Proceedings of the 2007 American Control Conference
Marriott Marquis Hotel at Times Square
New York City, USA, July 11-13, 2007

Petri Net Supervisors for Disjunctive Constraints

Marian V. Iordache and Panos J. Antsaklis

Abstract— **The paper presents an approach for the design of supervisors for disjunctive constraints in which the supervisors are represented by labeled Petri nets. This approach extends our previous results in two ways. First, the supervisors are now guaranteed to be least restrictive. Second, the constraints may now also include the firing vector. The approach is illustrated on the readers/writers problem. While the results are obtained in the fully controllable and observable setting, issues arising when the system is partially controllable and partially observable are also discussed. The approach is developed under certain boundedness assumptions.**

I. Introduction

The coordination of concurrent systems, that is, systems in which several processes may operate at the same time, has raised a number of challenges. These include the need to ensure safety constraints (such as mutual exclusion), the absence of deadlocks, and fair access to common resources for all processes. These problems are especially difficult when the systems can only be partially controlled and observed. A theoretical framework for the study of these problems is provided by the supervisory control of Petri nets (PNs). PNs are computer science models of concurrent systems.

Mutual exclusion is a well known type of requirement on the operation of a concurrent system. In the context of PNs it is described by simple inequalities in terms of the PN state, called marking. This type of inequalities on the PN state where applied to describe constraints on the operation of AGVs in manufacturing systems [1] and also for batch chemical processes [2]. However, for other purposes, such as liveness enforcement [3], [4], a more general type of constraints was needed, called general mutual exclusion constraints (GMEC) [5]. GMECs involve linear inequalities in terms of the marking μ of the PN and have the form

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

where L is an integer matrix and b an integer vector. GMECs constrain the operation of the PN to the states that satisfy the inequalities.

GMECs can be seen as static constraints, as they only constrain the state of the system. Dynamic constraints that add explicit requirements on transition firings have also been needed in the context of pipe/valve networks in chemical process control [6] and railway networks [7]. They can also describe more complex requirements for AGV coordination problems [8]. They involve not only the marking μ but also the firing vector q, where the firing vector describes the transitions that are fired at a firing instant. They have the form

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

where H is an integer matrix. In this paper, this type of constraints are called generalized linear constraints (GLCs).

An important property of the types of requirements considered so far is that a supervisor enforcing them can be represented by a PN. Thus, the closed-loop system of the plant and the supervisor is still a PN. Therefore, the closed-loop model does not require more advanced analysis or design methods than the plant model. On one hand, it is desirable to be able to describe more general requirements for the supervision of PNs. On the other hand, it is desirable that such requirements can be enforced by a supervisor that is a PN. This paper shows that a general type of requirements, called disjunctive constraints, admits also a PN supervisor solution. Disjunctive constraints require that at any time, at least one of a set of GLC subspecifications is satisfied. They are formally expressed by

$$\bigvee_{k=1}^{n_d} [L_k\mu + H_kq \leq b_k] \tag{3}$$

Thus, at any time, at least one of $L_i\mu + H_iq \leq b_i$ must be satisfied.

In the literature, related work on disjunctive constraints includes [9] and [10]. The first paper provides conditions under which the least restrictive supervisor enforcing that $\mu \in \mathcal{M}_1 \cup \mathcal{M}_2$ is obtained by combining the two least restrictive supervisors enforcing $\mu \in \mathcal{M}_1$ and $\mu \in \mathcal{M}_2$, respectively. The second paper provides a method to calculate the maximal controlled invariant set for disjunctive constraints involving the marking only, under certain assumptions on the structure of the PN.

In this paper we will distinguish between two possible interpretations of constraint disjunctions, a dynamic interpretation and a state-based interpretation. The state-based interpretation has been considered in our previous work [11] for the case in which $H_k = 0$ for all k. For the same problem, we provide a least restrictive solution in section III. The general form (3) is considered in section IV under the dynamic interpretation. A least restrictive solution is given there, based on the method introduced in section III. An example is also included in section IV. We assume the reader familiar with PNs. For an introduction to PNs and their supervision we refer the reader to [12]. The PN notation and preliminary results needed here are described in section II.

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

1-4244-0989-6/07/$25.00 ©2007 IEEE.

II. PRELIMINARIES

A PN will be denoted by $\mathcal{N} = (P, T, D^-, D^+)$, where P is the set of places, T the set of transitions, D^- the input matrix, and D^+ the output matrix. We will refer both to the **no concurrency** and to **concurrency** settings of operation of a PN. In the no concurrency setting, the firing vector is a binary vector in which only one element is nonzero. In a concurrency setting, the firing vector may be any integer vector of nonnegative elements. In either case, a firing vector is enabled at the marking μ when $D^- q \leq \mu$. A labeled PN will be denoted by $\mathcal{N} = (P, T, D^-, D^+, \rho)$, where $\rho : T \to \Sigma$ is a labeling function, associating events to transitions, and Σ is the set of events. Without loss of generality we have assumed each transition is labeled by a single event. We assume the reader familiar with the parallel composition of labeled PNs [13], [12].

In specifications (2) we assume $L \in \mathbb{Z}^{u \times m}$, $H \in \mathbb{Z}^{k \times n}$, and $b \in \mathbb{Z}^u$, where $m = |P|$, $n = |T|$, k is the number of constraints, and $\mathbb{Z}$ is the set of integers. The specifications (2) are interpreted as follows. 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 $L\mu' \leq b$. As shown in [8], the least restrictive supervisor for specifications (2) can be designed as a set of places (called monitors or control places) added to the transitions of the plant $\mathcal{N}$ according to the input and output matrices

$$D_c^+ = \max(0, -LD, H - LD) \quad (4)$$

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

where the marking of the supervisor places is $\mu^s = b - L\mu$. Note that the $\max$ operation is applied on the matrix elements with the same indices: $Z = \max(X, Y) \Leftrightarrow Z_{ij} = \max(X_{ij}, Y_{ij})$ for all indices i and j. When the supervisor is defined by (4–5), a firing vector q is supervisor enabled when $D_c^- q \leq \mu^s$, that is, when $L\mu + D_c^- q \leq b$. Denoting $H_d = D_c^-$, the concurrency interpretation of (2) is as follows. A marking μ satisfies (2) if $L\mu \leq b$. Further, q may fire at μ only if it satisfies $L\mu + H_d q \leq b$ (which implies $L\mu' \leq b$ for μ' such that $\mu \xrightarrow{q} \mu'$) [12].

III. STATE-BASED INTERPRETATION

Here we consider specifications

$$\bigvee_{k=1}^{n_d} [L_k \mu \leq b_k] \quad (6)$$

requiring that only markings satisfying (6) should be reachable. The following construction can be made for the enforcement of (6). First, because each set of constraints $L_k\mu \leq b_k$ is a conjunction of single constraints $l\mu \leq c$, where $l \in \mathbb{Z}^{1 \times n}$ and $c \in \mathbb{Z}$, the disjunction (6) can also be written as

$$\bigwedge_{j=1}^{n_c} \bigvee_{i \in A_j} l_i \mu \leq c_i, \quad (7)$$

where $l_i \in \mathbb{Z}^{1 \times |P|}$, $c_i \in \mathbb{Z}$, n_c is an integer, and A_j is a set of integers. For each constraint $l_i\mu \leq c_i$, let δ_i be a Boolean variable such that

$$\delta_i = [l_i \mu \leq c_i] \quad (8)$$

where $[l_i\mu \leq c_i]$ denotes the truth value of $l_i\mu \leq c_i$. Now, consider the markings reachable in the plant under the supervision of a least restrictive supervisor enforcing (7). Assuming that for all these reachable markings each term $l_i\mu$ has some known finite lower and upper bounds m_i and M_i, (8) is equivalent to the system of inequalities

$$l_i\mu + (M_i - c_i)\delta_i \leq M_i, \quad (9)$$

$$l_i\mu + (c_i + 1 - m_i)\delta_i \geq c_i + 1. \quad (10)$$

Then, the disjunction $\bigvee_{i \in A_j} l_i\mu \leq c_i$ can be replaced by (9–10) and

$$\sum_{i \in A_j} \delta_i \geq 1. \quad (11)$$

In our construction, the supervisor enforcing (7) is a PN $\mathcal{N}^s$ obtained by several operations, including a parallel composition of several components $\mathcal{N}_i$, as described next. Now, the construction assumes fully controllable and observable PNs. Therefore, the transitions of the supervisor are individually controllable and observable. However, in order to describe how transitions are synchronized when the supervisor components are composed and when the supervisor is composed with the plant, we need to introduce labeling functions. Let $\rho : T \to \Sigma$ be a labeling function associating a unique label to each transition of the plant $\mathcal{N}$. For each variable δ_i, we define the PN $\mathcal{N}_i = (P_i, T_i, D_i^-, D_i^+, \rho_i)$. P_i consists of a single place d_i. T_i is defined as follows.

1) For each transition t such that $l_i D(\cdot, t) \neq 0$, define two transitions f_i and x_i of T_i having the labels $\rho_i(f_i) = \rho_i(x_i) = \rho(t)$.
2) If $l_i D(\cdot, t) > 0$, connect x_i to d_i by an arc of weight $D^-(d_i, x_i) = 1$.
3) If $l_i D(\cdot, t) < 0$, connect x_i to d_i by an arc of weight $D^+(d_i, x_i) = 1$.

In words, the role of this construction is as follows. The marking of d_i will represent δ_i: $\mu(d_i) = \delta_i$. Further, when the plant fires a transition t without changing the truth value of the inequality $l_i\mu \leq c_i$, $\mathcal{N}_i$ will fire f_i. However, if the truth value of $l_i\mu \leq c_i$ is changed by firing t, $\mathcal{N}_i$ will fire x_i. The supervisor $\mathcal{N}^s$ is obtained as follows.

1) Let $\mathcal{N}^c$ be the total parallel composition of the $\mathcal{N}_i$ components and of the plant.
2) Let μ^c be the marking of $\mathcal{N}^c$. Substitute $\delta_i = \mu^c(d_i)$ and $\mu(p) = \mu^c(p)$ $\forall p \in P$ in (9–11). Then, let $L\mu^c \leq b$ denote the constraints (9–10) for all i and the constraints (11) for all j.
3) Let $\mathcal{N}^t$ be the closed-loop of $\mathcal{N}^c$ with the supervisor (4–5) enforcing $L\mu^c \leq b$, where $H = 0$.
4) Delete from $\mathcal{N}^t$ all places of the plant $\mathcal{N}$ and then all transitions t such that $\bullet t = t\bullet = \emptyset$. Let $\mathcal{N}^s$ be the result.

5) Given the initial marking μ_0 of the plant, the initial marking μ_0^s of the supervisor is as follows. The marking μ_0^c satisfies $\mu_0^c(p) = \mu_0(p)\ \forall p \in P$ and $\mu_0^c(d_i) = [l_i\mu_0 \leq c_i]\ \forall i$. The initial marking μ_0^s is defined by:
   a) For all i, $\mu_0^s(d_i) = \mu_0^c(d_i)$.
   b) The marking vector of the places added at step 3 is $b - L\mu_0^c$.

In the algorithm above, note that $\mathcal{N}^t$ is the closed-loop.

Remark 3.1 This construction is very intuitive in the no concurrency setting. In this setting, the constraints (9–10) never disable the firing of a transition of the plant. They only ensure that the supervisor keeps track of which constraints $l_i\mu \leq c_i$ are satisfied and which not. Thus, when a transition is fired in the plant, (9–10) select one of the corresponding x_i and f_i transitions that should be fired in the supervisor component $\mathcal{N}_i$, such that the marking of d_i equals the δ_i of (8). The constraints (11) are used by the supervisor to determine whether a plant transition should be enabled. □

Note that in a concurrency setting, the supervisor may not be least restrictive, since the constraints (9–10) disable the firing vectors that require firing the transitions x_i and f_i at the same time.

Theorem 3.1 *For any initial marking μ_0 satisfying (6), $(\mathcal{N}^s, \mu_0^s)$ enforces (6). Moreover, under the no concurrency assumption, the supervision is least restrictive.*

Proof: By construction, (9–11) are enforced in the closed-loop $\mathcal{N}^t$. Therefore, (6) is also enforced. To prove that the supervision is least restrictive, we only need to show that at any initial marking μ_0 satisfying (6), if firing some transition t does not break the specification (6), then the supervisor enables also t. Let t be such that $\mu_0 \xrightarrow{t} \mu_1$ and both μ_0 and μ_1 satisfy (6). Let μ_0^t and μ_1^t be the corresponding closed-loop markings. Let U be the set of indices i such that δ_i of (8) does not change its value by firing t at μ_0, and C the set of indices i such that δ_i changes its value by firing t at μ_0. Let t_e be the closed-loop transition that is the synchronization of t with x_i for all $i \in C$ and with f_i for all $i \in U$. It can be easily verified that (9–10) do not restrict the firing of t_e. Moreover, since (11) is satisfied for all j by both μ_0^t and μ_1^t, it follows that the constraints (11) do not restrict the firing of t_e. Therefore, t is enabled by the supervisor. ■

IV. Dynamic Interpretation

Here we consider specifications of the form (3). They are interpreted as follows. First, at every reachable marking μ, there is some $k = 1 \ldots n_d$ such that $L_k\mu \leq b_k$; further, a firing vector q is enabled when there is some $k = 1 \ldots n_d$ such that $L_k\mu + H_{d,k}q \leq b_k$, where $H_{d,k} = \max(0, L_kD, H_k)$. Note that the state-based interpretation of the previous section is not a special case of the dynamic interpretation of (3) when all $H_k = 0$. The dynamic interpretation is more restrictive. In the dynamic case, a firing vector q is enabled when there is some $k = 1 \ldots n_d$ such that $L_k\mu + \max(L_kD, 0)q \leq b_k$, which implies both $L_k\mu \leq b_k$ and $L_k\mu' \leq b_k$, where $\mu \xrightarrow{q} \mu'$. On the other hand, in the state-based interpretation, a transition t is to be enabled if $L_k\mu \leq b_k$ and $L_r\mu' \leq b_r$ for some $k, r = 1 \ldots n_d$, even if $k \neq r$, where $\mu \xrightarrow{t} \mu'$. For instance, firing t in Figure 1 satisfies the specification $[\mu_1 \geq 1] \vee [\mu_2 \geq 1]$ according to the state-based interpretation, but not according to the dynamic interpretation.

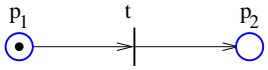

Fig. 1.

The supervisor is constructed as follows. The specification (3) is brought first to the form

$$\bigwedge_{j=1}^{n_c} \bigvee_{i \in A_j} l_i\mu + h_iq \leq c_i, \tag{12}$$

where $l_i \in \mathbb{Z}^{1\times|P|}$, $h_i \in \mathbb{Z}^{1\times|T|}$, $c_i \in \mathbb{Z}$, n_c is an integer, and A_j is a set of integers. Let $\gamma : T \to \mathbb{N}$ be a vector of nonnegative integers and $h_{d,i} = \max(0, l_iD, h_i)$. For all constraints $l_i\mu + h_iq \leq c_i$, let δ_i be a Boolean variable such that

$$\delta_i = [l_i\mu + h_{d,i}\gamma \leq c_i] \tag{13}$$

Now, consider the markings reachable in the plant under the supervision of a least restrictive supervisor enforcing (12). Assuming that for all these reachable markings and all enabled firing vectors q each term $l_i\mu + h_{d,i}q$ has some known finite lower and upper bounds m_i and M_i, the following constraints are defined:

$$l_i\mu + h_{d,i}\gamma + (M_i - c_i)\delta_i \leq M_i, \tag{14}$$

$$l_i\mu + h_{d,i}\gamma + (c_i + 1 - m_i)\delta_i \geq c_i + 1. \tag{15}$$

Let ρ be a labeling function associating a unique label to every transition of the plant. Let $T_s = \{t \in T : \exists i,\ l_iD(\cdot, t) \neq h_{d,i}(t)\}$. Let $\mathcal{N}_g = (P_g, T_g, D_g^-, D_g^+, \rho_g)$ be a PN defined as follows.

1) For each transition $t \in |T_s|$ define two transitions $t', t'' \in T_g$ such that $\rho_g(t') = \rho(t)$ and t'' has a label that was not assigned to any other transition.
2) For each transition $t \in |T_s|$ define one place g_t such that $D_g^-(g_t, t'') = 1$ and $D_g^+(g_t, t') = 1$

Let $\mathcal{N}^*$ be the parallel composition of the plant $\mathcal{N}$ and the supervisor component $\mathcal{N}_g$. Let μ^* be the marking of $\mathcal{N}^*$. Consider the term $l_i\mu + h_{d,i}\gamma$ in the relations (13–15). Note that in future considerations γ will be identified by $\gamma(t) = 0$ for all $t \notin T_s$ and $\gamma(t) = \mu^*(g_t)$ for all $t \in T_s$. Let $l_i^* \in \mathbb{Z}^{1\times|P^*|}$ be defined as follows:

$$\forall p \in P :\ l_i^*(p) = l_i(p) \tag{16}$$

$$\forall t \in T_s :\ l_i^*(g_t) = h_{d,i}(t) - l_iD(\cdot, t). \tag{17}$$

The next result reveals the significance of the vectors l^*.

Proposition 4.1 *Given is $(\mathcal{N}^*, \mu^*)$, the parallel composition of $(\mathcal{N}, \mu)$ and $(\mathcal{N}_g, \mu_g)$. Assume $\mu_g = 0$ and that for some $t \in T$ we have that $\mu \xrightarrow{t} \mu_1$ and $\mu_g \xrightarrow{t'} \mu_{g0} \xrightarrow{t''} \mu_{g1}$. Let μ^*, μ_0^*, and μ_1^* be the closed-loop markings representing the pairs (μ, μ_g), (μ_1, μ_{g0}), and (μ_1, μ_{g1}), respectively. Then $l_i^*\mu^* = l_i\mu$, $l_i^*\mu_0^* = l_i\mu + h_{d,i}\gamma$, and $l_i^*\mu_1^* = l_i\mu_1$.*

From this point on the construction of the supervisor $\mathcal{N}^s$ is almost identical to that of the previous section except for using $\mathcal{N}^*$ in the place of $\mathcal{N}$ and l^* in the place of l. For improved clarity, the construction is given again here.

Let $\mathcal{N}_i^*$ be constructed just as $\mathcal{N}_i$ in the previous section, but by using $\mathcal{N}^*$ instead of $\mathcal{N}$, l^* instead of l, and D^* instead of D. The supervisor $\mathcal{N}^s$ is obtained as follows.

1) Let $\mathcal{N}^c$ be the total parallel composition of the $\mathcal{N}_i^*$ components and of $\mathcal{N}^*$.
2) Let μ^c be the marking of $\mathcal{N}^c$. Substitute $\delta_i = \mu^c(d_i)$ and $\mu^*(p) = \mu^c(p)\ \forall p \in P^*$ in (11) and in

$$l_i^*\mu^* + (M_i - c_i)\delta_i \leq M_i, \quad (18)$$

$$l_i^*\mu^* + (c_i + 1 - m_i)\delta_i \geq c_i + 1. \quad (19)$$

   Then, let $L\mu^c \leq b$ denote the constraints (11) for all j and the constraints (18–19) for all i.
3) Let $\mathcal{N}^t$ be the closed-loop of $\mathcal{N}^c$ with the supervisor (4–5) enforcing $L\mu^c \leq b$, where $H = 0$.
4) Delete from $\mathcal{N}^t$ all places of the plant $\mathcal{N}$ and then all transitions t such that $\bullet t = t\bullet = \emptyset$. Let $\mathcal{N}^s$ be the result.
5) Given the initial marking μ_0 of the plant, the initial marking μ_0^s of the supervisor is as follows. The marking μ_0^c satisfies $\mu_0^c(p) = \mu_0(p)\ \forall p \in P$, $\mu_0^c(g_t) = 0\ \forall t \in T_s$, and $\mu_0^c(d_i) = [l_i\mu_0 \leq c_i]\ \forall i$. The initial marking μ_0^s is defined by:
   a) For all i, $\mu_0^s(d_i) = \mu_0^c(d_i)$.
   b) For all $t \in T_s$, $\mu_0^s(g_t) = \mu_0^c(g_t)$.
   c) The marking vector of the places added at step 3 is $b - L\mu_0^c$.

In this algorithm, $\mathcal{N}^t$ also represents the closed-loop of the plant $\mathcal{N}$ and the supervisor $\mathcal{N}^s$.

Remark 4.1 By construction, $\mathcal{N}^t$ is the closed-loop of $\mathcal{N}$ and $\mathcal{N}^s$. However, $\mathcal{N}^t$ is also the closed-loop of $\mathcal{N}^*$ with the supervisor enforcing

$$\bigwedge_{j=1}^{n_c} \bigvee_{i \in A_j} l_i^*\mu^* \leq c_i \quad (20)$$

according to the state-based interpretation of section III. □

Remark 4.2 Not all transitions of the supervisor are synchronized with the plant $\mathcal{N}$. Indeed, recall that the transitions t'' of the $\mathcal{N}_g$ component were assigned a unique label. It is assumed that the supervisor transitions not synchronized with the plant are fired as soon as they are enabled. This assumption is necessary in order to ensure that the supervisor is not too restrictive. □

Proposition 4.2 *Consider the place g_t and transition t'' of $\mathcal{N}_g$ associated with a transition t of $\mathcal{N}$. If g_t contains at least one token, t'' is enabled in the closed-loop $\mathcal{N}^t$.*

Proof: By construction, t'' does not have input places from the plant $\mathcal{N}$. Thus, $\bullet t''$, when taken with respect to $\mathcal{N}^t$, contains g_t and may contain also supervisor places added by enforcing (18–19) and (11). It follows that t'' is enabled in $\mathcal{N}^*$. Therefore, to show that t'' is enabled, we only need to show that the supervisor enables t''. Let μ_1^* be the marking of $\mathcal{N}^*$. Since in $\mathcal{N}^*$ we have that $\bullet t'' = \{g_t\}$, if $\mu_1^* \xrightarrow{t''} \mu_2^*$, then for all i: $l_i^*\mu_2^* = l_i^*\mu_1^* - l_i^*(g_t)$. However, in view of (17) and $h_{d,i} = \max(0, l_iD, h_i)$, $l_i^*(g_t) \geq 0$. Therefore, $l_i^*\mu_2^* \leq l_i^*\mu_1^*$. So, if μ_1^* satisfies (20), so does μ_2^*. Then, the constraints (11) enable the firing of t''. Moreover, as mentioned in Remark 3.1, the constraints (18–19) do not disable t''. Therefore, t'' is enabled in $\mathcal{N}^t$. ■

Theorem 4.1 *For any initial marking μ_0 satisfying (3), $(\mathcal{N}^s, \mu_0^s)$ enforces (3). Moreover, under the no concurrency assumption, the supervision is least restrictive.*

Proof: Proving the fact that (3) is enforced does not need the assumption of Remark 4.2, that the supervisor fires the transitions t'' as soon as enabled. To prove that (3) is enforced, it is enough to show that if the supervisor allows the plant to fire q at the marking μ (where μ satisfies (3)) then μ and q satisfy (3). Since the assumption of Remark 4.2 is not made, it may be that some of the places g_t of the closed-loop have tokens when q is enabled by the supervisor. Thus, in terms of the marking μ^* of $\mathcal{N}^*$, for all i, $l_i^*\mu^* = l_i\mu + \sum_t l_i^*(g_t)\mu^*(g_t)$. By (17), for all g_t we have $l_i^*(g_t) > 0$. Therefore, $l_i^*\mu^* \geq l_i\mu$. If firing q results in the marking μ_2^* of $\mathcal{N}^*$, then $l_i^*\mu_2^* = l_i^*\mu^* + h_{d,i}q$, in view of (16–17). Thus, $l_i^*\mu_2^* \geq l_i\mu + h_{d,i}q$. By Theorem 3.1, (20) is enforced on $\mathcal{N}^*$. Therefore, since (20) is satisfied at μ_2^*, μ and q satisfy also (12). This concludes the proof of the first part of the theorem.

For the second part of the proof, we will assume that when the plant fires a transition t, the supervisor fires immediately the corresponding transition t''. By Proposition 4.2, this is always possible. Firing t'' immediately after t ensures that $\mu^*(g_t) = 0$ for all places g_t. To prove that the supervision is least restrictive, it is sufficient to show that if firing t at a marking μ satisfies (3), then the supervisor enables t. Let q be the firing vector associated with t. If (3) is satisfied, so is (12). Then, for all indices j there is $i \in A_j$ such that $l_i\mu + h_{d,i}q \leq c_i$. If μ^* is the marking of $\mathcal{N}^*$ corresponding to μ and μ_2^* is the marking reached by firing q, then $l_i^*\mu^* = l_i\mu$ and $l_i^*\mu_2^* = l_i\mu + h_{d,i}q$. Thus, (20) is satisfied at μ_2^*. By Theorem 3.1, the enforcement of (20) on $\mathcal{N}^*$ is least restrictive, so t is enabled in $\mathcal{N}^*$ at μ^*. Therefore, the supervisor enables t at the marking μ of the plant $\mathcal{N}$. This concludes our proof. ■

Example 4.1 The readers/writers problem is a classical coordination problem found in operating systems textbooks.

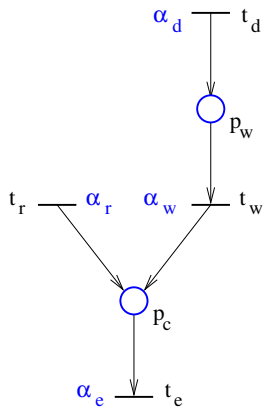

Fig. 2. Model of the reader/writer system. $\alpha_d \ldots \alpha_e$ denote the labels associated with each transition.

In this problem, several reader processes (RPs) and several writer processes (WPs) access a common segment of data. When a process accesses the data, we say that it is in the critical section (CS). When a WP is in the CS, no other processes may enter the CS. However, any number of RPs may be at the same time in the CS. Here we consider the version of the problem in which WPs have priority: no RP may enter the CS if a WP waits to access the CS.

A PN model of the reader/writer system is shown in Figure 2. The number of tokens in p_c is the number of processes in the CS. The transition t_e is fired when a process exits the CS, t_r when a RP enters the CS, and t_w when a WP enters the CS. The number of tokens in p_w represent the number of WPs waiting to enter the CS. A WP enters the p_w state by the firing of t_d.

The specification can be written as $[\mu_w \leq 0] \vee ([q_r \leq 0] \wedge [q_w \leq 0]) \vee ([q_r \leq 0] \wedge [\mu_c \leq 0])$. This expression has the form (3) and can be brought to the form (12): $([q_r \leq 0] \vee [\mu_w \leq 0]) \wedge ([\mu_w \leq 0] \vee [q_w \leq 0] \vee [\mu_c \leq 0])$. Note that we have four constraints $l_i\mu + h_i q \leq c_i$. We identify $l_i\mu + h_i q \leq c_i$ for $i = 1 \ldots 4$ with $[\mu_w \leq 0]$, $[q_r \leq 0]$, $[q_w \leq 0]$, and $[\mu_c \leq 0]$, in this order. The set of transitions T_s is $T_s = \{t_e, t_r, t_w\}$. The $\mathcal{N}_g$ PN is shown in Figure 3(a). Thus, the constraints $l_i^*\mu \leq c_i$, for $i = 1 \ldots 4$, are in this order $\mu_w + \mu_{g_w} \leq 0$, $\mu_{g_r} \leq 0$, $\mu_{g_w} \leq 0$, and $\mu_c + \mu_{g_e} \leq 0$. For the upper bounds M_i and m_i, all bounds m_i will be taken zero. We consider the no concurrency setting, thus all firing vectors are bounded by one. Assuming no more than two writers processes, we obtain $M_1 = 3$. Further, $M_2 = 1$ and $M_3 = 1$. Assuming no more than ten RPs can ever be in the CS at the same time, $M_4 = 11$.

To keep our example simple, we will only illustrate the enforcement of the subspecification $[q_r \leq 0] \vee [\mu_w \leq 0]$. The PN $\mathcal{N}^c$ is shown in Figure 4(a). For the constraint $q_r \leq 0$ the inequalities (18–19) are $\mu_{g_r}^* + \delta_2 \leq 1$ and $\mu_{g_r}^* + \delta_2 \geq 1$. For the constraint $\mu_w \leq 0$, the inequalities (18–19) are $\mu_w^* + \mu_{g_w}^* + 3\delta_1 \leq 3$ and $\mu_w^* + \mu_{g_w}^* + \delta_1 \geq 1$. The only constraint (11) is $\delta_1 + \delta_2 \geq 1$. The closed-loop $\mathcal{N}^t$ is shown in Figure 4(b) and the supervisor $\mathcal{N}^s$ in Figure 5. □

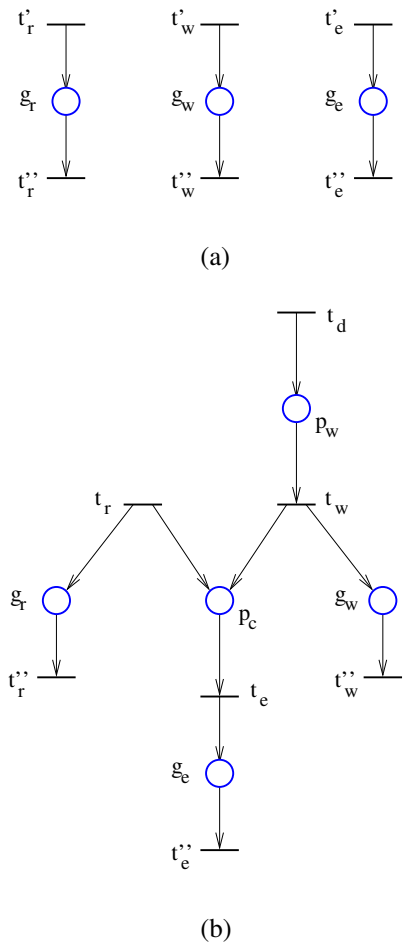

Fig. 3. (a) $\mathcal{N}_g$; (b) $\mathcal{N}^*$.

V. Final Remarks

The paper has considered fully controllable and observable PNs. For the general case, it is necessary to ensure that a supervisor is feasible, that is, it respects the uncontrollability and unobservability constraints of the plant. In the case of the constraints (2), it is known that the supervisor (4–5) is feasible if a simple structural test is satisfied [12]. Thus, given a PN labeled by $\rho_0 : T \to \Sigma_0$ in which the set of uncontrollable events is Σ_{uc} and the set of unobservable events is Σ_{uo}, the supervisor (4–5) is feasible when

$$\forall t \in T,\ \rho_0(t) \in \Sigma_{uc} \Rightarrow D_c^-(\cdot, t) = 0, \quad (21)$$

$$\forall t \in T,\ \rho_0(t) \in \Sigma_{uo} \Rightarrow D_c(\cdot, t) = 0, \quad (22)$$

$$\forall t_1, t_2 \in T,\ \rho_0(t_1) = \rho_0(t_2) \Rightarrow D_c(\cdot, t_1) = D_c(\cdot, t_2), \quad (23)$$

where $D_c = D_c^+ - D_c^-$.

It is interesting to determine a structural test also for disjunctive constraints. In the case of the constraints (7), a possible solution is to require each of the constraints $l_i\mu \leq c_i$ to satisfy (21–23). Then, a supervisor constructed as in section III is feasible. Indeed, the condition (23) ensures that the change in the supervisor marking can be determined only from the label of the transition that is fired. Further, the

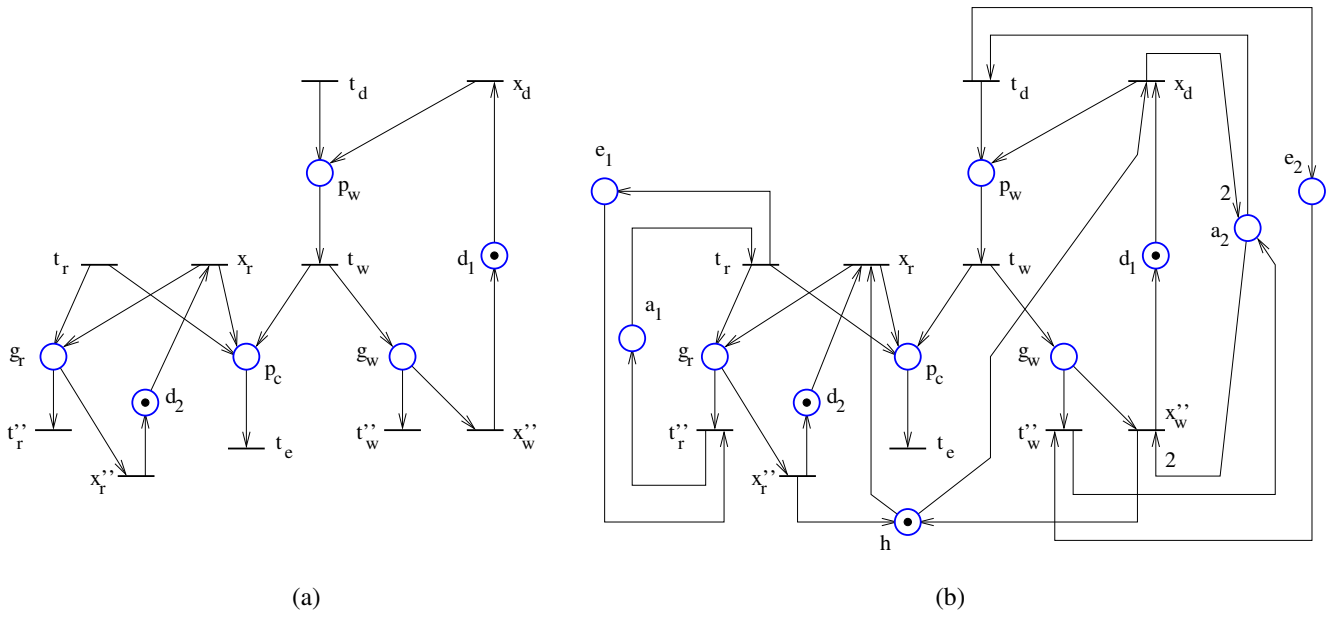

Fig. 4. $\mathcal{N}^c$ (a) and $\mathcal{N}^t$ (b) for the subspecification $[q_r \leq 0] \vee [\mu_w \leq 0]$.

condition (22) ensures that the supervisor marking will not be affected by firing unobservable transitions. Finally, the condition (21) ensures that the supervisor will never disable a transition labeled by an uncontrollable event.

The problem of determining a structural test for (12) that ensures the construction of section IV is feasible is more involved. It is to be addressed in future work.

Concerning the complexity of the supervisor, the number of places of the supervisor is upper bounded by $n_c + 2n_i + |T|$, where n_i is the number of constraints $l_i\mu + h_i q \leq c_i$ in (12). However, in the worst case, the number of transitions of the supervisor depends on 2^{n_i}. This is in contrast to the linear complexity of the supervisors of [11]. This is due to the fact that the approach of [11] is not least restrictive.

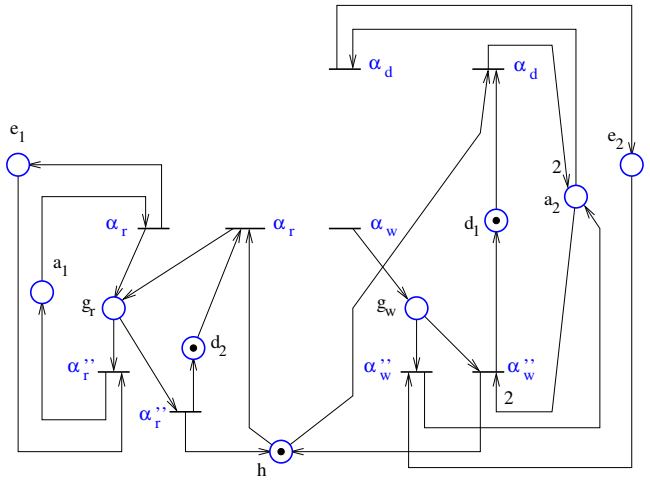

Fig. 5. The supervisor for the subspecification $[q_r \leq 0] \vee [\mu_w \leq 0]$. The events labeling the transitions indicate how transitions are synchronized when the plant is composed with the supervisor.

REFERENCES

[1] B. Krogh and L. Holloway, "Synthesis of feedback control logic for manufacturing systems," *Automatica*, vol. 27, no. 4, pp. 641–651, 1991.

[2] M. Tittus and B. Egardt, "Hierarchical supervisory control for batch processes," *IEEE Trans. Contr. Syst. Technol.*, vol. 7, no. 5, pp. 542–554, 1999.

[3] M. Iordache and P. Antsaklis, "Design of T-liveness enforcing supervisors in Petri nets," *IEEE Trans. Automat. Contr.*, vol. 48, no. 11, pp. 1962–1974, 2003.

[4] J. Park and S. Reveliotis, "Liveness-enforcing supervision for resource allocation systems with uncontrollable behavior and forbidden states," *IEEE Trans. Robot. Automat.*, vol. 18, no. 2, pp. 234–240, 2002.

[5] A. Giua, F. DiCesare, and M. Silva, "Generalized mutual exclusion constraints on nets with uncontrollable transitions," in *Proc. IEEE Internat. Conf. Syst., Man, Cybern.*, 1992, pp. 974–979.

[6] E. Yamalidou and J. Kantor, "Modeling and optimal control of discrete-event chemical processes using Petri nets," *Computers and Chemical Engineering*, vol. 15, no. 7, pp. 503–519, 1991.

[7] A. Giua and C. Seatzu, "Supervisory control of railway networks with Petri nets," in *Proc. 40th IEEE Conf. Decision Contr.*, Dec. 2001, pp. 5004–5009.

[8] M. V. Iordache and P. J. Antsaklis, "Synthesis of supervisors enforcing general linear vector constraints in Petri nets," *IEEE Trans. Automat. Contr.*, vol. 48, no. 11, pp. 2036–2039, 2003.

[9] G. Stremersch and R. K. Boel, "Decomposition of the supervisory control problem for Petri nets under preservation of maximal permissiveness," *IEEE Trans. Automat. Contr.*, vol. 46, no. 9, pp. 1490–1496, 2001.

[10] ——, "Structuring acyclic Petri nets for reachability analysis and control," *Discrete Event Dynamic Systems*, vol. 12, no. 1, pp. 7–41, 2002.

[11] M. V. Iordache and P. J. Antsaklis, "A structural approach to the enforcement of language and disjunctive constraints," in *Proc. 2005 Amer. Contr. Conf.*, 2005, pp. 3920–3925.

[12] ——, *Supervisory Control of Concurrent Systems: A Petri Net Structural Approach*. Birkhäuser, 2006.

[13] A. Giua and F. DiCesare, "Supervisory design using Petri nets," in *Proc. 30th IEEE Conf. Decision Contr.*, 1991, pp. 92–97.