Basis Coverability Graph for Partially Observable Petri Nets with Application to Diagnosability Analysis

Engel Lefaucheux[a,b], Alessandro Giua[c,d], Carla Seatzu[c]

a. Univ. Rennes, INRIA, Campus Universitaire de Beaulieu, Rennes, France
b. LSV, ENS Paris-Saclay, CNRS, Cachan, France
c. Dept. of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy
d. Aix Marseille Univ, Université de Toulon, CNRS, ENSAM, LSIS, Marseille, France

Abstract. Petri nets have been proposed as a fundamental model for discrete-event systems in a wide variety of applications and have been an asset to reduce the computational complexity involved in solving a series of problems, such as control, state estimation, fault diagnosis, etc. Many of those problems require an analysis of the reachability graph of the Petri net. The basis reachability graph is a condensed version of the reachability graph that was introduced to efficiently solve problems linked to partial observation. It was in particular used for diagnosis which consists in deciding whether some fault events occurred or not in the system, given partial observations on the run of the system. However this method is, with very specific exceptions, limited to bounded Petri nets. In this paper, we introduce the notion of basis coverability graph to remove this requirement. We then establish the relationship between the coverability graph and the basis coverability graph. Finally, we focus on the diagnosability problem: we show how the basis coverability graph can be used to get an efficient algorithm.

Introduction

The *marking reachability problem* is a fundamental problem of Petri nets (PNs) which can be stated as follows: *Given a net system* $\langle N, M_0 \rangle$ *and a marking* M*, determine if* M *belongs to the reachability set* $R(N, M_0)$. It plays an important role since many other properties of interest can be solved by reduction to this problem. The marking reachability problem has been shown to be decidable in [11] and was shown to be EXPSPACE-hard in [15].

In the case of *bounded* PNs, i.e., net systems whose reachability set is finite, a straightforward approach to solve this problem consists in constructing the *reachability graph*, which provides an explicit representation of the net behavior, i.e., its reachability set and the corresponding firing sequences of transitions. However, albeit finite, the reachability graph may have a very large number of nodes due to the so called *state space explosion* that originates from the combinatorial nature of discrete event systems. For this reason, practically efficient approaches, which do not require to generate the full state space, have been

explored. We mention, among others, partial order reduction techniques, such as the general approaches based on stubborn sets [18] and persistent sets [8] or the Petri net approaches based on unfolding [13] and maximal permissive steps [2].

In the case of *unbounded* PNs, whose reachability set is infinite, the authors of [9] have shown that a finite *coverability graph* may be constructed which provides a semi-decision procedure (necessary conditions) for the marking reachability problem. It provides an over-approximation of both the reachability set and the set of firing sequences. As was the case for the reachability graph, this approach is not efficient and improvements to the basic algorithm have later been proposed [14].

Recently some of us have proposed a quite general approach that exploits the notion of *basis marking* to practically reduce the computational complexity of solving the reachability problem for bounded nets. This method has originally been introduced to solve problems of state estimation under partial observation [7] but has later been extended to address fault diagnosis [4], state-based opacity [17] and general reachability problems [10].

The approach in [10] considers a partition of the set of transitions $T = T_e \cup T_i$: T_e is called set of *explicit transitions* and T_i is called set of *implicit transitions*. The main requirement is that the subnet containing only implicit transitions be acyclic. The firing of implicit transitions is abstracted and only the firing of explicit transitions need to be enumerated. The advantage of this technique is that only a subset of the reachability space — i.e., the set of the so-called basis markings — is enumerated. All other markings are reachable from a basis marking by firing only implicit transitions and can be characterized by the integer solutions of a system of linear equations. In a certain sense, this hybrid approach combines a behavioral analysis (limited to the the firing of transitions in T_e) with a structural analysis (which describes the firing of transitions in T_e).

The objective of this paper is mainly to show that the approach of [10] can be generalized to unbounded nets. We define a *basis coverability graph* where the firing of implicit transitions is abstracted, thus reducing the number of nodes of the standard coverability graph. In addition, we show how this approach can be applied to study the *diagnosability* of Petri nets in the logic framework of [16]. Diagnosability is achieved in a system where transitions can be observable or not is one can deduce from the observations that a specified faulty transition was fired. In this case, we consider as implicit the set of unobservable transitions. However, since the firing of unobservable faulty transitions need to be recorded, we further extend the approach of [10] by considering that there may exists a subset of implicit transitions (called *relevant transitions*) which, albeit abstracted, need to be handled with special care. In terms of computational cost, relevant transitions are in between observable and implicit transitions.

The paper is structured as follows. In Section 1, we recall some usual definitions for Petri Nets and their coverability graph. In Section 2, we introduce the notion of basis coverability graph and establish some of its properties. In Section 3 we give the definitions of the diagnosability of a Petri Net. Finally in Section 4 we

study unbounded Petri nets and show how to use the basis coverability graph for the diagnosability analysis.

1 Background on Petri nets and Coverability Graph

1.1 Petri Nets

In this section the formalism used in the paper is recalled. For more details on Petri nets the reader is referred to [12].

Definition 1. *A Petri net (PN) is a structure $N = (P, T, Pre, Post)$, where P is a set of m places; T is a set of n transitions; $Pre : P \times T \to \mathbb{N}$ and $Post : P \times T \to \mathbb{N}$ are the pre– and post– incidence functions that specify the arcs. We also define $C = Post - Pre$ as the incidence matrix of the net.*

A *marking* is a vector $M : P \to \mathbb{N}$ that assigns to each place of a PN a nonnegative integer number of tokens. A *net system* (NS) $\langle N, M_0 \rangle$ is a PN N with an initial marking M_0. A transition t is enabled at M iff $M \geq Pre(\cdot, t)$ and may fire yielding the marking $M' = M + C(\cdot, t)$. One writes $M\ [\sigma\rangle$ to denote that the sequence of transitions $\sigma = t_{j_1} \cdots t_{j_k}$ is enabled at M, and $M\ [\sigma\rangle\ M'$ to denote that the firing of σ yields M'. One writes $t \in \sigma$ to denote that a transition t is contained in σ. The length of the sequence σ (denoted$|\sigma|$) is the number of transitions in the sequence, here k.

The set of all sequences that are enabled at the initial marking M_0 is denoted $L(N, M_0)$, i.e., $L(N, M_0) = \{\sigma \in T^* \mid M_0[\sigma\rangle\}$. Given $k \geq 0$, the set of all sequences of length k is written T^k. A marking M is *reachable* in $\langle N, M_0 \rangle$ iff there exists a firing sequence σ such that $M_0\ [\sigma\rangle\ M$. The set of all markings reachable from M_0 defines the *reachability set* of $\langle N, M_0 \rangle$ and is denoted $R(N, M_0)$.

Let $\pi : T^* \to \mathbb{N}^n$ be the function that associates with the sequence $\sigma \in T^*$ a vector $y \in \mathbb{N}^n$, called the *firing vector* of σ. In particular, $y = \pi(\sigma)$ is such that $y(t) = k$ iff the transition t is contained k times in σ.

A PN having no directed circuits is called *acyclic*. Given $k \in \mathbb{N}$, a place p of an NS $\langle N, M_0 \rangle$ is *k-bounded* if for all $M \in R(N, M_0)$, $M(p) \leq k$. It is bounded if there exists $k \in \mathbb{N}$ such that p is k-bounded. An NS is bounded (resp. k-bounded) iff all of its places are bounded (resp. k-bounded).

A sequence is *repetitive* iff it can be repeated indefinitely (i.e. σ is repetitive in the marking M iff $M[\sigma\rangle M'$ with $M' \geq M$). There are two kinds of repetitive sequences: a repetitive sequence is *stationary* if it does not modify the marking (i.e. $M[\sigma\rangle M$), it is *increasing* otherwise. Remark that an NS containing an increasing sequence can not be bounded.

Example 1. Consider the NS of Figure 1, the sequence t_1, is increasing in the initial marking $M_0 = [2, 0, 0, 0, 0]$. Firing t_1 k times in M_0 leads to the marking $M_1 = [2, k, 0, 0, 0]$. Therefore the place p_2 is not bounded. However, every other place is 2-bounded.

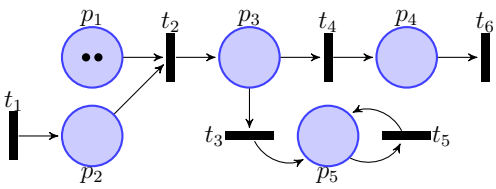

Fig. 1. A net system. Circles are places and rectangles are transitions. In the initial marking, p_1 has two tokens represented by the two black dots.

Definition 2. *Given a net $N = (P, T, Pre, Post)$, and a subset $T' \subseteq T$ of its transitions, let us define the $T'-$*induced subnet of N *as the new net $N' = (P, T', Pre', Post')$ where $Pre', Post'$ are the restrictions of $Pre, Post$ to T'. The net N' can be thought as obtained from N removing all transitions in $T \setminus T'$. Let us also write $N' \prec_{T'} N$.*

1.2 Coverability Graph

For a bounded NS $\langle N, M_0 \rangle$, one can enumerate the elements of the reachability set $R(N, M_0)$ and establish the transition function between the markings. The resulting graph is called *Reachability Graph*. If the NS is not bounded, this construction does not terminate. Instead, an usual method is to build the *Coverability Graph* which is a finite over-approximation of the reachability set and of the net language [9]. We will define in this section the coverability graph of an NS which if the NS is bounded is equal to the reachability graph of this NS.

An ω-marking is a vector from the set of places to $\mathbb{N} \cup \{\omega\}$, where ω should be thought of as "arbitrarily large": for all $k \in \mathbb{N}$, we have $k < \omega$ and $\omega \pm k = \omega$. An ω-marking M is (resp. strictly) covered by an ω-marking M', written $M \leq M'$ (resp. $M \lneq M'$) iff for every place p of the net, $M(p) \leq M'(p)$ (resp. and there exists at least one place p such that $M(p) < M'(p)$).

Definition 3. Given an NS $\langle N, M_0 \rangle$, the associated coverability graph $CG_{\langle N, M_0 \rangle} = (\mathcal{M}, M_0, \Delta)$ is defined in the following manner.

We first define inductively a temporary set $\mathcal{M}_t$ of pairs of ω-markings and set of ω-markings and the temporary transition function Δ_t by:

- $(M_0, \{M_0\}) \in \mathcal{M}_t$ and
- $(M', B') \in \mathcal{M}_t$ iff there exists $(M, B) \in \mathcal{M}_t$ and $t \in T$ such that
  - either $M[t\rangle M'$, $B' = B \cup \{M'\}$ and for all $M'' \in B, M' \not\geq M''$;
  - or, for M^t such that $M[t\rangle M^t$, there exists $M'' \in B$ such that $M^t \gneq M''$. For every such M'', let $p_1, \ldots, p_k$ be the set of places such that for all j, $M^t(p_j) \gneq M''(p_j)$, then $\forall j, M'(p_j) = \omega$. For every place p such that $M'(p) \neq \omega$, $M'(p) = M^t(p)$. Moreover $B' = B \cup \{M'\}$.

In both cases, $((M, B), t, (M', B')) \in \Delta_t$.

We then define $\mathcal{M} = \{M \mid \exists B, (M, B) \in \mathcal{M}_t\}$ and given M and M' in $\mathcal{M}$, $(M, t, M') \in \Delta$ iff there exists B, B' such that $((M, B), t, (M', B')) \in \Delta_t$.

The temporary graph built here is equivalent to the coverability tree of [5]. They proved in [9] that the coverability tree (and thus our temporary graph) terminates in a finite number of steps.

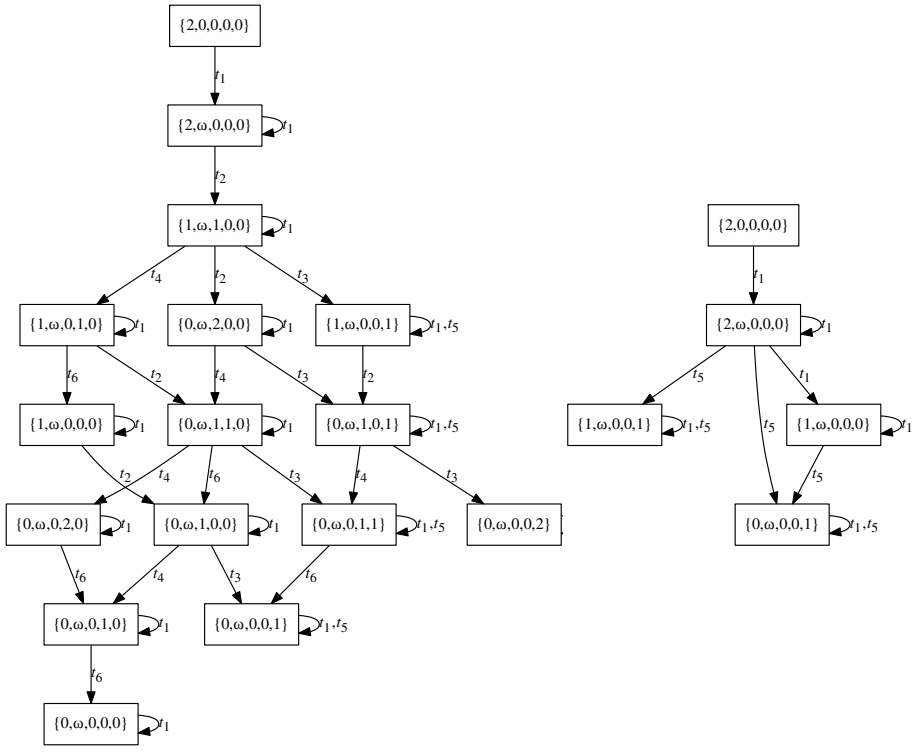

Fig. 2. Left: the coverability graph of the NS in Figure 1. Right: The BCG of the NS in Figure 1 where $T_i = \{t_2, t_3, t_4, t_6\}$ and $T_s = \{t_6\}$. The firing vectors are omitted on the edges.

Example 2. The coverability graph of the NS in Figure 1 is shown in Figure 2. The firing of t_1 at the initial marking adds a token to the second place, reaching a marking strictly greater than the initial marking in this place and equal everywhere else. Correspondingly in the coverability graph an ω appears in the second component of the marking to show that there is a repetitive sequence enabled by the system which increases the number of tokens in the second place.

A marking M is ω-covered by an ω-marking M_ω, denoted $M \leq_\omega M_\omega$ if for every place p such that $M_\omega(p) \neq \omega$, $M_\omega(p) = M(p)$. Using this definition

and the coverability graph, we define the coverability set of an NS which is an over-approximation of the reachability set.

Definition 4. *Given an NS $\langle N, M_0 \rangle$, let $\mathcal{M}$ be the set of ω-markings of its coverability graph, the coverability set of $\langle N, M_0 \rangle$ is*

$$CS(N, M_0) = \{M \in \mathbb{N}^m \mid \exists M_\omega \in \mathcal{M}, M \leq_\omega M_\omega\}$$

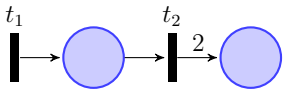

Fig. 3. A Petri net where the coverability set strictly subsumes the reachability set. Transition t_2 is unobservable.

Example 3. The coverability set of the NS in Figure 1 is equal to its reachability set. This is not the case however for the NS in Figure 3 where the reachability set is $\{(k, 2r) \mid k, r \in \mathbb{N}\}$ while the coverability set is $\{(k, r) \mid k, r \in \mathbb{N}\}$. We however clearly see that the coverability set subsumes the reachability set. The coverability graph of this NS is represented in Figure 4.

Fig. 4. Left: the coverability graph of the NS in Figure 3. Right: The BCG of the NS in Figure 3 where $T_i = \{t_2\}$ and $T_s = \emptyset$. The firing vectors are omitted on the edges.

We will use the rest of this section to recall a few known applications of the coverability graph and the coverability set. All those results can be found in [5]. First, as claimed earlier, the coverability set subsumes the reachability set.

Proposition 1. *Let $\langle N, M_0 \rangle$ be an NS, $R(N, M_0) \subseteq CS(N, M_0)$.*

The coverability graph can be used to determine if an NS is bounded.

Proposition 2. *Given an NS $\langle N, M_0 \rangle$,*

- *a place p is k-bounded $\Leftrightarrow$ for each marking M of $CG_{\langle N, M_0 \rangle}$, $M[p] \leq k$.*
- *the marked net is bounded $\Leftrightarrow$ no node of $CG_{\langle N, M_0 \rangle}$ contains the symbol ω*

Repetitiveness can be partially checked on the coverability graph.

Proposition 3. *Given an NS $\langle N, M_0\rangle$, a marking M and a non-empty sequence σ' of transitions enabled by M,*

- *σ is repetitive $\Rightarrow$ there exists a directed cycle in the coverability graph whose arcs form σ starting in an ω marking M_ω such that $M_\omega \geq_\omega M$.*
- *σ is stationary $\Leftarrow$ there exists a directed cycle starting in M in the graph that does not pass through markings containing ω and whose arcs form σ.*

The coverability graph can also be used to test whether a transition can eventually be fired by the NS. A transition t is dead if there is no reachable marking enabling it, it is quasi-live otherwise. It is live if for all reachable markings M, there is a marking M' reachable from M enabling it. A marking is dead if every transition is dead from this marking.

Proposition 4. *Consider a marked net $\langle N, M_0\rangle$, its coverability graph and an observable transition t.*

1. *Transition t is dead $\Leftrightarrow$ no arc labelled t belongs to the graph.*
2. *Transition t is quasi-live $\Leftrightarrow$ an arc labelled t belongs to the graph.*
3. *Transition t is live $\Rightarrow$ an arc labelled t belongs to each ergodic component of the graph.*
4. *A marking M is dead $\Leftarrow$ one ω-marking M_ω of the coverability graph ω-covering M has no output arc.*

2 Basis coverability graph

2.1 Building the basis coverability graph

While the reachability/coverability graph has many applications, one of its downside is its size. For bounded NS, the authors of [4, 6] introduced the notion of basis reachability graph which keeps most of the information relevant for partially observed systems of the reachability graph while decreasing, in some cases exponentially, the size of the graph. Their goal at the time was to study diagnosis. They then generalised this approach to study reachability (regardless of labeling on transitions) in [10]. The idea of the basis reachability graph is to select a set of transitions called "implicit" in [10] (and unobservable in [4]) that will be abstracted and to only represent the "explicit" transitions that can be fired (possibly after some implicit transition) in a given marking. In this section, we will describe how to apply this idea to unbounded NS and how to build instead a *Basis Coverability Graph* (BCG). When the NS is bounded, the BCG is equal to the basis reachability graph.

Given a set of transitions T of a PN, we denote $T_i \subseteq T$ and $T_e = T \setminus T_i$ the sets of *implicit* and *explicit* transitions respectively. Let C_i (C_e) be the restriction of the incidence matrix to T_i (T_e) and n_i and n_e, respectively, be the cardinality of the above sets of transitions. Given a sequence $\sigma \in T^*$, $P_i(\sigma)$, resp., $P_e(\sigma)$, denotes the projection of σ over T_i, resp., T_e.

We will sometimes need the following assumptions.

A1: The T_i-induced subnet is acyclic.
A2: Every sequence containing only implicit transitions is of finite length.

Remark that for bounded NS, the first assumption, which is an usual requirement for problems such as diagnosis of discrete event systems, implies the second one.

When the partition between implicit and explicit transitions is not given, one can always choose a partition respecting the two assumptions above (for example $T_e = T$). The authors of [10] discuss how to choose an appropriate partition for the basis reachability graph and how this choice affects the cardinality of the set of markings of the graph.

Definition 5. Given a marking M and an explicit transition $t \in T_e$, let

$$\Sigma(M,t) = \{\sigma \in T_i^* \mid M[\sigma\rangle M',\ M' \geq Pre(\cdot,t)\}$$

be the set of *explanations* of t at M, and let

$$Y(M,t) = \pi(\Sigma(M,t))$$

be the *e-vectors* (or *explanation vectors*), *i.e.*, firing vectors associated with the explanations.

Thus $\Sigma(M,t)$ is the set of implicit sequences whose firing at M enables t. Among the above sequences we will select those whose firing vector is minimal and those who are minimal while containing a transition among a chosen set $T_s \subseteq T_i$ which will be called the set of *relevant* transitions. This second category is used to solve problems where it may be necessary to keep track of the occurrence of a subset of implicit transitions. In particular it will be used in the section about diagnosis later in this paper. As they are transitions we want to take into account yet are not fully explicit, relevant transitions are more costly than implicit transitions yet not as much as explicit transitions as we will see later. The firing vector of these sequences are called *(T_s-) minimal e-vectors*.

Definition 6. Given a marking M, a transition $t \in T_e$ and a set of relevant transitions $T_s \subseteq T_i$, let

$$\Sigma_{\min}(M,t) = \{\sigma \in \Sigma(M,t) \mid \nexists\ \sigma' \in \Sigma(M,t) : \pi(\sigma') \lneq \pi(\sigma)\}$$

be the set of *minimal explanations* of t at M, and

$$\Sigma_{\min}^{T_s}(M,t) = \{\sigma \in \Sigma(M,t) \mid \sigma \cap T_s \neq \emptyset \wedge \nexists\ \sigma' \in \Sigma(M,t) : \sigma \cap T_s = \sigma' \cap T_s \wedge \pi(\sigma') \lneq \pi(\sigma)\}$$

the set of T_s-*minimal explanations* of t at M.

Remark that for two sets of relevant transitions $T_s \subseteq T_i$ and $T_s' \subseteq T_i$, if $T_s \subseteq T_s'$, for every marking M and explicit transition $t \in T_e$, $\Sigma_{\min}^{T_s}(M,t) \subseteq$

$\Sigma_{\min}^{T_s'}(M,t)$. We will now build the BCG with a construction similar to the one of the coverability graph. From a given marking, instead of choosing a transition and creating the marking obtained by firing this transition, we will fire a sequence composed of a minimal explanation of an explicit transition followed by the explicit transition in question. In other words, we skip all the intermediary markings that were reached by the firing of the implicit transitions. Moreover, in order to determine which places are labelled by ω, instead of only remembering the markings encountered, the temporary construction keeps pairs of marking encountered and of the e-vector of the minimal sequence fired from that marking. From these pairs, one can reconstruct every marking that could have been reached.

Definition 7. Given an NS $\langle N, M_0\rangle$ verifying Assumption (A1) and a set of relevant transition $T_s \subseteq T_i$, the associated basis coverability graph (BCG) with relevant transitions T_s $BCG_{\langle N,M_0\rangle}^{T_s} = (\mathcal{M}, M_0, \Delta)$ is defined in the following manner.

We first define inductively a temporary set $\mathcal{M}_t$ of pairs of ω-markings and set of pairs of ω-markings and firing vectors and the temporary transition function Δ_t by:

- $(M_0, \emptyset) \in \mathcal{M}_t$ and
- $(M', B') \in \mathcal{M}_t$ iff there exists $(M, B) \in \mathcal{M}_t$, $t \in T_e$ and $\sigma \in \Sigma_{\min}(M,t) \cup \Sigma_{\min}^{T_s}(M,t)$ with $M[\sigma t\rangle M_n$, where $B' = B \cup \{(M, \pi(\sigma))\}$ and
  - either $M_n = M'$ and for all $(M'', \pi) \in B$, $M[\sigma_1\rangle M_1$ and $M''[\sigma_2\rangle M_2$ with $\pi(\sigma_1) \leq \pi(\sigma t)$ and $\pi(\sigma_2) \leq \pi$, we have $M_1 \not\geq M_2$;
  - or there exists $(M'', \pi) \in B$, $M[\sigma_1\rangle M_1$ and $M''[\sigma_2\rangle M_2$ with $\pi(\sigma_1) \leq \pi(\sigma t)$ and $\pi(\sigma_2) \leq \pi$ such that $M_1 \geq M_2$. Then let $p_1, \ldots, p_k$ be the places such that $\forall i, M_1(p_i) > M_2(p_i)$. Let $\tilde{M}$ be the marking obtained from M by replacing the number of tokens of the places p_i by ω. We repeat the tests from the marking $\tilde{M}$ until no new place can be modified. Let $p_1, \ldots, p_n$ be the places of M where an ω was added in this process. Then for every place p, if $p \in \{p_1, \ldots, p_n\}$, $M'(p) = \omega$, otherwise $M'(p) = M_n(p)$.

In both cases $((M, B), (\pi(\sigma), t), (M', B')) \in \Delta_t$.

We then define $\mathcal{M} = \{M \mid \exists B, (M, B) \in \mathcal{M}_t\}$ and given M and M' in $\mathcal{M}$, $(M, (\pi(\sigma), t), M') \in \Delta$ iff there exists B, B' such that $((M, B), (\pi(\sigma), t), (M', B')) \in \Delta_t$.

The markings of the BCG are called *basis markings*.

This construction does not require to check every implicit sequence of transitions. Indeed, it only focuses on the firing vectors which can be more efficiently analysed. This is only possible thanks to Assumption (A1), or more precisely thanks to Theorem 3.8 of [4] which requires (A1) (this is the result used every time Assumption (A1) is required in the following). This results implies that due to the acyclicity of the implicit net, the implicit transitions of an explanation that are not part of the minimal explanation can be postponed after the explicit transition. This gives an important leeway on the order in which the implicit transitions have to be in. Removing the Assumption (A1) would allow the construction of

a variant of the BCG defined here, but its construction would be more costly as we would need to consider the minimal explanations instead of their e-vector and the variant may construct more states than the one built here.

We denote the projection of a sequence $\sigma = (\sigma_1, t_1) \dots (\sigma_k, t_k) \dots$ of the BCG on its second component by $P_t(\sigma) = t_1 \dots t_k \dots$.

Example 4. Let us first consider the NS in Figure 3 with $T_i = \{t_2\}$ and no relevant transition and the associated coverability graph and BCG in Figure 4. In order to fire t_1, firing t_2 is not required. As a consequence, the firing of the transition t_2 is never used in the construction of the BCG.

As another example, we represent the BCG of the NS in Figure 1 (for $T_i = \{t_2, t_3, t_4, t_6\}$ and $T_s = \{t_6\}$) in Figure 2. For readability the firing vectors on the edges are omitted in the figure. This BCG has 11 less states than the coverability graph.

Choosing $T_s = \{t_6\}$ adds the states $\{1, \omega, 0, 0, 0\}$ and $\{0, \omega, 0, 0, 1\}$ and the edges affecting those states. The edge from $\{2, \omega, 0, 0, 0\}$ to $\{0, \omega, 0, 0, 1\}$ corresponds to the $\{t_6\}$-minimal explanation $t_2 t_2 t_3 t_4 t_6$ of t_5 which is not a minimal explanation.

2.2 Properties of the basis coverability graph

We will list here some of the properties of the BCG. We will first give a few results on the size of the BCG compared to the coverability graph and under variations of the sets of explicit, implicit and relevant transitions. Then we will define the notion of basis coverability set and show it is a better approximation of the reachability set than the coverability set. Finally, we will see how the properties of boundedness, repetitiveness and liveness translate from the coverability graph to the BCG.

The BCG was introduced in order to gain in efficiency compared to the coverability graph. The first property to mention is thus that the BCG is always smaller than or equal to the coverability graph. This is formally proved in the following.

Proposition 5. *Given an NS $\langle N, M_0 \rangle$ verifying Assumption (A1) with set of implicit transitions T_i, for any set of relevant transitions $T_s \subseteq T_i$ it holds that every basis marking M of $BCG^{T_s}_{\langle N, M_0 \rangle}$ is a marking of $CG_{\langle N, M_0 \rangle}$.*

Proof. As any marking of the BCG is reachable from M_0, we will show the result by induction on the length of a path reaching this marking. Let M be a marking of $BCG^{T_s}_{\langle N, M_0 \rangle}$ and σ a sequence such that $M_0[\sigma\rangle M$.

If $|\sigma| = 0$, $M = M_0$ which is a marking of $CG_{\langle N, M_0 \rangle}$.

Given $n \in \mathbb{N}$, suppose that the property is true for every marking reached by a path of length at most n. If $|\sigma| = n + 1$, there exists a sequence σ_1 and a transition (e, t) of $BCG^{T_s}_{\langle N, M_0 \rangle}$ such that $\sigma = \sigma_1 (e, t)$, let M_1 such that $M_0[\sigma_1\rangle M_1$, then by hypothesis M_1 belongs to $CG_{\langle N, M_0 \rangle}$. Moreover, as there is a transition $M_1[(e, t)\rangle M$ in the BCG, there exists a minimal explanation

$\sigma' = t_1, \dots t_n \in \Sigma_{\min}(M_1, t) \cup \Sigma^{T_s}_{\min}(M_1, t)$ such that $\pi(\sigma') = e$ and one of the two conditions for a BCG transition between M_1 and M is validated. If it is the first condition, there is a path $M_1[t_1\rangle M_2 \dots [t_n\rangle M_n[t\rangle M$ in $CG_{\langle N, M_0\rangle}$, thus M is a marking of $CG_{\langle N, M_0\rangle}$. If it is the second condition, assume the process ends in a single round. Then there exists a marking $M_<$ either encountered while reading σ in the BCG or reachable by a subset of a minimal explanation that is smaller than a marking $M_>$ reachable from M_1. As all the markings of the BCG encountered along σ_1 be longs to the coverability graph, using Assumption (A1) there is a path in the coverability graph from $M_<$ to an ω-marking $M^\omega_>$ with $M^\omega_> \geq_\omega M_>$ and as the process occurs only once, the only places where $M^\omega_>$ contains an ω and $M_>$ does not are the places where $M_>$ is strictly greater than $M_<$. By firing the transitions corresponding to the firing vector e that are left after reaching $M_>$ in the coverability graph from $M^\omega_>$ we reach M. The same idea works if the process requires multiple rounds, however, in order to visit every states that are covered and covering, one may need to extend the run. As a consequence, M is a marking of $CG_{\langle N, M_0\rangle}$ □

How much is gained depends on the partition between implicit, explicit and relevant transitions. For example, if every transition is explicit, the BCG is exactly equal to the coverability graph. On the contrary, increasing the number of implicit transitions reduce the size of the BCG.

Proposition 6. *consider an NS $\langle N, M_0\rangle$ verifying Assumption (A1) and two sets of implicit transitions T_i and T'_i with $T'_i \subseteq T_i$. For any set of relevant transitions T_s such that $T_s \subseteq T'_i$, every basis marking of the BCG of $\langle N, M_0\rangle$ with implicit transitions T_i is a basis marking of the BCG of $\langle N, M_0\rangle$ with implicit transition T'_i.*

Proof. We call C and C' the two BCG with implicit sets of transitions T_i and T'_i. We will show that any basis marking M of C is a basis marking of C' by induction on the length n of the sequence reaching it. If $n = 0$, $M = M_0$ and belongs to C'. Else, there is a sequence $\sigma = \sigma_1(e, t)$ (with e a firing vector of implicit transition and t an explicit transition) and a basis marking M_0 such that $M[\sigma_1\rangle M_0[(e, t)\rangle M$ in C. By induction hypothesis, M_0 is a basis marking of C'. Let σ' be a minimal explanation of t with $\pi(\sigma') = e$. $\sigma' = \sigma_0 t_0 \sigma_1 \dots t_k \sigma_{k+1}$ where for all $i \leq k + 1$ the transitions t_i are explicit transitions and the σ_i are sequences of implicit transitions with respect to T'_i. Due to Assumption (A1), we can assume without loss of generality that the σ_i, $i \leq k$, are minimal explanations of t_i. Therefore there exists basis markings in C', $M_1, \dots M_k$, such that $M_0[(\pi(\sigma_0), t_0)\rangle M_1 \dots [(\pi(\sigma_k), t_k)\rangle M_k[(\pi(\sigma_{k+1}), t)\rangle M$. Thus M belongs to C'. □

With a similar proof, we can show that turning implicit transitions into relevant transitions increases the number of markings.

Proposition 7. *Consider an NS $\langle N, M_0\rangle$ verifying Assumption (A1) with set of implicit transitions T_i. For any two sets of relevant transitions $T_s, T'_s \subseteq T_i$ with $T_s \subseteq T'_s$, every basis marking of $BCG^{T_s}_{\langle N, M_0\rangle}$ is a basis marking of $BCG^{T'_s}_{\langle N, M_0\rangle}$.*

Fig. 5. Left: the BCG of the NS in Figure 3 with t_1 and t_2 explicit. Right: the BCG of the NS in Figure 3 with t_1 relevant and t_2 explicit. The firing vectors are omitted on the edges.

Relevant transitions are in between explicit and implicit transitions in terms of cost. This is strict as seen for example on the NS in Figure 3 when choosing t_2 explicit and t_s either explicit or relevant (the associated BCG are represented in Figure 5). Here, making the transition relevant instead of explicit removes one basis marking. In fact, on this example making t_1 relevant or implicit does not change anything contrary to what was seen in Example 4.

Let us now discuss about the importance of the gain of the BCG construction through an example.

Example 5. Consider the NS in Figure 6, transitions t_0, t_i and t_{end} being explicit while the others are implicit. The BCG has exactly $\frac{(s+3)(s+2)}{2}$ basis markings, thus is quadratic in s and does not depend on r or k. However, the coverability graph has at least $\sum_{j=0}^{s} \binom{r+j}{j}^k$ markings (this is the number of markings reached while never firing t_0). Thus is among others exponential in k. Moreover, as this is without firing t_0, this only describes a part of the coverability graph that do not contain any ω.

We will now give some results showing that the BCG can effectively be used in many cases instead of the coverability graph. As a first step, we will show that the BCG can be used to define a set of markings that are an over-approximation of the reachability set. We denote by $R_i(N, M)$ the set of markings reachable from M using only implicit transitions in the Petri net N. Given an ω-marking M_ω and a marking M, $M_\omega =_\omega M$ iff for every place p such that $M_\omega(p) \neq \omega$, $M_\omega(p) = M(p)$.

Definition 8. *Given an NS $\langle N, M_0\rangle$ with m places and a set of implicit transitions T_i, let $T_s \subseteq T_i$ be a set of relevant transitions and let V be the set of basis markings of $BCG^{T_s}_{\langle N,M_0\rangle}$. The basis coverability set of $\langle N, M_0\rangle$ with relevant transitions T_s is*

$$BCS^{T_s}(N, M_0) = \{M \in \mathbb{N}^m \mid \exists M_\omega \in V, \exists M^u_\omega \in R_i(N, M_\omega), M^u_\omega \geq_\omega M\}$$

This set can be easily computed for NS verifying (A1). For every possible choice of T_s, the basis coverability set is an over-approximation of the reachability set.

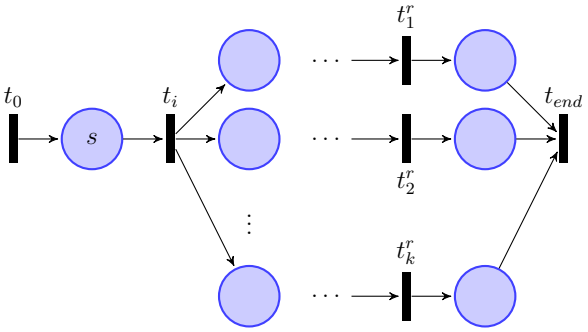

Fig. 6. A Petri net where the BCG has exponentially less states than the coverability graph. s is the number of tokens contained in this place in the initial marking and there is $r+1$ places in each of the parallel lines.

Proposition 8. *Given an NS $\langle N, M_0\rangle$ with set of implicit transitions T_i verifying Assumption (A1) and a set of relevant transitions $T_s \subseteq T_i$, it holds $R(N, M_0) \subseteq BCS^{T_s}(N, M_0)$.*

Proof. Let σ be a sequence such that $M_0[\sigma\rangle M$ in the NS. We will proceed by induction on the length of σ.

If $|\sigma| = 0$, $M = M_0$ which is a marking of the BCG.

Given $n \in \mathbb{N}$, supposing that the property is true for every marking reached by a path of length at most n. For $|\sigma| = n+1$, $\sigma = \sigma_1 t$. Let $M_0[\sigma_1\rangle M_1$. By the induction hypothesis there exists a basis marking M_ω^b and an ω-marking M_ω^u such that $M_\omega^u \in R_i(N, M_\omega^b)$ and $M_\omega^u \geq_\omega M_1$.

• if t is implicit, as $M_\omega^u \geq_\omega M_1$, t is enabled by M_ω^u and the marking reached by firing t in M_ω^u, let's call it $M_\omega^{u,2}$, verifies $M_\omega^{u,2} \geq_\omega M$ and $M_\omega^{u,2} \in R_i(N, M_\omega^b)$.

• if t is explicit, let σ_t such that $M_\omega^b[\sigma_t\rangle M_\omega^u$. Since σ_t is an explanation of t, there thus exist a minimal explanation σ_{min} such that $\pi(\sigma_{min}) \leq \pi(\sigma_t)$ and a sequence $\sigma_e \in T_i^*$ such that $\pi(\sigma_{min}) + \pi(\sigma_e) = \pi(\sigma_t)$. Let $M_s \leq_\omega M_\omega^b$ such that $M_s[\sigma_t\rangle M_1$ and M_f the marking such that $M_s[\sigma_{min} t\rangle M_f$. Using Assumption (A1), $M_f[\sigma_e\rangle M$. By construction of the BCG, there exists a basis marking M_2^b reachable with transition $(\pi(\sigma_{min}), t)$ from M_ω^b such that $M_2^b \geq_\omega M_f$. Moreover, as $M_f[\sigma_e\rangle M$, triggering σ_e in M_2^b leads to a marking M_ω^2 such that $M_\omega^2 \geq_\omega M$. □

The following result characterizes a monotonicity property of the basis coverability set with respect to the corresponding set of relevant transitions. It is a direct corollary of Proposition 7.

Corollary 1. *Given an NS $\langle N, M_0\rangle$ verifying Assumption (A1) with set of implicit transitions T_i. For any two sets of relevant transitions T_s and T_s' such that $T_s \subseteq T_s' \subseteq T_i$, $BCS^{T_s}(N, M_0) \subseteq BCS^{T_s'}(N, M_0)$.*

The inclusion can be strict. Indeed, let us observe the NS of Figure 3 with t_2 implicit. The BCG with $T_s = \emptyset$ has two basis markings $[0, 0]$ and $[\omega, 0]$. The

associated basis coverability set is $\{[n, 2m] \mid n, m \in \mathbb{N}\}$, which is equal to the reachability set. However, the BCG with $T_s = \{t_2\}$ has the two previous basis markings plus $[\omega, \omega]$. Therefore its basis coverability set is $\{[n, m] \mid n, m \in \mathbb{N}\}$, which is equal to the coverability set. In fact the basis coverability set is always a better approximation than the coverability set.

Proposition 9. *Given an NS $\langle N, M_0\rangle$ verifying Assumption (A1) with set of implicit transitions T_i and a set of relevant transitions $T_s \subseteq T_i$, it holds $BCS^{T_s}(N, M_0) \subseteq CS(N, M_0)$.*

Proof. Let $M \in BCS(N, M_0)$. By definition, there exists $M' \geq_\omega M$ and M_b state of the BCG with $M' \in R_i(N, M_b)$. By Proposition 5, M_b is a state of $CG_{\langle N, M_0\rangle}$. Let σ be an implicit sequence such that $M_b[\sigma\rangle M'$. By definition of R_i and of the coverability graph there exists a state M_c of $CG_{\langle N, M_0\rangle}$ such that $M_b[\sigma\rangle M_c$ in the CG and $M_c \geq M'$. Thus $M_c \geq M$. Therefore $M \in CS(N, M_0)$. □

We now show how the results relative to the coverability graph recalled in the previous section (namely Propositions 2 and 3) can be transposed on the BCG. As those results hold for every choice of set of relevant transitions $T_s \subseteq T_i$, this set is omitted for the rest of the section.

Proposition 10. *Given an NS $\langle N, M_0\rangle$ with set of implicit transitions T_i verifying Assumptions (A1) and (A2),*

- *a place p is k-bounded $\Rightarrow$ for each basis marking M of the BCG $M[p] \leq k$.*
- *p is not k-bounded $\Rightarrow$ there exists a basis marking M_ω and an ω-marking $M_u \in R_i(N, M_\omega)$ with $M_u(p) > k$;*
- *the NS is bounded $\Leftrightarrow$ no basis marking of the BCG contains the symbol ω.*

Proof.
- The first item holds as this implication is true for every marking of the coverability graph according to Proposition 2 and Proposition 5 which claims that the markings of the BCG are markings of the coverability graph.
- Suppose that p is not k-bounded. There thus exists a marking $M \in R(N, M_0)$ with $M(p) > k$. As $R(N, M_0) \subseteq BCS(N, M_0)$ according to Proposition 8, there exists a basis marking M_ω and an ω-marking $M_u \in R_i(N, M_\omega)$ such that $M_u \geq_\omega M$. Thus $M_u(p) > k$.
- For the third item, the left to right implication is once again due to Proposition 5 and the fact that the equivalence holds when considering the coverability graph as stated in Proposition 2.
  For the right to left implication, suppose that no ω appears in the BCG. Then $BCS(N, M_0)$ is finite as in every basis marking, which are also markings reachable in the NS, there is finitely many sequences of implicit transitions enabled thanks to assumption (A2). Therefore, according to Proposition 8 the reachability set $R(N, M_0)$ is finite. This implies that the NS is bounded. □

The reverse implication of the first item is false. Indeed, observe the NS of Figure 3, the two basis markings of the BCG are $[0, 0]$ and $[\omega, 0]$, however the second place is not bounded by 0, in fact it is not bounded at all. In this respect, the BCG

may not explicitly show all the informations that appears in the coverability graph. The second item shows the stronger requirement, using the implicit reach, that is needed to get the reverse implication.

Proposition 11. *Given an NS $\langle N, M_0\rangle$ with set of implicit transitions T_i verifying Assumption (A1), a non-empty sequence σ' of explicit transitions and a marking M*

- *there exists a repetitive sequence σ with $P_e(\sigma) = \sigma'$ enabled by $M \Rightarrow$ there exists $k \in \mathbb{N}$, two basis markings M^1_ω, M^2_ω and two ω-markings $M^i_u \in R_i(N, M^i_\omega)$, $i \in \{1, 2\}$, such that:*
  - *$M \leq_\omega M^i_u$, $i \in \{1, 2\}$;*
  - *there is a path starting in M^1_ω and ending in M^2_ω in the BCG whose arcs, projected on the second component, form σ';*
  - *there is a directed cycle starting in M_ω in the BCG whose arcs, projected on the second component, form $(\sigma')^k$.*
- *there exists a directed cycle starting in M_ω in the BCG that does not pass through markings containing ω and whose arcs, projected on the second component, form σ' where M_ω is a basis marking such that $M \in R_i(N, M_\omega)$ $\Rightarrow$ there exists a stationary sequence σ with $P_e(\sigma) = \sigma'$ enabled by M.*

Proof. – Suppose that σ is repetitive from M. Due to Proposition 8, there exists a basis marking M^0_ω and an ω-marking M^0_u with $M^0_u \geq_\omega M$ and $M^0_u \in R_i(N, M^0_\omega)$. Let $\sigma = \sigma_1 t_1 \dots \sigma_n t_n \sigma_{n+1}$ where the σ_i's are sequences of implicit transitions and the t_i's are explicit transitions. As the NS verifies (A1) and by construction of the BCG, there exists a sequence $\sigma^1 = \sigma^1_1 t_1 \dots \sigma^1_n t_n$ enabled by M^0_ω where the σ^1_i's are minimal explanations of the t_i's and ending in a basis marking M^1_ω such that there exists an ω-marking M^1_u with $M^1_u \geq_\omega M$ and $M^1_u \in R_i(N, M^1_\omega)$. This translates in the BCG into a sequence $(\pi(\sigma^1_1), t_1) \dots (\pi(\sigma^1_n), t_n)$ from M^0_ω to M^1_ω. This can be repeated, giving a family of sequences $(\sigma^j)_{j\in\mathbb{N}}$, of basis markings $(M^j_\omega)_{j\in\mathbb{N}}$ and of ω-marking $(M^j_u)_{j\in\mathbb{N}}$ such that $M^{j-1}_\omega[\sigma^j\rangle M^j_\omega$, $M^j_u \geq_\omega M$ and $M^j_u \in R_i(N, M^j_\omega)$. Due to the finite number of basis markings, there exists $k, k', k < k'$, such that $M^k_\omega = M^{k'}_\omega$. There thus exists a directed cycle starting in M^k_ω whose arcs, projected on the second component, form $P_e(\sigma)^{k'-k}$.

– Suppose that there exists a directed cycle starting in the basis marking M_ω in the BCG that does not pass through markings containing ω and whose arcs, projected on the second component, form σ'. Using the Proposition 5, M_ω is a marking of $CG_{\langle N,M_0\rangle}$. Moreover due to the construction of the BCG there exists σ such that $P_e(\sigma) = \sigma'$ and a directed cycle starting in M_ω in $CG_{\langle N,M_0\rangle}$ that does not pass through markings containing ω and whose arcs form σ. Due to Proposition 3, this implies that σ is stationary. □

A marking M is *finitely dead* if there exists a bound k such that every sequence of transitions enabled by M does not contain an explicit transition and has a length smaller than k.

Proposition 12. *Consider an NS $\langle N, M_0\rangle$ with set of implicit transitions T_i verifying Assumptions (A1) and (A2), its BCG and an explicit transition t .*

1. *Transition t is dead $\Leftrightarrow$ there is no arc labelled by t' in the BCG with $P_t(t') = t$.*
2. *Transition t is quasi-live $\Leftrightarrow$ there is an arc labelled by t' in the BCG with $P_t(t') = t$.*
3. *Transition t is live $\Rightarrow$ there is an arc labelled by t' in each ergodic component of the BCG with $P_t(t') = t$.*
4. *A basis marking M_ω in the BCG has no output arc $\Rightarrow$ any marking M with $M_\omega \geq_\omega M$ is finitely dead.*

Proof. 1. $\Rightarrow$ If an arc labelled (p, t) belongs to the BCG, then there is a basis marking M_ω by which it is enabled. Thanks to Proposition 5, this basis marking is an ω-marking of the coverability graph. Moreover due to the construction of the BCG, this implies that there is a sequence σt, with σ implicit, enabled by M_ω in $CG_{\langle N,M_0\rangle}$. Thanks to Proposition 4 this implies that t is not dead.
$\Leftarrow$ If t is not dead, then there exists a reachable marking M in the NS such that t is enabled by M. Due to Proposition 8, there thus exists an ω-marking M_u and a basis marking M_ω such that $M_u \geq_\omega M$ and $M_u \in R_i(N, M_\omega)$. Let σ such that $M_\omega[\sigma\rangle M_u$. σ is an explanation of t, there thus exists a minimal explanation σ' of t. Therefore $(\pi(\sigma'), t)$ is enabled by M_ω.
2. This item is equivalent to the previous one.
3. Suppose that t is live. According to Proposition 4, there thus exists an arc labelled t in each ergodic component of $CG_{\langle N,M_0\rangle}$. Let M_ω be a basis marking, due to Proposition 5, it is a marking of $CG_{\langle N,M_0\rangle}$ too. There thus exists a path $\sigma = \sigma_1 t_1, \ldots, \sigma_n t_n$ in $CG_{\langle N,M_0\rangle}$ enabled by M_ω with $t_n = t$. Without loss of generalities thanks to the (A1) assumption, one can suppose the sequences σ_i to be minimal explanations of t_i. By construction of the BCG, there thus exists a path $\sigma' = (\pi(\sigma_1, t_1) \ldots (\pi(\sigma_n), t_n)$ enable in M_ω in the BCG. As it is true for every marking M_ω, there is an arc whose second component is t in every ergodic component.
4. Let M_ω be a basis marking with no output arc. Let M such that $M_\omega \geq_\omega M$, suppose there exists an explicit transition t and an implicit sequence σ such that σt is enabled by M. As $M_\omega \geq_\omega M$, σt is enabled by M_ω in $CG_{\langle N,M_0\rangle}$, which would imply by construction of the BCG that there exists an outgoing arc labelled by (p, t) in M_ω for some firing vector p, which is a contradiction. Therefore any sequence enabled by M is only composed of implicit transitions. As those sequences are finite due to (A2), this means that the number of implicit transitions that can be fired is bounded. Thus M is finitely dead. □

3 Diagnosability of Unbounded Net Systems

3.1 Definition of Diagnosability

In the following, we want to use the BCG to deal with the problem of fault diagnosis where the goal is to detect the occurrence of a fault under partial

observation. To this aim, we associate a well precise physical meaning to implicit, explicit, and relevant transitions. In more detail:

- Implicit transitions correspond to transitions that cannot be observed. They are called *silent* or *unobservable* and could either model a regular (nominal) behaviour or a faulty behaviour of the system.
- Conversely, explicit transitions model transitions that can be observed. Those *observable* transitions are assumed to be a regular behaviour of the system
- The set of faulty transitions is chosen as the set of relevant transitions.

We denote the above three sets as T_u, T_o, and T_f, respectively and choose $T_e = T_o$ and $T_i = T_u$.

In simple words, we may assume that observable transitions model events whose occurrence is detected by the presence of a sensor. On the contrary, unobservable transitions correspond to events to whom no sensor is associated. Note that, in the general case, the same output signal may correspond to different events (different transition firings). This can be easily modelled using the notion of *labeling function*. $\mathcal{L} : T \to L \cup \{\varepsilon\}$ that assigns to each transition $t \in T$ either a symbol from a given alphabet of events L (if $T \in T_o$) or the empty string ε (if $T \in T_u$). We extend naturally $\mathcal{L}$ to sequences of transitions with $\mathcal{L}(\sigma t) = \mathcal{L}(\sigma)\mathcal{L}(t)$. The observed word w of events associated with the sequence σ is $w = \mathcal{L}(\sigma)$. Note that the length of a sequence σ is always greater than or equal to the length of the corresponding word w (denoted $|w|$). In fact, if σ contains k' transitions in T_u then $|\sigma| = k' + |w|$. Given a word $w \in L^*$, we write $\mathbb{P}(w) = \sum_{\sigma \in P_e^{-1}(w)} \mathbb{P}(\sigma)$. Assuming (A2), this sum is finite.

The goal of diagnosis is to detect whether a faulty event occurred in the system. We denote by $T_f \subseteq T_u$ the set of faulty transitions. A sequence σ is faulty if there exists $t \in T_f$ such that $t \in \sigma$, otherwise it is correct. An observed word w is surely faulty (resp. correct) iff every sequence σ with $\mathcal{L}(\sigma) = w$ is faulty (resp. correct) sequences, otherwise it is ambiguous. An NS system is diagnosable iff all faults can be detected after a finite delay.

Definition 9. *An NS $\langle N, M_0 \rangle$ is diagnosable if for every faulty sequence σ enabled by M_0, there exists $n \in \mathbb{N}$ such that for all sequences $\sigma' \in T^n$ with $\sigma\sigma'$ enabled by M_0, $\mathcal{L}(\sigma\sigma')$ is surely faulty.*

Example 6. Consider again the NS in Figure 1,where the labelling function $\mathcal{L}$ is such that $\mathcal{L}(t_1) = b, \mathcal{L}(t_2) = a, \mathcal{L}(t_3) = \mathcal{L}(t_4) = \varepsilon$ and $\mathcal{L}(t_5) = \mathcal{L}(t_6) = c$. Thus, t_3 and t_4 are unobservable. Transition t_5 being observable, the T_u-induced subnet is acyclic.

Choosing $T_f = \{t_3\}$, the infinite sequence $\sigma_f = t_1t_2t_3(t_5)^3$ is faulty and its observed word bac^3 is surely faulty, so the fault can be detected here. However, the sequences $\sigma_f = t_1t_2t_3(t_1)^*$ are faulty but their observed word bab^* is ambiguous as it can also correspond to the correct sequences $t_1t_2(t_1)^*$ too. Thus this NS is not diagnosable.

3.2 Diagnosability Analysis

Diagnosability was proven decidable [3, 1]. To do so, the authors of [3] gave a characterisation of diagnosability using a tool called Verifier Net. The verifier net is obtained by a composition (related to a parallel composition of the studied NS and its $T \setminus T_f$-induced subnet with synchronisation on the observable transitions.

Definition 10. *Given an NS $\langle N, M_0\rangle$, let $\langle N', M_0'\rangle$ be the $T \setminus T_f$-induced subnet of $\langle N, M_0\rangle$ (prime are used to differentiate states and transitions of N' from those of N). We build the verifier net (VN) $\langle \tilde{N}, \tilde{M}_0$ of $\langle N, M_0\rangle$ with $\tilde{N} = (\tilde{P}, \tilde{T}, \tilde{Pre}, \tilde{Post})$ where:*

- $\tilde{P} = P \cup P'$,
- $\tilde{T} = (T_o' \times T_o) \cup (T \setminus T_f \times \{\lambda\}) \cup (\{\lambda\} \times T)$,
- *for $t \in T, t' \in T' \setminus T_f, p \in P$, and $p' \in P'$, we have*
  - $\tilde{Pre}(p, (\lambda, t)) = Pre(p, t)$ *and* $\tilde{Post}(p, (\lambda, t)) = Post(p, t)$,
  - $\tilde{Pre}(p', (t', \lambda)) = Pre(p', t')$ *and* $\tilde{Post}(p', (t', \lambda)) = Post(p', t')$,
  - *if* $\mathcal{L}(t) = \mathcal{L}(t') \neq \varepsilon$, $\tilde{Pre}(p', (t', t)) = Pre(p', t')$ *and* $\tilde{Post}(p', (t', t)) = Post(p', t')$, $\tilde{Pre}(p, (t', t)) = Pre(p, t)$ *and* $\tilde{Post}(p, (t', t)) = Post(p, t)$.

  All unspecified values are equal to 0.

Theorem 1 ([3]). *An NS $\langle N, M_0\rangle$ verifying Assumption (A1) is diagnosable iff there does not exist any cycle in the coverability graph of the VN which (1) starts from an ω-marking reachable by a faulty sequence and (2) is associated with a repetitive sequence in the associated VN.*

We will now use this characterisation to formulate a similar one using the BCG instead of the coverability graph. A sequence of the BCG is called faulty if one of the minimal e-vector used activated a transition of T_f (i.e. the corresponding sequence belongs to $\Sigma_{min}^{T_f}$).

Theorem 2. *An NS $\langle P, M_0\rangle$ verifying Assumptions (A1) and (A2) is diagnosable iff there does not exist any cycle in the BCG with relevant set of transitions T_f of the VN which (1) starts from a basis marking reachable by a faulty sequence and (2) is associated with a repetitive sequence in the associated VN.*

Proof. We will show that the existence of such a cycle in the BCG is equivalent to the existence of this cycle in the coverability graph.

Supposing there exists a cycle associated with a firable repetitive sequence $\sigma \in T^*$ in the associated VN that starts from a basis marking M_ω reached by a faulty sequence in the BCG with relevant set of transition T_f of the VN, then by Proposition 5, M_ω is an ω-marking of the coverability graph and by construction of the BCG, there exists a directed cycle starting in M_ω in the coverability graph whose arcs form σ.

Now suppose that there is a firable repetitive sequence $\sigma = \sigma_1 t_1 \dots \sigma_n t_n$ in the VN that is associated to a cycle starting from an ω-marking reached by a faulty sequence in the coverability graph of the VN. There thus exists a marking M of the VN such that σ is repetitive starting in M. Because of the

assumption (A2), σ contains at least one observable transition. According to Proposition 11, there thus exists a basis marking M_ω and an ω-marking M_u such that $M_u \in R_i(N, M_\omega)$, $M_u \geq_\omega M$ and there is a $k \in \mathbb{N}$ and a directed cycle starting in M_ω whose arcs, projected on the second component, form $P_o(\sigma)^k$. Moreover, as M is reached by a faulty sequence $\sigma' = \sigma'_1 t'_1 \dots \sigma'_n t'_n \sigma'_{n+1}$, one can choose M_ω to be reached by a sequence that used a minimal explanation from $\Sigma_{min}^{T_f}$: if σ'_i is faulty, one can choose the minimal explanation of t_i to belong in $\Sigma_{min}^{T_f}$.

Consequently the characterisation of Theorem 1 and Theorem 2 are equivalent and can both be used to solve diagnosability. □

Conclusion

In this paper, we introduced the notion of basis coverability graph which provides an abstracted representation of the coverability graph. We established multiple properties of the basis coverability graph, especially how it can be used to approximate the reachability set efficiently. We then gave an application of the basis coverability graph with the diagnosability analysis problem. We showed how the basis reachability graph can be employed to efficiently replace a previously known characterisation of the diagnosability of an unbounded NS. The logical next step would be to implement the algorithms obtained and compare their efficiency with other algorithms ([1] for example) on case studies.

References

1. B. Bérard, S. Haar, S. Schmitz, and S. Schwoon. The Complexity of Diagnosability and Opacity Verification for Petri Nets. In *Petri nets 2017*, Lecture Notes in Computer Science. Springer, 2017.
2. H. Boucheneb and K. Barkaoui. Reducing interleaving semantics redundancy in reachability analysis of time Petri nets. *ACM Trans. Embed. Comput. Syst.*, 12(1):7:1–7:24, January 2013.
3. M. P. Cabasino, A. Giua, S. Lafortune, and C. Seatzu. A new approach for diagnosability analysis of petri nets using verifier nets. *IEEE Transactions on Automatic Control*, 57(12):3104–3117, Dec 2012.
4. 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.
5. M. P. Cabasino, A. Giua, and C. Seatzu. *Introduction to Petri Nets*, pages 191–211. Springer London, 2013.
6. 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.
7. A. Giua, C. Seatzu, and D. Corona. Marking estimation of Petri nets with silent transitions. *IEEE Transactions on Automatic Control*, 52(9):1695–1699, Sept 2007.
8. P. Godefroid. *Partial-Order Methods for the Verification of Concurrent Systems: An Approach to the State-Explosion Problem*, volume 1032. Springer, 1996.
9. R. M. Karp and R. E. Miller. Parallel program schemata. *Journal of Computer and System Sciences*, 3(2):147–195, 1969.

10. 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, 2017.
11. E. W. Mayr. An algorithm for the general Petri net reachability problem. In *Proceedings of the Thirteenth Annual ACM Symposium on Theory of Computing*, STOC '81, pages 238–246. ACM, 1981.
12. T. Murata. Petri nets: Properties, analysis and applications. *Proceedings of the IEEE*, 77(4):541–580, April 1989.
13. M. Nielsen, G. Plotkin, and G. Winskel. Petri nets, event structures and domains, part I. *Theoretical Computer Science*, 13(1):85 – 108, 1981. Special Issue Semantics of Concurrent Computation.
14. P.-A. Reynier and F. Servais. Minimal coverability set for Petri nets: Karp and miller algorithm with pruning. *Fundamenta Informaticae*, 122(1-2):1–30, January 2013.
15. R.Lipton. The Reachability Problem Requires Exponential Space. Technical report, Yale University, 1976.
16. M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis. Diagnosability of discrete-event systems. *IEEE Trans. Aut. Cont.*, 40(9):1555–1575, 1995.
17. Y. Tong, Z. Li, C. Seatzu, and A. Giua. Verification of state-based opacity using Petri nets. *IEEE Transactions on Automatic Control*, 62(6):2823–2837, June 2017.
18. A. Valmari. *The state explosion problem*, pages 429–528. Springer Berlin Heidelberg, 1998.