C_0)^{|X|})^{2^{d_2 \cdot k \cdot \log k}}$  can be found, for some constants  $d_1, d_2$ . This bound corresponds to the  $b$  value in the statement of Theorem 2.

The next step is to start with  $v_1 = (\theta_1, \omega, \dots, \omega)$  with  $\theta_1 < d_1 \cdot (D \cdot (|X| \cdot C_0)^{|X|})^{2^{d_2 \cdot k \cdot \log k}}$ . Let this value be  $C_1$ . In this case, those clock constraints involving  $\theta_1$  can no longer be ignored. We construct a new VASS simulating the associated clocked PN, and such a VASS has its number of states bounded by  $O((|X| \cdot C_1)^{|X|})$ , implying that a witness for ‘ $\text{reg}(v_1) \cap S(\theta_1, \dots, \theta_n) \neq \emptyset$ ?’ (if it exists) of max-value bounded by  $d_1 \cdot (D \cdot (|X| \cdot C_1)^{|X|})^{2^{d_2 \cdot k \cdot \log k}}$  can be found, which corresponds to the  $f$  function (w.r.t. variable  $C_1$ ) in Theorem 2. Finally, Theorem 2 immediately yields  $|\min(S(\theta_1, \dots, \theta_n))| = O((D \cdot |X|)^{2^{d_2 \cdot n \cdot k \cdot \log k} \cdot |X|^n})$ .  
**■**

### 4.3. Subclasses of Petri nets

Consider the following problem:

- **Input:** A PN  $\mathcal{P} = (P, T, \varphi)$ , a marking  $\mu'$ , and a system of linear (in)equalities  $L(v_1, \dots, v_m)$ , where  $m = |T|$ . Clearly, the set  $\text{pre}^*(\mathcal{P}, (\mu', L)) = \{\mu \mid \exists \sigma \in T^*, \mu \xrightarrow{\sigma} \mu'', \mu'' \geq \mu' \text{ and } L(\#_{\sigma}(t_1), \dots, \#_{\sigma}(t_m)) \text{ holds}\}$  is upward-closed. (Intuitively, the set contains those markings  $\mu$  from which there is a

computation covering  $\mu'$  and along which the transition firing count vector  $(\#_{\sigma}(t_1), \dots, \#_{\sigma}(t_m))$  satisfies  $L$ .)

- **Output:**  $\min(\text{pre}^*(\mathcal{P}, (\mu', L)))$

What makes the subclasses of PNs in Figure 2 of interest is that their reachability sets can be characterized by *integer linear programming (ILP)* – a relatively well-understood mathematical model (see [11]). In our subsequent discussion, we shall use normal PNs as an example to show how to derive the max-value of the minimal elements of the  $\text{pre}^*$  associated with a normal PN and an upward-closed goal set  $U$ . A PN is normal [10] iff no transition can decrease the token count of a minimal circuit by firing at any marking. For the definitions and the related properties for the rest of the PNs in Figure 2, the reader is referred to [11].

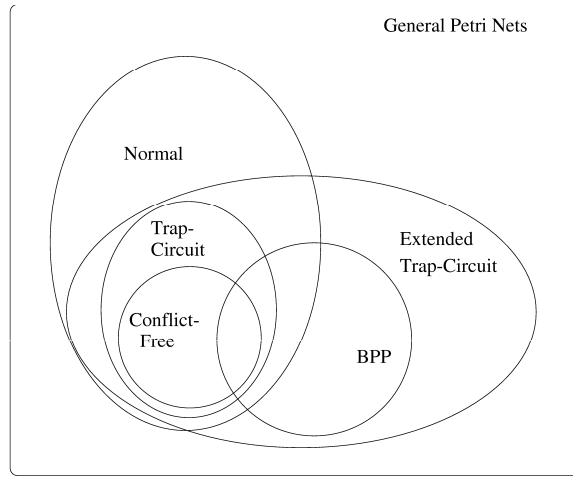


Fig. 2. Containment relationship among subclasses of PNs.

In [5], the reachability problem of normal PNs was equated with ILP using the so-called decompositional approach. The idea behind the decompositional technique relies on the ability to decompose a PN  $\mathcal{P}=(P, T, \varphi)$  (possibly in a nondeterministic fashion) into sub-PNs  $\mathcal{P}_i=(P, T_i, \varphi_i)$  ( $1 \leq i \leq n$ ,  $T_i \subseteq T$ , and  $\varphi_i$  is the restriction of  $\varphi$  to  $(P \times T_i) \cup (T_i \times P)$ ) such that for an arbitrary computation  $\mu_0 \xrightarrow{\sigma} \mu$  of PN  $\mathcal{P}$ ,  $\sigma$  can be rearranged into a canonical form  $\sigma_1 \sigma_2 \cdots \sigma_n$  with  $\mu_0 \xrightarrow{\sigma_1} \mu_1 \xrightarrow{\sigma_2} \mu_2 \cdots \mu_{n-1} \xrightarrow{\sigma_n} \mu_n = \mu$ , and for each  $i$ , a system of linear inequalities  $ILP_i(x, y, z)$  can be set up (based upon sub-PN  $\mathcal{P}_i$ , where  $x, y, z$  are vector variables) in such a way that  $ILP_i(\mu_{i-1}, \mu_i, z)$  has a solution for  $z$  iff there exists a  $\sigma_i$  in  $T_i^*$  such that  $\mu_{i-1} \xrightarrow{\sigma_i} \mu_i$  and  $z = \#_{\sigma_i}$ .

Consider a normal PN  $\mathcal{P}=(P, T, \varphi)$  and let  $P=\{p_1, \dots, p_k\}$  and  $T=\{t_1, \dots, t_m\}$ . In [5], it was shown that an arbitrary computation of a normal PN can be decomposed according to a sequence of distinct transitions  $\tau=t_{j_1} \cdots t_{j_n}$ . More precisely, we define the *characteristic system of inequalities* for  $\mathcal{P}$  and  $\tau$  as  $S(\mathcal{P}, \tau)=\bigcup_{1 \leq h \leq n} S_h$ , where

- $S_h = \{x_{h-1}(i) \geq \varphi(p_i, t_{j_h}), x_h = x_{h-1} + A_h \cdot y_h \mid 1 \leq i \leq k\}$ ,  $A_h$  is an  $k \times h$  matrix whose columns are  $\bar{t}_{j_1}, \dots, \bar{t}_{j_h}$ ,  $y_h$  is a  $h \times 1$  column vector, for  $1 \leq h \leq n$ .

The variables in  $S$  are the components of the  $k$ -dimensional column vectors  $x_0, \dots, x_n$  and the  $h$ -dimensional column vectors  $y_h, 1 \leq h \leq n$ . In [5], it was shown that  $\mu' \in R(\mathcal{P}, \mu)$  iff there exists a sequence of distinct transitions  $\tau = t_{j_1} \cdots t_{j_n}$  such that  $\{x_0 = \mu\} \cup \{x_n = \mu'\} \cup S(\mathcal{P}, \tau)$  has a nonnegative integer solution. In particular, for each  $1 \leq h \leq n$ , the  $i$ -th coordinate of the  $y_h$  variable (an  $h \times 1$  column vector) represents the number of times transition  $t_{j_i}$  ( $1 \leq i \leq h$ ) is used along the path reaching from  $x_{h-1}$  to  $x_h$ . Intuitively speaking, the decomposition is carried out in such a way that

- stage  $h$  involves one more transition (namely  $t_{j_h}$ ) than its preceding stage  $h - 1$ ; furthermore,  $t_{j_h}$  must be enabled in  $x_{h-1}$  as the condition ' $x_{h-1}(i) \geq \varphi(p_i, t_{j_h})$ ' in  $S_h$  enforces,
- $x_h$  represents the marking at the end of stage  $h$  and the beginning of stage  $h + 1$ ,
- the computation from  $x_{h-1}$  to  $x_h$  is captured by  $S_h$ , in which ' $x_h = x_{h-1} + A_h \cdot y_h$ ' simply says that the *state equation* associated with the sub-PN in stage  $h$  is sufficient and necessary to capture reachability between two markings.

For convenience, we define  $y'_h$  to be a vector in  $\mathbb{N}^m$  such that  $y'_h(j_i) = y_h(i)$ ,  $1 \leq i \leq h$ , and the remaining coordinates are zero. Note that  $y'_h$  is an  $m$  dimensional vector w.r.t. the ordering  $t_1, t_2, \dots, t_m$  and  $y_h$  is an  $h$  dimensional vector w.r.t. the ordering  $t_{j_1}, t_{j_2}, \dots, t_{j_h}$ . Intuitively speaking,  $y'_h(i)$  serves as the purpose of rearranging the vector  $y_h$  w.r.t. the ordering  $t_1, t_2, \dots, t_m$ , while filling those coordinates not corresponding to  $t_{j_1}, t_{j_2}, \dots, t_{j_h}$  with zero.

Now we are in a position to derive a bound for the minimal elements of  $pre^*$  for normal PNs.

**Theorem 8.** *Given a normal PN  $\mathcal{P} = (P, T, \varphi)$  with  $|P| = k$  and  $|T| = m$ , a marking  $\mu'$ , and a linear constraint  $L(v_1, \dots, v_m)$ , then  $||\min(pre^*(\mathcal{P}, (\mu', L)))|| \leq (a_1)^{(c \cdot a_2)^k}$ , where  $c$  is some constant,  $a_1 = \max\{||\bar{T}||, s, (m+k) \cdot m\} \cdot m \cdot ||\bar{T}||$ ,  $a_2 = (m \cdot k + r)$ ,  $r$  the number of (in)equalities in  $L$ , and  $s$  the absolute value of the largest integer mentioned in  $L$ .*

**PROOF.** Given a subset of places  $Q \subseteq P$ , we define a *restriction* of  $\mathcal{P}$  on  $Q$  as PN  $\mathcal{P}_Q = (Q, T, \varphi_Q)$ , where  $\varphi_Q$  is the restriction of  $\varphi$  on  $Q$  and  $T$  (i.e.,  $\varphi_Q(p, t) = \varphi(p, t)$ ;  $\varphi_Q(t, p) = \varphi(t, p)$  if  $p \in Q$ ). It is obvious from the definition of normal PNs that  $\mathcal{P}_Q$  is normal as well.

Now consider a vector  $v \in \mathbb{N}_\omega^k$ . To find a witness for  $reg(v) \cap pre^*(\mathcal{P}, (\mu', L)) \neq \emptyset$ , if one exists, it suffices to consider sub-PN with  $Q(v) = \{p \mid v(p) \neq \omega, p \in$

$P\}$  as the set of places (as opposed to the original set  $P$ ), since each  $\omega$  place can supply an arbitrary number of tokens to each of its output transitions. (That is, places associated with  $\omega$  components in  $v$  can be ignored as far as reaching a goal marking in  $U$  is concerned.) Hence,  $reg(v) \cap pre^*(\mathcal{P}, (\mu', L)) \neq \emptyset$  iff for some  $\tau$  (of length  $\leq m$ ), the following system of linear inequalities has a solution  $H \equiv S(\mathcal{P}_Q, \tau) \cup \{x_0 = v\} \cup \{x_n \geq \mu'\} \cup L(v_1, \dots, v_m) \cup \{(v_1, \dots, v_m)^{tr} = y'_1 + \dots + y'_n\}$ .<sup>2</sup> Notice that in the above,  $\{(v_1, \dots, v_m)^{tr} = y'_1 + \dots + y'_n\}$  ensures that for each transition  $t_i$ , the number of times  $t_i$  being used in the computation (i.e.,  $y'_1(i) + y'_2(i) + \dots + y'_n(i)$ ) captured by  $S(\mathcal{P}_Q, \tau)$  equals  $v_i$ . Recall that  $y'_h$  captures the firing count vector in segment  $h$ .

A careful examination reveals that in  $H$ , the number of inequalities is bounded by  $O(m * k + r)$ , and the number of variables is bounded by  $O((m + k) * m)$ . Furthermore, the absolute value of the maximal numbers in  $H$  is bounded by  $max\{\|v\|, \|\bar{T}\|, s\}$ . Using Lemma 3, if  $H$  has a solution, then a ‘small’ solution of max-value bounded by  $(max\{\|v\|, \|\bar{T}\|, s, (m + k) * m\})^{b * (m * k + r)}$  exists, for some constant  $b$ . Recall that the  $y'_h$  vector variable represents the numbers of times the respective transitions are used along segment  $h$  of the reachability path. As a result, an initial marking with at most  $m * (max\{\|v\|, \|\bar{T}\|, s, (m + k) * m\})^{b * (m * k + r)} * \|\bar{T}\|$  tokens in each of the  $\omega$  places suffices for such a path to be valid in the original PN, since each transition consumes at most  $\|\bar{T}\|$  tokens from a place. The above is bounded by  $(a_1 * \|v\|)^{b * a_2}$  (for  $a_1, a_2$  given in the statement of the theorem), where  $b$  is a constant. Now define  $f(\|v\|) = (a_1 * \|v\|)^{b * a_2}$ . From Theorem 2,  $\|min(pre^*(\mathcal{P}, (\mu', L)))\|$  is bounded by  $f^{(k-1)}(\|(\omega, \dots, \omega)\|)$ , which can easily be shown to be bounded by  $(a_1)^{(c * a_2)^k}$ , for some constant  $c$ . ■

The above theorem provides a framework for analyzing a number of upward-closed sets associated with normal PNs. The *BR* problem mentioned at the end of Section 4.1 clearly falls into this category. Our results for normal PNs carry over to the rest of the subclasses listed in Figure 2, although the bounds are slightly different. Due to space limitations, the details are omitted here.

#### 4.4. Lossy Petri nets

*Lossy Petri nets* (or equivalently, *lossy vector addition systems with states*) were first defined and investigated in [3] with respect to various model checking problems. A *lossy Petri net*  $(P, T, \varphi)$  is a PN for which tokens may be *lost* spontaneously without transition firing during the course of a computation. To be more precise, an *execution step* from markings  $\mu$  to  $\mu'$ , denoted by

<sup>2</sup> The superscript *tr* denotes the transpose of a matrix.

$\mu \Rightarrow \mu'$ , of a lossy PN can be of one of the following forms: (1)  $\exists t \in T, \mu \xrightarrow{t} \mu'$ , or (2)  $\mu > \mu'$  (denoting token loss spontaneously at  $\mu$ ). As usual,  $\xrightarrow{*}$  is reflexive and transitive closure of  $\Rightarrow$ . It is easy to observe that for arbitrary goal set  $U$  (not necessarily upward-closed), the set  $pre^*(\mathcal{P}, U)$  for lossy PN  $\mathcal{P}$  is always upward-closed. Consider the case when  $U = \{\mu'\}$ . The following is easy to show:

**Theorem 9.** *Given a lossy PN  $\mathcal{P} = (P, T, \varphi)$ , and a goal marking  $\mu'$ , the minimal elements of the set  $pre^*(\mathcal{P}, \{\mu'\}) = \{\mu \mid \mu \xrightarrow{*} \mu'\}$  have their max-values bounded by  $n^{2^{d \times k \times \log k}}$ , where  $n = \max\{|\bar{T}|, |\mu'|\}$  and  $d$  is a constant.*

The above result can be easily extended to the case when  $U$  is an upward-closed set.

In [3], the *global model checking* problem for (conventional or lossy) VASSs with respect to formula of the form  $\exists \mathcal{A}_\omega(\pi_1, \dots, \pi_m)$  has been shown to be decidable.

An *upward-closed constraint*  $\pi$  over variable set  $X = \{x_1, \dots, x_k\}$  is of the form  $\bigvee_{x_i \in X} x_i \geq c_i$ , where  $c_i \in \mathbb{N}, 1 \leq i \leq k$ . A  $k$ -dimensional vector  $v$  is said to satisfy  $\pi$ , denoted by  $v \models \pi$ , if  $v(i) \geq c_i, \forall 1 \leq i \leq k$ . Consider a  $k$ -dim VASS  $\mathcal{V} = (v_0, V, s_1, S, \delta)$  with  $S = \{s_1, \dots, s_h\}$ . Given  $h$  upward-closed constraints  $\pi_1, \dots, \pi_h$  over variable set  $X = \{x_1, \dots, x_k\}$ , and a configuration  $\sigma_1$ , we write  $\sigma_1 \models \exists_\omega(\pi_1, \dots, \pi_h)$ , iff there is an infinite computation  $\sigma_1, \sigma_2, \dots, \sigma_i, \dots$ , such that  $\forall i \geq 1$ , if  $state(\sigma_i) = s_j$ , then  $val(\sigma_i) \models \pi_j$ . In words, there exists an infinite path from configuration  $\sigma_1$  along which the vector value of each configuration satisfies the upward-closed constraint associated with the state of the configuration. In [3], it was shown the following *global model checking problem* to be decidable:

- Given a  $k$ -dim VASS  $\mathcal{V} = (v_0, V, s_1, S, \delta)$  with  $S = \{s_1, \dots, s_h\}$  and a formula  $\phi = \exists_\omega(\pi_1, \dots, \pi_h)$ , for upward-closed constraints  $\pi_1, \dots, \pi_h$ ,
- Output: The set  $[[\phi]]_{\mathcal{V}} = \{\sigma \mid \sigma \models \phi \text{ in } \mathcal{V}\}$ .

The following result gives a complexity bound for the above problem.

**Theorem 10.** *For each state  $s \in S$ ,  $|\min(\{v \in \mathbb{N}^k \mid (s, v) \in [[\phi]]_{\mathcal{V}}\})|$  is bounded by  $n^{2^{d \times k \times \log k}}$ , where  $n = \max\{|\bar{T}|, u\}$ ,  $u$  is the absolute value of the largest number mentioned in  $\phi$ , and  $d$  is a constant.*

**PROOF.** The proof is done by constructing a VASS  $\mathcal{V}' = (v'_0, V', s'_1, S', \delta')$  from  $\mathcal{V}$  such that  $(s_1, v_0) \models \phi$  in  $\mathcal{V}$  iff there exists an infinite path from  $(s'_1, v'_0)$  in  $\mathcal{V}'$ .

Assume that  $\pi_i = \bigvee_{1 \leq l \leq k} (x_l \geq c_{i,l})$ . For convenience, for a value  $c$  and an index  $l$ , we define  $[c]_l$  to be a vector whose  $l$ -th coordinate equals  $c$ ; the rest of the coordinates are zero. The construction is as follows:

- $S' = S \cup \{q_{i,l,j} \mid 1 \leq i \leq h, 1 \leq l \leq k, 1 \leq j \leq h\}$
- For each addition rule  $v \in \delta(s_i, s_j)$ ,  $k$  addition rules are used to test the  $k$  primitive constraints in  $\pi_i$ , by including the following rules:  $\forall 1 \leq l \leq k$ ,  $[-c_{i,l}]_l \in \delta'(s_i, q_{i,l,j})$ . Furthermore, we also have  $(v + [c_{i,l}]_l) \in \delta'(q_{i,l,j}, s_j)$  to restore the testing of  $c_{i,l}$  as well as adding vector  $v$ .
- $v'_0 = v_0$  and  $s'_1 = s_1$

Based upon the above construction, it is reasonably easy to show that  $(s_1, v_0) \models \phi$  in  $\mathcal{V}$  iff there exists an infinite path from  $(s'_1, v'_0)$  in  $\mathcal{V}'$ . The bound of the theorem then follows from Theorem 6. ■

## References

- [1] R. Alur, and D. Dill, A theory of timed automata, *Theoret. Comput. Sci.* 126 , 183-235, 1994.
- [2] R. Alur, T. Henzinger, M. Vardi, Parametric real-time reasoning, in *Proc. 25th ACM STOC*, 592–601, 1993.
- [3] A. Bouajjani and R. Mayr, Model checking lossy vector addition systems. *STACS'99*, Trier, Germany. LNCS 1563, 323-333. 1999.
- [4] I. Borosh, and L. Treybis, Bounds on positive integral solutions to linear diophantine equations, *Proc. Amer. Math. Soc.*, 55, 299-304, 1976.
- [5] R. Howell, L. Rosier, and H. Yen, Normal and sinkless Petri nets, *J. Comput. System Sci.*, 46, 1–26, 1993.
- [6] C. Rackoff, The covering and boundedness problems for vector addition systems, *Theoret. Comput. Sci.*, 6, 223-231, 1978.
- [7] L. Rosier, and H. Yen, A multiparameter analysis of the boundedness problem for vector addition systems, *J. Comput. System Sci.*, 32, 105-135, 1986.
- [8] R. Valk, M. Jantzen. The residue of vector sets with applications to decidability in Petri nets, *Acta Informatica*, 21, 643-674, 1985.
- [9] F. Wang, and H. Yen, Timing parameter characterization of real-time systems, *Proc. CIAA 2003*, LNCS 2759, 23-34, 2003.
- [10] H. Yamasaki, Normal Petri nets, *Theoret. Comput. Sci.*, 31, 307–315, 1984.
- [11] H. Yen, Integer linear programming and the analysis of some Petri net problems, *Theory of Computing Systems*, 32(4), 467-485, 1999.