Generalized Conditions for Liveness Enforcement and Deadlock Prevention in Petri Nets

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

We consider the following liveness properties of a PN:

1. Deadlock-freedom
2. Liveness
3. T-liveness (i.e. *the transitions in a set T are live*)

We are interested in *supervisors* of the PN which enforce either of these properties. We present new theoretical results related to this problem.

The talk is organized as follows:

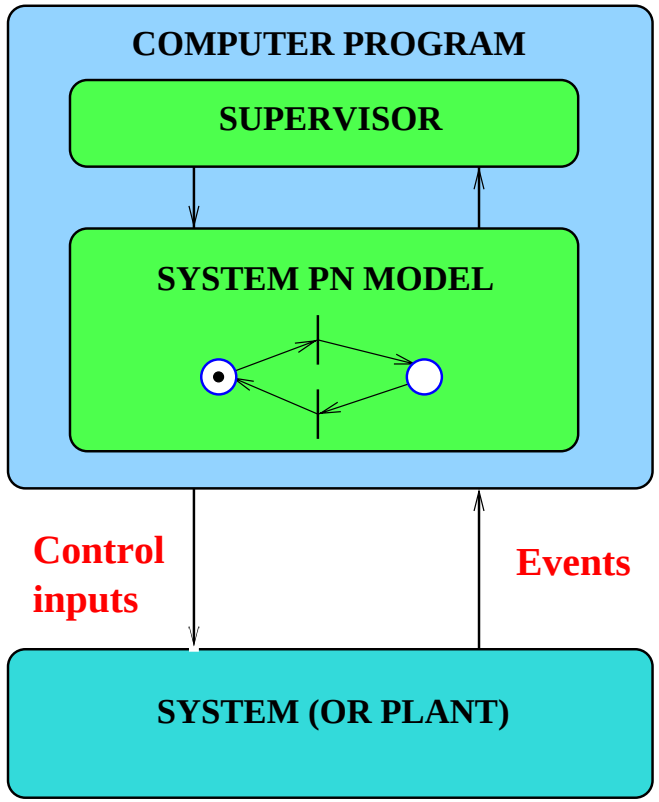
1. Conditions for Deadlock Prevention and Liveness Enforcement
2. Deadlock and Liveness Characterization of PNs Based on Active Subnets
3. Implications for Supervisor Synthesis

Why be interested in PN supervisors?

Supervisors force a system to satisfy desirable properties (such as deadlock-freedom and safety constraints) by restricting the range of the inputs of the system as a function of the system state.

A Control Paradigm:

1. Start with a PN model of the system
2. Enforce safety constraints such that the supervised PN is still a PN
3. Find a liveness supervisor



How to define a supervisor of a PN?

Input: The current marking μ ($the\ state$) and the firing sequence σ ($the\ history$) such that $\mu_0 \xrightarrow{\sigma} \mu$.

Output: The transitions t which may fire, if enabled.

In our problem it turns out that without loss of performance, we can restrict our attention to *marking based supervisors*, which depend only on the current marking.

Definition. *Let* $\mathcal{N} = (P, T, F, W)$ *be a Petri net,* $\mathcal{M}$ *the set of all markings of* $\mathcal{N}$, $\mathcal{M}_0 \subseteq \mathcal{M}$ *and* $U \subseteq \mathcal{M} \times T^*$ *such that* $\forall \mu_0 \in \mathcal{M}_0$*:* $(\mu_0, \varepsilon) \in U$*. A* **supervisor** *is a map* $\Xi : U \to 2^T$ *such that* $\forall (\mu, \sigma) \in U\ \forall t \in \Xi(\mu, \sigma)$*, if* $\mu \xrightarrow{t} \mu'$*, then* $(\mu', \sigma t) \in U$*. We say that* $\mathcal{M}_0$ *is the set of initial markings for which* Ξ *is defined. We also say that* Ξ *is a* **marking based supervisor** *if* $\Xi(\mu, \sigma)$ *depends only on* μ *and* $\forall (\mu, \sigma) \in U$*:* $\{\mu\} \times T^* \subseteq U$*.*

The following type of supervisors will be considered:

- deadlock prevention supervisors
- liveness enforcing supervisors
- T-liveness enforcing supervisors

Some of the results apply to particular classes of PNs:

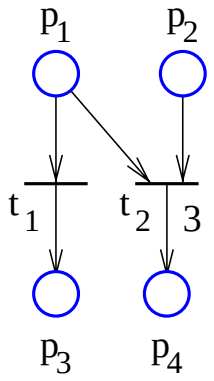
Let $\mathcal{N} = (P, T, F, W)$ be a PN.

We call $\mathcal{N}$ PT-**ordinary** if for all $(p, t) \in F$: $W(p, t) = 1$.

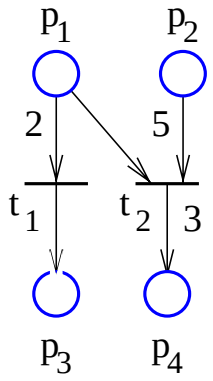
A deadlocked PT-ordinary PN contains an unmarked siphon.

$\mathcal{N}$ has **asymmetric choice** if for all places p_1 and p_2, if $p_1\bullet \cap p_2\bullet \neq \emptyset$ then $p_1\bullet \subseteq p_2\bullet$ or $p_2\bullet \subseteq p_1\bullet$.

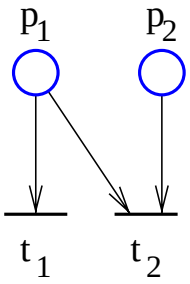
A PT-ordinary PN with asymmetric choice is live if and only if all siphons are controlled.



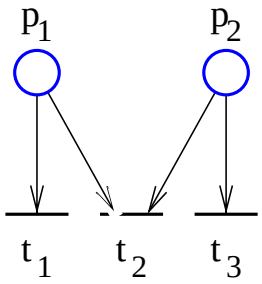
PTO



NOT PTO



AC

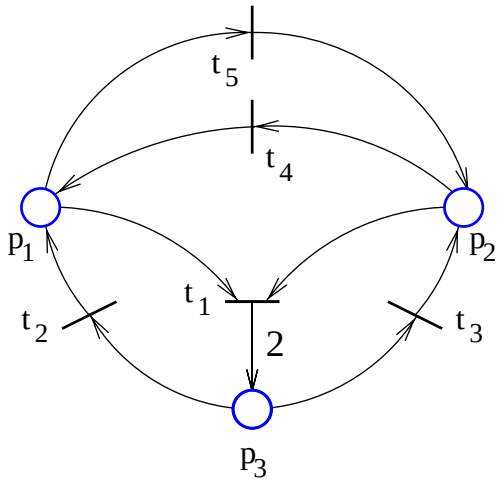


NOT AC

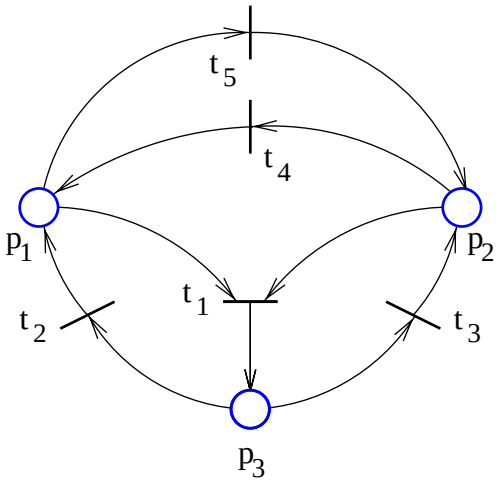
We will *not* restrict our attention to bounded PNs or to *repetitive* PNs.

A PN is **(partially) repetitive** *if there is a marking* μ_0 *and a firing sequence* σ *from* μ_0 *such that every (some) transition occurs infinitely often in* σ*.*

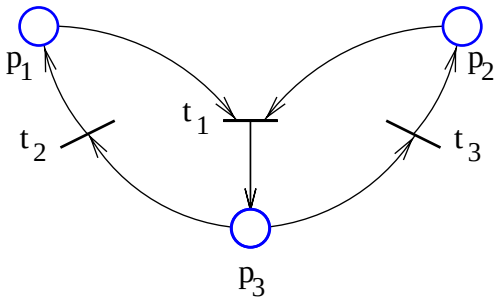
A PN of incidence matrix D is (partially) repetitive iff a vector x of positive (nonnegative) integers exists, such that $Dx \geq 0$ and $x \neq 0$.



repetitive



partially repetitive



not (partially) repetitive

Deadlock Prevention and Liveness Enforcing Conditions

Proposition. *Let $\mathcal{N} = (P, T, F, W)$ be a Petri net.*

(a) Initial markings μ_0 exist s.t. deadlock can be prevented in $(\mathcal{N}, \mu_0)$ iff $\mathcal{N}$ is partially repetitive.

(b) Initial markings μ_0 exist s.t. liveness can be enforced in $(\mathcal{N}, \mu_0)$ iff $\mathcal{N}$ is repetitive.

(c) Initial markings μ_0 exist such that T-liveness can be enforced in $(\mathcal{N}, \mu_0)$ iff there is an initial marking μ_0 enabling an infinite firing sequence in which all transitions of T appear infinitely often.

Lemma. *Let $\mathcal{N} = (P, T, F, W)$ be a PN of incidence matrix D. Assume that there is an initial marking μ_I enabling an infinite firing sequence σ. Let $U \subseteq T$ be the set of transitions which appear infinitely often in σ. There is a nonnegative integer vector x such that*

(a) $Dx \geq 0$, $\forall t_i \in U$: $x(i) \neq 0$ and $\forall t_i \in T \setminus U$: $x(i) = 0$.

(b) there is a firing sequence σ_x containing only the transitions with $x(i) \neq 0$, such that $\exists \mu_1^*, \mu_2^* \in \mathcal{R}(\mathcal{N}, \mu_I)$: $\mu_1^* \xrightarrow{\sigma_x} \mu_2^*$, each transition t_i appears $x(i)$ times in σ_x, σ can be written as $\sigma = \sigma_a \sigma_x \sigma_b$, and $\mu_I \xrightarrow{\sigma_a} \mu_1^*$.

Deadlock Prevention and Liveness Enforcing Conditions

(P_1) $(\exists \sigma\ \exists \mu_1', \mu_1 \in \mathcal{R}(\mathcal{N}, \mu)\colon\ \mu_1 \xrightarrow{\sigma} \mu_1'$ and $\mu_1' \geq \mu_1)$

(P_2) $(\exists \sigma\ \exists \mu_1', \mu_1 \in \mathcal{R}(\mathcal{N}, \mu)\colon\ \mu_1 \xrightarrow{\sigma} \mu_1',\ \mu_1' \geq \mu_1$ and all transitions of T are in $\sigma)$

(P_3) $(\exists \sigma\ \exists \mu_1', \mu_1 \in \mathcal{R}(\mathcal{N}, \mu)\colon\ \mu_1 \xrightarrow{\sigma} \mu_1',\ \mu_1' \geq \mu_1$ and all transitions of T_x are in $\sigma)$

Theorem. *Let $\mathcal{N} = (P, T, F, W)$ be a PN and $T_x \subseteq T$.*

(a) Deadlock can be prevented in $(\mathcal{N}, \mu)$ iff (P_1) is true.

(b) Liveness can be enforced in $(\mathcal{N}, \mu)$ iff (P_2) is true.

(c) T_x-liveness can be enforced in $(\mathcal{N}, \mu)$ iff (P_3) is true.

(d) Let μ_0 be an arbitrary marking for which liveness can be enforced, Ξ_L the least restrictive liveness enforcing supervisor of $(\mathcal{N}, \mu_0)$, and $\mathcal{S}$ the set of all deadlock prevention supervisors of $(\mathcal{N}, \mu_0)$ at least as permissive as Ξ_L. Then all $\Xi \in \mathcal{S}$ enforce liveness in $(\mathcal{N}, \mu_0)$ iff $\forall \mu \in \mathcal{R}(\mathcal{N}, \mu_0)\colon (P_1) \Rightarrow (P_2)$.

(e) Let μ_0 be an arbitrary marking for which T_x-liveness can be enforced, Ξ_L the least restrictive T_x-liveness enforcing supervisor of $(\mathcal{N}, \mu_0)$, and $\mathcal{S}$ the set of all deadlock prevention supervisors of $(\mathcal{N}, \mu_0)$ at least as permissive as Ξ_L. Then all $\Xi \in \mathcal{S}$ enforce T_x-liveness in $(\mathcal{N}, \mu_0)$ iff $\forall \mu \in \mathcal{R}(\mathcal{N}, \mu_0)\colon (P_1) \Rightarrow (P_3)$.

DP & LE Conditions

Theorem. *Let $\mathcal{N} = (P, T, F, W)$ be a PN, D its incidence matrix, $T_x \subseteq T$, $n = |T|$, and:*

$$M = \{x \in \mathbb{Z}_+^n : x \neq 0, Dx \geq 0\}$$
$$N = \{x \in M : \forall i = 1 \ldots n : x(i) \neq 0\}$$
$$P = \{x \in M : \forall t_i \in T_x : x(i) \neq 0\}.$$

(a) The following statements are equivalent:

(i) $M \neq \emptyset$ *and* $M = N$

(ii) supervisors which prevent deadlock exist for some initial marking, and for all such initial markings μ_0 *all supervisors preventing deadlock in* $(\mathcal{N}, \mu_0)$ *also enforce liveness in* $(\mathcal{N}, \mu_0)$

(b) The following statements are equivalent:

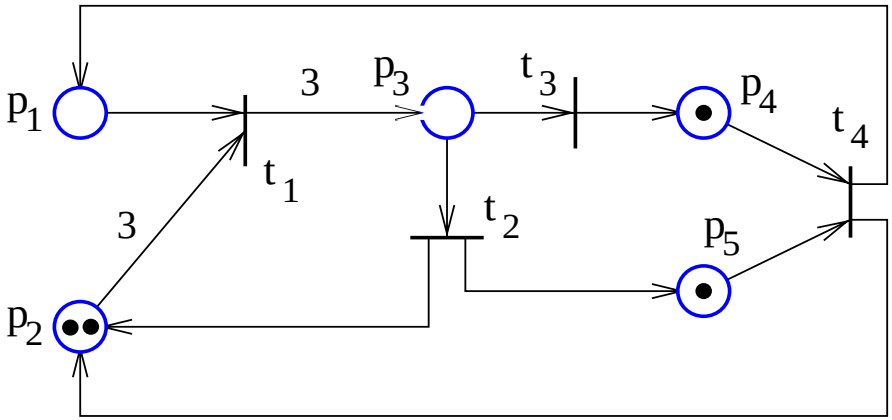
(i) $M \neq \emptyset$ *and* $M = P$

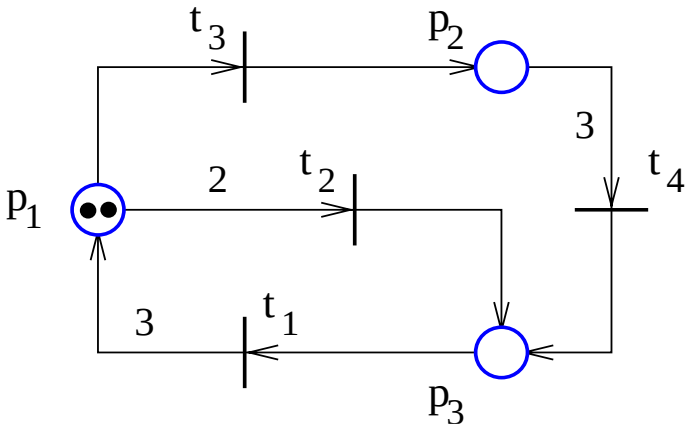
(ii) supervisors which prevent deadlock exist for some initial marking, and for all such initial markings μ_0 *all supervisors preventing deadlock in* $(\mathcal{N}, \mu_0)$ *also enforce* T_x*-liveness in* $(\mathcal{N}, \mu_0)$

(c) The following statements are equivalent:

(i) $N \neq \emptyset$ *and* $N = P$

(ii) supervisors which enforce T_x*-liveness exist for some initial marking, and for all such initial markings* μ_0 *all supervisors enforcing* T_x*-liveness in* $(\mathcal{N}, \mu_0)$ *also enforce liveness in* $(\mathcal{N}, \mu_0)$





$x \geq 0$ and $Dx \geq 0 \Rightarrow$

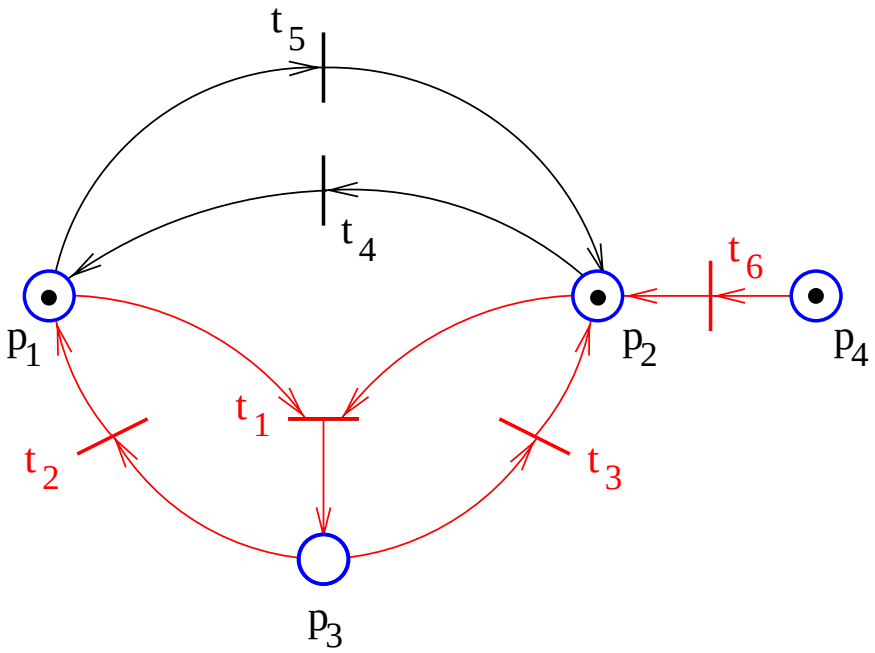
$$x = \alpha_1 \begin{bmatrix} 1 \\ 2 \\ 1 \\ 1 \end{bmatrix} + \alpha_2 \begin{bmatrix} 2 \\ 3 \\ 3 \\ 3 \end{bmatrix}$$

for $\alpha_1, \alpha_2 \geq 0$.

$(P_1) \Rightarrow (P_2)$

DP & LE Conditions

Theorem. *Consider a Petri net $\mathcal{N} = (P, T, F, W)$ which is not repetitive. At least one transition exists such that for any initial marking it cannot fire infinitely often. Let T_D be the set of all such transitions. There are initial markings μ_0 and a supervisor Ξ such that $\forall \mu \in \mathcal{R}(\mathcal{N}, \mu_0, \Xi)$ no transition in $T \setminus T_D$ is dead.*

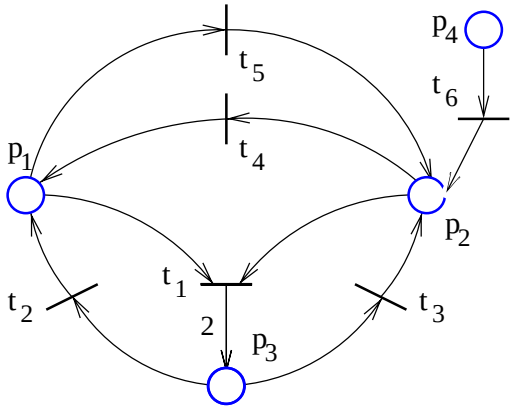


$$T_D = \{t_1, t_2, t_3, t_6\}$$

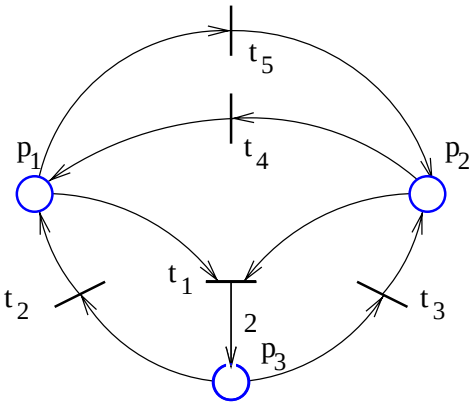
Given $\mathcal{N} = (P, T, F, W)$ *of incidence matrix* D, $\mathcal{N}^A = (P^A, T^A, F^A, W^A)$ *is an* **active subnet** *of* $\mathcal{N}$ *if there is* $x \geq 0$, $x \neq 0$, *such that* $Dx \geq 0$ *and* $T^A = \|x\|$, $P^A = T^A\bullet$, $F^A = F \cap \{(T^A \times P^A) \times (P^A \times T^A)\}$ *and* W^A *is* W *restricted to* F^A.

If all nonnegative vectors y *satisfying* $Dy \geq 0$ *satisfy also* $\|y\| \subseteq \|x\|$, $\mathcal{N}^A$ *is the* **maximal active subnet**. *If no such vector* $y \neq x$ *satisfies* $\|y\| \subset \|x\|$, $\mathcal{N}^A$ *is a* **minimal active subnet**.

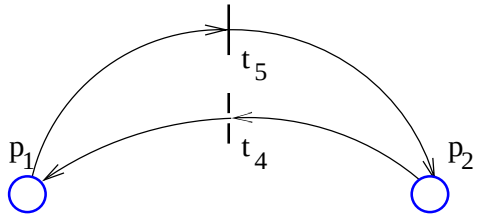
If $T_x \subseteq T^A$ *and there is no other active subnet* $\mathcal{N}_1^A = (P_1^A, T_1^A, F_1^A, W_1^A)$ *such that* $T_x \subseteq T_1^A$ *and* $T_1^A \subset T^A$, *we say that* $\mathcal{N}^A$ *is a* T_x**-minimal active subnet** *of* $\mathcal{N}$.



Petri net



Maximal active subnet

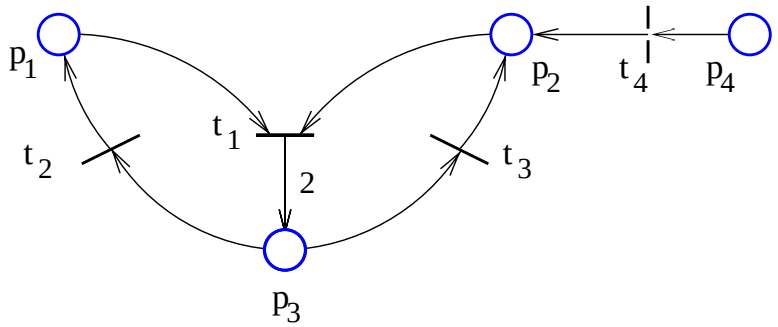


$\{t_4, t_5\}$*-minimal active subnet*

We say that S is an **active siphon** w.r.t. the active subnet $\mathcal{N}^A$ if S is a siphon and $S \cap P^A \neq \emptyset$. We say that S is **minimal** if there is no other active siphon S' w.r.t. $\mathcal{N}^A$ such that $S' \subseteq S$.

The only nonempty active subnet has $T^A = \{t_1, t_2, t_3\}$.

The active siphons are $\{p_1, p_3\}$, $\{p_2, p_3, p_4\}$ and $\{p_1, p_2, p_3, p_4\}$; the first two are also minimal.



Proposition. *A siphon which contains places from an active subnet is an active siphon with respect to that subnet.*

Prior necessary condition for deadlock:

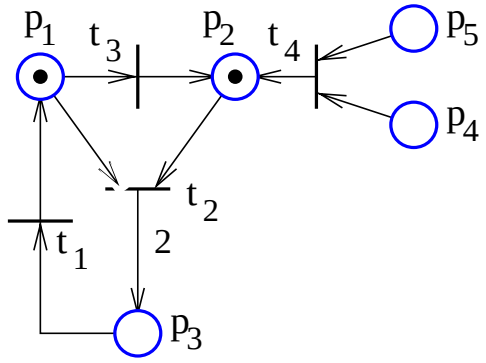
A deadlocked ordinary Petri net has an empty siphon.

New extension based on active siphons:

Proposition. *Let $\mathcal{N}^A$ be an arbitrary active subnet of a PT-ordinary Petri net $\mathcal{N}$. If μ is a deadlock marking of $\mathcal{N}$, then there is an empty minimal active siphon with respect to $\mathcal{N}^A$.*

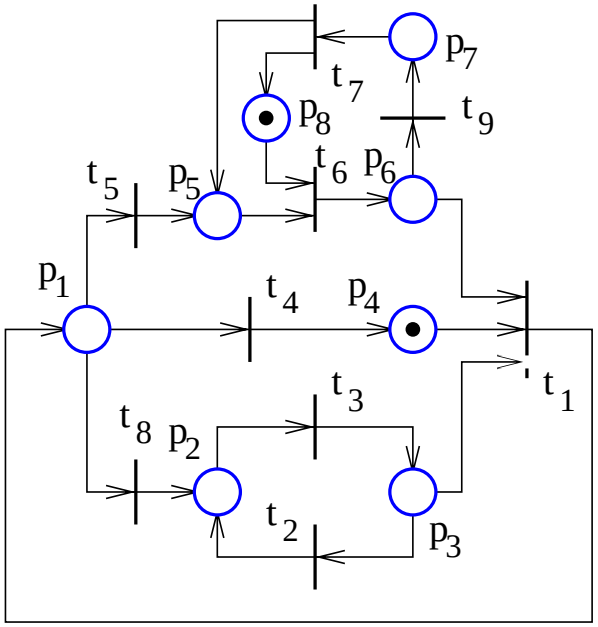
Our result detects that the PN is not in deadlock, even though there are two empty siphons: $\{p_4\}$ and $\{p_5\}$:

The only minimal active siphon is $\{p_1, p_3\}$, which is not empty.

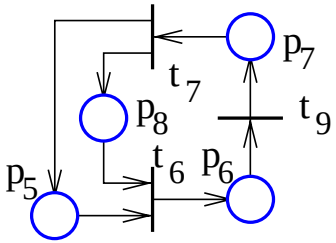


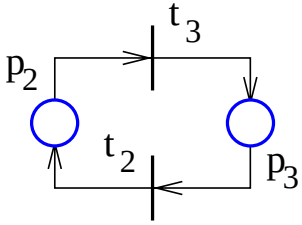
New sufficient condition based on active siphons:

Proposition. *Deadlock is unavoidable for the marking μ if for all minimal active subnets $\mathcal{N}^A$ there is an empty active siphon with respect to $\mathcal{N}^A$.*



PN





minimal active subnets

Active siphons:

W.r.t. the first subnet:
$\{p_6, p_7, p_8\}$ is not empty
$\{p_1, p_5, p_6, p_7\}$ is empty

W.r.t. the second subnet:
$\{p_1, p_2, p_3\}$ is empty

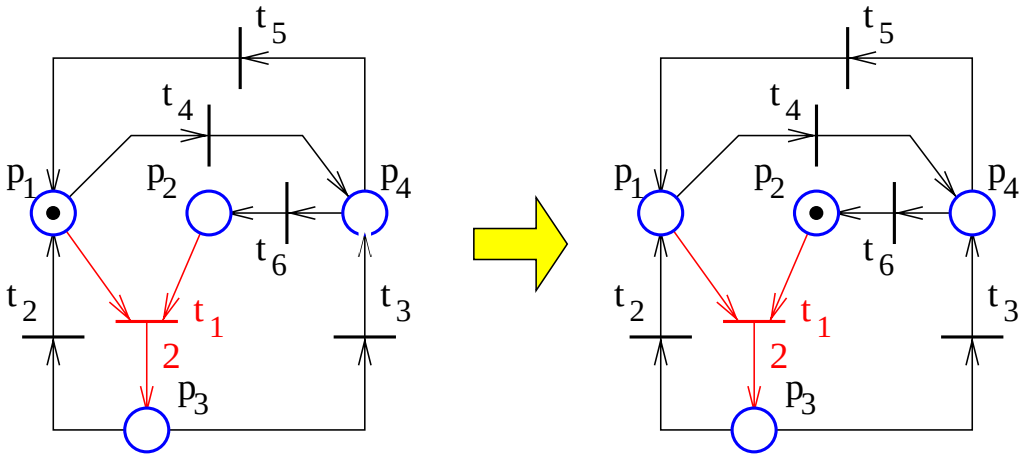
Therefore, deadlock!

Prior result:

If t is dead in $(\mathcal{N}, \mu)$ and $\mathcal{N}$ is ordinary and with asymmetric choice, there is a reachable marking such that a siphon is empty.

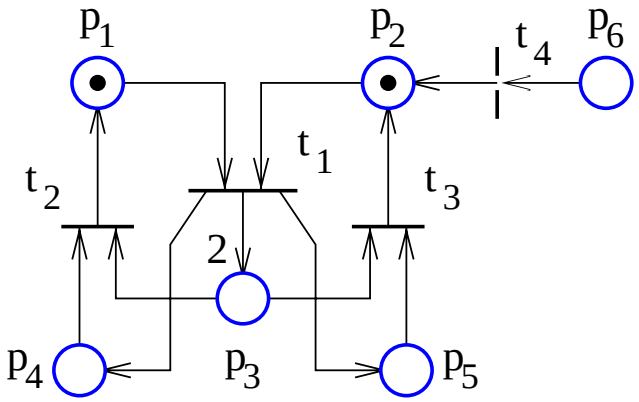
New extension relating t to the empty siphon:

Theorem. *Consider a PT-ordinary asymmetric-choice Petri net $\mathcal{N}$ and a marking μ such that a transition t is dead. Then there is $\mu' \in \mathcal{R}(\mathcal{N}, \mu)$ such that S is an empty siphon for the marking μ' and $t \in S\bullet$.*



t_1 is dead. The siphon $S = \{p_1, p_3, p_4\}$ is emptied by firing t_4, t_6, and $t_1 \in S\bullet$.

Theorem. *Given a PT-ordinary asymmetric-choice net $\mathcal{N}$, let T be a set of transitions and $\mathcal{N}^A$ a T-minimal active subnet which contains the transitions in T. If all the minimal siphons with respect to $\mathcal{N}^A$ are controlled, the PN is T-live (and T^A-live). If the PN is T-live, there is no reachable marking such that for each T-minimal active subnet $\mathcal{N}^A$ there is an empty minimal active siphon with respect to $\mathcal{N}^A$.*



The PN is T-live for $T = \{t_1, t_2, t_3\}$.

Indeed, there is a single T-minimal active subnet $\mathcal{N}^A$ (the one with $T^A = T$.)

All minimal active siphons w.r.t. $\mathcal{N}^A$ are controlled: $\{p_1, p_3\}$, $\{p_1, p_4\}$, $\{p_2, p_3, p_6\}$, and $\{p_2, p_5, p_6\}$

Implications

Even though our previous results may apply to particular classes of PNs (PT-ordinary and/or asymmetric-choice nets), we can still use them for the synthesis of supervisors for arbitrary PNs.

The following problems can be approached:

- Deadlock prevention
- Least restrictive deadlock prevention
- Least restrictive T-liveness enforcement

Input: *The target Petri net* $\mathcal{N}_0$
Output: *Two sets of constraints* (L, b) *and* (L_0, b_0)

For deadlock prevention, take the active siphons w.r.t. the maximal active subnet; for T*-liveness enforcement, take them w.r.t. a* T*-minimal active subnet.*

repeat

1. *Transform the current net to a PT-ordinary Petri net. In addition, in the case of* T*-liveness enforcement, transform the current net to have asymmetric choice.*

2. **For** *every uncontrolled minimal active siphon* S **do**

   If S *needs to be controlled with a* control place **then**

   add control place to PN and inequality in (L, b)*.*

   Else

   add inequality to (L_0, b_0)*.*

until *no uncontrolled minimal siphon is found at 2.*

Restrict the final constraints (L, b) *and* (L_0, b_0) *to the places of the target PN* $\mathcal{N}_0$*.*

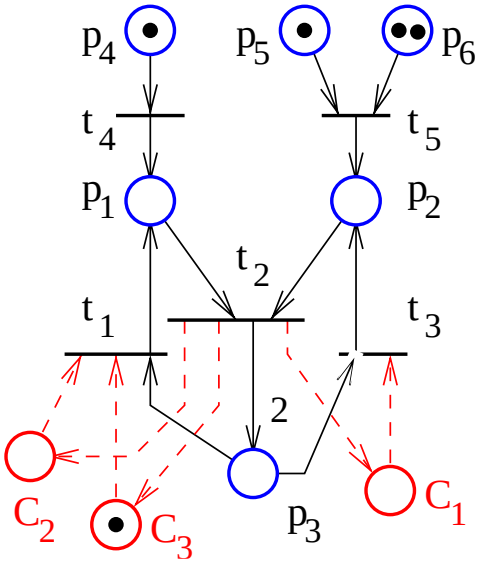
Deadlock is prevented (T-liveness is enforced) for all initial markings μ_0 such that $L\mu_0 \geq b$ and $L_0\mu_0 \geq b_0$, by supervising $\mathcal{N}_0$ with $L\mu \geq b$.

Let Ξ_1, Ξ_2, $\ldots$ Ξ_u be u marking based supervisors.

Assume each supervisor to be defined for initial markings in the sets $\mathcal{M}_1$, $\mathcal{M}_2$, $\ldots$ $\mathcal{M}_u$.

We denote by $\Xi = \bigvee_{i=1}^{u} \Xi_i$ the supervisor defined for initial markings in $\mathcal{M} = \bigcup_{i=1\ldots u} \mathcal{M}_i$ which allows a transition t to fire at the marking μ only if at least one of the supervisors Ξ_i defined at μ allows t to fire.

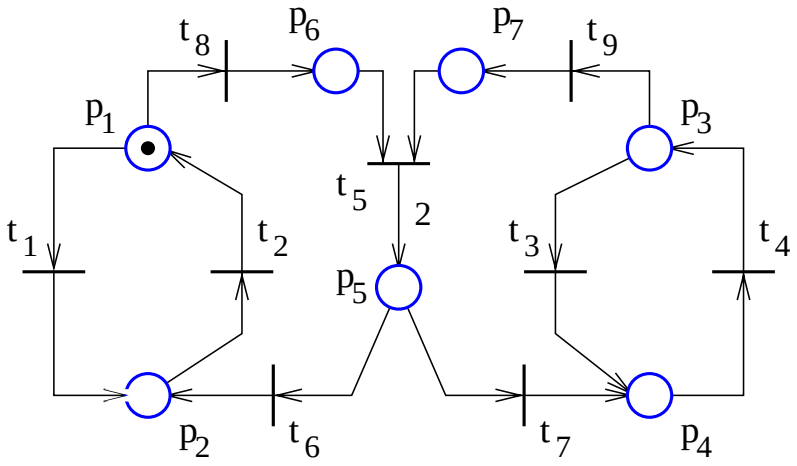
Theorem. *Let $\mathcal{N}_0$ be a PN and $\mathcal{N}_i^A$, for $i = 1 \ldots u$, the minimal active subnets of $\mathcal{N}_0$. Let T_i denote the set of transitions of $\mathcal{N}_i^A$ and let Ξ_i, for $i = 1 \ldots u$, be deadlock prevention supervisors. Assume that each Ξ_i is defined for all initial markings for which T_i-liveness can be enforced and that each Ξ_i is at least as permissive as any T_i-liveness enforcing supervisor. Then $\Xi = \bigvee_{i=1}^{u} \Xi_i$ is the least restrictive deadlock prevention supervisor of $\mathcal{N}_0$.*



The supervisor is defined by:

$$\mu(p_1) + \mu(p_3) + \mu(p_4) \geq 1$$
$$\mu(p_2) + \mu(p_3) + \mu(p_5) \geq 1$$
$$\mu(p_2) + \mu(p_3) + \mu(p_6) \geq 1$$

$$\mu_0(p_1) + \mu_0(p_2) + \mu_0(p_3) + \mu_0(p_4) + \mu_0(p_5) \geq 2$$
$$\mu_0(p_1) + \mu_0(p_2) + \mu_0(p_3) + \mu_0(p_4) + \mu_0(p_6) \geq 2$$



The supervisor is $\Xi = \Xi_1 \vee \Xi_2 \vee \Xi_3$ where:

Ξ_1 is defined by: $(T_1^A = \{t_1, t_2\})$

$$\mu_1 + \mu_2 + \mu_5 + \mu_6 \geq 1$$

$$\mu_1 + \mu_2 + \mu_3 + \mu_4 + \mu_5 + \mu_7 \geq 1$$

Ξ_2 is defined by: $(T_2^A = \{t_3, t_4\})$

$$\mu_3 + \mu_4 + \mu_5 + \mu_7 \geq 1$$

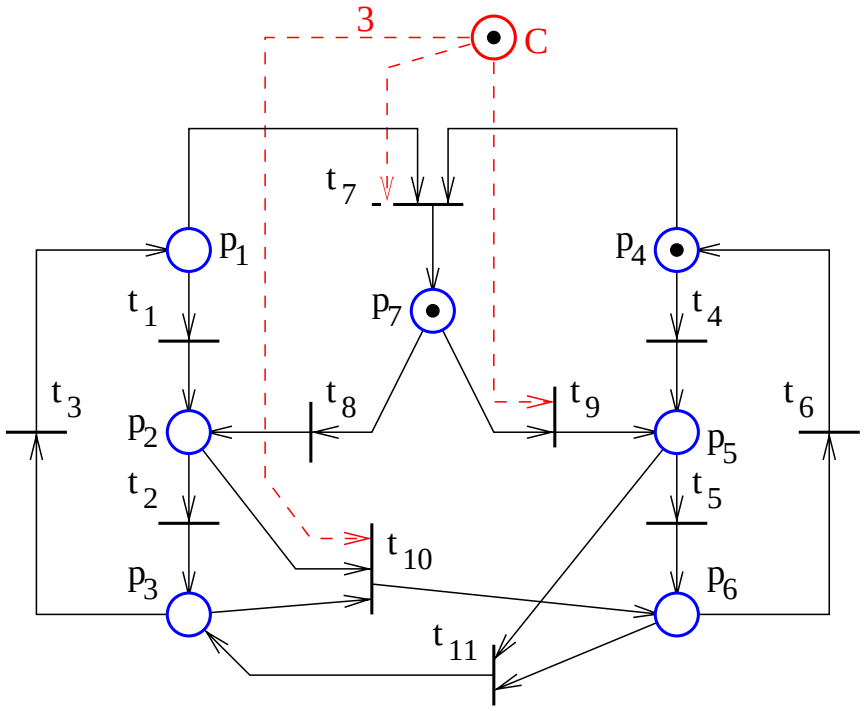
$$\mu_1 + \mu_2 + \mu_3 + \mu_4 + \mu_5 + \mu_6 \geq 1$$

Ξ_3 is defined by: $(T_3^A = \{t_2, t_4, t_5, \ldots t_9\})$

$$\mu_1 + \mu_2 + \mu_5 + \mu_6 \geq 1$$

$$\mu_3 + \mu_4 + \mu_5 + \mu_7 \geq 1$$

$$\sum_{i=1\ldots7} \mu_{0,i} \geq 2$$



The supervisor is defined by

$$2\mu_1 + 2\mu_2 + 2\mu_3 + \mu_4 + \mu_5 + \mu_6 + 2\mu_7 \geq 2$$

Conclusions

The relation between deadlock prevention and liveness enforcement has been characterized.

A class of subnets and siphons has been defined. This has allowed extending existing results to nonrepetitive PNs. Specifically we have presented:

- Necessary and sufficient conditions for deadlock in PT-ordinary PNs
- Necessary and sufficient conditions for T-liveness in PT-ordinary asymmetric-choice PNs.

An extension of the Commoner's Theorem has also been presented.

The presented theoretical results can be used to supervise arbitrary PNs for

- deadlock prevention and least restrictive deadlock prevention
- T-liveness enforcement and least restrictive T-liveness enforcement