A Petri net structure based deadlock prevention solution for sequential resource allocation systems

Fernando Tricas García, F.García–Vallés, J.M. Colom, J. Ezpeleta

ftricas@unizar.es – `http://www.cps.unizar.es/~ftricas/`

Departamento de Informática e Ingeniería de Sistemas

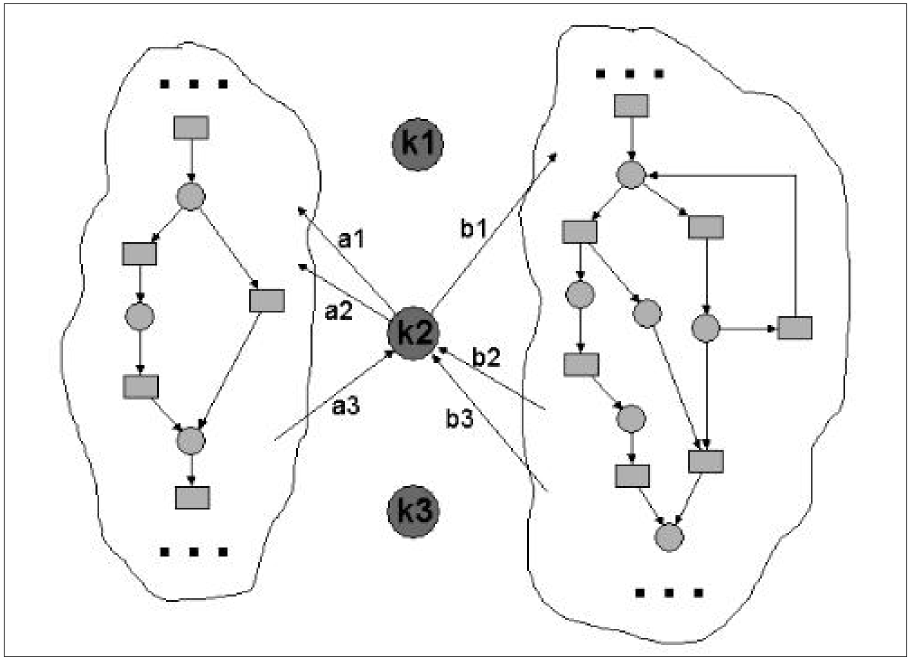
Universidad de Zaragoza

Outline

- Framework
- Deadlock prevention in S^4PR
- Conclusions

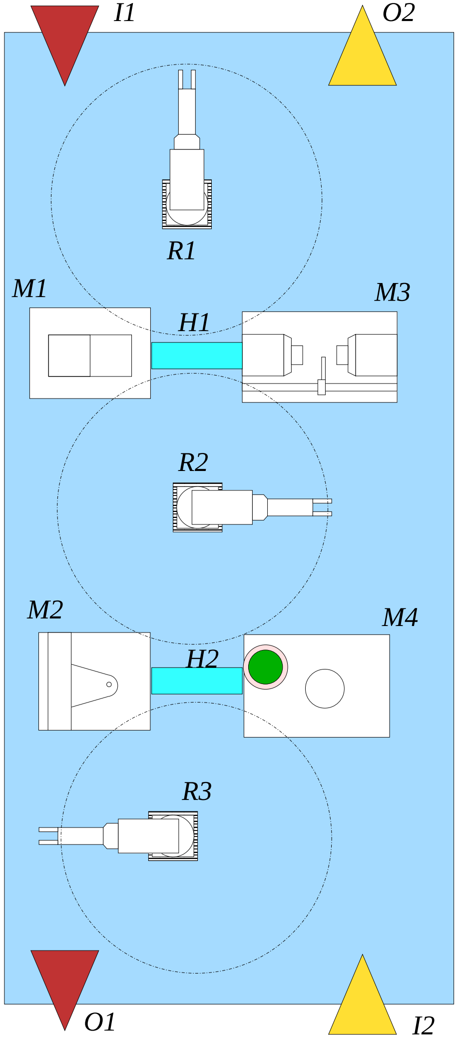
Framework

- Resource Allocation Systems (RAS)
  - A set of processes
  - A set of (reusable) resources
  - They have a concurrent nature

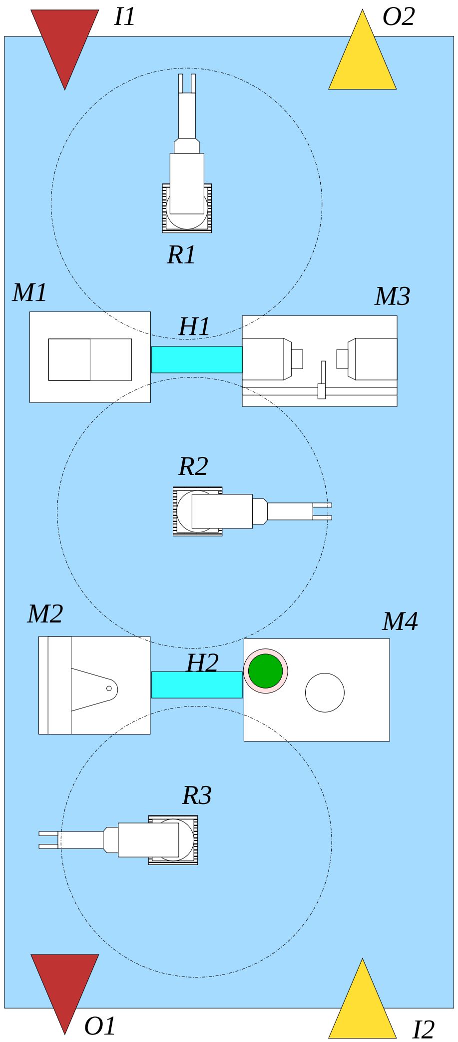


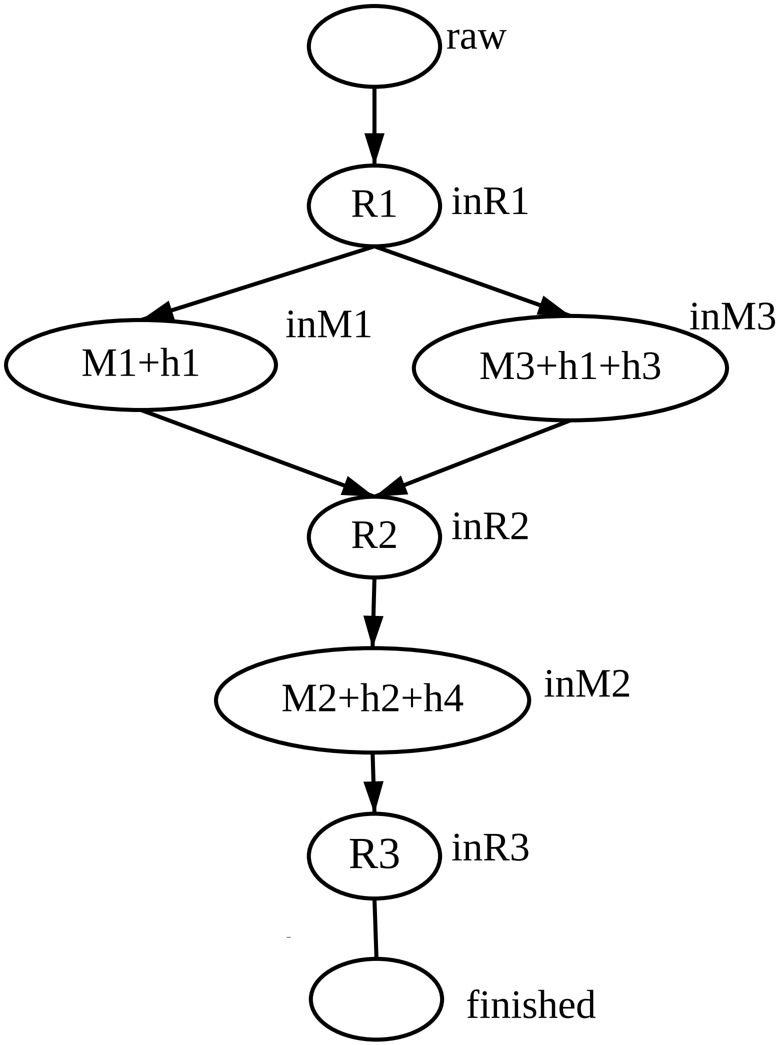
Objective: to control the system so that no deadlock can occur

An example

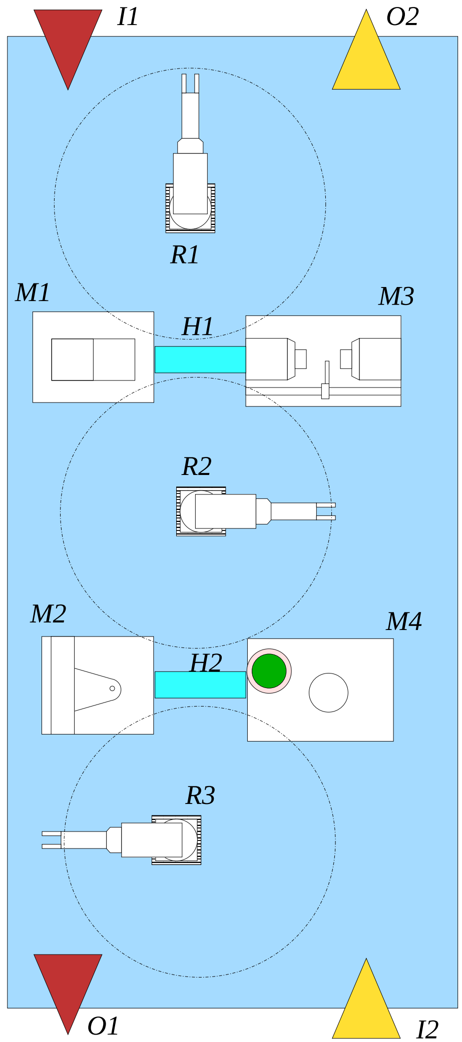


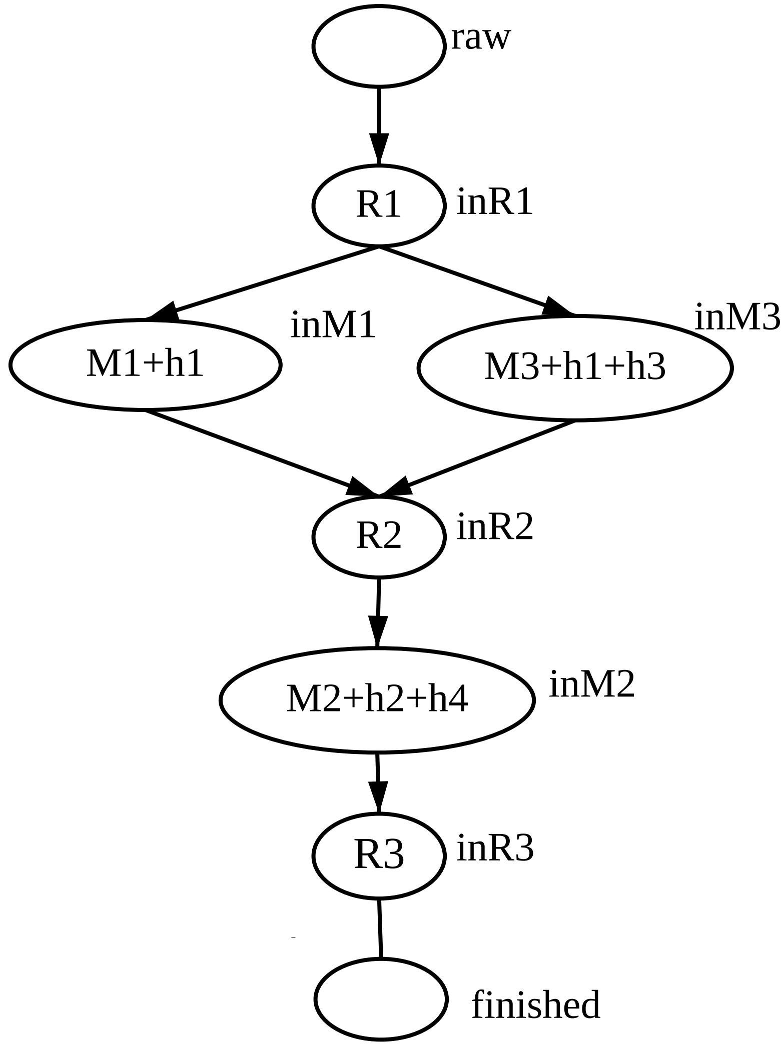
An example

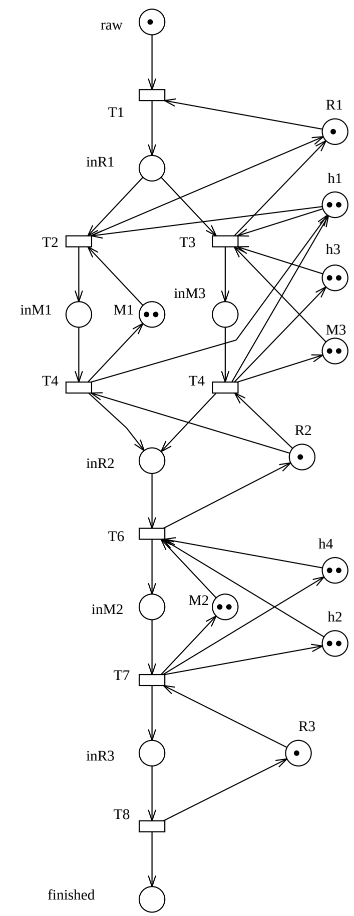

I1
O2
R1
M1
M3
H1
R2
M2
M4
H2
R3
O1
I2


raw
R1
inR1
M1+h1
inM1
M3+h1+h3
inM3
R2
inR2
M2+h2+h4
inM2
R3
inR3
finished

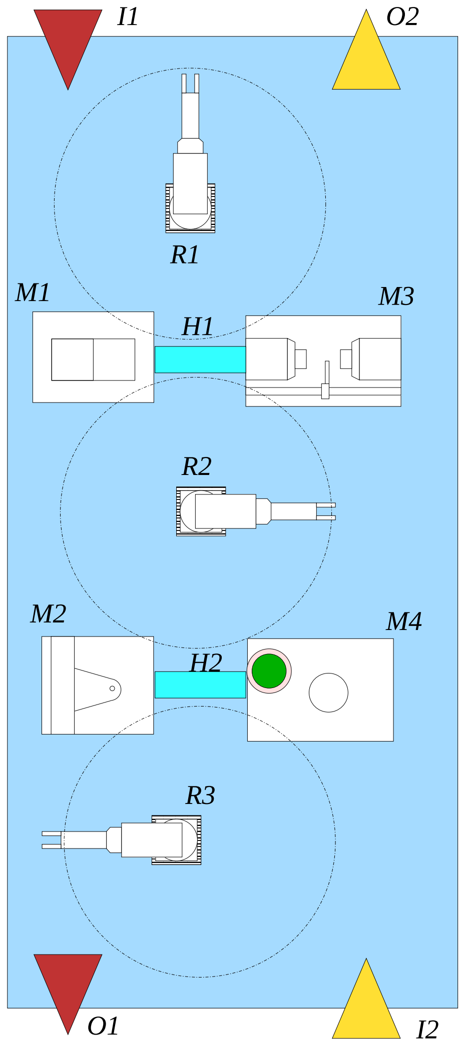
An example

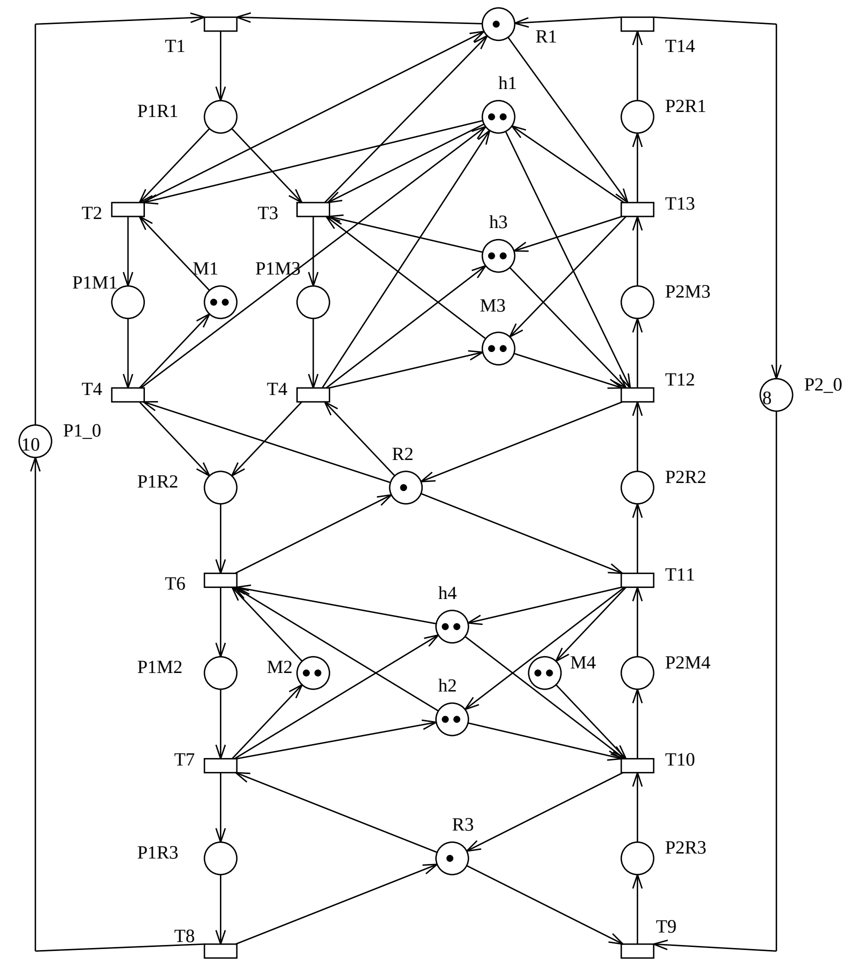

I1
O2
R1
M1
M3
H1
R2
M2
M4
H2
R3
O1
I2


raw
R1
inR1
M1+h1
inM1
M3+h1+h3
inM3
R2
inR2
M2+h2+h4
inM2
R3
inR3
finished


raw
T1
R1
inR1
h1
T2
T3
h3
inM1
M1
inM3
M3
T4
T4
R2
inR2
T6
h4
inM2
M2
h2
T7
R3
inR3
T8
finished

An example


I1
O2
R1
M1
M3
H1
R2
M2
M4
H2
R3
O1
I2


T1
R1
T14
h1
P1R1
P2R1
T2
T3
T13
h3
M1
P1M3
P1M1
P2M3
M3
T4
T4
T12
P2_0
8
P1_0
10
R2
P1R2
P2R2
T6
T11
h4
P1M2
M2
M4
P2M4
h2
T7
T10
R3
P1R3
P2R3
T8
T9

S4PR nets: a general class of S–RAS

Compositional definition

RAS features	PN model features
• Processes	
◦ Sequential process nature ◦ On–line routing decisions ◦ No internal cycles	• Process as a strongly connected state machine whose cycles contain the idle state.
• Resources	
◦ Conservative use of resources ◦ Multiple copies of each resource ◦ Multiple types of resources ◦ Free acquiring/releasing	• Resources defined as SIP • Related weighted arcs

Features of the model

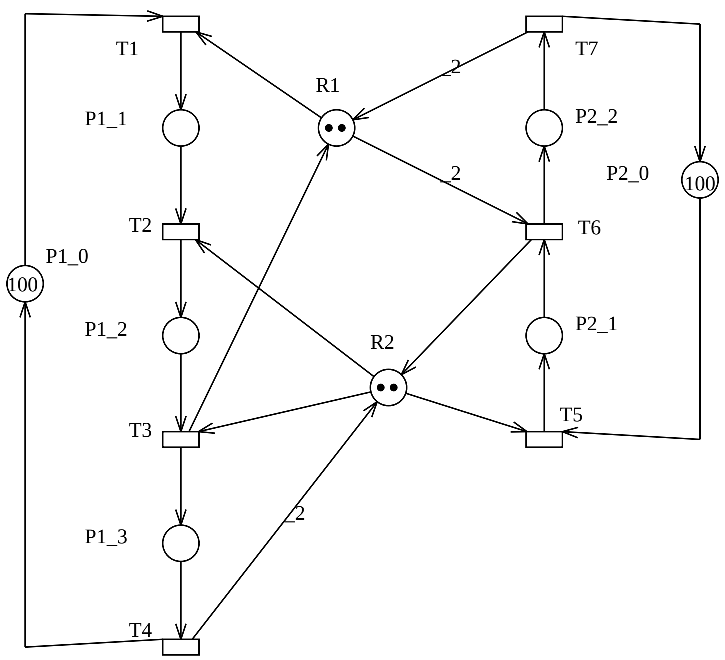
- Clear mapping between model structure and system features
  - Minimal T–Semiflows $\rightarrow$ production sequences
  - Resource related Minimal P–Semiflows $\rightarrow$ Resource reusability
  - State places related minimal P–Semiflows $\rightarrow$ State of parts in the system

Liveness analysis

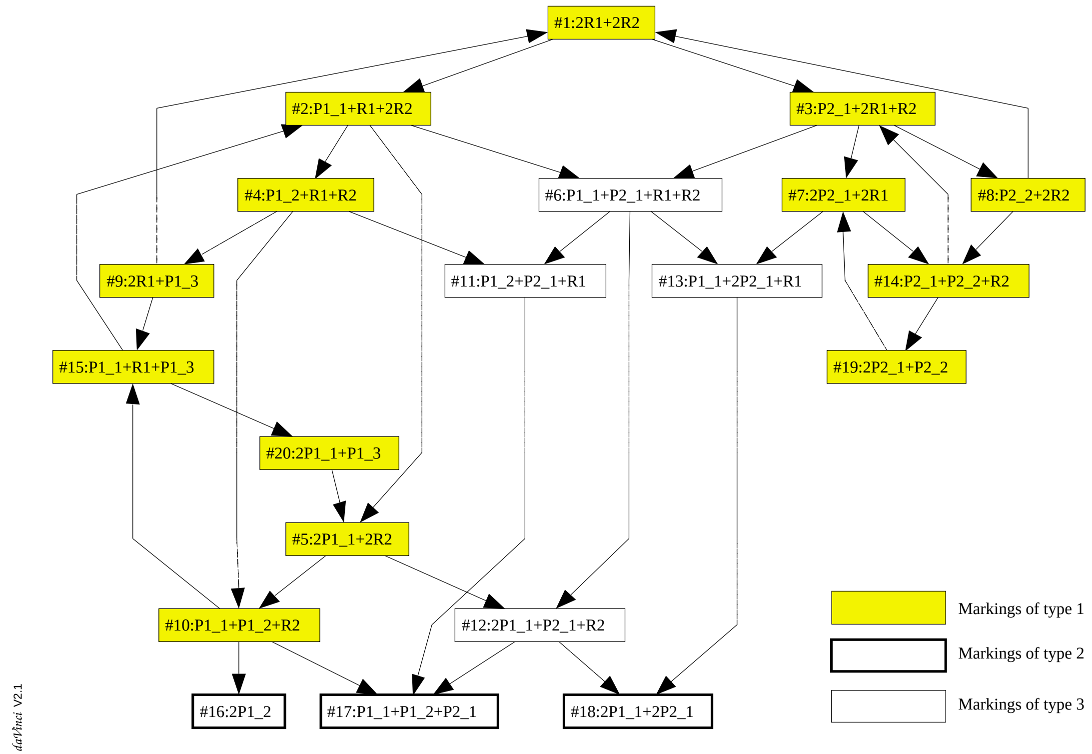
We provide a Liveness analysis

- Characterization of the problem
  - circular waits involving resources
- Reformulation of this characterization in terms of siphons
  - for deadlock prevention

An example



T1
T7
R1
2
P1_1
P2_2
2
P2_0
100
T2
T6
P1_0
100
P1_2
P2_1
R2
T5
T3
2
P1_3
T4

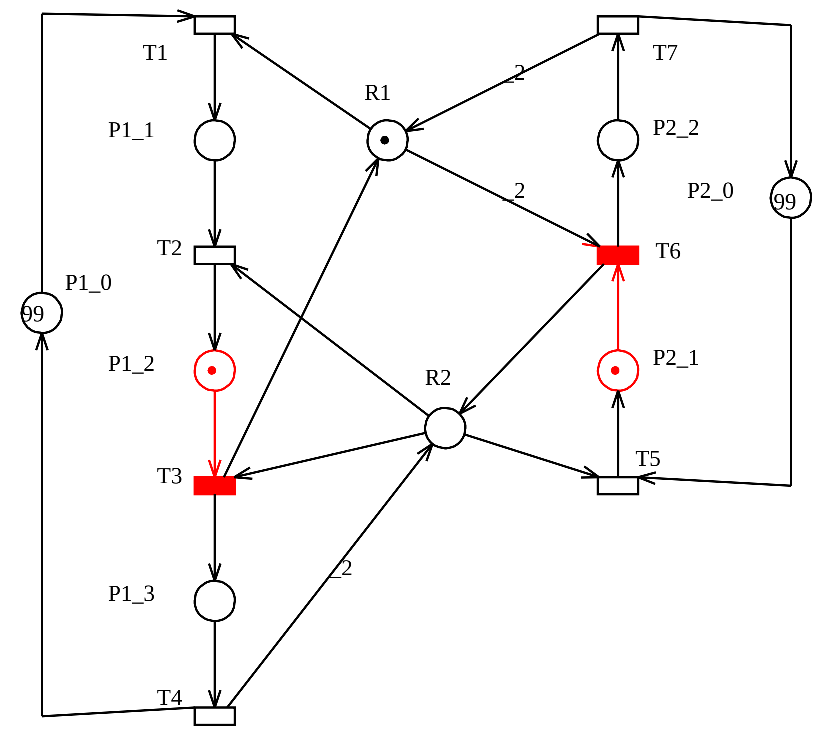


#1:2R1+2R2
#2:P1_1+R1+2R2
#3:P2_1+2R1+R2
#4:P1_2+R1+R2
#6:P1_1+P2_1+R1+R2
#7:2P2_1+2R1
#8:P2_2+2R2
#9:2R1+P1_3
#11:P1_2+P2_1+R1
#13:P1_1+2P2_1+R1
#14:P2_1+P2_2+R2
#15:P1_1+R1+P1_3
#19:2P2_1+P2_2
#20:2P1_1+P1_3
#5:2P1_1+2R2
#10:P1_1+P1_2+R2
#12:2P1_1+P2_1+R2
#16:2P1_2
#17:P1_1+P1_2+P2_1
#18:2P1_1+2P2_1
Markings of type 1
Markings of type 2
Markings of type 3
daVinci V2.1

Liveness: circular waits

Theorem
Let $\langle \mathcal{N}, \mathbf{m_0} \rangle$, $\mathcal{N}$= $\langle P_0 \cup P_S \cup P_R, T, \mathbf{C} \rangle$, be a marked S^4PR. The net is non–live if and only if there exists a marking $\mathbf{m} \in \mathrm{RS}(\mathcal{N}, \mathbf{m_0})$ such that:

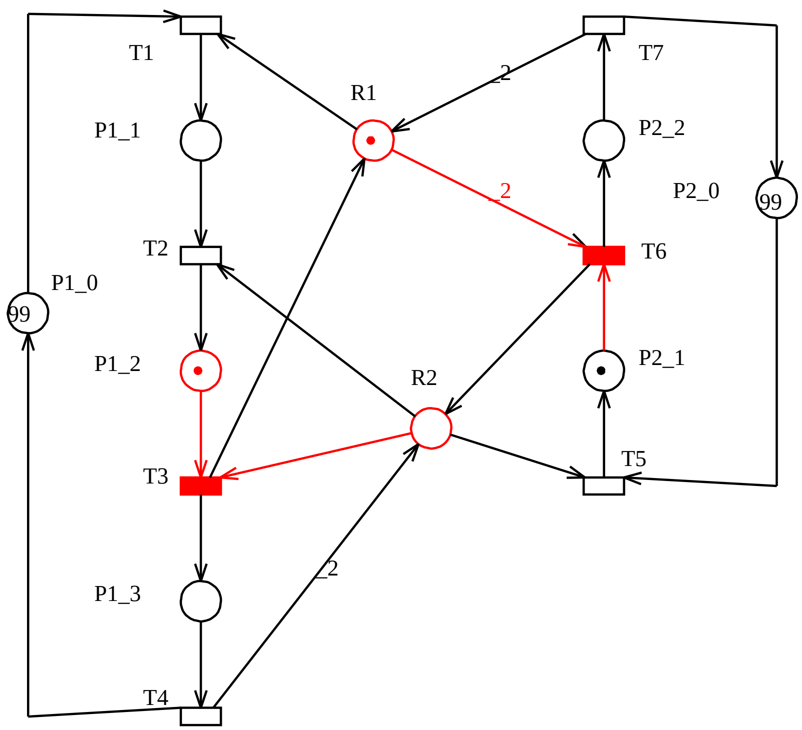
- the set of $\mathbf{m}$–process–enabled transitions is non–empty
- each one of these transitions is $\mathbf{m}$–resource–disabled.



Liveness: circular waits

Theorem
Let $\langle\mathcal{N},\mathbf{m_0}\rangle$, $\mathcal{N}= \langle P_0 \cup P_S \cup P_R, T, \mathbf{C}\rangle$, be a marked S^4PR. The net is non–live if and only if there exists a marking $\mathbf{m} \in \mathrm{RS}(\mathcal{N},\mathbf{m_0})$ such that:

- the set of $\mathbf{m}$–process–enabled transitions is non–empty
- each one of these transitions is $\mathbf{m}$–resource–disabled.

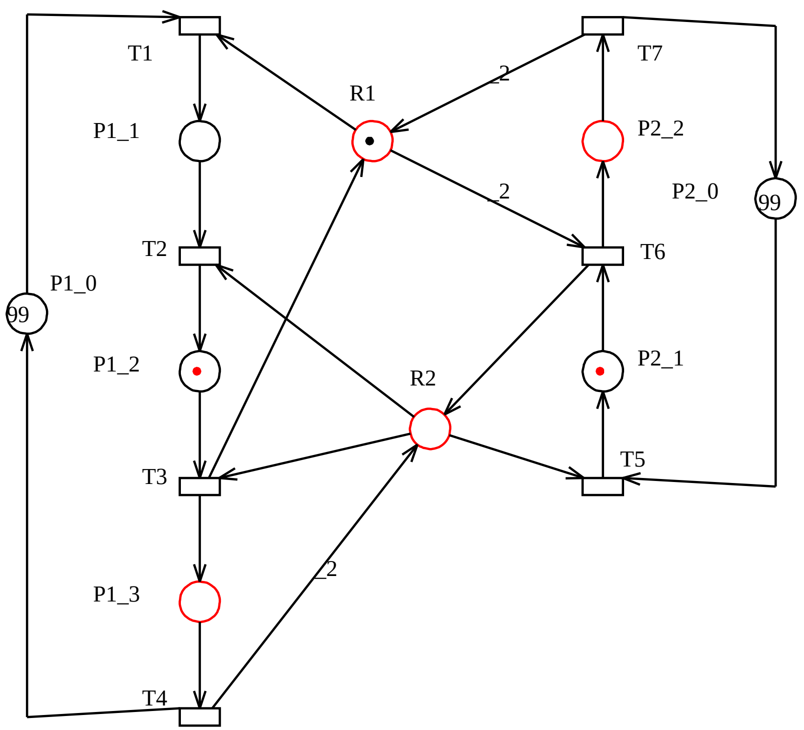


Liveness: siphons

Theorem

Let $\langle \mathcal{N}, \mathbf{m_0} \rangle$, $\mathcal{N}$= $\langle P_0 \cup P_S \cup P_R, T, \mathbf{C} \rangle$, be a marked S^4PR. The net is non–live if, and only if, there exists a marking $\mathbf{m} \in \mathrm{RS}(\mathcal{N}, \mathbf{m_0})$, and a siphon D such that $\mathbf{m}[P_S] > 0$ and the firing of each $\mathbf{m}$–process–enabled transition is prevented by a set of resource places belonging to D.

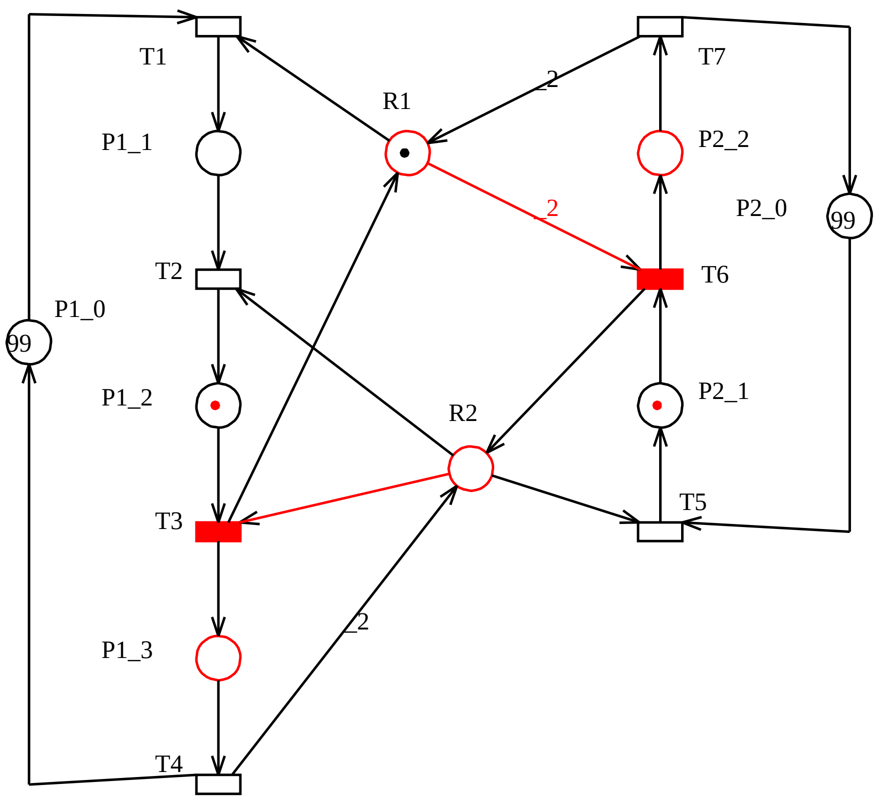
1. $D_R = D \cap P_R = \{r \in P_R \mid \exists t \in r^\bullet$ such that $\mathbf{m}[r] < \mathbf{Pre}[r, t]$ and $\mathbf{m}[{}^\bullet t \cap P_S] > 0\} \neq \emptyset$;
2. $D_S = D \cap P_S = \{p \in \mathcal{H}_{D_R} \mid \mathbf{m}[p] = 0\} \neq \emptyset$;



Liveness: siphons (improved)

Theorem
Let $\langle \mathcal{N}, \mathbf{m_0} \rangle$, $\mathcal{N} = \langle P_0 \cup P_S \cup P_R, T, \mathbf{C} \rangle$, be a marked S^4PR. The net is non–live if, and only if, there exists a siphon D, and a marking $\mathbf{m}_D \in \mathrm{RS}(\mathcal{N}, \mathbf{m_0})$, such that:

1. $\mathbf{m}_D[P_S] > 0$.
2. $\mathbf{m}_D[P_S \setminus \mathcal{T}h_D] = 0$.
3. $\forall p \in \mathcal{T}h_{D_R}$ such that $\mathbf{m}_D[p] > 0$, the firing of each $t \in p^\bullet$ is prevented by a set of resource places belonging to D.



Using these liveness characterizations

Deadlock problems $\leftrightarrow$ bad siphons + bad markings

Objective: Preventing bad states

- Without computing the reachability set

Solution: potential reachability set approximation

- Advantage: linear description
- Drawback: spurious solutions
  - No bad makings in PRS $\rightarrow$ No bad markings in RS

How to compute a bad siphon

If $\mathbf{m}$ is a bad marking, the following set of inequalities has a solution

$$\left\{\begin{array}{l}
\forall p \in P \setminus P_0, \forall t \in {}^\bullet p, v_p \geq \sum_{q \in {}^\bullet t} v_q - |{}^\bullet t| + 1 \\
\sum_{p \in P \setminus P_0} v_p < |P \setminus P_0| \\
\mathbf{m}[P_S] > 0 \\
\quad \forall t \in T \setminus P_0{}^\bullet, \quad \text{being } \{p\} = {}^\bullet t \cap P_S, \\
\qquad \mathbf{m}[p] \geq e_t \\
\qquad e_t \geq \mathbf{m}[p]/\mathbf{sb}[p] \\
\forall r \in P_R, \\
\quad \forall t \in r^\bullet \setminus P_0{}^\bullet, \quad \mathbf{m}[r]/\mathbf{Pre}[r,t] + v_r \geq e_{rt} \\
\qquad e_{rt} \geq (\mathbf{m}[r] - \mathbf{Pre}[r,t] + 1)/(\mathbf{m_0}[r] - \mathbf{Pre}[r,t] + 1) \\
\qquad e_{rt} \geq v_r \\
\quad \forall t \in T \setminus P_0{}^\bullet, \sum_{r \in {}^\bullet t \cap P_R} e_{rt} < |{}^\bullet t \cap P_R| + 1 - e_t \\
\quad \forall p \in P \setminus P_0, v_p \in \{0,1\}, \forall t \in T \setminus P_0{}^\bullet, e_t \in \{0,1\}, \forall r \in P_R, \forall t \in r^\bullet \setminus P_0{}^\bullet, e_{rt} \in \{0,1\}
\end{array}\right. \quad (0)$$

$[Sil85]: Siphon$ $Property$

e_t $Processes$ $enabled/$ $disabled$

e_{rt} $Resources$ $enabled/$ $disabled$

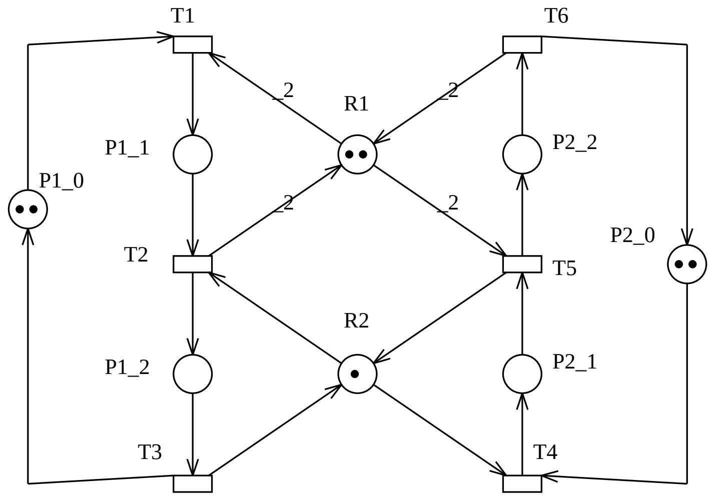
How to compute a bad siphon

Let $\langle \mathcal{N}, \mathbf{m_0} \rangle$, $\mathcal{N}$= $\langle P_0 \cup P_S \cup P_R, T, \mathbf{C} \rangle$, be a marked S^4PR. If net is non–live, there exists a marking $\mathbf{m} \in \mathrm{PRS}(\mathcal{N}, \mathbf{m_0})$, with $\mathbf{m}[P_S] > 0$, and a siphon D such that the following system of inequalities has, at least, one solution with $D = \{p \in P_S \cup P_R \mid v_p = 0\}$:

$$(0) \qquad \begin{cases} \text{maximize} \sum_{p \in P \setminus P_0} v_p \\ \text{such that} \\ \mathbf{m} = \mathbf{m_0} + \mathbf{C} \cdot \overline{\boldsymbol{\sigma}} \\ \mathbf{m} \geq 0, \ \overline{\boldsymbol{\sigma}} \in \mathbb{Z}_+^{|T|} \\ System \text{ (Previous Slide)} \end{cases}$$

We need more

Problems happen when ...
Too many resources are used at the same time



Or, alternatively, too many active processes

Computing representative markings

m_D^{max} = maximize $\sum_{r \in D_R} \mathbf{m}[r]$ s.t.

$$
\left\{
\begin{array}{ll}
\quad \mathbf{m} = \mathbf{m_0} + \mathbf{C} \cdot \overline{\boldsymbol{\sigma}} & \\
\quad \mathbf{m} \geq 0,\ \overline{\boldsymbol{\sigma}} \in \mathbb{Z}_+^{|T|} & \\
\quad \mathbf{m}[P_S \setminus \mathcal{T}h_D] = 0 & \\
\mathbf{m}[P_S] > 0 & \\
\forall t \in T \setminus P_0{}^\bullet, & \text{being } \{p\} = {}^\bullet t \cap P_S, \\
 & \mathbf{m}[p] \geq e_t \\
 & e_t \geq \mathbf{m}[p]/\mathbf{sb}[p] \\
\forall r \in D_R, & \\
\forall t \in r^\bullet \setminus P_0{}^\bullet, & \mathbf{m}[r]/\mathbf{Pre}[r,t] \geq e_{rt} \\
 & e_{rt} \geq (\mathbf{m}[r] - \mathbf{Pre}[r,t] + 1)/(\mathbf{m_0}[r] - \mathbf{Pre}[r,t] + 1) \\
\forall r \in P_R \setminus D_R, & \forall t \in r^\bullet \setminus P_0{}^\bullet, e_{rt} = 1 \\
\forall t \in T \setminus P_0{}^\bullet, & \sum_{r \in {}^\bullet t \cap P_R} e_{rt} < |{}^\bullet t \cap P_R| + 1 - e_t \\
\forall t \in T \setminus P_0{}^\bullet, & e_t \in \{0,1\} \\
\forall r \in P_R, & \forall t \in r^\bullet \setminus P_0{}^\bullet, e_{rt} \in \{0,1\}
\end{array}
\right.
$$

Control place

Let $\langle \mathcal{N}, \mathbf{m_0} \rangle$, $\mathcal{N}= \langle P_0 \cup P_S \cup P_R, T, \mathbf{C} \rangle$, be a non–live S^4PR. Let D be a bad siphon, and m_D^{max} as in previous Definition. Then,

- The associated D–resource place, p_D, is defined by means of the addition of the following incidence matrix row and initial marking:

$$\begin{array}{rcl} \mathbf{C^{p_D}}[p_D, T] & = & - \sum_{p \in \mathcal{T}h_D} \mathbf{Y_{D_R}}[p] \cdot \mathbf{C}[p, T] \\ \mathbf{m_0}^{p_D}[p_D] & = & \mathbf{m_0}[D] - (m_D^{max} + 1) \end{array}$$

Computing representative markings

m_D^{min} = minimize $\sum_{p \in \mathcal{T}h_D} \mathbf{m}[p]$ s.t.

$$
\begin{cases}
\quad \mathbf{m} = \mathbf{m_0} + \mathbf{C} \cdot \overline{\boldsymbol{\sigma}} & \\
\quad \mathbf{m} \geq 0,\ \overline{\boldsymbol{\sigma}} \in \mathbb{Z}_+^{|T|} & \\
\quad \mathbf{m}[P_S \setminus \mathcal{T}h_D] = 0 & \\
\mathbf{m}[P_S] > 0 & \\
\forall t \in T \setminus P_0{}^\bullet, & \text{being } \{p\} = {}^\bullet t \cap P_S, \\
 & \mathbf{m}[p] \geq e_t \\
 & e_t \geq \mathbf{m}[p]/\mathbf{sb}[p] \\
\forall r \in D_R, & \\
\forall t \in r^\bullet \setminus P_0{}^\bullet, & \mathbf{m}[r]/\mathbf{Pre}[r,t] \geq e_{rt} \\
 & e_{rt} \geq (\mathbf{m}[r] - \mathbf{Pre}[r,t] + 1)/(\mathbf{m_0}[r] - \mathbf{Pre}[r,t] + 1) \\
\forall r \in P_R \setminus D_R, & \forall t \in r^\bullet \setminus P_0{}^\bullet, e_{rt} = 1 \\
\forall t \in T \setminus P_0{}^\bullet, & \sum_{r \in {}^\bullet t \cap P_R} e_{rt} < |{}^\bullet t \cap P_R| + 1 - e_t \\
\forall t \in T \setminus P_0{}^\bullet, & e_t \in \{0,1\} \\
\forall r \in P_R, & \forall t \in r^\bullet \setminus P_0{}^\bullet, e_{rt} \in \{0,1\}
\end{cases}
$$

Control places

Let $\langle \mathcal{N}, \mathbf{m_0} \rangle$, $\mathcal{N} = \langle P_0 \cup P_S \cup P_R, T, \mathbf{C} \rangle$, be a non–live S^4PR. Let D be a bad siphon, and m_D^{min} as in previous Definition. Then,

- The associated D–process place, p_D, is defined by means of the addition of the following incidence matrix row and initial marking:

$$
\begin{array}{lcll}
\mathbf{C^{p_D}}[p_D, T] & = & - & \sum_{p \in \mathcal{T}h_D} \mathbf{C}[p, T], \\
\mathbf{m_0}^{p_D}[p_D] & = & & m_D^{min} - 1
\end{array}
$$

Which one to use?

- Using D–resource approach usually gives more permissive solutions
  But ...
- Not always possible (sometimes the marking is not acceptable)
  So ...
- First try with resources, and if it fails use processes

So ... how to control?

$\rightarrow$ No more D–deadlocked states

- The control places can be seen as ‘virtual’ resources, which add generalized mutual exclusion properties.
  - The obtained system is a S^4PR
  - It is analyzable in the same terms as the original

Iterative process

An sketch of the algorithm

1. Compute a bad siphon
2. Compute the control place
3. Repeat

Does it terminate?

S4PR: Conclusions

Advantages:

- More general than previous approaches
- At least as permissive as others (more in most cases)
- It does not need siphon enumeration

Drawbacks:

- Sub–optimal
- It does not scale well (modification, reconfiguration)

The End

Thanks!