SYSTEMS & CONTROL LETTERS

A valuation-based analysis of conflict-free Petri nets

Hsu-Chun Yen

Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan 106, Republic of China

Abstract

We propose a novel *valuation-based* approach for analyzing *conflict-free Petri nets*. The basic idea is to associate a natural number, called the *valuation*, to each marking in the Petri net. If the set of markings of zero valuation is *forward closed*, then the valuation along any Petri net computation is nonincreasing, and in many cases, has the tendency to move towards zero valuation. Using the valuation-based method, we demonstrate a number of problems for conflict-free Petri nets to be decidable. © 2001 Elsevier Science B.V. All rights reserved.

Keywords: Controllability; Decidability; Fairness; Petri net; Reachability analysis

1. Introduction

In spite of their popularity and usefulness in modeling concurrent systems, Petri nets remain one of the least understood computational models analytically. Analyzing the behaviors of Petri nets, in many cases, is a costly endeavor. Because of this, an important research direction in the study of Petri nets is to devise new analytical techniques, in hope of a better understanding of the intricate nature of Petri nets. As a step in this direction, in this article we propose a new technique, called the *valuation method*, for analyzing various problems for *conflict-free Petri nets*. A Petri net is *conflict-free* if every place which is an input of more than one transition is on a self-loop with each such transition [4]; hence, once a transition becomes enabled, the only way to disable the transition is to fire the transition itself. The class of conflict-free Petri nets properly contains that of *marked graphs*, in which

each place of the Petri net has one input and output transitions exactly [5,6]. Given a conflict-free Petri net $\mathscr{P}$, the idea is to associate a value in $N \cup \{\infty\}$ (N is the set of natural numbers) with each marking in $\mathscr{P}$. Such a value is called the *valuation* of the marking. If the set of markings of zero valuation is *forward closed*, then the valuation along any Petri net computation is nonincreasing, and in many cases, has the tendency to move towards the ground level (i.e., valuation zero). Our valuation function is defined based upon the *shortest path* criterion. Once the set of markings of zero valuation is given, the valuation of a marking is the length of the shortest computation from the marking to the ground level. (If the ground level is not reachable, then the valuation is ∞.) As we shall see later, in our analysis we actually do not compute the valuation function; instead, the above strategy merely serves as a foundation using which certain properties (including *deadlock*, *fair nontermination*, *home state*, (*fair*) *self-stabilization*, and *fair controllability*) of conflict-free Petri nets are verified. To a certain degree, the basic idea of our valuation method is

E-mail address: yen@cc.ee.ntu.edu.tw (H.-C. Yen).

analogous to the use of *Lyapunov functions* in stability analysis. See also [7] for work on valuation-based methods for the semantics of languages.

The main contribution of this work lies in the development of a valuation-based approach through which necessary and sufficient conditions for a variety of properties concerning conflict-free Petri nets are established in a unified framework. Although conflict-free Petri nets constitute a small subclass with limited modeling capabilities and one might argue that due to the structural simplicity of conflict-free Petri nets the results obtained in Section 3, could be derived using alternate proof techniques (for example, those summarized in [1]), we feel that our valuation-based approach is of theoretical interest and deserves further investigation. Our approach offers an umbrella under which several interesting Petri net problems are answered in a clear and unified framework. It is also interesting to investigate potential applications (not limited to conflict-free Petri nets) of our valuation-based methodology. More will be said about this in our subsequent discussion.

The remainder of this paper is organized as follows: Section 2 gives the basic definitions of Petri nets and the problems under investigation. In Section 3, we study the basic theory behind our *valuation-based* approach for conflict-free Petri nets, and then demonstrate how such an approach can be used as a unified tool for solving those problems defined in Section 2.

2. Preliminaries

Let N denote the set of nonnegative integers, and N^k the set of vectors of k nonnegative integers. A *Petri net* (PN, for short) is a 3-tuple (P, T, φ), where

- P is a finite set of *places*,
- T is a finite set of *transitions*, and
- φ is a *flow function* $\varphi: (P \times T) \cup (T \times P) \rightarrow \{0, 1\}$.

In this paper, k is reserved for $|P|$ (the number of places in P). A *marking* is a mapping $\mu: P \rightarrow N$. A transition $t \in T$ is *enabled* at a marking μ iff for every $p \in P$, $\varphi(p, t) \leqslant \mu(p)$. In a PN (P, T, φ), a transition t may *fire* at a marking μ if t is enabled at μ; we then write $\mu \xrightarrow{t} \mu'$, where $\mu'(p) = \mu(p) - \varphi(p, t) + \varphi(t, p)$

for all $p \in P$. (We also write $\mu \rightarrow \mu'$ to denote the reachability of μ' from μ in one step.) A sequence of transitions $\sigma = t_1 \ldots t_n$ is a *firing sequence* from μ_0 in a PN iff $\mu_0 \xrightarrow{t_1} \mu_1 \xrightarrow{t_2} \cdots \xrightarrow{t_n} \mu_n$ for some sequence of markings $\mu_1, \ldots, \mu_n$; we also write $\mu_0 \xrightarrow{\sigma} \mu_n$. In a PN, we write $\mu_0 \xrightarrow{\sigma}$ to denote that σ is enabled and can be fired from μ_0, i.e., $\mu_0 \xrightarrow{\sigma}$ iff there exists a marking μ such that $\mu_0 \xrightarrow{\sigma} \mu$. An infinite sequence σ is a firing sequence from μ, written as $\mu \xrightarrow{\sigma}$, iff for every finite prefix σ' of σ, $\mu \xrightarrow{\sigma'}$. We write $\mu \xrightarrow{*} \mu'$ to denote the existence of a firing sequence σ such that $\mu \xrightarrow{\sigma} \mu'$.

The *reachability set* of a PN $\mathscr{P}$ with respect to initial marking μ_0 is the set $R(\mathscr{P}, \mu_0) = \{\mu \mid \mu_0 \xrightarrow{\sigma} \mu$ for some $\sigma \in T^*\}$. Given a set of markings S, the *successor* (resp., *predecessor*) of S, written as succ(S) (resp., pred(S)), is the set $\{\mu \mid \exists t \in T, \mu' \in S, \mu' \xrightarrow{t} \mu\}$ (resp., $\{\mu \mid \exists t \in T, \mu' \in S, \mu \xrightarrow{t} \mu'\}$). Let pred* (resp., succ*) be the reflexive and transitive closure of pred (resp., succ). (That is, succ$^*(S) = \{\mu \mid \exists \mu' \in S, \mu' \xrightarrow{*} \mu\}$, and pred$^*(S) = \{\mu \mid \exists \mu' \in S, \mu \xrightarrow{*} \mu'\}$.) The sets succ$^*(S)$ and pred$^*(S)$ will be referred to as the *forward reachability set* and the *backward reachability set* of S, respectively. Notice that $R(\mathscr{P}, \mu_0) = $ succ$^*(\{\mu_0\})$. A set of markings S is said to be *forward closed* if $\forall \mu \in S, \forall t \in T, \mu \xrightarrow{t} \mu'$ implies $\mu' \in S$. An infinite computation $\mu_1 \xrightarrow{t_1} \mu_2 \xrightarrow{t_2} \cdots \mu_i \xrightarrow{t_i} \mu_{i+1} \cdots$ is *fair* if for every transition t, if t is enabled at infinitely many μ_{i_l} ($l \geqslant 1$), then there exist infinitely many j_l ($l \geqslant 1$) such that $t_{j_l} = t$. (In words, if a transition is enabled infinitely many times, then the transition must occur infinitely often as well.) See, e.g., [5,6] for more about Petri nets and their related problems.

For ease of expression, the following notations will be used throughout the rest of this paper. Let σ, σ' be transition sequences, and t be a transition.

- $\#_\sigma(t)$ represents the number of occurrences of t in σ.
- $\text{Tr}(\sigma) = \{t \mid t \in T, \#_\sigma(t) > 0\}$, denoting the set of transitions used in σ.
- $\sigma \dot{-} \sigma'$ is defined inductively as follows. Suppose $\sigma' = t_1 \ldots t_n$. Let σ_0 be σ. If t_i is in σ_{i-1}, let σ_i be σ_{i-1} with the leftmost occurrence of t_i deleted; otherwise, let $\sigma_i = \sigma_{i-1}$. Finally, let $\sigma \dot{-} \sigma' = \sigma_n$. For example, if $\sigma = t_1 t_2 t_3 t_4 t_5$ and $\sigma' = t_4 t_3 t_1$, then $\sigma \dot{-} \sigma' = t_2 t_5$.

For firing sequences σ and σ', σ' is said to be a *rearrangement* of σ if $\#_\sigma(t) = \#_{\sigma'}(t) \forall t \in T$.

In this paper, we focus on the following problems:

- *The deadlock problem*: Given a PN $\mathscr{P}$, compute the set $\mathrm{DL}(\mathscr{P}) = \{\mu \mid$ there does not exist an infinite computation from $\mu\}$. (That is, $\mathrm{DL}(\mathscr{P})$ contains those markings from which all computations eventually terminate.)
- *The fair nontermination problem*: Given a PN $\mathscr{P}$ and a set of markings S (called the *termination set*), compute the set $\mathrm{FNT}(\mathscr{P}, S) = \{\mu \mid$ there exists a fair infinite computation $\mu \xrightarrow{\sigma}$ avoiding $S\}$. (That is, $\mathrm{FNT}(\mathscr{P}, S)$ contains those markings from which fair nonterminating computations (i.e., avoiding S) of infinite length exist.)
- *The home state problem*: Given a PN $\mathscr{P}$, a marking μ is said to be a *home state* with respect to a marking μ_0 if $\forall \mu' \in R(\mathscr{P}, \mu_0)$, $\mu' \xrightarrow{*} \mu$. The home state problem is that of, given a PN $\mathscr{P}$ and a marking μ, computing the set $\mathrm{HS}(\mathscr{P}, \mu) = \{\mu_0 \mid \mu$ is a home state with respect to $\mu_0\}$.
- *The self-stabilization* and *the fair self-stabilization problems*: Given a PN $\mathscr{P}$ with initial marking μ_0, a computation σ from marking μ_1 is said to be *nonself-stabilizing* iff one of the following holds:
  (1) σ ($\mu_1 \to \mu_2 \to \cdots \to \mu_m$, for some m) is finite such that μ_m is a 'dead' marking (i.e., μ_m has no immediate successor in $\mathscr{P}$) and $\mu_m \notin R(\mathscr{P}, \mu_0)$, or
  (2) σ ($\mu_1 \to \mu_2 \to \cdots \to \mu_i \to \cdots$) is infinite such that $\forall i \geqslant 1, \mu_i \notin R(\mathscr{P}, \mu_0)$.

  The *self-stabilization problem* is to compute the set $\mathrm{SS}(\mathscr{P}, \mu_0) = \{\mu \mid$ none of the computations emanating from μ is *nonself-stabilizing*\}. *Fair nonself-stabilizing* computations are similar to *nonself-stabilizing* ones except that Condition (2) above is replaced by

  (2′) σ ($\mu_1 \to \mu_2 \to \cdots \to \mu_i \to \cdots$) is infinite and fair such that $\forall i \geqslant 1, \mu_i \notin R(\mathscr{P}, \mu_0)$.

  The *fair self-stabilization problem* is to compute the set $\mathrm{FSS}(\mathscr{P}, \mu_0) = \{\mu \mid$ none of the computations emanating from μ is *fair nonself-stabilizing*\}.
- *The fair controllability problem*: A *controlled* PN is simply a PN (P, T, φ) with its T partitioned into T_c (the set of *controllable transitions*) and T_u (the

set of *uncontrollable transitions*). A *control policy* is a mapping $N^k \to 2^{T_c}$. (What it means is that at each marking, the control policy selects a subset of controllable transitions from which the next transition to fire must come, unless the next transition is an uncontrollable transition.) A control policy h is said to be *fair* if along every infinite path, if a $t \in T_c$ is enabled infinitely often, then h must select t infinitely many times along the path. With respect to a control policy h, an infinite path $\sigma: \mu_1 \to \mu_2 \to \cdots$ is *fair* if for every transition t, if t is included and enabled in infinitely many $h(\mu_i)$, then t must be fired infinitely often along σ. The *fair controllability problem* is that of, given a controlled PN and a set S of *forbidden markings*, computing the set $\mathrm{FC}(\mathscr{P}, S) = \{\mu \mid$ there exists a fair control policy h such that from μ all the fair infinite computations under h always avoid S regardless of how such computations are interleaved with transitions in $T_u\}$. Intuitively, $\mathrm{FC}(\mathscr{P}, S)$ represents the set of markings from which the computation can be controlled in a fair fashion to stay away from S. The interested reader is referred to [2] for more about *controlled Petri nets* and the related issues.

As *fairness* is frequently used as a qualitative measure to capture the notion of a quantitative measure of 'something happens with probability one', our fairness-related results are applicable to *probabilistic* conflict-free PNs (in which a probability is assigned to the firing of an enabled transition) with respect to questions like 'reaching a deadlock with probability one', 'self-stabilized with probability one', and more.

3. Analysis of conflict-free Petri nets using the valuation method

Given a PN $\mathscr{P} = (P, T, \varphi)$, a *valuation function* f is a mapping $N^k \to N \cup \{\infty\}$, i.e., f maps each marking μ to a number in $N \cup \{\infty\}$. (The value of $f(\mu)$ is called the *valuation* of marking μ.) A valuation function f is said to be *monotone* if for every marking μ, if $\mu \xrightarrow{t} \mu'$ (for some marking μ' and transition t), then $f(\mu) \geqslant f(\mu')$. It is obvious that if f is monotone and $\mu \xrightarrow{\sigma} \mu'$ (where $\sigma \in T^*$), then $f(\mu) \geqslant f(\mu')$.

In this paper, we mainly focus on the following subclass of Petri nets:

(i) $|p^\bullet| \leqslant 1$, <u>or</u>
(ii) $\forall t \in p^\bullet$, t and p are on a self-loop (i.e., $t \in (p^\bullet \cap {}^\bullet p)$),

where $p^\bullet = \{t \mid \varphi(p,t) > 0\}$ (resp., ${}^\bullet p = \{t \mid \varphi(t,p) > 0\}$) represents the set of output (resp., input) transitions of place p. In words, a PN is conflict-free if every place which is an input of more than one transition is also an output of each such transition [4]. In a conflict-free PN, once a transition becomes enabled, the only way to disable the transition is to fire the transition itself. (That is $\forall t, t' \in T$, $t \neq t'$, $\mu \xrightarrow{t} \mu'$ and $\mu \xrightarrow{t'}$ implies $\mu' \xrightarrow{t'}$.) In fact, it has been shown in [4] that suppose σ and τ are two fireable sequences (at a marking μ) in a conflict-free PN, then $\sigma \cdot (\tau \mathbin{\dot{-}} \sigma)$ is fireable at μ as well. A direct consequence of the above is that if $\mu \xrightarrow{\sigma}$, $\mu \xrightarrow{\delta}$ and $\mathrm{Tr}(\sigma) \cap \mathrm{Tr}(\delta) = \emptyset$, then $\mu \xrightarrow{\sigma\delta}$.

Example 1. Fig. 1 illustrates a conflict-free PN describing a system consisting of *m producers* and one *consumer*. (Notice that Fig. 1 is not a marked graph.) The *i*th producer iterates a loop consisting of a sequence of two actions, *produce* (denoted p_i) followed by *send* (denoted by s_i), whereas the consumer iterates a loop containing the actions of *receive* (denoted by r) and *consume* (denoted c). With respect to a producer, the number of *produces* is never less than that of *sends* and never exceeds the number of *sends* by more than one in any computation. In addition, the number of *receives* can never exceeds the total number of *sends*. Thus, if we let the alphabet of the system be $\Sigma = \{p_i, s_i \mid 1 \leqslant i \leqslant m\} \cup \{r, c\}$, the system's behaviors can be captured by the following sequential language, which contains all strings σ such that

- $\#_\sigma(s_i) \leqslant \#_\sigma(p_i) \leqslant \#_\sigma(s_i) + 1$ for $1 \leqslant i \leqslant m$,
- $\#_\sigma(c) \leqslant \#_\sigma(r) \leqslant \#_\sigma(c) + 1$,
- $\#_\sigma(r) \leqslant \sum_{1 \leqslant i \leqslant m} \#_\sigma(s_i)$.

Given a conflict-free PN $\mathscr{P} = (P, T, \varphi)$ and a set of markings S, the following valuation function f will be used throughout the rest of this paper: $f(\mu)$ is defined to be the length of the shortest path from μ to a marking

in S; if μ cannot reach S, $f(\mu)$ is ∞. Notice that $\forall \mu \in S, f(\mu) = 0$ (i.e., S defines the set of markings of zero valuation). What follows is another way to view such a valuation function. We partition N^k into a sequence of disjoint sets of markings $U_0, U_1, \ldots, U_\infty$ such that

$$U_0 = S,$$
$$U_1 = (\mathrm{pred}(U_0)) - U_0,$$
$$\cdots$$

$$U_i = (\mathrm{pred}(U_{i-1})) - \left(\bigcup_{j=0,\ldots,i-1} U_j \right), \quad i \geqslant 1,$$

$$U_\infty = N^k - \left(\bigcup_{j \geqslant 0} U_j \right).$$

It is not hard to see that $f(\mu) = i$ iff $\mu \in U_i$.

Before getting into the details of our analysis, we require a few lemmas concerning conflict-free PNs as well as the valuation function defined above.

Lemma 3.1. *Given a conflict-free PN $\mathscr{P}$ and a forward-closed set S, let f be the valuation function based upon the shortest path criterion defined above. The following hold*:

(1) *f is always monotone, i.e., for every markings μ, μ' and transition t, $\mu \xrightarrow{t} \mu'$ implies $f(\mu) \geqslant f(\mu')$.*
(2) *For an arbitrary μ and a path $\mu \xrightarrow{\delta} \mu''$, if $\mu \xrightarrow{\sigma} \mu'$ ($\mu' \in S$) is one of the shortest paths reaching S and $\mathrm{Tr}(\delta) \cap \mathrm{Tr}(\sigma) \neq \emptyset$, then $f(\mu'') < f(\mu)$. What this statement says is that if δ uses some transition(s) belonging to the shortest path to S, then δ will constitute a drop in valuation.*

Proof. We first consider (1). It suffices to show that $\mu \xrightarrow{t} \mu_1$ implies $f(\mu) \geqslant f(\mu_1)$. Consider the following cases:

(a) ($f(\mu) = \infty$) In this case, $f(\mu_1) = \infty$; otherwise, $\mu \xrightarrow{t} \mu_1 \xrightarrow{*} \mu''$, $\mu'' \in S$, violating the assumption that $f(\mu) = \infty$.
(b) ($0 < f(\mu) < \infty$) Let $\mu \xrightarrow{\sigma} \mu'(\mu' \in S)$ be one of the shortest paths reaching S. Consider two cases:
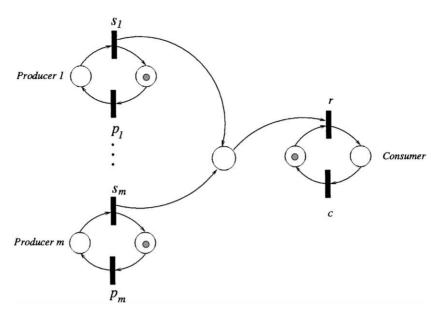
Fig. 1. A conflict-free Petri net modeling a system of m producers and one consumer.

(i) $t \notin \mathrm{Tr}(\sigma)$. Since the PN is conflict-free, t is enabled at μ'. Suppose $\mu' \xrightarrow{t} \mu''$, for some $\mu'' \in S$ (since S is forward-closed). Clearly, $\mu_1 \xrightarrow{\sigma} \mu''$, yielding $f(\mu_1) \leqslant f(\mu)$.

(ii) $t \in \mathrm{Tr}(\sigma)$. Suppose $\mu \xrightarrow{\sigma_1} \mu_2 \xrightarrow{t} \mu_3 \xrightarrow{\sigma_2} \mu'$ (for some μ_2, μ_3), where $\sigma = \sigma_1 t \sigma_2$ and t is not in σ_1. Again due to the conflict-freedom property of the PN, $\mu_1 \xrightarrow{\sigma_1} \mu_3 \xrightarrow{\sigma_2} \mu'$; hence, $f(\mu_1) \leqslant f(\mu) - 1$.

Fig. 2 illustrates the monotone property of the valuation function for paths in a conflict-free PN.

Now consider (2). Due to the assumption that $\mathrm{Tr}(\delta) \cap \mathrm{Tr}(\sigma) \neq \emptyset$, there must exist a transition $t \in T$ such that

- $\sigma = \sigma_1 t \sigma_2$ and $\mu \xrightarrow{\sigma_1} \mu_1 \xrightarrow{t} \mu_2 \xrightarrow{\sigma_2} \mu'$ for some $\sigma_1, \sigma_2 \in T^*$, and markings μ_1 and μ_2,
- $\delta = \delta_1 \delta_2$ and $\mu \delta_1 \bar{\mu} \xrightarrow{t} \bar{\mu}_1 \xrightarrow{\delta_2} \mu''$ for some $\delta_1, \delta_2 \in T^*$, and markings $\bar{\mu}$ and $\bar{\mu}_1$,
- $t \notin \mathrm{Tr}(\sigma_1)$, $t \notin \mathrm{Tr}(\delta_1)$, and
- $\mathrm{Tr}(\delta_1) \cap \mathrm{Tr}(\sigma) = \emptyset$.

That is, t is chosen to be the first occurrence of a transition along δ that is also in σ. Notice that $f(\mu) = 1 + |\sigma_1 \sigma_2|$, since σ is assumed to be one of the shortest
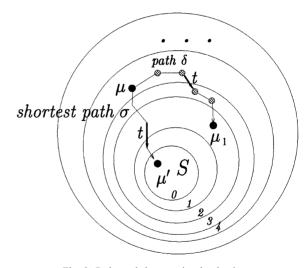

Fig. 2. Paths and the associated valuations.

paths reaching S. From the selection of t and PN $\mathscr{P}$ being conflict-free, we immediately have the following (see Fig. 3):

(i) σ_1 is enabled at $\bar{\mu}_1$ (because $\mathrm{Tr}(\sigma_1) \cap \mathrm{Tr}(\delta_1 t) = \emptyset$); let $\bar{\mu}_1 \xrightarrow{\sigma_1} \bar{\mu}_2$ for some $\bar{\mu}_2$,

(ii) $\mu_2 \xrightarrow{\delta_1} \bar{\mu}_2$ (because $\mathrm{Tr}(\delta_1) \cap \mathrm{Tr}(\sigma_1 t) = \emptyset$),
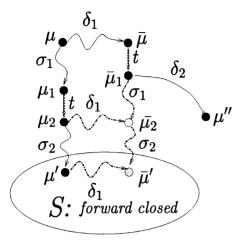
Fig. 3. Illustration of the proof of Lemma 3.1.

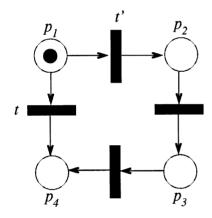Fig. 4. A non-conflict-free Petri net.

(iii) $\mu' \xrightarrow{\delta_1} \bar{\mu}'$, for some $\bar{\mu}' \in S$ (because $\mathrm{Tr}(\delta_1) \cap \mathrm{Tr}(\sigma) = \emptyset$),

(iv) $\bar{\mu}_2 \xrightarrow{\sigma_2} \bar{\mu}'$ (because $\mathrm{Tr}(\delta_1) \cap \mathrm{Tr}(\sigma_2) = \emptyset$).

From cases (i) and (iv) above, we have $\bar{\mu}_1 \xrightarrow{\sigma_1 \sigma_2} \bar{\mu}'$; hence, $f(\bar{\mu}_1) \leqslant |\sigma_1 \sigma_2| = f(\mu) - 1$. Using the result of (1) (i.e., f being monotone) and the fact that $\bar{\mu}_1 \xrightarrow{\delta_2} \mu''$, we have $f(\mu'') \leqslant f(\bar{\mu}_1) < f(\mu)$; as a result, (2) follows. $\square$

It should be noticed that being conflict-free plays an important role in Lemma 3.1 as the following example indicates. Consider a non-conflict-free PN $\mathscr{P}$ shown in Fig. 4. (In $\mathscr{P}$, t and t' are in conflict with each other.) The initial marking is $(1, 0, 0, 0)$ (i.e., one token in p_1 while p_2, p_3, and p_4 are empty) and suppose $S = \{(0, 0, 0, 1)\}$, which is clearly forward-closed as none of the transitions is enabled in S. From the easy fact that $f((1, 0, 0, 0)) = 1$, $(1, 0, 0, 0) \xrightarrow{t'} (0, 1, 0, 0)$ and $f(0, 1, 0, 0) = 2$, the monotonicity property does not hold for $\mathscr{P}$.

At first glance, it appears that our valuation-based approach resembles that of the so-called *stubborn set method* reported in [8]. The idea behind the stubborn set method is to narrow the set of transitions to be expanded next in the process of a search. Conceptually, the stubborn set guides the computation to its destination in a faster and more intelligent fashion. Suppose T_s is a function that maps each non-deadlock marking μ to a set of transitions $T_s(\mu)$ (called a *dynamically stubborn set*) such that

(D1) If $t \in T_s(\mu)$ and $t_1, \ldots, t_n \notin T_s(\mu)$, then $\mu \xrightarrow{t_1 \cdots t_n t} \mu'$ implies $\mu \xrightarrow{t t_1 \cdots t_n} \mu'$.

(D2) There exists a $t \in T_s(\mu)$ such that if $t_1, \ldots, t_n \notin T_s(\mu)$ and $\mu \xrightarrow{t_1 \cdots t_n} \mu'$, then $\mu' \xrightarrow{t}$.

The above (D1) and (D2) are the basic conditions of the stubborn set method under which deadlock detection can be faithfully carried out in the reduced state space [8]. In subsequent research, a number of additional conditions have been introduced in order to cope with a variety of Petri net properties such as liveness, fairness, and more.

On the surface, Conditions (D1) and (D2) seem to suggest the legitimacy of rearranging the firing order of certain transitions, resembling a key property of conflict-free PNs (i.e., for $t \neq t'$, $\mu \xrightarrow{t}$ and $\mu \xrightarrow{t'}$ imply $\mu \xrightarrow{t t'}$). By a careful examination, it becomes apparent that neither (D1) nor (D2) is sufficient to guarantee that every enabled transition remains enabled until it is executed—a key for which our subsequent analysis relies.

Now we are in a position to reason about the list of problems mentioned in Section 2 in the framework of the valuation method.

Theorem 3.2. *Given a conflict-free PN $\mathscr{P} = (P, T, \varphi)$, let $S = \{\mu \mid \forall t \in T, t$ is disabled at $\mu\}$ (i.e., S is the set of all dead markings). $\mu \in \mathrm{DL}(\mathscr{P})$ iff $\mu \in \mathrm{pred}^*(S)$.*

Proof. First notice that S is forward-closed. We let $f(\mu) = 0 \; \forall \mu \in S$. Clearly, if $\mu \notin \mathrm{pred}^*(S)$, then there exists an infinite path from μ. The *only-if part* follows. Now we show the *if* part. Suppose $\mu \in \mathrm{pred}^*(S)$. Let $\mu \xrightarrow{\sigma} \mu' \in S$ be one of the shortest paths reaching some marking in S (guaranteed by the assumption that $\mu \in \mathrm{pred}^*(S)$). Now for every transition t fireable at μ, we claim that if $\mu \xrightarrow{t} \mu''$, then $f(\mu'') < f(\mu)$. To see this, first observe that t must be in σ; otherwise, t remains enabled at μ'—violating the assumption that S being the set of dead markings. It follows from [4] that $\mu \xrightarrow{t} \mu'' \xrightarrow{\sigma'} \mu'$ for some sequence σ' such that $t\sigma'$ is a rearrangement of σ. Hence, $f(\mu'') < f(\mu)$ (due to the definition of the valuation function f). By repeating the above argument, the valuation decreases as the computation advances. A marking of zero valuation must be reached eventually. $\quad\square$

Theorem 3.3. *Given a conflict-free PN $\mathscr{P} = (P, T, \varphi)$ and a forward-closed set S, $\mu \in \mathrm{FNT}(\mathscr{P})$ iff $\mu \notin (\mathrm{DL}(\mathscr{P}) \cup \mathrm{pred}^*(S))$.*

Proof. We let $f(\mu) = 0 \; \forall \mu \in S$. If $\mu \notin (\mathrm{DL}(\mathscr{P}) \cup \mathrm{pred}^*(S))$, at every marking reachable from μ, every enabled transition can be taken without being blocked or entering S; hence, there exists a fair nonterminating infinite path from μ. The *if-part* follows. Now we show the *only-if* part. According to Theorem 3.2, all computations from $\mathrm{DL}(\mathscr{P})$ eventually get blocked. It suffices to consider the case $\mu \in \mathrm{pred}^*(S)$. If μ has a fair nonterminating path, then there must exist a marking μ_1 and sequences σ_1 and σ_2 such that $\mu \xrightarrow{\sigma_1} \mu_1 \xrightarrow{\sigma_2}$, $f(\mu) \geqslant f(\mu_1) > 0$ and $\mu_1 \xrightarrow{\sigma_2}$ is fair along which the valuation never drops. Let $\mu_1 \xrightarrow{t_1 t_2 \cdots t_i} \mu' (\mu' \in S)$ be one of the shortest paths reaching some marking in S. The fairness assumption ensures that $t_1 \in \mathrm{Tr}(\sigma_2)$; otherwise, t_1 would have been enabled infinitely often without being fired. By Lemma 3.1, the valuation along σ_2 eventually drops—a contradiction. As a consequence, all infinite computations from μ are unfair. $\quad\square$

Theorem 3.4. *Given a conflict-free PN $\mathscr{P} = (P, T, \varphi)$ and an initial marking μ_0, if every infinite computation $\mu_0 \xrightarrow{\sigma}$ satisfies $\{t \mid t$ occurs infinitely often in $\sigma\} = T$, then $\mu \in \mathrm{SS}(\mathscr{P}, \mu_0)$ iff $\mu \in \mathrm{pred}^*(R(\mathscr{P}, \mu_0))$.*

Proof. It is obvious that if $\mu \notin \mathrm{pred}^*(R(\mathscr{P}, \mu_0))$, then μ cannot be in $\mathrm{SS}(\mathscr{P}, \mu_0)$. Now it suffices to prove the *if-part*, i.e., $\mu \in \mathrm{pred}^*(R(\mathscr{P}, \mu_0)) \Rightarrow \mu \in \mathrm{SS}(\mathscr{P}, \mu_0)$. Suppose, in contrast, that $\mu \in \mathrm{pred}^*(R(\mathscr{P}, \mu_0))$ yet $\mu \notin \mathrm{SS}(\mathscr{P}, \mu_0)$. According to Lemma 3.1, there exists an infinite path from μ: $\mu \xrightarrow{\sigma_1} \mu_1 \xrightarrow{\sigma_2}$ such that $f(\mu) \geqslant f(\mu_1) > 0$ and the valuation along $\mu_1 \xrightarrow{\sigma_2}$ remains $f(\mu_1)$. Let $\mu_1 \xrightarrow{\delta} \mu'$ be one of the shortest paths reaching some marking in $R(\mathscr{P}, \mu_0)$. If $\mathrm{Tr}(\delta) \cap \mathrm{Tr}(\sigma_2) \neq \emptyset$, then the valuation along σ_2 must eventually drop below $f(\mu_1)$ (Lemma 3.1), which is a contradiction. Suppose $\mathrm{Tr}(\delta) \cap \mathrm{Tr}(\sigma_2) = \emptyset$, then σ_2 is fireable at marking μ' (conflict-freedom property), implying that $\mathrm{Tr}(\sigma_2) = T$—again a contradiction. Our lemma follows. $\quad\square$

It is interesting to see whether the valuation method remains useful when the condition "$\{t \mid t$ occurs infinitely often in $\sigma\} = T$" is removed from the statement of the above theorem.

Theorem 3.5. *Given a conflict-free PN $\mathscr{P} = (P, T, \varphi)$ and an initial marking μ_0, $\mu \in \mathrm{FSS}(\mathscr{P}, \mu_0)$ iff $\mu \in \mathrm{pred}^*(R(\mathscr{P}, \mu_0))$.*

Proof. Clearly, $R(\mathscr{P}, \mu_0)$ is forward-closed. We let the valuations of those markings in $R(\mathscr{P}, \mu_0)$ be zero. If $\mu \notin \mathrm{pred}^*(R(\mathscr{P}, \mu_0))$, none of the (finite or infinite) computations can reach $R(\mathscr{P}, \mu_0)$; hence, $\mu \notin \mathrm{FSS}(\mathscr{P}, \mu_0)$. On the other hand, if $\mu \in \mathrm{pred}^*(R(\mathscr{P}, \mu_0))$, then following an argument similar to the proof of Theorem 3.2, all the fair infinite computations must eventually reach a marking of zero valuation, i.e., reaching $R(\mathscr{P}, \mu_0)$. Hence $\mu \in \mathrm{FSS}(\mathscr{P}, \mu_0)$. $\quad\square$

Theorem 3.6. *Given a conflict-free PN $\mathscr{P} = (P, T, \varphi)$ and a marking μ, $\mu' \in \mathrm{HS}(\mathscr{P}, \mu)$ iff $R(\mathscr{P}, \mu) \subseteq \mathrm{pred}^*(\{\mu\})$ and $\mu' \in \mathrm{pred}^*(R(\mathscr{P}, \mu))$.*

Proof. A necessary condition for μ to be a home state is that $\forall \mu' \in R(\mathscr{P}, \mu), \mu' \xrightarrow{*} \mu$, which is ensured by $R(\mathscr{P}, \mu) \subseteq \mathrm{pred}^*(\{\mu\})$ (That is, $\mathscr{P}$ is reversible with respect to initial marking μ.) We then assign zero to the valuation of each marking in $R(\mathscr{P}, \mu)$, which is clearly a forward-closed set. For each $\mu' \in \mathrm{pred}^*(R(\mathscr{P}, \mu))$, $f(\mu') < \infty$ and if $\mu' \xrightarrow{*} \mu''$, then

$f(\mu'') \leqslant f(\mu')$ (Lemma 3.1), implying that μ'' can reach some marking in $R(\mathscr{P}, \mu)$. Our result follows as $\mathscr{P}$ is reversible with respect to μ. $\quad\square$

Theorem 3.7. *Given a controlled conflict-free PN* $\mathscr{P} = (P, T_u \cup T_c, \varphi)$ *and a forward-closed set* S *of forbidden markings,* $\mu \in \mathrm{FC}(\mathscr{P}, S)$ *iff* $\mu \notin \mathrm{pred}^*(S)$.

Proof. It is obvious that if $\mu \notin \mathrm{pred}^*(S)$, any computation from μ (regardless of whether it is controlled or not) never encounters S. It suffices to show that if $\mu \in \mathrm{pred}^*(S)$, then any fair computation has the tendency to move towards S, in spite of the presence of a fair control policy. Suppose, to the contrary, that $\mu \xrightarrow{\sigma}$ were an infinite computation which never visits S. It is clear that σ can be decomposed into $\delta_0 \sigma_1 \delta_1 \cdots \sigma_m \delta_m \sigma_{m+1}$ such that $\delta_0, \delta_1, \ldots, \delta_m \in (T_u)^*$, $\sigma_1, \ldots, \sigma_m \in (T_c)^*$, and σ_{m+1} is an infinite computation consisting of transitions from T_c. (As transitions in T_u cannot be controlled by the control policy, one may view the $\delta_0, \delta_1, \ldots, \delta_m$ segments as the steps performed by an 'adversary' trying to force the computation into S. This explains why the infinite suffix computation σ_{m+1} is assumed to use transitions in T_c only.) Using an argument parallels to the proof of Theorem 3.3, σ_{m+1} must eventually enter S under the fairness assumption. $\quad\square$

The following known result serves as a vehicle for us to compute the forward and backward reachability sets, which play a vital role in using the valuation method as our earlier theorems show.

Lemma 3.8 (Howell et al. [3]). *Given a conflict-free PN* $\mathscr{P} = (P, T, \varphi)$, *we can construct in nondeterministic polynomial time a system of linear inequalities* $\mathscr{L}(\mathscr{P}, \mu_0, \mu)$ *in such a way that* $\mu \in R(\mathscr{P}, \mu_0)$ *iff* $\mathscr{L}(\mathscr{P}, \mu_0, \mu)$ *has an integer solution. Furthermore,* $\mathscr{L}(\mathscr{P}, \mu_0, \mu)$ *remains linear even if* μ_0 *and* μ *are replaced by variables.* (*The reader is referred to Lemma 4.3 in* [3] *for a detailed description of the system of linear inequalities associated with* $\mathscr{L}(\mathscr{P}, \mu_0, \mu)$.)

What Lemma 3.8 says is that checking reachability for conflict-free PNs can be equated with solving the integer linear programming problem, which is known to be in NP. It is important to point out that, as μ_0 and μ can be regarded as variables, the forward and backward reachability sets are readily expressible in terms of integer linear programming.

Theorems 3.2–3.7, in conjunction with Lemma 3.8, immediately yield the following result.

Theorem 3.9. *Given a conflict-free PN* $\mathscr{P}$ *and a forward-closed set* S *expressible in integer linear programming, the following sets are computable:* $\mathrm{DL}(\mathscr{P})$, $\mathrm{FNT}(\mathscr{P}, S)$, $\mathrm{HS}(\mathscr{P}, \mu)$, $\mathrm{SS}(\mathscr{P}, \mu_0)$ (*assuming* $\mathscr{P}$ *satisfies the condition stated in Theorem* 3.4), $\mathrm{FSS}(\mathscr{P}, \mu_0)$, *and* $\mathrm{FC}(\mathscr{P}, S)$.

In our future study, it is of interest to investigate potential applications (not limited to conflict-free Petri nets) of our valuation-based methodology. As a step in that direction, consider the *forbidden state problem* in supervisory control. Consider a k-place controlled PN $\mathscr{P}$ with its transition set partitioned as T_u and T_c. Let μ_0 be the initial marking and S ($\subseteq N^k$) be the set of *forbidden markings*. The *forbidden state problem* is to determine whether there exists a control policy such that none of the computations of $\mathscr{P}$ from μ_0 ever encounters a state in S. Recall that a control policy is a mapping from N^k to 2^{T_c}. A control policy h is said to be *live* provided that for every marking μ, if all the enabled transitions at μ are controllable, then $h(\mu) \neq \emptyset$. What it says is that the control policy is not allowed to turn μ into a dead making by disabling all potentially fireable controllable transitions. Now we consider the following slightly generalized forbidden state problem of computing $\mathrm{FSP}(\mathscr{P}, S) = \{\mu|$ there exists a *live* control policy such that from μ, none of $\mathscr{P}$'s computations reaches a state in $S\}$. In what follows, we demonstrate how an idea similar to our valuation-based approach is applicable to computing $\mathrm{FSP}(\mathscr{P}, S)$.

We partition N^k into a sequence of (possibly infinite) disjoint sets of markings $U_0, U_1, \ldots,$ and $(N^k - \bigcup_{i \geqslant 0} U_i)$ such that

(1) $U_0 = S$, and
(2) $\forall 1 \leqslant i$, $\mu \in U_i$ iff there exist a marking μ' and a $\sigma \in T_u^*$ such that
    (a) $\mu \xrightarrow{\sigma} \mu'$,
    (b) $\forall t$ enabled at μ', $t \in T_c$, and
    (c) if $\mu' \xrightarrow{t} \mu''$ (for some marking μ''), then $\mu'' \in U_j$, for some $j < i$.

In words, from μ' all the outgoing transitions are controllable and each of such transitions leads to a marking in a U_j of a lower index.

Suppose we define a valuation function f to be $f(\mu) = i$, if $\mu \in U_i$; otherwise, $f(\mu) = \infty$. It is not hard to see that under every live control policy, if $f(\mu) = i \ (\neq \infty)$ then there is a computation $\mu \overset{\sigma}{\to} \mu'$, for some $\mu' \in S$, such that along σ the valuation gradually decreases till a marking in S is reached. As a consequence, no live control policy can keep the computation from reaching S should the computation begin at a marking in $\bigcup_{i \geqslant 0} U_i$. With this observation, we can conclude immediately that $\mathrm{FSP}(\mathcal{P}, S) = N^k - \bigcup_{i \geqslant 0} U_i$.

It should, however, be noted that the above strategy is by no means a panacea for solving the forbidden state problem. The partition of N^k into $U_i, i \geqslant 0$ may be infinite and may not even be effectively constructible. A natural question to ask is: are there nontrivial models (of practical interest) for which the partition is guaranteed to be finite and effectively constructible? Another direction of future research is to see whether a *symbolic* approach can be incorporated into the above valuation-based strategy to accelerate the computation of the set FSP in real applications.

Acknowledgements

References

[1] J. Esparza, Decidability and complexity of Petri net problems—an introduction, in: G. Rozenberg, W. Reisig (Eds.), Advances in Petri Nets, Lecture Notes in Computer Science, Vol. 1491, Springer, Berlin, 1998, pp. 374–428.

[2] L. Holloway, B. Krogh, Controlled Petri nets: a tutorial survey, in: G. Cohen, J.-P. Quadrat (Eds.), Discrete Event Systems, Lecture Notes in Control and Information Sciences, Vol. 199, Springer, Berlin, 1994, pp. 158–168.

[3] R. Howell, L. Rosier, H. Yen, Normal and sinkless Petri nets, J. Comput. System Sci. 46 (1993) 1–26.

[4] L. Landweber, E. Robertson, Properties of conflict-free and persistent Petri nets, J. Assoc. Comput. Mach. 25 (3) (1978) 352–364.

[5] T. Murata, Petri nets: properties, analysis and applications, Proc. IEEE 77 (4) (1989) 541–580.

[6] J. Peterson, Petri Net Theory and the Modeling of Systems, Prentice-Hall, Englewood Cliffs, NJ, 1981.

[7] D. Schmidt, Denotational Semantics, Allyn & Bacon, Newton, MA, 1986.

[8] A. Valmari, A stubborn attack on state explosion, Formal Methods System Design 1 (1992) 297–322.