Non-Blockingness Verification of Bounded Petri Nets Using Basis Reachability Graphs

Chao Gu, Ziyue Ma, Zhiwu Li, and Alessandro Giua

Abstract

In this paper, we study the problem of non-blockingness verification by tapping into the basis reachability graph (BRG). Non-blockingness is a property that ensures that all pre-specified tasks can be completed, which is a mandatory requirement during the system design stage. We develop a condition of transition partition of a given net such that the corresponding *conflict-increase BRG* contains sufficient information on verifying non-blockingness of its corresponding Petri net. Thanks to the compactness of the BRG, our approach possesses practical efficiency since the exhaustive enumeration of the state space can be avoided. In particular, our method does not require that the net is deadlock-free.

Index Terms

Petri nets, non-blockingness verification, basis reachability graph.

Published as:

C. Gu, Z. Ma, Z. Li and A. Giua, "Non-blockingness verification of bounded Petri nets using basis reachability graphs," *IEEE Control Systems Letters*, vol. 6, pp. 1220−1225, 2022. DOI: 10.1109/LCSYS.2021.3087937

C. Gu is with the School of Electro-Mechanical Engineering, Xidian University, Xi'an 710071, China, and also with DIEE, University of Cagliari, Cagliari 09124, Italy (e-mail: cgu1992@stu.xidian.edu.cn)

Z. Ma is with the School of Electro-Mechanical Engineering, Xidian University, Xi'an 710071, China (e-mail: maziyue@xidian.edu.cn)

Z. Li is with the School of Electro-Mechanical Engineering, Xidian University, Xi'an 710071, China, and also with the Institute of Systems Engineering, Macau University of Science and Technology, Macau (e-mail: zhwli@xidian.edu.cn)

A. Giua is with DIEE, University of Cagliari, Cagliari 09124, Italy (e-mail: giua@unica.it)

I. Introduction

Discrete event systems (DESs) [9] are *event-driven* systems whose state space can be described as a discrete set. As a mathematical characterization for studying, modelling, and analyzing DES, Petri nets [2], [10] offer various vantages over automata. For instance, states in Petri nets can be represented as vectors, namely *markings*; ergo, techniques such as linear algebra [1] can be applied. On the other hand, structural-based approaches can be adopted to avert exhaustively enumerating the state space, therefore mitigating the *state explosion* problem.

In DESs, *non-blockingness* [17] is a property that ensures that all pre-specified tasks can be completed, which is a mandatory requirement during the system design stage. Given its importance, efficient techniques are desired to verify if a given system is non-blocking. Past works [4], [16] propose several methods to verify the non-blockingness of a given Petri net: these methods are based on the reachability graph (RG) and *theory of regions*. On the other hand, [8] propose methods to synthesize non-blocking enforcing supervisors in some subclasses of Petri nets.

Recently, a *semi-structural* analysis technique in Petri nets, called the *basis reachability analysis*, was proposed [3]. In the basis reachability analysis, only a subset of the reachable markings called *basis markings* is enumerated and an automaton-like structure called *basis reachability graph (BRG)* is constructed. Initially created for *diagnosis* problems [3], basis reachability analysis has been gradually developed and adopted on solving other issues such as *marking reachability* and *opacity* problems, etc.

Although the BRG-based techniques have been proved to be operative and efficient, it is showed that a conventional BRG is, in general, not applicable to tackle the non-blockingness verification problem [6]. The reason is that in a BRG there may exist livelocks among a set of non-basis markings. In such a case, the blocking behavior of the plant net cannot be detected by inspecting the structure of the BRG. To overcome such a problem, in [6], an augmented version of BRGs called *minimax-BRG* is developed. Although the minimax-BRG exhibits practical efficiency in solving the non-blockingness verification problem, unlike the basis-marking-based approach [14], currently, there are no analysis methods for addressing with minimax-BRGs on state estimation and supervisory control problems, in which non-blockingness analysis plays a key role. This motivated us to develop an alternative non-blocking verification method based on the conventional types of BRGs whose analysis methods are relatively mature.

In this paper we introduce a particular type of BRGs called *conflict-increase BRGs* (CI-BRGs) that encode sufficient non-blockingness-related information by referring to a particular partition of the transition set. Differently from the minimax-BRG [6] whose construction has a higher complexity than that of a BRG with the same transition partition, a CI-BRG is identical in essence with BRG. We characterize the main properties of basis markings in CI-BRGs and prove that the non-blockingness of a system can be verified by checking if all basis markings in its corresponding CI-BRG are non-blocking. Although there exist restrictions on obtaining of CI-BRGs, which depend on the system structure and the parameters of the linear constraint that describes the final markings set, thanks to the compactness of BRGs, our approach still achieves practical efficiency compared with the RG-based analysis, according to numerical results.

II. Preliminaries

A. Petri Nets

A Petri net is a four-tuple $N = (P, T, Pre, Post)$, where P is a set of m *places* and T is a set of n *transitions*. $Pre : P \times T \to \mathbb{N}$ and $Post : P \times T \to \mathbb{N}$ ($\mathbb{N} = \{0, 1, 2, \cdots\}$) are the *pre-* and *post- incidence functions* that specify the *arcs* in the net and are

represented as matrices in $\mathbb{N}^{m\times n}$. The *incidence matrix* of N is defined by $C = Post - Pre$. A Petri net is *acyclic* if there are no directed cycles in its underlying digraph.

Given a Petri net $N = (P,T,Pre,Post)$ and a set of transitions $T_x \subseteq T$, the *T_x-induced sub-net* of N is a net resulting by removing all transitions in $T \setminus T_x$ and corresponding arcs from N, denoted as $N_x = (P,T_x,Pre_x,Post_x)$ where $T_x \subseteq T$ and Pre_x ($Post_x$) is the restriction of Pre ($Post$) to P and T_x.

A *marking* M of a Petri net N is a mapping: $P \to \mathbb{N}$ that assigns to each place of a Petri net a non-negative integer number of *tokens*. The number of tokens in a place p at a marking M is denote by $M(p)$. A Petri net N with an initial marking M_0 is called a *marked net*, denoted by $\langle N,M_0\rangle$. For a place $p \in P$, the *set of its input transitions* is defined by ${}^\bullet p = \{t \in T \mid Post(p,t) > 0\}$ and the *set of its output transitions* is defined by $p^\bullet = \{t \in T \mid Pre(p,t) > 0\}$. The notions for ${}^\bullet t$ and $t^\bullet$ are analogously defined. A Petri net $N = (P,T,Pre,Post)$ is *conflict-free* if for all $p \in P$, $|p^\bullet| \leq 1$.

A transition $t \in T$ is *enabled* at a marking M if $M \geq Pre(\cdot,t)$, denoted by $M[t\rangle$; otherwise it is said to be *disabled* at M, denoted as $\neg M[t\rangle$. If t is enabled at M, the *firing* of t yields marking $M' = M + C(\cdot,t)$, which is denoted as $M[t\rangle M'$. A marking M is *dead* if for all $t \in T$, $M \ngeq Pre(\cdot,t)$.

Marking M' is *reachable* from M_1 if there exist a firing sequence of transitions $\sigma = t_1 t_2 \cdots t_n$ and markings $M_2, \cdots, M_n$ such that $M_1[t_1\rangle M_2[t_2\rangle \cdots M_n[t_n\rangle M'$ holds. We denote by T^* the set of all finite sequences of transitions over T. Given a transition sequence $\sigma \in T^*$, $\varphi : T^* \to \mathbb{N}^n$ is a function that associates to σ a vector $\mathbf{y} = \varphi(\sigma) \in \mathbb{N}^n$, called the *firing vector* of σ. Let $\varphi^{-1} : \mathbb{N}^n \to T^*$ be the inverse function of φ, namely for $\mathbf{y} \in \mathbb{N}^n$, $\varphi^{-1}(\mathbf{y}) := \{\sigma \in T^* | \varphi(\sigma) = \mathbf{y}\}$. The set of markings reachable from M_0 is called the *reachability set* of $\langle N,M_0\rangle$, denoted by $R(N,M_0)$. A marked net $\langle N,M_0\rangle$ is said to be *bounded* if there exists an integer $k \in \mathbb{N}$ such that for all $M \in R(N,M_0)$ and for all $p \in P$, $M(p) \leq k$ holds.

Proposition 1: [13] Given an acyclic net N, markings $M,M' \in \mathbb{N}^m$, and a firing vector $\mathbf{y} \in \mathbb{N}^n$, the following holds:

$M' = M + C \cdot \mathbf{y} \geq \mathbf{0} \Leftrightarrow (\exists \sigma \in \varphi^{-1}(\mathbf{y}))\ M[\sigma\rangle M'$. □

Let $G = (N,M_0,\mathscr{F})$ denote a *plant* consisting of a marked net and a finite set of final markings $\mathscr{F} \subseteq R(N,M_0)$. Instead of explicitly listing all the elements in $\mathscr{F}$, as a general form, in this paper, we characterize set $\mathscr{F}$ as a linear constraints namely *generalized mutual exclusion constraints* (GMECs) [5]. A GMEC is a pair $(\mathbf{w},k)$, where $\mathbf{w} \in \mathbb{Z}^m$ and $k \in \mathbb{Z}$ ($\mathbb{Z}$ is the set of integers), that defines a set of markings $\mathscr{L}_{(\mathbf{w},k)} = \{M \in \mathbb{N}^m | \mathbf{w}^T \cdot M \leq k\}$.

Definition 1: A marking $M \in R(N,M_0)$ of a plant $G = (N,M_0,\mathscr{F})$ is *blocking* if $R(N,M) \cap \mathscr{F} = \emptyset$; otherwise M is *non-blocking*. Plant G is *non-blocking* if all reachable markings are non-blocking; otherwise G is *blocking*. ♢

B. Basis Marking and Basis Reachability Graph

Given a Petri net $N = (P,T,Pre,Post)$, transition set T can be partitioned into $T = T_E \cup T_I$ where the sets T_E and T_I are called the *explicit* transition set and the *implicit* transition set, respectively.

A pair $\pi = (T_E,T_I)$ is called a *basis partition* [12] of T if (i) $T_E \cup T_I = T$, $T_E \cap T_I = \emptyset$; (ii) the T_I-induced subnet is acyclic. We denote $|T_E| = n_E$, $|T_I| = n_I$, and C_I be the incidence matrix of the T_I-induced subnet. Note that in a BRG with basis partition (T_E,T_I), the firing of explicit transitions in T_E is explicitly represented in the BRG, while the firing of implicit transitions in T_I is abstracted. Note that no physical meaning needs to be associated with implicit transitions: the set T_I can be arbitrarily selected, provided that the T_I-induced subnet is acyclic.

Definition 2: Given a Petri net $N = (P,T,\mathrm{Pre},\mathrm{Post})$, a basis partition $\pi = (T_E,T_I)$, a marking M, and a transition $t \in T_E$, we define $\Sigma(M,t) = \{\sigma \in T_I^* | M[\sigma\rangle M', M' \geq \mathrm{Pre}(\cdot,t)\}$ as the set of *explanations* of t at M, and $Y(M,t) = \{\varphi(\sigma) \in \mathbb{N}^{n_I} | \sigma \in \Sigma(M,t)\}$ as the set of *explanation vectors*; meanwhile we define $\Sigma_{\min}(M,t) = \{\sigma \in \Sigma(M,t) | \nexists \sigma' \in \Sigma(M,t) : \varphi(\sigma') \lneq \varphi(\sigma)\}$ as the set of

minimal explanations of t at M, and $Y_{\min}(M,t) = \{\varphi(\sigma) \in \mathbb{N}^{n_I} | \sigma \in \Sigma_{\min}(M,t)\}$ as the corresponding set of *minimal explanation vectors*. ♢

Definition 3: Given a bounded marked net $\langle N, M_0 \rangle$ with a basis partition $\pi = (T_E, T_I)$, its *basis reachability graph* (BRG) is a deterministic automaton $\mathscr{B}$ output by Algorithm 2 in [12]. The BRG $\mathscr{B}$ is a quadruple $(\mathscr{M}_{\mathscr{B}}, \mathrm{Tr}, \Delta, M_0)$, where the state set $\mathscr{M}_{\mathscr{B}}$ is the set of basis markings, the event set Tr is the set of pairs $(t,y) \in T_E \times \mathbb{N}^{n_I}$, the transition relation $\Delta = \{(M_1,(t,y),M_2) | t \in T_E, y \in Y_{\min}(M_1,t), M_2 = M_1 + C_I \cdot y + C(\cdot,t)\}$, and the initial state is the initial marking M_0. ♢

The set $Y_{\min}(M,t)$ and the BRG can be computed using Algorithms 1 and 2 in [12], respectively. We extend the definition of transition relation to consider sequence of pairs $\sigma \in \mathrm{Tr}^*$ and write $M_1 \xrightarrow{\sigma} M_2$ to denote that from M_1 sequence σ yields M_2.

Note that the upper bound of states in a BRG is the size of the reachability space of a net. However, many BRG-related work [3], [12] have shown that in practical cases a BRG can be much smaller than the corresponding reachability space, i.e., $|\mathscr{M}_{\mathscr{B}}| \ll |R(N,M_0)|$ holds. Besides, in some cases, a BRG may grow much slower than the reachability space of a net. For instance, [15] shows an example in which the number of states in a Petri net grows cubically (i.e., $O(k^3)$) when the initial marking increases, while the corresponding BRG growth linearly (i.e., $O(k)$). Therefore, the construction of the BRG achieves practical efficiency.

Definition 4: Given a marked net $\langle N, M_0 \rangle$, a basis partition $\pi = (T_E, T_I)$, and a basis marking $M_b \in \mathscr{M}_{\mathscr{B}}$, we define $R_I(M_b)$ the *implicit reach* of M_b as:

$$R_I(M_b) = \{M \in \mathbb{N}^m | (\exists \sigma \in T_I^*)\, M_b[\sigma\rangle M\}.$$ ♢

Since the T_I-induced subnet is acyclic, we have:

$$R_I(M_b) = \{M \in \mathbb{N}^m | (y_I \in \mathbb{N}^{n_I})\, M = M_b + C_I \cdot y_I\}.$$

Proposition 2: [12] Given a marked net $\langle N, M_0 \rangle$ with a basis partition $\pi = (T_E, T_I)$, the set of basis markings of the system is $\mathscr{M}_{\mathscr{B}}$. Consider a marking $M \in \mathbb{N}^m$. $M \in R(N,M_0)$ if and only if there exists a basis marking $M_b \in \mathscr{M}_{\mathscr{B}}$ such that $M \in R_I(M_b)$.□

III. Non-Blockingness Verification Using Conflict-Increase BRGs

Given a plant net, in general there exist several valid basis partitions, each of which leads to a different BRG. According to Example 1 presented in [6], a BRG constructed with a randomly selected basis partition may not encode all information needed to test if a plant is non-blocking. The reason lies in the fact that in a BRG there may exist some *livelocks* among a set of non-basis markings; thus, the blocking behavior of the plant net cannot be detected by checking the structure of the BRG.

A. Conflict-Increase BRGs

In this part, we show how a BRG corresponding to a suitable basis partition may allow one to verify non-blockingness. For a given plant, we first introduce the notion of *conflict-increase BRGs* (CI-BRGs).

Definition 5: Consider a plant $G = (N, M_0, \mathscr{F})$ with $N = (P, T, Pre, Post)$ and $\mathscr{F} = \mathscr{L}_{(\mathbf{w},k)}$. A transition set $T' \subseteq T$ is said to be *non-conflicting* if $T' \subseteq T \setminus T_{conf}$, where

$$T_{conf} = \{t \in T \mid (\exists p \in P) t \in p^\bullet, |p^\bullet| \geq 2\}; \tag{1}$$

it is said to be *non-increasing* if $T' \subseteq T \setminus T_{inc}$, where

$$T_{inc} = \{t \in T \mid \mathbf{w}^T \cdot C(\cdot,t) > 0\}. \tag{2}$$

According to Definition 5, a transition set is non-conflicting and non-increasing if it does not contain two types of transitions:

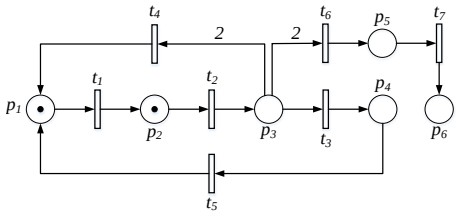

Fig. 1: A plant $G = (N, M_0, \mathscr{F})$.

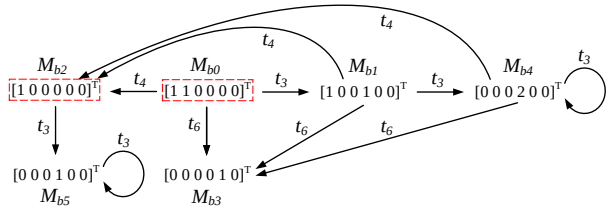

Fig. 2: The CI-BRG $\mathscr{B}$ with respect to $T_E = \{t_3, t_4, t_6\}$. For readability, explanation vectors are not shown.

(1) T_{conf} — all transitions that are in structural conflicts (depends only on the structure of the net);

(2) T_{inc} — all transitions whose influence on $(\mathbf{w}, k)$ are positive (depends only on the corresponding GMEC), i.e., at a marking M, by firing a transition $t \in T_{inc}$, the token count of the obtained marking $M' = M + C(\cdot, t)$ will be increased in terms of the corresponding GMEC since $\mathbf{w}^T \cdot C(\cdot, t) > 0$.

Definition 6: Consider a plant $G = (N, M_0, \mathscr{F})$ with $N = (P, T, Pre, Post)$ and $\mathscr{F} = \mathscr{L}_{(\mathbf{w},k)}$. The BRG corresponding to partition $\pi = (T_E, T_I)$ is called a *conflict-increase BRG* (CI-BRG) if T_I is non-conflicting and non-increasing. ♢

Note that to construct a CI-BRG, the corresponding implicit transition set T_I in $\pi = (T_E, T_I)$ should be both non-conflicting and non-increasing. In addition to that, some other transitions (if necessary) may also need to be eliminated in T_I to ensure the acyclicity of the T_I-induced subnet of G. For a bounded plant, there always exists a CI-BRG (e.g., the BRG with respect to $T_E = T$ and $T_I = \emptyset$). Since CI-BRG is a particular type of BRG, it can be computed by Algorithm 2 in [12] and the complexity analysis of the BRG (described in Section II-B) also applies to the CI-BRG.

On the other hand, in the previous works [3], [12], it is often preferred to choose a basis partition π with a T_I that is maximal (in the sense of set containment) since the size of its corresponding BRG is relatively small. Here, a non-conflicting and non-increasing T_I may not be maximal, therefore the corresponding CI-BRG may not be minimal as well. However, as a trade-off, we show hereinafter that necessary information regarding non-blockingness will be appropriately encoded in CI-BRGs and the non-blockingness verification procedure can be therefore facilitated. Moreover, as shown by simulations in Section IV, a CI-BRG is still significantly smaller than the corresponding RG in size.

Example 1: Consider a plant $G = (N, M_0, \mathscr{F})$ in Fig. 1. Let $\mathscr{F} = \mathscr{L}_{(\mathbf{w},k)}$ where $\mathbf{w} = [0\ 0\ 0\ 1\ 1\ 1]^T$ and $k = 0$. In this plant, $T_{conf} = \{t_3, t_4, t_6\}$ and $T_{inc} = \{t_3, t_6\}$; thus, $T_{conf} \cup T_{inc} = \{t_3, t_4, t_6\}$. Notice that the subnet induced by $T \setminus \{t_3, t_4, t_6\} = \{t_1, t_2, t_5, t_7\}$ is acyclic. Ergo, to construct a CI-BRG, we can choose the set of implicit transitions $T_I = \{t_1, t_2, t_5, t_7\}$ that is non-conflicting and non-increasing, which leads to $T_E = \{t_3, t_4, t_6\}$. According to Definition 4 in [12], $M_{b0} = M_0$ is a basis marking. Next, we compute the minimal explanation vectors of all explicit transitions (i.e., t_3, t_4, and t_6) at M_{b0} and derive the other basis markings. For instance, for t_3, $\mathbf{y}_{min} = [0\ 1\ 0\ 0]^T$. Since $M_{b1} = M_{b0} + C_I \cdot \mathbf{y}_{min} + C(\cdot, t_3) = [1\ 0\ 0\ 1\ 0\ 0]^T \neq M_{b0}$, let M_{b1} be another basis marking. Analogously, the corresponding CI-BRG $\mathscr{B}$ can be constructed and is shown in Fig. 2. Meanwhile, the basis markings that are also final (i.e., M_{b0} and M_{b2}) in $\mathscr{B}$ are boxed with red dashed lines. ♢

B. Properties of CI-BRGs

In this subsection we prove a series of results on the properties of CI-BRGs. These results will be eventually used to establish our non-blocking verification algorithm. Before delving into the mathematical details, we note that here we do *not* assume that the net is deadlock-free: the results presented in this subsection hold for both deadlock-free nets and nets with deadlocks. The cases of non-deadlock-free nets will be further discussed in the next subsection.

First, the following proposition shows that for any basis marking M_b, if an explicit transition t is enabled by firing a minimal explanation from M_b, then t remains enabled when any other implicit transitions fires.

Proposition 3: Given a plant $G = (N, M_0, \mathscr{F})$ with $\mathscr{F} = \mathscr{L}_{(\mathbf{w},k)}$, let $\mathscr{B}$ be its CI-BRG with respect to $\pi = (T_E, T_I)$. Let $\mathbf{y}_{min} \in Y_{min}(M_b, t)$ be a minimal explanation vector of explicit transition t at M_b. For any implicit firing vector $\mathbf{y} \geq \mathbf{y}_{min}$, $M_b + C_I \cdot \mathbf{y} = M \geq \mathbf{0}$ implies $M[t\rangle$.

Proof: According to Proposition 1, there exists $\sigma_{min} \in T_I^*$ such that $M_b[\sigma_{min}\rangle M_{min} \geq \mathbf{0}$ where $\varphi(\sigma_{min}) = \mathbf{y}_{min}$. Since $\mathbf{y}_{min} \leq \mathbf{y}$, the trajectory $M_b[\sigma_{min}\rangle M_{min}[\sigma'\rangle M$ is feasible, where $\varphi(\sigma') = \mathbf{y} - \mathbf{y}_{min}$. By Eq. (1), in G no implicit transition shares any input place with transition t. Hence, once t is enabled at M_{min}, it remains enabled regardless other implicit transitions fire, which implies $M[t\rangle$. ■

Next, we define the concept of *maximal implicit firing vector* and *i-maximal marking* as follows.

Definition 7: Given a plant $G = (N, M_0, \mathscr{F})$ with $\mathscr{F} = \mathscr{L}_{(\mathbf{w},k)}$, let $\mathscr{B}$ be its CI-BRG with $\pi = (T_E, T_I)$. At a basis marking M_b in $\mathscr{B}$, an implicit firing vector (IFV) $\mathbf{y} \in \mathbb{N}^{n_I}$ is said to be *maximal* if there exists a firing sequence $\sigma \in T_I^*, \sigma \in \varphi^{-1}(\mathbf{y})$ such that $M_b[\sigma\rangle$ and there does not exist any other $\sigma' \in T_I^*, \varphi(\sigma) \gneq \mathbf{y}$ such that $M_b[\sigma\rangle M$. A marking $M_{\max}$ is said to be *i-maximal* at M_b if there exists a maximal IFV $\mathbf{y}$ such that $M_b + C_I \cdot \mathbf{y} = M_{\max}$. ♢

Further, we show in Proposition 4 that, in a CI-BRG, for any basis marking there exists a unique maximal IFV and a unique i-maximal marking.

Proposition 4: Given a marked net $\langle N, M_0\rangle$, let $\mathscr{B}$ be its BRG with respect to $\pi = (T_E, T_I)$ where the T_I-induced subnet of N is acyclic and conflict-free. At any basis marking M_b in $\mathscr{B}$, there exists a unique maximal IFV $\mathbf{y}$.

Proof: By contradiction, suppose that at M_b there exist two different maximal IFVs $\mathbf{y}_1, \mathbf{y}_2$. Since the T_I-induced subnet is acyclic, there exist two firing sequences $\sigma_1 = t_{i_1}^{k_1} \cdots t_{i_n}^{k_n}, \sigma_2 = t_{i_1}^{k'_1} \cdots t_{i_n}^{k'_n}$ corresponding to $\mathbf{y}_1, \mathbf{y}_2$, respectively, in which t_{i_j}'s are sorted from upstream to downstream of the T_I-induced subnet. Since $\mathbf{y}_1 \neq \mathbf{y}_2$, there exists a minimal j such that $k_j \neq k'_j$ and for all $j' < j$, $k_j = k'_{j'}$. Without loss of generality, suppose that $k_j < k'_j$. Consider $\bar{\sigma}_1 = t_{i_1}^{k_1} \cdots t_{i_{j-1}}^{k_{j-1}} t_{i_j}^{k_j}$ that is a prefix of σ_1. Since $t_{i_1}^{k_1} \cdots t_{i_{j-1}}^{k_{j-1}} t_{i_j}^{k'_j}$ is a prefix of σ_2, transition t_{i_j} can fire at least once after $\bar{\sigma}_1$. Moreover, since the transitions in σ_1 appear from upstream to downstream and the T_I-induced subnet is conflict-free, the firing of t_{i_j} after $\bar{\sigma}_1$ does not affect the firing of the rest of transitions in σ_1, which implies that sequence $t_{i_1}^{k_1} \cdots t_{i_j}^{k_j+1} \cdots t_{i_n}^{k_n}$ is firable at M_b. This means that $\mathbf{y}_1$ is not a maximal IFV. ■

According to Proposition 4, in a CI-BRG each basis marking has a unique i-maximal marking. In the sequel, for each basis marking M_b we denote its i-maximal marking as $M_{b,max}$. From Propositions 3 and 4 we immediately have the following Proposition.

Proposition 5: Given a marked net $\langle N, M_0\rangle$ with $N = (P, T, Pre, Post)$, let $\mathscr{B}$ be its BRG with respect to $\pi = (T_E, T_I)$ where T_I is non-conflicting. For any basis marking M_b in $\mathscr{B}$, it holds that

$$M_b[\sigma_{min} t\rangle \Rightarrow M_{b,\max}[t\rangle,$$

where $t \in T_E$, $\sigma_{min} \in \Sigma_{min}(M_b, t)$, and $M_{b,\max}$ is an i-maximal marking at M_b.

Proof: Since T_I is non-conflicting, any transition $t \in T_E$ is not in conflict with transitions in T_I. Also, the fact that $M_{b,\max}$ is an i-maximal marking at M_b implies that there exists a maximal IFV $\mathbf{y} \in \mathbb{N}^{n_I}$ at M_b such that $M_b + C_I \cdot \mathbf{y} = M_{b,\max}$ holds. Thus, this statement follows Proposition 3, since $\mathbf{y} \geq \varphi(\sigma_{min})$ by Definition 7. ■

Next, we show in Proposition 6 that in a CI-BRG, for any marking M in the implicit reach of M_b, there necessarily exists a firing sequence consisting of implicit transitions σ in T_I^* such that $M[\sigma\rangle M_{b,\max}$.

Proposition 6: Given a plant $G = (N, M_0, \mathscr{F})$ with $N = (P, T, Pre, Post)$ and $\mathscr{F} = \mathscr{L}_{(\mathbf{w},k)}$, let $\mathscr{B}$ be its CI-BRG with respect to $\pi = (T_E, T_I)$. Given a basis marking M_b and its i-maximal marking $M_{b,\max} \in R_I(M_b)$, the following holds:

$$(\forall M \in R_I(M_b), \exists \sigma \in T_I^*)\ M[\sigma\rangle M_{b,\max}.$$

Proof: Consider trajectories $M_b[\sigma_I\rangle M$ and $M_b[\sigma_{max}\rangle M_{b,\max}$, where $\varphi(\sigma_{max}) = \mathbf{y}_{max} \in \mathbb{N}^{n_I}$ is the unique maximal IFV at M_b and $\varphi(\sigma_I) = \mathbf{y}_I \in \mathbb{N}^{n_I}$. Since $M = M_b + C_I \cdot \mathbf{y}_I \geq \mathbf{0}$ and $M_{b,\max} = M_b + C_I \cdot \mathbf{y}_{max} \geq \mathbf{0}$, it holds that $M_{b,\max} = M + C_I \cdot (\mathbf{y}_{max} - \mathbf{y}_I)$. Since $\mathbf{y}_{max} \geq \mathbf{y}_I$ (according to Definition 7), based on Proposition 1, there must exists a firing sequence $\sigma \in T_I^*$ such that $M[\sigma\rangle M_{b,\max}$ where $\varphi(\sigma) = \mathbf{y}_{max} - \mathbf{y}_I$. ■

The next proposition shows that in a CI-BRG, the implicit reach of any basis marking M_b contains at least one final marking (i.e., $R_I(M_b) \cap \mathscr{F} \neq \emptyset$) if and only if the i-maximal marking of M_b is a final marking (i.e., $M_{b,\max} \in \mathscr{F}$).

Proposition 7: Given a plant $G = (N, M_0, \mathscr{F})$ with $N = (P, T, Pre, Post)$ and $\mathscr{F} = \mathscr{L}_{(\mathbf{w},k)}$, let $\mathscr{B}$ be its CI-BRG with respect to $\pi = (T_E, T_I)$. For any basis marking M_b and its i-maximal marking $M_{b,\max} \in R_I(M_b)$, $R_I(M_b) \cap \mathscr{F} \neq \emptyset$ if and only if $M_{b,\max} \in \mathscr{F}$.

Proof: (if) This part holds since $M_{b,\max} \in R_I(M_b) \cap \mathscr{F}$.

(only if) Suppose that $M_{b,\max} \notin \mathscr{F}$, i.e., $\mathbf{w}^T \cdot M_{b,\max} > k$. Notice that $M_{b,\max} = M_b + C_I \cdot \mathbf{y}_{max}$ where $\mathbf{y}_{max} \in \mathbb{N}^{n_I}$ is the maximal IFV at M_b. Since by Eq. (2), $\mathbf{w}^T \cdot C(\cdot, t) \leq 0$ holds for all $t \in T_I$, we can conclude that for any $M \in R_I(M_b)$ such that $M = M_b + C_I \cdot \mathbf{y}$, $\mathbf{y} \leq \mathbf{y}_{max}$ holds. Therefore we have:

$$\begin{aligned} \mathbf{w}^T \cdot M = \mathbf{w}^T \cdot M_b + \mathbf{w}^T \cdot C_I \cdot \mathbf{y} &\geq \mathbf{w}^T \cdot M_b + \mathbf{w}^T \cdot C_I \cdot \mathbf{y}_{max} \\ &= \mathbf{w}^T \cdot M_{b,\max} > k. \end{aligned}$$

Therefore $R_I(M_b) \cap \mathscr{F} = \emptyset$. ■

Intuitively speaking, since the firing of T_I does not increase (and possibly decreases) the token count of $(\mathbf{w}, k)$, the token count at any marking in $R_I(M_b)$ is not less than that of $M_{b,\max}$ (which is reached by firing the maximal number of T_I transitions from M_b). Hence, if the token count of $(\mathbf{w}, k)$ at $M_{b,\max}$ exceeds k, then the token count at any other marking in $R_I(M_b)$ also exceeds k.

Finally, we are ready to present the main result of this work. The following theorem provides a necessary and sufficient condition for the non-blockingness verification.

Theorem 1: Given a plant $G = (N, M_0, \mathscr{F})$ with $N = (P, T, Pre, Post)$ and $\mathscr{F} = \mathscr{L}_{(\mathbf{w},k)}$, let $\mathscr{B}$ be its CI-BRG with respect to $\pi = (T_E, T_I)$. System G is non-blocking if and only if for any basis marking M_b in $\mathscr{B}$, there exists a basis marking M_b' accessible from M_b and $R_I(M_b') \cap \mathscr{F} \neq \emptyset$.

Proof: (only if) Suppose that G is non-blocking. For any basis marking M_b in $\mathscr{B}$, there exists a sequence σ such that $M_b[\sigma\rangle M \in \mathscr{F}$. We write $\sigma = \sigma_1 t_{i_1} \cdots \sigma_n t_{i_n} \sigma_{n+1}$ where all $\sigma_i \in T_I^*, t_{i_j} \in T_E, j = 1, \ldots, n$. Following the procedure in the proof of Theorem 3.8 in [3], we can repeatedly move transitions in each σ_j ($j \in \{1, \ldots, n\}$) to somewhere after t_{i_j} to obtain a new sequence $\sigma_{min,1} t_{i_1} \sigma_{min,2} t_{i_2} \cdots \sigma_{min,n} t_{i_n} \sigma'_{n+1}$ such that

$$M_b[\sigma_{min,1} t_{i_1}\rangle M_{b,1}[\sigma_{min,2} t_{i_2}\rangle \cdots [\sigma_{min,n} t_{i_n}\rangle M_{b,n}[\sigma'_{n+1}\rangle M$$

where each $\sigma_{\min,j}$ is a minimal explanation of t_{i_j} at $M_{b,j}$ for $j = 1,\ldots n$. Hence, basis marking M'_b is accessible from M_b, and $M \in R_I(M'_b)$ holds.

(if) Let $M_{b,0}$ be an arbitrary basis marking and M be an arbitrary marking in $R_I(M_{b,0})$. Suppose that in $\mathscr{B}$ there exists a basis marking $M_{b,n}$ accessible from $M_{b,0}$, i.e.,

$$M_{b,0} \xrightarrow{(t_{i_1},\mathbf{y}_{min,1})} M_{b,1} \xrightarrow{(t_{i_2},\mathbf{y}_{min,2})} M_{b,2} \cdots \xrightarrow{(t_{i_n},\mathbf{y}_{min,n})} M_{b,n},$$

where $R_I(M_{b,n}) \cap \mathscr{F} \neq \emptyset$. By Proposition 6, $M_{j,\max}[t_{i_j}\rangle$ holds where $M_{j,\max}$ is the i-maximal marking at $M_{b,j}$ $(j \in \{1,2,\ldots,n\})$. Now we prove that from M there exists a firing sequence that reaches $M_{n,\max}$. We use $M \to M'$ to denote that there exists sequence σ such that $M[\sigma\rangle M'$.

By Proposition 6, it holds that $M \to M_{0,\max}$. By Proposition 3, $M_{0,\max}[t_{i_1}\rangle M_1$ where $M_1 \in R_I(M_{b,1})$. By regarding $M_{b,1}$ and M_1 as the original $M_{b,0}$ and M, respectively, the above reasoning can be repeatedly applied. Hence, the following trajectory is feasible:

$$M \to M_{0,\max} \to M_1 \to M_{1,\max} \to \cdots \to M_n \to M_{n,\max}$$

where $M_j \in R_I(M_{b,j})$ $(j \in \{1,2,\ldots,n\})$. By Proposition 7, $M_{n,\max} \in \mathscr{F}$ holds. Therefore, G is non-blocking. ■

Theorem 1 indicates that the non-blockingness of a plant G can be verified by checking if all basis markings in the CI-BRG are accessible to some basis markings whose implicit reach contains final markings. By Proposition 7, to check $R_I(M_b) \cap \mathscr{F} \neq \emptyset$ it suffices to test if the i-maximal marking $M_{b,\max}$ is final. This can be done by solving the following *integer linear programming problem* (ILPP) for all M_b in $\mathscr{B}$:

$$\begin{cases} \max & \mathbf{1}^T \cdot \mathbf{y}_I \\ s.t. & M_b + C_I \cdot \mathbf{y}_I = M_{b,max} \\ & \mathbf{w}^T \cdot M_{b,max} \leq k \\ & M_{b,max} \in \mathbb{N}^m \\ & \mathbf{y}_I \in \mathbb{N}^{n_I} \end{cases} \tag{3}$$

Note that the final marking set $\mathscr{F}$ can be further generalized to the conjunction of a finite number of GMECs (namely an *AND-GMEC*) or the union of a finite number of GMECs (namely an *OR-GMEC*). See Discussion 1 in [7] for details.

C. Non-blockingness Verification in Non-deadlock-free Nets

As we mentioned, Theorem 1 does not require G to be deadlock-free. In this subsection, we discuss the reason behind it. The following result shows that if G is not deadlock-free, all dead markings are exactly the i-maximal markings of some basis markings in the CI-BRG. We denote by $\mathscr{D}$ the set of dead markings in $R(N,M_0)$, i.e., $\mathscr{D} = \{M \in R(N,M_0) \mid (\forall t \in T)\neg M[t\rangle\}$.

Proposition 8: Given a plant $G = (N,M_0,\mathscr{F})$ with $\mathscr{F} = \mathscr{L}_{(\mathbf{w},k)}$, let $\mathscr{B}$ be its CI-BRG with respect to $\pi = (T_E,T_I)$. For any basis marking M_b in $\mathscr{B}$ such that $R_I(M_b) \cap \mathscr{D} \neq \emptyset$, $R_I(M_b) \cap \mathscr{D} = \{M_{b,\max}\}$ holds.

Proof: The "if" trivially holds. For the "only if" part, suppose that $R_I(M_b) \cap \mathscr{D} \neq \emptyset$. By Proposition 4, all markings $M \in R_I(M_b)$ are coreachable to $M_{b,\max}$, which indicates that all $M \in R_I(M_b) \setminus \{M_{b,\max}\}$ are not dead. Therefore, the only dead marking in $R_I(M_b) \cap \mathscr{D} \neq \emptyset$ is $M_{b,\max}$. ■

Notice that $R(N,M_0) = \bigcap_{M_b \in \mathscr{B}} R_I(M_b)$. Proposition 8 indicates that all dead markings in $R(N,M_0)$ are $M_{b,\max}$. Note that we do not need to explicitly compute all the i-maximal markings thanks to the following proposition.

Proposition 9: Given a plant $G = (N,M_0,\mathscr{F})$ with $\mathscr{F} = \mathscr{L}_{(\mathbf{w},k)}$, let $\mathscr{B}$ be its CI-BRG with respect to $\pi = (T_E,T_I)$. For any basis marking M_b in $\mathscr{B}$, $R_I(M_b) \cap \mathscr{D} \neq \emptyset$ if and only if M_b does not have any outbound arc in $\mathscr{B}$.

Proof: (only if) By contrapositive. Suppose that M_b has an outbound arc labeled by $(t,\mathbf{y})$. It indicates that there exists a sequence σ whose firing vector is $\varphi(\sigma)=\mathbf{y}$ such that $M_b[\sigma\rangle M[t\rangle$. By Propositions 3 and 4, $M_b[\sigma\rangle M[\sigma'\rangle M_{b,\max}[t\rangle$ holds, which means that t is enabled at the i-maximal marking $M_{b,\max}$, i.e., $M_{b,\max}$ is not dead. By Proposition 8, $R_I(M_b)\cap\mathscr{D}=\emptyset$ holds.

(if) Suppose that M_b does not have any outbound arc. This implies that from M_b no explicit transition can fire any more. Since the T_I-induced subnet is acyclic, the number of implicit transitions firable from M_b is bounded, which implies that $M_{b,max}\in R_I(M_b)$ is dead. ■

Corollary 1: In a CI-BRG, if the i-maximal marking $M_{b,\max}$ of a basis marking M_b is dead and not final, then M_b is not accessible to any M'_b such that $R_I(M'_b)\cap\mathscr{F}\neq\emptyset$.

Proof: This corollary holds since M_b has no outbound arc (Proposition 9) and $R_I(M_b)\cap\mathscr{F}=\emptyset$ (Proposition 7). ■

One can see that the case in Corollary 1 is included in Theorem 1. Thus, the non-blockingness can be verified by Theorem 1 regardless of the deadlock-freeness of G.

D. Algorithm

Algorithm 1 Non-blockingness Verification Using CI-BRG

Require: A bounded plant $G=(N,M_0,\mathscr{F})$

Ensure: "G is non-blocking" / "G is blocking"

1: Find a basis partition $\pi=(T_E,T_I)$ where T_I is non-conflicting and non-increasing;
2: Construct the CI-BRG $\mathscr{B}=(\mathscr{M}_{\mathscr{B}},\mathrm{Tr},\Delta,M_0)$ of G;
3: $\hat{\mathscr{M}}_{\mathscr{B}}:=\emptyset$;
4: **for all** $M_b\in\mathscr{M}_{\mathscr{B}}$, **do**
5: **if** ILPP (3) has a feasible solution, **then**
6: $\hat{\mathscr{M}}_{\mathscr{B}}:=\hat{\mathscr{M}}_{\mathscr{B}}\cup\{M_b\}$;
7: **end if**
8: **end for**
9: **for all** $M'_b\in\mathscr{M}_{\mathscr{B}}\setminus\hat{\mathscr{M}}_{\mathscr{B}}$, **do**
10: **if** $\nexists\hat{M}_b\in\hat{\mathscr{M}}_{\mathscr{B}}$, $\nexists\sigma\in\mathrm{Tr}^*$ s.t. $M'_b\xrightarrow{\sigma}\hat{M}_b$, **then**
11: Output "G is blocking" and Exit;
12: **else**
13: Continue;
14: **end if**
15: **end for**
16: Output "G is non-blocking" and Exit.

Based on the results we have obtained so far, in this subsection we develop a method to verify non-blockingness of a plant using CI-BRG. In brief, Algorithm 1 consists of two stages:

- Stage (i), steps 1–8: construct the CI-BRG and determine for each basis marking M_b if $R_I(M_b)\cap\mathscr{F}\neq\emptyset$. The latter done by solving ILPP 3 for all basis markings;

TABLE I: Benchmark for the plant in Fig. 3 in [7].

Run	$\lvert R(N,M_0)\rvert$	$\lvert\mathscr{M}_{\mathscr{B}_{\mathscr{M}}}\rvert$	Time (s)	$\lvert\mathscr{M}_{\mathscr{B}}\rvert$	Time (s)	NB?
1	1966	284	2	604	1.7	Yes
2	12577	1341	15	2145	11	Yes
3	76808	5961	179	7718	105	No
4	-[a]	14990	1028	16438	470	No
5	-	26716	3126	26648	1248	Yes
6	-	38551	6697	37118	2492	Yes
7	-	67728	22018	59315	6449	No
8	-	-	-	101420	19491	No

[a]Symbol "-" denotes "no result" since the program does not terminate in 10 hours.

- Stage (ii), steps 9–16: check if any basis marking in $\mathscr{B}$ is co-reachable to at least a basis marking that is coreachable to some final markings, which can be done by applying a search algorithm (e.g., *Dijkstra*) in the underlying digraph of the CI-BRG, whose complexity is polynomial in the size of $\mathscr{B}$.

Proposition 10: Algorithm 1 is correct.

Proof: The set $\hat{\mathscr{M}}_{\mathscr{B}}$ in Algorithm 1 records all basis markings whose i-maximal marking is final. By Theorem 1, the net is blocking if and only if there exists a basis marking inaccessible to any basis marking in $\hat{\mathscr{M}}_{\mathscr{B}}$. This coincide with Algorithm 1 who outputs BLOCKING if and only if such a basis marking is detected in step 10. ■

Example 2: [Ex. 1 cont.] Consider again the plant $G=(N,M_0,\mathscr{F})$ with $\mathscr{F}=\mathscr{L}_{(\mathbf{w},k)}$, $\mathbf{w}=[0\ 0\ 0\ 1\ 1\ 1]^T$, $k=0$ that is described in Example 1. Its CI-BRG $\mathscr{B}$ with respect to $T_E=\{t_3,t_4,t_6\}$ is shown in Fig. 2. By Algorithm 1, we verify if G is non-blocking. First, by solving ILPP (3) for all M_b in $\mathscr{B}$, we conclude that $\hat{\mathscr{M}}_{\mathscr{B}}=\{M_{b0},M_{b1},M_{b2},M_{b4},M_{b5}\}$. Then, by analyzing $\mathscr{B}$, it shows that M_{b3} is not co-reachable to any of the basis marking in $\hat{\mathscr{M}}_{\mathscr{B}}$; thus, the system is blocking. ♢

IV. Simulation Results

We use the parameterized Petri net in Fig. 5 in [2] (which consists of 46 places and 39 transitions) to test the efficiency of our approach. Due to the limit of space, the net is not graphically depicted here. For different values of parameters, the size of the RG ($|R(N,M_0)|$), minimax-BRG ($|\mathscr{M}_{\mathscr{B}_{\mathscr{M}}}|$) [6], and CI-BRG ($|\mathscr{M}_{\mathscr{B}}|$), as well as their computing times are reported in Table I in col. $2-6$. Also, the non-blockingness of each case is reported in col. 7. A detailed analysis of this benchmark can be found in [7]. The results of these benchmark indicates that the CI-BRG-based approach outperforms that of the RG- and minimax-BRG based method in all cases for the plant in [7]. Moreover, in [7], a real-world *Hospital Emergency Service System* model [11] is additionally tested to show the verification procedure in detail.

V. Conclusion

We have developed a novel method for non-blockingness verification in Petri nets. By adopting a basis partition with transition set T_I being non-conflicting and non-increasing, we have proposed a particular type of BRGs called the CI-BRGs. Based on CI-BRGs, we have proposed a necessary and sufficient condition for verifying the non-blockingness of a plant. Our method can be applied to both deadlock-free nets and non-deadlock-free ones. Simulation shows that our approach achieves practical efficiency.

REFERENCES

[1] F. Basile and G. De Tommasi. An algebraic characterization of language-based opacity in labeled Petri nets. *IFAC-PapersOnLine*, 51(7):329–336, 2018.

[2] M. P. Cabasino, A. Giua, M. Pocci, and C. Seatzu. Discrete event diagnosis using labeled Petri nets. an application to manufacturing systems. *Control Engineering Practice*, 19(9):989–1001, 2011.

[3] M. P. Cabasino, A. Giua, and C. Seatzu. Fault detection for discrete event systems using Petri nets with unobservable transitions. *Automatica*, 46(9):1531–1539, 2010.

[4] A. Ghaffari, N. Rezg, and X. L. Xie. Design of a live and maximally permissive Petri net controller using the theory of regions. *IEEE transactions on robotics and automation*, 19(1):137–141, 2003.

[5] A. Giua, F. DiCesare, and M. Silva. Generalized mutual exclusion contraints on nets with uncontrollable transitions. In *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics*, pages 974–979. IEEE, 1992.

[6] C. Gu, Z. Y. Ma, Z. W. Li, and A. Giua. Verification of nonblockingness in bounded Petri nets with minimax basis reachability graphs. *arXiv preprint*, arXiv:2003.14204, 2020.

[7] C. Gu, Z. Y. Ma, Z. W. Li, and A. Giua. Non-blockingness verification of bounded Petri nets using basis reachability graphs — an extended version with benchmarks. *arXiv preprint*, arXiv:2103.02475, 2021.

[8] H. S. Hu, Y. Liu, and M. C. Zhou. Maximally permissive distributed control of large scale automated manufacturing systems modeled with Petri nets. *IEEE Transactions on Control Systems Technology*, 23(5):2026–2034, 2015.

[9] S. Lafortune. Discrete event systems: Modeling, observation, and control. *Annual Review of Control, Robotics, and Autonomous Systems*, 2:141–159, 2019.

[10] D. Lefebvre. Near-optimal scheduling for Petri net models with forbidden markings. *IEEE Transactions on Automatic Control*, 63(8):2550–2557, 2017.

[11] L. Li, M. C. Zhou, T. Guo, Y. H. Gan, and X. Z. Dai. Robust control reconfiguration of resource allocation systems with Petri nets and integer programming. *Automatica*, 50(3):915–923, 2014.

[12] Z. Y. Ma, Y. Tong, Z. W. Li, and A. Giua. Basis marking representation of Petri net reachability spaces and its application to the reachability problem. *IEEE Transactions on Automatic Control*, 62(3):1078–1093, 2016.

[13] T. Murata. Petri nets: Properties, analysis and applications. *Proceedings of the IEEE*, 77(4):541–580, 1989.

[14] Y. Ru, M. P. Cabasino, A. Giua, and C. N. Hadjicostis. Supervisor synthesis for discrete event systems with arbitrary forbidden state specifications. In *Proceedings of the 47th IEEE Conference on Decision and Control*, pages 1048–1053. IEEE, 2008.

[15] Y. Tong, Z. W. Li, C. Seatzu, and A. Giua. Verification of state-based opacity using Petri nets. *IEEE Transactions on Automatic Control*, 62(6):2823–2837, 2016.

[16] M. Uzam. An optimal deadlock prevention policy for flexible manufacturing systems using Petri net models with resources and the theory of regions. *The International Journal of Advanced Manufacturing Technology*, 19(3):192–208, 2002.

[17] X. Yin and S. Lafortune. Synthesis of maximally permissive nonblocking supervisors for the lower bound containment problem. *IEEE Transactions on Automatic Control*, 63(12):4435–4441, 2018.