An approach to determine controllability of monolithic supervisors

Ziyue Ma, Zhiwu Li, and Alessandro Giua

August 24, 2014

Abstract

In this paper we study the problem of supervisory design using Petri nets. We consider a monolithic supervisor candidate, i.e., a net obtained by concurrent composition of plant and specification, and we say that the control problem has an OR-AND GMEC solution if the set of the legal markings of such a net can be described by a disjunction/conjunctions of linear constraints. We derive some sufficient conditions, based on the boundedness of some places of the net, for the existence of such a solution.

Published as:

[Z. Y. Ma, Z. W. Li, A. Giua, "An approach to determine controllability of monolithic supervisors," 19th IFAC World Congress (Cape Town, South Africa), August 24-29, 2014.]
DOI: 10.3182/20140824-6-ZA-1003.01888.

Z. Ma is with the School of Electro-Mechanical Engineering, Xidian University, Xi'an 710071, China (e-mail: maziyue@gmail.com), and also with Dipartimento di Ingegneria Elettrica ed Elettronica, Università degli Studi di Cagliari, Cagliari 09123, Italy.

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

A. Giua is with Aix Marseille Université, CNRS, ENSAM, Université de Toulon, LSIS UMR 7296, Marseille 13397, France (e-mail: alessandro.giua@lsis.org), and also with Dipartimento di Ingegneria Elettrica ed Elettronica, Università degli Studi di Cagliari, Cagliari 09123, Italy (e-mail: giua@diee.unica.it).

1 Introduction

Supervisory Control Theory, originally proposed by [1], is considered as one of the most successful approaches for the control of discrete event systems. A supervisor runs parallel with the plant and at each step, computes a suitable control input to ensure that the behavior of the plant in closed loop satisfies a given specification.

Petri nets have been used as models for supervisory control since the early 90's. They extends the class of control problems that can be solved by automata and provide many efficient and well founded approaches for supervisory control [2]. In particular several interesting results, have been obtained when the desired behavior of the plant is described by state specification: in this case efficient algorithms exists to compute a controller even in the presence of uncontrollable transition: we recall in this context the work of [3–9].

In comparison, relatively few works have discussed how Petri net models may be used to design supervisors for language specifications. We consider the monolithic supervisory design that requires: (a) to construct a *monolithic supervisor candidate* (MSC) by the concurrent composition of the plant with the specification, to check this structure for controllability and nonblockingness, and eventually to refine it. The concurrent composition is particularly suited to Petri nets [10] because in this case its complexity depends on the size of the net structure, and not on the size of its state space. However, the resulting MSC is not always trim, e.g., it may require further modifications to make sure it is *controllable* and *nonblocking*, and so far very few efficient approaches for trimming have been presented. Some authors [11] have addressed nonblockingness and the closely related *deadlock prevention* problems. Very few works, however, have addressed the *controllability* problem, because a typical brute-force approach requires to compute its entire reachability graph, which suffers from the well-known *state explosion problem*. It is known that given an unbounded MSC it may not always be possible to trim it to be controllable [12], i.e., there exists control problems where both plant and specification are Petri net but a maximally permissive Petri net supervisor does not exists. Here, we are concerned about the criteria of the trimmability, i.e., for a given MSC, is it possible to determine if it is trimmable or not?

Firstly, building on the results of [10], we review the notion of supervisory design using a recently proposed definition of controllability [13] and use it to characterize the set of legal and weakly forbidden markings of a MSC.

Secondly, we focus on the existence of OR-AND GMEC solutions, i.e., we study when the set of weakly uncontrollable markings can be characterized by an OR-AND of *generalized mutual exclusion constraints* (GMECs) [3]. This determination is worthwhile: under general conditions an OR-AND GMEC solution can be easily implemented by a Petri net structure [14, 15] and thus the MSC can be trimmed.

In particular, for each uncontrollable transition t'_u of the plant we consider in the MSC the associated

uncontrollable subnet that contains a set of places $P'_{t'_u}$ that belong to the plant and a set of places $P''_{t'_u}$ that belong to the specification. If either of these two sets are bounded for all all uncontrollable transitions, then we show that an OR-AND GMEC solution exists.

The paper is organized in five sections. Section 2 gives the basic notion of Petri net and the supervisor. Section 3 introduces the problem. Section 4 the existence of OR-AND GMEC solution is studied. Section 5 discusses the case in which an OR-AND GMEC solution may not exist. Section 6 draws the conclusions.

2 Preliminaries

2.1 Petri Net

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

The *incidence matrix* of a net is defined by $C = Post - Pre \in \mathbb{Z}^{m\times n}$ (here $\mathbb{Z} = \{0,\pm 1,\pm 2,\ldots\}$).

For a transition $t \in T$ we define its *set of input places* as ${}^\bullet t = \{p \in P \mid Pre(p,t) > 0\}$ and its *set of output places* as $t^\bullet = \{p \in P \mid Post(p,t) > 0\}$. The notion for ${}^\bullet p$ and $p^\bullet$ are analogously defined.

A *marking* is a vector $M : P \to \mathbb{N}$ that assigns to each place of a Petri net a non-negative integer number of tokens, represented by black dots and can also be represented as a m component vector. We denote by $M(p)$ the marking of place p. A *marked net* $\langle N, M_0\rangle$ is a net N with an initial marking M_0.

A transition t is *enabled* at M if $M \geq Pre(\cdot,t)$ and may fire reaching a new marking $M' = M_0 + C(\cdot,t)$. We write $M[\sigma\rangle$ to denote that the sequence of transitions σ is enabled at M, and we write $M[\sigma\rangle M'$ to denote that the firing of σ yields M'.

Given a marked net $\langle N, M_0\rangle$ we denote by $L(N,M_0)$ the set of all sequences firable from the initial marking and by $R(N,M_0)$ the set of all markings reachable from the initial one.

A place $p \in P$ is *bounded* if there exists a $k \in \mathbb{N}$ such that $M(p) \leq k$ for all $M \in R(N,M_0)$. A set of places $X \subseteq P$ is bounded if all places in X are bounded. A marked net is bounded if all its places are bounded, i.e., P is bounded. The set $R(N,M_0)$ is finite if and only if net$\langle N, M_0\rangle$ is bounded.

A *labeled net* is a four-tuple $\langle N, M_0, E, l\rangle$ where $\langle N, M_0\rangle$ is a marked net, E is an *alphabet* and $l : T \to E$ is a *labeling function* that associates a label in E to each transition.

A labeled net is *deterministic* if for all $M \in R(N,M_0)$ and for pairs of distinct transitions t,t' such that

$M[t\rangle$ and $M[t'\rangle$ it holds $l(t) \neq l(t')$. In the following we will only consider deterministic generators.

Finally, given a net $N = (P, T, Pre, Post)$ we say that $\hat{N} = (\hat{P}, \hat{T}, \hat{Pre}, \hat{Post})$ is a subnet of N if $\hat{P} \subset P$, $\hat{T} \subset T$ and $\hat{Pre}$ (resp., $\hat{Post}$) is the restriction of Pre (resp., $Post$) to $\hat{P} \times \hat{T}$.

2.2 GMECs

A Generalized Mutual Exclusion Constraint (GMEC) is a pair $(\mathbf{w}, k)$ where $\mathbf{w} \in \mathbb{Z}^m$ and $k \in \mathbb{N}$. A GMEC defines a set of legal markings:

$$\mathscr{M}(\mathbf{w}, k) = \{M \in \mathbb{N}^m \mid \mathbf{w}^T \cdot M \leq k\}$$

An *AND GMEC* is a pair $(\mathbf{W}, \mathbf{k})_{AND}$, where $\mathbf{W} = [\mathbf{w}_1 \ \cdots \ \mathbf{w}_r] \in \mathbb{Z}^{m \times r}$ and $\mathbf{k} = [k_1 \ \cdots \ k_r]^T \in \mathbb{N}^r$. An AND GMEC defines a set of legal markings $\mathscr{M}_{AND}(\mathbf{W}, \mathbf{k}) = \{M \in \mathbb{N}^m \mid \forall i \in \{1, \ldots, r\}, \mathbf{w}_i^T \cdot M \leq k_i\}$ that is obviously *convex*.

An *OR-AND GMEC* is a set $\xi = \{(\mathbf{W}_1, \mathbf{k}_1), \ldots, (\mathbf{W}_s, \mathbf{k}_s)\}$, where $(\mathbf{W}_i, \mathbf{k}_i)$ is an AND GMEC for all $i = \{1, 2, \ldots, s\}$. This constraint defines a set of legal markings

$$\mathscr{M}_{OR-AND}(\xi) = \bigcup_{i=1}^{s} \mathscr{M}_{AND}(\mathbf{W}_i, \mathbf{k}_i).$$

For sake of simplicity in the following we denote $\mathscr{M}_{OR-AND}(\xi)$ by $\mathscr{M}(\xi)$. Finally we say that a constraint ξ is *finite* if $s < +\infty$.

3 Monolithic supervisory design and problem statement

In this section we will briefly recall the monolithic supervisory design technique for Petri with language specifications and will characterize the set of legal marking for a candidate supervisor.

3.1 Design by concurrent composition

A system to be controlled (or *plant*) will be described by a labeled net $G = \langle N', M_0', E, l' \rangle$ with $N' = \langle P', T', Pre', Post' \rangle$, while a *specification* on its behavior is described by a labeled net $H = \langle N'', M_0'', E, l'' \rangle$ with $N'' = \langle P'', T'', Pre'', Post'' \rangle$.

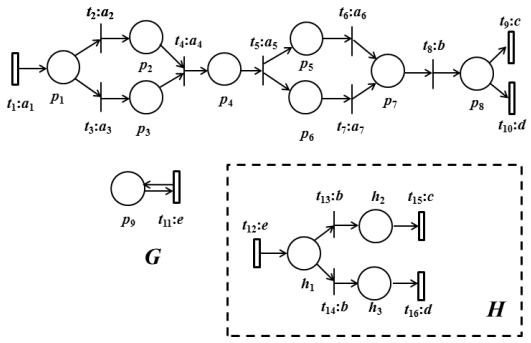

Figure 1: A plant G and a specification H.

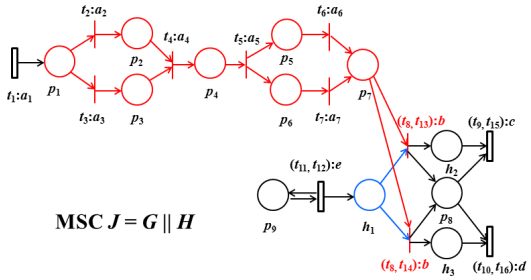

Figure 2: The monolithic candidate supervisor J obtained by concurrent composition of G and H in Figure 1.

A specification H defines a set of legal firing sequences of G given by

$$\Sigma(G,H) = \{\sigma' \in L(N',M'_0) \mid \quad (\exists \sigma'' \in L(N'',M''_0)) \\ l'(\sigma') = l''(\sigma'')\} \tag{1}$$

Assume that the event set E is partitioned into the sets of *controllable* events E_c and *uncontrollable* events E_u. This also induces a partition of the transition set T' of G into the set of controllable transitions $T'_c = \{t' \in T' \mid l'(t') \in E_c\}$ and uncontrollable transitions $T'_u = T' \setminus T_c$. A supervisor is a control agent that may disable controllable transitions to ensure that the controlled plant G only generates sequences in $\Sigma(G,H)$.

Given a plant G and a specification H, a *monolithic supervisor candidate* (MSC) is a labeled net denoted as $J = G \parallel H$ constructed by the operator of *concurrent composition*, that fuses the transitions in G and H which share the same label. Formally, we say that $J = (N, M_0, E, l)$, with $N = \langle P, T, Pre, Post \rangle$, where $P = P' \cup P''$,

$$\begin{aligned} T \quad = \quad & \{(t',t'') \mid t' \in T', t'' \in T'', l'(t') = l''(t'')\} \\ & \cup \{(t',\lambda) \mid t' \in T', (\nexists t'' \in T'') l'(t') = l''(t'')\} \\ & \cup \{(\lambda,t'') \mid t'' \in T'', (\nexists t' \in T') l'(t') = l''(t'')\}, \end{aligned}$$

$$Pre(p,t) = \begin{cases} Pre'(p,t') & \text{if } p \in P', t' \neq \lambda, t = (t',t'') \\ Pre''(p,t'') & \text{if } p \in P'', t'' \neq \lambda, t = (t',t'') \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

$$Post(p,t) = \begin{cases} Post'(p,t') & \text{if } p \in P', t' \neq \lambda, t = (t',t'') \\ Post''(p,t'') & \text{if } p \in P'', t'' \neq \lambda, t = (t',t'') \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

$l((t',t'')) = l'(t')$ if $t' \neq \lambda$ else $l((t',t'')) = l''(t'')$, and $M_0 = (M'_0, M''_0)$. Here λ denotes the empty sequence and is used to denote that a transition in G (resp., H) is not synchronized with a transition in H (resp., G). We also partition the transition set T of J into the sets of controllable transitions $T_c = \{t \in T \mid l(t) \in E_c\}$ and uncontrollable transitions $T_u = T \setminus T_c$.

An example of concurrent composition operation is given in Figure 1 where transitions of the form (t', λ) or (λ, t'') are simply denoted t' or t''; details can be found in [10].

Note we assume that the alphabet of the specification H coincide with the alphabet E of the plant G. Furthermore, without loss of generality, we assume that each label in E is assigned to at least one transition in the plant: if not we can define a new alphabet $E' \subsetneq E$ with this property. This implies that in a candidate supervisor no transition of the type (λ, t'') will be present.

3.2 Trimming a supervisor candidate

Given a sequence $\sigma = (t'_1, t''_1)(t'_2, t''_2) \cdots (t'_k, t''_k)$ of an MSC J let us denote by $\sigma_{\uparrow G} = t'_1 t'_2 \cdots t'_k$ the corresponding sequence in the plant G. It is easy to show that

$$L(N, M_0) = \{\sigma \in T^* \mid \sigma_{\uparrow G} \in \Sigma(G, H)\}$$

hence J describes the behavior of G that satisfies specification H. However, this desired behavior may not be enforceable by a supervisor.

To characterize this situation, let us recall some definitions.

Given an MSC J and an uncontrollable transition $t'_u \in T'_u$ the set of *weakly uncontrollable markings for* t'_u is[1]:

$$\begin{aligned} \mathscr{W}_J(t'_u) = \{ \quad & M = (M', M'') \in \mathbb{N}^{|P|} \mid (\exists \sigma' \in (T'_u)^*)\ M'[\sigma' t'_u\rangle_G, \\ & (\nexists \sigma \in T_u^*)\ M[\sigma\rangle_J \wedge \sigma_{\uparrow G} = \sigma' t'_u \} \end{aligned} \tag{4}$$

[1] Here $[\cdot\rangle_G$ (resp., $[\cdot\rangle_J$) denotes the enabling in G (resp., J).

and correspondingly we define the set of *weakly uncontrollable markings* of J as

$$\mathscr{W}_J = \bigcup_{t'_u \in T'_u} \mathscr{W}(t'_u) \tag{5}$$

A weakly uncontrollable marking characterizes an anomalous situation in which the plant G has reached a marking M' from which a sequence of uncontrollable transitions $\sigma' t'_u$ may fire, but that sequence is not legal. Since there is not way to prevent the firing of such uncontrollable sequence, all such markings should be avoided and correspondingly we define the set of *legal markings* as

$$\mathscr{L}_J = \mathbb{N}^{|P|} \setminus \bigcup_{t'_u \in T'_u} \mathscr{W}(t'_u). \tag{6}$$

Remark 1 *The definition of the set of weakly uncontrollable marking given in eqs.* (4) *and* (5) *is original and deserves some comments. First, we point out that it is based on the definition of uncontrollable markings proposed by [13]. This new definition corrects an imprecise definition used in previous works [10, 16] that correctly characterizes uncontrollability only for free–labeled specifications details can be found in [13]. Secondly, we remark that the set $\mathscr{W}_J$ is written as the union of the (possibly non disjoints) sets $\mathscr{W}_J(t'_u)$: the reason to do to so, will be clear in the following section when each set will be studied by means of the uncontrollable subnet associated of transition t'_u.* △

We say that J is *controllable* if $R(N,M_0) \subseteq \mathscr{L}_J$, otherwise J is said to be *uncontrollable*. It can be shown that J can be used as a supervisor for G to ensure that only sequences in $\Sigma(G,H)$ are generated if and only if $J = G \parallel H$ is controllable.

If an MSC $J = G \parallel H$ is not controllable, is it necessary to *trim* it, i.e., to restrict its behavior, to ensure that only legal marking in $\mathscr{L}_J$ are reachable: the trimmed net, if it exists, is a *maximally permissive supervisor* for the given control problem and at the same time represents the behavior of the controlled plant.

We conclude with a property of the legal and weakly uncontrollable sets of a MSC that will be used later.

Lemma 1 *For a marking (M',M'') in J: (1) if $M \in \mathscr{L}_J$, then any marking $(M',\bar{M}'') \in \mathscr{L}_J$ for all $\bar{M}'' \geq M''$; (2) if $M \in \mathscr{W}_J$, then any marking $(\bar{M}',M'') \in \mathscr{W}_J$ for all $\bar{M}' \geq M'$;*

Proof: (1) If $(M',M'') \in \mathscr{L}_J$, according to the definition, $\forall \sigma' \in (T'_u)^*$ such that $M'[\sigma' t'_u\rangle_G$ there is a corresponding $\sigma \in T_u^*$ such that $M[\sigma\rangle_J$ and $\sigma_{\uparrow G} = \sigma' t'_u$. We put all such pairs $(\sigma' t_u, \sigma)$ in Σ: $\Sigma = \{(\sigma' t_u, \sigma)\}$. For any marking $(M',\bar{M}'')$ with $\bar{M}'' \geq M''$, for each $M'[\sigma' t'_u\rangle_G$, we pick σ which corresponds to the pair (σ',σ). Since $(M',\bar{M}'') \geq (M',M'')$, σ can fire in J under (M',M'') and $\sigma_{\uparrow G} = \sigma' t'_u$ then $(M',\bar{M}'') \in \mathscr{L}_J$.

(2) If $(M',M'') \in \mathscr{W}_J$, according to the definition, there exists $\sigma' \in (T'_u)^*$ such that $M'[\sigma' t'_u\rangle_G$ and there

does not exist a corresponding $\sigma \in T_u^*$ such that $M[\sigma\rangle_J$ and $\sigma_{\uparrow G} = \sigma' t'_u$. This means that under (M', M'') all σ such that $\sigma_{\uparrow G} = \sigma' t'_u$ are blocked by some specification place. For any marking $(\bar{M}', M'')$ with $\bar{M}' \geq M'$, we consider the same σ. Because M'' remains unchanged, all σ such that $\sigma_{\uparrow G} = \sigma' t'_u$ are still blocked by the same specification places. Thus $(\bar{M}', M'') \in \mathscr{W}_J$. □ ■

3.3 Problem Statement

When the set of legal markings of an MSC can be described by means of an OR-AND GMEC, we say that the corresponding control problem has an OR-AND GMEC solution. In such a case, in fact, an uncontrollable MSC can be easily trimmed by adding to it a simple control structure as shown by [15]. Furthermore this control structure can be designed by structural analysis and it is not necessary to analyze the reachability set of the net J, that may be very large. This provides and efficient technique for the design of a maximally permissive Petri net supervisor, i.e., a supervisor compiled into a net structure.

It is known that a maximally permissible Petri net supervisor may not exist if J is not bounded [10]. Therefore for a given system it is worthwhile to determine under which conditions a OR-AND GMEC solution exists. The problem can be stated as follows:

Problem 1 (Existence of OR-AND GMEC solution) *Given an MSC J, determine if there exists a finite OR-AND GMEC* ξ *such that* $\mathscr{M}(\xi) = \mathscr{L}_J$. △

4 Existence of OR-AND GMEC solutions

In this section we present some sufficient conditions that ensure the existence of an OR-AND GMEC solution. Let us first define some particular classes of subsets of $\mathbb{N}^m$ that will allow us study the algebraic property of legal sets.

First we define right-closed sets and show that in $\mathbb{N}^m$ they have a finite set of generators following [17].

Definition 1 *A set* $S \in \mathbb{N}^m$ *is called* right-closed *if* $\{s \in \mathbb{N}^m \mid (\exists s' \in S)\ s \geq s'\} \subseteq S$ △

Lemma 2 (Dickson's lemma) *Let* $S \subseteq \mathbb{N}^m$ *be a right-closed set. Then the set* $S_{\min}$ *of minimal markings of S for the ordering* $\leq$ *is finite.* △

Secondly we define star-free sets and prove that they can be described by OR-AND GMECs.

Definition 2 *A set $S \in \mathbb{N}^m$ is called* star-free *[18] if it is a finite union of sets of the form*

$$K(I,v) = \{x \in \mathbb{N}^m \mid x \geq v, \forall i \in I, x_i = v_i\} \tag{7}$$

where $v \in \mathbb{N}^m, I \subseteq \{1,\ldots,m\}$. △

Proposition 1 *Given a set $S \subseteq \mathbb{N}^m$ there exists a finite OR-AND GMEC ξ such that $\mathscr{M}(\xi) = S$ if either S or its complement $\complement S$ is star-free. Proof: Assume S is star-free. Obviously each set $K(I,v)$ in* (7) *can be be written as the legal set of and AND GMEC. Hence finite union of these sets can be written as the legal set of a finite OR-AND GMEC.*

Also in [18] it was shown that if a set S is star-free, then also its complement $\complement S$ is star-free. This conclude the proofs. □ ■

We now provide a structural characterization of the set of legal markings for a a given control problem.

Definition 3 *Given an MSC J with underlying net N, and an uncontrollable transition $t'_u \in T'_u$ consider the following sets.*

- *$P'_{t'_u}$ is set of places from which in G there exists is a path[2] directed to t'_u containing only uncontrollable transitions.*
- *$T_{t'_u} = \{t \in T_u \mid t^\bullet \cap P'_{t_u} \neq \emptyset\} \cup \{t \in T_u \mid t = (t'_u, \cdot)\}$ is the set of uncontrollable transitions in J that either have an arc going to a place in $P'_{t'_u}$ or correspond to transition t'_u.*
- *$P''_{t'_u} = \{p'' \in P'' \mid (p'')^\bullet \cap T_{t'_u} \neq \emptyset\}$ is the set of places of H that have an arc going to a transition in $T_{t'_u}$*

We define the uncontrollable subnet of transition *t'_u, as the subnet $N_{t'_u}$ of N with set of places $P_{t'_u} = P'_{t'_u} \cup P''_{t'_u}$ and set of transitions $T_{t'_u}$.* △

Example 1 *Consider the MSC J in Figure 2 with uncontrollable transition $t_u = t_8$. The subnet N_{t_u} is composed by the nodes and arcs colored in red and blue.* △

Remark 2 *The interest of the previous definition is the following. In eqs.* (4) *and* (6) *we have written the set of bad markings of an MSC as the union of the weakly uncontrollable marking sets $\mathscr{W}_j(t'_u)$ for all uncontrollable transitions t'_u of the plant G. It is clear that to characterize each set $\mathscr{W}_j(t'_u)$ one only needs to study the uncontrollable subnet $N_{t'_u}$ of transition t'_u and this will allow us to simplify the derivation of the results presented in the following.* △

[2] A path directed from a node x_1 to a node x_k in a net $N = (P,T,Pre,Post)$ is a sequence $x_1 x_2 \cdots x_k$ such that $x_i \in P \cup T$ for all $i = 1,\ldots,k$, and $x_i \in {}^\bullet x_{i+1}$ for all $i = 1,\ldots,k-1$.

We can finally prove the main result of this section.

Theorem 1 *Consider a MSC $J = G \parallel H = (N, M_0, E, l)$ and assume that for all uncontrollable transitions $t'_u \in T'_u$ of the plant G either one of the following two sets is bounded in J:*

- $P'_{t'_u}$*: places of its uncontrollable subnet belonging to G;*
- $P''_{t'_u}$*: places of its uncontrollable subnet belonging to H.*

Then there exists an OR-AND GMEC ξ such that

$$\mathscr{M}(\xi) \cap R(N, M_0) = \mathscr{L}_J \cap R(N, M_0).$$

Proof: As mentioned in Remark 2, it is sufficient to show that for each uncontrollable transition $t'_u \in T'_u$ the result applies to the uncontrollable subnet $N_{t'_u}$.

For sake of simplicity, in the following we denote $\hat{N}$ such a net and denote the set of its places $\hat{P} = \hat{P}' \cup \hat{P}''$, where $\hat{P}' = P'_{t'_u}$ and $\hat{P}' = P'_{t'_u}$. We also denote $\hat{\mathscr{W}}$ and $\hat{R}$ the restriction to $\hat{N}$ of the sets $\mathscr{W}(t'_u)$ and $R(N, M_0)$, respectively. Thus defining $\hat{\mathscr{L}} = \mathbb{N}^{|\hat{P}|} \setminus \hat{\mathscr{W}}$ we show that there exists an OR-AND GMEC $\hat{\xi}$ such that

$$\mathscr{M}(\hat{\xi}) \cap \hat{R} = \hat{\mathscr{L}} \cap \hat{R}. \tag{8}$$

We consider two cases.

(a) Assume all places in $\hat{P}'$ are bounded. Then the set $\Omega' = \{M' \in \mathbb{N}^{|\hat{P}'|} \mid (M', M'') \in \hat{R}\}$ is finite.

Consider a marking $M = (M', M'')$ of $\hat{N}$. As shown in Lemma 1, if such a marking is legal, i.e., $M \in \hat{\mathscr{L}}$ then any other marking $(M', \bar{M}'')$ with $\bar{M}'' \geq M''$ is also legal. Thus for each marking $M' \in \Omega'$ the set

$$\mathscr{C}(M') = \{M'' \in \mathbb{N}^{|\hat{P}''|} \mid (M', M'') \in \hat{\mathscr{L}}\}$$

is right closed and has a finite set of minimal generators $\mathscr{C}_{\min}(M')$ by Lemma 2.

This means that the set $\hat{\mathscr{L}} \cap \hat{R}$ of legal markings reachable in the subnet $\hat{N}$ can be written as:

$$\bigcup_{M' \in \Omega'} \bigcup_{M'' \in \mathscr{C}_{\min}(M')} K(I, (M', M''))$$

where the set I denotes the components of M'. This set if obviously star-free hence by Proposition 1 there exists an OR-AND GMEC constraint $\hat{\xi}$ such that $\mathscr{M}(\hat{\xi}) = \hat{\mathscr{L}} \cap \hat{R}$. Obviously this constraint also satisfies condition (8).

(b) Assume all places in $\hat{P}''$ are bounded. Then the set $\Omega'' = \{M'' \in \mathbb{N}^{|\hat{P}''|} \mid (M', M'') \in \hat{R}\}$ is finite.

Consider a marking $M = (M', M'')$ of $\hat{N}$. As shown in Lemma 1, if such a marking is weakly forbidden, i.e., $M \in \hat{\mathscr{W}}$ then any other marking $(\bar{M}', M'')$ with $\bar{M}' \geq M'$ is also weakly forbidden. Thus for each marking $M'' \in \Omega''$ the set

$$\mathscr{C}(M'') = \{M' \in \mathbb{N}^{|\hat{P}'|} \mid (M', M'') \in \hat{\mathscr{W}}\}$$

is right closed and has a finite set of minimal generators $\mathscr{C}_{\min}(M'')$ by Lemma 2.

This means that the set $\hat{\mathscr{W}} \cap \hat{R}$ of weakly forbidden markings reachable in the subnet $\hat{N}$ can be written as:

$$\bigcup_{M'' \in \Omega''} \bigcup_{M' \in \mathscr{C}_{\min}(M'')} K(I, (M', M''))$$

where the set I denotes the components of M''. This set if obviously star-free hence by Proposition 1 there exists an OR-AND GMEC constraint $\hat{\xi}^c$ such that $\mathscr{M}(\hat{\xi}^c) = \hat{\mathscr{W}} \cap \hat{R}$.

Consider finally the OR-AND GMEC ξ complementary of ξ^c that defines a set of legal marking $\mathscr{M}(\hat{\xi}) = \hat{\mathscr{L}} \cup (\mathbb{N}^{|\hat{P}|} \setminus \hat{R}$. Obviously this constraint also satisfies condition (8). □ ■

Remark 3 *We explain why $\mathscr{L}_J$ is not a subset of $R(N, M_0)$ in Theorem 1. Therefore there may exist some illegal markings from which the plant may violate the control policy ($\mathscr{L}_J$ is defined on $\mathbb{N}^m$), however, these markings are not reachable from the initial marking. Since it is difficult to determine if a marking is reachable, in this paper we focus on the control policy ξ which eliminates all illegal markings regardless if they are reachable.*

Remark 4 *Theorem 1 provides a sufficient condition under which an "OR-AND GMEC based" controller exists. However, the method to construct the OR-AND GMEC in Theorem 1 is not efficient: the number of single GMECs is usually very large, leading to an unnecessary complicated Petri net controller. An optimized controller based on structural analysis will be relatively simple. We have found some efficient method to construct the more compact OR-AND GMEC controllers for some specific subclasses of MSC.*

If both G and H are unbounded, a GMEC solution may not exists as will be discussed in the following section.

5 Non-Existence of OR-AND GMEC solutions

For a MSC J in which an uncontrollable subnet $J_{t'_u}$ does not satifies the conditions of Theorem 1, i.e., both $P'_{t'_u}$ and $P''_{t'_u}$ are unbounded, an OR-AND GMEC soluion may not exists. We will show that this unexpected

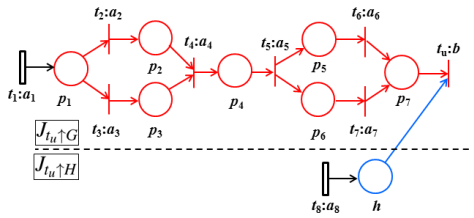

Figure 3: A MSC J which is free-labeled.

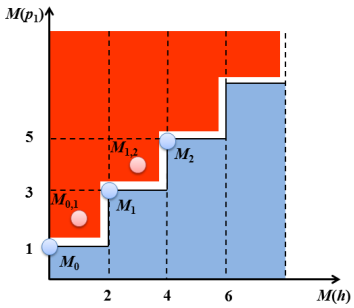

Figure 4: $\mathscr{L}(J_{t_u})$ in Figure 3 projected on $\langle p_1, h_1 \rangle$. Each vertical/horizontal segment along the zigzag boundary represents a single GMEC.

phenomenon occurs in very simple uncontrollable structures, e.g., free-labeled, ordinary and acyclic.

We first present a lemma that will be used in the following example.

Lemma 3 *For a set $S \subseteq \mathbb{N}^m$, if there exists a projection $S_{\langle u \rangle} \subseteq \mathbb{N}^m$ such that $S_{\langle u \rangle}$ cannot be written as the union of finite number of convex sets, then there does not exists a finite ξ such that $\mathscr{M}(\xi) = S$.*

Proof: If there exists a ξ such that $\mathscr{M}(\xi) = S$, from the definition of OR-AND GMEC, S can be written as $S = \bigcup_i^k S_i$ and each S_i is a convex set. For any given subspace u, the projection of any $S_i : S_{i\langle u \rangle}$ is also a convex set. This indicates $S_{\langle u \rangle}$ can always be written as $S_{\langle u \rangle} = \bigcup_i^k S_{i\langle u \rangle}$ and each $S_{i\langle u \rangle}$ is a convex set. □ ■

Example 2 *Consider the MSC J in Figure 3. Here both $\mathscr{W}_J$ and $\mathscr{L}_J$ are too complicate to be defined explicitly, we cannot easily determine if there exists a ξ such that $\mathscr{M}(\xi) = \mathscr{L}_J$. However, if we project $\mathscr{L}_J$ on the space $\langle p_1, h \rangle$, denoted as $\mathscr{L}_{\langle p_1,h \rangle}(J)$, we cannot find a finite ξ such that $\mathscr{M}(\xi) = \mathscr{L}_{\langle p_1,h \rangle}(J)$.*

Actually, $\mathscr{L}_{\langle p_1,h \rangle}(J)$ is not a star-free set. The legal marking set (blue) and weakly uncontrollable marking set (red) is illustrated in Figure 4. One can see that there does not exist an OR-AND GMEC solution since each M_k $(k \geq 0)$ is an extreme point of $\mathscr{L}_J$. For each M_k we need to introduce at least two constraints: $(M(p_1) \leq 2k+1) \wedge (M(h) \geq 2k)$, and $\mathscr{L}_{\langle p_1,h \rangle}(J)$ can be expressed by an infinite ξ such as:

$$\left\{ \bigvee_{k=0}^{+\infty} (M(p_1) \leq 2k+1) \wedge (M(h) \geq 2k) \right. \tag{9}$$

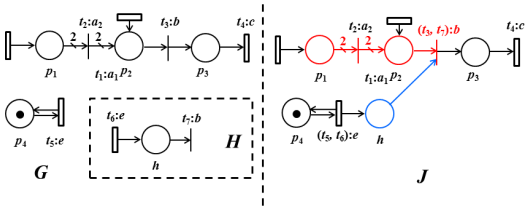

Figure 5: A generalized Petri net MSC which does not have an OR-AND GMEC solution.

One can easily verify that all constraints in ξ are non-redundant. Since $\mathscr{L}_{\langle p_1,h\rangle}(J)$ cannot be written as the union of finite number of convex sets, we cannot find a finite ξ such that $\mathscr{M}(\xi) = \mathscr{L}_{\langle p_1,h\rangle}(J)$. From Lemma 3, we cannot find a finite ξ such that $\mathscr{M}(\xi) = \mathscr{L}_J$. △

For a certain J and t_u, it may happen there does not exist a ξ such that $\mathscr{M}(\xi) = \mathscr{L}(J_{t_u})$, but there may exist ξ such that $\mathscr{M}(\xi) = \mathscr{L}_J$. This is because there may exist $t'_u \neq t_u$ in J such that there exists a $\xi' : \mathscr{M}(\xi) = \mathscr{L}(J_{t'_u})$ and by applying ξ' J_{t_u} becomes bounded. If there is only one J_{t_u} in J and it fails the test, there is no OR-AND GMEC solution for J. We are exploiting an algorithm to determine the existence of ξ. Unfortunately, actually most generalized MSCs (even it is very simple) fails the test. For example, the MSC J in Figure 5 does not have an OR-AND GMEC solution, although J_{t_u} (colored) only contains three plant places and two uncontrollable transitions. This observation indicates the high difficulty in the issue of generalized supervisor trimming. This determination is worthwhile since any approach seeking for a maximal controllable OR-AND GMEC solution should not takes J_{t_u} as an input, otherwise it will not halt.

6 Conclusion

In this paper we characterized the existence of maximally controllable supervisor in the framework of supervisor control. For an monolithic supervisor J, an OR-AND GMEC solution always exists if for each of its uncontrollable subnet J_{t_u}, either $J_{t_u\uparrow G}$ or $J_{t_u\uparrow H}$ is bounded.

References

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

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

[3] A. Giua, F. DiCesare, and M. Silva, "Generalized mutual exclusion constraints for Petri nets with uncontrollable transitions," in *Proc. IEEE Int. Conf. on Systems, Man, and Cybernetics*, Chicago, USA, 1992, pp. 947–949.

[4] J. Moody and P. Antsaklis, "Petri net supervisors for DES with uncontrollable and unobservable transitions," *IEEE Transactions on Automatic Control*, vol. 45, no. 3, pp. 462–476, 2000.

[5] L. E. Holloway, A. S. Khare, and Y. Gong, "Computing bounds for forbidden state reachability functions for controlled Petri nets," *IEEE Transactions on Systems, Man, and Cybernetics, Part A*, vol. 34, no. 2, pp. 219–228, 2004.

[6] F. Basile, C. Carbone, and P. Chiacchio, "Feedback control logic for backward conflict free choice nets," *IEEE Transactions on Automatic Control*, vol. 52, no. 3, pp. 387–400, 2007.

[7] J. L. 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.

[8] M. Uzam, "On suboptimal supervisory control of Petri nets in the presence of uncontrollable transitions via monitor places," *International Journal of Advanced Manufacturing Technology*, vol. 47, no. 5, pp. 567–579, 2010.

[9] M. V. Iordache, P. Wu, F. Zhu, and P. J. Antsaklis, "Efficient design of Petri-net supervisors with disjunctive specifications," in *Proc. IEEE Int. Conf. on Automation Science and Engineering*, Madison, USA, 2013, pp. 936–941.

[10] A. Giua, "Supervisory control of Petri nets with language specifications," in *Control of discrete-event systems*, C. Seatzu, M. Silva, and J. van Schuppen, Eds. London: Springer, 2013, vol. 433, pp. 235–255.

[11] Z. W. Li and M. C. Zhou, *Deadlock Resolution in Automated Manufacturing Systems: A Novel Petri Net Approach*. London: Springer, 2009.

[12] 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.

[13] B. Lacerda and P. U. Lima, "On the notion of uncontrollable marking in supervisory control of Petri nets," *IEEE Transactions on Automatic Control*, vol. 59, no. 11, pp. 53–61, 2014.

[14] M. V. Iordache and P. J. Antsaklis, "Petri net supervisors for disjunctive constraints," in *Proc. 26th American Control Conference*, New York, USA, 2007, pp. 4951–4956.

[15] Z. Y. Ma, Z. W. Li, and A. Giua, "Petri net controllers for disjunctive generalized mutual exclusion constraints," in *Proc. IEEE Int. Conf. on Emerging Technologies and Factory Automation*, Cagliari, Italy, 2013, pp. 1–8.

[16] R. Kumar and L. E. Holloway, "Supervisory control of deterministic Petri nets with regular specification languages," *IEEE Transactions on Automatic Control*, vol. 41, no. 2, pp. 245–249, 1996.

[17] A. Giua and F. DiCesare, "Decidability and closure properties of weak Petri net languages in supervisory control," *IEEE Transactions on Automatic Control*, vol. 40, no. 5, pp. 906–910, 1995.

[18] S. Gaubert and A. Giua, "Petri net languages and infinite subsets of $\mathbb{N}^m$," *Journal of Computer and System Sciences*, vol. 59, no. 3, pp. 373–391, 1999.