Generalized Mutual Exclusion Constraints on Nets with Uncontrollable Transitions

Alessandro Giua,

Dip. di Ingegneria Elettrica ed Elettronica, Università di Cagliari,

Piazza d'Armi — 09123 Cagliari, Italy

Phone: +39-070-675-5892 – Fax: +39-070-675-5900 – Email: giua@diee.unica.it.

Frank DiCesare

Electrical, Computer, and Systems Eng. Dept., Rensselaer Polytechnic Institute

Troy, NY 12180-3590, USA

Manuel Silva

Dpto. Ing. Eléctrica e Informática, Universidad de Zaragoza

50015, Zaragoza, Spain

Abstract

We study a class of specifications, called generalized mutual exclusion constraints, for discrete event systems modeled using Place/Transition nets. These specifications may be easily enforced on a net system where all transitions are controllable, by a set of places called monitors. However, when some of the transitions of the net are uncontrollable this technique is not always applicable. For some classes of nets, we prove that generalized mutual exclusion constraints may always be enforced by monitors, even in the presence of uncontrollable transitions.

Published as:

A. Giua, F. DiCesare, M. Silva, "Generalized Mutual Exclusion Constraints for Nets with Uncontrollable Transitions", Proc. IEEE Int. Conf. on Systems, Man, & Cybernetics (Chicago, USA), pp. 974-9, October 1992.

1 Introduction

Mutual exclusion constraints are a natural way of expressing the concurrent use of a finite number of resources, shared among different processes. In the framework of Petri nets and from a very general perspective, we define a generalized mutual exclusion constraint (GMEC) as a condition that limits a weighted sum of tokens contained in a subset of places. Let $\langle N, M_0 \rangle$ be a net system with set of places P. A constraint $(\vec{w}, k)$ defines a set of *legal* markings:

$$\mathcal{M}(\vec{w}, k) = \{M \in \mathbb{N}^{|P|} \mid \vec{w}^T \cdot M \leq k\},$$

where $\vec{w}$ is a weight vector of nonnegative integers, and k is a positive integer. Markings in $\mathbb{N}^{|P|}$ that are not legal will be denoted *forbidden* markings.

In the first part of this paper we present a methodology, based on linear algebraic techniques [8], to compare and simplify GMEC. An equivalence notion among GMEC is introduced and studied from the point of view of structural net theory.

In traditional Petri net modeling all transitions are assumed to be *controllable*, i.e., may be prevented from firing by a control agent. A problem addressed for those systems with shared resources has been that of deadlock prevention or avoidance [1, 9, 10]. A single GMEC may be easily implemented by a *monitor*, i.e., a place whose initial marking represents the available units of a resource and whose outgoing and incoming transitions represent, respectively, the acquisition and release of units of the resource.

In the framework of Supervisory Control [3, 7] the complexity of enforcing a GMEC is enhanced by the presence of *uncontrollable* transitions, i.e., transitions that may be observed but not prevented from firing by a control agent. To enforce a given GMEC, it is necessary to prevent the system from reaching a superset of the forbidden markings, containing all those markings from which a forbidden one may be reached by firing a sequence of uncontrollable transitions. Unfortunately, in this case we prove that the set of legal markings cannot *always* be represented by a linear domain in the marking space, thus there exist problems which do not have a "monitor-based" solution.

The paper is structured as follows. In Section 2 is introduced the notation on Petri nets. In Section 3 generalized mutual exclusions constraints are defined. We also discuss the modeling power of this kind of constraints. In Section 4 it is shown how these constraints may be enforced by a monitor place if all transitions of the net are controllable. In

Section 5 it is shown that a monitor-based solution may not exists if some of the transitions of a net are uncontrollable.

2 Generalities

A *Place/Transition net* (P/T net) [6] is a structure $N = (P, T, Pre, Post)$, where P is a set of *places* represented by circles, $|P| = m$; T is a set of *transitions* represented by bars, $|T| = n$; $Pre : P \times T \to \mathbb{N}$ is the *pre-incidence function* that specifies the arcs directed from places to transitions; $Post : P \times T \to \mathbb{N}$ is the *post-incidence function* that specifies the arcs directed from transitions to places.

If the net is *pure*, i.e., it has no selfloops, the incidence functions can be represented by a single matrix, the *incidence matrix* of the net, defined as $C(p,t) = Post(p,t) - Pre(p,t)$.

A *marking* is a vector $M : P \to \mathbb{N}$ that assigns to each place of a P/T net a non-negative integer number of tokens, represented by black dots. $\mathbb{N}^{|P|}$ will denote the set of all possible markings that may be defined on the net. A *P/T system* or *net system* $\langle N, M_0 \rangle$ is a net N with an initial marking M_0.

A transition $t \in T$ is *enabled* at a marking M iff $M \geq Pre(\cdot, t)$. If t is enabled at M, then t may fire yielding a new marking M' with $M' = M + C(\cdot, t)$. We will write $M\ [t\rangle\ M'$ to denote that t may fire at M yielding M'.

A *firing sequence* from M_0 is a (possibly empty) sequence of transitions $\sigma = t_1 \ldots t_k$ such that $M_0\ [t_1\rangle\ M_1\ [t_2\rangle\ M_2 \cdots\ [t_k\rangle\ M_k$. A marking M is *reachable* in $\langle N, M_0 \rangle$ iff there exists a firing sequence σ such that $M_0\ [\sigma\rangle\ M$.

Given a system $\langle N, M_0 \rangle$, the set of firing sequences (also called *language* of the net) is denoted $L(N, M_0)$ and the set of reachable markings (also called *reachability set* of the net) is denoted $R(N, M_0)$.

If marking M is reachable in $\langle N, M_0 \rangle$ by firing a sequence σ, then the following *state equation* is satisfied: $M = M_0 + C\vec{\sigma}$, where $\vec{\sigma} : T \to \mathbb{N}$ is a vector of non-negative integers, called the *firing count vector*. $\vec{\sigma}(t)$ represents the number of times transition t appears in σ. The set of markings M such that there exists a vector $\vec{\sigma}$ satisfying the previous state equation is called *potentially reachable set* and is denoted $PR(N, M_0)$. Note that $PR(N, M_0) \supseteq R(N, M_0)$.

A *P-semiflow* is a vector $Y : P \to \mathbb{N}$ such that $Y \geq \vec{0}$ and $Y^T \cdot C = \vec{0}$. Let B be a basis of P-semiflows of the net N. For any M_0, a marking $M \in PR(N, M_0)$ satisfies the following system of equations: $B^T \cdot M = B^T \cdot M_0$. The set markings satisfying the previous system of equations is denoted $PR^B(N, M_0)$ [2]. Note that $PR^B(N, M_0) \supseteq PR(N, M_0)$.

Let $X : P \to \mathbb{N}$ be a vector and $P' \subseteq P$. The *support* of X is $Q_X = \{p \in P \mid X(p) > 0\}$. The *projection* of X on P' is the restriction of X to P' and will be denoted $X \uparrow_{P'}$. This definition is extended in the usual way to the projection of a set of vectors $\mathcal{X}$, i.e., $\mathcal{X} \uparrow_{P'} = \{X \uparrow_{P'} \mid X \in \mathcal{X}\}$.

3 Generalized Mutual Exclusion Constraints

In this section we define a *generalized mutual exclusion constraint* (GMEC) as a condition that limits the weights sum of tokens in a set of places. We discuss the modeling power of this kind of constraint and prove that only for restricted classes of systems a *forbidden marking problem* may be expressed as a mutual exclusion problem.

3.1 Redundancy, Equivalence and Simplification of Mutual Exclusion Constraints

Definition 1. *Let $\langle N, M_0 \rangle$ be a net system with set of places P. A single* generalized mutual exclusion constraint *$(\vec{w}, k)$ defines a set of legal markings*

$$\mathcal{M}(\vec{w}, k) = \{M \in \mathbb{N}^{|P|} \mid \vec{w}^T \cdot M \leq k\},$$

where $\vec{w} : P \to \mathbb{N}$ is a weight vector, and $k \in \mathbb{N}^+$. The support *of $\vec{w}$ is the set $Q_w = \{p \in P \mid w(p) > 0\}$.*

A set of generalized mutual exclusion constraints $(W, \vec{k})$, with $W = [\vec{w}_1 \dots \vec{w}_m]$ and $\vec{k} = (k_1 \dots k_m)^T$, defines a set of legal markings

$$\begin{aligned} \mathcal{M}(W, \vec{k}) &= \textstyle\bigcap_{i=1}^{m} \mathcal{M}(\vec{w}_i, k_i) \\ &= \{M \in \mathbb{N}^{|P|} \mid W^T \cdot M \leq \vec{k}\}. \end{aligned}$$

As a particular case, when $\vec{w} \leq \vec{1}$, i.e., $w(p) = 1$ $(\forall p \in Q_w)$, the *unweighted* GMEC $(\vec{w}, k)$ is reduced to the *set condition* considered in [5].

In the following we will discuss redundancy and equivalence between constraints.

Definition 2. *Let $\langle N, M_0\rangle$ be a system. A GMEC $(\vec{w}, k)$ is* redundant *with respect to (wrt) a set of markings $A \subseteq I\!N^{|P|}$ if $A \subseteq \mathcal{M}(\vec{w}, k)$.*

A GMEC $(\vec{w}, k)$ is redundant wrt a system $\langle N, M_0\rangle$ *if $R(N, M_0) \subseteq \mathcal{M}(\vec{w}, k)$.*

A set of GMEC $(W, \vec{k})$, where $W = [\vec{w}_1 \dots \vec{w}_m]$ and $\vec{k} = (k_1 \dots k_m)^T$, is redundant wrt $\langle N, M_0\rangle$ if $(\vec{w}_i, k_i)$ is redundant for all $i = 1, \dots, m$.

Linear programming techniques may be used to derive sufficient conditions for redundancy.

Proposition 1. *If the following Linear Programming Problem (LPP) has optimal solution $x^* < k + 1$ then the GMEC $(\vec{w}, k)$ is* redundant *wrt $\langle N, M_0\rangle$:*

$$\begin{array}{rll} x = & \max & \vec{w}^T \cdot M \\ & s.t. & M = M_0 + C \cdot \vec{\sigma}, \\ & & M, \vec{\sigma} \geq \vec{0}. \end{array}$$

Proof: If $x^* < k + 1$ then $PR(N, M_0) \subseteq \mathcal{M}(\vec{w}, k)$ and this implies that $R(N, M_0) \subseteq \mathcal{M}(\vec{w}, k)$. ◇

The proposition gives a sufficient condition for redundancy. There are classes of nets, such as marked graphs, for which the condition is necessary and sufficient [2]. Also for the nets for which $PR(N, M_0) = PR^B(N, M_0)$ we may equivalently check for redundancy solving the following linear programming problem:

$$\begin{array}{rll} x = & \max & \vec{w}^T \cdot M \\ & s.t. & B^T \cdot M = B^T \cdot M_0, \\ & & M \geq \vec{0}. \end{array}$$

where B is a basis of P-semiflows of the net.

Definition 3. *Two sets of GMEC $(W_1, \vec{k}_1)$ and $(W_2, \vec{k}_2)$ are* equivalent *wrt $\langle N, M_0\rangle$ if $R(N, M_0) \cap \mathcal{M}(W_1, \vec{k}_1) = R(N, M_0) \cap \mathcal{M}(W_2, \vec{k}_2)$.*

We may check for equivalence between constraints using the same approach we used to check for redundancy. In fact from the definition it follows that two sets of GMEC $(W_1, \vec{k}_1)$ and $(W_2, \vec{k}_2)$ are equivalent wrt $\langle N, M_0\rangle$ if and only if $(W_1, \vec{k}_1)$ is redundant wrt $R(N, M_0) \cap \mathcal{M}(W_2, \vec{k}_2)$, and $(W_2, \vec{k}_2)$ is redundant wrt $R(N, M_0) \cap \mathcal{M}(W_1, \vec{k}_1)$.

Example 1. Consider the system in Figure 1a whose reachable set is $R(N, M_0) = \{M \mid \vec{1}^T \cdot M = 3\}$. Let $(\vec{w}_1, k_1)$ and $(\vec{w}_2, k_2)$ be two GMEC with: $\vec{w}_1 = (1330)^T, k_1 = 5$, and $\vec{w}_2 = (0110)^T, k_2 = 1$.

To prove that the two constraints are equivalent wrt the system considered we may proceed as follows. The LPP

$$\begin{aligned} x_1 = \quad & \max \quad \vec{w}_1^T \cdot M \\ & s.t. \quad \vec{1}^T \cdot M = 3, \\ & \qquad \vec{w}_2^T \cdot M \leq 1, \\ & \qquad M \geq \vec{0}, \end{aligned}$$

has optimal value $x_1^* = 5 < k_1 + 1$, hence by Proposition 1 $R(N, M_0) \cap \mathcal{M}(\vec{w}_2, k_2) \subseteq \mathcal{M}(\vec{w}_1, k_1)$. The LPP

$$\begin{aligned} x_2 = \quad & \max \quad \vec{w}_2^T \cdot M \\ & s.t. \quad \vec{1}^T \cdot M = 3, \\ & \qquad \vec{w}_1^T \cdot M \leq 5, \\ & \qquad M \geq \vec{0}, \end{aligned}$$

has optimal value $x_2^* = \frac{5}{3} < k_2 + 1$, hence $R(N, M_0) \cap \mathcal{M}(\vec{w}_1, k_1) \subseteq \mathcal{M}(\vec{w}_2, k_2)$. This proves that the two constraints are equivalent for the given system.

The equivalence between constraints leads to the idea of *simplification* of a constraint. Given a constraint $(\vec{w}, k)$, we may look for a simpler, but equivalent, constraint. A constraint $(\vec{w}', k')$ is simpler than $(\vec{w}, k)$ if $\vec{w}' < \vec{w}$. In the next subsection we will see that simpler constraints require simpler control structure to be enforced. Next example shows another advantage of simplifying constraints.

Example 2. For the system in Figure 1a consider, in addition to the two constraints discussed in Example 1, the constraint $(\vec{w}_3, k_3)$ with: $\vec{w}_3 = (0330)^T, k_3 = 5$. By definition, $(\vec{w}_2, k_2)$ is simpler than $(\vec{w}_3, k_3)$ that is simpler than $(\vec{w}_1, k_1)$. It is immediate to see that $\mathcal{M}(\vec{w}_3, k_3) = \mathcal{M}(\vec{w}_2, k_2)$, i.e., $(\vec{w}_3, k_3)$ is equivalent to $(\vec{w}_2, k_2)$ wrt $\langle N, M_0 \rangle$. Since we have proved in Example 1 that $(\vec{w}_1, k_1)$ is equivalent to $(\vec{w}_2, k_2)$, the equivalence between $(\vec{w}_1, k_1)$ and $(\vec{w}_3, k_3)$ also follows.

Note, however, that if we try to use a LPP to prove that $(\vec{w}_1, k_1)$ is redundant wrt $R(N, M_0) \cap (\vec{w}_3, k_3)$ we have an inconclusive answer. In fact the LPP

$$\begin{aligned} x_1 = \quad & \max \quad \vec{w}_1^T \cdot M \\ & s.t. \quad \vec{1}^T \cdot M = 3, \\ & \qquad \vec{w}_3^T \cdot M \leq 5, \\ & \qquad M \geq \vec{0}, \end{aligned}$$

has optimal value: $x_1^* = \frac{19}{3} > 6$, hence we cannot conclude that $(\vec{w}_1, k_1)$ is redundant wrt $R(N, M_0) \cap (\vec{w}_3, k_3)$.

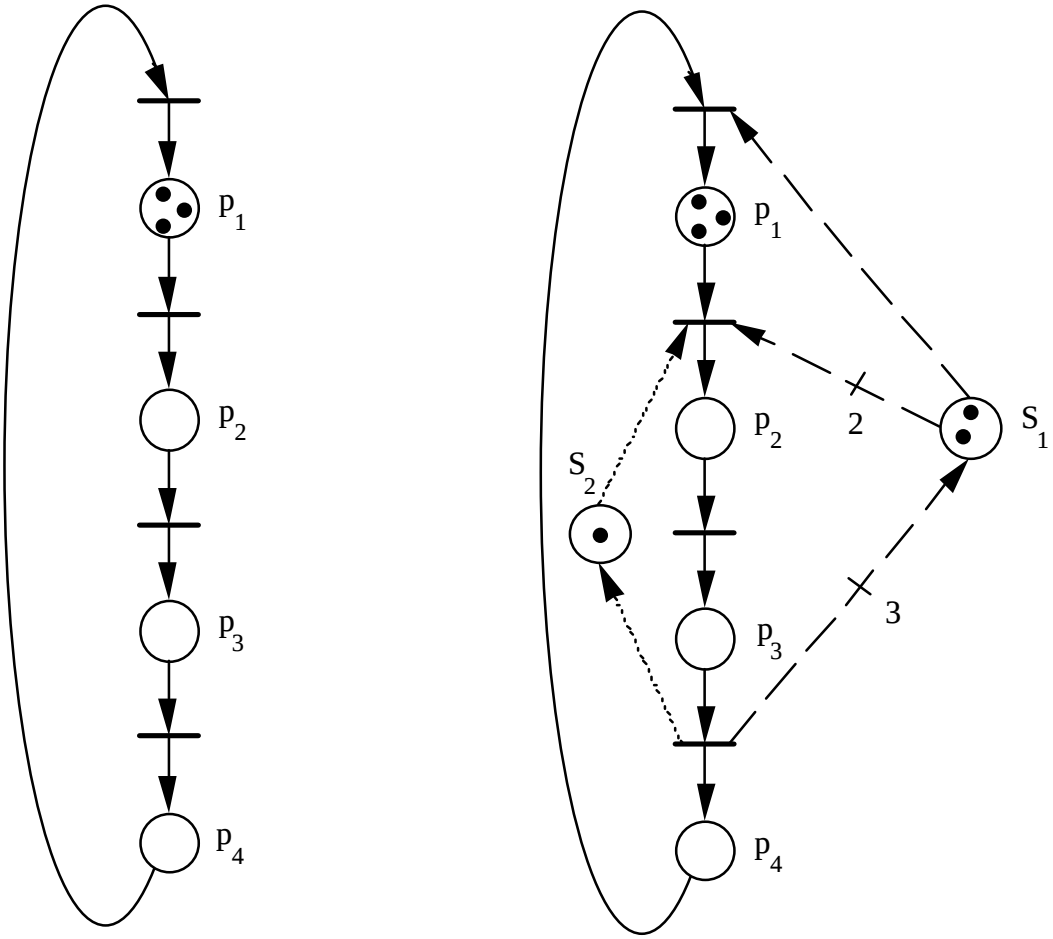

Figure 1: System in Example 1.

It is important, in the previous example, to pinpoint the advantage of using the simpler unweighted constraint $(\vec{w}_2, k_2)$ rather than the weighted one $(\vec{w}_3, k_3)$ to prove equivalence to $(\vec{w}_1, k_1)$. The system considered in the example is a live marked graph, and the constraint set that defines the set of reachable markings has integer extremal points, hence any optimal solution of the Linear Programming Program is also a solution of the corresponding Integer Programming Problem. This property is preserved if we add any number of unweighted constraints to the constraint set that defines the set of reachable markings.

3.2 Modeling Power of Generalized Mutual Exclusion Constraints

The use of weights in the definition of $(\vec{w}, k)$ may be a useful way to compactly express more than one unweighted constraint, i.e., it may be the case that a weighted constraint may be decomposed into a set of unweighted ones.

Example 3. In the case of safe (i.e., 1-bounded) systems, the constraint $(\vec{w}, k)$ with $\vec{w} = (1234)^T$ and $k = 5$ is equivalent to the set of constraints $(W, \vec{k})$ with

$$W = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix},$$

and $\vec{k} = (211)^T$. In fact $\mathcal{M}(\vec{w}, k) \cap \{0,1\}^4 = \mathcal{M}(W, \vec{k}) \cap \{0,1\}^4$.

We point out that there does not always exist a set of unweighted constraints equivalent to a set of weighted ones.

Example 4. Consider again the system in Figure 1a. Let $(\vec{w}, k)$ be a GMEC with: $\vec{w} = (1200)^T, k = 4$. Markings $M_1 = (2100)^T$ and $M_2 = (0210)^T$ are legal, while marking $M_3 = (1200)^T$ is forbidden by $(\vec{w}, k)$. If there exists a set of unweighted constraints $(W, \vec{k})$ equivalent to $(\vec{w}, k)$, then one of the constraints in this set must be $(\vec{w}', k')$, with $\vec{w}' = \vec{1}$, such that $M_1, M_2 \in \mathcal{M}(\vec{w}', k')$, and $M_3 \notin \mathcal{M}(\vec{w}', k')$. We will prove, by contradiction, that no such $(\vec{w}', k')$ may exists. In fact, $\vec{w}' \cdot M_1 < \vec{w}' \cdot M_3 \Longrightarrow w'(p_1) < w'(p_2)$, and $\vec{w}' \cdot M_2 < \vec{w}' \cdot M_3 \Longrightarrow w'(p_3) < w'(p_1)$. That is, in order to have an unweighted constraint that forbids M_3 but that does not forbid M_1 and M_2 we need to chose a $\vec{w}'$ such that $(\forall p)\ w'(p) \in \{0,1\}$ and $w'(p_3) < w'(p_1) < w'(p_2)$. This is clearly impossible.

For safe systems, however, the following theorem proves that any weighted constraint is equivalent to a set of unweighted constraints.

Theorem 1. *Let $\langle N, M_0\rangle$ be a safe system with set of places P and $(\vec{w}, k)$ a weighted GMEC. There exists a set of unweighted constraints $(W, \vec{k})$ equivalent to $(\vec{w}, k)$ wrt $\langle N, M_0\rangle$.*

Proof: Consider the set of vectors V such that $\forall \vec{v} \in V$ the following conditions are verified: $(C1)$ $\vec{v} \in \{0,1\}^{|P|}$; $(C2)$ $Q_v \subseteq Q_w$; $(C3)$ $\vec{w}^T \cdot \vec{v} > k$; $(C4)$ $(\forall \vec{v}' \in \{0,1\}^{|P|}, \vec{v}' < \vec{v})$ $\vec{w}^T \cdot \vec{v}' \leq k$. Let $(W, \vec{k})$ be such that $W = (\vec{w}_1 \dots \vec{w}_r)$ and $\vec{k} = (k_1 \dots k_r)^T$, where $\bigcup_{i=1}^{r} \{\vec{w}_i\} = V$, and where $k_i = |Q_{w_i}| - 1$ $(\forall i = 1, \dots, r)$.

a) Let us prove $R(N, M_0) \cap \mathcal{M}(\vec{w}, k) \subseteq \mathcal{M}(W, \vec{k})$.
$M \in R(N, M_0) \cap \mathcal{M}(\vec{w}, k) \Longrightarrow M \leq \vec{1} \wedge \vec{w}^T \cdot M \leq k \Longrightarrow M \leq \vec{1} \wedge (\forall \vec{v} \in V)\ \exists p \in Q_v \ni M(p) = 0 \Longrightarrow (\forall \vec{v} \in V)\ \vec{v}^T \cdot M \leq k_i \Longrightarrow M \in \mathcal{M}(W, \vec{k})$.

b) Let us prove $R(N, M_0) \cap \mathcal{M}(W, \vec{k}) \subseteq \mathcal{M}(\vec{w}, k)$. It is enough to prove that $M \in R(N, M_0) \wedge M \notin \mathcal{M}(\vec{w}, k) \Longrightarrow M \notin \mathcal{M}(W, \vec{k})$.
$M \in R(N, M_0) \wedge M \notin \mathcal{M}(\vec{w}, k) \Longrightarrow M \leq \vec{1} \wedge \vec{w}^T \cdot M > k$. Let $\vec{v}_0$ be defined as: if $p \in Q_w$ then $v_0(p) = M(p)$ else $v_0(p) = 0$. Clearly $\vec{v}_0$ satisfies conditions C1-C3 listed above. We will show that there exists a vector $\vec{v}_j \leq \vec{v}_0$ and such that $\vec{v}_j \in V$. Consider $p' \in Q_{v_0} \ni (\forall p \in Q_{v_0}) w(p') \leq w(p)$. Let $\vec{v}_1$ be a new vector such that: if $p \neq p'$ then $v_1(p) = v_0(p)$ else $v_1(p) = 0$. If $\vec{w}^T \cdot \vec{v}_1 \leq k$ stop else repeating this procedure construct $\vec{v}_2, \cdots, \vec{v}_{j+1}$ such that $M \geq \vec{v}_0 > \vec{v}_1 > \cdots > \vec{v}_{j+1}$ and $\vec{w}^T \cdot \vec{v}_{j+1} \leq k$ while $\vec{w}^T \cdot \vec{v}_j > k$. This means that $\vec{v}_j \in V$, hence $\vec{v}_j^T \cdot M = |Q_{v_j}| \Longrightarrow M \notin \mathcal{M}(W, \vec{k})$. $\diamond$

Let us compare GMEC with the most general kind of constraint that can be defined on the markings of a system, the *forbidden markings* constraint [4]. A forbidden marking constraint consists of an *explicit list* of markings F that we want to forbid.

Let us now consider a net system $\langle N, M_0\rangle$ and let F be any set of forbidden markings. Is it possible to find a set of GMEC $(W, \vec{k})$ equivalent to F, i.e., such that $R(N, M_0) \setminus F = R(N, M_0) \cap \mathcal{M}(W, \vec{k})$? In general the answer is no. In fact given three markings $M_1, M_2, M_3 \in R(N, M_0)$ with $M_3 = (M_1 + M_2)/2$ we have that $M_1, M_2 \in \mathcal{M}(W, \vec{k}) \Longrightarrow M_3 \in \mathcal{M}(W, \vec{k})$, since $\mathcal{M}(W, \vec{k})$ is a convex set. However, F may be chosen such that $M_1, M_2 \notin F$ and $M_3 \in F$. This proves that there may not exist a GMEC equivalent to a forbidden marking constraint.

It is possible to prove that for some classes of nets there exists a set of GMEC equivalent to any forbidden marking constraint.

Theorem 2. *Let $\langle N, M_0\rangle$ be a safe and conservative net system. Then given a set of forbidden markings F there exists a set of GMEC $(W, \vec{k})$ such that $R(N, M_0) \setminus F =$*

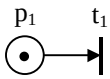

Figure 2: System in Example 5.

$R(N, M_0) \cap \mathcal{M}(W, \vec{k})$.

Proof: Let us first state two obvious facts. 1) If a net is safe there do not exist two different markings with the same support, i.e., $M, M' \in R(N, M_0) \wedge Q_M = Q_{M'} \Longrightarrow M = M'$. 2) If a net is conservative no marking is covering another one, i.e., $(\forall M \in R(N, M_0))$ $\nexists M' \in R(N, M_0) \ni M < M'$.

Then, given a set of forbidden markings F we may forbid any $M \in F$ with a constraint $(\vec{w}, k)$ where: $\vec{w}(p) = 1$ if $p \in Q_M$ else $\vec{w}(p) = 0$, and $k = |Q_M| - 1$. Clearly $M \notin \mathcal{M}(\vec{w}, k)$ and any other marking $M' \in R(N, M_0)$ is such that $M' \in \mathcal{M}(\vec{w}, k)$. Thus $(W, \vec{k})$ may be constructed as the union of all the GMEC constraints forbidding a marking in F. $\diamond$

The requirement that the net be conservative may be shown necessary by the following example.

Example 5. Consider the 1-bounded but not conservative system in Figure 2. The two possible markings of the system are $M_1 = (1)$ and $M_2 = (0)$. Clearly for a set of forbidden markings $F = \{(0)\}$ it is not possible to find an equivalent GMEC since $(\forall \vec{w}, k)$ $\vec{w}^T \cdot M_0 \leq \vec{w}^T \cdot M_1^T \leq k$.

4 Monitors

Definition 4. *Given a system $\langle N, M_0 \rangle$, with $N = (P, T, Pre, Post)$, and a GMEC $(\vec{w}, k)$, the* monitor *that enforces this constraint is a new place S to be added to N. The resulting system is denoted $\langle N^S, M_0^S \rangle$, with $N^S = (P \cup \{S\}, T, Pre^S, Post^S)$. Let C be the incidence matrix of N. Then N^S will have incidence matrix*

$$C^S = \begin{bmatrix} C \\ -\vec{w}^T \cdot C \end{bmatrix}.$$

We are assuming that there are no selfloops containing S in N^S, hence Pre^S and $Post^S$ may be uniquely determined by C^S. The initial marking of $\langle N^S, M_0^S\rangle$ is

$$M_0^S = \begin{pmatrix} M_0 \\ k - \vec{w}^T \cdot M_0 \end{pmatrix}.$$

We assume that the initial marking M_0 of the system satisfies the constraint $(\vec{w}, k)$.

As an example, in Figure 1b we have represented the two monitors corresponding to the two constraints discussed in Example 1.

Proposition 2. *Let $\langle N, M_0\rangle$ be a system, $(\vec{w}, k)$ a GMEC, and $\langle N^S, M_0^S\rangle$ the system with the addition of the corresponding monitor S.*

1) S ensures that the projection on P of the reachability set of $\langle N^S, M_0^S\rangle$ is contained in the set of legal reachable markings of $\langle N, M_0\rangle$, i.e., $R(N^S, M_0^S) \uparrow_P \subseteq R(N, M_0) \cap \mathcal{M}(\vec{w}, k)$.

2) S ensures that the projection on P of the potentially reachable set of $\langle N^S, M_0^S\rangle$ is identical to the set of legal potentially reachable markings of $\langle N, M_0\rangle$, i.e., $PR(N^S, M_0^S) \uparrow_P = PR(N, M_0) \cap \mathcal{M}(\vec{w}, k)$.

3) S minimally restricts the behavior of $\langle N^S, M_0^S\rangle$, in the sense that it prevents only transition firings that yield forbidden markings.

Proof:

1) Clearly $R(N^S, M_0^S) \uparrow_P \subseteq R(N, M_0)$, since the addition of a place can only further constrain the behavior of a system. To prove $R(N^S, M_0^S) \uparrow_P \subseteq \mathcal{M}(\vec{w}, k)$, let $M^S \in R(N^S, M_0^S)$ and $M = M^S \uparrow_P$. Then there exist $\vec{\sigma}$ such that $M^S = M_0^S + C^S \cdot \vec{\sigma}$ or, equivalently, $M = M_0 + C \cdot \vec{\sigma}$, and $M^S(S) = M_0^S(S) - \vec{w}^T \cdot C \cdot \vec{\sigma} = k - \vec{w}^T \cdot (M_0 + C \cdot \vec{\sigma}) \geq 0$. Hence $\vec{w}^T \cdot M = \vec{w}^T \cdot (M_0 + C \cdot \vec{\sigma}) \leq k$, i.e., $M \in \mathcal{M}(\vec{w}, k)$.

2) With the same reasoning of the previous point we can immediately conclude that $PR(N^S, M_0^S) \uparrow_P \subseteq PR(N, M_0) \cap \mathcal{M}(\vec{w}, k)$. Let us prove the reverse inclusion. Let $M \in PR(N, M_0) \cap \mathcal{M}(\vec{w}, k)$, i.e., $\exists \vec{\sigma} \geq 0$ such that $M = M_0 + C \cdot \vec{\sigma}$, and $\vec{w}^T \cdot M \leq k$. This implies that $\vec{w}^T (M_0 + C \cdot \vec{\sigma}) \leq k$, i.e., $k - \vec{w}^T \cdot (M_0 + C \cdot \vec{\sigma}) \geq 0$. Then we also have that

$$M^S = \begin{pmatrix} M \\ k - \vec{w}^T \cdot (M_0 + C \cdot \vec{\sigma}) \end{pmatrix}$$

is a non negative solution of $M^S = M_0^S + C^S \cdot \vec{\sigma}$, i.e., $M^S \in PR(N^S, M_0^S)$.

3) Let $\sigma t \in L(N, M_0)$ be such that: $M_0[\sigma\rangle M[t\rangle M'$ and $\sigma \in L(N^S, M_0^S)$ be such that:

$M_0^S[\sigma\rangle M^S$. We need to prove that $\sigma t \notin L(N^S, M_0^S) \Longrightarrow \vec{w}^T \cdot M' > k$. Let $C(\cdot, t)$ be the column of C corresponding to transition t. Then $Pre^S(S,t) - Post^S(t,S) = -C^S(S,t) = \vec{w}^T \cdot C(\cdot,t)$. Since t is not enabled by marking M^S and since there are no selfloops containing S, it follows that $0 \leq M^S(S) < Pre^S(S,t) \Longrightarrow Post^S(t,S) = 0$, i.e., $Pre^S(S,t) = \vec{w}^T \cdot C(\cdot,t)$. Then $k - \vec{w}^T \cdot M = M^S(S) < Pre^S(S,t) = \vec{w}^T \cdot C(\cdot,t)$, from which follows $\vec{w}^T \cdot M' = \vec{w}^T \cdot [M + C(\cdot,t)] > k$. ◇

The addition of a monitor to the net structure modifies the behavior of a system, in order to avoid reaching markings that do not satisfy the corresponding GMEC. We pinpoint three facts:

- The addition of a monitor does not always preserve liveness of the system.
- Not all markings that satisfy the GMEC may be reached on the net with the addition of a monitor. In the net in Figure 3, a monitor has been added to enforce the constraint $M(p_1) + M(p_3) \leq 1$. From the initial marking $M_0^S = (000111)^T$ the marking $M^S = (100010)^T$ will never be reached even if it is legal and $M^S \uparrow_P = (10001)^T$ belongs to the reachability set of the unconstrained net.
- Even if liveness is preserved, the system may lose reversibility, as shown in the system in Figure 3. In the same figure is shown the reachability graph of the original system (all arcs and states) and of the system with monitor (only continuous arcs). The initial marking, that satisfies the constraint, will never be reached again in the system with monitor.

5 Nets With Uncontrollable Transitions

We assume, now, that the set of transitions T of a net is partitioned into the two disjoints subsets T_u, the set of *uncontrollable* transitions, and T_c, the set of *controllable* transitions. A controllable transition may be disabled by the supervisor, a controlling agent which ensures that the behavior of the system is within a legal behavior. An uncontrollable transition represents an event which may not be prevented from occurring by a supervisor.

Given a system $\langle N, M_0\rangle$ and a set of GMEC $(W, \vec{k})$, the set of legal markings is given as a linear domain:

$$\mathcal{M}(W, \vec{k}) = \{M \in \mathbb{N}^{|P|} \mid W^T \cdot M \leq \vec{k}\}.$$

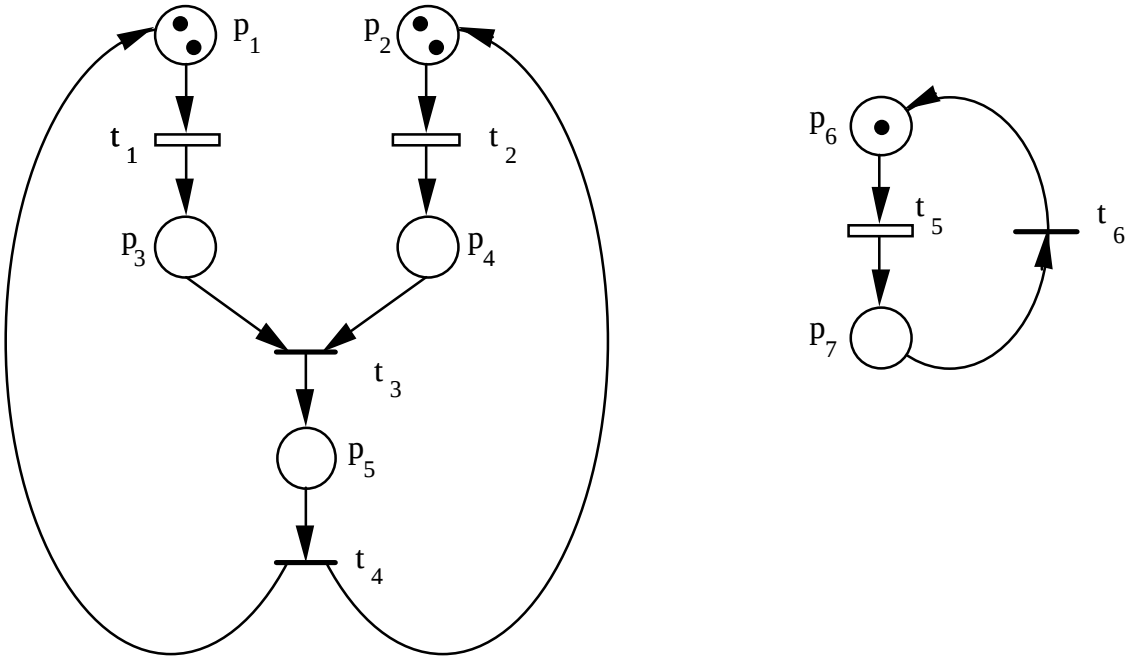

Figure 3: A system not reversible under constraint.

In the presence of uncontrollable transitions, we need to further restrict the behavior of the system, avoiding all those markings from which a forbidden marking may be reached by firing only uncontrollable transitions. The set of legal markings is in this case:
$\mathcal{M}_c(W, \vec{k}) = \mathcal{M}(W, \vec{k}) \setminus$
$\{M \in \mathbb{N}^{|P|} \mid \exists M' \notin \mathcal{M}(W, \vec{k}), M[\sigma\rangle M' \wedge \sigma \in T_u^*\}$,
i.e., we do not consider legal the markings that satisfy $(W, \vec{k})$ but from which a forbidden marking may be reached by firing only uncontrollable transitions. We need to introduce this restriction because a firing sequence $\sigma \in T_u^*$ may not be prevented by a controlling agent.

It is possible to prove that there may not exist a GMEC $(W, \vec{k})$ such that $R(N, M_0) \cap \mathcal{M}(W, \vec{k}) = R(N, M_0) \cap \mathcal{M}_c(\vec{w}, k)$. Thus we may have cases in which a monitor-based solution to a given mutual exclusion problem does not exist.

Example 6. In the net in Figure 4, we have represented as empty boxes the controllable transitions t_1, t_2, t_5. Assume we want to enforce a constraint $(\vec{w}, k)$ with $\vec{w} = (00100010)^T$ and $k = 1$, i.e., such that $M(p_5) + M(p_7) \leq 1$. Is is easy to see that the markings $M_1 = (2002001)^T$ and $M_2 = (0220001)^T$ are in $\mathcal{M}_c(\vec{w}, k)$, but $M = (1111001)^T = (M_1 + M_2)/2$ is not. Thus, there does not exist a GMEC $(W, \vec{k})$ such that $R(N, M_0) \cap \mathcal{M}(W, \vec{k}) =$

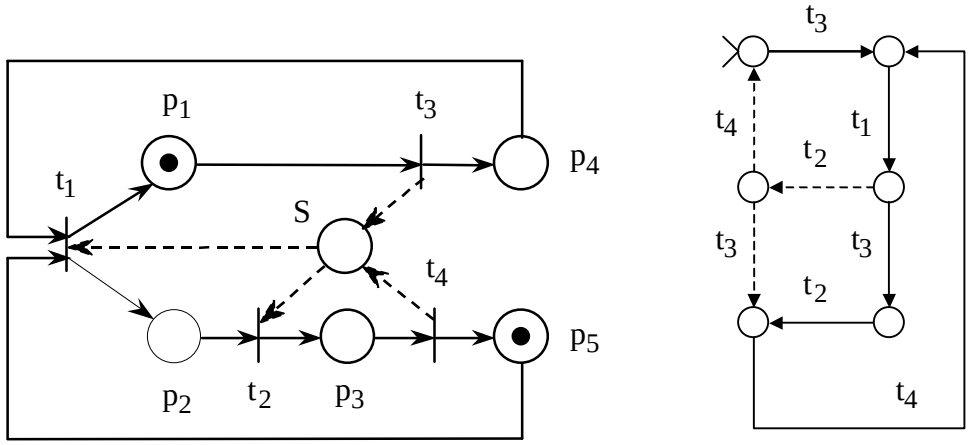

Figure 4: A mutual exclusion problem with uncontrollability that does not admit a monitor-based solution.

$R(N, M_0) \cap \mathcal{M}_c(\vec{w}, k)$.

The example shows that in presence of *uncontrollable* transitions, a problem of mutual exclusion is transformed into a more general *forbidden marking problem*, which is a qualitatively different problem, in the sense that it may not always be solved with the same techniques used in the case that all transitions are controllable. Note, however, that for safe and conservative systems the result of Theorem 2 ensures that, even if some transitions are not controllable, $(\vec{w}, k)$ may be enforced by a set of monitors.

6 Conclusions

We have presented and studied a class of specifications, called generalized mutual exclusion constraints. These specifications may be easily enforced on a net system where all transitions are controllable, by a set of places called monitors. Unfortunately, we have shown that this technique is not always applicable when some of the transitions of the net are uncontrollable.

For safe and conservative nets, we have proved that GMEC are equivalent to a forbidden marking specification and may always be enforced by monitors, even in the presence of uncontrollable transitions.

Future work will focus on the structure of the supervisors capable of enforcing GMEC on

nets with uncontrollable transitions.

References

[1] Z.A. Banaszak, B.H. Krogh, "Deadlock Avoidance in Flexible Manufacturing Systems with Concurrently Competing Process Flows," *IEEE Trans. on Robotics and Automation*, Vol. 6, No. 6, pp. 724–734, December, 1990.

[2] J.M. Colom, "Análisis Estructural de Redes de Petri, Programación Lineal y Geometria Convexa," *Tesis Doctoral*, Universidad de Zaragoza (Zaragoza, Spain), 1989.

[3] C.H. Golaszewski, P.J. Ramadge, "Mutual Exclusion Problems for Discrete Event Systems with Shared Events," *Proc. IEEE 27th Int. Conf. on Decision and Control* (Austin, Texas), pp. 234–239, December, 1988.

[4] L.E. Holloway, B.H. Krogh, "Synthesis of Feedback Control Logic for a Class of Controlled Petri Nets," *IEEE Trans. on Automatic Control*, Vol. 35, No. 5, pp. 514–523, May, 1990.

[5] B.H. Krogh, L.E. Holloway, "Synthesis of Feedback Control Logic for Discrete Manufacturing Systems," *Automatica*, Vol. 27, No. 4, pp. 641–651, July-August, 1991.

[6] T. Murata, " Petri Nets: Properties, Analysis and Applications," *Proceedings IEEE*, Vol. 77, No. 4, pp. 541–580, April, 1989.

[7] P.J. Ramadge, W.M. Wonham, "The Control of Discrete Event Systems," *Proceedings IEEE*, Vol. 77, No. 1, pp. 81–98, January, 1989.

[8] M. Silva, J.M. Colom, J. Campos, "Linear Algebraic Techniques for the Analysis of Petri Nets," *Proc. Int. Symp. on Mathematical Theory of Networks and Systems*, MITA Press, Tokyo, Japan, (to appear) 1992.

[9] N. Viswanadham, Y. Narahari, T.J. Johnson, "Deadlock Prevention and Deadlock Avoidance in Flexible Manufacturing Systems Using Petri Net Models," *IEEE Trans. on Robotics and Automation*, Vol. 6, No. 6, pp. 713–723, December, 1990.

[10] M.C. Zhou, F. DiCesare, "Parallel and Sequential Mutual Exclusions for Petri Net Modeling of Manufacturing Systems with Shared Resources," *IEEE Trans. on Robotics and Automation*, Vol. 7, No. 4, pp. 515–527, August, 1991.