8th International Workshop on Discrete Event Systems (WODES'06)
University of Michigan, Ann Arbor, July 10-12, 2006.

Reduction of the Supervisor Design Problem with Firing Vector Constraints

Marian V. Iordache and Panos J. Antsaklis

***Abstract*— This paper presents a new result concerning the design of supervisors for specifications involving firing vectors. The result shows that without loss of permissiveness, a solution to the design problem can be found by solving another supervisor design problem, involving only marking specifications, in a transformed Petri net. On one hand, this result shows that the methods for marking specifications can be applied to specifications involving also firing vectors. On the other hand, the specifications involving firing vectors have been shown to be necessary in order to describe the P-type languages of free-labeled Petri nets. Since the method of this paper could be used without loss of permissiveness, it is complementary to our previous work on structural and suboptimal methods for the design of supervisors with firing vector specifications.**

I. Introduction

The constraints of the form

$$L\mu + Hq + Cv \leq b \tag{1}$$

have been proposed in [3], as a description of the constraints enforced by a set of places arbitrarily connected to a set of transitions. Thus, (1) describe the P-type languages of free-labeled Petri nets (PNs). In (1), μ is the marking, q is the firing vector, and v is a parameter called the Parikh vector, representing the number of firings of each transition since the initialization of the system. Further, L, H, C, and b are integer matrices of appropriate dimensions. As the Parikh vector term can be easily incorporated in the marking term by adding a sink place to each transition [3], we will only refer to constraints of the form

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

Given a PN $\mathcal{N} = (P, T, D^-, D^+)$, where P is the set of places, T the set of transitions, D^- the input matrix, and D^+ the output matrix, a specification (2) on $\mathcal{N}$ is interpreted as follows. First, a marking μ satisfies (2) if $L\mu \leq b$. Further, a transition t may fire at μ only if its corresponding firing vector q satisfies $L\mu + Hq \leq b$ and the next reached marking μ' (that is, $\mu \xrightarrow{t} \mu'$) satisfies $L\mu' \leq b$. Moreover, in a concurrency setting, a firing vector q is enabled only if for all integer vectors $q', q'' \geq 0$, $q' + q'' \leq q \Rightarrow L\mu' + Hq'' \leq b$, where $\mu \xrightarrow{q'} \mu'$.

M. V. Iordache is with the School of Engineering & Engineering Technology, LeTourneau University, Longview, TX 75607, USA MarianIordache@letu.edu

P. J. Antsaklis is with the Department of Electrical Engineering, University of Notre Dame, Notre Dame, IN 46556, USA antsaklis.1@nd.edu

In this paper we consider disjunctions of the form

$$\bigvee_{i=1}^{n_d} [L_i\mu + H_iq \leq b_i] \tag{3}$$

requiring that there is $i = 1 \ldots n_d$ such that μ and q satisfy the specification $L_i\mu + H_iq \leq b_i$, in the sense discussed at (2). Due to partial controllability and observability issues, the problem of enforcing specifications (3) is difficult. The main result of this paper is that given a specification $\mathcal{S}$ of the form (3) on a PN $(\mathcal{N}, \mu_0)$, a solution to the supervisor design problem can be found by solving first a supervision design problem on a transformed PN $(\mathcal{N}_H, \mu_{H0})$ for a specification $\mathcal{S}_H$ of the form

$$\bigvee_{i=1}^{n_d} [L_{H,i}\mu_H \leq b_i]. \tag{4}$$

Note that $(\mathcal{N}_H, \mu_{H0})$ and the matrices $L_{H,i}$ are obtained from $(\mathcal{N}, \mu_0)$ and (3) by means of a PN and constraint transformation that we call *the H-transformation*. Thus, our results show that if we find a specification $\mathcal{S}'_H$ of the form (4) that is at least as restrictive as $\mathcal{S}_H$ and that satisfies also certain feasibility and compatibility constraints, then a specification $\mathcal{S}'$ of the form (3) can be easily derived, such that $\mathcal{S}'$ is feasible and at least as restrictive as $\mathcal{S}$. Further, we show that if $\mathcal{S}'_H$ is optimal with respect to permissiveness, so is $\mathcal{S}'$. Note that the paper does not show how to find $\mathcal{S}'_H$; it only shows that without loss of permissiveness, the problem of enforcing (3) can be reduced to a problem of enforcing a specification (4) (in which the term Hq is missing).

The results of this paper are obtained under the concurrency setting of the transition bag assumption [7], [6], in which bags of transitions can fire at the same time. This means that a firing vector q may be any nonnegative integer vector $q \in \mathbb{N}^{|T|}$, provided there are enough many tokens to enable q. Further, note that a supervisor derived under the transition bag assumption is valid also under other concurrency settings, though it may be more restrictive than necessary. The setting of partial controllability and observability considered in this paper is general. We consider a class of labeled PNs in which different labeling functions are used for control events and for observation events. In this way, the settings of the (conventional) labeled Petri nets and of the Petri nets with uncontrollable/unobservable transitions appear as special cases.

Concerning the significance of the results, further work is necessary in order to determine whether this reduction

method is the best way to approach constraints (3). It should be emphasized that the reduction method in itself has very little computational complexity: the transformation required to go between $(\mathcal{N}, \mu_0)$ and (3) on one hand, and $(\mathcal{N}_H, \mu_{H0})$ and (4) on the other hand, has low polynomial complexity. However, more work is needed in order to investigate the benefit of working with specifications in the simplified form (4). In any case, these results are a step forward towards understanding the permissiveness properties of the structural method of [3], which uses the same reduction technique.

II. Preliminaries

Let $D = D^+ - D^-$ denote the incidence matrix. It is known [3] that in the fully controllable and observable case, a least restrictive supervisor enforcing (2) can be implemented by a PN supervisor of input and output matrices

$$D_c^+ = \max(0, -LD, H - LD) \quad (5)$$

$$D_c^- = \max(0, LD, H) \quad (6)$$

In the equations (5–6), the operator $\max$ is taken element by element. That is, $Y = \max(0, X)$ means $Y_{ij} = \max(0, X_{ij})$ and $Z = \max(X, Y)$ means $Z_{ij} = \max(X_{ij}, Y_{ij})$. By definition, the constraints $L\mu + Hq \leq b$ are interpreted as requiring that $\forall q', q'' \geq 0$, $q' + q'' \leq q \Rightarrow L\mu' + Hq'' \leq b$, where $\mu \xrightarrow{q'} \mu'$. It is important to notice that this interpretation of (2) can be simply expressed by the inequality

$$L\mu + H_d q \leq b \quad (7)$$

for $H_d = D_c^-$, as proved in the following lemma.

Lemma 2.1 *μ and $q \geq 0$ satisfy (7) iff $\forall q', q'' \geq 0$, $q' + q'' \leq q \Rightarrow L\mu' + Hq'' \leq b$, where $\mu \xrightarrow{q'} \mu'$.*

Proof: First, let's note that $L\mu' + Hq'' \leq b$ can be written as $L\mu + LDq' + Hq'' \leq b$.

"$\Rightarrow$" In view of (6), the conclusion follows based on the observation that $D_c^- q \geq D_c^-(q' + q'') \geq (LD)q' + Hq''$.

"$\Leftarrow$" Let l, h and e denote the k'th row of L, H and b. We prove that if $\forall q', q'' \geq 0$, $q' + q'' \leq q \Rightarrow l\mu + lDq' + hq'' \leq e$, then $l\mu + d_c^- q \leq e$, where $d_c^- = \max(0, lD, h)$. We prove it by showing that the maximum of $[lDq' + hq'']$ subject to $q', q'' \geq 0$ and $q' + q'' \leq q$, equals $d_c^- q$.

Let $q = [q_1, q_2, \ldots q_n]^T$, $q' = [q'_1, q'_2, \ldots q'_n]^T$ and $q'' = [q''_1, q''_2, \ldots q''_n]^T$. Note that $\max[lDq' + hq''] = \max[\sum_i ((lD)_i q'_i + h_i q''_i)]$, where $(lD)_i$ and h_i are the i'th components of lD and h. Since $\max[(lD)_i q'_i + h_i q''_i)] = q_i \max(0, (lD)_i, h_i)$, we obtain $\max[(lD)q' + hq''] = \sum_i q_i \max(0, (lD)_i, h_i) = d_c^- q$, which ends the proof. ∎

Let Q denote the set of firing vectors, Q^* the set of firing sequences $\sigma = q_1 q_2 \ldots$, and $\mathcal{M}$ the set of initial states (initial markings). In this paper, we consider deterministic **supervisors** defined as maps $\Xi : \mathcal{M} \times Q^* \to Q$. For all $x \in \mathcal{M} \times Q^*$, $\Xi(x)$ represents the set of supervisor-enabled firing vectors, where a firing vector q is enabled when $q \leq \Xi(x)$. As defined, supervisors may or may not be feasible, where a supervisor is infeasible if it cannot be implemented due to the controllability and observability constraints of the plant.

A specification is said to be **enforced** by a supervisor Ξ of a plant $(\mathcal{N}, \mu_0)$ if the closed-loop $(\mathcal{N}, \mu_0, \Xi)$ allows only firing sequences that satisfy the specification. A specification is said to be **optimally enforced** if the closed-loop $(\mathcal{N}, \mu_0, \Xi)$ disables only the firing sequences of the plant that do not satisfy the specification. In other words, a supervisor Ξ that optimally enforces the specification has the permissiveness of a least restrictive supervisor designed in the setting of fully controllable and observable PNs.

In this paper we consider **double-labeled PNs**, which are PNs enhanced with two labeling functions, as follows. Each transition is labeled by control events and by one observation event. A transition may fire only if one of the control events is enabled. Further, when a transition fires, it generates the observation event that labels it. Without loss of generality, we will assume each transition is labeled by a single control event. Let $\mathcal{K}$ and $\mathcal{O}$ denote the sets of control and observation events. The events used for control are mapped by $\rho : T \to \mathcal{K}$, and the events used for observation by $o : T \to \mathcal{O}$. In particular, for labeled PNs $\rho(t) = o(t)$ $\forall t \in T$ and $\mathcal{K} = \mathcal{O} = \Sigma$, where Σ is the set of events. Further, for PNs with individually controllable and observable transitions, $\rho(t) = o(t) = \{t\}$ $\forall t \in T$ and $\mathcal{K} = \mathcal{O} = T$. In order to define formally the feasibility of a specification, the following notation is introduced.

1) Let $\mathcal{K}_c \subseteq \mathcal{K}$ denote the set of controllable events. Given a firing vector q, $\rho^*(q)$ denotes a vector $z \in \mathbb{N}^{|\mathcal{K}_c|}$ indexed by the events of $\mathcal{K}_c$, such that $\forall e \in \mathcal{K}_c$, $z(e) = \sum_{t \in \rho^{-1}(e)} q(t)$.
2) Let $\mathcal{O}_o \subseteq \mathcal{O}$ denote the set of observable events. Given a firing vector q, $o^*(q)$ denotes a vector $z \in \mathbb{N}^{|\mathcal{O}_o|}$ indexed by the events of $\mathcal{O}_o$, such that $\forall e \in \mathcal{O}_o$, $z(e) = \sum_{t \in o^{-1}(e)} q(t)$.
3) Given a firing sequence $\sigma = q_1 q_2 q_3 \ldots$ let $o^*(\sigma)$ denote the sequence of observation vectors $o^*(q_1) o^*(q_2) o^*(q_3) \ldots$.

Definition 2.1 *A specification on a PN $(\mathcal{N}, \mu_0)$ is* **feasible** *if a supervisor optimally enforcing it ensures that*

1) *If q and q' are two plant-enabled firing vectors and $\rho^*(q) = \rho^*(q')$, then the closed-loop enables either both q and q' or none of them.*
2) *If σ_1 and σ_2 are two firing sequences closed-loop enabled at the initial state, $o^*(\sigma_1) = o^*(\sigma_2)$, and $q \neq 0$ is a firing vector such that both $\sigma_1 q$ and $\sigma_2 q$ are plant-enabled at the initial state, then either both $\sigma_1 q$ and $\sigma_2 q$ or none of them are closed-loop enabled at the initial state.*

In Definition 2.1, note that the firing vectors q and q' are not necessarily nonzero, and the sequences σ_1 and σ_2 are not necessarily nonempty. In our convention, a firing vector $q = 0$ and an empty firing sequence σ are always enabled. Next, we define feasible supervisors. Let Ω denote the set

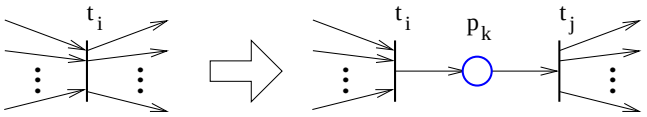

Fig. 2. Illustration of the transition split operation.

of observation vectors $o^*(q)$ for $q \in Q$ and Ω^* the set of sequences of observation vectors $o^*(q_1)o^*(q_2)o^*(q_3)\ldots$. Let Γ denote the set of control vectors $\rho^*(q)$ for $q \in Q$. A *feasible* supervisor should be implementable by observing only observation vectors and controlling only controllable events. A formal definition follows.

Definition 2.2 *A supervisor Ξ is* **feasible** *if there is a map $\overline{\Xi} : \mathcal{M} \times \Omega^* \to \Gamma$ such that $\forall s \in \mathcal{M}$, $\forall \sigma \in Q^*$, $\gamma = \overline{\Xi}(s, \pi_o(\sigma)) \Rightarrow \Xi(s,\sigma) = \{q \in Q : \rho^*(q) \leq \gamma\}$.*

Note that a feasible specification has the property that there is a feasible supervisor that optimally enforces it. Next, we define the PN and constraint transformations used in this paper. The H-transformation is a modification of the indirect method for enforcing firing vector constraints in [5]. The idea of the transformation is illustrated on the following example. Consider the PN of Figure 1(a). Assume that we desire to enforce

$$\mu_1 + \mu_2 + 2\mu_3 + q_3 \leq 5 \tag{8}$$

Then, we can transform the PN as shown in Figure 1(b). The transformation adds a place and a transition which correspond to the factor q_3. Then

$$\mu_1 + \mu_2 + 2\mu_3 + 4\mu_5 \leq 5 \tag{9}$$

is the transformed constraint, where the term $4\mu_5$ 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 (8). Thus we obtain $a = 4$. The transformation is defined as follows.

The H-Transformation

Input: The PN $\mathcal{N}$ of structure $\mathcal{N} = (P, T, D^-, D^+)$, the constraints $L\mu + Hq \leq b$, and optionally the initial marking μ_0 and a set $T_{s,H} \subseteq T$ (by default, $T_{s,H} = \emptyset$).

Output: The H-transformed PN $\mathcal{N}_H$ of structure $\mathcal{N}_H = (P_H, T_H, D_H^-, D_H^+)$, the H-transformed constraints $L_H\mu_H \leq b$, and the initial marking μ_{H0} of $\mathcal{N}_H$.

1) Let $H_d = \max(LD, H, 0)$, $T^1 = T_{s,H} \cup \{t \in T : \overline{H_d(\cdot,t) \neq 0\}}$ and $T_s = \{t \in T : \rho(t) = \rho(t') \text{ for some } t' \in T^1\}$. (Thus $T_s \supseteq T^1$.)
2) Initialize $\mathcal{N}_H$ to be identical to $\mathcal{N}$, with the same controllability and observability attributes. Initialize also L_H to L and μ_{H0} to μ_0.
3) For all $t \in T_s$:
   a) Add a new place p_k and a new transition t_j to $\mathcal{N}_H$ as in Figure 2.
   b) Set $L_H(\cdot, p_k) = H_d(\cdot, t_i) + LD^-(\cdot, t_i)$ and $\mu_{H0}(p_k) = 0$.
4) For all $t \in T_s$, the controllability and observability of the transitions t_j is defined as follows:
   a) $o(t \bullet\bullet) = o(t)$.
   b) The set of control events is extended such that $\rho(t \bullet\bullet) \notin \{\rho(t) : t \in T\}$.
   c) $\rho(t \bullet\bullet)$ is controllable iff $\rho(t)$ is controllable.
   d) For $t, t' \in T_s$, $\rho(t\bullet\bullet) = \rho(t'\bullet\bullet)$ iff $\rho(t) = \rho(t')$.

The H^{-1}-Transformation

Input: The PN $\mathcal{N} = (P, T, D^-, D^+)$, the H-transformed net $\mathcal{N}_H = (P_H, T_H, D_H^-, D_H^+)$, and a set of constraints $L_H\mu_H \leq b$ on $\mathcal{N}_H$.

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

1) Set $L(\cdot, p) = L_H(\cdot, p)$ $\forall p \in P$ and H to the null matrix.
2) For all $p_k \in P_H \setminus P$
   a) Let t_i be the transition such that $\{t_i\} = \bullet p_k$.
   b) Set $H(\cdot, t_i) = L_H(\cdot, p_k) - L_H D_H^-(\cdot, t_i)$.

Note several properties of the H- and H^{-1}-transformations. To simplify our notation, assume single constraints $l\mu + hq \leq b$ and $l_H\mu_H \leq b$. Further, let $\overline{P}_H = P_H \setminus P$. Thus, if $l_H\mu_H \leq b$ is the H-transformation of $l\mu + hq \leq b$, then:

$$l_H(p) = \begin{cases} l(p) \text{ if } p \in P \\ h_d(\bullet p) + lD^-(\cdot, \bullet p) \text{ if } p \in \overline{P}_H \end{cases} \tag{10}$$

In addition, the relation between $\mathcal{N}_H$ and $\mathcal{N}$ is such that

$\forall t \in T \setminus \bullet\overline{P}_H$:

$$D_H^-(p,t) = \begin{cases} D^-(p,t) & \text{for } p \in P \\ 0 & \text{for } p \in \overline{P}_H \end{cases} \tag{11}$$

$$D_H^+(p,t) = \begin{cases} D^+(p,t) & \text{for } p \in P \\ 0 & \text{for } p \in \overline{P}_H \end{cases} \tag{12}$$

$\forall t \in T \cap \bullet\overline{P}_H$:

$$D_H^-(p,t) = \begin{cases} D^-(p,t) & \text{for } p \in P \\ 0 & \text{for } p \notin \overline{P}_H \end{cases} \tag{13}$$

$$D_H^+(p,t) = \begin{cases} 0 & \text{for } p \notin \overline{P}_H \cap t\bullet \\ 1 & \text{for } p = \overline{P}_H \cap t\bullet \end{cases} \tag{14}$$

$\forall t \in T_H \setminus T$:

$$D_H^-(p,t) = \begin{cases} 0 & \text{for } p \neq \bullet t \\ 1 & \text{for } p = \bullet t \end{cases} \tag{15}$$

$$D_H^+(p,t) = \begin{cases} D^+(p, \bullet\bullet t) & \text{for } p \in P \\ 0 & \text{for } p \notin P \end{cases} \tag{16}$$

Furthermore, if $l\mu + hq \leq b$ is the H^{-1}-transformation of $l_H\mu_H \leq b$

$$l(p) = l_H(p) \; \forall p \in P \tag{17}$$

$$h(t) = \begin{cases} l_H(p) - l_H D_H^-(\cdot, t), \text{ if } t\bullet \cap \overline{P}_H = p \\ 0, \text{ if } t\bullet \cap \overline{P}_H = \emptyset \end{cases} \tag{18}$$

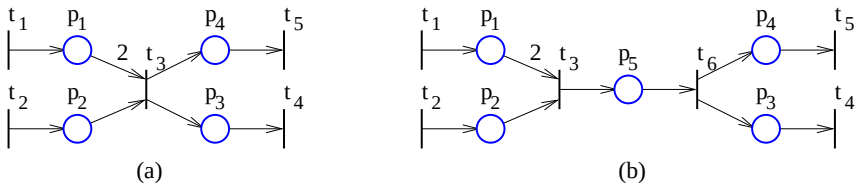

Fig. 1. Example for the H-transformation.

The following relation can be easily verified based on (10–16). The relation will prove very useful in the further developments.

$$L_H D_H(\cdot,t) = \begin{cases} LD(\cdot,t) & \text{for } t \in T \setminus \bullet\overline{P}_H \\ H_d(\cdot,t) & \text{for } t \in T \cap \bullet\overline{P}_H \\ LD(\cdot,\bullet\bullet t) - H_d(\cdot,\bullet\bullet t) & \\ & \text{for } t \in T_H \setminus T \end{cases} \tag{19}$$

Let D_c, D_c^- and D_c^+ denote the incidence, output, and input matrices of the supervisor enforcing $L\mu + Hq \le b$. Similarly, let's define $D_{c,H}$, $D_{c,H}^-$ and $D_{c,H}^+$ for the supervisor enforcing $L_H\mu_H \le b$ in $\mathcal{N}_H$. Note that $D_{c,H} = -L_H D_H$ and $D_{c,H}^- = \max(0, L_H D_H)$. Thus, based on (19), the following is obtained:

$$D_{c,H}^-(\cdot,t) = \begin{cases} D_c^-(\cdot,t) & \text{for } t \in T \\ 0 & \text{for } t \in T_H \setminus T \end{cases} \tag{20}$$

Further, since $D_{c,H}^+ = \max(0, -L_H D_H)$

$$D_{c,H}^+(\cdot,t) = \begin{cases} D_c^+(\cdot,t) & \text{for } t \in T \setminus \bullet\overline{P}_H \\ 0 & \text{for } t \in T \cap \bullet\overline{P}_H \\ D_c^+(\cdot,\bullet\bullet t) & \text{for } t \in T_H \setminus T \end{cases} \tag{21}$$

III. Main Results

First, we introduce the following notation. If a transition t_i is split in the H-transformation as in Figure 2, let $\sigma_H(t_i)$ be the firing sequence $t_i t_j$. If a transition t_i is not split, let $\sigma_H(t_i)$ equal t_i. Further, we also use σ_H for firing vectors: $\sigma_H(q) = q_H q'_H$, where $q_H(t_i) = q'_H(t_j) = q(t_i)$ for a transition t_i split in t_i and t_j, $q_H(t_i) = q(t_i)$ for a transition t_i that is not split, $q'_H(t_i) = 0\ \forall t_i \in T$ and $q_H(t_j) = 0\ \forall t_j \in T_H \setminus T$. If $\sigma = q_1 q_2 \ldots$ is a firing sequence in $\mathcal{N}$, let $\sigma_H(\sigma) = \sigma_H(q_1)\sigma_H(q_2)\ldots$. Further, let m_H map the markings of $\mathcal{N}$ into markings of $\mathcal{N}_H$ as follows:

$$\mu_H = m_H(\mu) \Rightarrow \mu_H(p) = \begin{cases} \mu(p) & \text{for } p \in P \\ 0 & \text{for } p \in \overline{P}_H \end{cases} \tag{22}$$

Proposition 3.1 *Given $(\mathcal{N}, \mu_0)$ and $(\mathcal{N}_H, m_H(\mu_0))$, let q be a firing vector in $\mathcal{N}$ and $\sigma_H(q) = q_H q'_H$.*

(a) *At all reachable markings, q_H is enabled iff $\sigma_H(q)$ is enabled.*

(b) *q is enabled at the marking μ_1 iff $\sigma_H(q)$ is enabled at the marking $m_H(\mu_1)$.*

Proof: (a) By (14) and (15), q_H is enabled iff $q_H q'_H$ is enabled.

(b) Let $\mu_{H1} = m_H(\mu_1)$. Note that $\mu_1 \ge D^- q \Leftrightarrow \mu_{H1} \ge D_H^- q_H$, by (11) and (13). Therefore, q is enabled iff q_H is enabled, which concludes our proof by part (a). ■

Proposition 3.2 *Consider $(\mathcal{N}, \mu_0)$ in closed-loop with a supervisor Ξ optimally enforcing $L\mu + Hq \le b$, and $(\mathcal{N}_H, m_H(\mu_0))$ in closed-loop with a supervisor Ξ_H optimally enforcing $L_H\mu_H \le b$. Let q be a firing vector in $\mathcal{N}$ and $\sigma_H(q) = q_H q'_H$.*

(a) *At all reachable markings, q_H is closed-loop enabled iff $\sigma_H(q)$ is closed-loop enabled.*

(b) *μ is reachable and q is closed-loop enabled at μ iff $\mu_H = m_H(\mu_1)$ is reachable and $\sigma_H(q)$ is closed-loop enabled at μ_H.*

Proof: (a) By (20), $D_{c,H}^- q'_H = 0$. Thus, Ξ_H never restricts the firing of q'_H. Therefore, in view of Proposition 3.1(a), q_H is closed-loop enabled iff $q_H q'_H$ is closed-loop enabled.

(b) We show that a sequence $\mu_0 \xrightarrow{q_1} \mu_1 \xrightarrow{q_2} \mu_2 \ldots \xrightarrow{q_k} \mu_k$ is possible in the closed-loop of $\mathcal{N}$ iff $\mu_{H0} \xrightarrow{\sigma_H(q_1)} \mu_{H1} \xrightarrow{\sigma_H(q_2)} \mu_{H2} \ldots \xrightarrow{\sigma_H(q_k)} \mu_{Hk}$ is possible in the closed-loop of $\mathcal{N}_H$. Note that $q_1 q_2 \ldots q_k$ is plant-enabled iff $\sigma_H(q_1 q_2 \ldots q_k)$ is plant-enabled, based on Propositions 3.1(b) and 3.3(a), where Proposition 3.3(a) shows that $\mu_{Hi} = m_H(\mu_i)$ for $i = 0, 1, \ldots k$. Thus, we only need to prove that if $q_1 q_2 \ldots q_i$ and $\sigma_H(q_1 q_2 \ldots q_i)$ are closed-loop enabled, then $q_1 q_2 \ldots q_i q_{i+1}$ is supervisor-enabled iff $\sigma_H(q_1 q_2 \ldots q_i q_{i+1})$ is supervisor-enabled.

Note that the constraints $L_H\mu_H \le b$ are not violated by firing q_H when $L_H\mu_H + D_{c,H}^- q_H \le b$. Further, the constraints $L\mu + Hq \le b$ are not violated by firing q when $L\mu + H_d q \le b$. By definition, $H_d = D_c^-$. Further, by (20) $D_{c,H}^- q_H = H_d q$, and by (10) and $\mu_H = m_H(\mu)$, $L_H\mu_H = L\mu$. It follows that $L_H\mu_{Hi} + D_{c,H}^- q_{Hi+1} \le b \Leftrightarrow L\mu_i + H_d q_{i+1} \le b$ (where q_{Hi+1} is the first term of $\sigma_H(q_{i+1}) = q_{Hi+1} q'_{Hi+1}$). Therefore, q_{i+1} is supervisor-enabled iff q_{Hi+1} is supervisor-enabled. By part (a), this concludes the proof. ■

Given a firing sequence σ of $\mathcal{N}$, we have already defined $\sigma_H(\sigma)$ to denote the equivalent firing sequence σ_H of $\mathcal{N}_H$. In the following developments, we will need also the converse operation $\sigma(\sigma_H)$, associating a firing sequence σ of $\mathcal{N}$ to each firing sequence σ_H of $\mathcal{N}_H$. Assume μ_0 and $\mu_{H0} = m_H(\mu_0)$ are the initial markings of $\mathcal{N}$ and $\mathcal{N}_H$. Given a firing sequence σ_H of $\mathcal{N}_H$, let $\overline{\sigma}_H$ be the firing

count vector. Let $\nu_H(\sigma_H)$ be the largest integer vector v_H such that $v_H \leq \overline{\sigma}_H$ and $\forall t \in \bullet\overline{P}_H$, $v_H(t) = v_H(t \bullet \bullet)$. Further, let $\chi_H(\sigma_H) = \overline{\sigma}_H - \nu_H(\sigma_H)$. Thus, if $q_H = \chi_H(\sigma_H)$, then $\forall t \in T_H \setminus \bullet\overline{P}_H$, $q_H(t) = 0$. Let $\nu(\sigma_H)$ and $\chi(\sigma_H)$ be the restrictions of $\nu_H(\sigma_H)$ and $\chi_H(\sigma_H)$ to the transitions in T. If $\sigma_H = q_{H1}q_{H2}\dots q_{Hx}$, let σ_{H0} be an empty sequence, $\sigma_{H1} = q_{H1}$, $\sigma_{H2} = q_{H1}q_{H2}$, $\dots\sigma_{Hx} = q_{H1}q_{H2}\dots q_{Hx}$ and $q_i = \nu(\sigma_{Hi}) - \nu(\sigma_{Hi-1})$ for $i = 1\dots x$. We define $\sigma(\sigma_H)$ as the sequence $q_1q_2\dots q_x$.

Proposition 3.3 *Consider $(\mathcal{N}, \mu_0)$, the set of constraints $L\mu + Hq \leq b$, and their H-transformation $(\mathcal{N}_H, \mu_{H0})$ and $L_H\mu_H \leq b$, where $\mu_{H0} = m_H(\mu_0)$.*

(a) *If $\sigma_H(q) = q_Hq'_H$, $\mu_1 \xrightarrow{q} \mu_2$, $\mu_{H1} \xrightarrow{q_H} \mu'_{H1} \xrightarrow{q'_H} \mu_{H2}$ and $\mu_{H1} = m_H(\mu_1)$, then $\mu_{H2} = m_H(\mu_2)$ and $L_H\mu'_{H1} = L\mu_1 + H_dq$.*

(b) *If $\mu_{H0} \xrightarrow{\sigma_H} \mu_H$, then $\sigma(\sigma_H)$ is enabled at μ_0 and firing it results in $\mu = \mu_0 + D\nu(\sigma_H)$. Further, $q = \chi(\sigma_H)$ is enabled at μ and $L_H\mu_H = L\mu + H_dq$.*

(c) *Given σ_H and q_H, if σ_Hq_H is enabled at μ_{H0} and x is the restriction of q_H to T, then $\sigma(\sigma_H)q$ is enabled at μ_0, where $q = \chi(\sigma_H) + x$.*

(d) *Let Ξ be a supervisor optimally enforcing $L\mu + Hq \leq b$ in $(\mathcal{N}, \mu_0)$ and Ξ_H a supervisor optimally enforcing $L_H\mu_H \leq b$ in $(\mathcal{N}_H, \mu_{H0})$. If σ_H is closed-loop enabled at μ_{H0}, then $\sigma(\sigma_H)$ is closed-loop enabled at μ_0.*

Proof: (a) $L_H\mu'_{H1} = L\mu_1 + H_dq$ follows from (10–14) and $\mu_{H2} = m_H(\mu_2)$ from (11–16).

(b) Let μ_{H1}, μ_{H2}, $\dots\mu_{Hx}$ be markings such that $\mu_{H0} \xrightarrow{q_{H1}} \mu_{H1} \xrightarrow{q_{H2}} \mu_{H2}\dots \xrightarrow{q_{Hx}} \mu_{Hx}$. Let σ_{H0} be an empty sequence, $\sigma_{H1} = q_{H1}$, $\sigma_{H2} = q_{H1}q_{H2}$, $\dots\sigma_{Hx} = q_{H1}q_{H2}\dots q_{Hx}$. Further, let $\mu_i = \mu_{i-1} + D(\nu(\sigma_{Hi}) - \nu(\sigma_{Hi-1}))$ and $u_i = \chi(\sigma_{Hi})$ for $i = 1\dots x$. We show by induction that μ_i is reachable from μ_{i-1} by firing $q_i = \nu(\sigma_{Hi}) - \nu(\sigma_{Hi-1})$, where $\mu_i = \mu_{i-1}$ if $q_i = 0$, and that $L_H\mu_{Hi} = L\mu_i + H_du_i$ for $i = 1\dots x$. For $i = 1$, note that $\nu(\sigma_{H1}) = 0$ and $\mu_1 = \mu_0$. Further, $L_H\mu_{H1} = L\mu_1 + H_du_1$ is satisfied by part (a). Now, assume the induction hypothesis satisfied at step i. Let $q_{i+1} = \nu(\sigma_{Hi+1}) - \nu(\sigma_{Hi})$. Let's show first that if $q_{i+1} \neq 0$ then q_{i+1} is plant-enabled, that is, $\mu_i \geq D^-q_{i+1}$. Note that $\mu_{Hi} = \mu_{H0} + D_H\nu_H(\sigma_{Hi}) + D_H\chi_H(\sigma_{Hi})$, and so $\mu_{Hi} = m_H(\mu_i) + D_H\chi_H(\sigma_{Hi})$. Since q_{Hi+1} is enabled, $\mu_{Hi} \geq D_H^-q_{Hi+1}$. Then, by (11–14), $\mu_i \geq D^-(u_i + x)$, where x is the restriction of q_{Hi+1} to T. Note that since $\mu_{H0} = m_H(\mu_0)$, any firing of a transition $t \in T_H \setminus T$ must be preceded by a firing of the transition $\bullet\bullet t$. Thus, $\forall t \in T_H \setminus T$: $q_{Hi+1}(t) \leq u_i(\bullet\bullet t)$ and $q_{Hi+1}(t) = q_{i+1}(\bullet\bullet t)$. Further, $\forall t \in T \setminus \bullet\overline{P}_H$: $x(t) = q_{i+1}(t)$. Therefore, we can conclude that $q_{i+1} \leq u_i + x$ and so $\mu_i \geq D^-q_{i+1}$. Next we show that $L_H\mu_{Hi+1} = L\mu_{i+1} + H_du_{i+1}$. Now, $L_H\mu_{Hi+1} = L_H\mu_{Hi} - D_{c,H}q_{Hi+1}$. Let's decompose q_{Hi+1} as $q_{Hi+1} = \alpha_H + \beta_H + \gamma_H$, where $\alpha_H(t) = q_{Hi+1}(t)$ for $t \in T_H \setminus T$ and $\alpha_H(t) = 0$ otherwise, $\beta_H(t) = q_{Hi+1}(t)$ if $t \in T \setminus \bullet\overline{P}_H$ and $\beta_H(t) = 0$ otherwise, and $\gamma_H(t) = q_{Hi+1}(t)$ if $t \in T \cap \bullet\overline{P}_H$ and $\gamma_H(t) = 0$ otherwise. By (11–16), $D_{c,H}q_{Hi+1} = D_c^+\alpha + D_c\beta - D_c^-\gamma$, where β and γ are the restrictions of β_H and γ_H to T, and $\alpha(t) = \alpha_H(t \bullet \bullet)$ for $t \in T \cap \bullet\overline{P}_H$ and $\alpha(t) = 0$ otherwise. Thus, from $L_H\mu_{Hi+1} = L_i\mu_i + H_du_i - D_{c,H}q_{Hi+1}$ and $D_c^- = H_d$ we obtain $L_H\mu_{Hi+1} = L_i\mu_i - D_c(\alpha + \beta) + H_d(u_i - \alpha + \gamma)$. Note that $q_{i+1} = \alpha + \beta$ and $u_{i+1} = u_i - \alpha + \gamma$, so $L_H\mu_{Hi+1} = L_{i+1}\mu_{i+1} + H_du_{i+1}$, which concludes our induction proof.

It only remains to show that $q = \chi(\sigma_H)$ is enabled at μ. Let q'_H be defined as $q'_H(t) = \mu_H(\bullet t)$ $\forall t \in T_H \setminus T$ and $q'_H(t) = 0$ otherwise. Thus, μ_H enables q'_H. Therefore, by the first part of the proof, μ enables $q_z = \nu(\sigma_Hq'_H) - \nu(\sigma_H)$. Note that $q_z = q$. Therefore, μ enables q.

(c) Let $x_H = q_H(t)$ $\forall t \in T$ and $x_H(t) = 0$ otherwise. Let q'_H be defined as $q'_H(t) = \mu_H(\bullet t)$ $\forall t \in T_H \setminus T$ and $q'_H(t) = 0$ otherwise, where $\mu_H \xleftarrow{\sigma_H} \mu_{H0}$. Note that $\sigma_Hx_Hq'_H$ is enabled. Further, let x^*_H and q^*_H be defined as $x^*_H(t) = x_H(t)$ $\forall t \in T \cap \bullet\overline{P}_H$, $x^*_H(t) = 0$ otherwise, $q^*_H(t) = x_H(t)$ $\forall t \in T \setminus \bullet\overline{P}_H$, $q^*_H(t) = q'_H(t)$ $\forall t \in T_H \setminus T$, and $q^*_H(t) = 0$ otherwise. (So $x^*_H + q^*_H = x_H + q'_H$.) In view of (11–16), since $\sigma_Hx_Hq'_H$ is enabled, $\sigma_Hx^*_Hq^*_H$ is too. Note that $\sigma(\sigma_Hx^*_Hq^*_H) = \sigma(\sigma_H)q$ for $q = \chi(\sigma_H) + x$. Then, $\sigma(\sigma_H)q$ is enabled by part (b).

(d) The induction proof of part (b) can be used, once we show that q_{i+1} is supervisor-enabled at the marking μ_i, that is, $L\mu_i + H_dq_{i+1} \leq b$. Since q_{Hi+1} is closed-loop enabled, $L_H\mu_{Hi} + D_{c,H}^-q_{Hi+1} \leq b$. By (20), $D_{c,H}^-q_{Hi+1} = H_dx$. By $L_H\mu_{Hi} = L\mu_i + H_du_i$, $L\mu_i + H_dq_{i+1} + H_d(x + u_i - q_{i+1}) \leq b$. Since $x + u_i \geq q_{i+1}$, $L\mu_i + H_dq_{i+1} \leq b$, and so q_{i+1} is supervisor-enabled. ■

Next, a relaxed concept of feasibility is introduced for specifications on $\mathcal{N}_H$. Compared to Definition 2.1, the second requirement is relaxed to constrain only the firing sequences σ_H of $\mathcal{N}_H$ that have the form $\sigma_H = \sigma_H(\sigma)$, where σ is a sequence of $\mathcal{N}$.

Definition 3.1 *A specification on $(\mathcal{N}_H, \mu_{H0})$ is* **h-feasible** *if a supervisor optimally enforcing it ensures that*

1) *If q_H and q'_H are two plant-enabled firing vectors and $\rho^*(q_H) = \rho^*(q'_H)$, then the closed-loop enables either both q_H and q'_H or none of them.*
2) *Let $q \neq 0$ be a firing vector of $\mathcal{N}$ and σ_1 and σ_2 be two sequences of firing vectors of $\mathcal{N}$. If $\sigma_H(\sigma_1)$ and $\sigma_H(\sigma_2)$ are enabled by the closed-loop at the initial state, $o^*(\sigma_H(\sigma_1)) = o^*(\sigma_H(\sigma_2))$, and both $\sigma_H(\sigma_1q)$ and $\sigma_H(\sigma_2q)$ are plant-enabled at the initial state, then either both $\sigma_H(\sigma_1q)$ and $\sigma_H(\sigma_2q)$ or none of them are closed-loop enabled at the initial state.*

The H-transformation can be defined also for disjunctions of constraints (3), requiring all reachable states to satisfy

$$\bigvee_{i=1}^{n_d} [L_i\mu \leq b_i] \tag{23}$$

and that a firing vector q should be enabled only if μ and q satisfy

$$\bigvee_{i=1}^{n_d} [L_i\mu + H_{d,i}q \leq b_i] \tag{24}$$

where $H_{d,i} = \max(L_iD, H_i, 0)$. $H_{d,i}$ is the H_d matrix defined in the H-transformation, which is also the same as $D^-_{c,i}$ calculated by (6). Note that this interpretation of a disjunction (3) is not the most general. Recall, the constraints (1) were defined to require the inequality $L\mu + Hq \leq b$ satisfied for all possible intermediary states reached during the firing of q, that is, for all $q', q'' \geq 0$, if $q' + q'' \leq q$ then $L\mu' + Hq'' \leq b$, where $\mu \xrightarrow{q'} \mu'$. Thus, it was shown in Lemma 2.1 that the constraints (1) enable a firing vector q iff the inequality $L\mu + H_dq \leq b$ is satisfied. On the other hand, the requirement that for all $q', q'' \geq 0$, if $q' + q'' \leq q$ then $\bigvee_i L_i\mu' + H_iq'' \leq b_i$, is weaker than the requirement that μ and q satisfy (24). However, (24) is easier to check online and allows us to easily extend our results from conjunctions of constraints to disjunctions of constraints. In the particular case of no concurrency and $H_i = 0$ for all i, these two interpretations of (3) are equivalent.

The H-transformation for constraints (3)

1) Let $H_{d,i} = \max(L_iD, H_i, 0)$ and modify $T_{s,H}$ to $T_{s,H} = T_{s,H} \cup \bigcup_{i=1}^{n_d} \{t \in T : H_{d,i}(\cdot, t) \neq 0\}$.
2) For all $i = 1 \dots n_d$, apply the H-transformation to the constraints $L_i\mu + H_iq \leq b_i$ with the argument $T_{s,H}$ calculated at step 1. Let $L_{H,i}\mu_H \leq b_i$ be the transformed constraints.
3) The result of the H-transformation consists of the disjunction (4), the PN $\mathcal{N}_H$, and the initial marking μ_{H0}, where $\mathcal{N}_H$ and μ_{H0} are obtained from any of the H-transformations of step 2.

Note that the choice of the set $T_{s,H}$ guarantees that the same PN $\mathcal{N}_H$ is obtained by all H-transformations of step 2. The H^{-1}-transformation of a disjunction (4) results in a disjunction (3), obtained by taking the disjunction of the H^{-1}-transformations of the constraints $L_{H,i}\mu_H \leq b_i$.

The H^{-1}-transformation for constraints (4)

1) For all $i = 1 \dots n_d$, apply the H^{-1}-transformation to the constraints $L_{H,i}\mu_H \leq b_i$. Let $L_i\mu + H_iq \leq b_i$ be the transformed constraints.
2) The result of the H^{-1}-transformation is the disjunction (3).

The next result shows that Proposition 3.2 can be extended to disjunctions of constraints.

Proposition 3.4 *Consider $(\mathcal{N}, \mu_0)$ in closed-loop with a supervisor Ξ optimally enforcing (3), and $(\mathcal{N}_H, m_H(\mu_0))$ in closed-loop with a supervisor Ξ_H optimally enforcing (4). Let q be a firing vector in $\mathcal{N}$ and $\sigma_H(q) = q_Hq'_H$.*

(a) *At all reachable markings, q_H is closed-loop enabled iff $\sigma_H(q)$ is closed-loop enabled.*

(b) *μ is reachable and q is closed-loop enabled at μ iff $\mu_H = m_H(\mu_1)$ is reachable and $\sigma_H(q)$ is closed-loop enabled at μ_H.*

Proof: (a) By Proposition 3.1(a), q_H is plant-enabled iff $\sigma_H(q)$ is plant-enabled. By (20), $D^-_{c,H,i}q'_H = 0$ for all $i = 1 \dots n_d$, and so firing q'_H cannot violate any of the constraints $L_{Hi}\mu_H \leq b_i$ that are satisfied. The conclusion follows.

(b) The proof is the same as in Proposition 3.2(b), once we substitute $L\mu + Hq \leq b$ ($L_H\mu_H \leq b$) by the constraints $L_j\mu + H_jq \leq b_j$ ($L_{Hj}\mu_H \leq b_j$), $j \in \{1, 2, \dots n_d\}$, that are satisfied when q_{i+1} (q_{Hi+1}) is fired at μ_i (μ_{Hi}). ■

Part (a) of the next result shows that Proposition 3.3(c,d) can also be extended to disjunctions of constraints.

Proposition 3.5 *Let Ξ be a supervisor optimally enforcing (3) in $(\mathcal{N}, \mu_0)$ and Ξ_H a supervisor optimally enforcing (4) in $(\mathcal{N}_H, \mu_{H0})$, where $\mu_{H0} = m_H(\mu_0)$.*

(a) *If σ_H is closed-loop enabled at μ_{H0}, then $\sigma(\sigma_H)$ is closed-loop enabled at μ_0.*
(b) *Assume that σ_H is closed-loop enabled at μ_{H0} and σ_Hq_H is plant-enabled at μ_{H0}. Then σ_Hq_H is closed-loop enabled at μ_{H0} iff $q = \chi(\sigma_H) + x$ is closed-loop enabled at $\mu = \mu_0 + D\nu(\sigma_H)$, where x is the restriction of q_H to T.*

Proof: (a) The proof of Proposition 3.3(d) can be adapted here based on the following observation. For any closed-loop enabled sequence $\mu_{H0} \xrightarrow{q_{H1}} \mu_{H1} \xrightarrow{q_{H2}} \mu_{H2} \dots \xrightarrow{q_{Hx}} \mu_{Hx}$, there is a sequence of indices $k_0, k_1, \dots k_{x-1} \in \{1, 2, \dots n_d\}$ such that $L_{H,k_i}\mu_{Hi} + D^-_{c,H,k_i}q_{Hi+1} \leq b_{k_i}$, for all $i = 0, 1, \dots x-1$. Thus, the proof of Proposition 3.3(d) can be used to show that $L_{H,k_i}\mu_{Hi} + D^-_{c,H,k_i}q_{Hi+1} \leq b_{k_i} \Rightarrow L_{k_i}\mu_i + H^-_{d,k_i}q_{i+1} \leq b_{k_i}$, where $q_1q_2 \dots q_x$ denotes the sequence $\sigma(\sigma_H)$.

(b) By part (a) and Proposition 3.3(b), μ is reachable in the closed-loop by firing $\sigma(\sigma_H)$. Let $\mu_H \xleftarrow{\sigma_H} \mu_{H0}$. For all $i = 1, 2, \dots n_d$, $D^-_{c,H,i}q_H = D^-_{c,i}x$ by (20), and $L_{H,i}\mu_H = L_i\mu + H_{d,i}\chi(\sigma_H)$ by Proposition 3.3(b). Thus, $L_{H,i}\mu_H + D^-_{c,H,i}q_H = L_i\mu + H_{d,i}q$. If q is closed-loop enabled, then there is $i \in \{1, 2, \dots n_d\}$ such that $L_i\mu + H_{d,i}q \leq b_i$. Thus, $L_{H,i}\mu_H + D^-_{c,H,i}q_H \leq b_i$, which shows that q_H is supervisor-enabled at μ_H. On the other hand, if q_H is closed-loop enabled at μ_H, there is $i \in \{1, 2, \dots n_d\}$ such that $L_{H,i}\mu_H + D^-_{c,H,i}q_H \leq b_i$, so $L_i\mu + H_{d,i}q \leq b_i$. Thus, q is supervisor-enabled at μ. Therefore, in view of Proposition 3.3(c), q is closed-loop enabled at μ. ■

Theorem 3.1 *Let (4) denote the H-transformation of (3), μ_0 the initial marking of $\mathcal{N}$ and $\mu_{H0} = m_H(\mu_0)$ the initial marking of $\mathcal{N}_H$. Then (4) is h-feasible iff (3) is feasible.*

Proof: The proof shows that each of the two requirements of Definition 2.1 implies its corresponding requirement in Definition 3.1 and vice-versa. The proof for the first requirement is by contradiction.

Case 1a: The first requirement is satisfied in Definition 3.1 but not in Definition 2.1. Thus, there is a reachable marking μ of $\mathcal{N}$ such that two plant-enabled firing vectors q_1 and q_2 satisfy that $\rho^*(q_1) = \rho^*(q_2)$ and that the closed-loop enables q_1 but disables q_2. Since q_1 is supervisor-enabled and q_2 is supervisor-disabled, there is $k \in \{1, 2, \dots n_d\}$ such that $L_k\mu + H_{d,k}q_1 \leq b_k$, and $L_i\mu + H_{d,i}q_2 \not\leq b_i$ for all $i = 1 \dots n_d$. Let $\sigma_H(q_1) = q_{H1}q'_{H1}$ and $\sigma_H(q_2) = q_{H2}q'_{H2}$. By Propositions 3.4(b) and 3.1(b), $\mu_H = m_H(\mu)$ is reachable in the closed-loop, q_{H1} is closed-loop enabled and q_{H2} is only plant-enabled. However, this contradicts the first requirement of Definition 3.1, since $\rho^*(q_1) = \rho^*(q_2) \Rightarrow \rho^*(q_{H1}) = \rho^*(q_{H2})$.

Case 1b: The first requirement is satisfied in Definition 2.1 but not in Definition 3.1. Thus, there is a reachable marking μ_H of $\mathcal{N}_H$ such that two firing vectors q_{H1} and q_{H2} satisfy that $\rho^*(q_{H1}) = \rho^*(q_{H2})$ and that q_{H1} is closed-loop enabled and q_{H2} is only plant-enabled. For $i = 1, 2$, let x_{Hi} be defined as $x_{Hi}(t) = q_{Hi}(t)\ \forall t \in T$ and $x_{Hi}(t) = 0$ otherwise. By (20), x_{H1} is closed-loop enabled and x_{H2} is only plant-enabled. Let σ_H be a firing sequence such that $\mu_{H0} \xrightarrow{\sigma_H} \mu_H$ and let x_1 and x_2 be the restrictions of x_{H1} and x_{H2} to T, $q_1 = \chi(\sigma_H) + x_1$ and $q_2 = \chi(\sigma_H) + x_2$. By Propositions 3.5 and 3.3(b–c), $\mu_0 \xrightarrow{\sigma(\sigma_H)} \mu$, q_1 is closed-loop enabled at μ and q_2 is only plant-enabled at μ. This contradicts the first requirement of Definition 2.1, since $\rho^*(q_{H1}) = \rho^*(q_{H2}) \Rightarrow \rho^*(q_1) = \rho^*(q_2)$.

Case 2: We show that the second requirement in Definition 3.1 is not satisfied iff the second requirement in Definition 2.1 is not satisfied. The second requirement of Definition 2.1 is not satisfied iff there are two sequences σ_1 and σ_2 and a firing vector q such that $\sigma_1 q$ and σ_2 are closed-loop enabled, $\sigma_2 q$ is only plant-enabled, and $o^*(\sigma_1) = o^*(\sigma_2)$. Further, $\sigma_1 q$ and σ_2 are closed-loop enabled and $\sigma_2 q$ is only plant-enabled iff $\sigma_H(\sigma_1 q)$ and $\sigma_H(\sigma_2)$ are closed-loop enabled and $\sigma_H(\sigma_2 q)$ is only plant-enabled, by Propositions 3.4(b) and 3.1(b). Since $o^*(\sigma_1) = o^*(\sigma_2) \Leftrightarrow o^*(\sigma_H(\sigma_1)) = o^*(\sigma_H(\sigma_2))$, the conclusion follows. ■

Given $(\mathcal{N}, \mu_0)$, we say that a supervisor Ξ_1 is at least as restrictive as a supervisor Ξ_2, which we write $\Xi_1 \preceq \Xi_2$, if any sequence σ closed-loop enabled at the initial state of $(\mathcal{N}, \mu_0, \Xi_1)$ is also closed-loop enabled at the initial state of $(\mathcal{N}, \mu_0, \Xi_2)$. Further, Ξ_1 is more restrictive than Ξ_2, which we write $\Xi_1 \prec \Xi_2$, if $\Xi_1 \preceq \Xi_2$ and there is a sequence σ closed-loop enabled at the initial state of $(\mathcal{N}, \mu_0, \Xi_2)$ that is not closed-loop enabled at the initial state of $(\mathcal{N}, \mu_0, \Xi_1)$. Let $\mathcal{S}$ denote a set of constraints $\bigvee_{i=1}^{n_d}[L_i\mu + H_i q \leq b_i]$ and $\mathcal{S}'$ denote $\bigvee_{i=1}^{n'_d}[L'_i\mu + H'_i q \leq b_i]$. Let $\mathcal{S}_H$ denote $\bigvee_{i=1}^{n_d}[L_{Hi}\mu_H \leq b_i]$, the H-transformation of $\mathcal{S}$, and $\mathcal{S}'_H$ denote $\bigvee_{i=1}^{n'_d}[L'_{Hi}\mu_H \leq b'_i]$, the H-transformation of $\mathcal{S}'$. In order to ensure that the H-transformations of $\mathcal{S}$ and $\mathcal{S}'$ result in the same PN $\mathcal{N}_H$, we define the **joint H-transformation** of $\mathcal{S}$ and $\mathcal{S}'$ to consist of an H-transformation of $\mathcal{S}$ and an H-transformation of $\mathcal{S}'$ that use the same parameter $T_{s,H} \supseteq \bigcup_{i=1}^{n_d}\{t \in T : H_{d,i}(\cdot, t) \neq 0\} \cup \bigcup_{i=1}^{n'_d}\{t \in T : H'_{d,i}(\cdot, t) \neq 0\}$, where $H_{d,i} = \max(L_i D, H_i, 0)$ and $H'_{d,i} = \max(L'_i D, H'_i, 0)$.

Theorem 3.2 *Let $\mathcal{S}$ and $\mathcal{S}'$ be two sets of constraints (3), and $\mathcal{S}_H$ and $\mathcal{S}'_H$ their joint H-transformation. Let Ξ, Ξ', Ξ_H and Ξ'_H be supervisors optimally enforcing $\mathcal{S}$, $\mathcal{S}'$, $\mathcal{S}_H$ and $\mathcal{S}'_H$, respectively, in $(\mathcal{N}, \mu_0)$ and $(\mathcal{N}_H, \mu_{H0})$, where $\mu_{H0} = m_H(\mu_0)$. $\Xi \preceq \Xi'$ ($\Xi \prec \Xi'$) iff $\Xi_H \preceq \Xi'_H$ ($\Xi_H \prec \Xi'_H$).*

Proof: The proof is by contradiction. First, we prove $\Xi_H \preceq \Xi'_H \Rightarrow \Xi \preceq \Xi'$. Assume σ enabled at μ_0 in $(\mathcal{N}, \mu_0, \Xi)$ and not in $(\mathcal{N}, \mu_0, \Xi')$. Then, $\sigma_H(\sigma)$ is enabled at μ_{H0} in $(\mathcal{N}_H, \mu_{H0}, \Xi_H)$ but not in $(\mathcal{N}_H, \mu_{H0}, \Xi'_H)$, by Proposition 3.4(b). This contradicts $\Xi_H \preceq \Xi'_H$. Next we prove that $\Xi \preceq \Xi' \Rightarrow \Xi_H \preceq \Xi'_H$. Assume σ_H enabled at μ_{H0} in $(\mathcal{N}_H, \mu_{H0}, \Xi_H)$ and $(\mathcal{N}_H, \mu_{H0}, \Xi'_H)$, but $\sigma_H q_H$ enabled only in $(\mathcal{N}_H, \mu_{H0}, \Xi_H)$. Let q be defined as in Proposition 3.5(b). Then, $\sigma(\sigma_H)q$ is enabled at μ_0 in $(\mathcal{N}, \mu_0, \Xi)$ and not in $(\mathcal{N}, \mu_0, \Xi')$, by Proposition 3.5(b). This contradicts $\Xi \preceq \Xi'$. Now, we prove $\Xi \prec \Xi' \Rightarrow \Xi_H \prec \Xi'_H$. Assume $\Xi_H \not\prec \Xi'_H$. Since $\Xi \prec \Xi' \Rightarrow \Xi \preceq \Xi' \Rightarrow \Xi_H \preceq \Xi'_H$, it must be that Ξ_H and Ξ'_H are equally permissive. Thus, $\Xi_H \succeq \Xi'_H$. Then, $\Xi \succeq \Xi'$, which contradicts $\Xi \prec \Xi'$. The proof of $\Xi_H \prec \Xi'_H \Rightarrow \Xi \prec \Xi'$ is similar. ■

In the following developments, it will be useful to guarantee that the successive application of the H^{-1}- and H-transformations to a set of constraints (4) produces exactly the same set of constraints. To this end, each component $L_H\mu_H \leq b$ of a disjunction (4) will be constrained to satisfy

$$\forall p \in \overline{P}_H: \quad \begin{cases} L_H(\cdot, p) \geq L_H D_H^+(\cdot, p\bullet) \\ L_H(\cdot, p) \geq L_H D_H^-(\cdot, \bullet p) \end{cases} \tag{25}$$

$$\forall t \in T \setminus \bullet\overline{P}_H: \quad L_H D_H(\cdot, t) \leq 0 \tag{26}$$

The following result summarizes the properties of (25–26).

Theorem 3.3 *(a) The H-transformation of any set of constraints $L\mu + Hq \leq b$ satisfies (25–26).*

(b) Given an H-transformed net $\mathcal{N}_H$ and a set of constraints $L_H\mu_H \leq b$, let $L\mu + Hq \leq b$ denote the H^{-1}-transformation of $L_H\mu_H \leq b$ and let $L'_H\mu'_H \leq b$ and $\mathcal{N}'_H$ denote the H-transformation of (2). If L_H satisfies (25–26) and the H-transformation generating $L'_H\mu'_H \leq b$ has the parameter $T_{s,H} = \bullet\overline{P}_H$, then $\mathcal{N}_H$ and $\mathcal{N}'_H$ are identical, and $L'_H = L_H$.

Proof: (a) By definition, $H_d(\cdot, \bullet p) = \max(0, LD(\cdot, \bullet p), H(\cdot, \bullet p))\ \forall p \in \overline{P}_H$. Further, by (13) and (16), $LD(\cdot, \bullet p) = L_H D_H^+(\cdot, p\bullet) - L_H D_H^-(\cdot, \bullet p)$ and $LD^-(\cdot, \bullet p) = L_H D_H^-(\cdot, \bullet p)$. Then, (25) is obtained by substituting LD in H_d, then H_d and LD^- in $\forall p \in \overline{P}_H$: $L_H(\cdot, p) = H_d(\cdot, \bullet p) + LD^-(\cdot, \bullet p)$, where this expression is true by (10). According to the H-transformation, all transitions t for which $H_d(\cdot, t) \neq 0$ are split. Therefore, $\forall t \in T \setminus \bullet\overline{P}_H$, $H_d(\cdot, t) = 0$, and so $LD(\cdot, t) \leq 0$. By (19), this proves (26).

(b) By definition, $H_d = \max(LD, H, 0)$. For $t \in T \cap \bullet\overline{P}_H$ we have $H_d(\cdot, t) = H(\cdot, t)$, in view of (25),

$LD(\cdot,t) = L_H D_H^+(\cdot, t\bullet\bullet) - L_H D_H^-(\cdot,t)$, and $H(\cdot,t) = L_H(\cdot,t\bullet) - L_H D_H^-(\cdot,t)$ (by (18)). For $t \in T \setminus \bullet\overline{P}_H$, $H_d(\cdot,t) = H(\cdot,t) = 0$, in view of (18), (19), and (26). This shows that $H_d = H$. Then, by (10), (13) and (18) we get $L'_H(\cdot,p) = L_H(\cdot,p)\ \forall p \in P'_H$. Note that $H_d = H \Rightarrow P'_H \subseteq P_H$; $P'_H = P_H$ is guaranteed by $T_{s,H} = \bullet\overline{P}_H$. ■

Let $\mathcal{S}$ denote the specification (3) on $(\mathcal{N}, \mu_0)$. Based on the results obtained so far, the following procedure could be used to find a feasible specification $\mathcal{S}_a$ that is at least as restrictive as $\mathcal{S}$. The procedure could be used whenever $\mathcal{S}$ is not feasible or its feasibility is not known.

Procedure 3.1

1) Apply the H-transformation. Let $\mathcal{S}_H$ and $(\mathcal{N}_H, \mu_{H0})$ be the transformed constraints and PN.
2) Find h-feasible constraints $\mathcal{S}_{Ha}$ that satisfy (25–26) such that $\Xi_{Ha} \preceq \Xi_H$, where Ξ_{Ha} and Ξ_H are supervisors optimally enforcing $\mathcal{S}_{Ha}$ and $\mathcal{S}_H$, respectively. If no solution is found, declare failure and exit.
3) Apply to $\mathcal{S}_{Ha}$ the H^{-1}-transformation. Let $\mathcal{S}_a$ be the result. Enforce $\mathcal{S}_a$ in $(\mathcal{N}, \mu_0)$.

The set of constraints obtained by this procedure has interesting properties when the H-transformation splits all transitions and the C-transformation adds sink places to all transitions. Therefore, let's define the **total H-transformation** as the H-transformation with parameter $T_{s,H} = T$. Let $\mathcal{X}$ be the set of all supervisors optimally enforcing feasible constraints of the form (3). Let $\mathcal{X}_{HC}$ be the set of all supervisors optimally enforcing h-feasible constraints of the form (3) that satisfy (25–26).

Theorem 3.4 *Given the notation of Procedure 3.1, let Ξ and Ξ_a be supervisors optimally enforcing $\mathcal{S}$ and $\mathcal{S}_a$, respectively.*

(a) *$\mathcal{S}_a$ is feasible and $\Xi_a \preceq \Xi$.*

Assume that the total H-transformation is applied at the first step of the procedure.

(b) *Ξ_a is least restrictive among the supervisors of $\mathcal{X}$ enforcing $\mathcal{S}$ iff Ξ_{HCa} is least restrictive among the supervisors of $\mathcal{X}_{HC}$ enforcing $\mathcal{S}_{HC}$.*
(c) *There is no supervisor $\Xi^* \succ \Xi_a$ of $\mathcal{X}$ that enforces $\mathcal{S}$ if there is no supervisor $\Xi^*_{HC} \succ \Xi_{HCa}$ of $\mathcal{X}_{HC}$ that enforces $\mathcal{S}_{HC}$.*

Proof: (a) Let P_C and P_{HC} be the set of places of the PNs obtained by the C- and H-transformation of $\mathcal{S}$. In view of Theorem 3.3(b), the same PN $\mathcal{N}_{HC}$ is obtained by the C- and H-transformations of $\mathcal{S}_a$, when the transformations use the parameters $T_{s,C} = \bullet(P_C \setminus P)$ and $T_{s,H} = \bullet(P_{HC} \setminus P_C)$. Further, $\mathcal{S}_{HCa}$ is the C- and H-transformation of $\mathcal{S}_a$. Therefore, $\mathcal{S}_a$ is feasible by Theorem 3.1 and $\Xi_a \preceq \Xi$ in view of $\Xi_{HCa} \preceq \Xi_{HC}$ and Theorem 3.2.

(b) Note that the total C- and H-transformation of any set of constraints (3) results in the same PN $\mathcal{N}_{HC}$. By Theorem 3.3(b), the total C- and H-transformation of $\mathcal{S}_a$ is $\mathcal{S}_{HCa}$. The proof is by contradiction. Assume there is another supervisor $\Xi' \in \mathcal{X}$ enforcing $\mathcal{S}$ such that $\Xi' \not\preceq \Xi_a$. Since $\Xi' \in \mathcal{X}$, Ξ' optimally enforces a feasible set of constraints $\mathcal{S}'$ of the form (3). By Theorems 3.1 and 3.3(a), $\Xi'_{HC} \in \mathcal{X}_{HC}$, where Ξ'_{HC} is a supervisor optimally enforcing the $\mathcal{S}'_{HC}$, the total C- and H-transformation of $\mathcal{S}'$. By Theorem 3.2, $\Xi'_{HC} \preceq \Xi_{HC}$. Therefore, $\Xi'_{HC} \preceq \Xi_{HCa}$, since Ξ_{HCa} is least restrictive. By Theorem 3.2, $\Xi' \preceq \Xi_a$, which contradicts the original assumption.

(c) The proof is similar to that of part (b). ■

Theorem 3.4 shows that the problem of enforcing constraints (3) can be solved in terms of the simpler constraints (4) in a transformed PN, without loss of permissiveness. Since our results were derived under the transition-bag concurrency setting, a loss of permissiveness is possible when the Procedure 3.1 is used for other concurrency settings. Indeed, a feasible least restrictive supervisor enforcing (3) may be too restrictive for other concurrency settings, though it would still enforce (3). This suggests that for a different concurrency setting, the second step of Procedure 3.1 should incorporate additional constraints besides (25–26), to ensure the design remains optimal. Finally, no specific method has been referenced for the second step of the procedure. Under certain assumptions, including no concurrency, a solution for specifications (4) is available [8]. However, an optimal solution appears to be difficult to obtain in the general case. A structural solution is possible, and we plan to present it in a future paper. The structural solution, while applying to double-labeled PNs and the most common concurrency settings, including the one of this paper, can use previous methods developed for constraints $L\mu \leq b$, such as in [1], [2], [4], [7], to obtain a suboptimal solution.

REFERENCES

[1] F. Basile, P. Chiacchio, and A. Giua. On the choice of suboptimal monitor places for supervisory control of Petri nets. In *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics*, pages 752–757, 1998.

[2] H. Chen. Control synthesis of Petri nets based on s-decreases. *Discrete Event Dynamic Systems: Theory and Applications*, 10(3):233–250, 2000.

[3] M.V. Iordache and P.J. Antsaklis. Synthesis of supervisors enforcing general linear vector constraints in Petri nets. *IEEE Transactions on Automatic Control*, 48(11):2036–2039, 2003.

[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, 2000.

[6] J. L. Peterson. *Petri Net Theory and the Modeling of Systems*. Englewood Cliffs, New Jersey: Prentice Hall, Inc., 1981.

[7] G. Stremersch. *Supervision of Petri Nets*. Kluwer Academic Publishers, 2001.

[8] G. Stremersch and R. K. Boel. Structuring acyclic Petri nets for reachability analysis and control. *Discrete Event Dynamic Systems*, 12(1):7–41, 2002.