ON THE DECIDABILITY OF PROBLEMS IN LIVENESS OF CONTROLLED DISCRETE EVENT SYSTEMS MODELED BY PETRI NETS

BY

ARUN RAMAN

DISSERTATION

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Systems and Entrepreneurial Engineering
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2020

Urbana, Illinois

Doctoral Committee:

Professor R. S. Sreenivas, Chair
Professor Tamer Başar
Professor Carolyn Beck
Assistant Professor Jugal Garg

ABSTRACT

A *Discrete Event System* (DES) is a discrete-state system, where the state changes at discrete-time instants due to the occurrence of events. Informally, a liveness property stipulates that a 'good thing' happens during the evolution of a system. Some examples of liveness properties include starvation freedom – where the 'good thing' is the process making progress; termination – in which the good thing is for an evolution to *not* run forever; and guaranteed service – such as in resource allocation systems, when every request for resource is satisfied eventually. In this thesis, we consider supervisory policies for DESs that, when they exist, enforce a *liveness property* by appropriately disabling a subset of preventable events at certain states in the evolution of DES.

One of the main contributions of this thesis is the development of a *system-theoretic framework* for the analysis of *Liveness Enforcing Supervisory Policies* (LESPs) for DESs. We model uncertainties in the forward- and feedback-path, and present necessary and sufficient conditions for the existence of *Liveness Enforcing Supervisory Policies* (LESPs) for a general model of DESs in this framework. The existence of an LESP reduces to the membership of the initial state to an appropriately defined set. The membership problem is *undecidable*. For characterizing *decidable* instances of this membership problem, we consider a modeling paradigm of DESs known as *Petri Nets*, which have applications in modeling concurrent systems, software design, manufacturing systems, etc.

Petri Net (PN) models are inherently monotonic in the sense that if a transition (which loosely represents an event of the DES) can fire from a marking (a non-negative integer-valued vector that represents the state of the DES being modeled), then it can also fire from any larger marking. The monotonicity creates a possibility of representing an infinite-state system using what can be called a "finite basis" that can lead to decidability. However, we prove that several problems of our interest are still undecidable for arbitrary PN models. That is, informally, a general PN model is still too powerful for the analysis that we are interested in. Much of the thesis is devoted to the characterization of decidable instances of the existence of LESPs for arbitrary PN models within the system-theoretic framework introduced in the thesis.

The philosophical implication of the results in this thesis is the existence of what can be called a "finite basis" of an infinite state system under supervision, on which the membership tests can be performed in finite time; hence resulting in the decidability of problems and finite-time termination of algorithms. The thesis discusses various scenarios where such a finite basis exists and how to find them.

ACKNOWLEDGMENTS

I thank everyone for being them, for that made me who I am.

TABLE OF CONTENTS

CHAPTER 1

CONTEXT

1.1 Discrete Event Systems

A *Discrete Event System* (DES) is a discrete-state system, where the state changes at discrete-time instants due to the occurrence of events.

Definition 1. *A Discrete-Event System $\mathcal{D}$ is a two-tuple $\mathcal{D} = (S, R)$ where S is the set of states and $R \subseteq S \times S$ is a binary relation between pair of states denoting the set of events. We use $\mathcal{D}(s_0)$ to denote the DES $\mathcal{D}$ along with its initial state $s_0 \in S$.*

That is, if two states s_i and s_j are related: $s_i R s_j$, then it means that there is an event whose occurrence at s_i takes the DES to s_j. We write $Succ(s)$ (resp. $Pred(s)$) for the set $\{s' \in S : sRs'\}$ of immediate successors ($\{s' \in S : s'Rs\}$ of immediate predecessors) of state s. A DES $\mathcal{D}$ is called *finitely branching* if $Succ(s)$ is finite for all $s \in S$. In this thesis, we restrict our attention to finitely branching DESs. We make a simplifying assumption that all events in the DES occur instantaneously and asynchronously and that no two events occur simultaneously.

1.2 Liveness

Informally, a liveness property stipulates that a 'good thing' happens during the evolution of a system. Some examples of liveness properties include starvation freedom, termination, and guaranteed service. In starvation freedom, which states that a process makes progress infinitely often, the 'good thing' equates to making progress. A *deadlock* in which the system is *hung* is an example in which the system stops making progress. In termination, which asserts that an evolution does not run forever, the 'good thing' can be specified as reaching an appropriately defined final state. In guaranteed service, such as in resource allocation systems, every request for resource is satisfied eventually, the 'good thing' is a resource being allocated. For example, in *Autonomous Traffic Management* at intersections, if we

interpret the right-of-way as a resource, then a liveness property is every vehicle waiting at the intersection is guaranteed to enter the intersection eventually [1].

To further illustrate the significance and generality of liveness, let us consider the example of UAVs flying in a formation. The leader-follower architecture is one of the commonly studied formation architectures, in which one vehicle is designated as a leader and the others as followers. The nominal trajectory for the formation is set by the leader and the other vehicles continuously communicate with each other through sensors etc. to ensure that they are in the right position. Suppose there is a temporary communication breakdown and a subset of followers are completely on their own (that is, autonomous) for some amount of time. What should each vehicle do during that frame of time? Generally, the primary requirement (good thing) is that the vehicles do not collide with each other. The secondary requirement (good thing) is that they should not enter a state from which they cannot be a part of the formation anymore. Another example in which the same questions can be posed is the case when a Robot tasked to traverse a set of trajectories in a hostile environment suddenly loses control over some of its actuators, thus temporarily becoming an underactuated system. Being in a hostile environment, the primary requirement (good thing) can be that the Robot remains safe (see [2] for an actual case on similar lines). Next, we interpret the definition of liveness proposed by Alpern in [3] for DESs.

A sequence of states $s_0 s_1 s_2 \ldots$ is called a *valid sequence* if $\forall i \geq 0$: $(s_i, s_{i+1}) \in R$. That is, for all $i \geq 0$, there is an event that takes the system from state s_i to s_{i+1}. Let $S^\omega(s_0)$ ($S^*(s_0)$) denote the set of valid infinite (finite) sequences of states in S from the initial state s_0. Without loss of generality, an evolution of a DES can be modeled as a member of S^ω—if there is a terminating state, then the infinite sequence can be obtained by repeating the final state. That is, an evolution of $\mathcal{D}(s_0)$ is a valid infinite sequence (string) of states:

$$\mathcal{E}(\mathcal{D}(s_0)) = s_0 s_1 s_2 \ldots \tag{1.1}$$

We call elements of S^ω as *evolutions* and elements of S^* as *partial evolutions*. A *property* is a set of such sequences of states. We say that a property B holds true for an evolution $\mathcal{E}$ of $\mathcal{D}(s_0)$ if $\mathcal{E}(\mathcal{D}(s_0)) \subseteq B$. For ease of exposition, we will drop the argument $\mathcal{D}(s_0)$ when it is clear from the context. We write $\sigma \vDash B$ when evolution σ is in property B.

Definition 2. *A DES is live with respect to a property B if*

$$\forall \alpha \in S^*(s_0), \exists \beta \in S^\omega \text{ such that } \alpha\beta \vDash B \tag{1.2}$$

That is, every partial evolution can be extended to an evolution for which property B is

true. We introduce the semantics of *Supervisory Control* of DESs in the next section before moving on to investigating the existence and synthesis of liveness enforcing supervisory policies for the rest of the thesis.

1.3 Supervisory Control of Discrete Event Systems

We consider supervisory policies that, when they exist, enforce their desired objective by appropriately disabling a subset of preventable events at certain states in the evolution. We refer to such events as controllable events, and call its complementary subset of events as uncontrollable events. For specifying a supervisory policy, we need: (i) appropriate semantics that describe events in a DES, and (ii) an effective method that identifies the set of events that can occur at any state. We achieve the former by associating a labeling map L from the relation R (from Definition 1) to an alphabet Σ, and the latter by defining a transition function $\delta : \Sigma \times S \to 2^S$ defined as: $s' \in \delta(a, s)$ if and only if sRs' and $L((s, s')) = a$. We use $\Sigma_e : S \to 2^\Sigma$ to denote the *active event function* that identifies the set of all events $a \in \Sigma$ for a state s for which $\delta(a, s)$ is defined. If an event $e \in \Sigma_e(s)$ for some state s, we say that e is *state-enabled* at s.

Definition 3. *A Labeled Discrete Event System is a tuple $\mathcal{D} = (S, \Sigma, \delta)$ where S and Σ denote the set of states and labeled events respectively. The function $\delta : \Sigma \times S \to S$ is the state transition function, where for $s \in S, \sigma \in \Sigma : \delta(e, s) = \widehat{s}$, implies there is an event labeled e from state s to state $\widehat{s}$.*

Following the additional structure above, the set of events can be partitioned into controllable (Σ_c) and uncontrollable (Σ_u) events. We denote the supervisory policy by a function $\mathcal{P} : S \times \Sigma \to \{0, 1\}$ that returns a 0 or 1 for each state and each event. We say the event e is *control-enabled* at s if $\mathcal{P}(s, e) = 1$ for some state s. An event has to be state- and control-enabled before it can occur. The occurrence of an event e at state s changes the state to $s' = \delta(e, s)$. We would also represent this state-transition as: $s \xrightarrow{e} s'$. The supervisory policy does not control-disable any uncontrollable event, that is, $\mathcal{P}(s_i, e) = 1 \ \forall e \in \Sigma_u$. We would use the expression $\mathcal{D}(s_0)$ to denote a DES $\mathcal{D} = (S, \Sigma, \delta)$ with *initial state* $s_0 \in S$. Henceforth, we only consider *Labeled Discrete Event Systems* and will refer to them as just *Discrete Event Systems*.

1.4 Liveness Enforcing Supervisory Policies

If a DES is not live with respect to a property B, then it is of interest to evaluate a supervisory policy that can enforce liveness. In this section, we first define liveness in the context of supervisory control of DESs. Then we present necessary and sufficient conditions for the existence of a liveness enforcing supervisory policy.

A sequence of states of the DES $s_0 s_1 \ldots$ is said to be a *valid sequence under supervision* if $\forall i \geq 0$, $\exists e \in \Sigma_e(s_i)$ such that $\mathcal{P}(s_i, e) = 1$ and $s_{i+1} = \delta(e, s_i)$. Let $S^{\omega}_{\mathcal{P}}(s_0)$ ($S^{*}_{\mathcal{P}}(s_0)$) denote the set of valid infinite (finite) sequences of DES states starting from s_0 under supervision of $\mathcal{P}$. A DES is *live* under supervision of a policy $\mathcal{P}$ with respect to a property B if

$$\forall \alpha \in S^{*}_{\mathcal{P}}(s_0), \exists \beta \in S^{\omega}_{\mathcal{P}} \text{ such that } \alpha\beta \vDash B \tag{1.3}$$

We refer to such a policy as a *liveness enforcing supervisory policy* with respect to property B (B-LESP). Let σ_i denote the first i elements of a valid sequence of states σ. We can characterize a B-LESP by the set $\Delta(\mathcal{D})$, where we do not have B as an argument of $\Delta(\cdot)$ for simplicity, defined as follows:

Definition 4. *For a DES $\mathcal{D} = (S, \Sigma, \delta)$, $\Delta(\mathcal{D}) \subseteq S$ is the set of states with the following properties:*

1. *$\forall s \in \Delta(\mathcal{D})$, $\forall \alpha \in S^{*}(s), \exists \beta \in S^{\omega}$ such that:*
   - *(a) $\alpha\beta \vDash B$*
   - *(b) $\forall i$ such that $(\alpha\beta)_i \widehat{s} = (\alpha\beta)_{i+1}$, $\widehat{s} \in \Delta(\mathcal{D})$.*
2. *It is control invariant. That is, $\forall s_1 \in \Delta(\mathcal{D}), e_u \in \Sigma_e(s_1) \cap \Sigma_u$ and $s_1 \xrightarrow{e_u} s_2$, then $s_2 \in \Delta(\mathcal{D})$.*

Item 1 states that every partial evolution from a state in $\Delta(\mathcal{D})$ can be extended to an evolution for which property B holds. However, for every partial evolution from a state in $\Delta(\mathcal{D})$, there can also exist an evolution for which property B is not true— that is, it reaches a state that is *not* in $\Delta(\mathcal{D})$. The control invariance property assures that only a controllable event can take the DES to a state from where the property B cannot be made true. Then a supervisory policy $\widehat{\mathcal{P}}$ that disables a controllable event if and only if its occurrence takes the DES state outside the set $\Delta(\mathcal{D})$ is a B-LESP.

Definition 5. *$\forall s \in S$, $\forall e \in \Sigma$, the supervisory policy $\widehat{\mathcal{P}}$ is such that:*

1. *if $e \in \Sigma_u$, $\widehat{\mathcal{P}}(s, e) = 1$,*

2. *if* $e \in \Sigma_c$, *then* $\widehat{\mathcal{P}}(s,e) = 1$, *if and only if* $s \xrightarrow{e} s'$ *(in the absence of supervision), and* $s' \in \Delta(\mathcal{D})$.

The definitions also lead to the interpretation that $\Delta(\mathcal{D})$ is the collection of states for which a supervisory policy that can enforce liveness with respect to property B exists.

$$\Delta(\mathcal{D}) = \{s_0 \in S : \exists \text{ a B-LESP for } \mathcal{D}(s_0)\} \tag{1.4}$$

The following theorem follows directly from the definitions.

Theorem 1. *(*$s_0 \in \Delta(\mathcal{D})$*)* $\Leftrightarrow$ *(*$\exists$ *a B-LESP for* $\mathcal{D}(s_0)$*).*

Proof. (*Sketch*) If $s_0 \in \Delta(\mathcal{D})$, then the supervisory policy $\widehat{\mathcal{P}}$ defined above is a B-LESP for $\mathcal{D}(s_0)$.
It follows from Definition 4 that if $s_0 \notin \Delta(\mathcal{D})$, then $\exists\ \alpha \in S^*(s_0)$ for which $\nexists \beta \in S^\omega$ such that $\alpha\beta \vDash B$. □

A B-LESP $\mathcal{P}$ is said to be *minimally restrictive* if for every B-LESP $\widetilde{\mathcal{P}}$, the following condition holds: $\forall s \in S, \forall e \in \Sigma, \mathcal{P}(s,e) \geq \widetilde{\mathcal{P}}(s,e)$. Now, from Theorem 1, there exists a B-LESP for $\mathcal{D}(s_0)$ if and only if $s_0 \in \Delta(\mathcal{D})$. Definition 5 constrains the state of the DES to the set $\Delta(\mathcal{D})$. We get the following lemma:

Lemma 1. *If* $s_0 \in \Delta(\mathcal{D})$*, then the supervisory policy in Definition 5 is the minimally restrictive B-LESP for* $\mathcal{D}(s_0)$*.*

Proof. $\widehat{\mathcal{P}}$ disables an event only if its occurrence will take the state of the DES outside $\Delta(\mathcal{D})$. If there is a supervisory policy $\widetilde{\mathcal{P}}$ that is less restrictive than $\mathcal{P}$, then it must enable an event that takes the DES state outside $\Delta(\mathcal{D})$, upon which the DES will not be live. Then $\widetilde{\mathcal{P}}$ cannot be a B-LESP. □

1.5 Problem Statement and Background

The preceding discussion shows that the synthesis of a B-LESP reduces to the evaluation of $\Delta(D)$ or some subset of it having similar properties. How to evaluate $\Delta(\mathcal{D})$ is a critical question which we will be returning to at several points in the thesis. We discuss the computational aspects of this evaluation and a general framework for B-LESP synthesis next.

A *decision-problem*, that is posed as a "*yes*" or "*no*" question for each input, is *decidable* (resp. *undecidable*) if there exists (resp. does not exist) a single algorithm that correctly

answers "*yes*" or "*no*" to all possible inputs. It is *semi-decidable* if there exists a single algorithm that will always correctly answer "*yes*", but does not answer at all when the answer is "*no*". Every decision-problem has an associated *complementary* decision-problem. The answer to the complementary problem is "*yes*" if and only if the answer to the original decision problem is "*no*". A decision-problem is decidable if and only if the decision-problem *and* its complement, are semi-decidable (cf. section 1.2.2, [4]).

Informally, the definition of decidability suggests that decidable problems are those for which an algorithm that gives the correct answer, for all inputs, in finite time, exists. In other words, for a decidable problem, an algorithm that gives the correct answer, for all inputs, does so by performing finite number of tests. In the context of B-LESP synthesis, first and foremost is the nature of property B. There has been work in literature on how to characterize these properties; for example: [5] where they formally characterize liveness properties in terms of the structure of the Buchi automaton ([6]) that specifies the property. A discussion along these lines is not in the scope of this thesis. We tacitly assume that testing if a given string of states (evolution) satisfies property B is decidable.

Several important liveness properties of interest can be specified in one of the following two ways:

1. Condition on states: if a particular subset of states can be reached from every state in an evolution of the DES, for example: termination, starvation freedom etc..

2. Condition on events: for example, there must exist a state reachable from every state in the evolution such that a particular subset of events are state-enabled.

With these considerations, it is reasonable to expect the existence of B-LESPs to be decidable for several properties of interest for DES with finite state space. DES with finite state space were studied extensively by Ramadge and Wonham [7]. The accepted model for a finite state DES is that of a finite state automaton which is the model of Definition 3 with a finite number of states. A detailed treatment of this subject can be found in the book by Cassandras [8]. In this thesis we are particularly interested in DESs with infinite state-spaces. Infinite state systems have found applications in modeling of software systems, communication protocols etc..

Abdulla and others presented general principles for decidability results for infinite state systems in [9]. They observed that the main requirement for decidability is for the state-space to be equipped with a well-quasi order (Chapter 2 presents a formal definition) such that the transitions between states is "monotonic", in the sense that events from larger states lead to larger states. The condition of well-quasi order ensures every infinite sequence of states

contains an element that is equal to or larger than a previous element in the sequence. Such systems are referred to as *well-structured systems*. The theory for well structured transition systems (WSTS) is presented in detail in [10] where they even show that several classical computational models like basic process algebra ([11]), petri nets ([12]), communicating finite-state machines([13]) are instances of WSTS. In this thesis, we consider the Petri Net modeling paradigm, which is one particular instance of WSTS.

A PN model is a directed bipartite graph where the two sets of nodes are referred to as *places* and *transitions*. The edges connecting the places with the transitions and vice-versa are referred to as *arcs*. The arcs have weights associated with them. The initial marking, $\mathbf{m}^0$, of the PN associates a non-negative, integer-valued token-load to each place. A PN $N(\mathbf{m}^0)$ is essentially the *PN-structure* N along with an *initial-marking* $\mathbf{m}^0$. A transition is said to be *state-enabled* if the token-load of each of its input places is no less than the weight associated with the arc from the place to the transition. A state-enabled transition could *fire*, which reduces (resp. increases) the token-load of each of its input (resp. output) places according to the associated arc weights. This process repeats at the newly created token-load distribution (marking), as often as necessary.

There are several variations to the basic PN model discussed above, with many of them obtained by generalizing the properties of arcs [14, 15, 16]. *Inhibitor arcs* are those that forbid the firing of a transition unless a given subset of places is empty. They are also referred to as zero-test arcs. *Transfer arcs* are those which say whether all the tokens of a place must be added to another place. A similar idea is used define *reset arcs* that specify how the firing of transitions empties certain places. In an extension of PNs known as *Self Modifying Nets*, the arc weights are not constant but are a linear combination of the current token-load of places [17]. Another extension of PNs that has found application in modeling several behaviours is that of *Colored Petri Nets* in which colors are associated with tokens. [18] showed that the expressive power of colored PNs is equivalent to that of the basic model if the number of colors are finite. We will be considering only the basic model of PNs in this thesis.

In the context of PNs, we work with a specific case of liveness with respect to a particular property and would not explicitly write B with LESP, unless needed in the context. A PN is said to be *live* if it is possible to fire any transition, although not necessarily immediately, from any marking that is reachable from the *initial marking*. The supervisory policy enforces liveness by preventing the firing of a subset of *controllable* transitions, which correspond to controllable activities (or events) of the DES. On the other hand, the *uncontrollable* transitions represent activities (or events) that are external to the DES, which cannot be prevented from occurring by the supervisory policy. We present the notations and definitions

related to Petri Nets that we will be using in this thesis in Chapter 2.

We present a brief review of the literature pertinent to the synthesis of *liveness enforcing supervisory policies* (LESPs) for different classes of PNs. Giua [19] introduced *monitors* to supervisory control of PNs. Moody and Antsaklis [20] used monitors to enforce liveness in certain classes of PNs. This work was extended by Iordache and Antsaklis [21] to include a sufficient condition for the existence of policies that enforce liveness in a class of PNs called *Asymmetric Choice Petri nets*. Reveliotis et al. used the *theory of regions* to identify policies that enforce liveness in *Resource Allocation Systems* [22]. Ghaffari, Rezg and Xie [23] used the theory of regions to obtain a *minimally restrictive* supervisory policy that enforces liveness for a class of PNs. Marchetti and Munier-Kordon [24] presented a sufficient condition for liveness, that can be tested in polynomial time, for a class of general PNs known as *Unitary Weighted Event Graphs*. Basile et al. [25] presented sufficient conditions for minimally-restrictive, closed-loop liveness of a class of *Marked Graph* PNs supervised by monitors that enforce *Generalized Mutual Exclusion Constraints* (GMECs). [26] presented a necessary and sufficient condition for the existence of GMECs that enforces, among other things, liveness, in a bounded PN. Luo et al. [27] considered various properties of supervisory policies that ensure the marking of a PN stays within an appropriately defined polyhedron. Specifically, they consider the problem of eliminating redundant constraints in the polyhedron, which can be used to reduce the number of monitors in an invariant-based supervisor. Dideban et al. [28] used the concept of an *over-state* to reduce the number of monitors in an invariant-based controller for *safe* PNs. Tricas et al. [29] studied deadlocks in terms of *circular waits* in S^4PR nets. They showed the circular wait situation corresponds to a particular marking related to a siphon of this model. Cordone et al. [30] investigated simplified *linear and nonlinear classifiers* that are maximally permissive for deadlock avoidance in resource allocation systems. Chen and Li [31] used the vector covering approach to reduce the sets of legal markings and *first met bad* markings, resulting in a maximally permissive control policy. Hu et al. [32] found that the liveness of the PNs with flexible routes and assembly operations can be attributed to the absence of *undermarked siphons*, which is realizable by synthesizing a proper supervisory controller.

We are interested in the analysis of existence and synthesis of LESPs for a general class of PNs. Specifically, for a PN structure N with n places, we are interested in understanding the nature of the set $\Delta(N)$ defined as follows:

$$\Delta(N) = \{\mathbf{m}^0 \in \mathcal{N}^n : \text{there exists an LESP for } N(\mathbf{m}^0)\}, \tag{1.5}$$

where $\mathcal{N}$ denotes the set of non-negative integers. The set $\Delta(N)$ is analogous to the set

$\Delta(\mathcal{D})$ discussed in Definition 4. The test for existence (resp. non-existence) of an LESP for an initial marking reduces to the decision-problem – "*Is* $\mathbf{m}^0 \in \Delta(N)$?" (resp. "*Is* $\mathbf{m}^0 \notin \Delta(N)$?"). Reference [33] proved that "*Is* $\mathbf{m}^0 \in \Delta(N)$?" is undecidable for arbitrary PNs by reducing it to the *Reachability Inclusion Problem* [34]. This result was further refined in [35]. Although undecidable for arbitrary PNs, there are classes of PNs, with certain structural properties, for which the existence of an LESP is decidable [35, 36, 37, 38]. The $\mathcal{H}$-class of PN structures is the largest among the decidable classes identified in those references [37]. The $\mathcal{H}$-class has the following structural properties: (1) for each place, the weights associated with the outgoing arcs that terminate on uncontrollable transitions must be the smallest of all outgoing arc-weights; (2) the set of input places to each uncontrollable transition is no larger than the set of input places of any transition which shares a common input place with it. For these classes of PNs, $\Delta(N)$ is *right-closed*. That is, if there exists an LESP for an initial marking, then there exists a (possibly different) LESP for all term-wise larger initial markings as well.

If a transition is permitted to fire by a *marking monotone* policy (MM-policy) at a marking $\mathbf{m} \in \mathcal{N}^n$, then it will be permitted to fire at any marking $\widehat{\mathbf{m}} \geq \mathbf{m}$, as well. If an MM-policy that is an LESP for $N(\mathbf{m}^0)$ is also an LESP for $N(\widehat{\mathbf{m}}^0)$ for any $\widehat{\mathbf{m}}^0 \geq \mathbf{m}^0$, then we say there is a *marking monotone LESP* (MM-LESP) for $N(\mathbf{m}^0)$. That is, if there is an MM-LESP for $N(\mathbf{m}^0)$, then there is an MM-LESP for $N(\widehat{\mathbf{m}}^0)$ for any $\widehat{\mathbf{m}}^0 \geq \mathbf{m}^0$, which means the set

$$\Delta_M(N) = \{\mathbf{m}^0 \in \mathcal{N}^n : \text{ there exists an MM-LESP for } N(\mathbf{m}^0)\},$$

is right-closed, and $\Delta_M(N) \subseteq \Delta(N)$. Note that if $\Delta(N)$ is right-closed, then $\Delta_M(N) = \Delta(N)$ (because the firing of a transition results in a larger marking if it is fired from a larger initial marking). Coincidentally, if $N \in \mathcal{H}$, then $\Delta(N) = \Delta_M(N)$ [37]. These results in the literature provide pointers on a possible approach to expand the class of PNs for which the existence of an LESP is decidable. First, by restricting the properties of the set $\Delta(N)$ (for example, right-closure); and second, by restricting the nature of the LESP (for example, MM-LESPs). In Chapter 3, we explore this direction.

With an objective of characterizing the structure and properties of PNs for which the existence and non-existence of an LESP is decidable, we start with investigating if it is the right-closure of $\Delta(N)$ that is the reason for the decidability of LESP. We characterize the exhaustive class of PNs, $\widehat{\mathcal{H}}$, such that $(N \in \widehat{H}) \Leftrightarrow (\Delta(N)$ is right-closed). Testing membership in $\widehat{\mathcal{H}}$-class is posed as the decision problems: "*Is* $\Delta(N)$ *right-closed?*" and "*Is* $\Delta(N)$ *not right-closed?*". We then observe that an empty set is right-closed by definition. Consequently, a positive result for the decision problem "*Is* $\Delta(N)$ *right-closed?*" would mean

that there are either countably-infinite markings or no markings for which an LESP exists. Therefore, before venturing into the decision problem of right-closure, we investigate the decision-problems: "*Is* $\Delta(N) = \emptyset$*?*" and "*Is* $\Delta(N) \neq \emptyset$*?*". In addition to being associated with right-closure, these can also be interpreted as a generalization of the decision problems: "*Is* $\mathbf{m}^0 \in \Delta(N)$*?*" and "*Is* $\mathbf{m}^0 \notin \Delta(N)$*?*" studied in [33] and [35]. We then show that "*Is* $\Delta(N) = \emptyset$*?*" and "*Is* $\Delta(N) \neq \emptyset$*?*" are not semi-decidable for arbitrary PNs.

Coming back to right-closure, we prove that "*Is* $\Delta(N)$ *right-closed?*" is not decidable. Then we further reduce the scope of the problem and investigate a variation to right-closure. We attempt to determine that for a given PN N, if there exists a *subset* of markings, $\widetilde{\Delta}(N) \subseteq \Delta(N)$, that is right-closed. This relaxation does not improve the results, and the decision problems: "*Is there a right-closed subset of* $\Delta(N)$*?*" and "*Is there no right-closed subset of* $\Delta(N)$*?*" are also not semi-decidable.

At the end, we turn our attention at restricting the nature of LESPs. We pose the decision problems: *"Is* $\mathbf{m}^0 \in \Delta_M(N)$*?"* and *"Is* $\mathbf{m}^0 \notin \Delta_M(N)$*?"* and prove that it is decidable. That is, the existence and non-existence of an MM-LESP for an arbitrary PN is decidable. Moreover, the algorithm for decidability also evaluates the largest $\Delta_M(N)$, if $\Delta_M(N) \neq \emptyset$.

Thus, starting from the two decision problems: *"Is* $\mathbf{m}^0 \in \Delta(N)$*?"* and *"Is* $\mathbf{m}^0 \notin \Delta(N)$*?"* that are not semi-decidable, we present a string of results that culminate in decidable sub-problems: *"Is* $\mathbf{m}^0 \in \Delta_M(N)$*?"* and *"Is* $\mathbf{m}^0 \notin \Delta_M(N)$*?"*. These results lead to the conclusion that extracting any kind of information about $\Delta(N)$ for an arbitrary PN is most likely an extremely hard problem. Besides, we can also conclude that between the properties of the set of initial markings for which an LESP exists, and the characteristics of the LESP, it is the characteristics of the LESP that plays a prominent role in determining decidability. To be specific, let $\mathfrak{R}(N, \mathbf{m}, \mathcal{P})$ denote the set of reachable markings for $N(\mathbf{m})$ under the supervision of an LESP $\mathcal{P}$. If a supervisory policy $\mathcal{P}$ is such that $\mathfrak{R}(N, \mathbf{m}, \mathcal{P})$ (which can have an unbounded number of markings) can be reduced to a reachability graph with a finite number of appropriately defined symbolic markings such that the liveness property is preserved, then the existence of $\mathcal{P}$ is likely to be decidable. We take this direction forward in Chapter 4.

As noted earlier during the discussion of WSTSs, PNs have an inherent monotonicity in their operation in that if a transition can fire from a smaller marking, then it can also fire from any larger marking. In addition, the marking resulting from the firing of a transition from a larger marking is greater than the marking that results from the firing of the same transition at a smaller marking. Infinite (finite) state systems can be modeled by what are known as *unbounded (resp. bounded) PNs* (see for eg. [39]). However, an algorithm for determining the reachability of a state in unbounded PNs does not exist to date. Consequently a

majority of the automated analysis of PNs is done using an abstraction of reachability graphs known as *coverability graphs*. The coverability graph of a PN is essentially the *Karp and Miller Tree* [40], where duplicate nodes are merged as one. Due to the inherent monotonicity in the operation of PNs, if there is a string of transitions that can be fired from a marking that results in a larger marking, then the string of transitions can be fired as often as necessary, resulting in an infinite sequence of increasing markings. The main concept behind the coverability graph is to represent this infinite sequence of increasing markings by a single symbolic marking. With this abstraction, the coverability graph becomes a finite representation of a possibly infinite reachability graph of a PN, with possibly some loss of analytical fidelity. The loss of information in the coverability graph notwithstanding, they are easy to generate and have found use in testing for boundedness of places [41], existence of dead transitions, and Model Checking [42], and others. In Chapter 4, we develop a generalized notion of coverability graph by appropriately defining the *order* among markings. That is, a general interpretation of the operator "$\geq$". We illustrate the utility of this generalization through an algorithm that can be used to test the existence and non-existence LESPs for a wide class of PNs. The generalization presented in this chapter retains more information about the behaviour of the underlying PN as compared to the traditional coverability graph. Consequently, it can also be effectively used in other applications of coverability graphs like model checking.

Having investigated the existence and synthesis of B-LESP for general DES models and its decidability in the context of PN models of DES, we move towards a general framework for DES. From Theorem 1, the existence of a B-LESP for a DES $\mathcal{D}(s_0)$ reduces to a membership problem to the set $\Delta(\mathcal{D})$. Suppose the initial state is in $\Delta(\mathcal{D})$. Then for every state s received by the supervisor and every event e, the minimally restrictive B-LESP $\widehat{\mathcal{P}}$ of Definition 5 first tests if enabling e results in a marking in $\Delta(\mathcal{D})$; if yes, then e is control-disabled. In addition to evaluating $\Delta(\mathcal{D})$— aspects of which we will discuss in Chapters 3 and 4, there are three key components to this method: (i) the state s, (ii) the evaluation of the state resulting from occurrence of event e from s, and (iii) the action of enabling or disabling the event. Keeping these steps in mind, in Chapter 5, we tackle a general class of problem in which the supervisory action can be impeded due to various reasons:

1. Oftentimes due to limitations of the communication channel, partial observability of states, noise or faults, the supervisor may not receive precise state information. Besides, in some cases, like for the purpose of security and privacy, precise state information may be deliberately not communicated to the supervisor.

2. Invariably, whenever there is uncertainty, a natural thing to do is to bring in the

analysis of estimation or learning of parameters of the system in order to mitigate its effects. A detailed analysis in this direction, which can also include estimation of transition function, δ, of $\mathcal{D}$ among other things, is out of the scope of this thesis, but we do include a simplified interpretation. We assume that the supervisor receives a fixed set $\Theta \subseteq \mathcal{S}$ as the set of *ground states* or the *set of feasible actual states* from an estimator as supplemental information.

3. We also consider faults in the feedback channel that modify the supervisory action. As a consequence, the policy actually supervising the DES can be different to the one prescribed by the supervisor.

Figure 1.1 presents a block diagram of the framework that we have discussed. We will formally discuss the framework in Chapter 5 of the thesis.

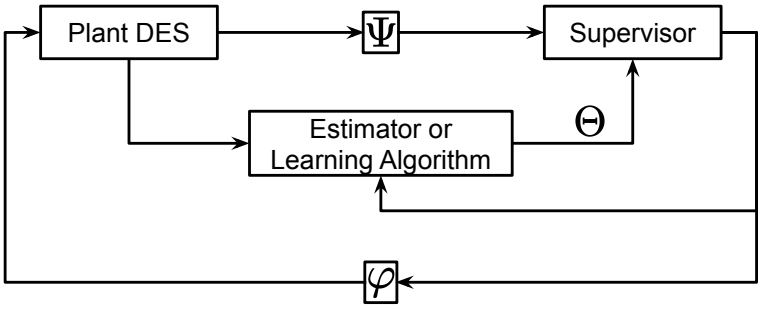


Figure 1.1: Supervisory Control Framework

We first define $\Delta(\mathcal{D})$-like sets for specifying the necessary and sufficient conditions for the existence of B-LESPs under this framework. Then we consider PN models and discuss the existence and synthesis of LESPs for two specific cases: partial observability in the forward path (an appropriately defined Ψ operator), and controllability faults in the feedback path (an appropriately defined φ operator).

There are two notions of observability in the PN paradigm ([43], [44], [45]). A large volume of literature on PNs considers the semantic in which information about the firing of transitions is communicated with the supervisor and the supervisor then reconstructs the marking of the PN based on the transition-firing sequence. Partial Observability in this paradigm refers to the case when the transitions of the PN are partitioned into observable and unobservable. Compatible with our framework of Figure 1.1, we are interested in the second notion of partial observation in which the token-load of some of the places of the PN is not known. The main idea behind controller synthesis in this set-up is that there is a

controller that can enforce a certain property only if the control action is same for all possible actual markings of the system reconstructed from the partial token-load information.

Fault-tolerance in DES modeled by PNs has largely been explored in the context of unreliable resources. Informally stated, resources are modeled as tokens and a resource (token) that was previously available can become unavailable due to faults. The unreliable availability of tokens in a PN model can take a PN from a live state to a deadlocked state. References [46, 47, 48, 49, 50] present Fault-tolerant deadlock avoidance algorithm with unreliable resources for assembly and several manufacturing processes respectively. Reference [51] presents a supervisory control framework for deadlock avoidance in sequential RASs with resource outages. References [52] and [53] discuss deadlock avoidance problem in Automated Manufacturing Systems modeled by PNs with unreliable resources. Reference [54] considers faults in controllers that are modeled by PNs. In this Chapter, we consider failure events where a subset of controllable transitions becomes temporarily uncontrollable at an arbitrary discrete-time instant. This could be due to a device- or line-fault, where communication between supervisor and plant is temporarily unavailable; or due to the activity of a malicious-user. We assume that the loss of controllability happens only for a finite number of event occurrences. The main idea behind LESP synthesis is to construct appropriately defined subsets of $\Delta(N)$ and nominally constrain the marking of the PN to those subsets, such that even when the fault does happen, the marking stays inside $\Delta(N)$.

We conclude the thesis in Chapter 6 where some areas for future research are also suggested.

CHAPTER 2

NOTATIONS AND DEFINITIONS

We use $\mathcal{N}$ ($\mathcal{N}^+$) to denote the set of non-negative (positive) integers. The term $card(\bullet)$ denotes the cardinality of the set argument. The symbol Σ^* denotes the set of all possible strings (including the empty string) that can be constructed from an alphabet Σ.

A binary relation $\sim$ on a set X is *reflexive* if $a \sim a$, *symmetric* if $(a \sim b) \Leftrightarrow (b \sim a)$, and *transitive* if $((a \sim b) \wedge (b \sim c)) \Leftrightarrow (a \sim c)$, for $a, b, c \in X$. A *Quasi Ordering* (qo) is any reflexive and transitive relation. A *well quasi ordering* (wqo) is a qo in which every strictly decreasing sequence and every subset of incomparable elements is finite. For a well quasi ordered set, every nonempty subset has atleast one but no more than finite number of minimal elements [55]. A wqo is a *well order* if every nonempty subset has exactly one minimal element.

The unit vector whose i-th value is unity is represented as $\mathbf{1}_i$. Given two integer-valued vectors $\mathbf{x}, \mathbf{y} \in \mathcal{N}^k$, we use the notation $\mathbf{x} \geq \mathbf{y}$ if $\mathbf{x}_i \geq \mathbf{y}_i$ for all $i \in \{1, 2, \ldots k\}$. We use the term $\max\{\mathbf{x}, \mathbf{y}\}$ to denote the vector whose i-th entry is $\max\{\mathbf{x}_i, \mathbf{y}_i\}$.

Suppose $\mathbf{x}_1, \ldots, \mathbf{x}_k \in \mathcal{R}^n$, and $\lambda_1, \ldots, \lambda_k \in \mathcal{R}$, where $\mathcal{R}$ denotes the set of real numbers. Then $\sum_{i=1}^{k} \lambda_i \mathbf{x}_i$ is a *convex combination* of the vectors $\mathbf{x}_1, \ldots, \mathbf{x}_k \in \mathcal{R}^n$ if $\forall i, \lambda_i \geq 0$ and $\sum_{i=1}^{k} \lambda_i = 1$. The *Minkowski sum* of $\mathcal{A} \subseteq \mathcal{R}^n$ and $\mathcal{B} \subseteq \mathcal{R}^n$ is the set $\{a + b : a \in \mathcal{A}, b \in \mathcal{B}\}$. The *convex-hull* $conv(\{\mathbf{x}_1, \ldots, \mathbf{x}_k\})$ of a set of vectors $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ is the smallest convex set that contains it. We use the term $Int(\bullet)$ to denote the set of integer-valued vectors contained in the set argument. For instance, $Int(conv(\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}))$ denotes the set of integer-valued vectors in the convex hull of $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$.

A *Petri net structure* $N = (\Pi, T, \Phi, \Gamma)$ is an ordered 4-tuple, where $\Pi = \{p_1, \ldots, p_n\}$ is a set of n *places*, $T = \{t_1, \ldots, t_m\}$ is a collection of m *transitions*, $\Phi \subseteq (\Pi \times T) \cup (T \times \Pi)$ is a set of *arcs*, and $\Gamma : \Phi \rightarrow \mathcal{N}^+$ is the *weight* associated with each arc. A PN is said to be *Ordinary* if the weights associated with its arcs is unitary. That is, $\forall \tau \in \Phi, \Gamma(\tau) = 1$. The *initial marking function* (or the *initial marking*) of a PN structure N is a function $\mathbf{m}^0 : \Pi \rightarrow \mathcal{N}^n$, which identifies the number of *tokens* in each place. The marking can be interpreted as an integer-valued vector where the i-th component represents the token load of the i-th place $p_i \in \Pi$. For ease of exposition, some of the symbols that we have used to denote a

marking are specific to that particular section. The meaning of a particular symbol should be clear from the context.

We use the notation $\mathbf{m}(p)$ to denote the tokens in place $p \in \Pi$. Let $\Pi_1 \subseteq \Pi_2 \subseteq \Pi$, $\mathbf{m}^1 \in \mathcal{N}^{card(\Pi_1)}$ and $\mathbf{m} \in \mathcal{N}^{card(\Pi_2)}$. We use the notation $\mathbf{m}(\Pi_1) = \mathbf{m}^1$ to denote $\mathbf{m}(p) = \mathbf{m}^1(p)$, for all $p \in \Pi_1$.

We will use the term *Petri net* (PN) and the symbol $N(\mathbf{m}^0)$ to denote a PN structure N along with its initial marking $\mathbf{m}^0$. In graphical representations of PNs, the places are represented by circles, transitions by rectangles, and arcs are represented by directed edges. For brevity, only the non-unitary arc-weights are placed alongside arcs in graphic representations of PNs in this paper. The tokens are represented by filled-circles that reside in the circles that represent places. The set of transitions in the PN is partitioned into controllable- ($T_c \subseteq T$) and uncontrollable-transitions ($T_u \subseteq T$). The controllable (uncontrollable) transitions are represented as filled (unfilled) boxes in graphical representation of PNs.

We define the sets ${}^\bullet x = \{y | (y,x) \in \Phi\}$ and $x^\bullet = \{y | (x,y) \in \Phi\}$. A transition $t \in T$ is said to be *state-enabled* at a marking $\mathbf{m}^i$ if $\forall p \in {}^\bullet t, \mathbf{m}^i(p) \geq \Gamma(p,t)$. The set of state-enabled transitions at marking $\mathbf{m}^i$ is denoted by the symbol $T_e(N, \mathbf{m}^i)$.

If $t_j \in T_e(N, \mathbf{m})$, then $\mathbf{m} \geq \mathbf{IN}_{\bullet,j}$, which is the j-th column of the $n \times m$ *input matrix* $\mathbf{IN}$, defined as

$$\mathbf{IN}_{i,j} = \begin{cases} \Gamma(p,t) & \text{if } p_i \in {}^\bullet t_j, \\ 0 & \text{otherwise.} \end{cases}$$

The *output matrix* is an $n \times m$ matrix that encodes the firing of an enabled transition:

$$\mathbf{OUT}_{i,j} = \begin{cases} \Gamma(t,p) & \text{if } p_i \in t_j^\bullet, \\ 0 & \text{otherwise.} \end{cases}$$

The *incidence matrix* $\mathbf{C}$ of the PN N is an $n \times m$ matrix, where $\mathbf{C} = \mathbf{OUT} - \mathbf{IN}$.

A supervisory policy $\mathcal{P} : \mathcal{N}^n \times T \rightarrow \{0,1\}$, is a function that returns a 0 or 1 for each marking and each transition. The supervisory policy $\mathcal{P}$ permits the firing of transition t_j at marking $\mathbf{m}^i$, if and only if $\mathcal{P}(\mathbf{m}^i, t_j) = 1$. If $\mathcal{P}(\mathbf{m}^i, t_j) = 1$ for some marking $\mathbf{m}^i$, we say the transition t_j is *control-enabled* at $\mathbf{m}^i$. A transition has to be state- and control-enabled before it can fire. To reflect the fact that the supervisory policy does not control-disable any uncontrollable transition, we assume that $\forall \mathbf{m}^i \in \mathcal{N}^n, \mathcal{P}(\mathbf{m}^i, t_j) = 1$, if $t_j \in T_u$. A state- and control-enabled transition t can fire, which changes the marking $\mathbf{m}^i$ to $\mathbf{m}^{i+1}$ according to $\mathbf{m}^{i+1}(p) = \mathbf{m}^i(p) - \Gamma(p,t) + \Gamma(t,p)$.

A string of transitions $\sigma = t_1 \ldots t_k$, where $t_j \in T$ ($j \in \{1, \ldots, k\}$), is said to be a *valid firing string* starting from the marking $\mathbf{m}^i$ if 1) the transitions $t_1 \in T_e(N, \mathbf{m}^i)$, $\mathcal{P}(\mathbf{m}^i, t_1) = 1$,

and 2) for $j \in \{1, 2, \ldots, k-1\}$, the firing of the transition t_j produces a marking $\mathbf{m}^{i+j}$ and $t_{j+1} \in T_e(N, \mathbf{m}^{i+j})$ and $\mathcal{P}(\mathbf{m}^{i+j}, t_{j+1}) = 1$. If $\mathbf{m}^{i+k}$ results from the firing of $\sigma \in T^*$ starting from the initial marking $\mathbf{m}^i$, we represent it symbolically as $\mathbf{m}^i \xrightarrow{\sigma} \mathbf{m}^{i+k}$. If $\mathbf{x}(\sigma)$ is an m-dimensional vector whose i-th component corresponds to the number of occurrences of t_i in a valid string σ, and if $\mathbf{m}^i \xrightarrow{\sigma} \mathbf{m}^j$, then $\mathbf{m}^j = \mathbf{m}^i + \mathbf{C}\mathbf{x}(\sigma)$.

Given an initial marking $\mathbf{m}^0$, the set of *reachable markings* for $\mathbf{m}^0$, which is denoted by $\mathfrak{R}(N, \mathbf{m}^0)$, is defined as the set of markings generated by all valid firing strings starting with marking $\mathbf{m}^0$ in the PN N. The set of reachable markings under the supervision of $\mathcal{P}$ in N from the initial marking $\mathbf{m}^0$ is denoted by $\mathfrak{R}(N, \mathbf{m}^0, \mathcal{P})$.

A PN $N(\mathbf{m}^0)$ is said to be *live* if $\forall t \in T, \forall \mathbf{m}^i \in \mathfrak{R}(N, \mathbf{m}^0), \exists \mathbf{m}^j \in \mathfrak{R}(N, \mathbf{m}^i)$ such that $t \in T_e(N, \mathbf{m}^j)$ (cf. *level 4 liveness*, [12, 56]). A transition t_k is *live* under the supervision of $\mathcal{P}$, if $\forall \mathbf{m}^i \in \mathfrak{R}(N, \mathbf{m}^0, \mathcal{P}), \exists \mathbf{m}^j \in \mathfrak{R}(N, \mathbf{m}^i, \mathcal{P})$ such that $t_k \in T_e(N, \mathbf{m}^j)$ and $\mathcal{P}(\mathbf{m}^j, t_k) = 1$. A policy $\mathcal{P}$ is a *liveness enforcing supervisory policy* (LESP) for $N(\mathbf{m}^0)$ if all transitions in $N(\mathbf{m}^0)$ are live under $\mathcal{P}$. The policy $\mathcal{P}$ is said to be *minimally restrictive* if for every LESP $\widehat{\mathcal{P}} : \mathcal{N}^n \times T \to \{0, 1\}$ for $N(\mathbf{m}^0)$, the following condition holds: $\forall \mathbf{m}^i \in \mathcal{N}^n, \forall t \in T, \mathcal{P}(\mathbf{m}^i, t) \geq \widehat{\mathcal{P}}(\mathbf{m}^i, t)$. The set

$$\Delta(N) = \{\mathbf{m}^0 : \exists \text{ an LESP for } N(\mathbf{m}^0)\}$$

represents the set of initial markings for which there is an LESP for a PN structure N. The set $\Delta(N)$ is *control invariant* with respect to N. That is, if $\mathbf{m}^1 \in \Delta(N), t_u \in T_e(N, \mathbf{m}^1) \cap T_u$ and $\mathbf{m}^1 \xrightarrow{t_u} \mathbf{m}^2$ in N, then $\mathbf{m}^2 \in \Delta(N)$. Equivalently, only the firing of a controllable transition at any marking in $\Delta(N)$ can result in a new marking that is not in $\Delta(N)$. There is an LESP for $N(\mathbf{m}^0)$ if and only if $\mathbf{m}^0 \in \Delta(N)$. If $\mathbf{m}^0 \in \Delta(N)$, the LESP that prevents the firing of a controllable transition at any marking when its firing would result in a new marking that is not in $\Delta(N)$, is the minimally restrictive LESP for $N(\mathbf{m}^0)$ [33].

A supervisory policy $\mathcal{P} : \mathcal{N}^n \times T \to \{0, 1\}$ is a *marking monotone policy* (MM-policy) if $\forall \widehat{\mathbf{m}} \geq \mathbf{m}, \forall t \in T, \mathcal{P}(\widehat{\mathbf{m}}, t) \geq \mathcal{P}(\mathbf{m}, t)$. That is, if a transition is permitted by an MM-policy at a marking, it will be permitted at a larger marking as well. If an MM-policy that is an LESP for $N(\mathbf{m}^0)$, is also an LESP for $N(\widehat{\mathbf{m}}^0), \forall \widehat{\mathbf{m}}^0 \geq \mathbf{m}^0$, then it is said to be a *marking-monotone LESP* (MM-LESP) for $N(\mathbf{m}^0)$. The set

$$\Delta_M(N) = \{\mathbf{m}^0 : \exists \text{ an MM-LESP for } N(\mathbf{m}^0)\}$$

denotes the set of initial marking for there is an MM-LESP for the PN structure N. It follows that $\Delta_M(N) \subseteq \Delta(N)$.

A set of markings $\mathcal{M} \subseteq \mathcal{N}^n$ is said to be *right-closed* if $((\mathbf{m}^1 \in \mathcal{M}) \wedge (\mathbf{m}^2 \geq \mathbf{m}^1) \Rightarrow (\mathbf{m}^2 \in \mathcal{M}))$. A right-closed set, $\mathcal{M}$, is uniquely identified by its finite set of minimal elements denoted by $\min(\mathcal{M})$. The empty-set is right-closed by definition; and $\Delta_M(N) \subseteq \Delta(N)$, is right-closed for any PN structure N.

The $\mathcal{H}$-class of PN structures is identified by the following structural properties: (1) for each place, the weights associated with the outgoing arcs that terminate on uncontrollable transitions must be the smallest of all outgoing arc-weights; (2) the set of input places to each uncontrollable transition is no larger than the set of input places of any transition which shares a common input place with it. Formally stated, let $\Omega(t) = \{\widehat{t} \in T | {}^\bullet t \cap {}^\bullet \widehat{t} \neq \emptyset\}$ denote the set of transitions that share a common input place with $t \in T$ for a PN structure $N = (\Pi, T, \Phi, F)$. A PN structure $N \in \mathcal{H}$ if and only if $\forall p \in \Pi$, $\forall t_u \in p^\bullet \cap T_u$, we have $(\Gamma(p, t_u) = min_{t \in p^\bullet} \Gamma(p, t)) \wedge (\forall t \in \Omega(t_u), {}^\bullet t_u \subseteq^\bullet t)$. For these classes of PNs, $\Delta(N)$ is *right-closed* [37].

A PN structure is *free-choice* (FC) if $\forall p \in \Pi$, $card(p^\bullet) > 1 \Rightarrow {}^\bullet(p^\bullet) = \{p\}$, where $card(\bullet)$ denotes the cardinality of the set argument. In other words, a PN structure is free-choice if and only if an arc from a place to a transition is either the unique output arc from that place, or, is the unique input arc to the transition. $\Delta(N)$ is right-closed for an FCPN and the existence of an LESP for $N(\mathbf{m}_0)$ is decidable [35].

CHAPTER 3

EXISTENCE OF LIVENESS ENFORCING SUPERVISORY POLICIES FOR PETRI NETS

3.1 Interpretation of the definition of Liveness for Petri Nets

In Chapter 2, we mentioned that in the context of PNs, we say that transition t_k is *live* under the supervision of $\mathcal{P}$, if $\forall \mathbf{m}^i \in \mathfrak{R}(N, \mathbf{m}^0, \mathcal{P}), \exists \mathbf{m}^j \in \mathfrak{R}(N, \mathbf{m}^i, \mathcal{P})$ such that $t_k \in T_e(N, \mathbf{m}^j)$ and $\mathcal{P}(\mathbf{m}^j, t_k) = 1$. A policy $\mathcal{P}$ is a *liveness enforcing supervisory policy* (LESP) for $N(\mathbf{m}^0)$ if all transitions in $N(\mathbf{m}^0)$ are live under $\mathcal{P}$. In addition, the set $\Delta(N)$ represents the set of initial markings for which there is an LESP for a PN structure N.

In the context of the definitions given by Alpern [3], for a general case, enforcing $\Delta(N)$ is equivalent to enforcing a liveness property and not necessarily equivalent to enforcing a safety property. If B is a safety property, then $\forall \sigma \in S^\omega$:

$$(\sigma \not\vDash B) \Rightarrow (\exists i \in \mathcal{N} : \forall \beta \in S^\omega, \sigma_i \beta \not\vDash B) \tag{3.1}$$

A safety property means that if an infinite string is not in B, then there exists a finite substring for which every extension results in string not in B. Informally, a safety property implies that: (i) a bad thing never happens; (ii) if it happens, it is irremediable; and (iii) the point at which the bad thing happens is an identifiable point. Now, when the objective is to enforce $\Delta(N)$, the bad thing would be the marking leaving the set; and it leaves the set at an identifiable point.

Let us consider a marking $\mathbf{m}^0 \notin \Delta(N)$. It is possible that for every marking reachable from $\mathbf{m}^0$ there is an uncontrollable way of reaching a marking in $\Delta(N)$ and also an uncontrollable way of reaching a marking that is not in $\Delta(N)$. Because of the "every" clause in the definition of a safety property, enforcing $\Delta(N)$ is not equivalent to enforcing a safety property, for a general case, if we strictly go by the definition given by Alpern. However, we can draw some philosophical parallels. The relation between enforcing $\Delta(N)$ and a safety property depends entirely on the interpretation of "*irremediable*" in the context of supervisory control. We do not delve any deeper into this discussion in this thesis but just mention that if we interpret

irremediable as no *guaranteed* way of reaching $\Delta(N)$, then philosophically, enforcing $\Delta(N)$ is equivalent to enforcing a safety property.

3.2 Right-Closure of $\Delta(N)$

In Chapter 1, we noted that the $\mathcal{H}$-class of PN structures is the largest among the classes identified in [35, 36, 37, 38] for which the existence of an LESP is decidable and for which $\Delta(N)$ is right-closed. Consider the PN structure N_1 shown in Fig. 3.1. It does not belong to $\mathcal{H}$-class as the outgoing arcs of place p_1 violate the $\mathcal{H}$-class restriction. However, it can be verified that $\Delta(N_1) = \{\mathbf{m} \in \mathcal{N}^5 : (\mathbf{m}(p_1) + \mathbf{m}(p_2) + \mathbf{m}(p_3) + \mathbf{m}(p_4) + \mathbf{m}(p_5) \geq 1)\}$, is indeed right-closed. This example illustrates that there are PN structures that do not belong to $\mathcal{H}$-class but still have a right-closed $\Delta(N)$. In this section, we present a necessary and sufficient condition for the right-closure of $\Delta(N)$ for an arbitrary PN structure N.

Recall that for an uncontrollable transition t_u, $\mathbf{IN}_{t_u}$ is the smallest integer-valued vector that state-enables t_u. Let $\mathbf{P} = Int(conv(\{\mathbf{IN}_{t_u}\}_{t_u \in T_u}))$ (resp. $k \times \mathbf{P} = Int(conv(\{k \times \mathbf{IN}_{t_u}\}_{t_u \in T_u})), k \in \mathcal{N}$) denote the set of integer-valued vectors in the convex-hull of the columns of the input matrix $\mathbf{IN}$ (resp. k times the columns of the input matrix $\mathbf{IN}$) that correspond to the uncontrollable transitions in N.

Let $\widehat{\mathcal{H}}$ be a class of PN structures where for any $N \in \widehat{\mathcal{H}}$,

$$(\mathbf{m} \in \Delta(N)) \Rightarrow ((\mathbf{m} + \mathbf{P}) \subset \Delta(N)). \tag{3.2}$$

That is, if $\mathbf{m} \in \Delta(N)$, then $\forall \mathbf{x} \in \mathbf{P}, (\mathbf{m} + \mathbf{x}) \in \Delta(N)$. The operator "+" in Equation 3.2 denotes the Minkowski Sum as defined in Section 2. Note that recursing over the expression in Equation 3.2 will give us an equivalent condition: $(\mathbf{m} \in \Delta(N)) \Rightarrow ((\mathbf{m} + k \times \mathbf{P}) \subset \Delta(N)), k \in \mathcal{N}$. The following result shows that for any $N \in \widehat{\mathcal{H}}$ the set $\Delta(N)$ is right-closed; and if $\Delta(N)$ right-closed, then $N \in \widehat{\mathcal{H}}$.

Theorem 2. $(N \in \widehat{H}) \Leftrightarrow$ *($\Delta(N)$ is right-closed).*

Proof. See Appendix. □

Coming back to the Petri Net N_1 in Figure 3.1, the set $\mathbf{P}$ for N_1 consists of five vectors of $\mathcal{N}^5$, viz., $\{(1\ 0\ 0\ 0\ 0)^T, (0\ 2\ 0\ 0\ 0)^T, (0\ 0\ 1\ 0\ 0)^T, (0\ 0\ 0\ 1\ 0)^T, (0\ 0\ 0\ 0\ 1)^T\}$. For any marking $\mathbf{m} \in \Delta(N_1)$ (i.e. $\mathbf{m}(p_1) + \mathbf{m}(p_2) + \mathbf{m}(p_3) + \mathbf{m}(p_4) + \mathbf{m}(p_5) \geq 1$), it is easy to verify that $\mathbf{m}^* \in \mathbf{m} + \mathbf{P}$ satisfies $\mathbf{m}^*(p_1) + \mathbf{m}^*(p_2) + \mathbf{m}^*(p_3) + \mathbf{m}^*(p_4) + \mathbf{m}^*(p_5) \geq 1$. Thus, $N_1 \in \widehat{\mathcal{H}}$.

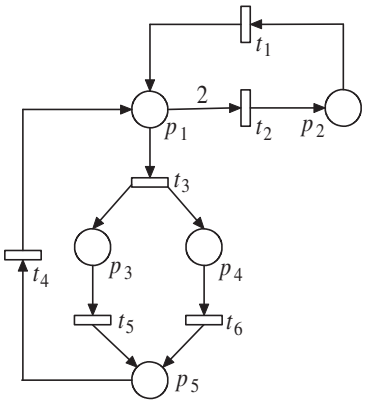


Figure 3.1: A PN structure $N_1 \notin \mathcal{H}$.

In subsequent sections, we prove that the necessary and sufficient condition of Theorem 2 cannot be tested for an arbitrary PN structure. To establish this, we need the results presented in the next section where we consider the decidability of "*Is* $\Delta(N) = \emptyset$*?*" and "*Is* $\Delta(N) \neq \emptyset$*?*" for arbitrary PN structures.

3.3 "*Is* $\Delta(N) = \emptyset$*?*" and "*Is* $\Delta(N) \neq \emptyset$*?*" are not Semi-Decidable

From an arbitrary PN structure $N = (\Pi, T, \Phi, \Gamma)$, we construct $\widetilde{N} = (\widetilde{\Pi}, \widetilde{T}, \widetilde{\Phi}, \widetilde{\Gamma})$ as follows:

1. Create $m+1$ places such that $\widetilde{\Pi} = \Pi \cup \{\pi_i\}_{i=1}^{m+1}$;
2. Create $n+2$ transitions such that $\widetilde{T} \leftarrow T \cup \{t_{m+i}\}_{i=1}^{n+2}$, where with the exception of t_{m+1}, all other newly added transitions are uncontrollable;
3. Create $m+1$ uncontrollable transitions: $\widetilde{T} \leftarrow \widetilde{T} \cup \{\tau_i\}_{i=1}^{m+1}$;
4. The arcs are:

$$\begin{aligned}\widetilde{\Phi} \leftarrow & \Phi \cup \{(t_{m+1}, p_i)\}_{i=1}^{n} \cup \{(t_i, \pi_i), (\pi_i, \tau_i), (\pi_i, \tau_{m+1})\}_{i=1}^{m} \\ & \cup \{(p_i, t_{m+2+i}), (\pi_{m+1}, t_{m+2+i}), (t_{m+2+i}, \pi_{m+1})\}_{i=1}^{n} \\ & \cup \{(t_{m+2}, \pi_{m+1}), (\pi_{m+1}, t_{m+2}), (\pi_{m+1}, t_{m+1})\} \\ & \cup \{(\tau_{m+1}, \pi_{m+1})\};\end{aligned}$$

5. The arc weights are: $\{\widetilde{\Gamma}((t_{m+1}, p_i) = m_i^0)\}_{i=1}^{n}$, $\widetilde{\Gamma}(\pi_{m+1}, t_{m+2}) = 2$. All other weights for the newly added arcs are unitary.

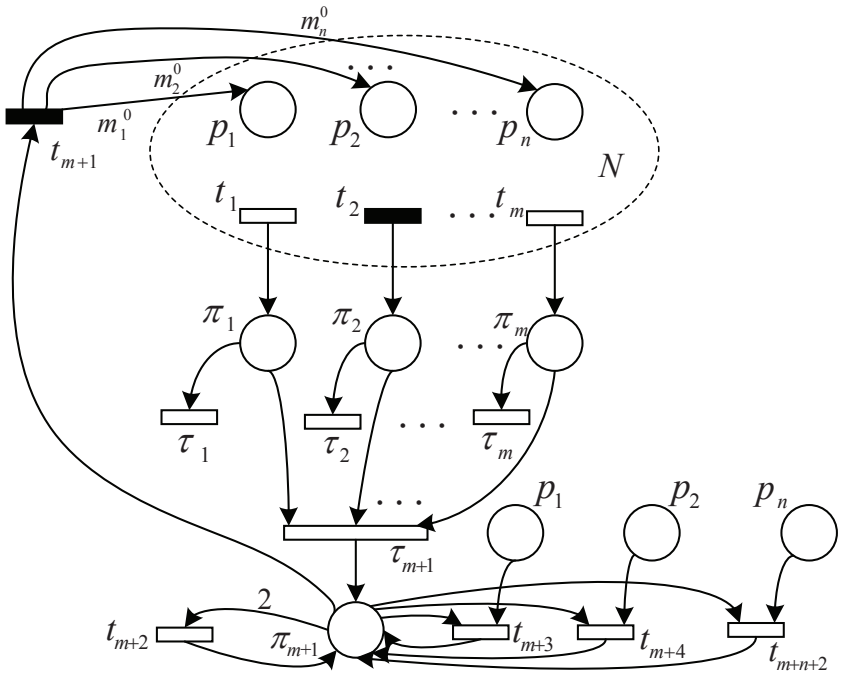


Figure 3.2: The PN structure $\widetilde{N} = (\widetilde{\Pi}, \widetilde{T}, \widetilde{\Phi}, \widetilde{\Gamma})$ used for deciding "*Is* $\Delta(N) = \emptyset$*?*".

The PN structure $\widetilde{N} = (\widetilde{\Pi}, \widetilde{T}, \widetilde{\Phi}, \widetilde{\Gamma})$ that results from this construction is shown in Fig. 3.2. N is an arbitrary PN and its structure is not drawn in the figure. The places $\{p_i\}_{i=1}^n$ and transitions $\{t_i\}_{i=1}^m$ denote the places and transitions of N.

Recall from Section 2 that a transition t_k is *live* under the supervision of $\mathcal{P}$ if $\forall \mathbf{m}^i \in \mathfrak{R}(N, \mathbf{m}^0, \mathcal{P}), \exists \mathbf{m}^j \in \mathfrak{R}(N, \mathbf{m}^i, \mathcal{P})$ such that $t_k \in T_e(N, \mathbf{m}^j)$ and $\mathcal{P}(\mathbf{m}^j, t_k) = 1$. A policy $\mathcal{P}$ is a *liveness enforcing supervisory policy* (LESP) for $N(\mathbf{m}^0)$ if all transitions in $N(\mathbf{m}^0)$ are live under $\mathcal{P}$.

Let $\widetilde{\mathbf{m}}^0$ be an initial marking of $\widetilde{N}$. Transition τ_{m+1} is live *if and only if* (iff) a marking that places at least a token in each of the places π_i, for all $i \in \{1, 2, \ldots, m\}$, is reachable from any marking that is reachable from $\widetilde{\mathbf{m}}^0$. Firing of the uncontrollable transition τ_i can empty the tokens in π_i, for all $i \in \{1, 2, \ldots, m\}$. Therefore, τ_{m+1} is live iff the token load of places π_i for all $i \in \{1, 2, \ldots, m\}$ can be replenished as often as necessary. Since transition t_i is the input transition of the place π_i for all $i \in \{1, 2, \ldots, m\}$, τ_{m+1} is live iff PN N can be made live. More formally, if $\mathbf{m}^0$ is an initial marking of N, then τ_{m+1} is live iff there exists a supervisory policy $\mathcal{P}$ such that $\forall t_i \in T, \forall \mathbf{m}^k \in \mathfrak{R}(N, \mathbf{m}^0, \mathcal{P}), \exists \mathbf{m}^j \in \mathfrak{R}(N, \mathbf{m}^k, \mathcal{P})$ such that $t_i \in T_e(N, \mathbf{m}^j)$ and $\mathcal{P}(\mathbf{m}^j, t) = 1$. This observation can also be restated as: a marking that places one (or arbitrarily large number of tokens) token in π_{m+1} is reachable from any marking that is reachable from the initial marking iff $N(\mathbf{m}^0)$ can be made live by supervision.

Consider the place π_{m+1} and assume for the sake of discussion that t_{m+1} is control-disabled. If π_{m+1} has more than one token, the uncontrollable transition t_{m+2} can fire repeatedly till there is just one token in π_{m+1}. That is, if a policy disables t_{m+1}, then a marking at which π_{m+1} has 1 token is always reachable from a marking at which π_{m+1} has $k > 0$ tokens.

Besides, if π_{m+1} has a non-zero token load, then the places $\{p_1, p_2, \ldots, p_n\}$ in PN N can be emptied through an appropriate number of firings of members of the uncontrollable transition set $\{t_{m+3}, t_{m+4}, \ldots, t_{m+n+2}\}$. In other words, if a policy disables t_{m+1} at marking $\mathbf{m}$ of $\widetilde{N}$ for which $\mathbf{m}(\pi_{m+1}) \neq 0$ and $\mathbf{m}(p_i) \neq 0$ for some $i \in \{1, \ldots, n\}$, then a marking at which the places $\{p_1, p_2, \ldots, p_n\}$ are all empty is reachable from $\mathbf{m}$.

We use $\overline{\mathbf{m}} \in \mathcal{N}^{card(\widetilde{\Pi})}$ to represent this marking of $\widetilde{N}$ at which π_{m+1} has one token while all other places have zero tokens in them. We use the ideas from the preceding two paragraphs to synthesize a policy which does not control-enable transition t_{m+1} until the PN reaches the marking $\overline{\mathbf{m}}$. At $\overline{\mathbf{m}}$, the firing of the transition t_{m+1} places m_i^0-many tokens in place p_i, where $i \in \{1, 2, \ldots, n\}$. This is akin to initializing the PN structure N with a marking $\mathbf{m}^0$, while the rest of the places of $\widetilde{N}$ are all empty. Here we have used $\mathbf{m}^0$ to denote the marking for which $\mathbf{m}^0(p_i) = m_i^0$. Following the discussion above, a token (or arbitrarily large number of tokens) is guaranteed to be added to place π_{m+1} if and only if $\mathbf{m}^0 \in \Delta(N)$. Once there is a token in π_{m+1}, transition t_{m+1} cannot be control-enabled until the PN reaches the marking $\overline{\mathbf{m}}$, and the sequence can be repeated, making $\widetilde{N}$ live. This is the main idea of the proofs given in Appendix.

Observation 1. $(\Delta(\widetilde{N}) \neq \emptyset) \Leftrightarrow (\overline{\mathbf{m}} \in \Delta(\widetilde{N}))$

Proof. See Appendix □

Observation 2. $(\overline{\mathbf{m}} \in \Delta(\widetilde{N})) \Leftrightarrow (\mathbf{m}^0 \in \Delta(N))$

Proof. See Appendix □

Theorem 3. *1. "Is $\Delta(N) \neq \emptyset$?" is not semi-decidable.*

2. "Is $\Delta(N) = \emptyset$?" is not semi-decidable.

Proof. By Observations 1 and 2, we have $(\Delta(\widetilde{N}) \neq \emptyset) \Leftrightarrow (\mathbf{m}^0 \in \Delta(N))$. This result follows directly from the fact that neither "*Is* $\mathbf{m}^0 \in \Delta(N)$*?*" nor "*Is* $\mathbf{m}^0 \notin \Delta(N)$*?*" is semi-decidable [35]. □

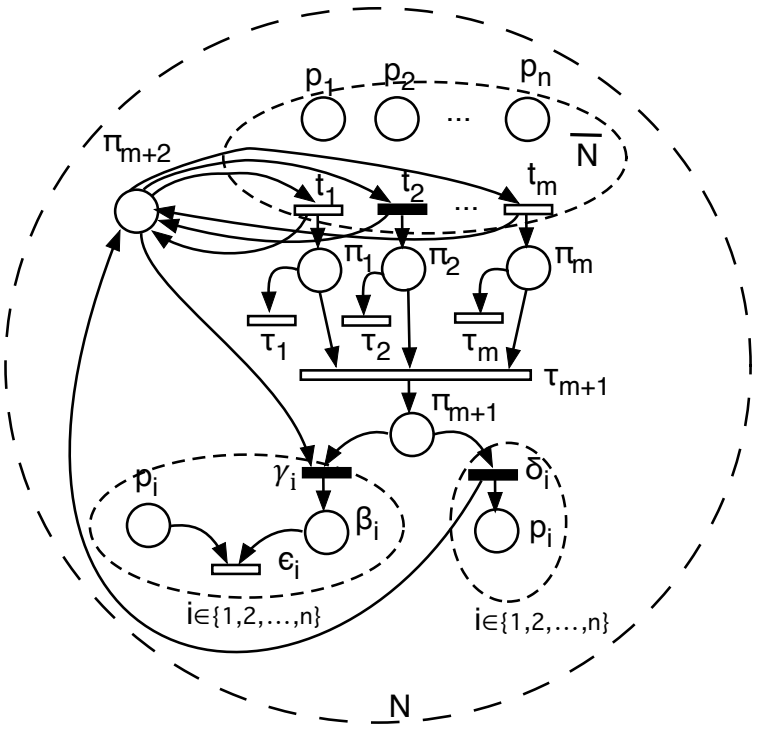


Figure 3.3: The PN structure $N = (\Pi, T, \Phi, \Gamma)$ used for deciding "*Is* $\Delta(N)$ *right-closed?*".

3.4 "*Is* $\Delta(N)$ *right-closed?*" is not decidable

In this section, we use the fact that $\Delta(N) = \emptyset$ is right-closed to prove that "*Is* $\Delta(N)$ *right-closed?*" is not decidable. We construct a partially controlled PN $N = (\Pi, T, \Phi, \Gamma)$ from an arbitrary partially controlled PN $\overline{N} = (\Pi_1, T_1, \Phi_1, \Gamma_1)$ as follows:

1. Create $m + n + 2$ places such that $\Pi = \Pi_1 \cup \{\pi_i\}_{i=1}^{m+2} \cup \{\beta_i\}_{i=1}^{n}$.

2. Create $3n+m+1$ transitions: $T = T_1 \cup \{\tau_i\}_{i=1}^{m+1} \cup \{\gamma_i\}_{i=1}^{n} \cup \{\epsilon_i\}_{i=1}^{n} \cup \{\delta_i\}_{i=1}^{n}$; where $\{\gamma_i\}_{i=1}^{n}$ and $\{\delta_i\}_{i=1}^{n}$ are controllable transitions, and $\{\tau_i\}_{i=1}^{m+1}$ and $\{\epsilon_i\}_{i=1}^{n}$ are uncontrollable transitions.

3. The arcs are:

$$\begin{aligned}\Phi_1 =& \Phi \cup \{(t_i, \pi_i), (\pi_i, \tau_i), (\pi_i, \tau_{m+1}), (\pi_{m+2}, t_i), (t_i, \pi_{m+2})\}_{i=1}^{m} \\ & \cup \{(\pi_{m+2}, \gamma_i), (\gamma_i, \beta_i), (\beta_i, \epsilon_i), (p_i, \epsilon_i), (\delta_i, p_i)\}_{i=1}^{n} \\ & \cup \{(\pi_{m+1}, \gamma_i), (\pi_{m+1}, \delta_i), (\delta_i, \pi_{m+2})\}_{i=1}^{n}.\end{aligned}$$

4. Weights for the newly added arcs are unitary.

The construction can be divided into five parts:

1. An arbitrary net $\overline{N}$, which is the core of the construction. Places $\{p_i\}_{i=1}^n$ and transitions $\{t_i\}_{i=1}^m$ belong to PN $\overline{N}$ whose structure is not drawn in the construction.

2. The *enable place* π_{m+2} which is required to have a non-zero token load if any transition in $\overline{N}$ is to be state-enabled.

3. Places $\{\pi_i\}_{i=1}^m$ and transitions $\{\tau_i\}_{i=1}^m$ capture the liveness property of subnet $\overline{N}$ as described in the introductory discussion in Section 3.3.

4. Places $\{\beta_i\}_{i=1}^n$ and transitions $\{\gamma_i, \epsilon_i\}_{i=1}^n$: Each time a (controllable) γ_i-transition is permitted to fire, it decreases (resp. increments) the token load of its input-place set (resp. output-place set) $\{\pi_{m+1}, \pi_{m+2}\}$ (resp. $\{\beta_i\}$). The subsequent firing of the (uncontrollable) ϵ_i-transition decrements the number of tokens in place p_i from $\overline{N}$ by unity.

5. Transitions $\{\delta_i\}_{i=1}^n$: The firing of a (controllable) δ_i-transition increments the token load of place p_i. It also replenishes the tokens in π_{m+2}. In essence, the firing of a δ_i-transition cancels the effect of permitting a γ_i-transition (cf. Item 4) on place π_{m+2}, and the effect of firing of ϵ_i-transition on place p_i. Since the transitions $\{\gamma_i, \delta_i\}_{i=1}^n$ are controllable, the supervisory policy can select which one of them is to be control-enabled at any marking.

The observation that is key to the decidability result in this section is that there is a marking in $\Delta(N)$ if and only if there is a marking in $\Delta(\overline{N})$. The main idea is as follows. Assume there exists a marking $\mathbf{m}^1 \in \Delta(\overline{N})$. Let us use $\overline{\mathbf{m}}^1$ to denote the marking of N that initializes $\overline{N}$ under $\mathbf{m}^1$, with a single token in π_{m+2}, and zero tokens elsewhere. We argue that $(\mathbf{m}^1 \in \Delta(\overline{N})) \Rightarrow (\overline{\mathbf{m}}^1 \in \Delta(N))$. Now, starting at $\overline{\mathbf{m}}^1$ the transitions in T_1 can be made live under supervision as $\mathbf{m}^1 \in \Delta(\overline{N})$. This ensures that the markings for which the place π_{m+1} has arbitrarily large number of tokens are reachable from any marking that is reachable from $\overline{\mathbf{m}}^1$. For illustration, let us use $\overline{\mathbf{m}}^j$ to denote one such marking.

1. At $\overline{\mathbf{m}}^j$, place π_{m+1} has two tokens, π_{m+2} has one token, $\overline{\mathbf{m}}^j(\Pi_1) \in \Delta(\overline{N})$ and all other places have zero tokens. As discussed earlier, $\overline{\mathbf{m}}^j$ is reachable from $\overline{\mathbf{m}}^1$. At $\overline{\mathbf{m}}^j$, pick any p_i that has a non-zero token load. The corresponding controllable transition γ_i is state- and control-enabled at this marking. In fact, since $\mathbf{m}^1 \in \Delta(\overline{N})$, markings for which γ_i is state- and control-enabled are reachable from $\overline{\mathbf{m}}^j$ for every $i \in \{1, \ldots n\}$.

2. We have $\gamma_i^\bullet = \beta_i$ and ${}^\bullet\epsilon_i = \{p_i, \beta_i\}$. The firing of γ_i will remove a token each from π_{m+1} and π_{m+2} and add one token to place β_i. Since π_{m+2} had only one token, none of

the transitions in T_1 can fire and the marking of $\overline{N}$ cannot change. Thus, a marking that state-enables the uncontrollable transition ϵ_i is reachable from $\overline{\mathbf{m}}^j$. In fact, since $\gamma_i^\bullet = \beta_i$ and ${}^\bullet\epsilon_i = \{p_i, \beta_i\}$, following the discussion in Item 1 above, markings for which ϵ_i is state-enabled are also reachable from $\overline{\mathbf{m}}^j$ for every $i \in \{1, \ldots n\}$. The firing of ϵ_i will decrease the token-load of p_i and β_i by one.

3. Following this, the corresponding transition δ_i is control-enabled. The firing of δ_i replenishes the token-load of p_i and π_{m+2} by one, effectively cancelling the effect of the firing of γ_i and ϵ_i on them, as discussed above.

4. Since $\mathbf{m}^1 \in \Delta(\overline{N})$, the tokens in place π_{m+1} can be replenished as often as necessary and the whole process can be repeated for each γ_i, ϵ_i and δ_i, for all $i \in \{1, 2, \ldots, n\}$. Thus, markings that state- and control-enable each of the transitions in N are reachable from every marking that is reachable from the initial marking ($\overline{\mathbf{m}}^1$). All transitions in $N(\overline{\mathbf{m}}^1)$ are live under supervision, and $\Delta(N) \neq \emptyset$.

Observation 3. $(\Delta(\overline{N}) \neq \emptyset) \Leftrightarrow (\Delta(N) \neq \emptyset)$

Proof. See Appendix. □

Observation 4. $(\Delta(N) \neq \emptyset) \Leftrightarrow$ *($\Delta(N)$ is not right-closed)*

Proof. See Appendix. □

Theorem 4. *"Is $\Delta(N)$ right-closed?" is not decidable.*

Proof. By Observation 4, we have that $(\Delta(N) \neq \emptyset) \Leftrightarrow (\Delta(N)$ is not right-closed). This result follows directly from the fact that neither "*Is* $\Delta(N) = \emptyset$?" nor "*Is* $\Delta(N) \neq \emptyset$?" is semi-decidable (by Theorem 3). □

In this section, we proved that "*Is $\Delta(N)$ is right-closed*?" is not decidable. In the next section we consider the decidability of "*Is there a (non-empty) right-closed subset of $\Delta(N)$?*".

3.5 "*Is there a right-closed subset of $\Delta(N)$?*" and "*Is there no right-closed subset of $\Delta(N)$?*" are not semi-decidable

In this section we look at procedures for finding right-closed subsets of $\Delta(N)$ for an arbitrary PN N. Every $\Delta(N)$, trivially, has the empty set as its right-closed subset. Therefore, we consider only the non-empty subsets of $\Delta(N)$. We use the construction in Fig. 3.2. Recall

from Section 3.3 that at the marking $\overline{\mathbf{m}}$, π_{m+1} has one token while all other places have zero tokens in them. In Observation 2, we noted that the supervisory policy that enforces liveness in $\widetilde{N}$ enables t_{m+1} only after $\widetilde{N}$ has reached the marking $\overline{\mathbf{m}}$. The marking $\overline{\mathbf{m}}$ is reachable from any marking larger than $\overline{\mathbf{m}}$ through the firing of uncontrollable transitions t_{m+2} to t_{m+n+2}. This observation forms the basis of the next result.

Observation 5. *Let* $\underline{\mathbf{m}} \geq \overline{\mathbf{m}}$*, then* $(\Delta(\widetilde{N}) \neq \emptyset) \Leftrightarrow (\underline{\mathbf{m}} \in \Delta(\widetilde{N}))$.

Proof. See Appendix. □

Observation 6. $(\Delta(\widetilde{N}) \neq \emptyset) \Leftrightarrow (\exists \mathcal{M} \subseteq \Delta(\widetilde{N})$*, such that* $\mathcal{M}$ *is right-closed, and* $\min(\mathcal{M}) = \{\overline{\mathbf{m}}\})$.

This observation follows directly from Observation 5. The next result follows from Observation 6 and Theorem 3.

Theorem 5. *For an arbitrary PN* N*,*

1. *"Is there a right-closed subset of* $\Delta(N)$*?" is not semi-decidable.*
2. *"Is there no right-closed subset of* $\Delta(N)$*?" is not semi-decidable.*

Till now, we showed that restricting the properties of $\Delta(N)$ does not result in decidable instances of the problem of existence of an LESP for $N(\mathbf{m}^0)$. In the next section, we focus on a restricted class of LESPs, i.e. *marking-monotone LESP* (MM-LESP), whose existence for arbitrary PNs is proved to be decidable.

3.6 Marking-Monotone LESP for Arbitrary PNs

An LESP $\mathcal{P}$ for $N(\mathbf{m}^0)$ is an MM-LESP if (1) $\forall \widehat{\mathbf{m}} \geq \mathbf{m}, \forall t \in T, \mathcal{P}(\widehat{\mathbf{m}}, t) \geq \mathcal{P}(\mathbf{m}, t)$, and (2) $\mathcal{P}$ is also an LESP for $N(\widehat{\mathbf{m}}^0)$ for any $\widehat{\mathbf{m}}^0 \geq \mathbf{m}^0$. For a PN structure N, the set $\Delta_M(N) := \{\mathbf{m}^0 \in \mathcal{N}^n : \exists$ an MM-LESP for $N(\mathbf{m}^0)\}$ is a right-closed subset of $\Delta(N)$. As an example, for the PN structure N_1 shown in Fig. 3.1, $\Delta(N_1) = \{\mathbf{m} \in \mathcal{N}^5 : (\mathbf{m}(p_1) + \mathbf{m}(p_2) + \mathbf{m}(p_3) + \mathbf{m}(p_4) + \mathbf{m}(p_5) \geq 1)\}$, and $\Delta_M(N_1) = \Delta(N_1)$. The trivial policy of enabling all transitions is an MM-LESP for $N(\mathbf{m}^0)$ for any $\mathbf{m}^0 \in \Delta(N)$. There are some known classes of PNs for which $\Delta_M(N) = \Delta(N)$, and the existence of the minimally restrictive LESP, which is also an MM-policy, for $N(\mathbf{m}^0)$ is decidable [35, 36, 37, 38].

We are interested in determining whether there is an MM-LESP for an arbitrary PN $N(\mathbf{m}^0)$ (i.e. "*Is* $\mathbf{m}^0 \in \Delta_M(N)$*?*" and "*Is* $\mathbf{m}^0 \notin \Delta_M(N)$*?*"). We present a (decidable)

necessary and sufficient condition for the existence of an MM-LESP for $N(\mathbf{m}^0)$. This result involves the *coverability graph* $G(N(\mathbf{m}^0), \mathcal{P}) = G(V, A, \Psi)$, which is essentially the *Karp-Miller tree*, where the duplicate nodes are merged as one (cf. Fig. 1, [35]). More formally, the *coverability graph* of a PN $N(\mathbf{m}^0)$ under the supervision of a marking monotone policy $\mathcal{P}$ is a directed graph $G(N(\mathbf{m}^0), \mathcal{P}) = (V, A, \Psi)$, where V is the set of *vertices*, A is the set of *directed edges*, and $\Psi : A \to V \times V$ is the *incidence function*. For each $a \in A$, if $\Psi(a) = (v_i, v_j)$, then the directed edge a is said to *originate* (*terminate*) at v_i (v_j) (cf. Fig. 1 and 2, [35]). Since each vertex in the coverability graph has at most one outgoing edge labeled by each transition in T, directed paths in the coverability graph can be unambiguously identified by strings in T^*. If there is a path from $v_i \in V$ to $v_j \in V$ with label $\sigma^* \in T^*$ in $G(N(\mathbf{m}^0), \mathcal{P})$, we denote it as $v_i \xrightarrow{\sigma^*} v_j$. Following Reference [35], we say $G(N(\mathbf{m}^0), \mathcal{P})$ satisfies the *path-requirement* if $\exists v_1, v_2 \in V, \exists \sigma_1, \sigma_2 \in T^*$, such that (1) $v_1 \xrightarrow{\sigma_1} v_2 \xrightarrow{\sigma_2} v_2$, (2) $\mathbf{x}(\sigma_2) \geq \mathbf{1}$, that is, all transitions in T appear at least once in σ_2, and (3) $\mathbf{C}\mathbf{x}(\sigma_2) \geq \mathbf{0}$, where $\mathbf{x}(\bullet) \in \mathcal{N}^m$ is an m-dimensional vector, which represents the number of occurrences of each $t \in T$ in the string argument.

Theorem 6. *There is an MM-LESP for $N(\mathbf{m}^0)$ if and only if $\exists \widehat{\Delta}(N) \subseteq \Delta(N)$, such that*

1. $\mathbf{m}^0 \in \widehat{\Delta}(N)$,
2. $\widehat{\Delta}(N)$ *is control invariant with respect to* N,
3. $\widehat{\Delta}(N)$ *is right-closed, and*
4. $\forall \mathbf{m}^i \in \min(\widehat{\Delta}(N))$, $G(N(\mathbf{m}^i), \mathcal{P})$ *satisfies the path requirement. That is,* $\forall \mathbf{m}^i \in \min(\widehat{\Delta}(N))$, *there is a path* $v_0 \xrightarrow{\sigma_1} v_1 \xrightarrow{\sigma_2} v_1$, *in the coverability graph* $G(N(\mathbf{m}^i), \mathcal{P}) = (V, A)$, *such that* $\mathbf{x}(\sigma_2) \geq \mathbf{1}$ *and* $\mathbf{C}\mathbf{x}(\sigma_2) \geq \mathbf{0}$, *where* $\mathbf{1}$ *is the* m*-dimensional vector of all ones,* $\mathcal{P}$ *ensures the reachable markings never leaves* $\widehat{\Delta}(N)$.

Proof. See Appendix. □

Algorithm 3, which strongly parallels the procedure in Fig. 8 of reference [35], is a procedure for determining the largest set $\widehat{\Delta}(N)$ that satisfies the properties listed in Theorem 6. Let $\Delta_f(N) \supseteq \Delta(N)$ denote the set of all initial markings for which an LESP exists for N when all transitions are assumed to be controllable. Reference [33] proved that $\Delta_f(N)$ is right-closed and is computable. $\Delta_f(N)$ is the initial estimate of $\Delta(N)$. Algorithm 3 finds, if it exists, by brute force, the largest right-closed control invariant subset of $\Delta_f(N)$, whose minimal elements satisfy the path-requirement. The current estimate of $\Delta(N)$ at any point in the algorithm is denoted by $\widehat{\Upsilon}$. If any of the two properties— control invariance or the

path requirement on the coverability graph, is violated then the minimal element that violated the condition is replaced by the smallest set of elements larger than that element, and $\widehat{\Upsilon}$ is appropriately modified. This process is repeated till we find $\Delta_M(N)$ or till $\mathbf{m}^0$ drops out of $\widehat{\Upsilon}$. Algorithms 1 and 2 respectively present procedures for "bumping-up" the minimal elements when the control invariance and path requirement are violated. They take the PN structure N and the current estimate $\widehat{\Upsilon}$ as inputs and respectively output the largest subset of $\widehat{\Upsilon}$ that satisfies the control invariance and path requirement. In Algorithm 3, the PN structure N is the input and the subset $\widehat{\Delta}(N)$ for $N(\mathbf{m}^0)$ is the output.

Algorithm 1 BumpUpForControlInvariance($N, \widehat{\Upsilon}$)

1: **while** $\exists t_u \in T_u$, $\exists \widetilde{\mathbf{m}}^i \in \min(\widehat{\Upsilon})$ such that $(\max\{\mathbf{IN}_{t_u}, \widetilde{\mathbf{m}}^i\} + \mathbf{C} \times \mathbf{1}_{t_u}) \notin \widehat{\Upsilon}$ **do**
2: Replace $\widetilde{\mathbf{m}}^i$ by a set of $k-1$ vectors $\{\widehat{\mathbf{m}}^l\}_{l=1}^{k-1}$ where for each $j \in \{1, 2, \ldots, k\} - \{i\}$, create a new marking $\widehat{\mathbf{m}}^l$, given by the expression $\widehat{\mathbf{m}}^l = \widetilde{\mathbf{m}}^i + max\{\mathbf{0}, \widetilde{\mathbf{m}}^j - (max\{\mathbf{IN} \times \mathbf{1}_{t_u}, \widetilde{\mathbf{m}}^i\} + \mathbf{C} \times \mathbf{1}_{t_u})\}$.
3: Replace the resulting set of $\{\widetilde{\mathbf{m}}^i\}_i$ vectors by their minimal elements, and modify the value of k to equal the size of the minimal set of vectors. $\widehat{\Upsilon}$ is the right-closed set identified by this minimal set of vectors.
4: **end while**

Algorithm 2 BumpUpForPathRequirement($N, \widehat{\Upsilon}$)

1: **for** $\widetilde{\mathbf{m}}^i \in \min(\widehat{\Upsilon})$ where $G(N(\widetilde{\mathbf{m}}^i), \widetilde{\mathcal{P}}_{\widehat{\Upsilon}})$ does not have the path **do**
2: Define a right-closed set $\overline{\Upsilon}$, where $\min(\overline{\Upsilon}) = (\min(\widehat{\Upsilon}) - \{\widetilde{\mathbf{m}}^i\}) \cup \{\widetilde{\mathbf{m}}^i + \omega \times \mathbf{1}_j | j \in \{1, 2, \ldots, n\}\}$, where $\mathbf{1}_j$ the unit-vector where the j-th component is unity.
3: Replace $\widetilde{\mathbf{m}}^i$ by the set:

$$\{\widetilde{\mathbf{m}}^i + \mathbf{1}_j | j \in \{1, 2, \ldots, n\}, G(N(\widetilde{\mathbf{m}}^i + \omega \times \mathbf{1}_j), \widetilde{\mathcal{P}}_{\overline{\Upsilon}}) \text{ satisfies the path requirement}\} \tag{3.3}$$

4: **end for**
5: Replace the resulting set of $\{\widetilde{\mathbf{m}}^i\}_i$ vectors by their minimal elements, and modify the value of k to equal the size of the minimal set of vectors. $\widehat{\Upsilon}$ is the right-closed set identified by this minimal set of vectors.

Algorithm 2 aims to compute the supremal controllable subset of the right closed set $\widehat{\Upsilon}$ with respect to the PN structure N. This supremal controllable subset is also right closed. Consequently, when there is an element $\widetilde{\mathbf{m}}^i$ that violates the control invariance requirement, it is elevated by an appropriate minimal amount, as stated in Step 2. During this elevation process, it might happen that we get some minimal elements that are ordered (that is, $\widetilde{\mathbf{m}}^i \geq \widetilde{\mathbf{m}}^j$ for some i, j). Step 3 trims the set of minimal elements of the current version of

$\widehat{\Upsilon}$ to ensure that only the smallest elements are retained. This process proceeds until (the current version of) $\widehat{\Upsilon}$ is control invariant.

Proceeding under the stipulation that (the current version of) $\widehat{\Upsilon}$ is control invariant with respect to N, for any $\mathbf{m}^0 \in \widehat{\Upsilon}$, there is a supervisory policy, $\widetilde{P}_{\widehat{\Upsilon}}$, that ensures $\mathfrak{R}(N, \mathbf{m}^0, \widetilde{P}_{\widehat{\Upsilon}}) \subseteq \widehat{\Upsilon}$. If $\forall \widetilde{\mathbf{m}}^i \in min(\widehat{\Upsilon})$, the required path condition in $G(N(\widetilde{\mathbf{m}}^i), \widetilde{P}_{\widehat{\Upsilon}})$ is satisfied, then $\widetilde{P}_{\widehat{\Upsilon}}$ is an LESP for $N(\mathbf{m}^0)$ for any $\mathbf{m}^0 \in \widehat{\Upsilon}$ (cf. [35]).

In Algorithm 3, when there exists an element $\widetilde{\mathbf{m}}^i \in \mathcal{N}^n$ where $G(N(\widetilde{\mathbf{m}}^i), \widetilde{P}_{\widehat{\Upsilon}})$ does not have the required path, it should be elevated by an appropriate set of unit-vectors. Step 2 identifies those among the n-many unit-vectors that are to be used to elevate the minimal element $\widetilde{\mathbf{m}}^i$. Specifically, if the placement of an unbounded number of tokens (i.e. ω-many tokens) in just the j-th place does *not* result in a coverability graph with the required path, then the j-th unit vector is *not* used to elevate the minimal element $\widetilde{\mathbf{m}}^i$. Otherwise, the corresponding vector $\widetilde{\mathbf{m}}^i + \mathbf{1}_j$ is retained in the current set $\overline{\Upsilon}$, as shown in Step 3. This process proceeds until all elements satisfy the path requirement.

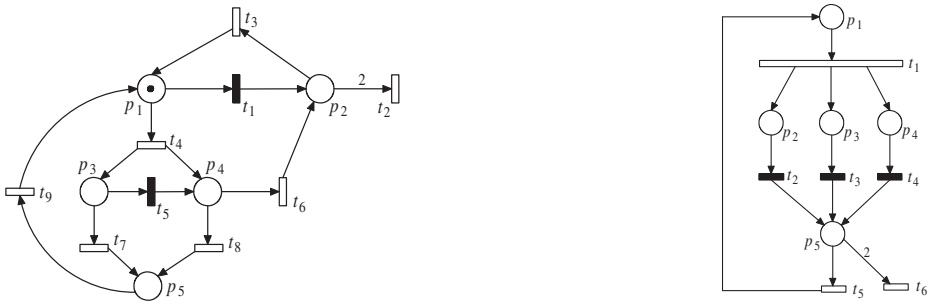
Algorithm 3 Test for existence of the subset $\widehat{\Delta}(N)$ for $N(\mathbf{m}^0)$

1: $\widehat{\Upsilon} = \Delta_f(N)$, and let $\{\widetilde{\mathbf{m}}^i\}_{i=1}^k = \min(\widehat{\Upsilon})$.
2: **while** $((\exists t_u \in T_u, \exists \widetilde{\mathbf{m}}^i \in \min(\widehat{\Upsilon})$, such that $\max\{\widetilde{\mathbf{m}}^i, \mathbf{IN}_u\} + \mathbf{C} \cdot \mathbf{1}_u \notin \widehat{\Upsilon}) \vee (\exists \widetilde{\mathbf{m}}^i \in \min(\widehat{\Upsilon})$ such that $G(N(\widetilde{\mathbf{m}}^i), \widetilde{\mathcal{P}}_{\widehat{\Upsilon}})$ does not have the path requirement)) $\wedge$ $(\mathbf{m}^0 \in \widehat{\Upsilon})$ **do**
3: BumpForControlInvariance$(N, \widehat{\Upsilon})$
4: BumpForPathCondition$(N, \widehat{\Upsilon})$
5: **end while**
6: **if** $\mathbf{m}^0 \notin \widehat{\Upsilon}$ **then**
7: **return**("no solution");
8: **else**
9: **return** $\widehat{\Upsilon}$
10: **end if**

Theorem 7. *The existence of an MM-LESP for an arbitrary PN $N(\mathbf{m}^0)$ is decidable.*

Proof. The existence (non-existence) of an MM-LESP for $N(\mathbf{m}^0)$ is subject to the existence (resp. non-existence) of a proper subset $\widehat{\Delta}(N)$ which is right-closed, control invariant, satisfies the path-requirement and contains $\mathbf{m}^0$. In Algorithm 3, we seek a sequence of proper subsets $\widehat{\Upsilon}$ (where $\widehat{\Delta}(N) \subseteq \widehat{\Upsilon} \subseteq \Delta(N) \subseteq \Delta_f(N)$) using exhaustive search until we find such a $\widehat{\Delta}(N)$ or until $\mathbf{m}^0 \notin \widehat{\Upsilon}$.

If there is an MM-LESP in $N(\mathbf{m}^0)$, from Lemma 5.13 in [35] we know that there is a finite set of minimal elements $\{\widetilde{\mathbf{m}}^i\}_{i=1}^k$ that define a control invariant, right-closed set and satisfy the path-requirement. The k-many, n-dimensional, minimal elements $\{\widetilde{\mathbf{m}}^i\}_{i=1}^k$ are



(a) PN N_4 (b) PN N_5

Figure 3.4: Examples to illustrate features of marking-monotone LESP.

determined using brute force by Algorithm 3, in finite time. On the other hand, this process will terminate when $\mathbf{m}^0 \notin \widehat{\Upsilon}$, thus certifying the non-existence of a candidate $\Upsilon = \widehat{\Delta}(N)$ with $\mathbf{m}^0 \in \widehat{\Delta}(N)$, in finite time; thus proving the semi-decidability of the existence (non-existence) of a MM-policy that enforces liveness in an arbitrary partially controllable PN $N(\mathbf{m}^0)$. □

Figure 3.4a presents an example $N_4(\mathbf{m}^0)$ where $\Delta(N_4)$ is not right-closed, but there is an MM-LESP for $N(\mathbf{m}^0)$. Specifically, $\Delta(N_4) = \{\mathbf{m}^0 \in \mathcal{N}^5 \mid (\mathbf{m}^0(p_1) + \mathbf{m}^0(p_3) + \mathbf{m}^0(p_5) \geq 1) \vee ((\mathbf{m}^0(p_2) + \mathbf{m}^0(p_4))_{mod2} = 1)\}$. Here $\Delta_M(N_4) = \{\mathbf{m}^0 \in \mathcal{N}^5 \mid \mathbf{m}^0(p_1) + \mathbf{m}^0(p_3) + \mathbf{m}^0(p_5) \geq 1\}$. The MM-LESP, $\mathcal{P}$, will ensure at least one token in $\{p_1, p_3, p_5\}$. However, it is to be noted that $\mathcal{P}$ is not the minimally restrictive for $N_4(\mathbf{m}^0)$, since $\Delta_M(N_4) \subset \Delta(N_5)$.

On the other hand, the existence of a right-closed subset of $\Delta(N)$ does not guarantee the existence of a MM-LESP. Consider N_5 with initial marking $(0\ 1\ 0\ 0\ 1)^T$. Following the procedures explicated in Algorithm 3, we end up with the control invariant $\widehat{\Upsilon}$ represented by $\min(\widehat{\Upsilon}) = \{\widetilde{\mathbf{m}}^i\}_{i=1}^7 = \{(1\ 0\ 0\ 0\ 0)^T, (0\ 2\ 0\ 0\ 0)^T, (0\ 1\ 1\ 0\ 0)^T, (0\ 1\ 0\ 1\ 0)^T, (0\ 0\ 2\ 0\ 0)^T, (0\ 0\ 1\ 1\ 0)^T, (0\ 0\ 0\ 2\ 0)^T\}$. Since the initial marking $\mathbf{m}^0$ is not in $\widehat{\Upsilon}$, there is no MM LESP for $N_5(\mathbf{m}^0)$. However, there is an LESP for $N_5(\mathbf{m}^0)$. Note that $\Delta(N_5) = \{\mathbf{m}^0 \in \mathcal{N}^5 \mid \mathbf{m}^0(p_1) + \mathbf{m}^0(p_2) + \mathbf{m}^0(p_3) + \mathbf{m}^0(p_4) \geq 1 \text{ or } \mathbf{m}^0(p_5)_{mod2} = 1\}$. A supervisory policy that ensures that there is at least one token in $\{p_1, p_2, p_3, p_4\}$ or there are odd tokens in p_5 is an LESP. This example also shows that even if there is no marking-monotone LESP for arbitrary PN $N(\mathbf{m}^0)$, there may be an LESP for $N(\mathbf{m}^0)$.

3.7 Additional Remarks about Marking-Monotone Policies

Although well established methods exist for synthesizing policies that enforce certain properties (like liveness, safety, boundedness etc.), it is likely that there do not exist systematic

procedures for the synthesis of policies that enforce complex objectives (like the combination of several objectives). One of the ways of accomplishing this is by decomposing the complex objective into simpler objectives and then synthesizing policies for enforcing these simpler objectives (cf. Figure 3.5).

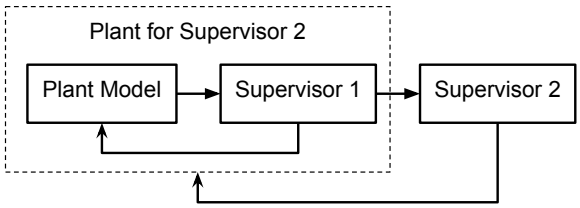


Figure 3.5: Sequential Synthesis of Supervisory Policies.

The issue with this approach is that while there was a model, within a modeling-paradigm, of the original infinite-state DES, there may not exist a model of the supervised system within the same modeling-paradigm. For instance, Example 3.1 of [57] presents a plant DES that is a *Petri Net* (PN), where the desired behavior $\mathcal{B}$ corresponds to the requirement to be *non-blocking*. Giua and DiCesare have shown that there is no PN that can model the resulting supervised-system. In the context of Figure 3.5, this result shows that while the plant for Supervisor 1 is a PN, the plant for Supervisor 2 cannot be a PN in any sequential attempt to the synthesis of supervisory policies. The identification of a necessary and sufficient condition for a DES modeling paradigm (different from *Finite State Automata*) where the supervised-DES can also be represented using the same modeling paradigm, plays a critical role in the sequential synthesis of supervisory policies for DES. Thus, there are two aspects to this problem– (i) the algebraic framework under which the supervisor construction is carried out; and, (ii) the model. We discuss each of these points in the remainder of the section.

Modular problem specification and supervisor construction for DES was first discussed by Ramadge and Wonham in [58, 7]. They modeled the behavior of DES as a prefix closed language L over the set of event alphabet Σ, where each $u \in L$ is a possible event sample path. The behaviour of the language L is modeled by a *generator* G which is an automaton (Σ, Q, δ, q_0). For multiple objective controller synthesis, if each objective is specified in terms of a controlled language K_i, then the overall desired behaviour is specified by the controlled language $\cap_i K_i$. There are two key points– controllability of the desired language and compatibility between multiple objectives. For prefix closed languages, if K_1 and K_2 are controllable, then $K_1 \cap K_2$ is also controllable (see Section IV in [7] for the definition of controllability). Compatibility between multiple objectives is formalized by the concept of

nonconflicting languages. Two controlled languages $K_1, K_2 \in \Sigma^*$, are said to *nonconflicting* if $pr(K_1 \cap K_2) = pr(K_1) \cap pr(K_2)$ where $pr(\bullet)$ denotes the prefix of the string argument. That is, whenever the two languages K_1 and K_2 share a prefix, they also share a word containing this prefix.

Modeling of a supervised Petri net by another Petri net was first discussed in [59], where the authors gave an algorithm for constructing the PN model of the supervised system. They proved that such a construction can always be carried out for conservative PNs (cf. Theorem 4.1 in [59]). Reference [57] proved by a counter-example that not all supervised Petri nets can be modeled by a PN. Using the work in the aforementioned papers as a starting point, in this section we first formally define the concept of *composition* of a PN model and a supervisory policy. We extend the algorithm in [59] to unbounded PNs, and prove that a composition of a PN model and a supervisory policy $\mathcal{P}$ that enforces a property $\mathcal{B}$ exists if and only if the supervisory policy is marking-monotone $\mathcal{B}$-enforcing supervisory policy (MM-$\mathcal{B}$ESP) over the reachable markings. By definition, if $\mathcal{P}$ is an MM-$\mathcal{B}$ESP for an initial marking, then it is an MM-$\mathcal{B}$ESP for all larger initial markings as well. Since the policy does not change for a larger initial marking, the composition of the PN and the policy also stays the same for a larger initial marking. This is an important property to have while designing a system as analysis for various initial markings become easy.

We use $\mathcal{B}$ESP as a shorthand to denote a property $\mathcal{B}$ enforcing supervisory policy. The set of initial markings for which property $\mathcal{B}$ can be enforced is defined as: $\mathfrak{D}(\mathcal{B}, N) = \{\mathbf{m}^0 \in \mathcal{N}^n : \exists \text{ a } \mathcal{B}\text{ESP for } N(\mathbf{m}^0)\}$. This can also be restated as: $(\exists \text{ a } \mathcal{B}\text{ESP for } N(\mathbf{m}^0)) \Leftrightarrow (\mathbf{m}^0 \in \mathfrak{D}(\mathcal{B}, N))$. Note that we have used different notations in this section because are only considering property $\mathcal{B}$ and *not* liveness with respect to it.

3.7.1 Main Results

Definition 6. *Let $\mathcal{P}$ be a $\mathcal{B}$ESP for $N_1(\mathbf{m}^0)$. $N_1(\mathbf{m}^0)$ and $\mathcal{P}$ are said to be $\mathcal{B}$-composable if there exists a Petri net N_2 such that $\mathfrak{R}(N_2, \mathbf{m}^0) = \mathfrak{R}(N_1, \mathbf{m}^0, \mathcal{P})$. We refer to $N_2(\mathbf{m}^0)$ as the $\mathcal{B}$-preserving composition of $N_1(\mathbf{m}^0)$ and $\mathcal{P}$.*

Theorem 8. *[60] There exists an MM-$\mathcal{B}$ESP for $N(\mathbf{m}^0)$ if and only if there exists a subset $\widehat{\mathfrak{D}}(\mathcal{B}, N) \subseteq \mathfrak{D}(\mathcal{B}, N)$ such that:*

1. $\mathbf{m}^0 \in \widehat{\mathfrak{D}}(\mathcal{B}, N)$.
2. $\widehat{\mathfrak{D}}(\mathcal{B}, N)$ *is right-closed.*
3. *A supervisory policy that enforces the set $\widehat{\mathfrak{D}}(\mathcal{B}, N)$ is a $\mathcal{B}$ESP.*

Proof. (If) Suppose $\widehat{\mathfrak{D}}(\mathcal{B},N)$ is right-closed and $\mathbf{m}^0 \in \widetilde{\mathfrak{D}}(\mathcal{B},N)$. Let $\{\widetilde{\mathbf{m}}^i\}_{i=1}^{l}$ denote the minimal elements of $\widehat{\mathfrak{D}}(\mathcal{B},N)$. Consider a supervisory policy that enforces the set $\widehat{\mathfrak{D}}(\mathcal{B},N)$, that is:

1. $\forall t_u \in T_u$, $(\mathbf{m}^0 \xrightarrow{t_u} \mathbf{m}^1) \Rightarrow (\mathbf{m}^1 \geq \widetilde{\mathbf{m}}^i$ for some $i \in \{1,\ldots,l\})$.
2. $\forall t_c \in T_c$, $(\mathcal{P}(\mathbf{m}^0,t_c)=1) \Leftrightarrow (\mathbf{m}^0 \xrightarrow{t_c} \mathbf{m}^1$, $\mathbf{m}^1 \geq \widetilde{\mathbf{m}}^i$ for some $i \in \{1,\ldots,l\})$

Let $\widehat{\mathbf{m}}^0 \geq \mathbf{m}^0$ and consider a transition t such that $\mathbf{m}^0 \xrightarrow{t} \mathbf{m}^1$ and $\widehat{\mathbf{m}}^0 \xrightarrow{t} \widehat{\mathbf{m}}^1$. Suppose $\mathcal{P}(\mathbf{m}^0,t)=1$. Then $(\mathbf{m}^1 \geq \widetilde{\mathbf{m}}^i) \Rightarrow (\widehat{\mathbf{m}}^1 \geq \widetilde{\mathbf{m}}^i)$. Therefore, a supervisory policy that enforces a right-closed set ($\widehat{\mathfrak{D}}(\mathcal{B},N)$ in this case) will permit the transition t to fire at $\widehat{\mathbf{m}}^0$ as well, and hence is marking-monotone. By Item 3, the supervisory policy that enforces $\widehat{\mathfrak{D}}(\mathcal{B},N)$ is a $\mathcal{B}$ESP. Therefore, a supervisory policy that enforces the set $\widehat{\mathfrak{D}}(\mathcal{B},N)$ is an MM-$\mathcal{B}$ESP.

(Only If) Suppose there exists an MM-$\mathcal{B}$ESP for $N(\mathbf{m}^0)$. Let $\widehat{\mathfrak{D}}(\mathcal{B},N) = \mathfrak{D}_M(\mathcal{B},N)$. Then $\widehat{\mathfrak{D}}(\mathcal{B},N)$ is right-closed by definition. Since there is an MM-$\mathcal{B}$ESP for $N(\mathbf{m}^0)$, it follows that $\mathbf{m}^0 \in \widehat{\mathfrak{D}}(\mathcal{B},N)$. Suppose $\mathbf{m}^1 \in \widehat{\mathfrak{D}}(\mathcal{B},N)$ and $\mathbf{m}^1 \xrightarrow{t_u} \mathbf{m}^2$ for some $t_u \in T_u$. Then we have that $\mathbf{m}^2 \in \widehat{\mathfrak{D}}(\mathcal{B},N)$. If not, the supervisory policy will not be an MM-$\mathcal{B}$ESP for $\mathbf{m}^2$ (as $\widehat{\mathfrak{D}}(\mathcal{B},N) = \mathfrak{D}_M(\mathcal{B},N)$). In fact, using the same argument, the MM-$\mathcal{B}$ESP will disable any controllable transition whose firing takes the PN outside $\widehat{\mathfrak{D}}(\mathcal{B},N)$. Therefore, the marking monotone policy that enforces the set $\widehat{\mathfrak{D}}(\mathcal{B},N)$ is a $\mathcal{B}$ESP. □

Let $\mathcal{T}_M(\mathcal{B},N,t) \subseteq \mathfrak{D}_M(\mathcal{B},N)$ be the set of markings such that $\forall \mathbf{m} \in \mathcal{T}_M(\mathcal{B},N,t)$, $\mathcal{P}_M(\mathbf{m},t) = 1$, where $\mathcal{P}_M$ is an MM-$\mathcal{B}$ESP that enforces the set $\mathfrak{D}_M(\mathcal{B},N)$. Since $\mathcal{P}_M$ is an MM-$\mathcal{B}$ESP, $\mathcal{T}_M(\mathcal{B},N,t)$ is right-closed.

Lemma 2. *Let* $\{\widetilde{\mathbf{m}}^i\}_{i=1}^{k} = \min(\mathfrak{D}_M(\mathcal{B},N))$. *For any* $t_c \in T_c$, $\min(\mathcal{T}_M(\mathcal{B},N,t_c)) = \{\max\{\mathbf{0}, \widetilde{\mathbf{m}}^i - \mathbf{C}\times\mathbf{1}_c\}\}_{i=1}^{k}$. *Here* $\mathbf{1}_c$ *is the unit-vector whose c-th element (corresponding to transition* t_c*) is unity, the* max *operator acts element-wise, and* $\mathbf{0}$ *represents a vector of all zeros of appropriate size.*

Proof. Recall that we need $\mathbf{m}^0 \in \mathcal{D}_M(\mathcal{B},N)$ for $\mathcal{P}_M$ to enforce property $\mathcal{B}$. First we note that $\forall \widetilde{\mathbf{m}}^i \in \min(\mathfrak{D}_M(\mathcal{B},N))$, $\max\{\mathbf{0}, \widetilde{\mathbf{m}}^i - \mathbf{C}\times\mathbf{1}_c\} \in \mathcal{T}_M(\mathcal{B},N,t_c)$. Since $(\widetilde{\mathbf{m}}^i - \mathbf{C}\times\mathbf{1}_c) + \mathbf{C}\times\mathbf{1}_c = \widetilde{\mathbf{m}}^i$, we have $\max\{\mathbf{0}, \widetilde{\mathbf{m}}^i - \mathbf{C}\times\mathbf{1}_c\} + \mathbf{C}\times\mathbf{1}_c \geq \widetilde{\mathbf{m}}^i$. That is, the firing of t_c keeps the marking in the set $\mathfrak{D}_M(\mathcal{B},N)$. That $\max\{\mathbf{0}, \widetilde{\mathbf{m}}^i - \mathbf{C}\times\mathbf{1}_c\}$ is the minimal element of $\mathcal{T}_M(\mathcal{B},N,t_c)$ follows from the observation that it is the largest non-negative marking greater than $(\widetilde{\mathbf{m}}^i - \mathbf{C}\times\mathbf{1}_c)$ and that $\widetilde{\mathbf{m}}^i$ is the minimal element of $\mathfrak{D}_M(\mathcal{B},N)$. □

Algorithm 4 presents a procedure for evaluating a $\mathcal{B}$-preserving composition, $N_2 = (\Pi_2, T_2, \Gamma_2)$, of a PN $N_1 = (\Pi_1, T_1, \Gamma_1)$ and an MM-$\mathcal{B}$ESP, $\mathcal{P}_M$, that enforces the set $\mathfrak{D}_M(\mathcal{B},N_1)$. We need

Algorithm 4 COMPOSE(N_1, $\mathfrak{D}_M(\mathcal{B}, N_1)$)

1: $\Pi_2 = \Pi_1$
2: $T_2 = T_{1u}$
3: $\Gamma_2(t,p) = \Gamma_1(t,p)$, $\Gamma_2(p,t) = \Gamma_1(p,t)\ \forall t \in T_{1u}$
4: **for** $i \in \{1, \ldots |T_{1c}|\}$ **do**
5: **for** $j \in \{1, \ldots k\}$ **do**
6: $T_2 \leftarrow T_2 \cup \{t_i^j\}$
7: **for** $\forall p \in \Pi_2$ **do**
8: $\Gamma(p, t_i^j) = (\max\{\mathbf{0}, \widetilde{\mathbf{m}}^j - \mathbf{C} \times \mathbf{1}_i\})(p)$
9: $\Gamma(t_i^j, p) = (\max\{\mathbf{0}, \widetilde{\mathbf{m}}^j - \mathbf{C} \times \mathbf{1}_i\} + \mathbf{C} \times \mathbf{1}_i)(p)$
10: **end for**
11: **end for**
12: **end for**

to construct N_2 such that $\mathfrak{R}(N_2, \mathbf{m}^0) = \mathfrak{R}(N_1, \mathbf{m}^0, \mathcal{P}_M)$. A supervisory policy has no control over the uncontrollable transitions. Therefore, intuitively, the behaviour of the system in the uncontrollable space should be the same for N_1 and N_2 (Steps 2 and 3). Lemma 2 identifies k minimal elements of the set $\mathcal{T}_M(\mathcal{B}, N, t)$ for a controllable transition t_i of N_1. Using this observation, each controllable transition, t_i, of N_1 is replaced by k-many controllable transitions, $\{t_i^j\}_{j=1}^k$ in N_2. The input arc-weights of $\{t_i^j\}_{j=1}^k$ correspond to these minimal elements of $\mathcal{T}_M(\mathcal{B}, N, t_i)$. The output arc-weights of $\{t_i^j\}_{j=1}^k$ correspond to effect of firing t_i. Steps 4 to 12 accomplish these tasks. T_{1c} and T_{1u} denote the set of controllable and uncontrollable transitions in N_1 respectively.

MM-$\mathcal{B}$ESPs are a generalized version of MM-$\mathcal{B}$ESPs-over-reachable-markings. While MM-$\mathcal{B}$ESPs consider the marking monotonicity over all markings, MM-$\mathcal{B}$ESPs over reachability only consider the markings that are reachable from the initial marking (that is, ignoring the markings that are not reachable from the initial marking). It follows that the existence of an MM-$\mathcal{B}$ESP implies the existence of an MM-$\mathcal{B}$ESPs over reachability. Lemma 2 and Algorithm 4 can be easily extended for MM-$\mathcal{B}$ESPs over reachable markings by constraining the analysis to reachability markings. We do not explicate the details in the interest of space.

Theorem 9. *For an arbitrary Petri Net N_1: ($\exists$ a $\mathcal{B}$-preserving composition of $N_1(\mathbf{m}^0)$ and $\mathcal{P}$) $\Leftrightarrow$ ($\mathcal{P}$ is an MM-$\mathcal{B}$ESP over reachable markings).*

Proof. ($\Rightarrow$) Suppose there exists a $\mathcal{B}$-preserving composition of $N_1(\mathbf{m}^0)$ and $\mathcal{P}$. Then $\mathfrak{R}(N_2, \mathbf{m}^0) = \mathfrak{R}(N_1, \mathbf{m}^0, \mathcal{P})$. Since we have to consider the unsupervised reachability graph of N_2, without loss of generality in the context of the proof, we assume all transitions in N_2 are uncontrollable. The condition $\mathfrak{R}(N_2, \mathbf{m}^0) = \mathfrak{R}(N_1, \mathbf{m}^0, \mathcal{P})$ implies that transitions

$\{t_i^j\} \in T_2$ are state-enabled at a marking if and only if $\mathcal{P}(\mathbf{m}, t_c) = 1$ for some $t_c \in T_{1c}$. To see this, assume $\exists t_i^j \in T_2$ and a marking $\mathbf{m}$ such that $t_i^j \in T_e(N_2, \mathbf{m})$ but $\mathcal{P}(\mathbf{m}, t_i) = 0$, where $t_i \in T_{1c}$. Then $(\mathbf{m} + \mathbf{C} \times \mathbf{1}_i^j) \in \mathfrak{R}(N_2, \mathbf{m}^0) - \mathfrak{R}(N_1, \mathbf{m}^0, \mathcal{P})$, which is a contradiction. In the same way if $\exists t_i \in T_{1c}$ and a marking $\mathbf{m}$ such that $\nexists t_i^j \in T_2$ such that $t_i^j \in T_e(N_2, \mathbf{m})$ but $\mathcal{P}(\mathbf{m}, t_c) = 1$, then $(\mathbf{m} + \mathbf{C} \times \mathbf{1}_i) \in \mathfrak{R}(N_1, \mathbf{m}^0, \mathcal{P}) - \mathfrak{R}(N_2, \mathbf{m}^0)$, which is again a contradiction.

Therefore, $\forall \mathbf{m}$, $\forall t_u \in T_2$, $(t_u \in T_e(N_2, \mathbf{m})) \Leftrightarrow (\mathcal{P}(\mathbf{m}, t) = 1$ for some $t \in T_1)$. A transition that is enabled at a marking is also enabled at all larger markings. This means that $\mathcal{P}$ is a marking-monotone policy. Since N_2 is a $\mathcal{B}$-preserving composition, it means that $\mathcal{P}$ is an MM-$\mathcal{B}$ESP.

($\Leftarrow$) We prove that the PN N_2 obtained by the construction in Algorithm 4 is a $\mathcal{B}$-preserving composition of N_1 and a $\mathcal{B}$ESP $\mathcal{P}$. We use induction to prove that $\mathfrak{R}(N_2, \mathbf{m}^0) = \mathfrak{R}(N_1, \mathbf{m}^0, \mathcal{P})$. The base case is the initial marking $\mathbf{m}^0$. Consider a string σ that is a valid firing string from $\mathbf{m}^0$. Suppose $\mathbf{m}^0 \xrightarrow{\sigma} \mathbf{m}^1$ and $\mathbf{m}^0 \xrightarrow{\sigma_1} \mathbf{m}^2$, where $\sigma_1 \in pr(\sigma)$. Here we use $pr(\bullet)$ to denote the set of prefixes of the string argument. The induction hypothesis is that $\mathbf{m}^2 \in \mathfrak{R}(N_2, \mathbf{m}^0)$ and $\mathbf{m}^2 \in \mathfrak{R}(N_1, \mathbf{m}^0, \mathcal{P})$ $\forall \sigma_1 \in pr(\sigma)$.

Since the input arc-weights of uncontrollable transitions are the same in N_1 and N_2, if $\exists t_u \in T_{1u} \cap T_e(N_1, \mathbf{m}^1)$, then $\exists t_u \in T_2 \cap T_e(N_2, \mathbf{m}^1)$. Since the output arc-weights of uncontrollable transitions are same in N_1 and N_2, if $\mathbf{m}^1 \xrightarrow{t_u} \mathbf{m}^3$, then $\mathbf{m}^3 \in \mathfrak{R}(N_2, \mathbf{m}^0)$ and $\mathbf{m}^3 \in \mathfrak{R}(N_1, \mathbf{m}^0, \mathcal{P})$. Next consider a $t_i \in T_{1c}$. If $\mathcal{P}(\mathbf{m}^1, t_i) = 1$, then from Lemma 2, we have that $\mathbf{m}^1 \geq \widehat{\mathbf{m}}_i$ for some $\widehat{\mathbf{m}}_i \in \min(\mathcal{T}_M(\mathcal{B}, N, t_i))$. Then it follows from the construction in Algorithm 4, that $\exists j$ such that $t_i^j \in T_e(N_2, \mathbf{m}^1)$ (Step 8). Moreover, the firing of t_i^j adds $\mathbf{C}_i(p)$-many tokens in places $p \in \Pi_2$, which is equal to the number of tokens added in $p \in \Pi_1$. Therefore, if $\mathbf{m}^1 \xrightarrow{t_i} \mathbf{m}^4$, then $\mathbf{m}^4 \in \mathfrak{R}(N_2, \mathbf{m}^0)$ and $\mathbf{m}^4 \in \mathfrak{R}(N_1, \mathbf{m}^0, \mathcal{P})$. On the other hand, if $\mathcal{P}(\mathbf{m}^1, t_i) = 0$, then from Lemma 2, we have that $\nexists \widehat{\mathbf{m}}_i \in \min(\mathcal{T}_M(\mathcal{B}, N, t_i))$ such that $\mathbf{m}^1 \geq \widehat{\mathbf{m}}_i$. Then it follows from the construction in Algorithm 4, that $\nexists j$ such that $t_i^j \in T_e(N_2, \mathbf{m}^1)$ (Step 8). This constitutes the induction step. □

An important consequence of the above theorem is that if there exists an MM-$\mathcal{B}$ESP $\mathcal{P}$ for $N(\mathbf{m}^0)$, then there exists a composition of $\mathcal{P}$ and $N(\mathbf{m}^0)$. Moreover, due to the marking-monotone nature over the whole space of markings, the composition remains the same for any $\widehat{\mathbf{m}}^0 \geq \mathbf{m}^0$. This is a desirable feature in the design of systems as analysis for various initial markings becomes easy, without having to evaluate the composition for each of them separately.

Suppose we want to synthesize a supervisory policy that enforces the property $\wedge_{c=1}^{l} \mathcal{B}_c$ in a Petri net $N_1(\mathbf{m}^0)$. We assume that the existence of an MM-$\mathcal{B}_c$ESP over reachable markings is decidable for all $c \in \{1, \ldots, l\}$, and that there exists a procedure for synthesis.

We also assume that the composed model and the supervisory policy that enforces $\wedge_{c=1}^{l}\mathcal{B}_c$ is independent of the order in which $\mathcal{B}_c$s are enforced. Algorithm 5 gives an *outline* of the procedure for the synthesis of a supervisory policy that enforces $(\wedge_{c=1}^{l}\mathcal{B}_c)$. A more specific procedure will depend on the properties that we want to enforce. Note that in Algorithm 5 we use the set $\widehat{\gamma}$ as a proxy for the MM policy, which due to result in Theorem 8 does not lead to any loss of generality.

Algorithm 5 SEQSYNTH($\mathcal{B}_c$, N_c)

1: $\widehat{\gamma} = \mathcal{N}^n$
2: **while** $(\mathbf{m}^0 \in \widehat{\gamma}) \wedge (\{\mathcal{B}_c\}_{c=1}^{l}$ are not enforced) **do**
3: **for** $c = 1$ to l **do**
4: $\widehat{\gamma}$=SYNTHESIZE($\widehat{\gamma}, \mathcal{B}_c, N_c$)
5: N_{c+1}=COMPOSE($\mathcal{B}_c, N_c$)
6: **end for**
7: **end while**

The algorithm stops either when the initial marking drops out of the estimate $\widehat{\gamma}$ or when property $\wedge_{c=1}^{l}\mathcal{B}_c$ can be enforced by enforcing $\widehat{\gamma}$. However, whether a specific instance of the procedure (for given $\{\mathcal{B}_c\}_{c=1}^{l}$) will terminate or not will depend on the subroutine SYNTHESIZE. The subroutine SYNTHESIZE takes the current estimate of $\widehat{\gamma}$ and modifies it so that another property $\mathcal{B}_c$ can be enforced. For several properties the while loop in Algorithm 5 will terminate in a single iteration. But a PN that is live can lose liveness if some markings that were originally reachable cannot be reached anymore. Therefore, if liveness is one of the $\mathcal{B}_i$s, then the while loop in Algorithm 5 might have to execute several times till all the properties are enforced.

3.7.2 An Illustrative Example

We illustrate the procedure in Algorithm 4 and 5 using an example. We are interested in synthesizing a supervisory policy, $\mathcal{P}$, for the PN N_1 as shown in Figure 3.6. If $\mathbf{m}^0$ is the initial marking, then the objectives for supervisions are: (1) $N_1(\mathbf{m}^0)$ should be live; and (2) $\forall \mathbf{m}^1 \in \mathfrak{R}(N_1, \mathbf{m}^0, \mathcal{P})$, $\mathbf{m}^1(p_6)+\mathbf{m}^1(p_7)+\mathbf{m}^1(p_8) \geq 1$. The set of initial markings for which an $\mathcal{L}$ESP exists, $\mathfrak{D}(\mathcal{L}, N_1)$, is given by the right-closed set with minimal elements $\widetilde{\mathbf{m}}_1 = (1\ 0\ 0\ 0\ 0\ 0\ 0\ 0)^T$ and $\widetilde{\mathbf{m}}_2 = (0\ 0\ 0\ 1\ 1\ 0\ 0\ 0)^T$ ([61]). Let $\mathbf{C}_1 = (\text{-}1\ 1\ 0\ 0\ 0\ 0\ 0\ 0)^T$ denote the column of the incidence matrix $\mathbf{C}$ corresponding to transition t_1. Applying the result from Lemma 2, we get two minimal elements of $\mathcal{T}_M(\mathcal{L}, N_1, t_1)$, $\{\widehat{\mathbf{m}}_i\}_{i=1,2}$, as: $\widehat{\mathbf{m}}_1 = \max\{\mathbf{0}, \widetilde{\mathbf{m}}_1 - \mathbf{C_1}\} = (2\ 0\ 0\ 0\ 0\ 0\ 0\ 0)^T$ and $\widehat{\mathbf{m}}_2 = \max\{\mathbf{0}, \widetilde{\mathbf{m}}_2 - \mathbf{C_1}\} = (1\ 0\ 0\ 1\ 1\ 0\ 0\ 0)^T$.

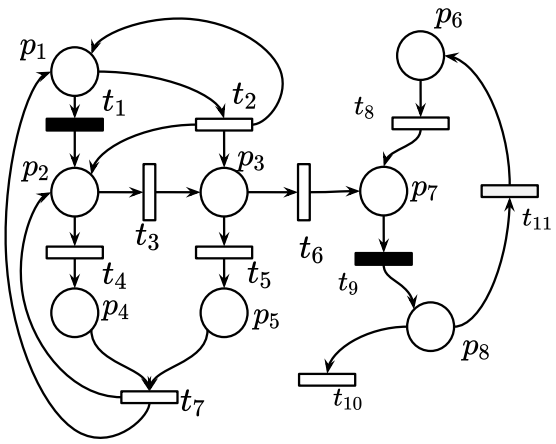


Figure 3.6: Petri Net, N_1, to illustrate the procedure of Algorithms 4 and 5.

Upon firing of t_1 from $\widehat{\mathbf{m}}_1$ and $\widehat{\mathbf{m}}_2$, we get the markings $\overline{\mathbf{m}}^1 = (1\ 1\ 0\ 0\ 0\ 0\ 0\ 0)^T$ and $\overline{\mathbf{m}}^2 = (0\ 1\ 0\ 1\ 1\ 0\ 0\ 0)^T$ respectively.

The first thing to note is that $\overline{\mathbf{m}}_1, \overline{\mathbf{m}}_2 \in \mathfrak{D}(\mathcal{L}, N_1)$. The PN N_2 which is a composition of N_1 and the $\mathcal{L}$ESP $\mathcal{P}_\mathcal{L}$ is shown in Figure 3.7. Transition t_1 in N_1 is replaced by two new controllable transitions t_1^1 and t_1^2. The input (output) arc-weights of t_1^1 and t_1^2 correspond to $\widehat{\mathbf{m}}^1$ and $\widehat{\mathbf{m}}^2$ (resp. $\overline{\mathbf{m}}^1$ and $\overline{\mathbf{m}}^2$) respectively. Transition t_9 will always be enabled by the $\mathcal{L}$ESP $\mathcal{P}_\mathcal{L}$. Therefore, there is no change in it. It can be verified that $\mathfrak{R}(N_2, \mathbf{m}^0) = \mathfrak{R}(N_1, \mathbf{m}^0, \mathcal{P}_\mathcal{L})$.

Next we synthesize an $\mathcal{L}$ESP that enforces the property: $\forall \mathbf{m}^1 \in \mathfrak{R}(N_1, \mathbf{m}^0, \mathcal{P})$, $\mathbf{m}^1(p_6) + \mathbf{m}^1(p_7) + \mathbf{m}^1(p_8) \geq 1$. Let $\mathfrak{D}_M(\mathcal{C}, N_1) = \{\mathbf{m} \in \mathcal{N}^n : \mathbf{m}(p_6) + \mathbf{m}(p_7) + \mathbf{m}(p_8) \geq 1\}$. Since the tokens in place p_8 can be lost by the uncontrolled firing of t_{10}, transition t_9 should be controlled enabled if and only if the resulting marking is in $\mathfrak{D}_M(\mathcal{C}, N_1)$. By Lemma 2, the minimal elements of $\mathcal{T}_M(\mathcal{C}, N_1, t_1)$ are: $\{(0\ 0\ 0\ 0\ 0\ 0\ 2\ 0)^T, (0\ 0\ 0\ 0\ 0\ 1\ 1\ 0)^T\}$. For this particular example, the intersection of $\mathfrak{D}_M(\mathcal{L}, N_1)$ and $\mathfrak{D}_M(\mathcal{C}, N_1)$ gives us an estimate of the set of markings for which a supervisory policy that enforces both properties exists.

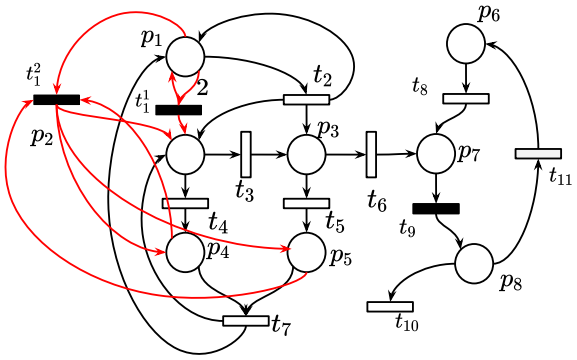


Figure 3.7: Petri Net, N_2.

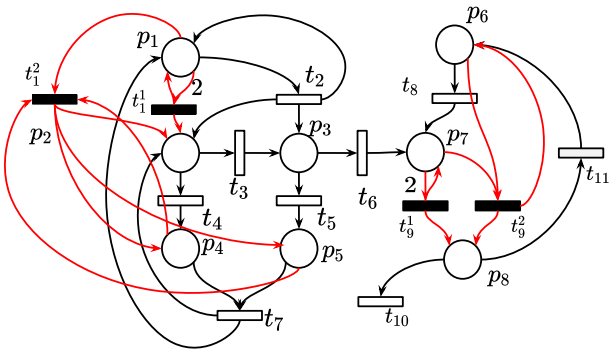


Figure 3.8: Petri Net, N_3.

CHAPTER 4

SYNTHESIS OF LIVENESS ENFORCING SUPERVISORY POLICIES FOR PETRI NETS USING A GENERALIZATION OF COVERABILITY GRAPHS

4.1 Generalized Coverability Graphs

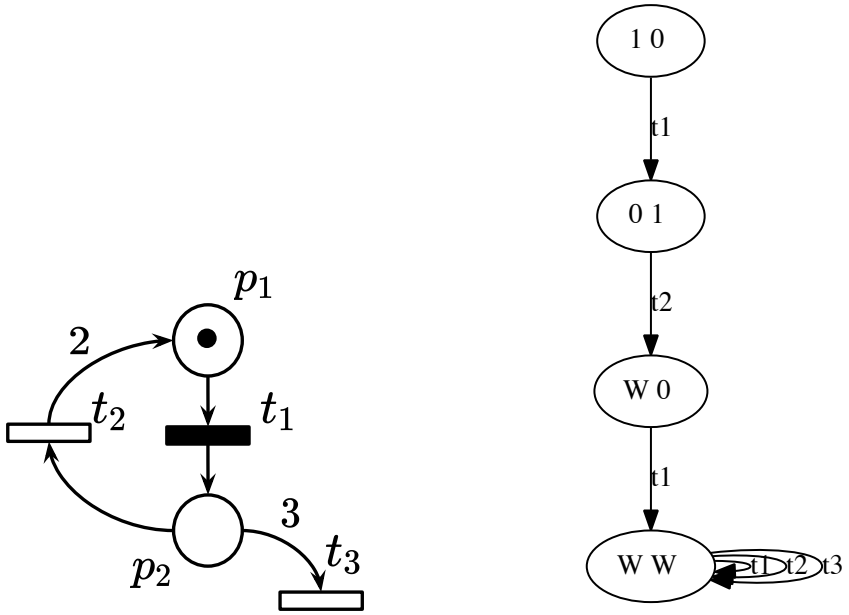
The traditional coverability graph (TCG) is the Karp and Miller tree [40], where duplicate nodes are merged as one. Due to the inherent monotonicity in the operation of PNs, if there is a string of transitions σ that can be fired from a marking $\mathbf{m}_1$ that results in a larger marking $\mathbf{m}_2(\geq \mathbf{m}_1)$, then σ can be fired from $\mathbf{m}_2$ also; resulting in an even larger marking $\mathbf{m}_3(\geq \mathbf{m}_2)$. This process can be repeated infinitely often to obtain an infinite sequence of increasing markings. The main concept behind the TCG is to represent this infinite sequence of increasing markings by a single marking. With this abstraction, the TCG becomes a finite representation of a possibly infinite reachability graph of a PN. The algorithm for drawing a TCG can be found in [56, 12].

We now discuss some important features of TCG using the PN N_1 and its TCG shown in Figure 4.1. The node (ω 0) of Figure 4.1b basically represents that the string t_1t_2 can be repeated from (1 0) as often as necessary to obtain an arbitrarily large number of tokens in place p_1 and zero tokens in p_2. ω is a symbol such that $\omega + 1 = \omega - 1 = \omega$. It can be interpreted as a very large positive integer. Our aim is to generalize the TCG so that it can elicit more information about the underlying system. However, we also want it to be finite.

Formally, let $\{\zeta_0, \zeta_1, \ldots, \zeta_{k-1}\}$ be a k-fold partition of $\mathcal{N}$ such that:

1. Each ζ_i is countably infinite.

2. The addition and subtraction operations are interpreted as binary operators: $\zeta_i \times \zeta_j \rightarrow \zeta_l$, for all i, j and some corresponding l in the set $\{0, \ldots, k-1\}$. That is, the result of addition and subtraction amongst any element of ζ_i and any element of ζ_j belongs to the same ζ_l.



(a) PN N_1

(b) Traditional Coverability Graph for N_1

Figure 4.1: An example PN N_1 with its traditional coverability Graph.

3. $\forall i, j \in \{0, \ldots, k-1\}$, $\forall x \in \zeta_i$, $\forall n \in \zeta_j$, $\exists h_i^j \in \mathcal{N}^+$ such that:

$$x + \underbrace{n + \ldots + n}_{h_i^j \text{ times}} = y, \text{ where } y \in \zeta_i$$

4. $\forall i, j \in \{0, \ldots, k-1\}$, for all large enough $x \in \zeta_i$, $\forall n \in \zeta_j$, $\exists g_i^j \in \mathcal{N}^+$ such that:

$$x - \underbrace{n - \ldots - n}_{g_i^j \text{ times}} = z, \text{ where } z \in \zeta_i$$

5. $\forall i \in \{0, \ldots, k-1\}$, we use the symbol ω_i to denote a very large number in ζ_i. That is, $\forall x \in \zeta_i$: $\omega_i > x$. Let $\{x_0, x_1, \ldots\}$ denote such a ζ_i, then ω_i will also be referred to as $\lim_n x_n$.

6. Let $m \in \zeta_j$. We use what can be called a *continuous extension* of addition: $\omega_i + m = \lim_n(x_n) + m = \lim_n(x_n + m) = \omega_l$, where $(x_n + m) \in \zeta_l$. Property 2 ensures that this operation is well-defined and ζ_l is unique for a given ζ_i and ζ_j.

7. We define a well quasi order $\precsim$ on $\mathcal{N}$ as: $(x \precsim y) \Leftrightarrow ((x \leq y) \wedge (x, y \in \zeta_i))$. If $x \neq y$,

then we denote the wqo by the symbol '$\prec$'.

The construction can be extended for n-dimensional vectors. Specifically, $\forall i \in \{1, \ldots, n\}$, let $\{\zeta_0^i, \zeta_1^i, \ldots, \zeta_{k_i-1}^i\}$ be a partition with largest elements denoted by $\{\omega_j^i\}_{j=0}^{k_i-1}$ and equipped with a wqo $\precsim_i$, as discussed above. Let $\mathbf{x}_i$ and $\mathbf{y}_i$ denote the i-th component of two integer-valued vectors $\mathbf{x}, \mathbf{y} \in \mathcal{N}^n$ for all $i \in \{1, 2, \ldots n\}$. We have:

$$(\mathbf{x}_i \precsim_i \mathbf{y}_i) \Leftrightarrow ((\mathbf{x}_i \leq \mathbf{y}_i) \wedge (\mathbf{x}_i, \mathbf{y}_i \in \zeta_j^i)) \quad j \in \{1, \ldots, k_i\} \tag{4.1}$$

$$(\mathbf{x} \precsim \mathbf{y}) \Leftrightarrow (\mathbf{x}_i \precsim_i \mathbf{y}_i,\ \forall i \in \{1, 2, \ldots n\}) \tag{4.2}$$

We sometimes use the notation $\succsim$ defined as: $(\mathbf{x} \precsim \mathbf{y}) \Leftrightarrow (\mathbf{y} \succsim \mathbf{x})$. Since we are partitioning the n-dimensional space into finitely-many sets and using the standard order $\leq$ within them, the following observation follows:

Observation 7. *$\precsim$ on $\mathcal{N}^n$ is a wqo.*

In line with the algorithm stated in reference [56], the generalized coverability graph (GCG) can be constructed by the following algorithm:

1. Label the initial marking $\mathbf{m}_0$ as the root and tag it *new*.
2. While *new* markings exist, do the following:
   (a) Select a new marking $\mathbf{m}$.
   (b) If $\mathbf{m}$ is identical to a marking on the path from the root to $\mathbf{m}$, then tag $\mathbf{m}$ *old* and go to another *new* marking.
   (c) If no transitions are enabled at $\mathbf{m}$, tag $\mathbf{m}$ as *dead-end*.
   (d) While there exists enabled transitions at $\mathbf{m}$, do the following for each enabled transition t:
      i. Obtain $\mathbf{m}'$ that results from the firing of t at $\mathbf{m}$.
      ii. On the path from the root to $\mathbf{m}$, if there exists a marking $\mathbf{m}''$ such that $\mathbf{m}''(p) \leq \mathbf{m}'(p)$ for each place p and $\mathbf{m}' \neq \mathbf{m}''$, that is, $\mathbf{m}''$ is coverable, then: for each place p such that $\mathbf{m}''(p) \prec_p \mathbf{m}'(p)$, replace $\mathbf{m}'(p)$ by ω_i^p, where $\prec_p$ denotes the wqo corresponding to place p.
      iii. introduce $\mathbf{m}'$ as a node, draw an arc with label t from $\mathbf{m}$ to $\mathbf{m}'$, and tag $\mathbf{m}'$ as *new*.

Recall that for a wqo every strictly decreasing sequence and every subset of incomparable elements is finite. As a consequence, we get the following result:

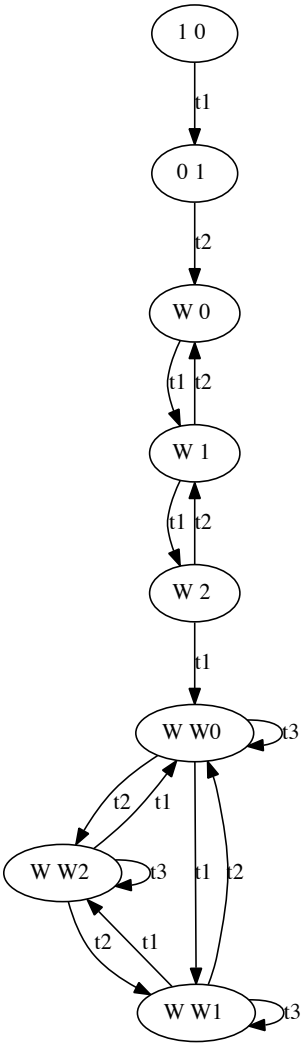


Figure 4.2: Generalized Coverability Graph for N_1, where $\zeta_0^1 = \mathcal{N}$ is used for place p_1; and $\zeta_i^2 = \{n \in \mathcal{N} \mid n(mod 3) = i\}$, and $\omega_i = \lim_n \zeta_i$, for $i \in \{0, 1, 2\}$ is used for place p_2.

Observation 8. *The Generalized Coverability Graph has finite number of nodes.*

Figure 4.2 shows the generalized Coverability Graph for the PN N_1 in Figure 4.1 with $\zeta_0^1 = \mathcal{N}$ (corresponding to p_1) and $\{\zeta_i^2 = i \ (mod) \ 3\}_{i=0}^2$ (corresponding to p_2). Token-value in place p_1 is equipped with the traditional notion of ω. For place p_2, ω_i denotes a very large integer that is $i \ (mod) \ 3$ for $i = 0, 1, 2$. We have: $\omega_0 + 1 = \omega_1$, $\omega_1 + 1 = \omega_2$ and $\omega_2 + 1 = \omega_0$. Since GCG conveys more information when compared to TCG, it could have significantly more nodes compared to TCG. In Section 4.2, we illustrate the application of GCG in testing the existence and non-existence of a large class of LESPs for arbitrary PNs.

4.2 Synthesis of LESPs using Generalized Coverability Graphs

Marking monotone supervisory policies have the feature that if they permit a transition to fire at a marking, then they permit the transition to fire at all larger markings as well. If a marking monotone supervisory policy $\mathcal{P}$, that is an LESP for $N(\mathbf{m}_0)$, is also an LESP for $N(\widehat{\mathbf{m}}_0)$ for any $\widehat{\mathbf{m}}_0 \geq \mathbf{m}_0$, then $\mathcal{P}$ is a marking-monotone LESP (MM-LESP). The set of initial markings for which an MM-LESP exists, $\Delta_M(N)$, is right-closed. While neither the existence nor the non-existence of an LESP for an arbitrary PN $N(\mathbf{m}_0)$ is semi-decidable [35], the existence of a marking monotone LESP (MM-LESP) for $N(\mathbf{m}_0)$ is decidable for an arbitrary PN [62].

We use the traditional interpretation of ordering of integers in determining marking-monotonicy and right-closure (eg. references [35, 62]). By generalizing the notion of *order*, we can generalize the algorithm for the synthesis of MM-LESP. This is the main idea of the results in this section. We first illustrate the process using the example PN N_1 from Figure 4.1a.

From [62], $\Delta_M(N)$ is a control-invariant right-closed subset of $\Delta(N)$ for which the following path requirement is true: $\forall \mathbf{m}^i \in \min(\Delta_M(N))$, there is a path $v_0 \xrightarrow{\sigma_1} v_1 \xrightarrow{\sigma_2} v_1$, in the TCG $G(N(\mathbf{m}^i), \mathcal{P}) = (V, A)$, such that $\mathbf{x}(\sigma_2) \geq \mathbf{1}$ and $\mathbf{C}\mathbf{x}(\sigma_2) \geq \mathbf{0}$, where $\mathbf{1}$ is the m-dimensional vector of all ones, $\mathcal{P}$ ensures the reachable markings never leaves $\Delta_M(N)$. There exists an MM-LESP for $N(\mathbf{m}^0)$ iff $\mathbf{m}^0 \in \Delta_M(N)$. In the first half of this section, we will define a set $\Delta_C(N)$, an instance of which is $\Delta_M(N)$.

First we generalize the definition of right-closure.

Definition 7. *A set of markings $\mathcal{M}$ is called right-closed with respect to a wqo $\precsim$ if:* $((\mathbf{m} \in \mathcal{M}) \wedge (\mathbf{m} \precsim \widehat{\mathbf{m}})) \Rightarrow (\widehat{\mathbf{m}} \in \mathcal{M})$.

The minimal elements of a set $\mathcal{M}$ that is right-closed with respect to a wqo $\precsim$, denoted by $\min_{\precsim}(\mathcal{M})$, is the set of markings such that: $\forall \mathbf{m} \in \mathcal{M}$, $\exists \widetilde{\mathbf{m}}^i \in \min_{\precsim}(\mathcal{M})$ such that $\widetilde{\mathbf{m}}^i \precsim \mathbf{m}$. Since $\precsim$ is a wqo, $\min_{\precsim}(\mathcal{M})$ is finite.

We use $\max_{\precsim}\{\mathbf{m}, \mathbf{IN}_t\}$ to denote the smallest (interpreted in the traditional sense) marking such that $\mathbf{IN}_t \leq \max_{\precsim}\{\mathbf{m}, \mathbf{IN}_t\}$ and $\mathbf{m} \precsim \max_{\precsim}\{\mathbf{m}, \mathbf{IN}_t\}$.

Let $\mathcal{M}$ be a set of markings which is right-closed with respect to $\precsim$. $\mathcal{M}$ is control invariant with respect to $(N, \precsim)$ if $\forall \mathbf{m}^1 \in \mathcal{M}, \forall t_u \in T_e(N, \mathbf{m}^1) \cap T_u$ and $\max_{\precsim}\{\mathbf{m}^1, \mathbf{IN}_{t_u}\} \xrightarrow{t_u} \mathbf{m}^2$ in N: $\widetilde{\mathbf{m}} \precsim \mathbf{m}^2$ for some $\widetilde{\mathbf{m}} \in \min_{\precsim}(\mathcal{M}, \precsim)$.

If two markings $\mathbf{m}^1$ and $\mathbf{m}^2$ are such that either $\mathbf{m}^1 \precsim \mathbf{m}^2$ or $\mathbf{m}^2 \precsim \mathbf{m}^1$, then, for ease of exposition, we would say that they belong to the same *class*.

Definition 8. *A supervisory policy $\mathcal{P} : \mathcal{N}^n \times T \to \{0,1\}$ is a class monotone policy (CM-policy) if $\forall \widehat{\mathbf{m}} \succsim \mathbf{m}, \forall t \in T, \mathcal{P}(\widehat{\mathbf{m}}, t) \geq \mathcal{P}(\mathbf{m}, t)$. That is, if a transition is permitted by a CM-policy at a marking, it will be permitted at all larger markings inside the class as well. If a CM-policy that is an LESP for $N(\mathbf{m}^0)$, is also an LESP for $N(\widehat{\mathbf{m}}^0), \forall \widehat{\mathbf{m}}^0 \succsim \mathbf{m}^0$, then it is said to be a class-monotone LESP (CM-LESP) for $N(\mathbf{m}^0)$.*

The set

$$\Delta_C(N, \precsim) = \{\mathbf{m}^0 : \exists \text{ a CM-LESP for } N(\mathbf{m}^0)\}$$

denotes the set of initial markings for which there is a CM-LESP for the PN structure N. It follows that $\Delta_C(N, \precsim) \subseteq \Delta(N)$.

Consider a PN N with the initial marking $\mathbf{m}^0 \in \Delta_C(N, \precsim)$. We define a class-monotone supervisory policy $\widehat{\mathcal{P}}$ for $N(\mathbf{m}^0)$ as follows— $\forall \mathbf{m}^i \in \mathfrak{R}(N, \mathbf{m}^0, \widehat{\mathcal{P}})$,

1. if $t_l \in T_u$, $\widehat{\mathcal{P}}(\mathbf{m}^i, t_l) = 1$,
2. if $t_l \in T_c$, then $\widehat{\mathcal{P}}(\mathbf{m}^i, t_l) = 1$, if and only if $t_l \in T_e(N, \mathbf{m}^i)$ and $\mathbf{m}^i \xrightarrow{t_l} \mathbf{m}^j$ in N (in the absence of supervision), and $\mathbf{m}^j \in \Delta_C(N, \precsim)$.

Theorem 10. *There exists a CM-LESP for $N(\mathbf{m}^0)$ if and only if $\mathbf{m}^0 \in \Delta_C(N)$ where $\Delta_C(N) \subseteq \Delta(N)$ is a set with the following properties:*

1. *it is right-closed with respect to $\precsim$;*
2. *it is control invariant with respect to $(N, \precsim)$;*
3. *$\forall \mathbf{m}^1 \in \Delta_C(N), \exists \mathbf{m}^2, \mathbf{m}^3 \in \Delta_C(N), \exists$ a valid firing string $\sigma = \sigma_1\sigma_2$ in N such that $\mathbf{m}^1 \xrightarrow{\sigma_1} \mathbf{m}^2 \xrightarrow{\sigma_2} \mathbf{m}^3, \mathbf{m}^3 \succsim \mathbf{m}^2$, all transitions appear at least once in σ_2, and $\forall \sigma_3 \in pr(\sigma_1\sigma_2)$, $(\mathbf{m}^1 \xrightarrow{\sigma_3} \mathbf{m}^4) \Rightarrow (\mathbf{m}^4 \in \Delta_C(N))$.*

Proof. (*Only if*) Suppose there exists a CM-LESP $\mathcal{P}$ for $N(\mathbf{m}^0)$. Then from Theorem 5.1 in [33], $\mathbf{m}^0 \in \Upsilon$, where Υ is a control invariant set such that: $\forall \mathbf{m}^1 \in \Upsilon, \exists \mathbf{m}^2, \mathbf{m}^3 \in \Upsilon, \exists$ a valid firing string $\sigma = \sigma_1\sigma_2$ in N such that $\mathbf{m}^1 \xrightarrow{\sigma_1} \mathbf{m}^2 \xrightarrow{\sigma_2} \mathbf{m}^3, \mathbf{m}^3 \geq \mathbf{m}^2$, all transitions appear at least once in σ_2, and $\forall \sigma_3 \in pr(\sigma_1\sigma_2)$, $(\mathbf{m}^1 \xrightarrow{\sigma_3} \mathbf{m}^4) \Rightarrow (\mathbf{m}^4 \in \Upsilon)$. Now, since, $\mathcal{P}$ is a class-monotone LESP for all $\mathbf{m} \in \Upsilon$, it is an LESP for and is class-monotone over all markings $\widehat{\mathbf{m}} \succsim \mathbf{m}$. Therefore, there exists a class-monotone LESP for all markings $\widehat{\mathbf{m}} \succsim \mathbf{m}$, and Υ is right-closed with respect to $\precsim$. Combining the above two observations, we get that $\mathbf{m}^3 \succsim \mathbf{m}^2$, which proves Item 3 of the theorem.
(*If*) If $\mathbf{m}^0 \in \Delta_C(N)$ with $\Delta_C(N)$ having the properties as elucidated in the statement of the theorem (items 2 and 3), then by Theorem 5.1 of [33], the supervisory policy $\widehat{\mathcal{P}}$ defined above is an LESP. By item 1, $\mathcal{P}$ is a CM-LESP. □

Observation 9. *The class-monotone supervisory policy $\widehat{\mathcal{P}}$ defined above is the minimally restrictive CM-policy that enforces liveness in $N(\mathbf{m}^0)$ where $\mathbf{m}^0 \in \Delta_C(N, \precsim)$.*

The takeaway from Observation 9 is that if we have an effectively computable procedure for testing membership of $\mathbf{m}^0$ in $\Delta_C(N, \precsim)$, then we can construct the minimally restrictive CM-policy that enforces liveness in $N(\mathbf{m}^0)$.

Lemma 3. *If the set $\min_{\precsim}(\mathcal{M})$ of a set of markings $\mathcal{M}$ which is right-closed with respect to $\precsim$ is effectively computable, its control invariance with respect to N can be decided in finite time.*

Proof. $\mathcal{M}$ is control invariant with respect $(N, \precsim)$ if and only if $\forall t_u \in T_u, \forall \mathbf{m}^i \in \min_{\precsim}(\mathcal{M}), \exists \widetilde{\mathbf{m}}^j \in \min_{\precsim}(\mathcal{M})$, such that

$$(\max\nolimits_{\precsim}\{\mathbf{m}^i, \mathbf{IN}_u\} + \mathbf{C} \times \mathbf{1}_u) \succsim \widetilde{\mathbf{m}}^j \tag{4.3}$$

where $\mathbf{1}_u$ is the m-dimensional unit-vector where the u-th component is unity, $\mathbf{IN}_u$ is the u-th column of the $n \times m$ input matrix of N, and $\mathbf{C}$ is the $n \times m$ incidence matrix of N.

By definition of $\max_{\precsim}\{\mathbf{m}^i, \mathbf{IN}_u\}$, there cannot be a marking $\mathbf{m}^k$ such that: $\mathbf{m}^i \precsim \mathbf{m}^k \prec \max_{\precsim}\{\mathbf{m}^i, \mathbf{IN}_u\}$. Consider a marking $\mathbf{m}^k \succsim \max_{\precsim}\{\mathbf{m}^i, \mathbf{IN}_u\}$. Then by item 2 of the characterization of $\precsim$, addition of $\mathbf{C} \times \mathbf{1}_u$ to $\mathbf{m}^k$ will result in a marking that is (ordered with and) greater than $\max_{\precsim}\{\mathbf{m}^i, \mathbf{IN}_u\} + \mathbf{C} \times \mathbf{1}_u$.

Therefore, if the control invariance condition is satisfied by elements in $\min_{\precsim}(\mathcal{M}, \precsim)$, then it is satisfied by all elements in $(\mathcal{M}, \precsim)$. On the other hand, if there is a minimal element that does not satisfy the control invariance condition, then obviously the set is not control invariant. Now, since $\precsim$ is a wqo, $\min(\mathcal{M}, \precsim)$ has finite number of elements, and hence the control invariance of $(\mathcal{M}, \precsim)$ can be decided in finite time. □

For a traditional coverability graph $G(N(\mathbf{m}^0), \mathcal{P}) = (V, A)$ constructed under the supervision of a marking monotone $\mathcal{P}$, where V and A denote the set of nodes and edges respectively, $\forall v \in V, \forall k \in \mathcal{N}$ there exists a valid firing string σ starting from $\mathbf{m}^0$ such that $\mathbf{m}^0 \xrightarrow{\sigma} \mathbf{m}^i$ and

$$\mathbf{m}^i(p_j) = \begin{cases} v(j) & \text{if } v(j) \neq \omega, \\ \geq k & \text{otherwise.} \end{cases} \tag{4.4}$$

That is, if the j-th entry of a vector denoting the node v in the TCG has a collection of ω-symbols, and if we replaced the ω-symbols with any integer k to obtain a marking $\widehat{\mathbf{m}}$, then there is a valid firing string $\sigma \in T^*$ such that $\mathbf{m}^0 \xrightarrow{\sigma} \mathbf{m}^i$ such that $\mathbf{m}^i \geq \widehat{\mathbf{m}}$ (see Theorem 4.2 of [63] and Equation 1 of [35]). We can obtain a similar observation for a GCG $G_{\precsim}(N(\mathbf{m}^0), \mathcal{P}) = (\widehat{V}, \widehat{A})$ constructed under the supervision of a class monotone $\mathcal{P}$, where $\widehat{V}$

and $\widehat{A}$ denote the set of nodes and edges respectively. $\forall \widehat{v} \in \widehat{V}, \forall k \in \zeta_l^j$ where $\mathbf{m}^0(p_j) \in \zeta_l^j$, there exists a valid firing string σ starting from $\mathbf{m}^0$ such that $\mathbf{m}^0 \xrightarrow{\sigma} \mathbf{m}^i$ and

$$\mathbf{m}^i(p_j) = \begin{cases} v(j) & \text{if } v(j) \neq \omega_l^j, \\ \succsim k & \text{otherwise.} \end{cases} \tag{4.5}$$

Observation 10. *Consider an initial marking $\mathbf{m}^0 \in \Delta_C(N, \precsim)$. Let $G_{\precsim}(N(\mathbf{m}^0), \widehat{\mathcal{P}}) = (V, A)$ be the GCG of $N(\mathbf{m}^0)$ under the supervision of a class-monotone LESP $\widehat{\mathcal{P}}$ defined earlier. Then $\exists v_i \in V$, $\exists \sigma_1, \sigma_2 \in T^*$, such that $v_0 \xrightarrow{\sigma_1} v_i \xrightarrow{\sigma_2} v_i$ in $G_{\precsim}(N(\mathbf{m}^0), \widehat{\mathcal{P}})$ and $\mathbf{x}(\sigma_2) \geq \mathbf{1}$, and $\mathbf{C}\mathbf{x}(\sigma_2) \geq \mathbf{0}$, where $\mathbf{1}$ is the m-dimensional vector of all ones.*

Proof. Since $\mathbf{m}^0 \in \Delta_C(N, \precsim)$, and $\widehat{\mathcal{P}}$ is a CM-LESP for $N(\mathbf{m}^0)$, from Theorem 10, $\forall \mathbf{m}^1 \in \Delta_C(N), \exists \mathbf{m}^2, \mathbf{m}^3 \in \Delta_C(N), \exists$ a valid firing string $\sigma = \sigma_1\sigma_2$ in N such that $\mathbf{m}^1 \xrightarrow{\sigma_1} \mathbf{m}^2 \xrightarrow{\sigma_2} \mathbf{m}^3, \mathbf{m}^3 \succsim \mathbf{m}^2$, all transitions appear at least once in σ_2, and $\forall \sigma_3 \in pr(\sigma_1\sigma_2)$, $(\mathbf{m}^1 \xrightarrow{\sigma_3} \mathbf{m}^4) \Rightarrow (\mathbf{m}^4 \in \Delta_C(N))$. Therefore, there is a path $v_0 \xrightarrow{\widehat{\sigma}_1\widehat{\sigma}_2} v_1 \xrightarrow{\widehat{\sigma}_2} v_1$ in $G_{\precsim}(N(\mathbf{m}^0), \widehat{\mathcal{P}})$ where $\mathbf{x}(\widehat{\sigma}_2) \geq \mathbf{1}$ and $\mathbf{C}\mathbf{x}(\widehat{\sigma}_2) \geq \mathbf{0}$. Letting $\sigma_1 = \widehat{\sigma}_1\widehat{\sigma}_2$ and $\sigma_2 = \widehat{\sigma}_2$, we get the above observation. □

For a control invariant set $\Upsilon \subseteq \mathcal{N}^n$, that is right-closed with respect to a wqo $\precsim$, we define the class monotone supervisory policy $\widetilde{\mathcal{P}}_\Upsilon : \mathcal{N}^n \times T \to \{0, 1\}$ as follows

$$\widetilde{\mathcal{P}}_\Upsilon(\mathbf{m}^i, t) = \begin{cases} 0 & \text{if } (t \in T_c) \wedge (\exists \mathbf{m}^j \in \Upsilon, \mathbf{m}^j \succsim \mathbf{m}^i) \\ & \wedge (\mathbf{m}^j \xrightarrow{t_c} \mathbf{m}^k \text{ in } N, \mathbf{m}^k \notin \Upsilon), \\ 1 & \text{otherwise,} \end{cases} \tag{4.6}$$

This supervisory policy is used in the following observation, which presents the necessary and sufficient conditions for the existence of a CM-LESP based on GCG.

Lemma 4. *There is a class-monotone supervisory policy that enforces liveness in $N(\mathbf{m}^0)$ if and only if there is a finite set of minimal elements, $\min_{\precsim}(\Upsilon)$, of a control invariant set $\Upsilon \subseteq \mathcal{N}^n$ that is right-closed with respect to $\precsim$, such that $\forall \widetilde{\mathbf{m}}^i \in \min_{\precsim}(\Upsilon)$, there is a path $v_0 \xrightarrow{\sigma_1} v_1 \xrightarrow{\sigma_2} v_1$, in the generalized coverability graph $G_{\precsim}(N(\widetilde{\mathbf{m}}^i, \widetilde{\mathcal{P}}_\Upsilon)) = (V, A)$, such that $\mathbf{x}(\sigma_2) \geq \mathbf{1}$ and $\mathbf{C}\mathbf{x}(\sigma_2) \geq \mathbf{0}$, where $\mathbf{1}$ is the m-dimensional vector of all ones, and $\mathbf{m}^0 \in \Upsilon$.*

Proof. (*Only if*) Let $\Upsilon = \Delta_C(N, \precsim)(\subseteq \Delta(N))$, in which case the class monotone policy $\widetilde{\mathcal{P}}_\Upsilon$ in the statement of the observation is identical to the class monotone policy $\widehat{\mathcal{P}}$ in Observation 9. The existence of a path with the specific structure in the statement of the observation follows from Observation 10.

(*If*) Since Υ is control invariant we have $\mathfrak{R}(N, \mathbf{m}^0, \widetilde{\mathcal{P}}_\Upsilon) \subseteq \Upsilon$. Since all members of $\widetilde{\mathbf{m}}^i \in \min_{\precsim}(\Upsilon)$ satisfy the requirement on the GCG, and $\widetilde{\mathcal{P}}_\Upsilon$ is class-monotone, the same is true of any $\mathbf{m}^1 \in \mathfrak{R}(N, \mathbf{m}^0, \widetilde{\mathcal{P}}_\Upsilon)(\subseteq \Upsilon)$. From equation 4.5 we note that $\exists \mathbf{m}^2 \in \mathfrak{R}(N, \mathbf{m}^1, \widetilde{\mathcal{P}}_\Upsilon)$ such that

$$\mathbf{m}^2(p_i) = \begin{cases} \succsim k & \text{if } v_1(i) = \omega_l^i, \text{ where } \mathbf{m}^1(p_i), k \in \zeta_l^i, \\ v_1(i) & \text{otherwise.} \end{cases}$$

By choosing k large enough, we can guarantee validity (under supervision) of σ_2 at $\mathbf{m}^2$. That is, for sufficiently large k, $\exists \sigma_3 \in T^*$, such that $\mathbf{m}^1 \to \sigma_3 \to \mathbf{m}^2 \to \sigma_2 \to \mathbf{m}^3$. Since $\mathbf{C}\mathbf{x}(\sigma_2) \geq 0$, it follows that $\mathbf{m}^3 \succsim \mathbf{m}^2$, and since $\mathbf{x}(\sigma_2) \geq \mathbf{1}$, we conclude the (class monotone) policy $\widetilde{\mathcal{P}}_\Upsilon$ enforces liveness in $N(\mathbf{m}^0)$. □

Algorithm 6 Test for existence of the subset $\widehat{\Delta}(N)$ for $N(\mathbf{m}^0)$

1: $\widehat{\Upsilon} = \mathcal{N}^n$, and let $\{\widetilde{\mathbf{m}}^i\}_{i=1}^k = \min_{\precsim}(\widehat{\Upsilon})$.
2: **while** $((\exists t_u \in T_u, \exists \widetilde{\mathbf{m}}^i \in \min_{\precsim}(\widehat{\Upsilon}),$ such that $\max_{\precsim} \{\widetilde{\mathbf{m}}^i, \mathbf{IN}_u\} + \mathbf{C} \cdot \mathbf{1}_u \notin \widehat{\Upsilon}) \vee (\exists \widetilde{\mathbf{m}}^i \in \min_{\precsim}(\widehat{\Upsilon})$ such that $G(N(\widetilde{\mathbf{m}}^i), \widetilde{\mathcal{P}}_{\widehat{\Upsilon}})$ does not have the path requirement)) $\wedge$ $(\mathbf{m}^0 \in \widehat{\Upsilon})$ **do**
3: BumpForControlInvariance$(N, \widehat{\Upsilon})$
4: BumpForPathCondition$(N, \widehat{\Upsilon})$
5: **end while**
6: **if** $\mathbf{m}^0 \notin \widehat{\Upsilon}$ **then**
7: **return**("no solution");
8: **else**
9: **return** $\widehat{\Upsilon}$
10: **end if**

Algorithm 7 BumpUpForControlInvariance$(N, \widehat{\Upsilon})$

1: **while** $\exists t_u \in T_u$, $\exists \widetilde{\mathbf{m}}^i \in \min_{\precsim}(\widehat{\Upsilon})$ such that $(\max_{\precsim}\{\mathbf{IN}_{t_u}, \widetilde{\mathbf{m}}^i\} + \mathbf{C} \times \mathbf{1}_{t_u}) \notin \widehat{\Upsilon}$ **do**
2: Replace $\widetilde{\mathbf{m}}^i$ by a set of $k-1$ vectors $\{\widehat{\mathbf{m}}^l\}_{l=1}^{k-1}$ where for each $j \in \{1, 2, \ldots, k\} - \{i\}$, create a new marking $\widehat{\mathbf{m}}^l$, given by the expression $\widehat{\mathbf{m}}^l = \lceil (\widetilde{\mathbf{m}}^i + \max\{\mathbf{0}, \widetilde{\mathbf{m}}^j - (\max\{\mathbf{IN} \times \mathbf{1}_{t_u}, \widetilde{\mathbf{m}}^i\} + \mathbf{C} \times \mathbf{1}_{t_u})\}) \rceil_{\precsim}$, where we use $\lceil \mathbf{m} \rceil_{\precsim}$ to denote the smallest marking such that $\mathbf{m} \precsim \lceil \mathbf{m} \rceil_{\precsim}$.
3: Replace the resulting set of $\{\widetilde{\mathbf{m}}^i\}_i$ vectors by their minimal elements with respect to $\precsim$, and modify the value of k to equal the size of the minimal set of vectors. $\widehat{\Upsilon}$ is the right-closed set with respect to $\precsim$ identified by this minimal set of vectors.
4: **end while**

We discuss the algorithm using the example PN N_1. Since $\Delta_C(N, \precsim)$ is right-closed with respect to $\precsim$, its minimal elements completely describe the set. For finding the minimal

Algorithm 8 BUMPUPFORPATHREQUIREMENT$(N, \widehat{\Upsilon})$

1: **for** $\widetilde{\mathbf{m}}^i \in \min_{\precsim}(\widehat{\Upsilon})$ where $G(N(\widetilde{\mathbf{m}}^i), \widetilde{\mathcal{P}}_{\widehat{\Upsilon}})$ does not have the path **do**

2: Define a right-closed set $\overline{\Upsilon}$, where $\min(\overline{\Upsilon}) = (\min(\widehat{\Upsilon}) - \{\widetilde{\mathbf{m}}^i\}) \cup \{\widetilde{\mathbf{m}}^i + \omega_k^j \times \mathbf{1}_k | j \in \{1, 2, \ldots, n\}, k \in \{0, 1, 2, \ldots, k_j - 1\}\}$, where $\mathbf{1}_k$ the unit-vector where the k-th component is unity.

3: Replace $\widetilde{\mathbf{m}}^i$ by the set:

$$\{\lceil \widetilde{\mathbf{m}}^i \rceil(k) | k \in \{1, 2, \ldots, n\}, G(N(\widetilde{\mathbf{m}}^i + \omega_k^j \times \mathbf{1}_j), \widetilde{\mathcal{P}}_{\overline{\Upsilon}}) \text{ satisfies the path requirement}\} \tag{4.7}$$

4: **end for**

5: Replace the resulting set of $\{\widetilde{\mathbf{m}}^i\}_i$ vectors by their minimal elements with respect to $\precsim$, and modify the value of k to equal the size of the minimal set of vectors. $\widehat{\Upsilon}$ is the right-closed set with respect to $\precsim$ identified by this minimal set of vectors.

elements we start with the initial estimate of $\mathcal{N}^n$ and remove elements that do not satisfy the conditions related to the existence of a CM-LESP.

The initial estimate $\widehat{\Upsilon}_0 = \mathcal{N}^n$ with minimal elements $\min_{\precsim}(\widehat{\Upsilon}_0) = \{(0,0), (0,1), (0,2)\}$ is control invariant with respect to $(N, \precsim)$. It is easy to see that the minimal element $(0,0)$ does not satisfy the path requirement on the GCG. As a consequence, we replace the minimal element $(0,0)$ with $\{(1,0), (1,1), (1,2)\}$ to obtain the new estimate $\widehat{\Upsilon}_1$, where $\min_{\precsim}(\widehat{\Upsilon}_1) = \min_{\precsim} \{(1,0), (1,1), (1,2), (0,1), (0,2)\} = \{(1,0), (0,1), (0,2)\}$. The set of markings $\widehat{\Upsilon}_1$ is control invariant with respect to $(N, \precsim)$. That is, the firing of any uncontrollable transition form any marking in $\widehat{\Upsilon}_1$ results in a marking that is also in $\widehat{\Upsilon}_1$. This can be seen by noting that the firing of $t_2 \in T_u$ from any marking $\mathbf{m}$, where $(1,0) \precsim \mathbf{m}$, results in the marking $\widehat{\mathbf{m}} \in \Upsilon_1$, as

$$\left(\underbrace{\max_{\precsim}\{(1,0), \mathbf{IN}_{t_2}\}}_{(1,3)} + \mathbf{C}_{t_2} = (3,2) \right) \precsim \widehat{\mathbf{m}}.$$

Similarly, if $(0,1) \precsim \mathbf{m}$, the firing of $t_2 \in T_u$ at marking $\mathbf{m}$ results in a marking $\widehat{\mathbf{m}} \in \Upsilon_1$, as $(\max_{\precsim}\{(0,1), \mathbf{IN}_{t_2}\} + \mathbf{C}_{t_2} = (2,0)) \precsim \widehat{\mathbf{m}}$; and if $(0,2) \precsim \mathbf{m}$, the firing of $t_2 \in T_u$ at marking $\mathbf{m}$ results in a marking $\widehat{\mathbf{m}} \in \Upsilon_1$, as $(\max_{\precsim}\{(0,2), \mathbf{IN}_{t_2}\} + \mathbf{C}_{t_2} = (2,0)) \precsim \widehat{\mathbf{m}}$.

Suppose $t_3 \in T_u$ fires from $\mathbf{m} \in \Upsilon_1$ resulting in the marking $\widehat{\mathbf{m}}$. If $(1,0) \precsim \mathbf{m}$, since $\max_{\precsim}\{(1,0), \mathbf{IN}_{t_3}\} + \mathbf{C}_{t_3} = (1,0) \precsim \widehat{\mathbf{m}}$, and $\widehat{\mathbf{m}} \in \Upsilon_1$. Likewise, if $(0,1) \precsim \mathbf{m}$ (resp. $(0,2) \precsim \mathbf{m}$), since $\max_{\precsim}\{(0,1), \mathbf{IN}_{t_3}\} + \mathbf{C}_{t_3} = (0,1) \precsim \widehat{\mathbf{m}}$ (resp. $\max_{\precsim}\{(0,2), \mathbf{IN}_{t_3}\} + \mathbf{C}_{t_3} = (0,2) \precsim \widehat{\mathbf{m}}$), and $\widehat{\mathbf{m}} \in \Upsilon_1$.

The GCG under the class-monotone policy $\mathcal{P}_{\widehat{\Upsilon}_1}$ (which ensures the reachable markings

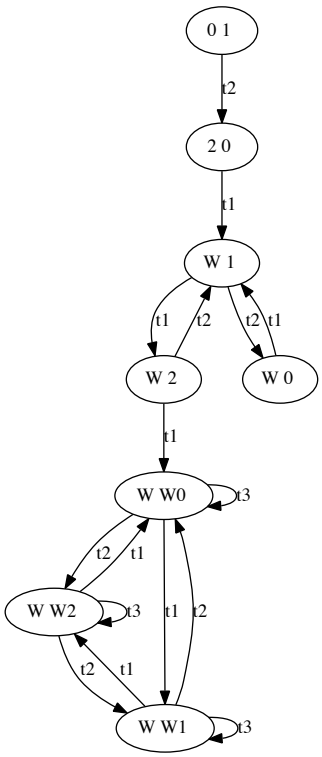


Figure 4.3: Generalized Coverability Graph for N_1, where $\zeta_0^1 = \mathcal{N}$ is used for place p_1; and $\zeta_i^2 = \{n \in \mathcal{N} \mid n(mod3) = i\}$, and $\omega_i = \lim_n \zeta_i$, for $i \in \{0, 1, 2\}$ is used for place p_2.

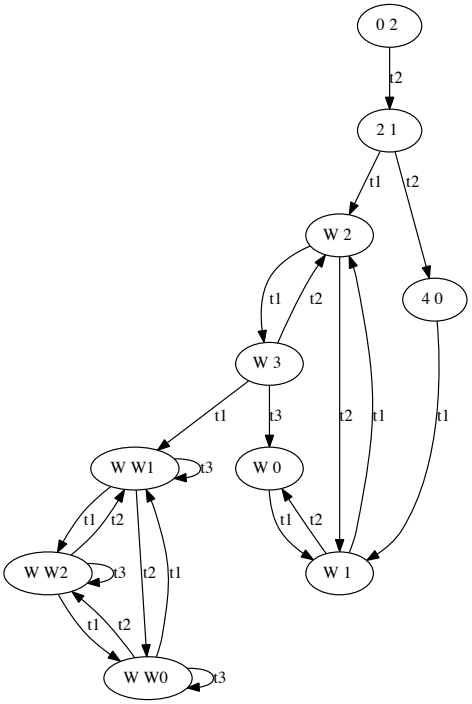


Figure 4.4: Generalized Coverability Graph for N_1, where $\zeta_0^1 = \mathcal{N}$ is used for place p_1; and $\zeta_i^2 = \{n \in \mathcal{N} \mid n(mod3) = i\}$, and $\omega_i = \lim_n \zeta_i$, for $i \in \{0, 1, 2\}$ is used for place p_2.

never leave $\widehat{\Upsilon}_1$) with initial-marking $(1, 0)$, $(0, 1)$ and $(0, 2)$ are identical to the GCG's shown in Figures 4.2, 4.3 and 4.4 respectively. Each of the GCG's under supervision satisfy the path-requirement. That is, they all have a closed-path $(\omega, \omega_0) \xrightarrow{(t_1 t_2 t_1)^3 t_3} (\omega, \omega_0)$. That is, all transitions appear at least once in this closed-path, and the net-change in token-load of all places is non-negative. Therefore, the class-monotone policy $\mathcal{P}_{\widehat{\Upsilon}_1}$ is a CM-LESP; from the construction procedure we also know that $\min(\Delta_c(N, \precsim)) = \{(1, 0), (0, 1), (0, 2)\}$. In the standard algebra, this set is defined as follows: if there are $0(mod)3$ tokens in p_2, then there must be at least one token in p_1 for an (CM-)LESP to exist for $N(\mathbf{m}^0)$.

CHAPTER 5

A GENERAL FRAMEWORK FOR LIVENESS ENFORCING SUPERVISORY POLICIES FOR DISCRETE EVENT SYSTEMS

In this chapter, we first present results for existence of a B-LESP in the framework of Figure 5.1 for a general model of DES as discussed in Chapter 1. Then we consider specific cases of uncertainties (partial observability in the forward path, and controllability faults in the feedback path) in PN models of DES. We prove that the existence of an LESP for arbitrary PN in the presence of these uncertainties is undecidable even if an LESP for a uncertainty-free case is known. We then present decidable instances of this problem.

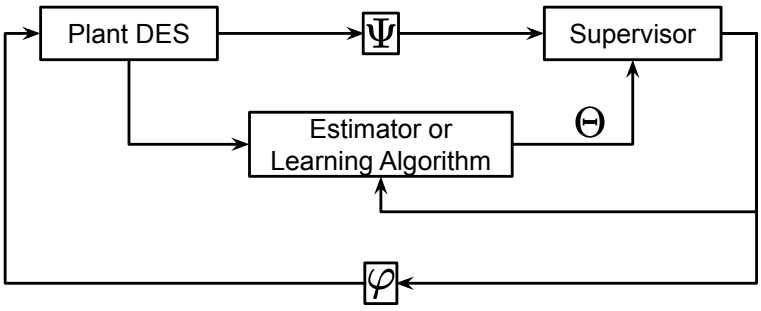


Figure 5.1: Supervisory Control Framework

Let the plant DES be $\mathcal{D} = (S, \Sigma, \delta)$ and consider some other DES $\mathcal{D}' = (S', \Sigma', \delta')$. We introduce the function $\Psi : S \to S'$ that transforms the states of DES $\mathcal{D}$ to the states of DES $\mathcal{D}'$ to model scenarios when the supervisor does not receive precise information about the state of the DES. Ψ is identity if the supervisor receives precise state information.

The first natural step in synthesizing a B-LESP in the presence of Ψ is to find the possible actual state(s) of the DES $\mathcal{D}$ given a received-state of $\mathcal{D}'$. Let $s \in S'$ be a state received by the supervisor and let $[s]_\Psi \subseteq S$ denote the set of states corresponding to $s \in S$ which *project* to the same state $\Psi(s)$. That is:

$$[s]_\Psi = \{\widehat{s} \in S : \Psi(s) = \Psi(\widehat{s})\} \tag{5.1}$$

$[s]_\Psi$ can also be characterized as the inverse of operator Ψ. For a state $s \in S$ such that

$\Psi(s) = \widetilde{s}$, we have:

$$\Psi^{-1}(\widetilde{s}) = \{\widehat{s} \in S : \ \Psi(\widehat{s}) = \widetilde{s}\} \tag{5.2}$$

Invariably, whenever there is uncertainty, a natural thing to do is to bring in the analysis of estimation or learning of parameters of the system in order to mitigate its effects. A detailed analysis in this direction, which can also include estimation of transition function, δ, of $\mathcal{D}$ among other things, is out of the scope of this thesis, but we do include a simplified interpretation. We assume that the supervisor receives a fixed set $\Theta \subseteq S$ as the set of *ground states* or the *set of feasible actual states* from an estimator as supplemental information in order to counter the effect of Ψ in the forward path. Consequently, the set of actual states that we evaluate using the Ψ^{-1} operator can be narrowed down to $\Psi^{-1} \cap \Theta$. We would denote the system consisting of the DES $\mathcal{D}$ along with Ψ and Θ by the three tuple $(\mathcal{D}(s_0), \Psi, \Theta)$.

The operator Ψ models scenarios in which the supervisor may not receive precise state information. We introduce the operator $\varphi : \{0,1\}^{card(\Sigma_c)} \rightarrow \{0,1\}^{card(\Sigma_c)}$, that acts on the supervisory action and modifies it, to model faults in the feedback channel. Here $card(\cdot)$ denotes the cardinality of the set argument. As a consequence, the policy actually supervising the DES can be different to the one prescribed by the supervisor. We would denote the system composed of the DES $\mathcal{D}$ along with Ψ, Θ and φ by the four tuple $(\mathcal{D}(s_0), \Psi, \Theta, \varphi)$. We discuss the operator φ in detail in Section 5.2.

5.1 B-LESPs for $(\mathcal{D}, \Psi, \Theta)$

The initial step in a brute-force approach for the synthesis of a B-LESP for $(\mathcal{D}(s_0), \Psi, \Theta)$ is to synthesize a B-LESP assuming precise state information (that is, Ψ is identity and $\Theta = S$). The supervisor takes an appropriate supervisory action by evaluating all possible actual states of the DES $\mathcal{D}$ corresponding to the received state s'. We define a supervisory policy for $(\mathcal{D}, \Psi, \Theta)$ as: $\mathcal{P}_{\Psi,\Theta} : S' \times \Sigma \rightarrow \{0,1\}$. Given a received state, we introduce a notion of equivalence of supervisory action among the possible actual states of the DES in the next definition.

Definition 9. *A supervisory policy $\mathcal{P}_{\Psi,\Theta} : S' \times \Sigma \rightarrow \{0,1\}$ is Ψ-invariant with respect to a supervisory policy $\mathcal{P} : S \times \Sigma \rightarrow \{0,1\}$ if $\forall e \in \Sigma$:*

$$(\mathcal{P}_{\Psi,\Theta}(s', e) = 1) \Rightarrow (\bigwedge_{s \in \Psi^{-1}(s') \cap \Theta} \mathcal{P}(s, e) = 1))$$

That is, $\mathcal{P}_{\Psi,\Theta}$ is Ψ-invariant with respect to $\mathcal{P}$ if $\mathcal{P}_{\Psi,\Theta}$ enables an event e at a state s' only if $\mathcal{P}$ enables e at all states $s \in [s']_\Psi \cap \Theta$. A straightforward observation from the definition is:

Observation 11. *Let $\mathcal{P}_{\Psi,\Theta_1}$ and $\mathcal{P}_{\Psi,\Theta_2}$ be two supervisory policies that are Ψ-invariant with respect to a supervisory policy $\mathcal{P}$. Then $(\Theta_1 \subseteq \Theta_2) \Leftrightarrow (\mathcal{P}_{\Psi,\Theta_1}(s,e) \geq \mathcal{P}_{\Psi,\Theta_2}(s,e))$.*

Let $\mathbf{I}$ denote the identity function. The case when the supervisor has precise information about the state of the DES can be represented as $\Psi = \mathbf{I}$ and $\Theta = S$. Then we can define $\mathcal{P}_{\Psi,\Theta}$ as follows. $\forall e \in \Sigma$:

$$(\mathcal{P}_{\Psi,\Theta}(s',e) = 1) \Leftrightarrow (\bigwedge_{s \in \Psi^{-1}(s') \cap \Theta} \mathcal{P}_{\mathbf{I},S}(s,e) = 1) \tag{5.3}$$

The motivation for defining $\mathcal{P}_{\Psi,\Theta}$ as in Equation 5.3 is very simple. Recall that $\Delta(\mathcal{D})$ is the set of initial states for which a B-LESP exists. Suppose $s_0 \in \Delta(\mathcal{D})$ and that $\mathcal{P}_{\mathbf{I},S}$ is of the form given in Definition 5. That is, it permits an event e if and only if its occurrence does not take the state of the DES $\mathcal{D}$ outside the set $\Delta(\mathcal{D})$. Then, what the definition of $\mathcal{P}_{\Psi,\Theta}$ above is saying is that $\mathcal{P}_{\Psi,\Theta}$ will permit e at a received state $s' \in S'$ only if all possible actual states of DES $\mathcal{D}$ are such that permitting event e will not take the DES $\mathcal{D}$ outside $\Delta(\mathcal{D})$. On the other hand, even if there is one possible actual state of $\mathcal{D}$, for which the received state is s', and for which the occurrence of e will take the DES state outside $\Delta(\mathcal{D})$, then $\mathcal{P}_{\Psi,\Theta}$ would disable e. We state the following lemma to formalize this discussion:

Lemma 5. *Let $\mathcal{P}_{\mathbf{I},S}$ be a B-LESP such that $\forall e \in \Sigma, \forall s_1 \in S$: $(\mathcal{P}_{\mathbf{I},S}(s_1,e) = 1) \Leftrightarrow ((s_1 \xrightarrow{e} s_2) \wedge (s_2 \in \Delta(\mathcal{D})))$. If $\mathcal{P}_{\Psi,\Theta}$ is a B-LESP for $(\mathcal{D},\Psi,\Theta)$, then $\mathcal{P}_{\Psi,\Theta}$ is Ψ-invariant with respect to $\mathcal{P}_{\mathbf{I},S}$.*

Proof. Suppose for contradiction that $\mathcal{P}_{\Psi,\Theta}$ is a B-LESP for $(\mathcal{D},\Psi,\Theta)$ but it is not Ψ-invariant with respect to $\mathcal{P}_{\mathbf{I},S}$. Then there exists a state s' for which $\mathcal{P}_{\Psi,\Theta}(s',e) = 1$, and there exists a state $s \in \Psi^{-1}(s') \cap \Theta$ such that $\mathcal{P}_{\mathbf{I},S}(s,e) = 0$. Now since $\mathcal{P}_{\mathbf{I},S}$ is the maximally permissive B-LESP (Lemma 1), there is no other B-LESP $\widehat{\mathcal{P}}$ such that $\widehat{\mathcal{P}}(s,e) = 1$. Consequently, if the actual state of the DES $\mathcal{D}$ is $s \in \Psi^{-1}(s') \cap \Theta$, then permitting e at a received state s' will take the state of $\mathcal{D}$ outside $\Delta(\mathcal{D})$, and $\mathcal{P}_{\Psi,\Theta}$ is not a B-LESP, which is a contradiction. □

Next, we intend to define a $\Delta(\mathcal{D})$-like set that describes the set of initial states of $\mathcal{D}$ for which a B-LESP exists for $(\mathcal{D},\Psi,\Theta)$. Let us denote that set by $\Delta(\mathcal{D},\Psi,\Theta)$.

$$\Delta(\mathcal{D},\Psi,\Theta) = \{s_0 \in S : \exists \text{ a B-LESP for } (\mathcal{D},\Psi,\Theta)\} \tag{5.4}$$

Obviously $\Delta(\mathcal{D}, \Psi, \Theta) \subseteq \Delta(\mathcal{D})$. Since we are looking to enforce liveness with respect to B, the set $\Delta(\mathcal{D}, \Psi, \Theta)$ must possess properties similar to $\Delta(\mathcal{D})$. The discussion of the property of Ψ-invariance and Lemma 5 gives hints on the additional properties that $\Delta(\mathcal{D}, \Psi, \Theta)$ should possess. We introduce the set $\xi(\mathcal{D}, e) \subseteq \Delta(\mathcal{D})$ as the set of states from which the occurrence of event e keeps the DES state in $\Delta(\mathcal{D})$.

$$\xi(\mathcal{D}, e) = \{s \in \Delta(\mathcal{D}) : \delta(e, s) \in \Delta(\mathcal{D})\} \tag{5.5}$$

In other words, $\xi(\mathcal{D}, e)$ is the set of states of $\mathcal{D}$ for which the the policy $\mathcal{P}_{\mathbf{I},S}(s, e)$ as defined in Lemma 5 would enable the event e. Note that $\xi(\mathcal{D}, e) = S,\ \forall e \in \Sigma_u$. As seen in Lemma 5, any B-LESP for $(\mathcal{D}, \Psi, \Theta)$ disables an event e at a received state s' if $\Psi^{-1}(s') \cap \Theta \nsubseteq \xi(\mathcal{D}, e)$. Now, if we have to characterize the set of states, $\Delta(\mathcal{D}, \Psi, \Theta)$, for which a B-LESP exists for $(\mathcal{D}, \Psi, \Theta)$, then the maximally permissive B-LESP for $(\mathcal{D}(s_0), \Psi, \Theta)$, where $s_0 \in \Delta(\mathcal{D}, \Psi, \Theta)$, should enable every event whose occurrence does not take the DES state outside $\Delta(\mathcal{D}, \Psi, \Theta)$. Consequently, if an event e from state $s \in \Delta(\mathcal{D}, \Psi, \Theta)$ results in a state $\widetilde{s} \in \Delta(\mathcal{D}, \Psi, \Theta)$, then $([s]_\Psi \cap \Theta) \subseteq \xi(\mathcal{D}, e)$. This is the main idea in the next definition. Recall that σ_i denotes the first i elements of a valid sequence of states σ.

Definition 10. *For a DES $\mathcal{D} = (S, \Sigma, \delta)$, $\Delta(\mathcal{D}, \Psi, \Theta) \subseteq S$ is the set of initial states with the following properties:*

1. *$\forall s \in \Delta(\mathcal{D}, \Psi, \Theta)$, $\forall \alpha \in S^*(s), \exists \beta \in S^\omega$ such that:*
   - *(a) $\alpha\beta \vDash B$*
   - *(b) $\forall i$ such that $(\alpha\beta)_i\widehat{s} = (\alpha\beta)_{i+1}$: $\widehat{s} \in \Delta(\mathcal{D}, \Psi, \Theta)$*
2. *$\forall s \in \Delta(\mathcal{D}, \Psi, \Theta)$, $\forall e \in \Sigma$: $(\delta(e, s) = \widetilde{s}$ and $\widetilde{s} \in \Delta(\mathcal{D}, \Psi, \Theta)) \Rightarrow (([s]_\Psi \cap \Theta) \subseteq \xi(\mathcal{D}, e))$.*
3. *It is control invariant. That is, $\forall s_1 \in \Delta(\mathcal{D}, \Psi, \Theta), e_u \in \Sigma_e(s_1) \cap \Sigma_u$ and $s_1 \xrightarrow{e_u} s_2$, then $s_2 \in \Delta(\mathcal{D}, \Psi, \Theta)$.*

Theorem 11. *($\exists$ a B-LESP for $(\mathcal{D}(s_0), \Psi, \Theta)$) $\Leftrightarrow$ ($s_0 \in \Delta(\mathcal{D}, \Psi, \Theta)$).*

Proof. ($\Leftarrow$) From property 2, every event from a state in $\Delta(\mathcal{D}, \Psi, \Theta)$ that results in a state in $\Delta(\mathcal{D}, \Psi, \Theta)$ will be permitted by the supervisory policy $\mathcal{P}_{\Psi,\Theta}$ as defined in Equation 5.3. From 1a, 1b and 3, if $s_0 \in \Delta(\mathcal{D}, \Psi, \Theta)$ then $\mathcal{P}_{\Psi,\Theta}$ is a B-LESP for $(\mathcal{D}(s_0), \Psi, \Theta)$.
($\Rightarrow$) If $\exists$ a B-LESP $\overline{P}_{\Psi,\Theta}$ for $(\mathcal{D}(s_0), \Psi, \Theta)$, then by Lemma 5, it is Ψ-invariant with respect to $\mathcal{P}_{\mathbf{I},S}$ as defined in the lemma. This implies that it will permit a controllable event at s' only if its occurrence from all $s \in \Psi^{-1}(s') \cap \Theta$ does not take the state outside $\Delta(\mathcal{D})$. That is, only

if $\Psi^{-1}(s') \cap \Theta \subseteq \xi(\mathcal{D}, e)$. Every state reached under every evolution under the supervision of $\overline{P}_{\Psi,\Theta}$ should satisfy this property. Therefore, Item 2 is a necessary condition. That Items 1a, 1b, 3 of Definition 10 are true for every evolution under the supervision of $\overline{P}_{\Psi,\Theta}$ follows from the fact that it is a B-LESP. Therefore, every state of every evolution under the supervision of $\overline{P}_{\Psi,\Theta}$ is in $\Delta(\mathcal{D}, \Psi, \Theta)$ and $s_0 \in \Delta(\mathcal{D}, \Psi, \Theta)$. Indeed, $\overline{P}_{\Psi,\Theta} = P_{\Psi,\Theta}$. □

Next, we build on this result to include the effect of φ.

5.2 B-LESPs for $(\mathcal{D}, \Psi, \Theta, \varphi)$

We noted that the operator φ can modify the sequence of supervisory action taken by the supervisor. That is, the policy actually supervising the DES can be different than the one prescribed by the supervisor. Intuitively, for an event e at a state s, φ can change the supervisory action from 1 (enable) to a 0 (resp. disable) or vice versa. That is, φ models a bit-flip operation. If φ is such that it can change infinitely-many control actions, then φ can, in some cases, ensure that property B is not satisfied for any evolution. Let us denote the property not-B by $\overline{B}$.

Theorem 12. *Suppose φ is such that it can flip infinitely many supervisory actions. Then there does not exist a B-LESP for $(\mathcal{D}, \Psi, \Theta, \varphi)$ if there exists a $\overline{B}$-LESP for $(\mathcal{D}, \Psi, \Theta)$.*

Proof. Suppose there exists a $\overline{B}$-LESP $\overline{P}_{\Psi,\Theta}$ for $(\mathcal{D}, \Psi, \Theta)$ for an initial state s_0. Then φ can mimic the supervisory action of $\overline{P}_{\Psi,\Theta}$ at each state to ensure that property B is never satisfied. Therefore, there does not exist a B-LESP for $(\mathcal{D}, \Psi, \Theta, \varphi)$. □

The non-existence of a $\overline{B}$-LESP means that it is not possible to enforce not-B by steering the controllable events. It is possible that there does not exist a $\overline{B}$-LESP but there still does not exist a B-LESP for $(\mathcal{D}, \Psi, \Theta)$. In that case, the existence and non-existence will be dependent on the uncontrollable events.

In this thesis, we pay attention to the case when φ can change finitely-many control actions. The minimally restrictive B-LESP permits an event if its occurrence will keep the DES in $\Delta(\mathcal{D}, \Psi, \Theta)$. Therefore, even if φ disables an event that was enabled by the supervisor, the state will still be in $\Delta(\mathcal{D}, \Psi, \Theta)$ and liveness can be enforced. The interesting case is when φ enables an event that was disabled by the supervisor. Then the occurrence of that event can take the DES state outside $\Delta(\mathcal{D}, \Psi, \Theta)$ resulting in loss of liveness. In this thesis, informally speaking, we work with the case when φ non-deterministically modifies a finite number of 0s to 1s. For ease of exposition, we model the effect of φ as an extraneous fault-event that

renders a subset of controllable events temporarily uncontrollable. As a result of the fault-event, the subset of controllable events affected by it can occur even when disabled by the supervisor. The interpretation is valid from an application point of view also, as this could happen due to a device- or line-fault, where communication between supervisor and plant is temporarily unavailable; or due to the activity of a malicious-user.

5.2.1 Motivation and Faults Semantics using a Petri Net Example

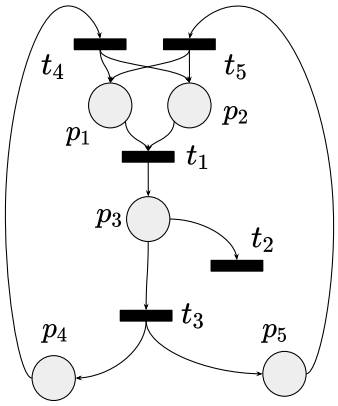


Figure 5.2: Petri Net N_i

Consider the fully controllable PN N_i shown in Figure 5.2. $\Delta(N_i)$ is right-closed with minimal elements $\{(1\ 1\ 0\ 0\ 0)^T, (0\ 0\ 1\ 0\ 0)^T, (0\ 0\ 0\ 1\ 0)^T, (0\ 0\ 0\ 0\ 1)^T\}$. Suppose an extraneous fault-event occurs at $(0\ 0\ 1\ 0\ 0)^T \in \Delta(N_i)$ that renders transition t_2 (temporarily) uncontrollable. That is, the supervisory policy cannot prevent it from firing. Then the affected transition t_2 can fire at $(0\ 0\ 1\ 0\ 0)^T$ and the resulting marking is not in $\Delta(N_i)$. The objective of this section is to analyse the existence and synthesis of LESPs tolerant to such *controllability failures*.

Formally, we use the term *fault-event*, denoted by ϕ, to refer to an extraneous discrete-event where an arbitrary subset of controllable transitions, $T_f \subseteq T_c$, becomes temporarily uncontrollable. The fault-event ϕ is followed (not necessarily immediately) by an extraneous *rectification-event*, denoted by ρ, where all transitions in $T_f \subseteq T_c$ become controllable again. That is, between the fault- and the rectification-event, the set of uncontrollable (resp. controllable) events is effectively $T_f \cup T_u$ (resp. $T_c - T_f$). Before the fault-event, and after the rectification-event, the set of uncontrollable (resp. controllable) events is T_u (resp. T_c).

Coming back to the PN in figure 5.2, we observed that the firing of t_2 from $(0\ 0\ 1\ 0\ 0)^T$ resulted in a marking that is not in $\Delta(N_i)$. An obvious way of making the PN tolerant to

fault is to constrain the marking of the PN to a subset of $\Delta(N_i)$ so that when a transition affected by fault does fire, the resulting marking is still inside $\Delta(N_i)$. In addition, that subset of $\Delta(N_i)$ should also satisfy the properties of $\Delta(N_i)$ so that the supervisory policy that constrains the marking to it enforces liveness. Consider the right-closed set $\widehat{\Delta}(N_i) \subseteq \Delta(N_i)$ with minimal elements $\{(2\ 2\ 0\ 0\ 0)^T, (0\ 0\ 2\ 0\ 0)^T, (0\ 0\ 0\ 2\ 0)^T, (0\ 0\ 0\ 0\ 2)^T, (1\ 1\ 1\ 0\ 0)^T, (1\ 1\ 0\ 1\ 0)^T, (1\ 1\ 0\ 0\ 1)^T, (0\ 0\ 1\ 1\ 0)^T, (0\ 0\ 1\ 0\ 1)^T, (0\ 0\ 0\ 1\ 1)^T\}$. Consider the policy $\widehat{\mathcal{P}}$ defined such that for any controllable transition $t_c \in T_c$ at any marking $\mathbf{m}_1 \in \widehat{\Delta}(N_i)$: $(\widehat{\mathcal{P}}(\mathbf{m}_1, t_c) = 0) \Leftrightarrow ((\mathbf{m}_1 \xrightarrow{t_c} \mathbf{m}_2) \wedge (\mathbf{m}_2 \notin \widehat{\Delta}(N_i)))$. $\widehat{\mathcal{P}}$ is an LESP for $N_i(\mathbf{m}_0)$ for any $\mathbf{m}_0 \in \widehat{\Delta}(N_i)$. It follows that, $\widehat{\mathcal{P}}(\mathbf{m}_0, t_2) = 0$ for $\mathbf{m}_0 = (0\ 0\ 2\ 0\ 0)^T$; and $\forall \mathbf{m} \in \widehat{\Delta}(N_i), \widehat{\mathcal{P}}(\mathbf{m}, t_4) = 1$ (cf. [64] for details).

We illustrate the detection semantics next. Suppose $\Psi = \mathbf{I}$ and that the fault-event ϕ occurs at $\mathbf{m}_0$, rendering the transition in the set $T_f = \{t_4\}$ to be uncontrollable. A fault-event can be detected if a controllable transition that was disabled by the LESP fired. But since the LESP $\widehat{\mathcal{P}}$ does not disable the transition t_4 for any marking in $\widehat{\Delta}(N_i)$, this fault will not be detected. In contrast, let $T_f = \{t_2, t_4\}$, and suppose $(0\ 0\ 2\ 0\ 0)^T \xrightarrow{\phi t_2} (0\ 0\ 1\ 0\ 0)^T$ under the supervision of $\widehat{\mathcal{P}}$. If the supervisor stores information about its past actions, then the fault can be detected by comparing the transition that fired to those that were enabled by the supervisor. However, we do not assume that the supervisor stores information about its past actions and consider a general setting in which the fault-event has to be inferred from *only* the current marking of the PN. For this example, the firing of a transition affected by the fault can be detected by observing that the current marking $(0\ 0\ 1\ 0\ 0)^T$ no longer belongs to $\widehat{\Delta}(N_i)$.

Due to cost considerations, a fault may not be rectified immediately after detection. We quantify the tolerance of $N(\mathbf{m}_0)$ to a fault-event by associating a positive integer k_r with it; where k_r is the mandatory number of detected firings of transitions that are affected by the fault before it is rectified. Under these semantics, the fault-free scenario is represented as the case when $k_r = 0$.

Continuing with the example for the case when $T_f = \{t_2, t_4\}$, if $k_r = 1$ then the fault *will* be rectified *immediately* at the marking $(0\ 0\ 1\ 0\ 0)^T$, $(0\ 0\ 2\ 0\ 0)^T \xrightarrow{\phi t_2 \rho} (0\ 0\ 1\ 0\ 0)^T$, and all transitions in T_c will be controllable afterwards. No other transition in N_i can fire at the marking $(0\ 0\ 1\ 0\ 0)^T$ before the occurrence of the rectification-event ρ. If $k_r > 1$, the rectification-event cannot occur at marking $(0\ 0\ 1\ 0\ 0)^T$, and $(0\ 0\ 2\ 0\ 0)^T \xrightarrow{\phi t_2 t_2} (0\ 0\ 0\ 0\ 0)^T$ under the supervision of $\widehat{\mathcal{P}}$. Thus, we can conclude that for $N_i(\mathbf{m}_0)$ where $\mathbf{m}_0 \in \widehat{\Delta}(N_i)$, the LESP $\widehat{\mathcal{P}}$ is tolerant to a fault-event if $k_r \leq 1$.

Consider the right-closed set $\widetilde{\Delta}(N_i) \subseteq \Delta(N_i)$ with minimal elements $\{(3\ 3\ 0\ 0\ 0)^T, (0\ 0\ 3\ 0\ 0)^T, (0\ 0\ 0\ 3\ 0)^T, (0\ 0\ 0\ 0\ 3)^T, (2\ 2\ 1\ 0\ 0)^T, (2\ 2\ 0\ 1\ 0)^T, (2\ 2\ 0\ 0\ 1)^T, (1\ 1\ 2\ 0\ 0)^T,$

$(1\ 1\ 0\ 2\ 0)^T$, $(1\ 1\ 0\ 0\ 2)^T$, $(0\ 0\ 2\ 1\ 0)^T$, $(0\ 0\ 2\ 0\ 1)^T$, $(0\ 0\ 1\ 2\ 0)^T$, $(0\ 0\ 1\ 0\ 2)^T$, $(0\ 0\ 0\ 2\ 1)^T$, $(0\ 0\ 0\ 1\ 2)^T$, $(1\ 1\ 1\ 1\ 0)^T$, $(1\ 1\ 1\ 0\ 1)^T$, $(1\ 1\ 1\ 1\ 0)^T$, $(1\ 1\ 0\ 1\ 1)^T$, $(1\ 1\ 1\ 0\ 1)^T$, $(1\ 1\ 0\ 1\ 1)^T$, $(0\ 0\ 1\ 1\ 1)^T$ }. It follows that $\widetilde{\Delta}(N_i) \subset \widehat{\Delta}(N_i) \subset \Delta(N_i)$. The policy $\widetilde{\mathcal{P}}$ that ensures all markings, that are reachable under supervision, are within the set $\widetilde{\Delta}(N_i)$ is an LESP for $N(\mathbf{m}_0)$ for any $\mathbf{m}_0 \in \widetilde{\Delta}(N_i)$. Following previous discussion, we can claim that for $N_i(\mathbf{m}_0)$ where $\mathbf{m}_0 \in \widetilde{\Delta}(N_i)$, the LESP $\widetilde{\mathcal{P}}$ is tolerant to a single-fault-event if $k_r \leq 2$.

To summarize the detection method for the example, if the initial marking of N_i is in $\widetilde{\Delta}(N_i)$, then the first firing of a transition affected by the fault will be detected when the current marking is in the set $\widehat{\Delta}(N) - \widetilde{\Delta}(N)$. The second firing of a transition affected by the fault will be detected when the current marking is in $\Delta(N_i) - \widehat{\Delta}(N_i)$. If $k_r = 2$, then the fault will be immediately rectified upon reaching $\Delta(N_i) - \widehat{\Delta}(N_i)$ and the PN can be supervised for liveness as in the fault-free case.

In what follows, we define a sequence of nested sets and use membership to them to detect firings of affected events by using only the current state of the PN. Under the semantics enunciated earlier, the rectification-event ρ occurs *immediately after* the k_r-th firing of affected transitions is detected.

5.2.2 Existence Results for a general DES model

Formally, a supervisory policy for $(\mathcal{D}, \Psi, \Theta, \varphi)$, $\mathcal{P}_{\Psi,\Theta,\varphi} : S' \times \Sigma \to \{0, 1\}$ returns a 0 or 1 for each state and event. It permits the occurrence of an event e at state s, if and only if $\mathcal{P}_{\Psi,\Theta,\varphi}(s', e) = 1$. As per convention, we have $\forall e_u \in \Sigma_u$, $s' \in S'$, $\mathcal{P}_{\Psi,\Theta,\varphi}(s', e_u) = 1$. In what follows, we first develop the theory by ignoring the effect of Ψ, that is by assuming $\Psi = \mathbf{I}$ and $\Theta = S$.

Definition 11. *Let* $\Delta_0(\mathcal{D}, \mathbf{I}, S, \varphi) = \Delta(\mathcal{D}, \mathbf{I}, S)$. *Then* $\Delta_k(\mathcal{D}, \mathbf{I}, S, \varphi) \subseteq \Delta(\mathcal{D}, \mathbf{I}, S)$, $k \in \mathcal{N}^+$, *is the set of all initial states that satisfies the following conditions:*

1. $\forall s \in \Delta_k(\mathcal{D}, \mathbf{I}, S, \varphi)$, $\forall \alpha \in S^*(s), \exists \beta \in S^\omega$ *such that:*
   - *(a)* $\alpha\beta \vDash B$
   - *(b)* $\forall i$ *such that* $(\alpha\beta)_i\widehat{s} = (\alpha\beta)_{i+1}$: $\widehat{s} \in \Delta_k(\mathcal{D}, \mathbf{I}, S, \varphi)$
2. *It is control invariant. That is,* $\forall s_1 \in \Delta_k(\mathcal{D}, \mathbf{I}, S, \varphi), e_u \in \Sigma_e(s_1) \cap \Sigma_u$ *and* $s_1 \xrightarrow{e_u} s_2$, *then* $s_2 \in \Delta_k(\mathcal{D}, \mathbf{I}, S, \varphi)$.
3. $\forall s_1 \in \Delta_k(\mathcal{D}, \mathbf{I}, S, \varphi)$, $\forall e \in \Sigma$: $(s_1 \xrightarrow{e} s_2) \Rightarrow (s_2 \in \Delta_j(\mathcal{D}, \mathbf{I}, S, \varphi))$, *where* $j \geq k - 1$.

Properties 1 and 2 in Definition 11 are the properties of $\Delta(\mathcal{D}, \mathbf{I}, S)$ ($= \Delta(\mathcal{D})$, Definition 4). Property 3 ensures that the state of the DES remains in a set that satisfies the properties of $\Delta(\mathcal{D}, \mathbf{I}, S)$ before and after the detection of occurrence of events affected by faults.

Suppose the number of occurrences of events affected by the fault detected till now is k_d, and the current state $s \in \Delta_{k_r-k_d}(\mathcal{D}, \mathbf{I}, S, \varphi)$. As $\Delta_k(\mathcal{D}, \mathbf{I}, S, \varphi)$ ($k = \{0, \ldots, k_r\}$) is control-invariant, only the occurrence of controllable events can take the state outside $\Delta_{k_r-k_d}(\mathcal{D}, \mathbf{I}, S, \varphi)$. Consider the supervisory policy $\mathcal{P}_f$ where $\forall s \in S$

1. $\forall e \in \Sigma_u$: $\mathcal{P}_f(s, e) = 1$.
2. $\forall e \in \Sigma_c$: $(\mathcal{P}_f(s, e) = 1) \Leftrightarrow (s \xrightarrow{e} \widetilde{s}$ such that $\widetilde{s} \in \Delta_{k_r-k_d}(\mathcal{D}, \mathbf{I}, S, \varphi))$.

Due to Properties 1 and 2 in Definition 11, $\mathcal{P}_f$ is a B-LESP for $(\mathcal{D}, \mathbf{I}, S)$. Since $\mathcal{P}_f$ disables any controllable event that takes the state outside $\Delta_{k_r-k_d}(\mathcal{D}, \mathbf{I}, S, \varphi)$, if the state of the supervised DES does not belong to $\Delta_{k_r-k_d}(\mathcal{D}, \mathbf{I}, S, \varphi)$, then it must be because of the occurrence of a (controllable) event affected by fault. This is the central idea for detection of occurrence of events affected by fault. For every state $\overline{s}$ reached under the supervision of $\mathcal{P}_f$ from $s \in \Delta_{k_r-k_d}(\mathcal{D}, \mathbf{I}, S, \varphi)$, the supervisor first tests if $\overline{s} \in \Delta_{k_r-k_d}(\mathcal{D}, \mathbf{I}, S, \varphi)$. If $\overline{s} \notin \Delta_{k_r-k_d}(\mathcal{D}, \mathbf{I}, S, \varphi)$, then by Property 3 of Definition 11, $\overline{s} \in \Delta_{k_r-k_d-1}(\mathcal{D}, \mathbf{I}, S, \varphi)$. At this point, the supervisor detects the occurrence of an event affected by the fault, updates $k_d \leftarrow k_d+1$, and continues with the same policy as explicated above. That is, it now enforces the set $\Delta_{k_r-k_d-1}(\mathcal{D}, \mathbf{I}, S, \varphi)$. We formalize these observations in the next theorem.

Theorem 13. $(s_0 \in \Delta_{k_r}(\mathcal{D}, \mathbf{I}, S, \varphi)) \Leftrightarrow (\exists$ *a B-LESP for* $(\mathcal{D}, \mathbf{I}, S, \varphi))$.

Proof. ($\Rightarrow$) Assume $s_0 \in \Delta_{k_r}(\mathcal{D}, \mathbf{I}, S, \varphi)$, and the fault-event ϕ renders $\Sigma_f \subseteq \Sigma_c$ to be temporarily uncontrollable when it occurs immediately after some state s reached under the supervision of $\mathcal{P}_f$. It follows that $k_d = 0$ when the the fault-event occurs. If the policy $\mathcal{P}_f$ ensures the state of the supervised DES never leaves $\Delta_{k_r}(\mathcal{D}, \mathbf{I}, S, \varphi)$, then $s \in \Delta_{k_r}(\mathcal{D}, \mathbf{I}, S, \varphi)$, as well. Properties 1 and 2 in Definition 11 imply that $\mathcal{P}_f$ is a B-LESP for $(\mathcal{D}, \mathbf{I}, S)$. We use property 3 to prove robustness against fault. Consider a controllable event $e_c \in \Sigma_e(s)$, and let $s \xrightarrow{\phi e_c} \overline{s}$. There are three possible cases:

1. $e_c \notin \Sigma_f$, that is e_c is not affected by the fault-event. Then e_c will occur if and only if $\mathcal{P}_f(s, e_c) = 1$, and we have $\overline{s} \in \Delta_{k_r}(\mathcal{D}, \mathbf{I}, S, \varphi)$. k_d remains 0.
2. $(e_c \in \Sigma_f) \wedge (\mathcal{P}_f(s, e_c) = 1)$, that is e_c is affected by the fault-event but its firing is as intended by $\mathcal{P}_f$. We have $\overline{s} \in \Delta_{k_r}(\mathcal{D}, \mathbf{I}, S, \varphi)$. k_d remains 0.

3. $(e_c \in \Sigma_f) \wedge (\mathcal{P}_f(s, e_c) = 0)$. Following Property 3, we have $\overline{s} \in \Delta_{k_r-1}(\mathcal{D}, \mathbf{I}, S, \varphi)$ and $k_d = 1$.

That there exists an B-LESP for $(\mathcal{D}, \mathbf{I}, S, \varphi)$ follows by replacing s by $\overline{s}$, and repeating the above argument by induction over k_r-many unintended occurrences of $e_f \in \Sigma_f$ (that is for k_d from 1 to k_r).

($\Leftarrow$) Assume there exists a B-LESP $\mathcal{P}_f$ for $(\mathcal{D}, \mathbf{I}, S, \varphi)$, and the fault-event ϕ renders $\Sigma_f \subseteq \Sigma_c$ to be temporarily uncontrollable when it occurs immediately after some marking that is reached under supervision. Let $s_0 \in S_{k_r}$ for some set S_{k_r}. Now, since $\mathcal{P}_f$ is a B-LESP for $(\mathcal{D}, \mathbf{I}, S, \varphi)$ it is a B-LESP for $(\mathcal{D}, \mathbf{I}, S)$ also. By Theorem 11, S_{k_r} satisfies Properties 1 and 2 in Definition 11. Since $\mathcal{P}_f$ is a B-LESP for $(\mathcal{D}, \mathbf{I}, S, \varphi)$, from all s, every string of states resulting from occurrences of events in which unintended occurrences of events affected by fault: $e_f \in \Sigma_f$ appear less than or equal to k_r-many times should result in a state that is in $\Delta(\mathcal{D}, \mathbf{I}, S)$. Specifically, $\forall s \in S_{k_r}$, $s \xrightarrow{\phi e_f} s_1$. Then $s_1 \in S_{k_r-1}$ for some set S_{k_r-1} such that $\forall s' \in S_{k_r-1}$:

1. every string of states resulting from occurrences of events in which unintended occurrences of events affected by fault: $e_f \in \Sigma_f$ appear less than or equal to $(k_r - 1)$-many times should result in a state that is in $\Delta(\mathcal{D}, \mathbf{I}, S)$; and

2. $(\mathcal{D}, \mathbf{I}, S, \varphi)$ can be made live— for the case when none of the $e_f \in \Sigma_f$ ever fire when $\mathcal{P}_f(s', e_f) = 0$.

Therefore, S_{k_r-1} also satisfies Properties 1 and 2 in Definition 11. The rest of the proof follows by induction by replacing k_r by $(k_r - 1)$ in the above argument. The induction will have k_r steps with the last iteration resulting in a marking in $\Delta(\mathcal{D}, \mathbf{I}, S)$. Therefore, $S_{k_r} \subseteq \Delta_{k_r}(\mathcal{D}, \mathbf{I}, S)$ and $S_{k_r-1} \subseteq \Delta_{k_r-1}(\mathcal{D}, \mathbf{I}, S, \varphi)$. Hence $s_0 \in \Delta_{k_r}(\mathcal{D}, \mathbf{I}, S, \varphi)$. □

Theorem 13 presented the necessary and sufficient condition for the existence of a B-LESP for $(\mathcal{D}, \mathbf{I}, S, \varphi)$. The B-LESP $\mathcal{P}_f$ first tests if a received state $s \in \Delta_{k_r-k_d}(\mathcal{D}, \mathbf{I}, S, \varphi)$ or not. If $s \notin \Delta_{k_r-k_d}(\mathcal{D}, \mathbf{I}, S, \varphi)$, then by Property 3 of Definition 11, $s \in \Delta_{k_r-k_d-1}(\mathcal{D}, \mathbf{I}, S, \varphi)$. At this point, the supervisor detects the occurrence of an event affected by the fault, updates $k_d \leftarrow k_d + 1$, and continues with the same policy as explicated above. The process becomes tedious in the presence of $\Psi \neq \mathbf{I}$ because the detection method described before cannot be applied in a straightforward manner. Taking a small detour from the framework that we have been considering, let us suppose, for the sake of discussion, that information regarding the occurrence of events of the DES is available to the supervisor (let's say through the learning algorithm) so that detection of occurrence of an event affected by fault is not a

problem. Then we can define the set $\Delta_k(\mathcal{D}, \Psi, \Theta, \varphi)$ as follows. The idea is the same as that in Definition 10 and Definition 11 combined together. Similar to Equation 5.5, we define a set $\xi(\mathcal{D}, \mathbf{I}, S, \varphi)$ as the set of states in $\Delta_k(\mathcal{D}, \mathbf{I}, S, \varphi, e)$ from which the occurrence of an event e results in a state in $\Delta_k(\mathcal{D}, \mathbf{I}, S, \varphi)$.

$$\xi_k(\mathcal{D}, \mathbf{I}, S, \varphi, e) = \{s \in \Delta_k(\mathcal{D}, \mathbf{I}, S, \varphi) : \delta(e, s) \in \Delta_k(\mathcal{D}, \mathbf{I}, S, \varphi)\} \tag{5.6}$$

Definition 12. *Let* $\widehat{\Delta}_0(\mathcal{D}, \Psi, \Theta, \varphi) = \Delta(\mathcal{D}, \Psi, \Theta)$. *Then* $\widehat{\Delta}_k(\mathcal{D}, \Psi, \Theta, \varphi) \subseteq \Delta(\mathcal{D}, \Psi, \Theta)$, $k \in \mathcal{N}^+$, *is the set of all initial states that satisfies the following conditions:*

1. $\forall s \in \widehat{\Delta}_k(\mathcal{D}, \Psi, \Theta, \varphi)$, $\forall \alpha \in S^*(s), \exists \beta \in S^\omega$ *such that:*
   (a) $\alpha\beta \vDash B$
   (b) $\forall i$ *such that* $(\alpha\beta)_i\widehat{s} = (\alpha\beta)_{i+1}$: $\widehat{s} \in \widehat{\Delta}_k(\mathcal{D}, \Psi, \Theta, \varphi)$
2. $\forall s \in \widehat{\Delta}_k(\mathcal{D}, \Psi, \Theta, \varphi)$, $\forall e \in \Sigma$:

$$(\delta(e, s) = \widetilde{s} \text{ and } \widetilde{s} \in \widehat{\Delta}_k(\mathcal{D}, \Psi, \Theta, \varphi)) \Rightarrow (([s]_\Psi \cap \Theta) \subseteq \xi_k(\mathcal{D}, \mathbf{I}, S, \varphi, e))$$

3. *It is control invariant. That is,* $\forall s_1 \in \widehat{\Delta}_k(\mathcal{D}, \Psi, \Theta, \varphi), e_u \in \Sigma_e(s_1) \cap \Sigma_u$ *and* $s_1 \xrightarrow{e_u} s_2$, *then* $s_2 \in \widehat{\Delta}_k(\mathcal{D}, \Psi, \Theta, \varphi)$.
4. $\forall s_1 \in \widehat{\Delta}_k(\mathcal{D}, \Psi, \Theta, \varphi)$, $\forall e \in \Sigma$: $(s_1 \xrightarrow{e} s_2) \Rightarrow (s_2 \in \widehat{\Delta}_j(\mathcal{D}, \Psi, \Theta, \varphi))$, *where* $j \geq k - 1$.

We can define a supervisory policy $\mathcal{P}_{\Psi,\Theta,\varphi}$ that is Ψ-invariant with respect to $\mathcal{P}_f$.

$$(\mathcal{P}_{\Psi,\Theta,\varphi}(s', e) = 1) \Leftrightarrow (\bigwedge_{s \in \Psi^{-1}(s') \cap \Theta} \mathcal{P}_f(s, e) = 1) \tag{5.7}$$

As discussed in Section 5.1, $\mathcal{P}_{\Psi,\Theta,\varphi}$ is a B-LESP for $(\mathcal{D}, \Psi, \Theta, \varphi)$, if information about occurrence of events that enables evaluation of $\mathcal{P}_f$ is available. Suppose the number of unintended occurrences of events affected by faults till now is k_d. If $\Psi \neq \mathbf{I}$, then for a received state s' an important step in this process is to infer if the actual state $s \in \Delta_{k_r - k_d}(\mathcal{D}, \mathbf{I}, S, \varphi)$ or not. This condition is captured in Item 2 of the following theorem.

Theorem 14. $\exists$ *a B-LESP for* $(\mathcal{D}(s_0), \Psi, \Theta, \varphi)$ *if and only if:*

1. $s_0 \in \widehat{\Delta}_{k_r}(\mathcal{D}, \Psi, \Theta, \varphi)$, *and*
2. $\forall i, j \in \{0, 1, \ldots, k_r\}$, $i \neq j$, $\forall s_m \in \widehat{\Delta}_i(\mathcal{D}, \Psi, \Theta, \varphi)$, $\forall s_n \in \widehat{\Delta}_j(\mathcal{D}, \Psi, \Theta, \varphi)$

$$[s_m]_\Psi \cap [s_n]_\Psi = \emptyset \tag{5.8}$$

In this section, we presented necessary and sufficient conditions for the existence of B-LESPs for a general class of problems. In the next section, we consider PN models of DES and present decidable instances of this problem for two cases– partial observability and controllability faults.

Theorems 3.1 and 3.2 in [35] prove that neither the existence nor the nonexistence of an LESP for an arbitrary PN is semidecidable. In light of this theorem, we expect that the existence of an LESP for an arbitrary PN with partial observability and/or controllability faults is also undecidable. We prove a stronger result in the appendix of the thesis where in the the existence of LESPs with partial observability and/or controllability faults is undecidable given $\mathbf{m}_0 \in \Delta(N)$. This result is significant because it proves that the complexity in the synthesis of an LESPs for arbitrary PNs with partial observability and/or controllability faults is not solely inherited from the complexity in the synthesis of an LESP.

5.3 LESPs with Partial State Observability for Petri Nets

Consider a PN $N = (\Pi, T, \Phi, \Gamma)$ with n places. In this section, we consider LESP synthesis for DES modeled by PNs with partial marking information; that is, when token information of only a subset of places $\Pi_0 \subseteq \Pi$ is received by the supervisor. Specifically, $\Psi_{\Pi_0} : \mathcal{N}^n \to \mathcal{N}^{card(\Pi_0)}$. Then $\Psi_{\Pi_0}^{-1}$ will be the set of all non-negative integer-valued n-dimensional vectors that project to the same vector in the $card(\Pi_0)$-dimensional space. We assume $\Theta = \mathcal{N}^n$. A Π_0-LESP $\mathcal{P}_p : \mathcal{N}^{card(\Pi_0)} \times T \to \{0, 1\}$ outputs a 0 or a 1 for each marking $\Psi_{\Pi_0}(\mathbf{m})$ and each transition. A transition t is control-enabled iff $\mathcal{P}_p(\Psi_{\Pi_0}(\mathbf{m}), t) = 1$. The policy does not control-disable any uncontrollable transition. Next we present some straightforward extension of notations defined previously.

$$[\mathbf{m}]_\Psi = \{\widehat{\mathbf{m}} \in \mathcal{N}^n : \Psi_{\Pi_0}(\mathbf{m}) = \Psi_{\Pi_0}(\widehat{\mathbf{m}})\} \tag{5.9}$$

For a marking $\mathbf{m} \in \mathcal{N}^n$ such that $\Psi_{\Pi_0}(\mathbf{m}) = \widetilde{\mathbf{m}}$, we have:

$$\Psi_{\Pi_0}^{-1}(\widetilde{\mathbf{m}}) = \{\widehat{\mathbf{m}} \in \mathcal{N}^n : \ \Psi_{\Pi_0}(\widehat{\mathbf{m}}) = \widetilde{\mathbf{m}}\} \tag{5.10}$$

We define the following set:

$$\Delta(N, \Psi_{\Pi_0}, \mathcal{N}^n) = \{\mathbf{m}^0 \in \mathcal{N}^n : \exists \text{ a } \Pi_0\text{-LESP for } N(\mathbf{m}^0)\} \tag{5.11}$$

and characterize it, from Definition 10 and Theorem 5.1 in [33], as follows:

Definition 13. *For a PN $N = (\Pi, T, \Phi, \Gamma)$, $\Delta(N, \Psi_{\Pi_0}, \mathcal{N}^n)$ is the set of initial markings with the following properties:*

1. $\forall \mathbf{m}_1 \in \Delta(N, \Psi_{\Pi_0}, \mathcal{N}^n), \exists \mathbf{m}_2, \mathbf{m}_3 \in \Delta(N, \Psi_{\Pi_0}, \mathcal{N}^n), \exists$ *a valid firing string* $\sigma = \sigma_1\sigma_2$ *in* N *such that* $\mathbf{m}_1 \xrightarrow{\sigma_1} \mathbf{m}_2 \xrightarrow{\sigma_2} \mathbf{m}_3, \mathbf{m}_3 \geq \mathbf{m}_2$*, all transitions appear at least once in* σ_2*, and* $\forall \sigma_3 \in pr(\sigma_1\sigma_2)$*,* $(\mathbf{m}_1 \xrightarrow{\sigma_3} \mathbf{m}_4) \Rightarrow (\mathbf{m}_4 \in \Delta(N, \Psi_{\Pi_0}, \mathcal{N}^n)$*. Here* $pr(\bullet)$ *denotes the prefix of the string argument.*

2. $\forall \mathbf{m} \in \Delta(N, \Psi_{\Pi_0}, \mathcal{N}^n)$*:* $\mathbf{m} \xrightarrow{t} \widetilde{\mathbf{m}}$ *and* $\widetilde{\mathbf{m}} \in \Delta(N, \Psi_{\Pi_0}, \mathcal{N}^n)) \Rightarrow ((t \in T_u) \vee ([\mathbf{m}]_{\Psi_{\Pi_0}} \cap \mathcal{N}^n) \subseteq \xi(N)))$

3. *It is control invariant.*

Theorem 15. $\exists$ *a* Π_0*-LESP for* $(N(\mathbf{m}^0), \Psi_{\Pi_0}, \mathcal{N}^n)$ *if and only if* $\mathbf{m}^0 \in \Delta(N, \Psi_{\Pi_0}, \mathcal{N}^n)$.

Proof. Special case of Theorem 11. □

Theorem 16. *The existence of a* Π_0*-LESP for* $N(\mathbf{m}^0)$ *such that* $\mathbf{m}^0 \in \Delta(N)$ *and for a given* Π_0 *is undecidable.*

Proof. See Appendix. □

Lemma 6. $\Delta(N)$ *is right-closed for* $N \in \mathcal{H}$*. Let* $N \in \mathcal{H}$*. There exists an LESP for* $(N(\mathbf{m}^0), \Psi_{\Pi_0}, \mathcal{N}^n)$ *if:*

1. $\mathbf{m}^0 \in \Delta(N)$*;*

2. $\forall \widetilde{\mathbf{m}}^i \in \min(\Delta(N))$*:*

$$\widetilde{\mathbf{m}}^i(p) = \begin{cases} \Psi(\widetilde{\mathbf{m}}^i)(p), & \text{if } p \in \Pi_0 \\ 0, & \text{otherwise} \end{cases}$$

Proof. If $\forall \widetilde{\mathbf{m}}^i \in \min(\Delta(N))$: $\widetilde{\mathbf{m}}^i(p) = \Psi(\widetilde{\mathbf{m}}^i)(p)\ \forall p \in \Pi_0$, and 0 otherwise; then the supervisor can determine if a marking $\mathbf{m}_1$ is greater than some $\widetilde{\mathbf{m}}^i$ (in other words, in $\Delta(N)$) or not by observing $\Psi(\mathbf{m}_1)$. Therefore, the minimally restrictive LESP that restricts the PN marking to $\Delta(N)$ can be applied in the presence of Ψ also. □

Theorem 17. *Let* $N \in \mathcal{H}$*. There exists an LESP for* $(N(\mathbf{m}^0), \Psi_{\Pi_0}, \mathcal{N}^n)$ *if and only if* $\exists \mathcal{M} \subseteq \Delta(N)$ *such that:*

1. $\min(\mathcal{M}) \subseteq \min(\Delta(N))$

2. $\forall \widetilde{\mathbf{m}}^i \in \min(\mathcal{M})$:

$$\widetilde{\mathbf{m}}^i(p) = \begin{cases} \Psi(\widetilde{\mathbf{m}}^i)(p), & \text{if } p \in \Pi_0 \\ 0, & \text{otherwise} \end{cases}$$

3. *$\mathcal{M}$ satisfies the conditions of $\widehat{\Delta}(N)$ as given in Theorem 6, which presents the necessary and sufficient condition for the existence of an MM-LESP.*

Proof. (*If*) Follows from Lemma 6, and the observation that a supervisory policy that restricts the markings of the PN to $\mathcal{M}$ is an MM-LESP.
(*Only If*) If there exists an LESP for $(N(\mathbf{m}^0), \Psi_{\Pi_0}, \mathcal{N}^n)$, then every transition enabled by the supervisory policy at a marking $\mathbf{m}$ is either uncontrollable or $\Psi^{-1}(\Psi(\mathbf{m})) \subseteq \xi(N)$ (as defined in Equation 5.5). This is only possible if $\mathbf{m}^0 \in \mathcal{M}$ where $\mathcal{M}$ is a right-closed subset of $\Delta(N)$ that satisfies the conditions of $\widehat{\Delta}(N)$ as given in Theorem 6, and $\forall \widetilde{\mathbf{m}}^i \in \min(\mathcal{M})$: $\widetilde{\mathbf{m}}^i(p) = \Psi(\widetilde{\mathbf{m}}^i)(p)\ \forall p \in \Pi_0$, and 0 otherwise. Every right-closed subset of $\Delta(N)$ has minimal elements greater than or equal to the minimal elements of $\Delta(N)$. Therefore, it is not possible $\min(\mathcal{M}) \not\subseteq \min(\Delta(N))$ but Item 2 is satisfied by $\min(\mathcal{M})$. □

Since $\mathbf{m}^0 \in \Delta(N)$ is decidable for $N \in \mathcal{H}$, and the conditions in Theorem 17 can be tested in finite time, we get the following theorem:

Theorem 18. *The existence of an LESP for $(N(\mathbf{m}^0), \Psi_{\Pi_0}, \mathcal{N}^n)$ is decidable if $N \in \mathcal{H}$.*

5.4 LESPs with Controllability Faults for Petri Nets

We assume that perfect marking information is available

5.4.1 Extension of Notations and Results for faults scenarios in Petri Nets

A *supervisory policy*, in the context of faults, $\mathcal{P}_f : \mathcal{N}^n \times T \times \{0, \ldots, k_r\} \to \{0, 1\}$, returns a 0 or 1 for each marking, each transition, and the observed number of (unintended) firings of controllable transitions affected by the fault. It permits the firing of transition t_j at marking $\mathbf{m}_i$ when k_d-many ($0 \leq k_d \leq k_r$) unintended firings of controllable transitions have been detected, if and only if $\mathcal{P}_f(\mathbf{m}_i, t_j, k_d) = 1$. We require $\mathcal{P}_f(\mathbf{m}_i, t_u, k_d) = 1\ \forall t_u \in T_u$, $\forall k_d$. For a given $T_f \subseteq T_c$, a state-enabled transition $t \in T_e(N, \mathbf{m}_i)$ *can fire* under the supervision of $\mathcal{P}_f$ at marking $\mathbf{m}_i$ when k_d-many ($0 \leq k_d \leq k_r$) unintended firings of controllable transitions have been detected, if either (1) $\mathcal{P}_f(\mathbf{m}_i, t, k_d) = 1$; or (2) $0 < k_d < k_r$, and $t \in T_f$.

A string of transitions $\sigma = t_1 \dots t_k$, where $t_j \in T$ $(j \in \{1, \dots, k\})$, is said to be a *valid firing string in the presence of controllability faults*, starting from the marking $\mathbf{m}_i$, after k_d-many $(0 \leq k_d \leq k_r)$ unintended firings of controllable transitions have been detected thus far, if (1) the transition $t_1 \in T_e(N, \mathbf{m}_i)$ can fire at the marking $\mathbf{m}_i$, and (2) for $j \in \{1, \dots, k\}$, the firing of the transition t_j produces a marking $\mathbf{m}_{i+j}$, $t_{j+1} \in T_e(N, \mathbf{m}_{i+j})$ and the transition t_{j+1} can fire at the marking $\mathbf{m}_{i+j}$. We denote this as $\mathbf{m}_i \xrightarrow{\sigma} \mathbf{m}_{i+k}$ under the supervision of $\mathcal{P}_f$. We say σ is a *valid firing string of transitions under faults* from marking $\mathbf{m}_i$ under the supervision of $\mathcal{P}_f$.

The set $\mathfrak{R}_\phi(N, \mathbf{m}_0, \mathcal{P}_f, k_r, T_f)$ denotes the set of markings generated by all valid firing strings of transitions from $\mathbf{m}_0$ under the supervision of $\mathcal{P}_f$ in N, under the influence of a fault ϕ that will be rectified immediately after k_r-many unintended firings of controllable transitions in the set $T_f \subseteq T_c$ are detected. Consequently, $\forall k_r^2 \leq k_r^1$, $\forall T_f^2 \subseteq T_f^1 \subseteq T_c$, $\mathfrak{R}_\phi$ $(N, \mathbf{m}_i, \mathcal{P}_f, k_r^2, T_f^2) \subseteq \mathfrak{R}_\phi(N, \mathbf{m}_i, \mathcal{P}_f, k_r^1, T_f^1) \subseteq \mathfrak{R}(N, \mathbf{m}_i)$, where we assume that $\mathcal{P}_f$ is defined for k_r^1.

For the example in Figure 5.2 with initial marking $(1\ 1\ 0\ 0\ 0)^T$ consider the supervisory policy $\mathcal{P}$ that constraints the marking to $\Delta(N_i)$ irrespective of faults. Then $\mathfrak{R}_\phi(N_i, (1\ 1\ 0\ 0\ 0)^T, \mathcal{P}$ $, 1, \{t_2\}) = \{(0\ 0\ 0\ 0\ 0)\} \cup \mathfrak{R}(N_i, (1\ 1\ 0\ 0\ 0)^T, \mathcal{P})$. Next, consider the initial marking $(0\ 0\ 2\ 0\ 0)^T$ with $k_r = 1$ and the supervisory policy $\widehat{\mathcal{P}}$ which constrains the PN marking to $\widehat{\Delta}(N_i)$ till the first unintended firing of t_2 is detected, and to $\Delta(N_i)$ afterwards. For this case, $\mathfrak{R}_\phi(N_i, (0\ 0\ 2\ 0\ 0)^T, \widehat{\mathcal{P}}, 1, \{t_2\}) = \mathfrak{R}(N_i, (0\ 0\ 2\ 0\ 0)^T, \mathcal{P})$. Note that $\mathfrak{R}(N_i, (0\ 0\ 2\ 0\ 0)^T, \mathcal{P})$ is the set of reachable markings *in the absence of faults* under the supervision of $\mathcal{P}$ defined above. On the other hand, since $\widehat{\Delta}(N_i) \subset \Delta(N_i)$, we have $\mathfrak{R}(N_i, (0\ 0\ 2\ 0\ 0)^T, \widehat{\mathcal{P}}) \subset \mathfrak{R}(N_i, (0\ 0\ 2\ 0\ 0)^T, \mathcal{P})$.

Definition 14. *A supervisory policy $\mathcal{P}_f : \mathcal{N}^n \times T \times \{0, \dots, k_r\} \to \{0, 1\}$, is said to be a Fault Tolerant Liveness Enforcing Supervisory Policy (FT-LESP) for a PN $N(\mathbf{m}_0)$ if $\forall t \in T, \forall T_f \subseteq T_c, \forall \mathbf{m}_i \in \mathfrak{R}_\phi(N, \mathbf{m}_0, \mathcal{P}_f, k_r, T_f)$, $\exists \mathbf{m}_j \in \mathfrak{R}_\phi(N, \mathbf{m}_i, \mathcal{P}_f, k_r - k_d, T_f)$ such that $\mathcal{P}_f(\mathbf{m}_j, t, k_d) = 1$ and $t \in T_e(N, \mathbf{m}_j)$, where k_d denotes the number of unintended firings of controllable transitions detected when the marking $\mathbf{m}_i$ is reached in the PN $N(\mathbf{m}_0)$ under the supervision of $\mathcal{P}_f$.*

Since a supervisory policy in the context of faults, $\mathcal{P}_f : \mathcal{N}^n \times T \times \{0, \dots, k_r\} \to \{0, 1\}$, can be effectively described by $(k_r + 1)$-many fault-free supervisory policies $\{\mathcal{P}_i : \mathcal{N}^n \times T \to \{0, 1\}\}_{i=0}^{k_r}$, where $\mathcal{P}_f(\mathbf{m}, t, i) = \mathcal{P}_i(\mathbf{m}, t)$, where $0 \leq i \leq k_r$, an FT-LESP can be represented by $(k_r + 1)$-many fault-free LESPs. Corollary 1 follows directly from this observation.

Corollary 1. *($\exists$ FT-LESP for $N(\mathbf{m}_0)$) $\Rightarrow$ ($\exists$ an LESP for $N(\mathbf{m}_0)$).*

An FT-LESP $\mathcal{P}_f : \mathcal{N}^n \times T \times \{0, \ldots, k_r\} \to \{0, 1\}$ is said to be *minimally restrictive* for $N(\mathbf{m}_0)$ if, for $0 \leq k_d \leq k_r$, every FT-LESP $\widehat{\mathcal{P}}_f : \mathcal{N}^n \times T \times \{0, \ldots, k_r\} \to \{0, 1\}$ satisfies the following condition : $\forall \mathbf{m}_i \in \mathcal{N}^n, \forall t \in T, \mathcal{P}_f(\mathbf{m}_i, t, k_d) \geq \widehat{\mathcal{P}}_f(\mathbf{m}_i, t, k_d)$. That is, if the FT-LESP $\mathcal{P}_f$ prevents the firing of a transition t at a marking $\mathbf{m}_i$ after k_d-many fault have been detected, then *all* FT-LESPs would do the same. We get the following definitiona as a straightforward extension of Definition 11 and Theorem 5.1 in [33]

Definition 15. *Let $\Delta_0(N) = \Delta(N)$. Then $\Delta_k(N) \subseteq \Delta(N)$, $k \in \mathcal{N}^+$, is the set of all initial markings that satisfies the following conditions:*

1. *It is control-invariant with respect to N.*
2. *$\forall \mathbf{m}_1 \in \Delta_k(N), \exists \mathbf{m}_2, \mathbf{m}_3 \in \Delta_k(N), \exists$ a valid firing string $\sigma = \sigma_1\sigma_2$ in N such that $\mathbf{m}_1 \xrightarrow{\sigma_1} \mathbf{m}_2 \xrightarrow{\sigma_2} \mathbf{m}_3, \mathbf{m}_3 \geq \mathbf{m}_2$, all transitions appear at least once in σ_2, and $\forall \sigma_3 \in pr(\sigma_1\sigma_2)$, $(\mathbf{m}_1 \xrightarrow{\sigma_3} \mathbf{m}_4) \Rightarrow (\mathbf{m}_4 \in \Delta_k(N))$. Here $pr(\bullet)$ denotes the prefix of the string argument.*
3. *$\forall \mathbf{m}_1 \in \Delta_k(N)$, $\forall t \in T$: $(\mathbf{m}_1 \xrightarrow{t} \mathbf{m}_2) \Rightarrow (\mathbf{m}_2 \in \Delta_j(N),$ where $j \geq k - 1)$.*

Properties 1 and 2 in Definition 15 are the properties of $\Delta(N)$ (Theorem 5.1 in [33]).

The detection mechanism and the policy $\mathcal{P}_f$ is a simple notational extension of what as discussed in the context of $\Delta(\mathcal{D}, \mathbf{I}, S, \varphi)$ in the discussion before Theorem 13.

Theorem 19. $(\mathbf{m}_0 \in \Delta_{k_r}(N)) \Leftrightarrow (\exists$ *an FT-LESP for* $N(\mathbf{m}_0))$.

Proof. Special case of Theorem 13. □

We get the following result as a direct consequence of Corollary 1 and Theorem 19.

Corollary 2. $\forall k \in \mathcal{N}$, $\Delta_k \subseteq \Delta_{k+1}$.

Another consequence of Theorem 19 is that for a given marking $\mathbf{m}$ and a value of k_d, there exists an FT-LESP for $N(\mathbf{m})$ if and only if $\mathbf{m} \in \Delta_{k_r - k_d}(N)$. That is, any FT-LESP must *at least* disable any controllable transition whose firing takes the PN marking outside $\Delta_{k_r - k_d}(N)$. We get the following corollary as a consequence of this observation:

Corollary 3. *Suppose $\mathbf{m}_0 \in \Delta_{k_r}(N)$. Then $\mathcal{P}_f$ is the minimally restrictive FT-LESP for $N(\mathbf{m}_0)$.*

Theorem 20. *Given an LESP for an arbitrary PN $\overline{N}(\mathbf{m}_0)$, the existence of an FT-LESP for a given set T_f and a given value of k_r is undecidable.*

Proof. See Appendix. □

5.4.2 FT-LESP for Fully Controllable Ordinary Free Choice PNs

The main result of this section is that $\Delta_{k_r}(N)$ is right-closed for a fully controllable *Ordinary* FCPN (O-FCPNs). We first prove an intermediate result that the minimally restrictive FT-LESP for a fully controlled O-FCPN will not disable any non-choice transitions. Recall that for an FCPN $N = (\Pi, T, \Phi, \Gamma)$, a transition $t \in T$ is said to be a *non-choice* (resp. *choice*) transition if $\{t\} = ({}^\bullet t)^\bullet$ (resp. if $\{t\} \subset ({}^\bullet t)^\bullet$).

Let the initial marking $\mathbf{m}_0 \in \Delta_{k_r}(N)$ and consider a marking $\mathbf{m} \in \Delta_k(N)$ reached under the supervision of $\mathcal{P}_f$ (that is, $(k_r - k)$-many faults have been detected) such that a non-choice transition $t \in T_e(N, \mathbf{m})$. From Corollary 3, $(\mathcal{P}_f(\mathbf{m}, t, k_r - k) = 1) \Leftrightarrow ((\mathbf{m} \xrightarrow{t} \mathbf{m}_1) \wedge (\mathbf{m}_1 \in \Delta_k(N)))$. We start with the stipulation that $\mathbf{m}_1 \in \Delta_k(N)$, which allows us to specify a supervisory policy corresponding to which we can define the unintended firings, and later prove that the stipulation is indeed correct. Let σ_f be a valid string of transitions under faults from $\mathbf{m}_1$ under the supervision of $\mathcal{P}_f$ in which the unintended occurrences of affected transitions (belonging to T_f) appear k times and $\mathbf{m}_1 \xrightarrow{\sigma_f} \mathbf{m}_2$. In what follows, we prove that our stipulation that $\mathbf{m}_1 \in \Delta_k(N)$ is indeed correct by proving $\mathbf{m}_2 \in \Delta(N)$. Note that the rectification event occurs at $\mathbf{m}_2$ and the supervisor regains control of all transitions.

Let σ_s denote the largest substring of σ_f that is a valid firing string from $\mathbf{m}$, and $\mathbf{m} \xrightarrow{\sigma_s} \widehat{\mathbf{m}}_1$, under the supervision of $\mathcal{P}_f$. Also, let $\sigma_f \backslash \sigma_s$ denote the ordered string of transitions in σ_f that did not appear in σ_s. In the first step of the proof we specify a string $(\sigma_s)(\omega_1)(t)(\sigma_f \backslash \sigma_s)$ that can be fired from $\mathbf{m}$ and observe that the resulting marking is in $\Delta(N)$.

$$\mathbf{m} \xrightarrow{t} \mathbf{m}_1 \xrightarrow{\sigma_f} \mathbf{m}_2 \xrightarrow{\omega_1} \widehat{\mathbf{m}}_4 \tag{5.12}$$

$$\mathbf{m} \xrightarrow{\sigma_s} \widehat{\mathbf{m}}_1 \xrightarrow{\omega_1} \widehat{\mathbf{m}}_2 \xrightarrow{t} \widehat{\mathbf{m}}_3 \xrightarrow{\sigma_f \backslash \sigma_s} \widehat{\mathbf{m}}_4 \tag{5.13}$$

In the second step, we prove that the string $t\sigma_f$ fired from $\mathbf{m}$ can be extended by ω_1 which we then use to prove that $\mathbf{m}_2 \in \Delta(N)$.

The scenario described by Equation (5.13) can be interpreted as a simulation of a specific path under supervision from $\mathbf{m}$ that replicates σ_f (that is, the effect of unintended firing of transitions). σ_s and $\sigma_f \backslash \sigma_s$ can be determined with the knowledge of σ_f. The string ω_1 is determined as follows. Suppose (unintended occurrences of) controllable transitions belonging to the set T_f appear $j \leq k$ times in σ_s. Since $\mathbf{m} \in \Delta_k(N)$, from Property 3 of Definition 15 and Corollary 2, we have $\widehat{\mathbf{m}}_1 \in \Delta_{k-j}(N)$. Consequently, there exists a valid firing string of transitions specified by the policy $\mathcal{P}_f$ from $\widehat{\mathbf{m}}_1$ after which t will be permitted by $\mathcal{P}_f$. That is, $\exists \omega_1 \in T^*$ such that (i) $\widehat{\mathbf{m}}_1 \xrightarrow{\omega_1} \widehat{\mathbf{m}}_2$, $\mathcal{P}_f(\widehat{\mathbf{m}}_2, t, k_r - k + j) = 1$; and (ii) $\widehat{\mathbf{m}}_1 \xrightarrow{\omega_2} \overline{\mathbf{m}}_1$, $\overline{\mathbf{m}}_1 \in \Delta_{k-j}(N)$ $\forall \omega_2 \in pr(\omega_1)$. For the example PN N_i in Figure 5.2, let $k = 1$,

$\mathbf{m} = (1\ 1\ 0\ 0\ 1)^T$, $t = t_1$, and $T_f = \{t_2\}$. Then from (5.12) and (5.13), we have:

$$(1\ 1\ 0\ 0\ 1)^T \xrightarrow{t_1} (0\ 0\ 1\ 0\ 1)^T \xrightarrow{t_2} (0\ 0\ 0\ 0\ 1)^T \xrightarrow{t_5} (1\ 1\ 0\ 0\ 0)^T$$
$$(1\ 1\ 0\ 0\ 1)^T \xrightarrow{\epsilon} (1\ 1\ 0\ 0\ 1)^T \xrightarrow{t_5} (2\ 2\ 0\ 0\ 0)^T \xrightarrow{t_1} (1\ 1\ 1\ 0\ 0)^T \xrightarrow{t_2} (1\ 1\ 0\ 0\ 0)^T$$

Observation 12. *$\sigma_f \backslash \sigma_s$ is a valid firing string from $\widehat{\mathbf{m}}_3$ (in the absence of supervision).*

Proof. Let t_1 denote the first transition that appears in $\sigma_f \backslash \sigma_s$. Then t_1 must have an input place that is an output place of t. That is, $\exists p \in \{{}^\bullet t_1\} \cap \{t^\bullet\}$. If not, then t_1 can be fired without firing transition t, which is a contradiction since t_1 does not appear in σ_s. There are two cases: (i) $\{{}^\bullet t_j^2\}^\bullet \neq t_1$; and (ii) $\{{}^\bullet t_j^2\}^\bullet = t_1$. In the first case, t_1 is a choice transition. Then since N is ordinary and free choice, $\{{}^\bullet t_1\} = p$ for some place $p \in \{t^\bullet\}$, and hence $t_1 \in T_e(N, \widehat{\mathbf{m}}_3)$. In the second case, t_1 is a non-choice transition. Then $\{{}^\bullet t_1\} \subset \{\sigma_s^\bullet\}$ and $\{{}^\bullet t_1\} \subseteq \{t^\bullet\}$. Here we use $\{\sigma_s^\bullet\}$ to denote the set of places populated by the firing of string σ_s from $\mathbf{m}_0$. The string ω_1 does not reduce the token load of the input places of the non-choice transition t_1 (as $\{{}^\bullet t_j^2\}^\bullet = t_1$), it follows that $t_1 \in T_e(N, \widehat{\mathbf{m}}_3)$. Continuing in the same way, if t_k is the k-th transition in $\sigma_f \backslash \sigma_s$, then $\exists p \in \{{}^\bullet t_k\} \cap (\cup_{i=1}^{k-1} \{t_i{}^\bullet\})$. The rest of the proof follows by induction by using the same arguments as for t_1. □

Observation 13. *ω_1 is a valid firing string from $\mathbf{m}_2$ under the supervision of $\mathcal{P}_f$.*

Proof. Let t^1 be the first transition in ω_1. Since ω_1 is a valid firing string from $\widehat{\mathbf{m}}_1$, it means that the firing of string σ_s from $\widehat{\mathbf{m}}_0$ populates the input places of t^1 with sufficient number of tokens so as to enable the transition. Now, since σ_s is a substring of σ_f, its firing from $\mathbf{m}_1$ also populates the input places of t^1 with sufficient number of tokens so as to enable transition t^1; and the input places of t^1 would not be emptied by transitions in $\sigma_f \backslash \sigma_s$. Suppose for contradiction that $t^1 \notin T_e(N, \mathbf{m}_2)$ and the firing of some transition in $\sigma_f \backslash \sigma_s$ emptied the input places of t^1. Then t^1 cannot be non-choice as $\{{}^\bullet t_j^2\}^\bullet = t^1$ and once populated $\{{}^\bullet t^1\}$ cannot be emptied without firing t^1. If t^1 is a choice transition, then it means that there exists $t' \in \{{}^\bullet t^1\}^\bullet$ that appears in σ_f. But then it appears in σ_s also, and hence does not appear in $\sigma_f \backslash \sigma_s$ which is a contradiction. The rest of the proof follows through recursion using the same arguments by taking $\sigma_s = \sigma_s t^1$ and $\sigma_f = \sigma_f t^1$. □

Observation 14. $\widehat{\mathbf{m}}_4, \mathbf{m}_2 \in \Delta(N)$.

Proof. The string $(\sigma_s)(\omega_1)(t)(\sigma_f \backslash \sigma_s)$ is such that the unintended firing of affected transitions in T_f appear k times. Since $\mathbf{m} \in \Delta_k(N)$, by Property 3 of Definition 15, $\widehat{\mathbf{m}}_4 \in \Delta(N)$. Since $\widehat{\mathbf{m}}_4 \in \Delta(N)$, there exists a valid firing string $\sigma = \sigma_1\sigma_2$ in N such that $\widehat{\mathbf{m}}_4 \xrightarrow{\sigma_1}$

$\widehat{\mathbf{m}}_5 \xrightarrow{\sigma_2} \widehat{\mathbf{m}}_6, \widehat{\mathbf{m}}_6 \geq \widehat{\mathbf{m}}_5$, all transitions appear at least once in σ_2, and $\forall \sigma_3 \in pr(\sigma_1\sigma_2)$, $(\widehat{\mathbf{m}}_1 \xrightarrow{\sigma_3} \widehat{\mathbf{m}}_7) \Rightarrow (\widehat{\mathbf{m}}_7 \in \Delta(N))$. Due to the fully controllable nature of the PN, a path with such properties, $\omega_1\sigma_1\sigma_2$, also exists for $\mathbf{m}_2$. Besides, the control invariance property is trivially true. Therefore, $\mathbf{m}_2 \in \Delta(N)$. □

Since $\mathbf{m}_2 \in \Delta(N)$ is true for all values of k such that $\mathbf{m} \in \Delta_k(N)$, it follows that $\mathbf{m}_1 \in \Delta_k(N)$. Therefore, the firing of a non-choice transition from $\mathbf{m} \in \Delta_k(N)$ does not take the marking outside the set. The minimally restrictive FT-LESP will not disable any non-choice transition.

Lemma 7. *The minimally restrictive FT-LESP for a fully controlled O-FCPN will not control disable any non-choice transitions.*

Theorem 21. $\Delta_{k_r}(N)$ *is right-closed for a fully controlled ordinary free choice PN.*

Proof. If $\Delta_{k_r}(N) = \emptyset$, then it is right-closed by definition. Let $\mathbf{m}_0 \in \Delta_{k_r}(N)$. We need to prove that $\widehat{\mathbf{m}}_0 \in \Delta_{k_r}(N)$ for all $\widehat{\mathbf{m}}_0 \geq \mathbf{m}_0$. We prove this by induction. The base case is established by letting $k_r = 0$ and observing that $\Delta_0(N)(= \Delta(N))$ for an FCPN is right-closed ([35]). The induction hypothesis is that $\Delta_i(N)$ for $i \in \{1, 2, \ldots, k_r - 1\}$ is right-closed. We know that $\mathbf{m}_0 \in \Delta_{k_r}(N)$. Since the PN is fully controlled, the path property and control invariance (Properties 1 and 2 in Definition 15) follow trivially for all $\widehat{\mathbf{m}}_0 \geq \mathbf{m}_0$. For the induction step, we need to prove that the firing of a single transition from every $\widehat{\mathbf{m}}_0 \geq \mathbf{m}_0$ results in a marking that is in $\Delta_{k_r-1}(N)$.

By Lemma 7 and the discussion preceding it, for a fully controlled O-FCPN, the firing of a non-choice transition from $\widehat{\mathbf{m}}_0$ will result in a marking in $\Delta_{k_r}(N)$. We consider the case of choice transitions and let $\widehat{\mathbf{m}}_0 = \mathbf{m}_0 + \widetilde{\mathbf{m}}$. If $T_e(N, \widehat{\mathbf{m}}_0) = T_e(N, \mathbf{m}_0)$, then $\widehat{\mathbf{m}}_0 \xrightarrow{t} \overline{\mathbf{m}}$ and $\mathbf{m}_0 \xrightarrow{t} \underline{\mathbf{m}}$, and $\overline{\mathbf{m}} = \underline{\mathbf{m}} + \widetilde{\mathbf{m}}$. We have: $(\mathbf{m}_0 \in \Delta_{k_r}(N)) \Rightarrow (\underline{\mathbf{m}} \in \Delta_{k_r-1}(N))$. By induction hypothesis, $\Delta_{k_r-1}(N)$ is right closed. Therefore, $\overline{\mathbf{m}} \in \Delta_{k_r-1}(N)$. If $T_e(N, \mathbf{m}_0) \subset T_e(N, \widehat{\mathbf{m}}_0)$, then $\widehat{\mathbf{m}}_0 \geq \mathbf{m}_0 + \sum_{t \in T_{en}} \mathbf{IN}_t$ where $T_{en} = T_e(N, \widehat{\mathbf{m}}_0) - T_e(N, \mathbf{m}_0)$. The firing of transition t_i from $\widehat{\mathbf{m}}_0$ would give:

$$\widehat{\mathbf{m}}_0 + \mathbf{C}_{t_i} \geq \mathbf{m}_0 + \mathbf{OUT}_{t_i} + \sum_{t \in T_{en} - \{t_i\}} \mathbf{IN}_t$$

$(\mathbf{m}_0 \in \Delta_{k_r}(N)) \Rightarrow (\mathbf{m}_0 \in \Delta_{k_r-1}(N))$. By induction hypothesis, $\Delta_{k_r-1}(N)$ is right closed. Therefore, $\widehat{\mathbf{m}}_0 + \mathbf{C}_{t_i} \in \Delta_{k_r-1}(N)$. □

In general, $\Delta_{k_r}(N)$ is not right-closed for arbitrary PNs. Figure 5.3 presents an example of a PN structure that is not an O-FCPN and for which $\Delta_1(N_j)$ is not right-closed. It is

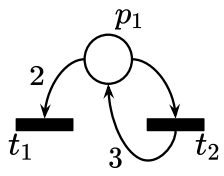


Figure 5.3: PN N_j for which $\Delta_1(N_j)$ is not right-closed for $k_r = 1$.

clear that $\Delta_0(N_j) = \{\mathbf{m} \in \mathcal{N} : \mathbf{m} \geq 1\}$. Let $k_r = 1$ and $T_f = \{t_1\}$. Then: $1 \xrightarrow{\phi t_2 t_1 \rho} 1$ which is in $\Delta_0(N_j)$. If the initial token load is 2 then: $2 \xrightarrow{\phi t_1 \rho} 0$, which is not in $\Delta(N_j)$. We have $\Delta_1(N_j) = \Delta_0(N_j) - \{2\}$.

Algorithm 9 presents a recursive procedure for the synthesis of FT-LESP for a fully controlled O-FCPN. Letting $\Delta_0 = \Delta(N)$, the procedure FTLESP_FCPN(N, $\Delta(N)$, $\mathbf{m}_0$) computes a sequence of sets $\Delta_1, \ldots, \Delta_{k_r}$ each satisfying the properties in Definition 15. The *while* condition in the algorithm tests for Property 3 of Definition 15. If it is not satisfied for any of the minimal elements of Δ_k (that is, there is a transition whose firing results in a marking not in Δ_{k-1}), then the minimal elements of the current estimate are raised (Step 3) by the smallest possible amount. Step 4 removes the redundant entries in the updated set by keeping only the minimal (smallest) elements. The updated estimate is then tested for Properties 1 and 2 in the (subroutine of) Step 5. We refer the reader to [35] for further details with only a note here that if any of the Properties 1 and 2 are not satisfied, then (the subroutine of) Step 5 essentially updates the estimate using a process similar to Steps 3 and 4 given here. The program exits the *while* loop either when the set Δ_k with required properties is found or if $\mathbf{m}_0$ drops out of the estimate.

We illustrate the algorithm using the PN N_i in Figure 5.2. $min(\Delta(N_i)) = \{(1\ 1\ 0\ 0\ 0)^T$, $(0\ 0\ 1\ 0\ 0)^T$, $(0\ 0\ 0\ 1\ 0)^T$, $(0\ 0\ 0\ 0\ 1)^T\}$. Firing of t_2 from $(0\ 0\ 1\ 0\ 0)^T$ will result in the marking $(0\ 0\ 0\ 0\ 0)^T$ which is not in $\Delta(N_i)$. The execution will go to Step 3 in the algorithm following which $(0\ 0\ 1\ 0\ 0)^T$ will be replaced by $\{(1\ 1\ 1\ 0\ 0)^T$, $(0\ 0\ 2\ 0\ 0)^T$, $(0\ 0\ 1\ 1\ 0)^T$, $(0\ 0\ 0\ 1\ 1)^T\}$ in $min(\Delta(N_i))$. In Step 5, we test the path property (control invariance is trivially true). While the path property for $(1\ 1\ 0\ 0\ 0)^T \xrightarrow{t_1 t_3 t_4 t_5 t_1 t_2} (1\ 1\ 0\ 0\ 0)^T$ for the original $\Delta(N_i)$ was true with the path $t_1 t_3 t_4 t_5 t_1 t_2$, it is not true for the updated version because $(1\ 1\ 0\ 0\ 0)^T \xrightarrow{t_1} (0\ 0\ 1\ 0\ 0)^T$ and $(0\ 0\ 1\ 0\ 0)^T$ is not in $\Delta(N_i)$ anymore. Therefore, the algorithm (subroutine of Step 5) will raise the minimal elements and replace $(1\ 1\ 0\ 0\ 0)^T$ by $\{(2\ 2\ 0\ 0\ 0)^T$, $(1\ 1\ 1\ 0\ 0)^T$, $(1\ 1\ 0\ 1\ 0)^T$, $(1\ 1\ 0\ 0\ 1)^T\}$. Further steps in the iterations to obtain $\Delta_1(N_i)$ (which was denoted as $\widehat{\Delta}(N_i)$ in Section 5.2.1) from $\Delta(N_i)$ are shown in the Figure 5.4.

Algorithm 9 FTLESP_FCPN$(N, \Delta_{k-1}, \mathbf{m}_0)$

$\Delta_k = \Delta_{k-1}$. Let $\min(\Delta_{k-1}) = \{\widetilde{\mathbf{m}}_j\}_{j=1}^{l}$
while ($\mathbf{m}_0 \in \Delta_k$, $\exists t \in T$, $\exists \overline{\mathbf{m}}_i \in \min(\Delta_k)$ such that $\max\{\overline{\mathbf{m}}_i, \mathbf{IN}_t\} + \mathbf{C}_t \notin \Delta_{k-1}$) **do**
    Replace $\overline{\mathbf{m}}_i$ by a set of l vectors $\{\widehat{\mathbf{m}}_c\}_{c=1}^{l}$ where each $\widehat{\mathbf{m}}_c$ is defined corresponding to each $j \in \{1, \ldots l\}$ as follows: $\widehat{\mathbf{m}}_c = \overline{\mathbf{m}}_i + \max\{\mathbf{0}, \widetilde{\mathbf{m}}_j - (\max\{\overline{\mathbf{m}}_i, \mathbf{IN}_t\} + \mathbf{C}_t)\}$
    Replace the resulting set of $\{\widetilde{\mathbf{m}}_i\}_i$ by its minimal elements and modify the value of l to equal the size of the minimal set of vectors. The updated Δ_k is denoted by this set of minimal elements.
    $\Delta_k \leftarrow$ The largest (right-closed) subset of Δ_k (from Step 3) such that Properties (a) and (b) are satisfied for all members.
    {/* This procedure parallels portions of the algorithm in figure 8 of reference [35], and is skipped for brevity */}
end while
if $\mathbf{m}_0 \notin \Delta_k$ **then**
    $\Delta_k = \emptyset$
    return $\{\Delta_i\}_{i=1}^{k}$
end if
if $k = k_r$ **then**
    return $\{\Delta_i\}_{i=1}^{k}$
else
    FTLESP_FCPN$(N, \Delta_k, \mathbf{m}_0)$
end if

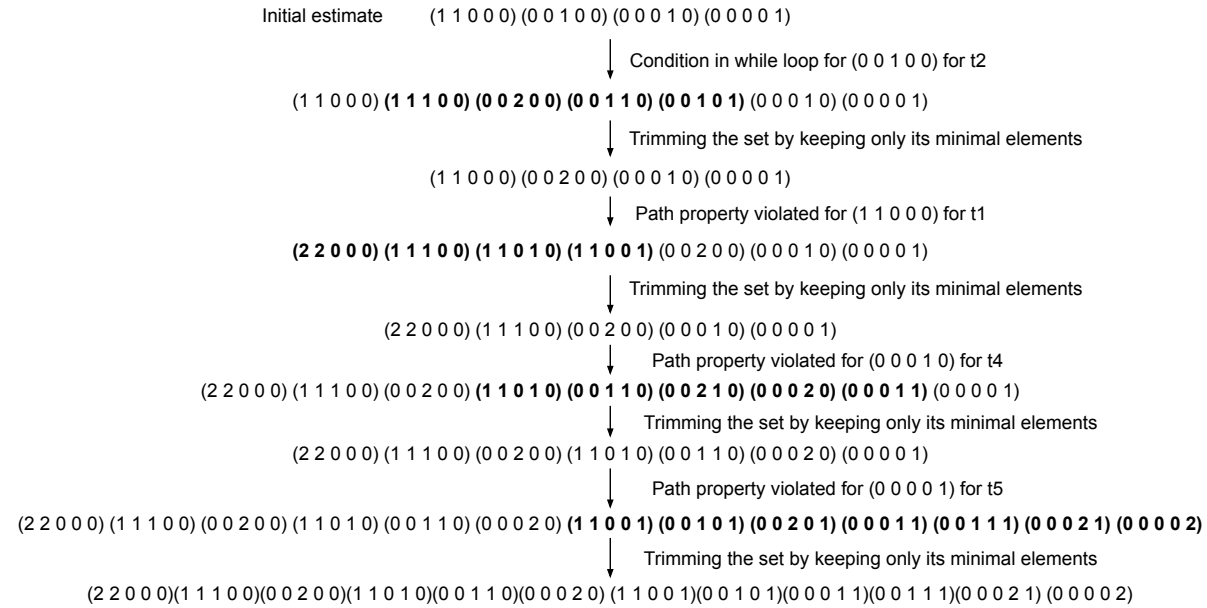


Figure 5.4: Iterations to obtain $\Delta_1(N_i)$ (which was denoted as $\widehat{\Delta}(N_i)$ in Section 5.2.1) from $\Delta(N_i)$

CHAPTER 6

CONCLUSION

This thesis is about the decidability of problems in liveness of controlled discrete event systems. The existence of an LESP for a DES depends on the membership of the initial state to an appropriately defined set. We considered a particular modeling paradigm of DES known as Petri Nets. There is an LESP for a PN $N(\mathbf{m}^0)$ if and only if $\mathbf{m}^0 \in \Delta(N)$ where

$$\Delta(N) := \{\mathbf{m}^0 \mid \exists \text{ an LESP for } N(\mathbf{m}^0)\},$$

In prior work, it was proved that neither the membership nor the non-membership of a marking in $\Delta(N)$ is semi-decidable for an arbitrary PN structure. We generalized this decision problem and showed that neither "*Is* $\Delta(N) = \emptyset$*?*" nor "*Is* $\Delta(N) \neq \emptyset$*?*" is semi-decidable.

An integer-valued set of vectors is said to be *right-closed* if the presence of a vector in the set implies that all term-wise larger vectors are also in the set. We presented a necessary and sufficient condition for $\Delta(N)$ to be right-closed for an arbitrary PN. Following this, we showed that "*Is* $\Delta(N)$ *right-closed?*" is undecidable for arbitrary PN structures. We also showed that for arbitrary PN structures the decision problems: "*Is there a right-closed subset of* $\Delta(N)$*?*" and "*Is there no right-closed subset of* $\Delta(N)$*?*" are not semi-decidable.

If a transition is control-enabled at some marking under the supervision of a *marking-monotone policy* (MM-policy), then it is control-enabled at all larger markings as well. An MM-policy $\mathcal{P}$ is a *marking-monotone LESP* (MM-LESP) for $N(\mathbf{m}^0)$ if it is an LESP for $N(\widehat{\mathbf{m}}^0)$ for all $\widehat{\mathbf{m}}^0 \geq \mathbf{m}^0$, as well. The set

$$\Delta_M(N) := \{\mathbf{m}^0 \mid \exists \text{ an MM-LESP for } N(\mathbf{m}^0)\},$$

is a right-closed subset of $\Delta(N)$ for any PN structure N. After introducing a class of PN structures for which the set $\Delta(N)$ is known to be right-closed, we showed that the existence of an MM-LESP for an arbitrary PN $N(\mathbf{m}^0)$ is decidable. That is, "*Is* $\mathbf{m}^0 \in \Delta_M(N)$*?*" is decidable for any PN structure N. Thus, starting from the two decision problems: *"Is* $\mathbf{m}^0 \in \Delta(N)?''$ and *"Is* $\mathbf{m}^0 \notin \Delta(N)?''$ that are not semi-decidable, we present a string of results

that culminates in decidable sub-problems: *"Is* $\mathbf{m}^0 \in \Delta_M(N)?''$ and *"Is* $\mathbf{m}^0 \notin \Delta_M(N)?''$.

These results lead to the conclusion that extracting any kind of information about $\Delta(N)$ for an arbitrary PN is most likely an extremely hard problem. Besides, we can also conclude that between the properties of the set of initial markings for which an LESP exists, and the characteristics of the LESP, it is the characteristics of the LESP that plays a prominent role in determining decidability. That is, if a supervisory policy $\mathcal{P}$ is such that $\mathfrak{R}(N, \mathbf{m}, \mathcal{P})$ (which can have an unbounded number of markings) can be represented by a reachability graph with a finite number of appropriately defined symbolic markings such that the liveness property is preserved, then the existence of $\mathcal{P}$ is likely to be decidable. Marking Monotone LESPs is one instance of such an LESP in which a reachability graph with possibly infinite number of markings is reduced to a coverability graph with finite number of nodes.

Using this idea, we presented a generalization of *coverability graphs*. The central idea for the generalization is to partition the set of non-negative integers into subsets with certain properties, and then defining *order* on those subsets. The overall procedure preserves the typical characteristics of coverability graph while eliciting additional information about the underlying system which makes it more general than traditional coverability graphs. We showed that the generalized coverability graphs can be used to test the existence and non-existence of LESPs for a larger class of PNs. The extension of coverability graphs discussed in this thesis provides a general method for creating a finite representation of the reachability graph of an unbounded PNs. The process of LESP synthesis discussed in this context is verification-based. That is, the user hypothesizes a $\Delta(N)$ based on the PN structure and other aspects, and defines the class/order accordingly, consistent with the algebra enunciated in Chapter 4. Then we make use of the result that the existence of a CM-LESP is decidable to verify if the hypothesis is correct. For instance, for the example PN N_1 illustrated in Chapter 4, after the sets $\{\zeta_0^i, \zeta_1^i, \ldots, \zeta_{k_i-1}^i\}, i \in \{1, \ldots, n\}$, and the set $\{\omega_j^i\}_{j=0}^{k_i-1}$ under the wqo $\precsim_i$ are assigned by the user, the results show how the existence of a (CM-)LESP can be certified to be correct. Using the generalization presented in this thesis in other areas of applications of coverability graph is a direction of future research.

The supervisory action discussed in this thesis is dependent on the current state s, the evaluation of the next-state resulting from occurrence of event e from s, and the action of enabling or disabling the event. Keeping these steps in mind, in Chapter 5, we tackled a general class of problem in which the supervisory action can be impeded due to various reasons. We considered scenarios in which precise state information is not available to the supervisor and when the control action is modified due to the occurrence of faults. We presented necessary and sufficient conditions for the existence of a B-LESP for a general DES model in this setting. We then discussed two specific cases for PN models of DES—

partial state observability and controllability faults. We showed that the existence of LESP for an arbitrary PN is undecidable in both scenarios, which is an expected result since the existence of an LESP in uncertainty-free case is undecidable. We go a step further and prove that it is undecidable even if an LESP for an uncertainty-free case is available. This leads to the conclusion that the complexity in LESP-synthesis under imprecise state information or controllability faults is not solely inherited from the complexity in LESP synthesis. One aspect of this framework which we did not investigate in this thesis is the learning algorithm. This is one major direction of future research.

APPENDIX A

PROOFS

A.1 LESPs for Arbitrary PNs

Theorem 2: $(N \in \widehat{H}) \Leftrightarrow (\Delta(N)$ is right-closed).

Proof. ($\Rightarrow$) If $\Delta(N) = \emptyset$, it is right-closed by definition. If $\Delta(N) \neq \emptyset$, we establish the result by proving the contrapositive. Assume $\Delta(N)$ is not right-closed. Particularly, assume there exists $\mathbf{m}^1 \in \Delta(N)$ such that $(\mathbf{m}^1 + \widehat{\mathbf{m}}) \notin \Delta(N)$. Now, $\Delta(N)$ for a fully controllable PN is right-closed. Therefore, if $(\mathbf{m}^1 + \widehat{\mathbf{m}}) \notin \Delta(N)$, then the set of uncontrollable transitions of N will be non-empty, and hence $\mathbf{P} = Int(conv(\{\mathbf{IN}_{t_u}\}_{t_u \in T_u}))$ is a non-empty set. Consider $\mathbf{m}^1 \in \Delta(N)$ and let Π_c denote the set of places connected to only controllable transitions (i.e. $\Pi_c^\bullet \cap T_u = \emptyset$). The initial token load of all $p \in \Pi_c$ can be increased to an arbitrarily large value and the initial marking will still be inside $\Delta(N)$. This is true because the supervisory policy can act as if the extra tokens in all $p \in \Pi_c$ never existed, and enforce liveness in the same way as for $\mathbf{m}^1$. Therefore, without loss of generality we can assume that the marking $(\mathbf{m}^1 + \widehat{\mathbf{m}}) \notin \Delta(N)$ has additional tokens in only those places that are connected to at least one uncontrollable transition. This implies, as $\mathbf{P}$ is the convex hull of the columns of the input matrix that correspond to the uncontrollable transitions, that there exists an integer k such that $(\mathbf{m}^1 + \widehat{\mathbf{m}}) \in (\mathbf{m}^1 + k \times \mathbf{P})$. On the other hand, we have $(\mathbf{m}^1 + \widehat{\mathbf{m}}) \notin \Delta(N)$. Then by the characterization of $\widehat{H}$ class above, we have $N \notin \widehat{H}$.

($\Leftarrow$) We prove this via the contrapositive. Assume $N \notin \widehat{H}$. This means that there exists an $\mathbf{m} \in \Delta(N)$ for which there exists a (larger) marking inside the set $\mathbf{m} + \mathbf{P}$ at which the PN is not live. This implies $\Delta(N)$ is not right-closed. □

Observation 1: $(\Delta(\widetilde{N}) \neq \emptyset) \Leftrightarrow (\overline{\mathbf{m}} \in \Delta(\widetilde{N}))$.

Proof. ($\Rightarrow$) If there is a marking $\mathbf{m}^1 \in \Delta(\widetilde{N})$, then following the introductory discussion above, there is a marking $\mathbf{m}^2 \in \Delta(\widetilde{N})$ reachable from $\mathbf{m}^1$ under the supervision of any LESP for $\widetilde{N}(\mathbf{m}^1)$, where $\mathbf{m}^2(\pi_{m+1}) \neq 0$. Additionally, $\exists \sigma_u \in (\{t_{m+2}, t_{m+3}, \ldots, t_{m+n+2}\} \cup \{\tau_1, \tau_2, \ldots, \tau_m\})^*$ (note, σ_u is string of uncontrollable transitions) such that $\mathbf{m}^2 \xrightarrow{\sigma_u} \overline{\mathbf{m}}$. That

is, $\overline{\mathbf{m}}$ is reachable from $\mathbf{m}^2$. Since $\mathbf{m}^2 \in \Delta(\widetilde{N})$, and $\mathbf{m}^2 \xrightarrow{\sigma_u} \overline{\mathbf{m}}$, where σ_u is a string of uncontrollable transitions, by control invariance, it follows that $\overline{\mathbf{m}} \in \Delta(\widetilde{N})$.

($\Leftarrow$) If $\overline{\mathbf{m}} \in \Delta(\widetilde{N})$ then $\Delta(\widetilde{N}) \neq \emptyset$ by definition. □

Observation 2: $(\overline{\mathbf{m}} \in \Delta(\widetilde{N})) \Leftrightarrow (\mathbf{m}^0 \in \Delta(N))$

Proof. ($\Rightarrow$) If $\overline{\mathbf{m}} \in \Delta(\widetilde{N})$, then since $T_e(\widetilde{N}, \overline{\mathbf{m}}) = \{t_{m+1}\}$, we have $\overline{\mathbf{m}} \xrightarrow{t_{m+1}} \overline{\mathbf{m}}^1$ under the supervision of any LESP for $\widetilde{N}(\overline{\mathbf{m}})$. At $\overline{\mathbf{m}}^1$, the PN structure N is initialized with a marking $\mathbf{m}^0$, while the rest of the places of $\widetilde{N}$ are all empty. Since $\overline{\mathbf{m}}^1 \in \Delta(\widetilde{N})$ it follows that $\mathbf{m}^0 \in \Delta(N)$. If it were otherwise, the transition τ_{m+1} cannot be made live in $\widetilde{N}(\overline{\mathbf{m}}^1)$, and we must conclude that $\overline{\mathbf{m}}^1 \notin \Delta(\widetilde{N})$.

($\Leftarrow$) If $\mathbf{m}^0 \in \Delta(N)$, there is an LESP $\mathcal{P}$ for $N(\mathbf{m}^0)$. This LESP is used to construct an LESP $\widetilde{\mathcal{P}}$ for $\widetilde{N}(\overline{\mathbf{m}})$ as follows for $\underline{\mathbf{m}} \in \mathcal{N}^{card(\widetilde{\Pi})}, \widetilde{t} \in \widetilde{T}$

$$\widetilde{\mathcal{P}}(\underline{\mathbf{m}}, \widetilde{t}) = \begin{cases} \mathcal{P}(\underline{\mathbf{m}}(\Pi), \widetilde{t}) & \text{if } \widetilde{t} \in T, \\ 1 & \text{if } \widetilde{t} \in (\widetilde{T} - T - \{t_{m+1}\}), \\ 1 & \text{iff } (\widetilde{t} = t_{m+1}) \wedge (\underline{\mathbf{m}} = \overline{\mathbf{m}}), \end{cases}$$

where, $\underline{\mathbf{m}}(\Pi)$ denotes the marking of the subnet N. The fact that $\widetilde{\mathcal{P}}$ is an LESP for $\widetilde{N}(\overline{\mathbf{m}})$ follows directly from the construction of $\widetilde{N}$ and the fact that $\mathcal{P}$ is an LESP for $N(\mathbf{m}^0)$. □

Observation 3: $(\Delta(\overline{N}) \neq \emptyset) \Leftrightarrow (\Delta(N) \neq \emptyset)$.

Proof. ($\Rightarrow$) Assume there exists a marking $\mathbf{m}^1 \in \Delta(\overline{N})$. Consider another marking $\overline{\mathbf{m}}^1$ of the PN N that initializes (a) the places of $\overline{N}$ (i.e. $\{p_1, \ldots p_n\}$) with token loads identified by the marking $\mathbf{m}^1$, that is $\overline{\mathbf{m}}^1(\Pi_1) = \mathbf{m}^1$, (b) a single token in π_{m+2} and (c) zero tokens in all other places. We show that $\overline{\mathbf{m}}^1 \in \Delta(N)$ by constructing an LESP $\mathcal{P}$ for $N(\overline{\mathbf{m}}^1)$.

Let $\mathcal{P}$ be a policy such that $\forall t_c \in T_1$:

$$(\mathcal{P}(\overline{\mathbf{m}}^2, t_c) = 0) \Leftrightarrow ((\overline{\mathbf{m}}^2 \xrightarrow{t_c} \overline{\mathbf{m}}^3) \wedge (\overline{\mathbf{m}}^3(\Pi_1) \notin \Delta(\overline{N}))) \tag{A.1}$$

That is, it prevents a controllable transition in T_1 if and only if its firing takes the marking of $\overline{N}$ outside $\Delta(\overline{N})$. Since $\mathbf{m}^1 \in \Delta(\overline{N})$, all transitions in T_1 are live when $N(\overline{\mathbf{m}}^1)$ is under the supervision of $\mathcal{P}$. Consequently, from the definition of liveness, $\forall k \in \mathcal{N}, \forall \overline{\mathbf{m}}^4 \in \Re(N, \overline{\mathbf{m}}^1, \mathcal{P}), \exists \overline{\mathbf{m}}^5 \in \Re(N, \overline{\mathbf{m}}^4, \mathcal{P})$ such that $\overline{\mathbf{m}}^5(\pi_{m+1}) \geq k$, $\overline{\mathbf{m}}^5(\Pi_1) \in \Delta(\overline{N})$, and $\overline{\mathbf{m}}^5(\pi_{m+2}) = 1$.

The supervisory policy $\mathcal{P}$ control-enables a transition γ_i, where $i \in \{1, \ldots, n\}$, at a marking $\overline{\mathbf{m}}^6 \in \Re(N, \overline{\mathbf{m}}^1, \mathcal{P})$ if and only if (a) $\overline{\mathbf{m}}^1 \xrightarrow{\sigma} \overline{\mathbf{m}}^6$ under the supervision of $\mathcal{P}$, and $\#(\sigma, \gamma_i) = \#(\sigma, \delta_i)$, (b) $\overline{\mathbf{m}}^6(p_i) \neq 0$, (c) $\overline{\mathbf{m}}^6(\pi_{m+2}) = 1$, and (d) $\overline{\mathbf{m}}^6(\pi_{m+1}) \geq 2$. That is, if

$\overline{\mathbf{m}}^6 \xrightarrow{\gamma_i} \overline{\mathbf{m}}^7$ under the supervision of $\mathcal{P}$, then $T_e(N, \overline{\mathbf{m}}^7) = \{\epsilon_i\}$ and $\overline{\mathbf{m}}^7(\pi_{m+2}) = 0$. Here we use the notation $\#(\sigma, t)$ to denote the number of occurrences of transition t in a valid firing string σ.

A transition in the set $\{\delta_i\}_{i=1}^n$ is control-enabled at $\overline{\mathbf{m}}^8 \in \Re(N, \overline{\mathbf{m}}^1, \mathcal{P})$ if and only if (i) $\overline{\mathbf{m}}^8(\pi_{m+2}) = 0$, and (ii) $\exists \overline{\mathbf{m}}^6 \in \Re(N, \overline{\mathbf{m}}^1, \mathcal{P})$ such that $\overline{\mathbf{m}}^6 \xrightarrow{\gamma_i \epsilon_i} \overline{\mathbf{m}}^8$ under the supervision of $\mathcal{P}$. That is, if $\overline{\mathbf{m}}^8 \xrightarrow{\delta_i} \overline{\mathbf{m}}^9$ under the supervision of $\mathcal{P}$, then $\overline{\mathbf{m}}^9(\pi_{m+2}) = 1$ and $\overline{\mathbf{m}}^9(\Pi_1) \in \Delta(\overline{N})$.

Thus, following the discussion in the paragraph preceding this observation, all transitions in $N(\overline{\mathbf{m}}^1)$ are live under supervision of $\mathcal{P}$, and $\Delta(N) \neq \emptyset$.
($\Leftarrow$) We prove this via the contrapositive. If $\Delta(\overline{N}) = \emptyset$, then τ_{m+1} cannot be made live, and $\Delta(N) = \emptyset$. □

Observation 4: $(\Delta(N) \neq \emptyset) \Leftrightarrow (\Delta(N)$ is not right-closed)

Proof. ($\Rightarrow$) Suppose $\Delta(N) \neq \emptyset$, consider the marking $\overline{\mathbf{m}}^1$ from Observation 3. Next consider a marking, $\overline{\mathbf{m}}^2 > \overline{\mathbf{m}}^1$, where $\overline{\mathbf{m}}^2(p) = \overline{\mathbf{m}}^1(p), \forall p \in (\Pi - \{\beta_i\}_{i=1}^n)$, and $\overline{\mathbf{m}}^2(\beta_i) \geq \overline{\mathbf{m}}^1(p_i)$, for each $p_i \in \Pi_1$. At the marking $\overline{\mathbf{m}}^2$, the uncontrollable transitions in the set $\{\epsilon_i\}_{i=1}^n$ can fire as often as necessary to empty all places in the set $\{p_i\}_{i=1}^n$. Consequently, there can be no LESP for $N(\overline{\mathbf{m}}^2)$, and $\overline{\mathbf{m}}^2 \notin \Delta(N)$ while $\overline{\mathbf{m}}^1 \in \Delta(N)$. Therefore, if $\Delta(N) \neq \emptyset$, it cannot be right-closed.

($\Leftarrow$) By definition, $(\Delta(N) = \emptyset) \Rightarrow (\Delta(N)$ is right-closed). □

Observation 3: Let $\underline{\mathbf{m}} \geq \overline{\mathbf{m}}$, then $(\Delta(\widetilde{N}) \neq \emptyset) \Leftrightarrow (\underline{\mathbf{m}} \in \Delta(\widetilde{N}))$.

Proof. ($\Rightarrow$) By Observations 1 and 2, $\Delta(\widetilde{N}) \neq \emptyset$ if and only if $\overline{\mathbf{m}} \in \Delta(N)$. Assume $\widetilde{N}$ is initialized with the marking $\underline{\mathbf{m}} \geq \overline{\mathbf{m}}$. We define a supervisory policy $\widetilde{\mathcal{P}}^1$ as follows. For $\underline{\mathbf{m}} \in \mathcal{N}^{card(\widetilde{\Pi})}, \widetilde{t} \in \widetilde{T}$

$$\widetilde{\mathcal{P}}^1(\underline{\mathbf{m}}, \widetilde{t}) = \begin{cases} 1 & \text{if } \widetilde{t} \in (\widetilde{T} - \{t_{m+1}\}), \\ 0 & \text{iff } (\widetilde{t} = t_{m+1}) \wedge (\underline{\mathbf{m}} \neq \overline{\mathbf{m}}), \\ \widetilde{\mathcal{P}}(\overline{\mathbf{m}}, \widetilde{t}) & \text{iff } (\widetilde{t} = t_{m+1}) \wedge (\underline{\mathbf{m}} = \overline{\mathbf{m}}). \end{cases}$$

The marking $\overline{\mathbf{m}}$ is reachable from all markings in $\Re(\widetilde{N}, \underline{\mathbf{m}}, \widetilde{\mathcal{P}}^1)$, and $\overline{\mathbf{m}} \in \Delta(\widetilde{N})$. Once the PN reaches the marking $\overline{\mathbf{m}}$, we switch to the supervisory policy $\widetilde{\mathcal{P}}$ as defined in Observation 2. Therefore, $\forall t \in \widetilde{T}, \forall \mathbf{m}^i \in \Re(N, \underline{\mathbf{m}}, \widetilde{\mathcal{P}}^1), \exists \mathbf{m}^j \in \Re(N, \mathbf{m}^i, \widetilde{\mathcal{P}}^1)$ such that $t \in T_e(N, \mathbf{m}^j)$ and $\widetilde{\mathcal{P}}^1(\mathbf{m}^j, t) = 1$. Thus, $\underline{\mathbf{m}} \in \Delta(\widetilde{N})$.

($\Leftarrow$) Straightforward by definition. □

Theorem 6: There is an MM-LESP for $N(\mathbf{m}^0)$ if and only if $\exists \widehat{\Delta}(N) \subseteq \Delta(N)$, such that

1. $\mathbf{m}^0 \in \widehat{\Delta}(N)$,

2. $\widehat{\Delta}(N)$ is control invariant with respect to N,

3. $\widehat{\Delta}(N)$ is right-closed, and

4. $\forall \mathbf{m}^i \in \min(\widehat{\Delta}(N))$, $G(N(\mathbf{m}^i), \mathcal{P})$ satisfies the path requirement. That is, $\forall \mathbf{m}^i \in \min(\widehat{\Delta}(N))$, there is a path $v_0 \xrightarrow{\sigma_1} v_1 \xrightarrow{\sigma_2} v_1$, in the coverability graph $G(N(\mathbf{m}^i), \mathcal{P}) = (V, A)$, such that $\mathbf{x}(\sigma_2) \geq \mathbf{1}$ and $\mathbf{C}\mathbf{x}(\sigma_2) \geq \mathbf{0}$, where $\mathbf{1}$ is the m-dimensional vector of all ones, $\mathcal{P}$ ensures the reachable markings never leaves $\widehat{\Delta}(N)$.

Proof. (*Only If*) Let $\widehat{\Delta}(N) = \Delta_M(N)$. Since there is an MM-LESP for $N(\mathbf{m}^0)$, it follows that $\mathbf{m}^0 \in \widehat{\Delta}(N)$. By definition, $\widehat{\Delta}(N)$ $(= \Delta_M(N))$ is right-closed. Suppose $\mathbf{m}^1 \in \widehat{\Delta}(N)$ and $\mathbf{m}^1 \xrightarrow{t_u} \mathbf{m}^2$ for some $t_u \in T_u$, then it must be that $\mathbf{m}^2 \in \widehat{\Delta}(N)$ $(= \Delta_M(N))$, as well. Otherwise, the supervisory policy will not be an MM-LESP for $\mathbf{m}^2$. Therefore, $\widehat{\Delta}(N)$ is control invariant with respect to N. In fact, using the same argument, it must be true that the supervisory policy disables any controllable transitions that result in a marking that is not in the set $\widehat{\Delta}(N)$. The supervisory policy $\mathcal{P}$ that ensures the reachable marking never leaves $\widehat{\Delta}(N) = \Delta_M(N)$ is an MM-LESP for $N(\mathbf{m}^0)$. From lemma 5.13, [35], we note that the path-requirement of Theorem 6 is satisfied, as well.

(*If*) Suppose there is a right-closed, control invariant subset $\widehat{\Delta}(N) \subseteq \Delta(N)$, such that $\mathbf{m}^0 \in \widehat{\Delta}(N)$ and each minimal element in $\min(\widehat{\Delta}(N))$ satisfies the path requirement addressed in Theorem 6. We consider a supervisory policy $\mathcal{P}$ for $N(\mathbf{m}^0)$, which prevents any controllable transition whose firing will take the marking outside $\widehat{\Delta}(N)$, and show that $\mathcal{P}$ is a marking-monotone LESP.

Suppose there exists an $\mathbf{m} \in \mathfrak{R}(N, \mathbf{m}^0, \mathcal{P})$ and $t \in T$ such that $\mathcal{P}(\mathbf{m}, t) = 1$. Since this supervisory policy prevents a controllable transition if and only if its firing takes the marking outside $\widehat{\Delta}(N)$, it implies that $\exists \mathbf{m}^j \in \min(\widehat{\Delta}(N))$ such that $\max\{\mathbf{m}, \mathbf{IN}_t\} + \mathbf{C} \times \mathbf{1}_t \geq \mathbf{m}^j$. Now consider all markings larger than $\mathbf{m}$. For all $\widehat{\mathbf{m}} \geq \mathbf{m}, \max\{\widehat{\mathbf{m}}, \mathbf{IN}_t\} + \mathbf{C} \times \mathbf{1}_t \geq \max\{\mathbf{m}, \mathbf{IN}_t\} + \mathbf{C} \times \mathbf{1}_t \geq \mathbf{m}^j$. Since the markings are in $\widehat{\Delta}(N)$ after the firing of t from all $\widehat{\mathbf{m}} \geq \mathbf{m}$, we have $\mathcal{P}(\widehat{\mathbf{m}}, t) = 1$. Hence the supervisory policy is marking-monotone.

Since $\widehat{\Delta}(N)$ is control-invariant with respect to N, and its minimal elements satisfy the path-requirement, there exists an LESP for all markings in $\widehat{\Delta}(N)$ (Theorem 5.1 in [33]). On the other hand, the right-closure property of $\widehat{\Delta}(N)$ indicates that if $\mathbf{m}^0 \in \widehat{\Delta}(N)$ then $\forall \widehat{\mathbf{m}}^0 \geq \mathbf{m}^0, \widehat{\mathbf{m}}^0 \in \widehat{\Delta}(N)$, as well. Thus, $\mathcal{P}$ enforces liveness for $N(\widehat{\mathbf{m}}^0)$, for any $\widehat{\mathbf{m}}^0 \geq \mathbf{m}^0$. Therefore, the policy is a marking-monotone LESP. □

A.2 LESPs for arbitrary Petri Nets with Partial Marking Observation and Controllability Faults

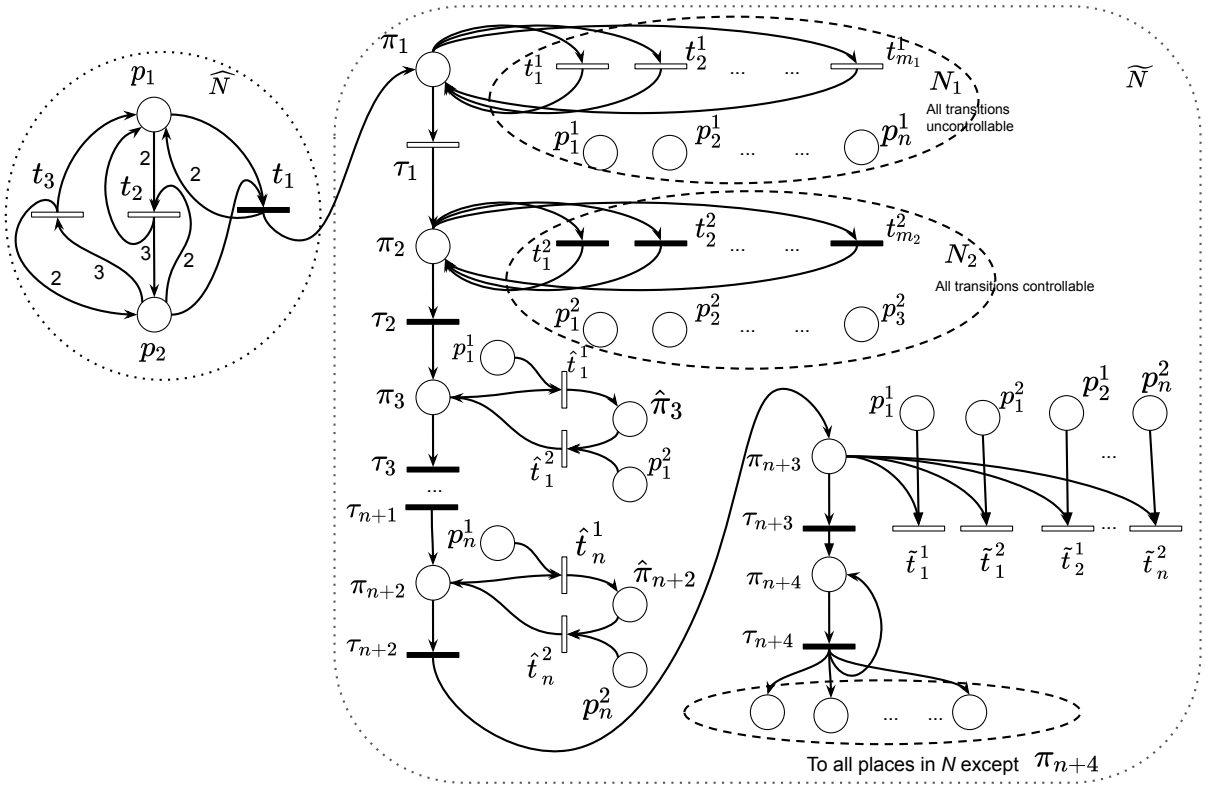


Figure A.1: A graphical illustration of the construction of the PN N using the PNs $\widehat{N}$ and $\widetilde{N}$

We construct a PN N from a PN $\widehat{N}$, and the PN $\widetilde{N}$ which was first discussed in [33]. The construction is shown in Figure A.1. $\widehat{N}$ is exactly as constructed in the figure with places $\{p_i\}_{i=1}^{2}$ and transitions $\{t_j\}_{j=1}^{3}$. Its reachability graph is shown in Figure A.2. $\widetilde{N}$ is constructed by connecting two arbitrary petri nets $N_l = (\Pi_l, T_l, \Phi_l, \Gamma_l)$ $(l = 1, 2)$. $\Pi_l = \{p_1^l, p_2^l, \ldots, p_n^l\}$ and $T_l = \{t_1^l, t_2^l, \ldots, t_{m_l}^l\}$ $(l = 1, 2)$ is the set of places and transitions respectively. Note that $card(\Pi_1) = card(\Pi_2) = n$. All transitions in N_1 (N_2) are uncontrollable (resp. controllable). Note that the arcs for N_1 and N_2 are not drawn in Figure A.1 since we do not stipulate any particular structure. $\widetilde{N} = (\widetilde{\Pi}, \widetilde{T}, \widetilde{\Phi}, \widetilde{\Gamma})$ is constructed as follows:

- $\widetilde{\Pi} \leftarrow \Pi_1 \cup \Pi_2$, $\widetilde{T} \leftarrow T_1 \cup T_2$ and $\widetilde{\Phi} \leftarrow \Phi_1 \cup \Phi_2$.
- Create $2n + 4$ new and unused places such that $\widetilde{\Pi} \leftarrow \widetilde{\Pi} \cup \{\pi_i\}_{i=1}^{n+4} \cup \{\widetilde{\pi}_j\}_{j=3}^{n+2}$.
- Create $5n + 4$ new and unused transitions: $\widetilde{T} \leftarrow \widetilde{T} \cup \{\tau_i\}_{i=1}^{n+4} \cup \{\hat{\tau}_j^i | i \in \{1, 2\}, j \in \{1, 2, \ldots, n\}\} \cup \{\widetilde{\tau}_j^i | i \in \{1, 2\}, j \in \{1, 2, \ldots, n\}\}$.

- $\forall t \in T_1$, modify $\widetilde{\Phi}$ as $\widetilde{\Phi} \leftarrow \widetilde{\Phi} \cup \{(\pi_1, t), (t, \pi_1)\}$. That is, π_1 self loops on all transitions of $\widetilde{N}$ that originally belonged to N_1.
- $\forall t \in T_2$, modify $\widetilde{\Phi}$ as $\widetilde{\Phi} \leftarrow \widetilde{\Phi} \cup \{(\pi_2, t), (t, \pi_2)\}$. That is, π_2 self loops on all transitions of $\widetilde{N}$ that originally belonged to N_2.
- Modify $\widetilde{\Phi}$ as $\widetilde{\Phi} \leftarrow \widetilde{\Phi} \cup \{(\pi_i, \tau_i), (\tau_i, \pi_{i+1})\}_{i=1}^{n+3} \cup \{(\pi_{n+4}, \tau_{n+4})\}$.
- $\forall p \in \widetilde{\Pi}$, modify $\widetilde{\Phi}$ as $\widetilde{\Phi} \leftarrow \widetilde{\Phi} \cup \{(\tau_{n+4}, p)\}$. That is every place of $\widetilde{N}$ is an output of τ_{n+4}.
- $\forall i \in \{1, 2, \ldots, n\}$, modify $\widetilde{\Phi}$ as $\widetilde{\Phi} \leftarrow \widetilde{\Phi} \cup \{(\pi_{i+2}, \hat{\tau}_i^1),\ (p_i^1, \hat{\tau}_i^1),\ (\hat{\tau}_i^1, \hat{\pi}_{i+3}),\ (\hat{\pi}_{i+3}, \hat{\tau}_i^2),\ (p_i^2, \hat{\tau}_i^2),\ (\hat{\tau}_i^2, \pi_{i+2})\}$.
- $\forall i \in \{1, 2\}, \forall j \in \{1, 2, \ldots n\}$, modify $\widetilde{\Phi}$ as $\widetilde{\Phi} \leftarrow \widetilde{\Phi} \cup \{(\pi_{n+3}, \widetilde{\tau}_j^i), (p_j^i, \widetilde{\tau}_j^i)\}$.

Weights of all arcs in $\widetilde{\Phi} - \Phi_1 - \Phi_2$ is one. We use $\mathbf{m}_i^0 \in \mathcal{N}^n$ to represent an arbitrary pair of initial markings of N_i, $i = \{1, 2\}$. The initial marking of $\widetilde{N}$, $\widetilde{\mathbf{m}}_0$, is such that $\widetilde{\mathbf{m}}_0(\pi_1) = 1$, $\widetilde{\mathbf{m}}_0(\Pi_1) = \mathbf{m}_1^0$, $\widetilde{\mathbf{m}}_0(\Pi_2) = \mathbf{m}_2^0$ and all other places have zero tokens. Theorem 5.3 of [33] provides a detailed proof that $\widetilde{N}$ has an LESP if and only if $\mathfrak{R}(N_1, \mathbf{m}_1^0) \subseteq \mathfrak{R}(N_2, \mathbf{m}_2^0)$. We briefly discuss the idea of the proof for completeness. Liveness of transition τ_1 can be guaranteed iff the token load of π_1 is repeatedly replenished. But since the initial marking is such that $\widetilde{\mathbf{m}}_0(\pi_1) = 1$, ${}^\bullet\pi_1 = \{\tau_{n+4}\}$ and $\widetilde{\mathbf{m}}^0(\pi_{n+4}) = 0$, the token load of π_1 can be repeatedly replenished iff the single token at π_1 at the initial marking is safely passed on to π_{n+4}. In fact, $\widetilde{N}$ is live once a token is placed in π_{n+4} as $\tau_{n+4}^\bullet = \widetilde{\Pi}$. Therefore, the presence of a token in π_{n+4} is a necessary and sufficient condition for liveness of $\widetilde{N}$. Now the token can reach π_{n+4} if and only if it is not lost at π_{n+3} by firing of the transitions $\widetilde{\tau}_j^i$, ($i = 1, 2$ and $j = 1, 2, \ldots n$). The firing of $\widetilde{\tau}_j^i$ can be prevented iff all places in N_1 and N_2 are empty, that is, $\{p_i^j\}_{j=1}^n = 0$ for $i = 1, 2$ and $j = 1, 2, \ldots n$. Now, places $\{p_i^j\}_{j=1}^n$ can be emptied by the firing of transitions $\widehat{\tau}_j^i$ for $i = 1, 2$ and $j = 1, 2, \ldots n$. But emptying of all $\{p_i^j\}_{j=1}^n$ is possible if and only if $N_1(\mathbf{m}_1^0)$ and $N_2(\mathbf{m}_2^0)$ reach the exact same marking, which is true iff $\mathfrak{R}(N_1, \mathbf{m}_1^0) \subseteq \mathfrak{R}(N_2, \mathbf{m}_2^0)$. To see this note that the places π_1 and π_2 act as enable places for PNs N_1 and N_2 respectively. From the initial marking, N_1 can reach any marking in $\mathfrak{R}(N_1, \mathbf{m}_1^0)$ till the firing of uncontrollable transition τ_1 which removes one token from π_1 and populates π_2. Since τ_2 and all transitions in N_2 are controllable, N_2 can be steered to any marking in $\mathfrak{R}(N_2, \mathbf{m}_2^0)$. Therefore, $N_1(\mathbf{m}_1^0)$ and $N_2(\mathbf{m}_2^0)$ can reach the exact same marking iff $\mathfrak{R}(N_1, \mathbf{m}_1^0) \subseteq \mathfrak{R}(N_2, \mathbf{m}_2^0)$. The reachability inclusion problem is undecidable for arbitrary PNs [34]. Therefore, determining the existence of an LESP for $\widetilde{N}$ is undecidable.

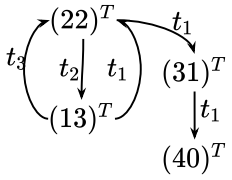


Figure A.2: Reachability graph of $\widehat{N}$ with initial marking $(2\ 2)^T$

We construct the PN $N = (\Pi, T, \Phi, \Gamma)$ with initial marking $\mathbf{m}_0$, from $\widehat{N}$ and $\widetilde{N}$ (see Figure A.1) as: $\Pi \leftarrow \hat{\Pi} \cup \widetilde{\Pi}$; $T \leftarrow \hat{T} \cup \widetilde{T}$; $\Phi \leftarrow \hat{\Phi} \cup \widetilde{\Phi} \cup (t_1, \pi_1) \cup (\tau_{n+4}, p_1) \cup (\tau_{n+4}, p_2)$; and, $\mathbf{m}_0(p_1) = \mathbf{m}_0(p_2) = 2$, $\mathbf{m}_0(\widetilde{\Pi}) = \widetilde{\mathbf{m}}_0$.

Observation 15. *The following statements are equivalent: (a) N is live; (b) $\widetilde{N}$ is live; and (c) $\widehat{N}$ is live.*

Proof. (a) $\Rightarrow$ (b) and (a) $\Rightarrow$ (c) follows from the definition of liveness.

The firing of transition t_1 places a token in π_1 without affecting the marking of $\widehat{N}$. If $\widehat{N}$ is live, then the token in π_1 is repeatedly replenishable. Therefore, the marking with a token in place π_{n+4} is reachable from every marking that is reachable from the initial marking thereby guaranteeing the liveness of the subnet $\widetilde{N}$. Hence (c) $\Rightarrow$ (b). From this, it follows that N is live and we have (c) $\Rightarrow$ (a)

$\widetilde{N}$ is live implies that a marking that places a token in π_{n+4} is reachable from every marking that is reachable from the initial marking. Liveness of subnet $\widehat{N}$ follows from the observation that $\{p_1, p_2\} \in \tau_{n+4}^{\bullet}$. Therefore, (b) $\Rightarrow$ (c). □

Observation 16. *$\mathcal{P}'$ is an LESP for $N(\mathbf{m}_0)$, where:*

$$\mathcal{P}'(\mathbf{m}, t) = \begin{cases} 1 & \text{if } (t = t_1) \wedge (\mathbf{m}(p_1) = 1) \wedge (\mathbf{m}(p_2) = 3) \\ 0 & \text{if } (t = t_1) \wedge (\mathbf{m}(p_1) \neq 1 \vee \mathbf{m}(p_2) \neq 3) \\ 1 & \text{if } t \in T - \{t_1\} \end{cases}$$

Proof. That $\mathcal{P}'$ is an LESP for $\widehat{N}((2\ 2)^T)$ is clear from the reachability graph in Figure A.2. From Observation 15, $\mathcal{P}'$ is an LESP for $N(\mathbf{m}_0)$. □

$\mathcal{P}'$ enforces liveness in N by making the subnet $\widehat{N}$ live. Suppose $k_r = 1$ and $T_f = \{t_1\}$. If the fault-event ϕ occurs at a marking $\mathbf{m} \in \mathfrak{R}(N, \mathbf{m}_0, \mathcal{P}')$ when $\mathbf{m}(p_1) = 2$ and $\mathbf{m}(p_2) = 2$, then an unintended firing of the affected transition t_1 will take the subnet $\widehat{N}$ to the marking $(3\ 1)^T$ following which the policy $\mathcal{P}'$ does not enforce liveness in the presence of faults. In fact, it is easy to see from the reachability graph that there does not exist an FT-LESP for $\widehat{N}$ for initial marking $(2\ 2)^T$, $k_r = 1$ and $T_f = \{t_1\}$. By construction, the only way to make

$N(\mathbf{m}_0)$ live in the presence of faults for $k_r = 1$ and $T_f = \{t_1\}$ is by synthesizing an LESP for $\widetilde{N}$.

Observation 17. *There exists a Π_0-LESP for $N(\mathbf{m}_0)$ for $\Pi_0 = \widetilde{\Pi}$ if and only if there exists an LESP for $\widetilde{N}$.*

Observation 18. *There exists an FT-LESP for $N(\mathbf{m}_0)$ for $k_r = 1$ and $T_f = \{t_1\}$ if and only if there exists an LESP for $\widetilde{N}$.*

As proved in Theorem 5.3 of [33], the existence of an LESP for $\widetilde{N}$ is undecidable due to the undecidability of the reachability inclusion problem.
Theorems 20 and 16: *Given an LESP for an arbitrary PN $\overline{N}(\mathbf{m}_0)$:*

1. *the existence of an FT-LESP for a given set T_f and a given value of k_r is undecidable.*

2. *the existence of a Π_0-LESP for a given Π_0 is undecidable.*

Proof. Suppose for contradiction that there exists an algorithm $\mathcal{A}_f$ that takes the PN structure $\overline{N}(\mathbf{m}_0)$, the set T_f and the value of k_r (respectively the set Π_0) as inputs and outputs *yes* if and only if $\mathbf{m}_0 \in \Delta_{k_r}(N)$ (resp. $\mathbf{m}_0 \in \Delta_{\Pi_0}(N)$). Then for inputs $N(\mathbf{m}_0)$ (as in the construction), $T_f = \{t_1\}$ and $k_r = 1$ (resp. $\widetilde{\Pi}$) the algorithm $\mathcal{A}_f$ can be used to decide if $\mathfrak{R}(N_1, \mathbf{m}_1^0) \subseteq \mathfrak{R}(N_2, \mathbf{m}_2^0)$ for arbitrary PNs N_1 and N_2, which is an undecidable problem. □

REFERENCES

[1] T.-C. Au, N. Shahidi, and P. Stone, "Enforcing liveness in autonomous traffic management," in *Twenty-Fifth AAAI Conference on Artificial Intelligence*, 2011.

[2] "Sols 2649-2652: Curiosity loses its attitude," Jan. 2020. [Online]. Available: https://mars.nasa.gov/msl/mission-updates/8587/sols-2649-2652-curiosity-loses-its-attitude/

[3] B. Alpern and F. B. Schneider, "Defining liveness," *Information processing letters*, vol. 21, no. 4, pp. 181–185, 1985.

[4] D. Osherson, M. Stob, and S. Weinstein, *Systems that Learn: An Introduction to Learning Theory for Cognitive and Computer Scientists*. Cambridge, MA: The MIT Press, 1986.

[5] B. Alpern and F. B. Schneider, "Recognizing safety and liveness," *Distributed computing*, vol. 2, no. 3, pp. 117–126, 1987.

[6] S. Eilenberg, *Automata, languages, and machines*. Academic press, 1974.

[7] P. J. Ramadge and W. M. Wonham, "The control of discrete event systems," *Proceedings of the IEEE*, vol. 77, no. 1, pp. 81–98, 1989.

[8] C. G. Cassandras and S. Lafortune, *Introduction to discrete event systems*. Springer Science & Business Media, 2009.

[9] P. A. Abdulla, K. Cerans, B. Jonsson, and Y.-K. Tsay, "General decidability theorems for infinite-state systems," in *Proceedings 11th Annual IEEE Symposium on Logic in Computer Science*. IEEE, 1996, pp. 313–321.

[10] A. Finkel and P. Schnoebelen, "Well-structured transition systems everywhere!" *Theoretical Computer Science*, vol. 256, no. 1-2, pp. 63–92, 2001.

[11] W. Fokkink, *Introduction to process algebra*. springer science & Business Media, 2013.

[12] J. L. Peterson, *Petri net theory and the modeling of systems*. Prentice Hall PTR, 1981.

[13] D. Brand and P. Zafiropulo, "On communicating finite-state machines," *Journal of the ACM (JACM)*, vol. 30, no. 2, pp. 323–342, 1983.

[14] G. Ciardo, "Petri nets with marking-dependent arc cardinality: Properties and analysis," in *International Conference on Application and Theory of Petri Nets*. Springer, 1994, pp. 179–198.

[15] C. Dufourd, A. Finkel, and P. Schnoebelen, "Reset nets between decidability and undecidability," in *International Colloquium on Automata, Languages, and Programming*. Springer, 1998, pp. 103–115.

[16] B. Heinemann, "Subclasses of self-modifying nets," in *Application and Theory of Petri Nets*. Springer, 1982, pp. 187–192.

[17] R. Valk, "Self-modifying nets, a natural extension of petri nets," in *International Colloquium on Automata, Languages, and Programming*. Springer, 1978, pp. 464–476.

[18] J. L. Peterson et al., "A note on colored petri nets," *Inf. Process. Lett.*, vol. 11, no. 1, pp. 40–43, 1980.

[19] A. Giua, "Petri nets as discrete event models for supervisory control," *Rensselaer Polytechnic Institute, Troy, NY*, 1992.

[20] J. O. Moody and P. J. Antsaklis, *Supervisory control of discrete event systems using Petri nets*. Springer Science & Business Media, 2012, vol. 8.

[21] M. Iordache and P. J. Antsaklis, *Supervisory control of concurrent systems: a Petri net structural approach*. Springer Science & Business Media, 2007.

[22] S. A. Reveliotis, E. Roszkowska, and J. Y. Choi, "Generalized algebraic deadlock avoidance policies for sequential resource allocation systems," *IEEE Transactions on Automatic Control*, vol. 52, no. 12, pp. 2345–2350, 2007.

[23] A. Ghaffari, N. Rezg, and X. Xie, "Design of a live and maximally permissive petri net controller using the theory of regions," *IEEE transactions on robotics and Automation*, vol. 19, no. 1, pp. 137–141, 2003.

[24] O. Marchetti and A. Munier-Kordon, "A sufficient condition for the liveness of weighted event graphs," *European Journal of Operational Research*, vol. 197, no. 2, pp. 532–540, 2009.

[25] F. Basile, L. Recalde, P. Chiacchio, and M. Silva, "Closed-loop live marked graphs under generalized mutual exclusion constraint enforcement," *Discrete Event Dynamic Systems*, vol. 19, no. 1, pp. 1–30, 2009.

[26] F. Basile, R. Cordone, and L. Piroddi, "Integrated design of optimal supervisors for the enforcement of static and behavioral specifications in petri net models," *Automatica*, vol. 49, no. 11, pp. 3432–3439, 2013.

[27] J. Luo and K. Nonami, "Approach for transforming linear constraints on petri nets," *IEEE Transactions on Automatic Control*, vol. 56, no. 12, pp. 2751–2765, 2011.

[28] A. Dideban and H. Alla, "Reduction of constraints for controller synthesis based on safe petri nets," *Automatica*, vol. 44, no. 7, pp. 1697–1706, 2008.

[29] F. Tricas, F. Garcia-Valles, J. M. Colom, and J. Ezpeleta, "A petri net structure-based deadlock prevention solution for sequential resource allocation systems," in *Proceedings of the 2005 IEEE international conference on robotics and automation.* IEEE, 2005, pp. 271–277.

[30] R. Cordone, A. Nazeem, L. Piroddi, and S. Reveliotis, "Designing optimal deadlock avoidance policies for sequential resource allocation systems through classification theory: existence results and customized algorithms," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2772–2787, 2013.

[31] Y. Chen and Z. Li, "Design of a maximally permissive liveness-enforcing supervisor with a compressed supervisory structure for flexible manufacturing systems," *Automatica*, vol. 47, no. 5, pp. 1028–1034, 2011.

[32] H. Hu, M. Zhou, Z. Li, and Y. Tang, "Deadlock-free control of automated manufacturing systems with flexible routes and assembly operations using petri nets," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 109–121, 2012.

[33] R. S. Sreenivas, "On the existence of supervisory policies that enforce liveness in discrete-event dynamic systems modeled by controlled petri nets," *IEEE Transactions on Automatic Control*, vol. 42, no. 7, pp. 928–945, 1997.

[34] M. H. T. Hack, "Decidability questions for petri nets." Ph.D. dissertation, Massachusetts Institute of Technology, 1976.

[35] R. Sreenivas, "On the existence of supervisory policies that enforce liveness in partially controlled free-choice petri nets," *IEEE Transactions on Automatic Control*, vol. 57, no. 2, pp. 435–449, 2012.

[36] N. Somnath and R. Sreenivas, "On deciding the existence of a liveness enforcing supervisory policy in a class of partially controlled general free-choice petri nets," *IEEE Transactions on Automation Science and Engineering*, vol. 10, no. 4, pp. 1157–1160, 2013.

[37] E. Salimi, N. Somnath, and R. Sreenivas, "A software tool for live-lock avoidance in systems modelled using a class of petri nets," *International Journal of Computer Science, Engineering and Applications*, vol. 5, no. 2, pp. 1–13, April 2015.

[38] R. Sreenivas, "On a decidable class of partially controlled petri nets with liveness enforcing supervisory policies," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 43, no. 5, pp. 1256–1261, 2013.

[39] R. S. Sreenivas and B. H. Krogh, "On petri net models of infinite state supervisors," *IEEE transactions on Automatic Control*, vol. 37, no. 2, pp. 274–277, 1992.

[40] R. M. Karp and R. E. Miller, "Parallel program schemata," *Journal of Computer and system Sciences*, vol. 3, no. 2, pp. 147–195, 1969.

[41] M. P. Cabasino, A. Giua, and C. Seatzu, "Identification of unbounded petri nets from their coverability graph," in *Proceedings of the 45th IEEE Conference on Decision and Control*. IEEE, 2006, pp. 434–440.

[42] K. Schmidt, "Model-checking with coverability graphs," *Formal Methods in System Design*, vol. 15, no. 3, pp. 239–254, 1999.

[43] A. Giua and C. Seatzu, "Observability of place/transition nets," *IEEE Transactions on Automatic Control*, vol. 47, no. 9, pp. 1424–1437, 2002.

[44] M. V. Iordache and P. J. Antsaklis, "Supervision based on place invariants: A survey," *Discrete Event Dynamic Systems*, vol. 16, no. 4, pp. 451–492, 2006.

[45] L. E. Holloway, B. H. Krogh, and A. Giua, "A survey of petri net methods for controlled discrete event systems," *Discrete Event Dynamic Systems*, vol. 7, no. 2, pp. 151–190, 1997.

[46] F.-S. Hsieh, "Fault-tolerant deadlock avoidance algorithm for assembly processes," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 34, no. 1, pp. 65–79, 2004.

[47] M. Lawley and W. Sulistyono, "Robust supervisory control policies for manufacturing systems with unreliable resources," *IEEE Transactions on Robotics and Automation*, vol. 18, no. 3, pp. 346–359, 2002.

[48] F.-S. Hsieh, "Robustness of deadlock avoidance algorithms for sequential processes," *Automatica*, vol. 39, no. 10, pp. 1695–1706, 2003.

[49] F.-S. Hsieh, "Reconfigurable fault tolerant deadlock avoidance controller synthesis for assembly production processes," in *Systems, Man, and Cybernetics, 2000 IEEE International Conference on*, vol. 4. IEEE, 2000, pp. 3045–3050.

[50] S. Wang, S. Chew, and M. Lawley, "Using shared-resource capacity for robust control of failure-prone manufacturing systems," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 38, no. 3, pp. 605–627, 2008.

[51] S. Reveliotis and Z. Fei, "Robust deadlock avoidance for sequential resource allocation systems with resource outages," *IEEE Transactions on Automation Science and Engineering*, vol. 14, no. 4, pp. 1695–1711, 2017.

[52] Y. Feng, K. Xing, Z. Gao, and Y. Wu, "Transition cover-based robust petri net controllers for automated manufacturing systems with a type of unreliable resources," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 47, no. 11, pp. 3019–3029, 2017.

[53] G. Liu, P. Li, Z. Li, and N. Wu, "Robust deadlock control for automated manufacturing systems with unreliable resources based on petri net reachability graphs," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2018.

[54] L. Li, C. Hadjicostis, and R. Sreenivas, "Designs of bisimilar petri net controllers with fault tolerance capabilities," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 38, no. 1, pp. 207–217, 2008.

[55] J. B. Kruskal, "The theory of well-quasi-ordering: A frequently discovered concept," *Journal of Combinatorial Theory, Series A*, vol. 13, no. 3, pp. 297–305, 1972.

[56] T. Murata, "Petri nets: Properties, analysis and applications," *Proceedings of the IEEE*, vol. 77, no. 4, pp. 541–580, 1989.

[57] A. Giua and F. DiCesare, "Blocking and controllability of petri nets in supervisory control," *IEEE Transactions on Automatic Control*, vol. 39, no. 4, pp. 818–823, 1994.

[58] P. J. Ramadge and W. M. Wonham, "Modular feedback logic for discrete event systems," *SIAM Journal on Control and Optimization*, vol. 25, no. 5, pp. 1202–1218, 1987.

[59] A. Giua and F. DiCesare, "Supervisory design using petri nets," in *Proceedings of the 30th IEEE Conference on Decision and Control*. IEEE, 1991, pp. 92–97.

[60] A. Raman and R. Sreenivas, "Sequential synthesis of supervisory policies for discrete-event systems modeled by petri nets," in *Proceedings of the 2019 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Bari, Italy*. IEEE, October 2019.

[61] S. Chandrasekaran, N. Somnath, and R. Sreenivas, "A software tool for the automatic synthesis of minimally restrictive liveness enforcing supervisory policies for a class of general petri net models of manufacturing-and service-systems," *Journal of Intelligent Manufacturing*, vol. 26, no. 5, pp. 945–958, 2015.

[62] C. Chen, A. Raman, H. Hu, and R. S. Sreenivas, "On liveness enforcing supervisory policies for arbitrary petri nets," *to appear, IEEE Transactions on Automatic Control*, circa December 2020.

[63] C. Reutenauer, *The mathematics of Petri nets*. Prentice-Hall, Inc., 1990.

[64] V. Deverakonda and R. Sreenivas, "On a sufficient information structure for supervisory policies that enforce liveness in a class of general petri nets," *IEEE Transactions on Automatic Control*, vol. 60, no. 7, pp. 1915–1921, 2015.