Reduction of the Supervisor Design Problem with Firing Vector Constraints

Marian V. Iordache
School of Engineering and Eng. Tech.
LeTourneau University
Longview, TX 75607-7001

Panos J. Antsaklis
Department of Electrical Engineering
University of Notre Dame
Notre Dame, IN 46556

June 10, 2005

Context

PNs developed in Computer Science to model concurrent processes (CPs).

Mutual exclusion: a common constraint type imposed on CPs.

Expressed in PNs by: $\sum_i \mu_i \leq c$.

Used also in the context of AGV coordination for manufacturing systems [Krogh and Holloway 1991] and batch chemical processes [Tittus and Lenartson, 1999].

More complex constraints $L\mu \leq b$ are necessary (L, b integer matrices)
- due to uncontrollability and unobervability
- to express more complex specifications

The constraints $L\mu \leq b$ have been used to describe liveness enforcing supervisors [Iordache and Antsaklis, 2000; Park and Reveliotis, 2002].

Context

In the context of chemical process control [Yamalidou and Kantor 1991], constraints describing how valves should be opened/closed result in:

$$L\mu + Hq \leq b.$$

The same arise also in railway networks [Giua and Seatzu 2001], describing safety constraints (trains should not collide).

The more general form

$$L\mu + Hq + Cv \leq b$$

used in a rather complex AGV coordination problem [Iordache and Antsaklis, 2003].

Fairness constraints of the form

$$Cv \leq b$$

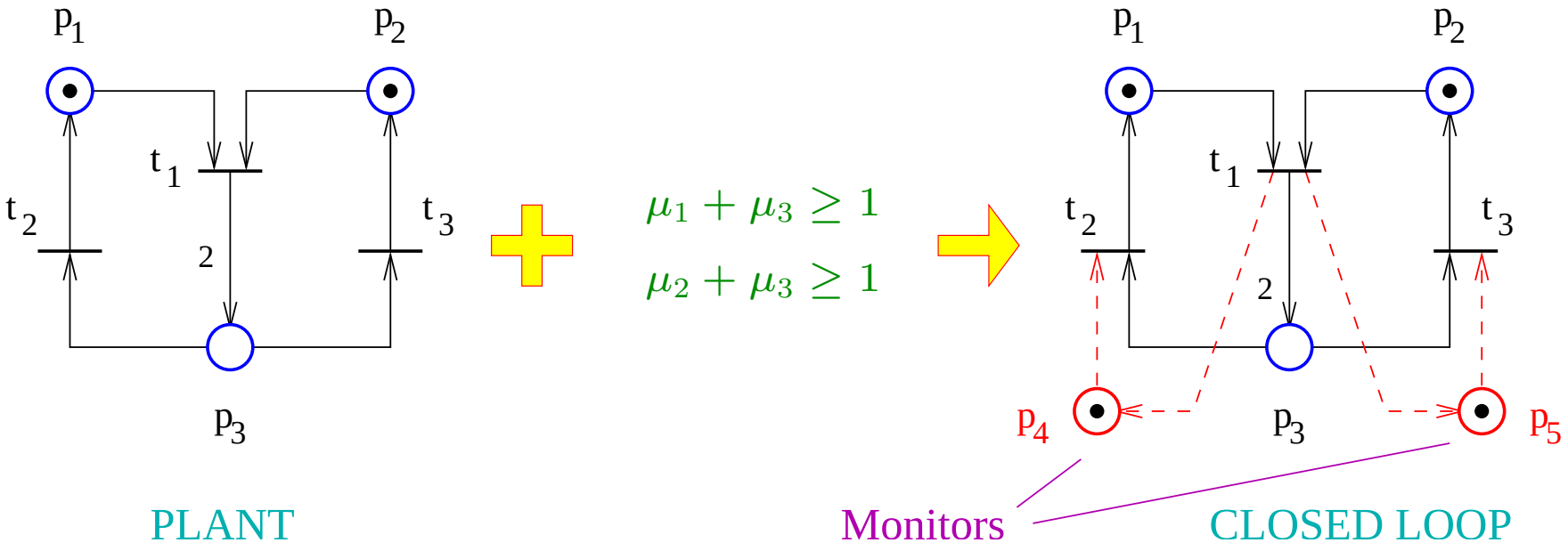
were used for a communication protocol [Genrich et al, 1980] and a manufacturing application [Li and Wonham, 1993].

The *supervision based on place invariants* developed for constraints $L\mu \leq b$.

(All reachable markings μ constrained to satisfy $L\mu \leq b$.)

Let D be the incidence matrix and μ_0 the initial marking.

The supervisor consists of *monitor places* connected according to $D_s = -LD$ and of initial marking $\mu_{s0} = b - L\mu_0$.

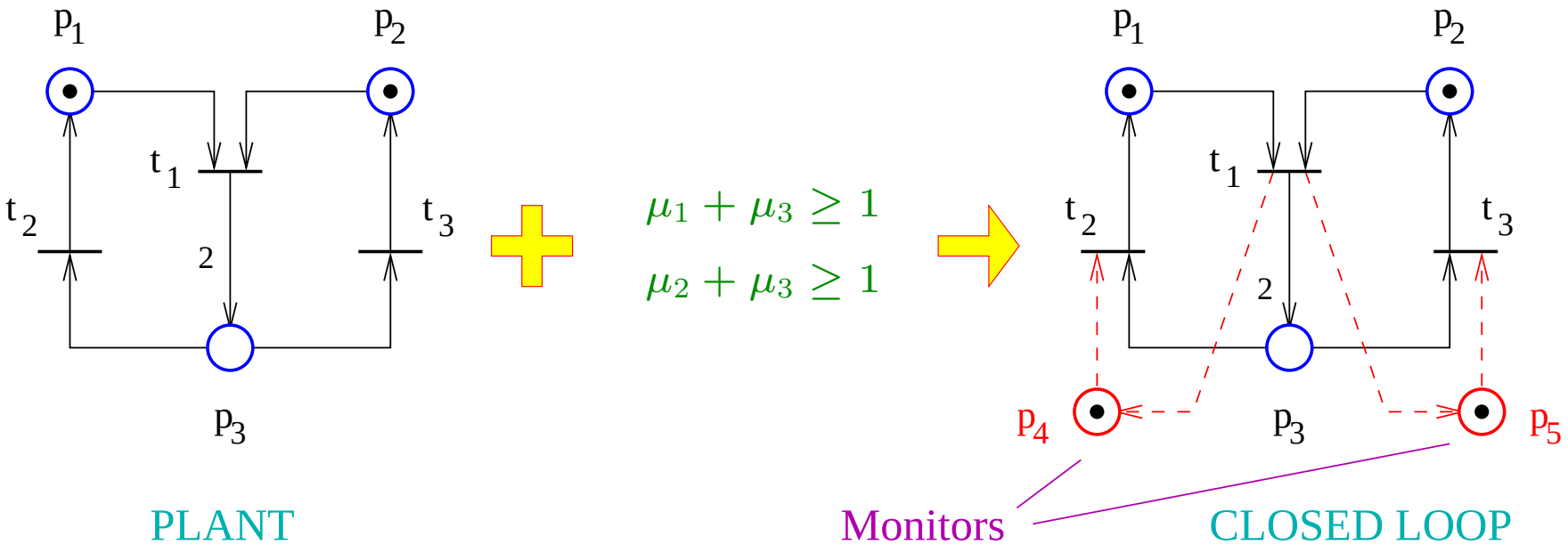


Conversely, given a set of monitors, what specification do they enforce?

$L\mu + Hq + Cv \leq b$, in general.

- The Cv term not needed if they participate in place invariants.

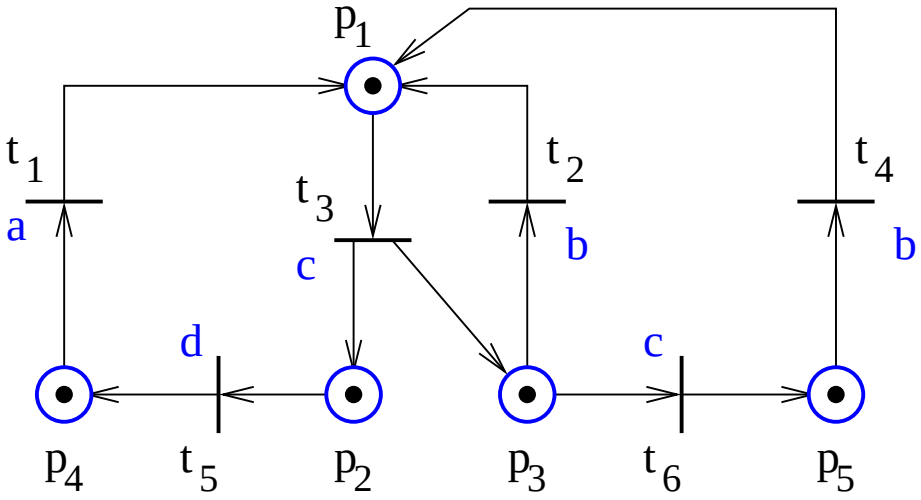
- The Hq term needed if they have selfloops.



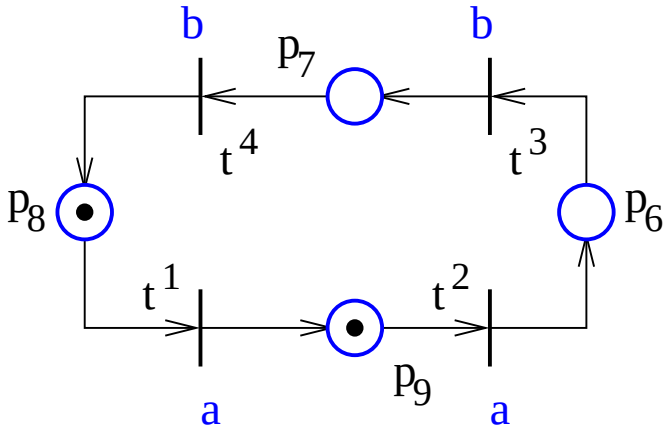
It is desirable to be able to deal with even more general specifications.

For what kind of specifications is the closed-loop still a Petri net?

- Prefix type language specifications.
- In particular, disjunctions $\bigvee_i L_i\mu \leq b_i$, under some boundedness assumptions.



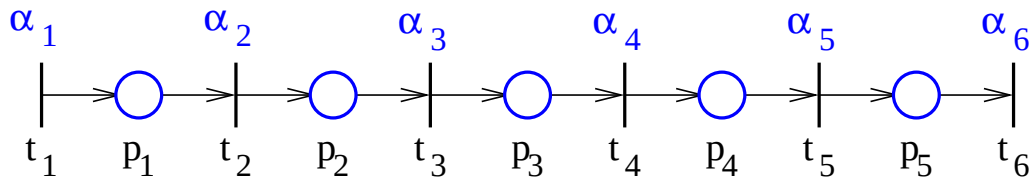
PLANT



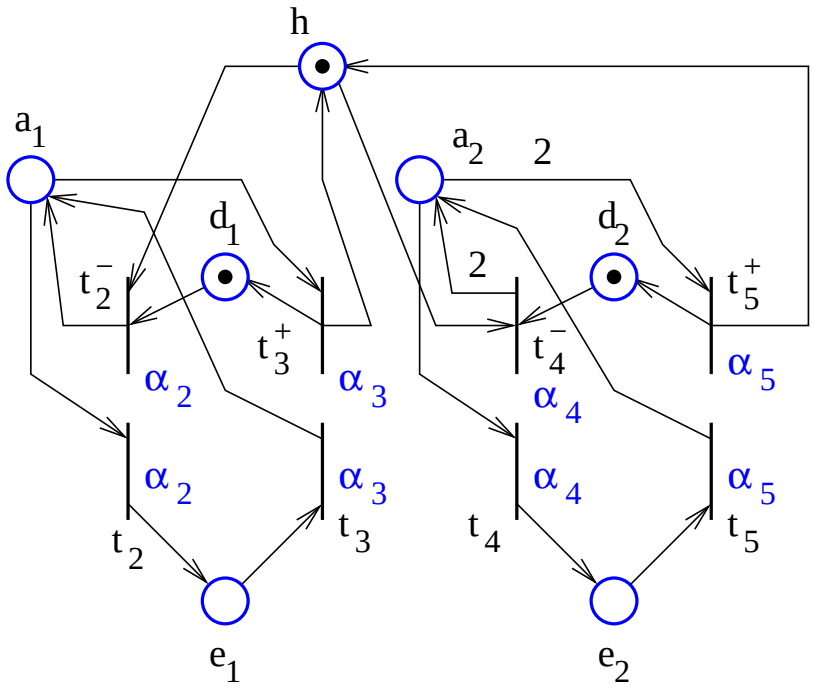
SPECIFICATION

As an example, this is the plant. The specification is

$$[\mu_2 \leq 0] \vee [\mu_4 \leq 0].$$



Assuming the bounds $\mu_2 \leq 2$ and $\mu_4 \leq 3$, this supervisor results:



Note that the supervisor is not free-labeled (though the plant is).

Difficulties arise due to partial uncontrollability and unobservability.

We have focused on structural and *suboptimal* methods of supervisor design.

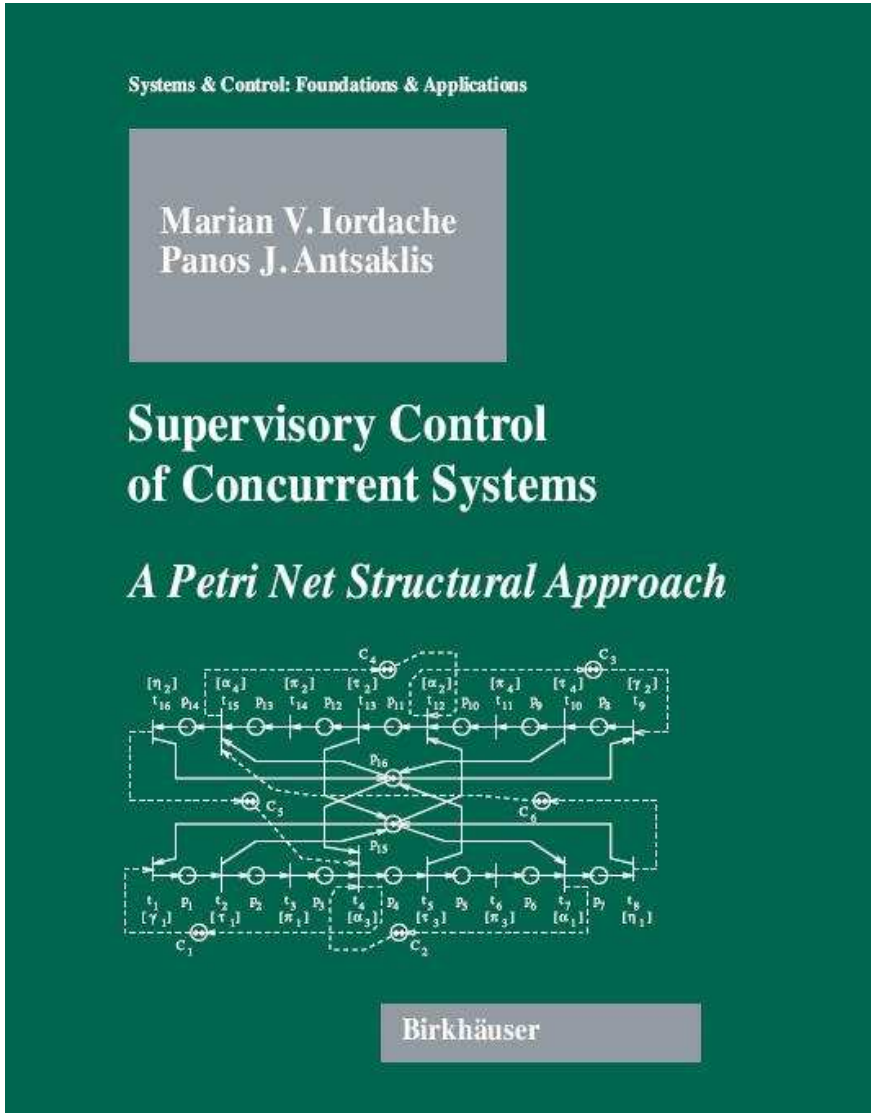
- Not necessarily least restrictive solutions; a solution may not be found even when one exists.
- The deadlock prevention problem needs to be dealt with separately.

+ The supervisor is parametrized by the initial marking μ_0:
  + a numerical value of μ_0 is not necessary to design a supervisor;
  + changes in the numerical value of μ_0 do not require recalculating the supervisor.
+ Potential computational benefits (reachability analysis avoided).

We have addressed:

- Centralized and decentralized control.
- Labeled PN plants with or without concurrency.
- Disjunctive, P-type language, generalized linear constraints. Also liveness specifications.

BOOK


Systems & Control: Foundations & Applications
Marian V. Iordache
Panos J. Antsaklis
Supervisory Control
of Concurrent Systems
A Petri Net Structural Approach
Birkhäuser

TOPIC

This presentation considers the supervision problem for specifications

$$\bigvee_{i=1}^{n_d} [L_i \mu + H_i q + C_i v \leq b_i] \tag{1}$$

By adding sink places, the Cv term can be incorporated in the $L\mu$ term.

Therefore, it is enough to focus on constraints

$$\bigvee_{i=1}^{n_d} [L_i \mu + H_i q \leq b_i] \tag{2}$$

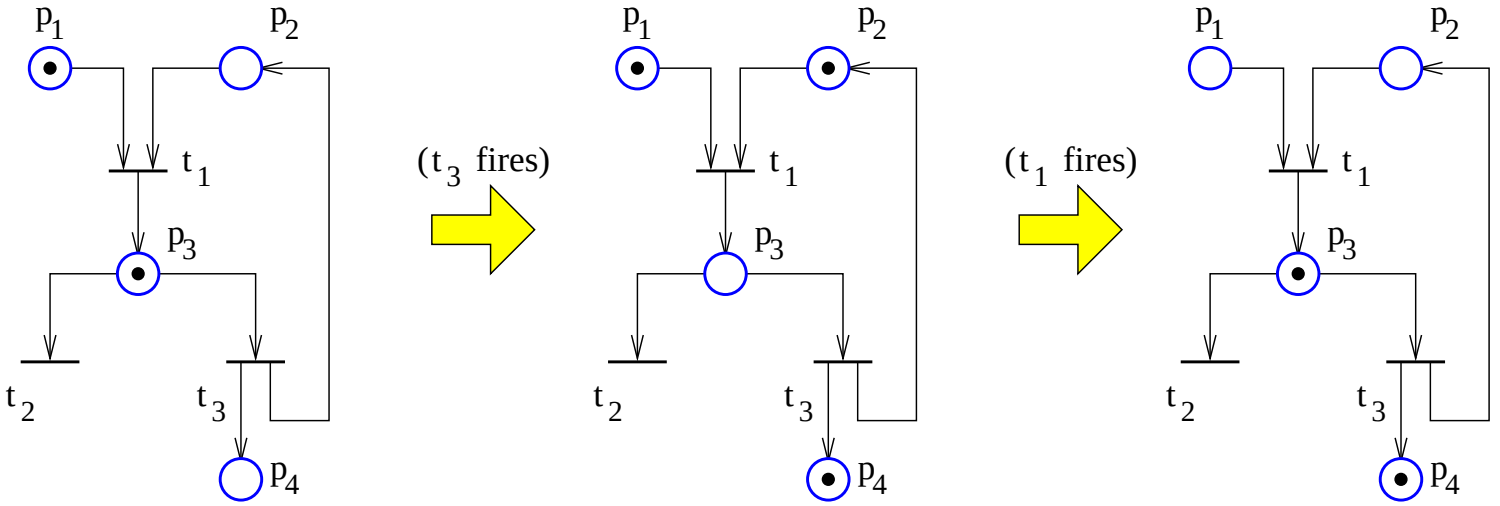
The paper shows that the problem of enforcing (2) can be reduced to the problem of enforcing (3) on a transformed Petri net, *without loss of permissiveness.*

$$\bigvee_{i=1}^{n_d} [L_{H,i} \mu_H \leq b_i] \tag{3}$$

Notation: μ – the marking, μ_0 – the initial marking, D – the incidence matrix, q – the firing vector, and v – the Parikh vector. Let $\mu_i = \mu(p_i)$, $q_j = q(t_j)$ and $v_j = v(t_j)$.

q_j: how many times t_j is to be fired; v_j: how many times t_j has been fired.

The state equation: $\mu = \mu_0 + Dv$.



$$\mu_0 = [\ 1 \quad 0 \quad 1 \quad 0\ ]^T \qquad \mu' = [\ 1 \quad 1 \quad 0 \quad 1\ ]^T \qquad \mu'' = [\ 0 \quad 0 \quad 1 \quad 1\ ]^T$$
$$v = [\ 0 \quad 0 \quad 0\ ]^T \qquad v = [\ 0 \quad 0 \quad 1\ ]^T \qquad v = [\ 1 \quad 0 \quad 1\ ]^T$$
$$q = [\ 0 \quad 0 \quad 1\ ]^T \qquad q = [\ 1 \quad 0 \quad 0\ ]^T$$

The *generalized linear constraints* can describe places arbitrarily connected to a PN.

They have the form:

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

They require the initial state (μ_0, v_0) to satisfy

$$L\mu_0 + Cv_0 \leq b$$

Further, a transition t_i may fire from a current state (μ, v) iff

(a) $L\mu + Hq + Cv \leq b$ for $q(i) = 1$ and $q(j) = 0\ \forall j \neq i$.

(b) $L\mu' + Cv' \leq b$, where $v' = v + q$ and $\mu \xrightarrow{t_i} \mu'$.

The generalized linear constraints describe the P-type languages of free-labeled PNs.

The enforcement of the *generalized linear constraints* has been studied by Iordache and Antsaklis [ACC 2002, TAC 48(11)].

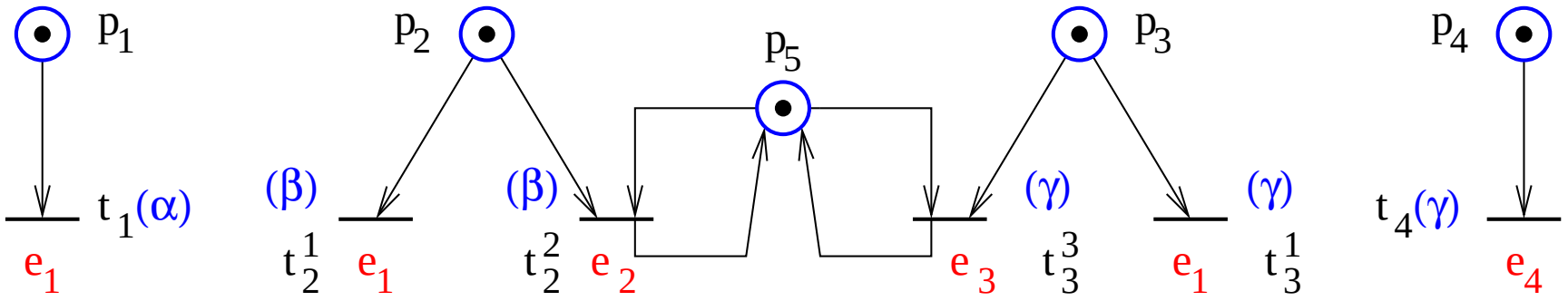
Setting

The plant is assumed to be a *double-labeled PN*. $\rho : T \rightarrow \mathcal{K}$ ($o : T \rightarrow \mathcal{O}$) associates control (observation) events to transitions.

$\mathcal{K}_c \subseteq \mathcal{K}$ ($\mathcal{O}_o \subseteq \mathcal{O}$) denote the sets of controllable (observable) events.

A double-labeled PN can model both the uncontrollability of CtlPNs (Krogh and Holloway) and the unobservability of labeled PNs.

The results are obtained under the concurrency setting (transition-bag assumption, $q \in \mathbb{N}$).



Above, $\mathcal{K} = \{e_1, e_2, e_3, e_4\}$ and $\mathcal{O} = \{\alpha, \beta, \gamma\}$.

GLCs and Concurrency

Interpreting $\bigvee_i L_i\mu + H_i q + C_i v \leq b_i$ is a nontrivial issue.

Let's begin with $L\mu + Hq + Cv \leq b$, *under concurrency.*

Let $H_d = \max(0, LD + C, H)$. Consider the monitors enforcing $L\mu + Hq + Cv \leq b$ that are constructed under the no concurrency assumption (Iordache and Antsaklis, 2003).

The monitors enable q when $H_d q \leq \mu_c = b - L\mu - Cv$.

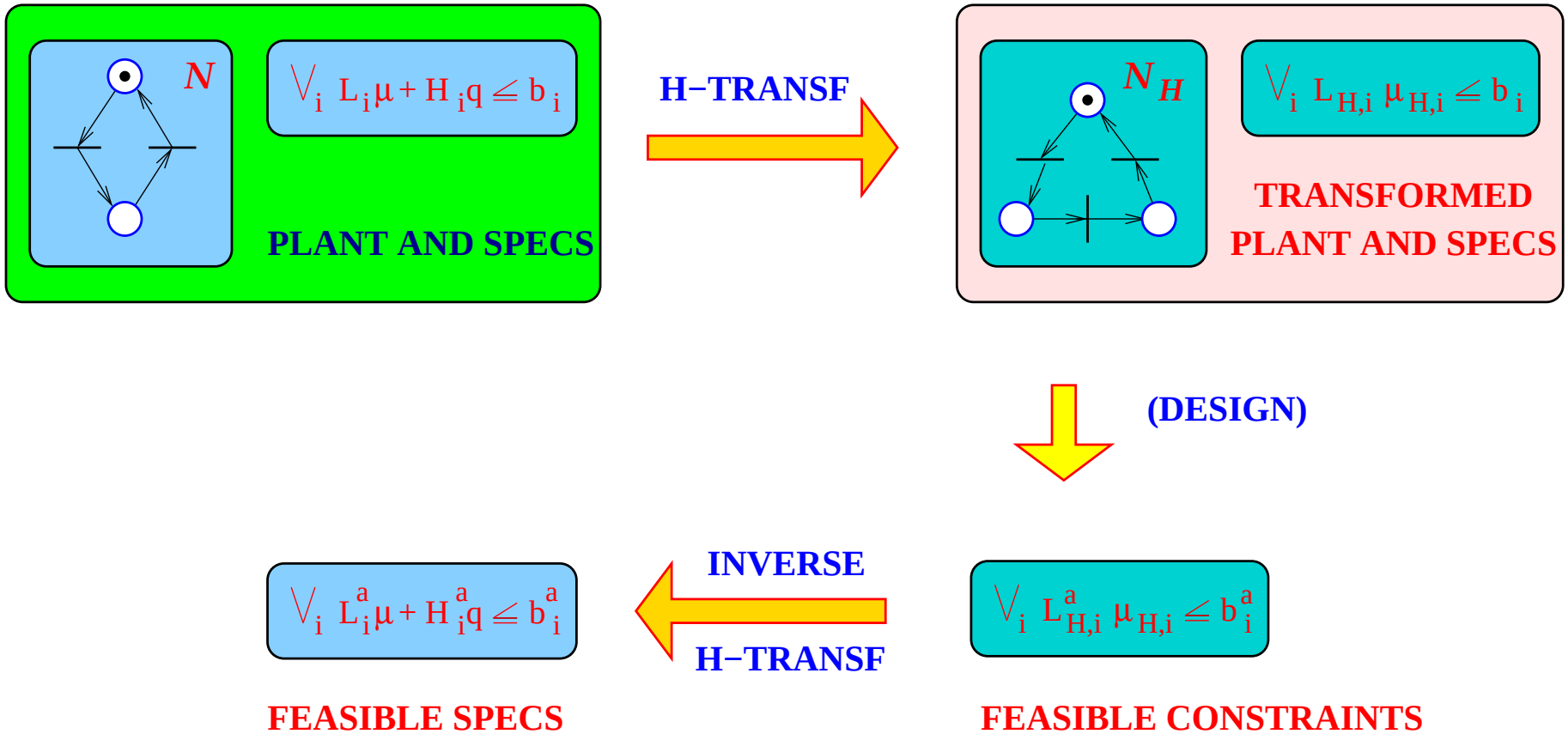
This will be the concurrency interpretation of $L\mu + Hq + Cv \leq b$: at any time, μ, q and v are permissible if they satisfy $H_d q \leq b - L\mu - Cv$.

Intuitively, this corresponds to q enabled iff at all intermediary stages of the firing of q, the specification is satisfied (Lemma 2.1).

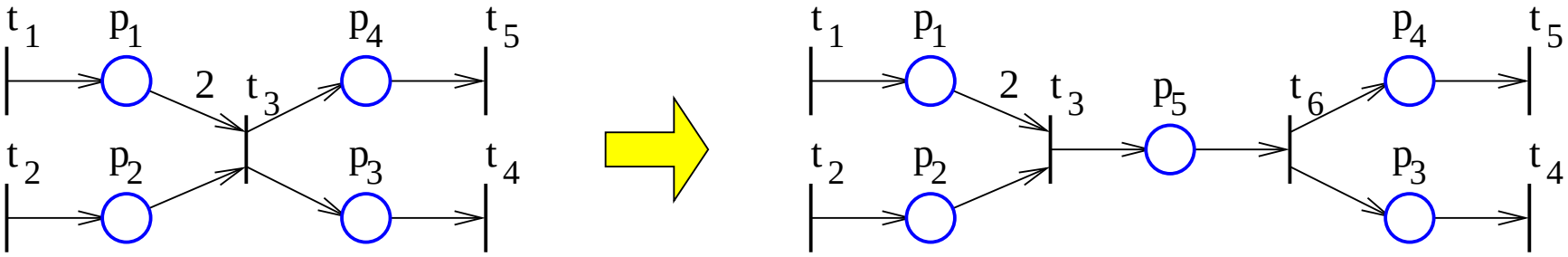
This will be the concurrency interpretation of $\bigvee_i L_i\mu + H_i q + C_i v \leq b_i$: at any time, μ, q and v are permissible if they satisfy $H_{d,i} q \leq b_i - L_i\mu - C_i v$ for some i.

Approach

Given $\bigvee_{i=1}^{n} L_i\mu + H_i q \leq b_i$, the approach is to find $\bigvee_{i=1}^{m} L_i^a\mu + H_i^a q \leq b_i^a$ that is feasible such that $\bigvee_{i=1}^{m} L_i^a\mu + H_i^a q \leq b_i^a \Rightarrow \bigvee_{i=1}^{n} L_i\mu + H_i q \leq b_i$.



The transformation splits transitions to substitute a q_i term by a marking term.



This transformation maps

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

into

$$\mu_1 + \mu_2 + 2\mu_3 + 4\mu_5 \leq 5 \tag{6}$$

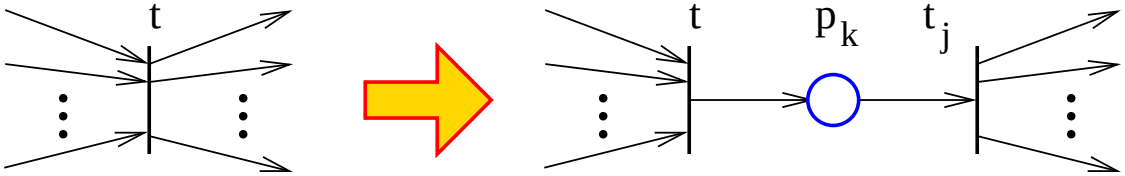
The term $4\mu_5$ is obtained as follows. Consider firing t_3 in the transformed net: $\mu \xrightarrow{t_3} \mu'$. The coefficient a of t_3 is to satisfy that

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

Input: $\mathcal{N} = (P, T, D^-, D^+)$, $L\mu + Hq \leq b$, and optionally μ_0 and a set $T_{s,H} \subseteq T$.

Output: $\mathcal{N}_H = (P_H, T_H, D_H^-, D_H^+)$, $L_H\mu_H \leq b$, and μ_{H0}.

1. Let $T_s = \{t \in T : \rho(t) = \rho(t') \text{ for some } t' \in T \text{ s.t. } t' \in T_{s,H} \text{ or } H_d(\cdot, t') \neq 0\}$, where $H_d = \max(LD, H, 0)$.
2. Let $\mathcal{N}_H = \mathcal{N}$, $L_H = L$, and $\mu_{H0} = \mu_0$.
3. For all $t \in T_s$:



   (a) Split t in t, p_k, and t_j.
   (b) Let $L_H(\cdot, p_k) = H_d(\cdot, t_i) + LD^-(\cdot, t_i)$ and $\mu_{H0}(p_k) = 0$.
4. For all $t \in T_s$:
   (a) $o(t \bullet \bullet) = o(t)$.
   (b) Extend the set of control events s.t. $\rho(t \bullet \bullet) \notin \{\rho(t) : t \in T\}$.
   (c) $\rho(t \bullet \bullet)$ is controllable iff $\rho(t)$ is controllable.
   (d) For all $t' \in T_s$, $\rho(t \bullet \bullet) = \rho(t' \bullet \bullet)$ iff $\rho(t) = \rho(t')$.

The H-transformation for a set of constraints $\bigvee_i L_i\mu + H_i q \leq b_i$:

1. Let $H_{d,i} = \max(L_i D, H_i, 0)$ and $T_{s,H} \rightarrow T_{s,H} \cup \bigcup_i \{t \in T : \ H_{d,i}(\cdot, t) \neq 0\}$.
2. For all i, apply the H-transformation to the constraints $L_i\mu + H_i q \leq b_i$ with the argument $T_{s,H}$ above. Let $L_{H,i}\mu_H \leq b_i$, $\mathcal{N}_H$, and μ_{H0} be the result.
3. Final result: $\bigvee_i L_{H,i}\mu_H \leq b_i$, $\mathcal{N}_H$, and μ_{H0}.

The H^{-1}-Transformation of $L_H\mu_H \leq b$

Input: $\mathcal{N} = (P, T, D^-, D^+)$, $\mathcal{N}_H = (P_H, T_H, D_H^-, D_H^+)$, and $L_H\mu_H \leq b$.

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 $H(\cdot, t_i) = L_H(\cdot, p_k) - L_H D_H^-(\cdot, t_i)$.

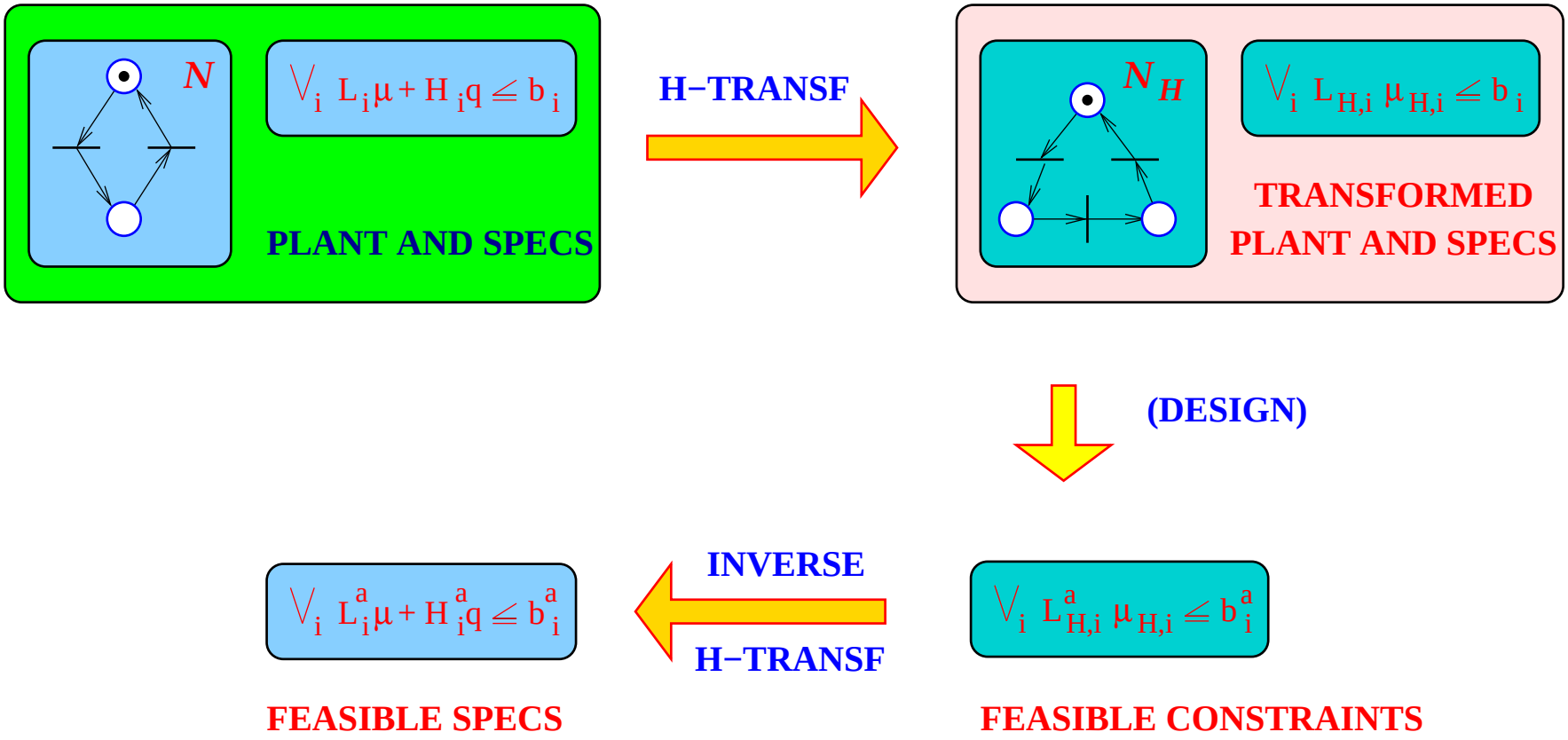
The H^{-1}-Transformation of $\bigvee_i L_{H,i}\mu_H \leq b_i$

1. For all i, 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. Final result: $\bigvee_i L_i\mu + H_iq \leq b_i$.

Notation

$\mathcal{S} \equiv \bigvee_i L_i\mu + H_i q \leq b_i$, $\mathcal{S}_H \equiv \bigvee_i L_{H,i}\mu_H \leq b_i$, $\mathcal{S}_H^a \equiv \bigvee_i L_{H,i}^a\mu_H \leq b_i^a$,

and $\mathcal{S}^a \equiv \bigvee_i L_i^a\mu + H_i^a q \leq b_i^a$.



Notation

Fact: $\mathcal{S} \xrightarrow{H} \mathcal{S}_H$ and $\mathcal{S}_H \xrightarrow{H^{-1}} \mathcal{S}' \Rightarrow \mathcal{S} = \mathcal{S}'$.

But is it true that $\mathcal{S}_H \xrightarrow{H^{-1}} \mathcal{S}$ and $\mathcal{S} \xrightarrow{H} \mathcal{S}'_H \Rightarrow \mathcal{S}_H = \mathcal{S}'_H$?

Theorem 3.3 (a) The H-transformation of any $\mathcal{S}$ satisfies

$$\forall p \in P_H \setminus P: \quad \begin{cases} L_H(\cdot, p) \geq L_H D_H^+(\cdot, p\bullet) \\ L_H(\cdot, p) \geq L_H D_H^-(\cdot, \bullet p) \end{cases} \tag{7}$$

$$\forall t \in T \setminus \bullet(P_H \setminus P): \quad L_H D_H(\cdot, t) \leq 0. \tag{8}$$

(b) Given $\mathcal{N}_H$ and $\mathcal{S}_H$, assume $\mathcal{S}_H \xrightarrow{H^{-1}} \mathcal{S}$ and $\mathcal{S} \xrightarrow{H} (\mathcal{S}'_H, \mathcal{N}'_H)$. If L_H satisfies (7–8) and the H-transformation has $T_{s,H} = \bullet(P_H \setminus P)$, then $\mathcal{N}_H = \mathcal{N}'_H$ and $\mathcal{S}_H = \mathcal{S}'_H$.

Feasibility

Let Ξ be the optimal supervisor for $\mathcal{S}$ (i.e. without restriction), Ξ_H for $\mathcal{S}_H$, Ξ_H^a for $\mathcal{S}_H^a$, and Ξ^a for $\mathcal{S}^a$.

Ξ is feasible if it respects the controllability and observability constraints of $(\mathcal{N}, \mu_0)$.

$\mathcal{S}$ is feasible when Ξ is feasible.

H-feasibility: *weaker* than feasibility. Defined for $\mathcal{S}_H$ such that the following result holds true.

Theorem 3.1 Assume $\mathcal{S} \xrightarrow{H} \mathcal{S}_H$. Then $\mathcal{S}$ is feasible iff $\mathcal{S}_H$ is h-feasible.

Permissiveness

The **joint H-transformation** of $\mathcal{S}$ and $\mathcal{S}'$ selects $T_{s,H}$ s.t. $\mathcal{S} \xrightarrow{H} (\mathcal{S}_H, \mathcal{N}_H)$ and $\mathcal{S}' \xrightarrow{H} (\mathcal{S}'_H, \mathcal{N}'_H) \Rightarrow \mathcal{N}_H = \mathcal{N}'_H$.

Notation:

$\Xi \preceq \Xi'$: Ξ is at least as restrictive as Ξ'.

$\Xi \prec \Xi'$: Ξ is more restrictive than Ξ'.

Theorem 3.2 $\Xi \preceq \Xi'$ ($\Xi \prec \Xi'$) iff $\Xi_H \preceq \Xi'_H$ ($\Xi_H \prec \Xi'_H$).

Procedure

1. $(\mathcal{S}, \mathcal{N}) \xrightarrow{H} (\mathcal{S}_H, \mathcal{N}_H)$.
2. Find h-feasible $\mathcal{S}_H^a$ that satisfy (7–8) and $\Xi_H^a \preceq \Xi_H$.
3. $\mathcal{S}_H^a \xrightarrow{H^{-1}} \mathcal{S}^a$. $\underline{\mathcal{S}^a \text{ is the solution.}}$

The **total H-transformation** splits all transitions: $T_{s,H} = T$.

$\mathcal{X}$: the set of supervisors optimally enforcing feasible constraints $\mathcal{S}$.

$\mathcal{X}_H$: the set of supervisors optimally enforcing h-feasible constraints $\mathcal{S}_H$ that satisfy (7–8).

Theorem 3.4

a) $\mathcal{S}^a$ is feasible and $\Xi^a \preceq \Xi$.

Assume that the *total* H-transformation is applied at step one.

b) Ξ^a is least restrictive among the supervisors of $\mathcal{X}$ enforcing $\mathcal{S}$ iff Ξ_H^a is least restrictive among the supervisors of $\mathcal{X}_H$ enforcing $\mathcal{S}_H$.

c) There is no supervisor $\Xi^* \succ \Xi^a$ of $\mathcal{X}$ that enforces $\mathcal{S}$ if there is no supervisor $\Xi_H^* \succ \Xi_H^a$ of $\mathcal{X}_H$ that enforces $\mathcal{S}_H$.

Remarks

The problem of enforcing $\bigvee_i L_i\mu + H_i q \leq b_i$ can be solved in terms of the simpler $\bigvee_i L_{H,i}\mu_H \leq b_i$ in a transformed PN, without loss of permissiveness.

The results were derived under the transition-bag concurrency setting. A loss of permissiveness is possible when this approach is used for other concurrency settings.

The results obtained under a very general uncontrollability and unobservability setting.

The problem of enforcing $\bigvee_i L_{H,i}\mu_H \leq b_i$ is still complex.

- Under certain assumptions, including no concurrency, a solution is available (Stremerssch and Boel, 2002).
- More work has been done on the particular form $L_H\mu_H \leq b$.
- A structural and suboptimal solution to the enforcement of $\bigvee_i L_{H,i}\mu_H \leq b_i$ appears in the book of Iordache and Antasklis, 2006. It applies to double-labeled PNs and the most common concurrency settings.