Synthesis of Supervisors Enforcing Firing Vector Constraints in Petri Nets

Technical Report of the ISIS Group
at the University of Notre Dame
ISIS-2002-002
February, 2002

Marian V. Iordache and Panos J. Antsaklis
Department of Electrical Engineering
University of Notre Dame
Notre Dame, IN 46556, USA
E-mail: iordache.1@nd.edu, antsaklis.1@nd.edu

Interdisciplinary Studies of Intelligent Systems

Synthesis of Supervisors Enforcing Firing Vector Constraints in Petri Nets

Marian V. Iordache and Panos J. Antsaklis*

Abstract

This paper considers the problem of enforcing linear constraints containing marking terms, firing vector terms, and Parikh vector terms. Such constraints increase the expressivity power of the linear marking constraints. We show how this new type of constraints can be enforced in Petri nets. In the case of fully controllable and observable Petri nets, we give the construction of a supervisor enforcing such constraints. In the case of Petri nets with uncontrollable and/or unobservable transitions, we reduce the supervisor synthesis problem to enforcing linear marking constraints on a transformed Petri net.

1 Introduction

In this paper we consider a supervisory control problem for discrete event systems modeled as Petri nets, in which we desire to enforce a certain type of specifications. Thus we have a plant which is abstracted as a Petri net, and a specification on the behavior of the Petri net plant. We desire to find a supervisor such that the closed-loop of the plant and the supervisor satisfies the specification. We restrict our attention to supervisors which can be represented as Petri nets, and to specifications in the form of conjunctions of inequalities involving the marking, the firing vector and the Parikh vector of the plant Petri net. We describe such specifications next.

Efficient methods have been proposed in [1, 5, 4, 8] for the synthesis of supervisors enforcing that the marking μ of a Petri net satisfies constraints of the form

$$L\mu \leq b \tag{1}$$

The methods address both the fully controllable and observable Petri nets and the Petri nets which may have uncontrollable and unobservable transitions. The constraints (1) have been extended in [4, 8] to the form below

$$L\mu + Hq \leq b \tag{2}$$

*Department of Electrical Engineering, University of Notre Dame, IN 46556, USA. E-mail: iordache.1, antsaklis.1@nd.edu.

which adds a firing vector term. In such constraints an element q_i of the firing vector q is set to 1 if the transition t_i is to be fired next from μ; else $q_i = 0$. Without loss of generality, H has been assumed to have nonnegative elements. In this paper we consider constraints which add to (2) a Parikh vector term:

$$L\mu + Hq + Cv \leq b \tag{3}$$

In (3) v is the Parikh vector, that is v_i counts how often the transition t_i has fired since the initial marking μ_0. As an example, Parikh vector constraints can be used to describe fairness requirements, such as the constraint that the difference between the number of firings of two transitions is limited by one. Adding the Parikh vector term in (3) increases the expressivity power of linear constraints. In fact, any supervisor implemented as additional places connected to the transitions of a plant Petri net can be represented by constraints of the form

$$Hq + Cv \leq b \tag{4}$$

The contribution of this paper is as follows. In sections 2.1 and 2.2 we show that any place of a Petri net can be seen as a supervisor place enforcing a constraint of the form (4). Previously this property was known for constraints of the form $Cv \leq b$ and Petri nets without self-loops [3]. Then we show how to obtain supervisors enforcing constraints (3) in Petri nets. We first give the solution for the case of fully controllable and observable Petri nets in section 2.3. Then, in section 2.4 we turn our attention to Petri nets which may have uncontrollable and unobservable transitions. There we first define admissible constraints as the constraints for which the method for fully controllable and observable Petri nets can still be used. Admissibility tests are provided. Then, by using net transformations, we reduce our problem to the supervisory synthesis problem for constraints of the form (1), for which effective methods exist. Our approach also extends the indirect method of [4] on enforcing constraints (2), as both coupled and uncoupled constraints can be considered. Finally, an example is given in section 2.5.

In the literature, Parikh vector constraints and marking constraints have been separately considered for vector DES (VDES) in [3]. The VDES considered in [3] correspond to Petri nets without self-loops. It has been shown there how to construct the optimal controller via integer programming. A less computationally burdensome approach, however not always optimal, has been given in [5, 4], which considers marking constraints and firing vector constraints. This paper extends some of the approaches of [5, 4] by including the Parikh vector constraints of [3].

2 Constraints Involving the Parikh Vector

2.1 An alternative algebraic representation of Petri nets

We will denote by D the incidence matrix, and by D^+ and D^- its components corresponding to weights of arcs from transitions to places, and weights of arcs from places to transitions, respectively.

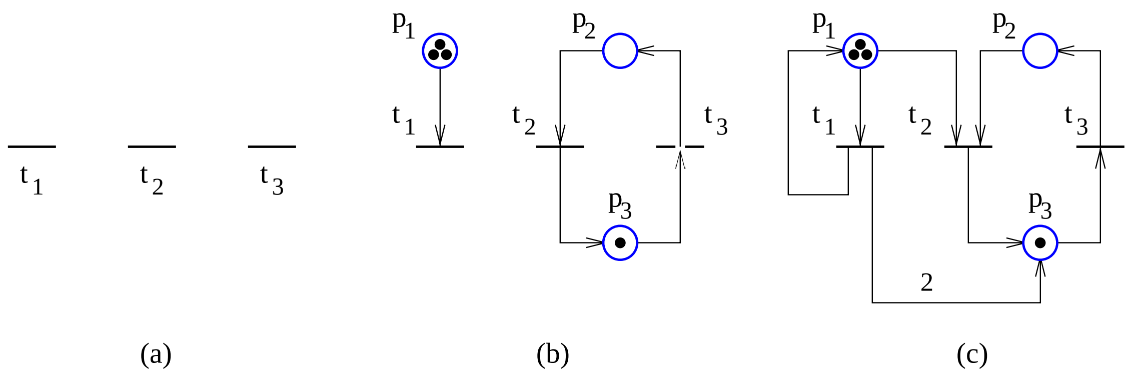

Figure 1: Petri nets for Example 2.1

The common algebraic Petri net representation is via the following state equation:

$$\mu = \mu_0 + Dv \tag{5}$$

where μ is the marking, μ_0 is the initial marking, D the incidence matrix, and v is the **Parikh vector**; that is, for all i, v_i counts how often the transition t_i has fired since the initial marking. The operation of a Petri net can also be described through inequalities of the form (4). Indeed, from (5) we derive:

$$(-D)v \leq \mu_0 \tag{6}$$

Let $C = -D$. The inequality $Cv \leq \mu_0$ determines the operation of a Petri net only if the net has no self-loops. To deal with self-loops, an additional term is introduced:

$$Hq + Cv \leq \mu_0 \tag{7}$$

where

$$H_{i,j} = \begin{cases} D^+_{i,j} & \text{if } D^-_{i,j} \neq 0 \\ 0 & \text{otherwise} \end{cases} \tag{8}$$

Note that $H_{i,j} \geq 0$ for all indices i and j. The vector q has the following meaning. After we fire from μ_0 a sequence σ of firing vector v, the transition t_i is enabled iff $Hq^{(i)} + C(v + q^{(i)}) \leq \mu_0$, where $q^{(i)}$ is the vector with zero elements except for the i'th one, which is one. We summarize this result in the following proposition:

Proposition 2.1 *Let σ be a firing sequence, v the firing vector corresponding to σ, and $\mu_0 \xrightarrow{\sigma} \mu$. The transition t_i is enabled by μ iff $Hq^{(i)} + C(v + q^{(i)}) \leq \mu_0$, where $q^{(i)}$ has all elements zero except for the i'th, which is one.*

Example 2.1 Consider the Petri nets of Figure 1. The Petri net (a) is not restricted: the firings of t_1, t_2 and t_3 are free. Thus H and C are empty matrices. By adding the places p_1, p_2 and p_3 as in the Petri net (b), we obtain the following inequalities for (7):

$$v_1 \leq 3 \quad (9)$$

$$v_2 - v_3 \leq 0 \quad (10)$$

$$-v_2 + v_3 \leq 1 \quad (11)$$

where the inequalities are generated, in this order, by p_1, p_2, and p_3. The inequalities of the Petri net (c) are:

$$q_1 + v_2 \leq 3 \quad (12)$$

$$v_2 - v_3 \leq 0 \quad (13)$$

$$-2v_1 - v_2 + v_3 \leq 1 \quad (14)$$

Note that both μ and v can describe the state of a Petri net. We choose to denote by $\mathcal{R}(\mathcal{N}, \mu_0)$ all pairs (μ, v) such that $\mu_0 \xrightarrow{\sigma} \mu$, and the Parikh vector of the firing sequence σ is v.

In the literature it has been noticed that Petri nets without self-loops correspond to inequalities $Cv \leq \mu_0$ [3]. In this section we have shown how to represent general Petri nets, which may also have self-loops.

2.2 Enforcing Generalized Linear Constraints

We consider the problem of enforcing constraints via supervision. Given a Petri net $\mathcal{N} = (P, T, F, W)$, we restrict our attention to supervisors which are defined as follows. Let[1] $\mathcal{M} \subseteq \mathbb{N}^{|P|} \times \mathbb{N}^{|T|}$. A **supervisor** of $\mathcal{N}$ is a map $\Xi : \mathcal{M} \to 2^T$ which associates to each state (μ, v) the set of transitions which may fire. For simplicity, we will also call *supervisor* the Petri net implementation of a supervisor Ξ. We say that $\mathcal{N}$ is in **closed-loop** with Ξ if Ξ supervises the operation of $\mathcal{N}$. When $\mathcal{N}$ has the state (μ, v) and $\mathcal{N}$ is supervised by Ξ, a transition t cannot be fired unless $(\mu, v) \in \mathcal{M}$ and $t \in \Xi(\mu, v)$. We denote by $(\mathcal{N}, \mu_0, \Xi)$ the Petri net $(\mathcal{N}, \mu_0)$ in closed-loop with Ξ. Given $(\mathcal{N}, \mu_0, \Xi)$, we denote the set of all reachable states (μ, v) by $\mathcal{R}(\mathcal{N}, \mu_0, \Xi)$.

Next we define the type of constraints we desire to enforce via supervision. In [5, 8], constraints of the form

$$L\mu + Hq \leq b \quad (15)$$

have been considered. We propose the following generalized form:

$$L\mu + Hq + Cv \leq b \quad (16)$$

The generalized type of constraints is more expressive. As an example, consider the Petri net of Figure 2. There is no place invariant involving the control place C, so the control place cannot be

[1] $|X|$ denotes the number of elements of X.

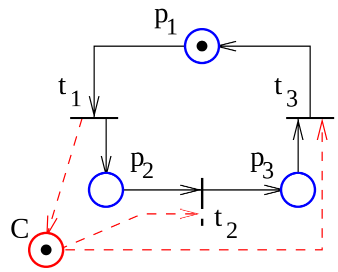

Figure 2:

described by (15). However the following constraint in the form (16) describes it:

$$-v_1 + v_2 + v_3 \leq 1$$

In fact, every place of a Petri net can be seen as a control place restricting the firings of the net transitions. This result is stated next.

Proposition 2.2 *Every place of a Petri net can be seen as a control place enforcing a single inequality of the form (16).*

Proof: The proof follows immediately from (7) and (8). Thus, the constraint of each place p_i is $hq + cv \leq \mu_{0i}$, where h and c are the i'th rows of H and C. $\square$

It can be noticed that negative entries in H have no effect. Therefore, without loss of generality, we can assume that

$$H_{ij} \geq 0 \tag{17}$$

for all indices i and j.

We say that a supervisor Ξ **enforces** (16) on a Petri net $(\mathcal{N}, \mu_0)$ if $\forall(\mu, v) \in \mathcal{R}(\mathcal{N}, \mu_0, \Xi)$: (16) is satisfied. We say that Ξ **optimally enforces** (16) if $\forall(\mu, v) \in \mathcal{R}(\mathcal{N}, \mu_0, \Xi)$: (a) Ξ is defined at (μ, v), and (b) a transition t_i enabled in the plant $(\mathcal{N}, \mu)$ is disabled by Ξ at (μ, v) (i.e. $t_i \notin \Xi(\mu, v)$) iff firing t_i leads to a state (μ', v') such that $L\mu' + Cv' \not\leq b$ or $L\mu + Hq^{(i)} + Cv \not\leq b$, where $q^{(i)}$ is the vector q corresponding to firing t_i.

2.3 Supervisor design in the fully controllable and observable case

In the case of Petri nets in which all transitions are controllable and observable, it is possible to optimally enforce constraints of the form (16). The method below appears as a simple extension of the formulas given in [6] for constraints of the form (15). Thus we first define:

$$D_{lc}^{+} = \max(0, -LD - C) \tag{18}$$

$$D_{lc}^{-} = \max(0, LD + C) \tag{19}$$

Then we define:

$$D_c^+ = D_{lc}^+ + \max(0, H - D_{lc}^-) \tag{20}$$

$$D_c^- = \max(D_{lc}^-, H) \tag{21}$$

Note that in equations (18-21) the operator max is defined as follows. If A is a matrix, $B = \max(0, A)$ is the matrix of elements $B_{ij} = 0$ for $A_{ij} < 0$, and $B_{ij} = A_{ij}$ for $A_{ij} \geq 0$. For two matrices A and B of the same size, $C = \max(A, B)$ is the matrix of elements $C_{ij} = \max(A_{ij}, B_{ij})$.

The matrices D_c^+ and D_c^- describe a Petri net structure with the same transitions as the plant. This Petri net structure represents the Petri net implementation of the supervisor. The initial marking μ_{c0} of the supervisor depends on the initial marking μ_0 of the plant as follows:

$$\mu_{c0} = b - L\mu_0 \tag{22}$$

We call the places of the supervisor **control places**.

Theorem 2.1 *Assume that we have a fully controllable and observable Petri net of incidence matrix D and initial marking μ_0. Assume also that μ_0 satisfies (16). The supervisor defined by the incidence matrices D_c^+ and D_c^- of (20) and (21) and of initial marking given by (22) is a supervisor optimally enforcing (16).*

Proof: First we prove that throughout the operation of the closed-loop PN, the supervisor marking μ_c satisfies

$$\mu_c = b - Cv - L\mu \tag{23}$$

Then we prove that a transition t_i is enabled if and only if $L\mu' + Cv' \leq b$ and $L\mu + Hq^{(i)} + Cv \leq b$, where μ' is the marking that would be reached by firing t_i, i.e. $\mu' = \mu + Dq^{(i)}$, $v' = v + q^{(i)}$, and $q^{(i)}$ is the column vector with the i-th entry one and the other entries zero.

The initial marking of the supervisor satisfies (23), as the initial value of v is 0. Now, assume (23) satisfied and consider firing a transition t_i. Let μ_c' be the next reached supervisor marking. Since $\mu' = \mu + Dq^{(i)}$, we are to prove that $\mu_c' = \mu_c - (C + LD)q^{(i)}$. Note that $\mu_c' = \mu_c - (C + LD)q^{(i)}$ $\Leftrightarrow$ $\mu_c' = \mu_c + (D_{lc}^+ - D_{lc}^-)$. In view of (20) and (21), for all indices j, if $H_{ji} \geq D_{lc,ji}^-$, then $\mu_{c,j}' = \mu_{c,j} + (D_c^+ - D_c^-)_{ji} \Leftrightarrow \mu_{c,j}' = \mu_{c,j} + (D_{lc}^+ - D_{lc}^-)_{ji}$. The same can be verified in the case $H_{ji} \leq D_{lc,ji}^-$. Therefore we can conclude that $\mu_c' = \mu_c - (C + LD)q^{(i)}$.

Note that as μ_c satisfies (23) and $\mu_c \geq 0$, we have that $L\mu + Cv \leq b$. The transition t_i enabled in the plant is also enabled in the closed-loop if and only if $\mu_c \geq D_c^- q^{(i)} \Leftrightarrow \mu_c \geq \max(0, LD + C, H)q^{(i)}$ $\Leftrightarrow [\mu_c \geq \max((LD + C)q^{(i)}, Hq^{(i)})] \wedge [\mu_c \geq 0] \Leftrightarrow (L\mu' + Cv' \leq b) \wedge (L\mu + Hq^{(i)} + Cv \leq b) \wedge (L\mu + Cv \leq b)$. This concludes the proof. □

The proof of the theorem has shown that the supervisor marking μ_c always satisfies (23). This implies that the supervisors we build for (16) may not create a place invariant. Note also that if we substitute (22) and $\mu = \mu_0 + Dv$ in (23), we have that

$$\mu_c = \mu_{c0} - (C + LD)v \tag{24}$$

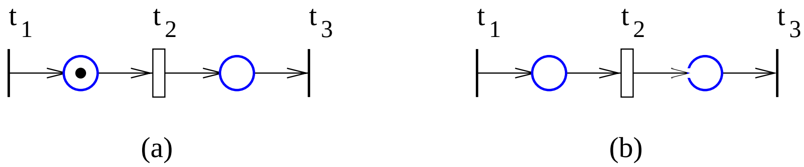

Figure 3:

2.4 Supervisor design in the case of Petri nets with uncontrollable and/or unobservable transitions

2.4.1 Admissibility

We say that a transition is uncontrollable if the supervisors are not given the ability to directly inhibit it. A transition is unobservable if the supervisors are not given the ability to directly detect its firing. In our paradigm the supervisors observe transition firings, not markings. For instance, consider the Petri net of Figure 3. First assume that t_1 is controllable and t_2 is uncontrollable. Then in case (a) t_2 cannot be directly inhibited; it will eventually fire. However in case (b) t_2 can be indirectly prevented to fire by inhibiting t_1. Now assume that t_2 is unobservable and t_3 is observable. This means that we cannot detect when t_2 fires. In other words, the state of a supervisor is not changed by firing t_2. However we can indirectly detect that t_2 has fired, by detecting the firing of t_3.

We are interested in *admissible* constraints, that is constraints which can be optimally enforced as in section 2.3, in spite of our inability to detect or control certain transitions. We formally define admissibility as follows.

Definition 2.1 *Let $(\mathcal{N}, \mu_0)$ be a Petri net. Assume that we desire to enforce a set of constraints (16). Consider the supervisor defined by (20), (21), and (22). We say that the constraints (16) are* **admissible** *if for all reachable states (μ, v) of the closed-loop net it is true that:*

1. *If t is uncontrollable and t is enabled by*[2] *$\mu|_{\mathcal{N}}$ in $\mathcal{N}$, then t is enabled by μ in the closed-loop net.*

2. *If t is unobservable and t is enabled by μ, firing t does not change the marking of the control places.*

Note that condition 2 in the definition corresponds to the requirement that the unobservable transitions which are not dead at the initial marking of the closed-loop net, have null columns in $D_c = D_c^+ - D_c^-$ (where D_c^+ and D_c^- are defined in (20) and (21)). For general Petri nets it may not be easy to check whether a constraint is admissible. However, when the supervisor part of the closed-loop Petri net is bounded, we have the following algorithm:

[2]We denote by $\mu|_{\mathcal{N}}$ the restriction of μ to the places of $\mathcal{N}$.

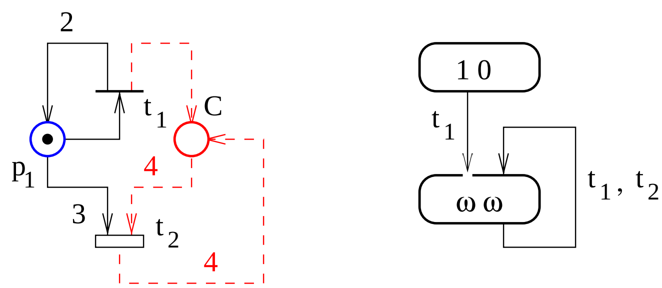

Figure 4:

1. Construct the coverability graph of the closed-loop Petri net. (The usual coverability graph construction is proposed; see [2, p. 171] or [7, pp. 66-71].)

2. For every node of the graph check the following:

   Let μ be the marking labeling the current graph node

   (a) Is any uncontrollable transition not enabled by μ, but enabled by $\mu|_{\mathcal{N}}$ in $\mathcal{N}$? Then exit and declare that the constraints are inadmissible.

   (b) Is any unobservable transition enabled by μ such that firing t changes the marking of the control places? Then exit and declare that the constraints are inadmissible.

3. Declare the constraints admissible.

The example of Figure 4 shows that it is not easy to extend the algorithm when the supervisor part of the closed-loop Petri net is unbounded. In the example, t_2 is uncontrollable and C is the control place corresponding to the constraint $4q_2 - v_1 \leq 0$. It can be seen that we cannot detect from the coverability graph of the closed-loop net (constructed with the usual approach [2, 7]) that the constraint is inadmissible.

2.4.2 Structural admissibility analysis

The coverability graph computation is usually time expensive. Alternatively, we may attempt to do a structural admissibility analysis. Structural admissibility analysis attempts to prove admissibility properties based on the structure of the Petri net, rather than the initial marking. Thus, from the structural perspective, the question is whether the constraints are admissible for all initial markings satisfying them or not.

A computationally simple test for marking constraints $L\mu \leq b$ to be admissible is that $LD_{uc} \leq 0$ and $LD_{uo} = 0$ [4, 5], where D_{uc} and D_{uo} are the restrictions of the incidence matrix D of the plant to the uncontrollable and unobservable transitions, respectively. In terms of the Petri net representing the supervisor, this corresponds to requiring $D^-_{c,uc}$ and $D_{c,uo}$ to have null columns, where $D^-_{c,uc}$ and $D_{c,uo}$ are the restrictions of D^-_c and D_c to the columns of the uncontrollable and unobservable transitions, respectively. It can be easily seen that requiring $D^-_{c,uc}$ and $D_{c,uo}$ to be null matrices is also a sufficient condition for admissibility in the case of the general constraints (16). This is stated in the next proposition.

Proposition 2.3 *The constraints (16) are admissible at all initial markings if both $D_{c,uo}$ and $D^-_{c,uc}$ are null matrices.*

The condition $D_{c,uo} = 0$ ensures that for any uncontrollable transition, a control place is either not connected to it, or is connected to it with input and output arcs of equal weight. The condition $D^-_{c,uc} = 0$ insures that no control place is in the preset of an uncontrollable transition.

Let $T_{r,uc}$ be the set of uncontrollable transitions with nonzero columns in $D^-_{c,uc}$. Similarly, let $T_{r,uo}$ be the set of unobservable transitions with nonzero columns in $D_{c,uo}$. The following algorithm could be used to identify constraints which are indamissible for some initial markings.

1. Assume $v = 0$ and check whether there are initial markings μ of the plant such that
   (a) (16) is satisfied.
   (b) $\exists t \in T_{r,uc}$: t is enabled by the plant and disabled by the supervisor.

   If such markings μ exist, exit and declare that the constraints (16) are inadmissible for some initial markings.

2. Assume $v = 0$ and check whether there are initial markings μ of the plant such that
   (a) (16) is satisfied.
   (b) $\exists t \in T_{r,uo}$: t is enabled in the closed-loop.

   If such markings μ exist, exit and declare that the constraints (16) are inadmissible for some initial markings.

3. Repeat the checks from the steps 1 and 2 for $v \geq 0$ rather than $v = 0$. If no μ and v exist such that the conditions of either of step 1 or step 2 are satisfied, declare the constraints (16) admissible for all initial markings satisfying them.

The operations of the steps 1 and 2 may require solving integer programs.

2.4.3 On transformations to admissible constraints

When a constraint is admissible, it can be enforced as in section 2.3. However, when a constraint is not admissible or we cannot discern whether it is admissible, we are interested to transform it to a form which we know is admissible. Thus we have the following problem. Given a set of constraints (16) on a Petri net $(\mathcal{N}, \mu_0)$, find a set of admissible constraints

$$L_a\mu + H_aq + C_av \leq b_a \tag{25}$$

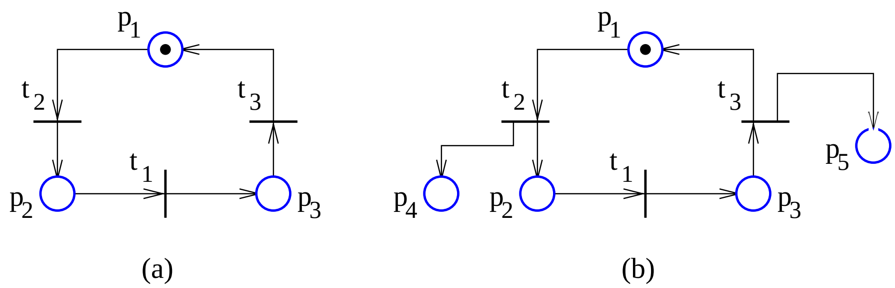

Figure 5: Illustration of the C-transformation.

such that if Ξ is a supervisor optimally enforcing (25) on $(\mathcal{N}, \mu_0)$, then $\forall(\mu, v) \in \mathcal{R}(\mathcal{N}, \mu_0, \Xi)$: (16) is satisfied.

We consider a transformation approach in which we transform the Petri net such that the constraints (16) are mapped into marking constraints. Then the marking constraints can be transformed to admissible constraints using, for instance, one of the approaches in [4, 5]. We begin by defining the transformations we use.

2.4.4 The C-Transformation

We illustrate the idea of the transformation on an example. Consider the Petri net of Figure 5(a), and assume that we desire to enforce the following constraint of the form (16):

$$\mu_1 + q_1 + v_2 - v_3 \leq 3 \tag{26}$$

The idea of the transformation is to transform the net such that the Cv term is transformed into a marking term. This is why we call the transformation C-transformation. Thus, by transforming the net as in Figure 5(b), (26) can be written without referring to v:

$$\mu_1 + q_1 + \mu_4 - \mu_5 \leq 3 \tag{27}$$

We say that the Petri net of Figure 5(b) and the constraint (27) are the C-transformation of the Petri net of Figure 5(a) and of (26).

The inverse C-transformation is also possible. Given the constraint

$$\mu_1 - 3\mu_4 + 2\mu_5 + q_1 \leq 5 \tag{28}$$

on the Petri net of Figure 5(b), we can map it to

$$\mu_1 + q_1 - 3v_4 + 2v_5 \leq 5 \tag{29}$$

in the original Petri net. We proceed next to formally define the direct and inverse transformations.

The C-Transformation

Input: The Petri net $\mathcal{N} = (P, T, F, W)$, the constraints $L\mu + Hq + Cv \leq b$, and optionally the initial marking μ_0.

Output: The C-transformed Petri net $\mathcal{N}_C = (P_C, T, F_C, W_C)$, the C-transformed constraint $L_C\mu_C + Hq \leq b$, and the initial marking μ_{0C} of $\mathcal{N}_C$.

1. Initialize $\mathcal{N}_C$ to equal $\mathcal{N}$, L_C to L, and let $k = |P|$.
2. For $i = 1$ to $|T|$

   If C_i, the i'th column of C, is not zero

   i. Set $k = k + 1$

   ii. Add a new place p_k to $\mathcal{N}_C$ such that $p_k\bullet = \emptyset$ and $\bullet p_k = \{t_i\}$.

   iii. Set $L_C = [L_C, C_i]$ and $\mu_{0C} = [\mu_{0C}^T, 0]^T$.

The C^{-1}-Transformation

Input: The Petri net $\mathcal{N} = (P, T, F, W)$, the C-transformed net $\mathcal{N}_C = (P_C, T, F_C, W_C)$, and a set of constraints $L_C\mu_C + Hq \leq b$ on $\mathcal{N}_C$.

Output: The C^{-1}-transformed constraint $L\mu + Hq + Cv \leq b$.

1. Set L to L_C restricted to the first $|P|$ columns and C to be a null matrix.
2. For $i = |P| + 1$ to $|P_C|$

   (a) Let j be the transition index such that $\bullet p_i = \{t_j\}$.

   (b) Set $C_j = L_{C,i}$. [3]

Lemma 2.1 *Consider the notations of the C-transformation. We have that:*

1. $L\mu + Hq + Cv \leq b$ *is admissible in* $(\mathcal{N}, \mu_0)$ *if* $L_C\mu_C + Hq \leq b$ *is admissible in* $(\mathcal{N}_C, \mu_{0C})$.
2. *Let* $L_1\mu + H_1q + C_1v \leq b_1$ *be a set of constraints in* $\mathcal{N}$, *and* $L_{C1}\mu_C + H_1q \leq b_1$ *the corresponding constraints in the C-transformed net* $\mathcal{N}_C$. *Let* $L_{C2}\mu_C + H_2q \leq b_2$ *be a set of admissible constraints in* $(\mathcal{N}_C, \mu_{0C})$, *and* $L_2\mu + H_2q + C_2v \leq b_2$ *be the* C^{-1}*-transformation of* $L_{C2}\mu_C + H_2q \leq b_2$. *Let* Ξ_C *be a supervisor optimally enforcing* $L_{C2}\mu_C + H_2q \leq b_2$ *in* $(\mathcal{N}_C, \mu_{0C})$, *and* Ξ *a supervisor optimally enforcing* $L_2\mu + H_2q + C_2v \leq b_2$ *in* $(\mathcal{N}, \mu_0)$. *Then* $(\forall(\mu_C, v_C) \in \mathcal{R}(\mathcal{N}_C, \mu_{0C}, \Xi_C)$: $L_{C1}\mu_C + H_1q \leq b_1) \Rightarrow (\forall(\mu, v) \in \mathcal{R}(\mathcal{N}, \mu_0, \Xi)$: $L_1\mu + H_1q + C_1v \leq b_1)$.

The proof of this lemma can be carried out similarly to the proof of Lemma 2.2, in the next section.

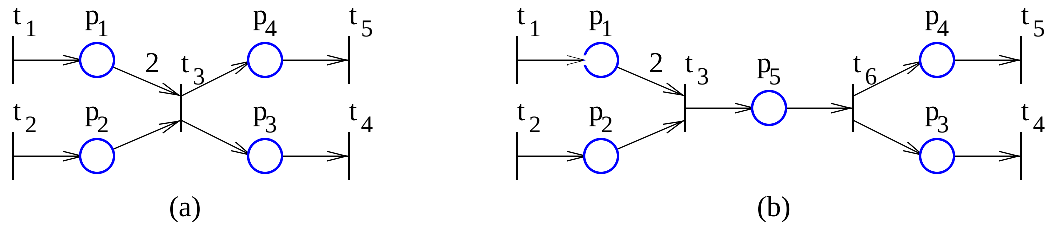

Figure 6: Example for the H-transformation.

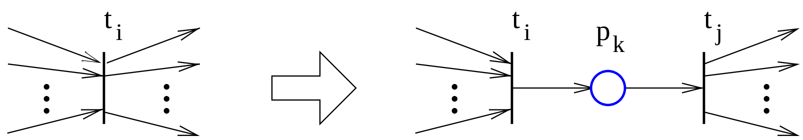

Figure 7: Illustration of the transition split operation.

2.4.5 The H-transformation

This transformation is a modification of the indirect method for enforcing firing vector constraints in [5]. We illustrate it on an example. Consider the Petri net of Figure 6(a). Assume that we desire to enforce

$$\mu_1 + \mu_2 + 2\mu_3 + q_3 \leq 5 \tag{30}$$

Then we transform the Petri net as shown in Figure 6(b). The transformation adds a place and a transition which correspond to the factor q_3. The transformed constraint is

$$\mu_1 + \mu_2 + 2\mu_3 + 4\mu_5 \leq 5 \tag{31}$$

where the term $5\mu_5$ is obtained as follows. Consider firing t_3 in the transformed net. If $\mu \xrightarrow{t_3} \mu'$ and a is the coefficient of μ_5, we desire

$$a + \mu'_1 + \mu'_2 + 2\mu'_3 = 1 + \mu_1 + \mu_2 + 2\mu_3$$

where the factor 1 is the coefficient of q_3 in (30). Thus we obtain $a = 5$.

Next we formally define the H-transformation.

The H-Transformation

Input: The Petri net $\mathcal{N} = (P, T, F, W)$, the constraints $L\mu + Hq \leq b$, and optionally the initial marking μ_0.

Output: The H-transformed Petri net $\mathcal{N}_H = (P_H, T_H, F_H, W_H)$, the H-transformed constraint $L_H\mu_H \leq b$, and the initial marking μ_{0H} of $\mathcal{N}_H$.

[3] $C_j/L_{C,i}$ is the column j/i of C/L_C.

1. Initialize $\mathcal{N}_H$ to equal $\mathcal{N}$, L_H to L, and let $j = |T|$ and $k = |P|$.

2. For $i = 1$ to $|T|$

   If H_i, the i'th column of H, is not zero

   i. Set $j = j + 1$ and $k = k + 1$.

   ii. Add a new place p_k and a new transition t_j to $\mathcal{N}_H$ as in Figure 7, where t_j has the same controllability and observability attributes as t_i.

   iii. Set $L_H = [L_H,\, H_i + LD_i^-]$ and $\mu_{0H} = [\mu_{0H}^T,\, 0]^T$, where D_i^- is the i'th column of D^-, and D^- corresponds to $\mathcal{N}$.

The H^{-1}-Transformation

Input: The Petri net $\mathcal{N} = (P, T, F, W)$, the H-transformed net $\mathcal{N}_H = (P_H, T_H, F_H, W_H)$, and a set of constraints $L_H\mu_H \leq b$ on $\mathcal{N}_H$.

Output: The H^{-1}-transformed constraint $L\mu + Hq \leq b$.

1. Set L to L_H restricted to the first $|P|$ columns and H to be a null matrix.

2. For $k = |P| + 1$ to $|P_H|$

   (a) Let i be the transition index such that $\bullet p_k = \{t_i\}$.

   (b) Set $H_i = L_{H,k} - L_H D_{H,i}^-$. [4]

Lemma 2.2 *Consider the notations of the H-transformation. We have that:*

1. *$L\mu + Hq \leq b$ is admissible in $(\mathcal{N}, \mu_0)$ if $L_H\mu_H \leq b$ is admissible in $(\mathcal{N}_H, \mu_{0H})$.*

2. *Let $L_1\mu + H_1q \leq b_1$ be a set of constraints in $\mathcal{N}$, and $L_{H1}\mu_H \leq b_1$ the corresponding constraints in the H-transformed net $\mathcal{N}_H$. Let $L_{H2}\mu_H \leq b_2$ be a set of admissible constraints in $(\mathcal{N}_H, \mu_{0H})$ and $L_2\mu + H_2q \leq b_2$ be the H^{-1}-transformation of $L_{H2}\mu_H \leq b_2$. Let Ξ_H be a supervisor optimally enforcing $L_{H2}\mu_H \leq b_2$ in $(\mathcal{N}_H, \mu_{0H})$, and Ξ a supervisor optimally enforcing $L_2\mu + H_2q \leq b_2$ in $(\mathcal{N}, \mu_0)$. Then $(\forall(\mu_H, v_H) \in \mathcal{R}(\mathcal{N}_H, \mu_{0H}, \Xi_H)$: $L_{H1}\mu_H \leq b_1) \Rightarrow (\forall(\mu, v) \in \mathcal{R}(\mathcal{N}, \mu_0, \Xi)$: $L_1\mu + H_1q \leq b_1)$.*

Proof: First, we introduce the following notation. If a transition t_i is split in the H-transformation as in Figure 7, let $\sigma_H(t_i)$ be the firing sequence t_it_j. If a transition t_i is not split, let $\sigma_H(t_i)$ equal t_i. If $\sigma = t_1t_2\ldots$ is a firing sequence in $\mathcal{N}$, let $\sigma_H(\sigma) = \sigma_H(t_1)\sigma_H(t_2)\ldots$.

1. The proof is by contradiction. Assume that $L\mu + Hq \leq b$ is not admissible. Let Ξ be the supervisor of $(\mathcal{N}, \mu_0)$ in Definition 2.1. Similarly, let Ξ_H be the supervisor of $(\mathcal{N}_H, \mu_{0H})$ in

[4] $H_i/L_{H,k}/D_{H,i}^-$ is the column $i/k/i$ of $H/L_H/D_H^-$, and D_H^- corresponds to $\mathcal{N}_H$.

Definition 2.1. Then there is a (possibly empty) sequence $\sigma = t_1 t_2 \dots t_k$ in $(\mathcal{N}, \mu_0, \Xi)$ such that $\mu_0 \xrightarrow{t_1} \mu_1 \xrightarrow{t_2} \mu_2 \dots \mu_k$, μ_k does not satisfy the requirements 1 and/or 2 of Definition 2.1, but all of $\mu_0 \dots \mu_{k-1}$ satisfy them. Then it can be seen that in $(\mathcal{N}_H, \mu_{0H}, \Xi_H)$ we have that $\mu_{0H} \xrightarrow{\sigma_H(\sigma)} \mu_{kH}$, where $\mu_{kH}(p) = 0$ for all places p created in the step ii of the H-transformation, and $\mu_k = \mu_{kH}|_{\mathcal{N}}$.

Case 1: μ_k does not satisfy the requirement 1 of Definition 2.1. Then there is an uncontrollable transition t_i of $\mathcal{N}$ such that at the marking μ_k we have that t_i is disabled by Ξ and t_i is enabled in the plant $\mathcal{N}$. Let μ_{k+1} and $\mu_{k+1,H}$ be the markings obtained by firing t_i and $\sigma_H(t_i)$ in the plants $\mathcal{N}$ and $\mathcal{N}_H$, respectively. Note that: $L\mu_k = L_H \mu_{kH}$ and $L\mu_{k+1} = L_H \mu_{k+1,H}$. We have two possibilities: (a) $\sigma_H(t_i) = t_i$; (b) $\sigma_H(t_i) = t_i t_j$. In case (a), $L\mu_{k+1} \not\leq b$, so $L_H \mu_{k+1,H} \not\leq b$. Therefore Ξ_H has to disable the uncontrollable transition t_i, which is a contradiction, since $L_H \mu_H \leq b$ is admissible. In case (b), let μ'_{kH} be the marking of $\mathcal{N}_H$ such that $\mu_{kH} \xrightarrow{t_i} \mu'_{kH}$. We have that either $L\mu_k + H_i q^{(i)} \not\leq b$ or $L\mu_{k+1} \not\leq b$. Note that $L_H \mu'_{kH} = L\mu_k + H_i q^{(i)}$ and $L_H \mu_{k+1,H} = L\mu_{k+1}$. The first situation implies that Ξ_H disables the uncontrollable transition t_i, while the second that Ξ_H disables the uncontrollable transition t_j. Both are a contradiction.

Case 2: μ_k does not satisfy the requirement 2 of Definition 2.1. Then there is an unobservable transition t_i of $\mathcal{N}$ such that at the marking μ_k we have that t_i is enabled, Ξ allows it to fire, $\mu_k \xrightarrow{t_i} \mu_{k+1}$, and $L\mu_k \neq L\mu_{k+1}$. Using the same notation as in Case 1, we have that $L_H \mu_{kH} \neq L_H \mu_{k+1,H}$. If $\sigma_H(t_i) = t_i$, this contradicts that $L_H \mu_H \leq b$ is admissible. If $\sigma_H(t_i) = t_i t_j$, either $L_H \mu_{kH} \neq L_H \mu'_{kH}$ or $L_H \mu'_{kH} \neq L_H \mu_{k+1,H}$; both contradict the admissibility of $L_H \mu_H \leq b$, as both t_i and t_j are unobservable.

2. The proof is by contradiction. So we assume that Ξ_H enforces $L_{H1} \mu_H \leq b_1$ and Ξ does not enforce $L_1 \mu + H_1 q \leq b$. Then there is a (possibly empty) sequence $\sigma = t_1 t_2 \dots t_k$ in $(\mathcal{N}, \mu_0, \Xi)$ such that $\mu_0 \xrightarrow{t_1} \mu_1 \xrightarrow{t_2} \mu_2 \dots \mu_k$, and μ_k is the only one of $\mu_0 \dots \mu_k$ such that $L_1 \mu_k \not\leq b_1$ and/or $L_1 \mu_k + H_1 q^{(i)} \not\leq b_1$ for some transition t_i enabled at μ_k and allowed by Ξ to fire. Note that $\sigma_H(\sigma)$ is enabled by μ_{0H} in $(\mathcal{N}_H, \mu_{0H}, \Xi_H)$. Using the notations from part 1, we have that $L_{H1} \mu_{kH} \not\leq b_1$, and/or $L_{H1} \mu'_{kH} \not\leq b_1$, since $L_{H1} \mu'_{kH} = L_1 \mu_k + H_1 q^{(i)}$. Both are contradictions. □

2.4.6 Algorithm for the transformation of a constraint to an admissible constraint

We can use the C- and H-transformations to obtain admissible constraints as follows.

Input: The Petri net $\mathcal{N}$, the constraint $L\mu + Hq + Cv \leq b$, and optionally[5] the initial marking μ_0.

Output: The admissible constraint $L_a \mu + H_a q + C_a v \leq b_a$

1. Initialize L_a, H_a, and C_a to L, H, and C, respectively.

2. Apply the C-transformation. Let $\mathcal{N}_C$, $L_C \mu_C + Hq \leq b$, and μ_{0C} be the C-transformed net, the constraints, and the initial marking, respectively.

[5]It is possible to carry out the algorithm independently of the initial marking.

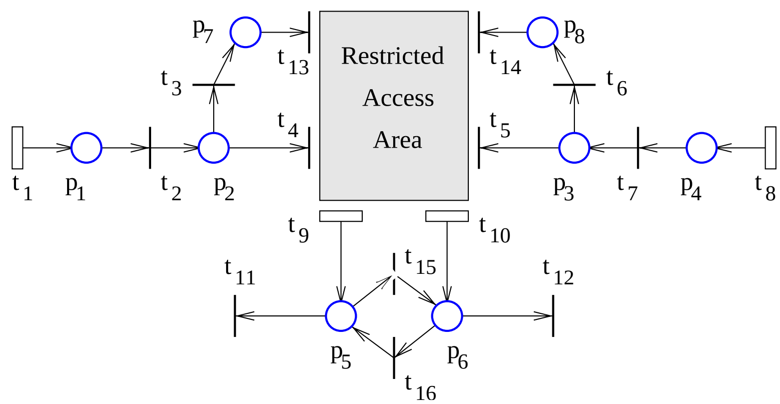

Figure 8: Plant Petri net in the example.

3. Apply the H-transformation to $\mathcal{N}_C$, $L_C\mu_C + Hq \leq b$, and μ_{0C}. Let $\mathcal{N}_{HC}$, $L_{HC}\mu_{HC} \leq b$, and μ_{HC0} be the H-transformed net, the constraints, and the initial marking, respectively.

4. Test whether $L_{HC}\mu_{HC} \leq b$ is admissible. If so, exit, and declare $L\mu + Hq + Cv \leq b$ admissible.

5. Transform $L_{HC}\mu_{HC} \leq b$ to an admissible constraint $L_{HCa}\mu_{HC} \leq b_a$, such that a supervisor optimally enforcing $L_{HCa}\mu_{HC} \leq b_a$ also enforces $L_{HC}\mu_{HC} \leq b$.[6] In case of failure, exit, and declare failure to find admissible constraints.

6. Apply the H^{-1}-transformation to $L_{HCa}\mu_{HC} \leq b_a$. Let $L_{Ca}\mu_C + H_aq \leq b_a$ be the transformed constraint.

7. Apply the C^{-1}-transformation to $L_{Ca}\mu_C + H_aq \leq b_a$. Set $L_a\mu + H_aq + C_av \leq b_a$ to the C^{-1}-transformed constraint.

Theorem 2.2 *Assume that the algorithm does not fail at step 5. Then $L_a\mu + H_aq + C_av \leq b_a$ is admissible, and a supervisor optimally enforcing it enforces also $L\mu + Hq + Cv \leq b$.*

Proof: The proof is an immediate consequence of Lemmas 2.1 and 2.2. □

2.5 Example

Consider the plant Petri net of Figure 8. It corresponds to a region of a factory cell in which autonomous vehicles (AV) access a restricted area (RA). The number of AVs which may be at the same time in the RA is limited. The AVs enter the RA from two directions: left and right; AVs coming on the left side enter via t_4 or t_{13}, and AVs coming on the right side via t_5 or t_{14}. The AVs exit the restricted area via t_9 or t_{10}. The total marking of p_1, p_2 and p_7 corresponds to the number

[6]Any of the approaches in [4, 5] can be used. Approaches generating disjunctive constraints can also be used by applying the steps 6 and 7 to each component of the disjunction.

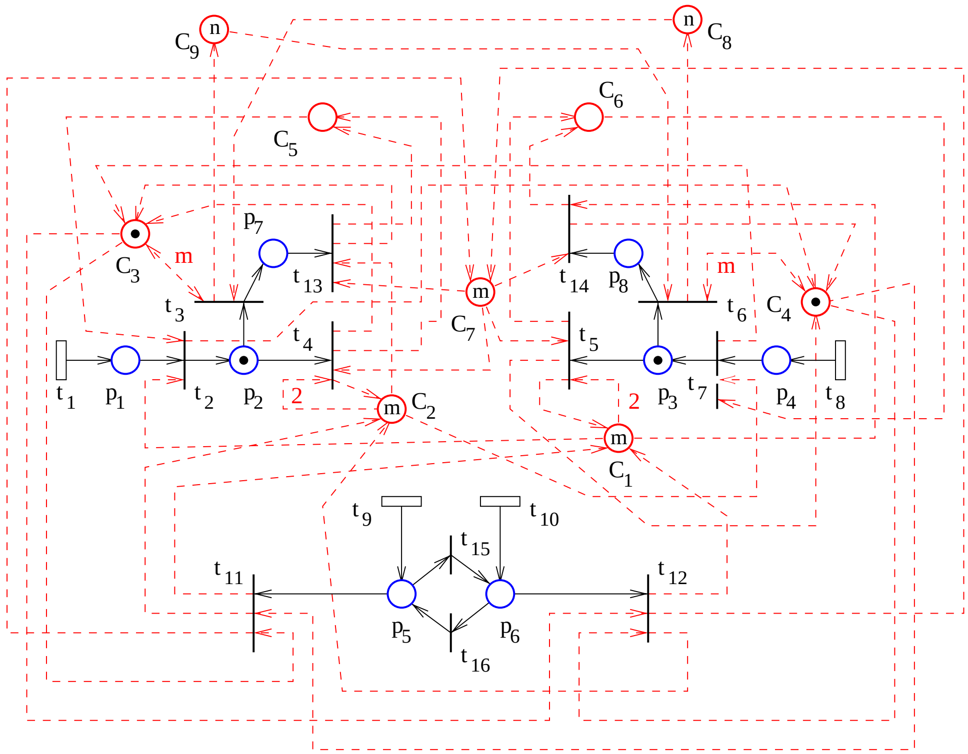

Figure 9: Closed-loop Petri net.

of left AVs waiting in line to enter the RA; only one AV should be in the states p_2 and p_7, that is $\mu_2 + \mu_7 \leq 1$. The marking of p_3, p_4, and p_8 has a similar meaning.

Let m be the maximum number of AVs which can be at the same time in the RA; note that the number of AVs in the RA is $v_{13} + v_{14} + v_4 + v_5 - v_9 - v_{10}$. When the number of vehicles in the restricted area is $m - 1$ and both a left and a right AV attempt to enter the restricted area (i.e. both $\mu_2 + \mu_7 = 1$ and $\mu_3 + \mu_8 = 1$), arbitration is required. When an AV is in p_2 and no arbitration is required, it can enter the RA without stopping. When arbitration is required, it stops (enters the state p_7) and waits the arbitration result. The same apply to p_3 and p_8. We desire the following. When an AV enters the RA, if an arbitration was required to decide that it may enter, the AV should enter via t_{13} or t_{14}; if no arbitration was required, it should enter via t_4 or t_5. These constraints can be written as follows:

$$2q_5 + \mu_2 + \mu_7 \leq m - (v_{13} + v_{14} + v_4 + v_5 - v_9 - v_{10}) + 1 \quad (32)$$

$$2q_4 + \mu_3 + \mu_8 \leq m - (v_{13} + v_{14} + v_4 + v_5 - v_9 - v_{10}) + 1 \quad (33)$$

$$mq_3 \leq \mu_3 + \mu_8 + v_{13} + v_{14} + v_4 + v_5 - v_9 - v_{10} \quad (34)$$

$$mq_6 \leq \mu_2 + \mu_7 + v_{13} + v_{14} + v_4 + v_5 - v_9 - v_{10} \quad (35)$$

In addition we have the requirements that

$$\mu_2 + \mu_7 \leq 1 \quad (36)$$

$$\mu_3 + \mu_8 \leq 1 \tag{37}$$

The requirement on the maximum number of AVs in the RA is

$$v_{13} + v_{14} + v_4 + v_5 - v_9 - v_{10} \leq m \tag{38}$$

We add the fairness constraints

$$\begin{aligned} v_3 - v_6 &\leq n & (39) \\ -v_3 + v_6 &\leq n & (40) \end{aligned}$$

As t_1, t_8, t_9, t_{10} are uncontrollable and t_9, t_{10} unobservable, the constraints (32−35) and (38) are inadmissible. They are transformed to[7]

$$\begin{aligned} 2q_5 + \mu_2 + \mu_5 + \mu_6 + \mu_7 + v_{13} + v_{14} + v_4 + v_5 - v_9 - v_{10} &\leq m + 1 & (41) \\ 2q_4 + \mu_3 + \mu_5 + \mu_6 + \mu_8 + v_{13} + v_{14} + v_4 + v_5 - v_9 - v_{10} &\leq m + 1 & (42) \\ mq_3 - \mu_3 - \mu_8 - \mu_5 - \mu_6 - (v_{13} + v_{14} + v_4 + v_5 - v_9 - v_{10}) &\leq 0 & (43) \\ mq_6 - \mu_2 - \mu_7 - \mu_5 - \mu_6 - (v_{13} + v_{14} + v_4 + v_5 - v_9 - v_{10}) &\leq 0 & (44) \\ v_{13} + v_{14} + v_4 + v_5 - v_9 - v_{10} + \mu_5 + \mu_6 &\leq m & (45) \end{aligned}$$

The closed-loop Petri net is shown next to the plant in Figure 9, where the control places $C_1 \ldots C_9$ correspond to the constraints (41), (42), (43), (44), (36), (37), (45), (39), and (40), in this order.

3 Conclusion

Enforcing linear marking and firing vector constraints can be done effectively in Petri nets. This paper has extended this class of constraints to include Parikh vector constraints. Then, we have shown how these more expressive constraints can be enforced as effectively as linear marking constraints. Our approach has also enhanced the previous technique for enforcing firing vector constraints in the presence of uncontrollable and unobservable transitions.

References

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

[2] M. Jantzen and R. Valk. Formal properties of place/transition nets. In Brauer, W., editor, *Lecture Notes in Computer Science: Net Theory and Applications, Proc. of the Advanced Course*

[7]The constraints (34) and (35) cannot be transformed to (more restrictive) admissible constraints; (43) and (44) represent relaxed (and admissible) forms of (34) and (35).

on General Net Theory of Processes and Systems, Hamburg, 1979, volume 84, pages 165–212, Berlin, Heidelberg, New York, 1980. Springer-Verlag.

[3] Y. Li and W. Wonham. Control of Vector Discrete-Event Systems II - Controller Synthesis. *IEEE Transactions on Automatic Control*, 39(3):512–530, March 1994.

[4] J. O. Moody and P. J. Antsaklis. *Supervisory Control of Discrete Event Systems Using Petri Nets*. Kluwer Academic Publishers, 1998.

[5] J. O. Moody and P. J. Antsaklis. Petri net supervisors for DES with uncontrollable and unobservable transitions. *IEEE Transactions on Automatic Control*, 45(3):462–476, March 2000.

[6] J. O. Moody, M. V. Iordache, and P. J. Antsaklis. Enforcement of event-based supervisory constraints using state-based methods. In *Proceedings of the 38th Conference on Decision and Control*, pages 1743–1748, 1999.

[7] W. Reisig. *Petri Nets*, volume 4 of *EATCS Monographs on Theoretical Computer Science*. Springer-Verlag, 1985.

[8] E. Yamalidou, J. O. Moody, P. J. Antsaklis, and M. D. Lemmon. Feedback control of Petri nets based on place invariants. *Automatica*, 32(1):15–28, January 1996.