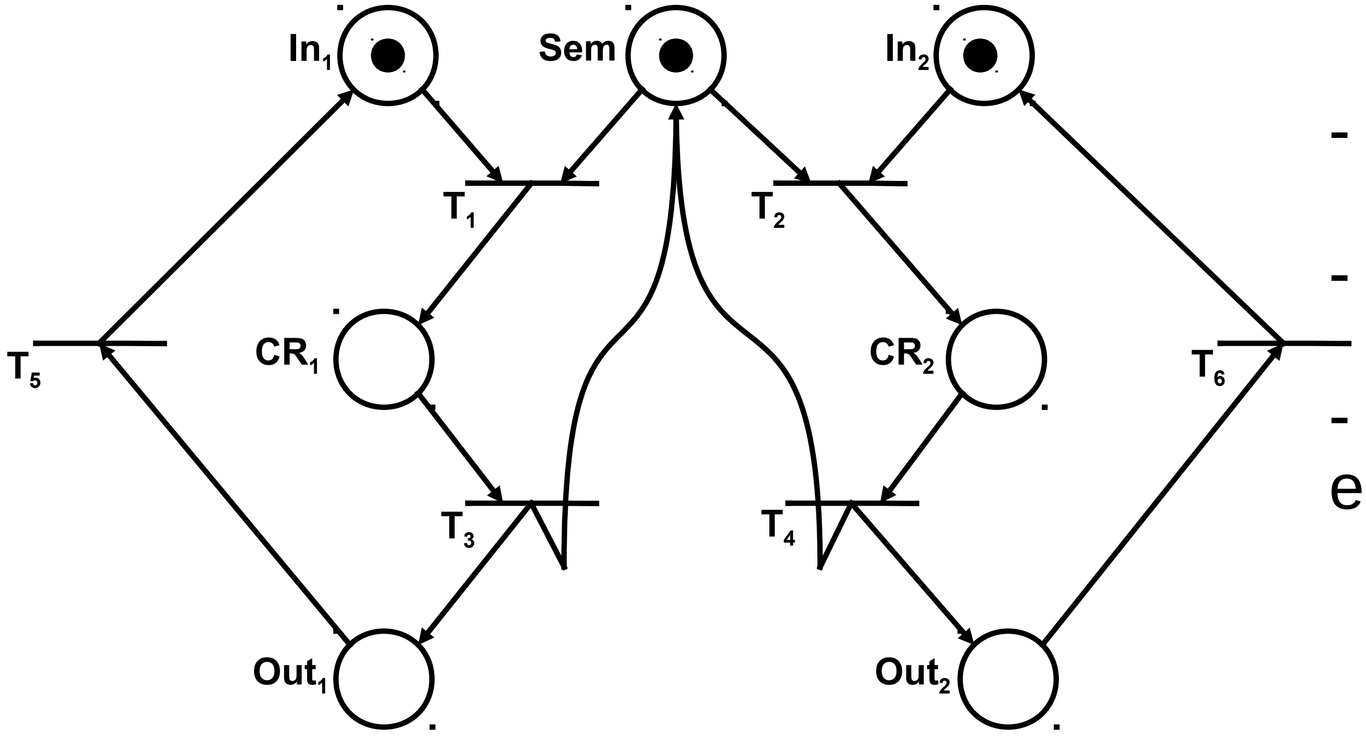
ECE 321 Software Requirements Engineering

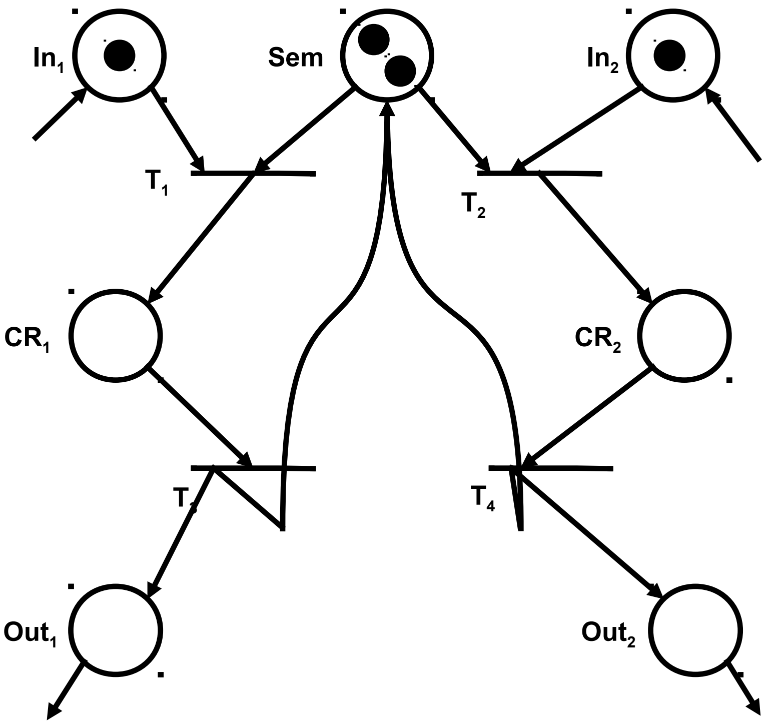
Lecture 13: Dynamic and Static Analysis of Petri Nets

Last week: Petri Nets



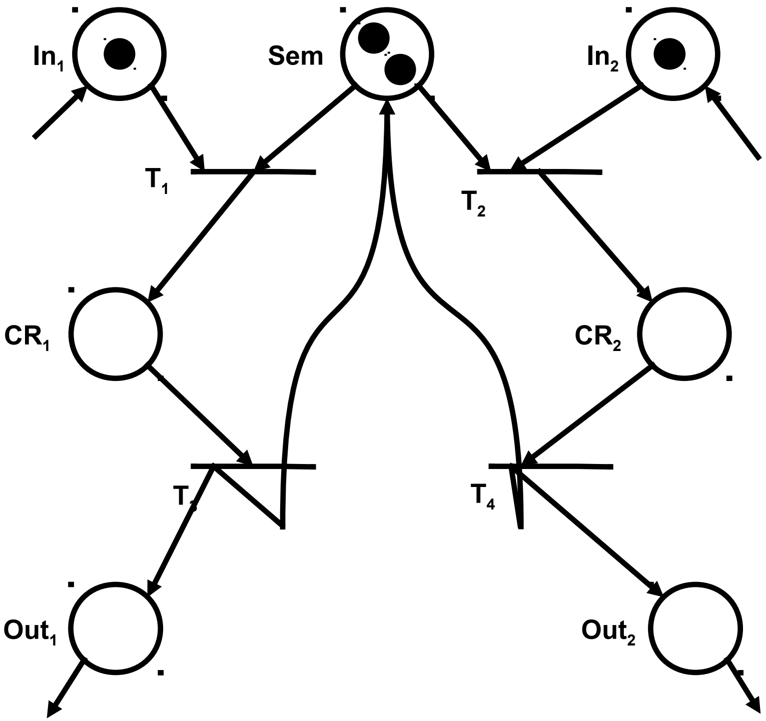
- How many places?
    - 7
- How many transitions?
    - 6
- Which transitions are enabled?
    - T_1, T_2

Last week: Concurrency in Petri Nets

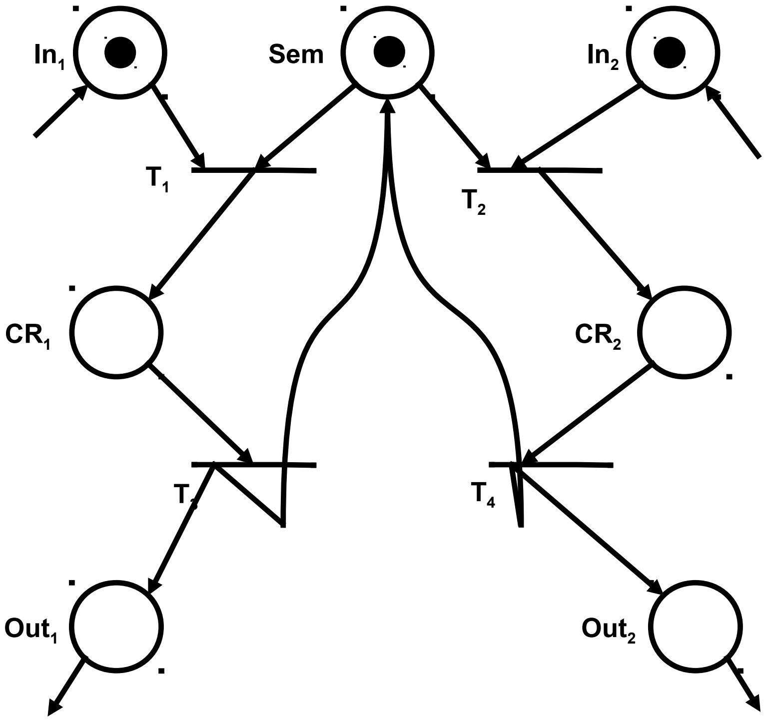


Are T_1 and T_2 concurrent?

Last week: Concurrency in Petri Nets

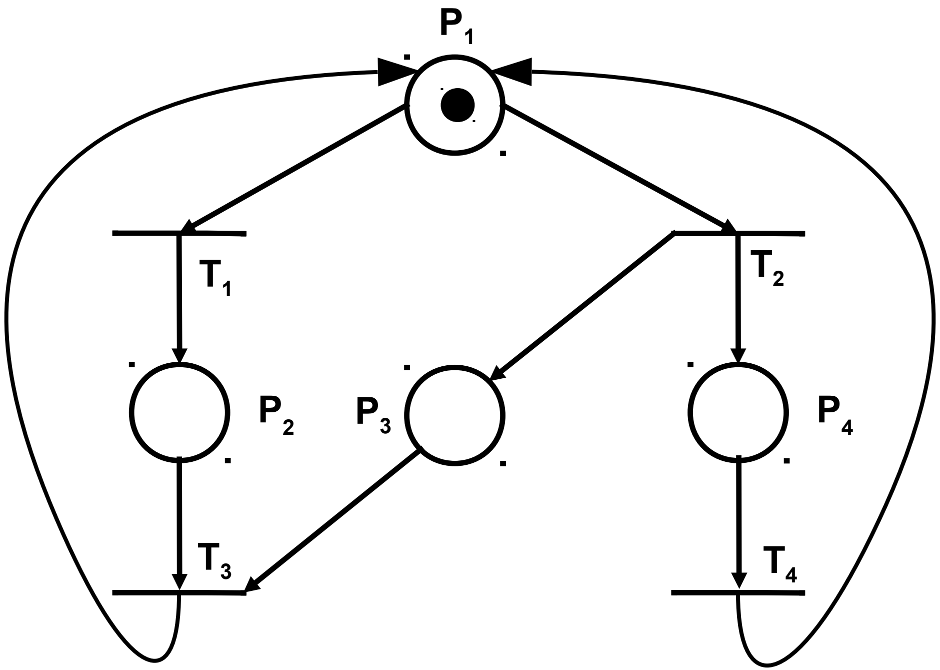


Are T_1 and T_2 concurrent? **YES**



And now? **NO**

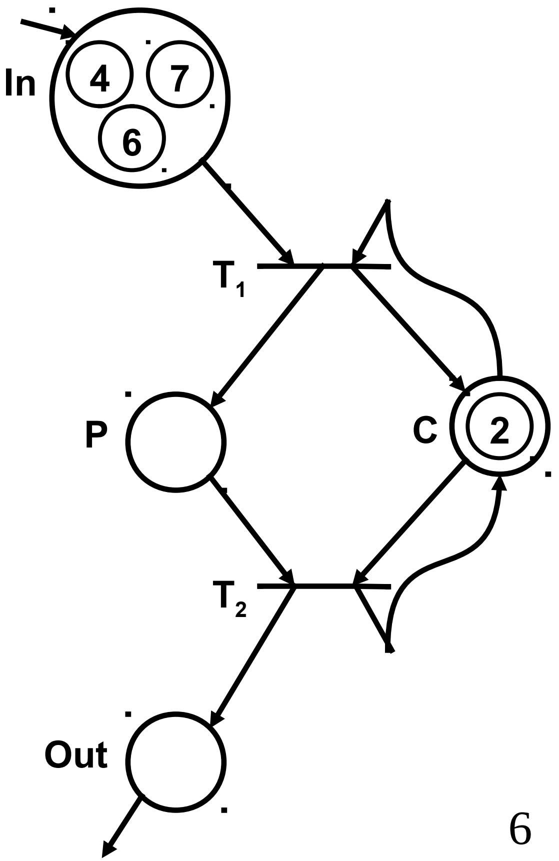
Last week: Will the execution of this model result in deadlock?



Yes:
< T_1 >

Last week: Petri Net extensions: Assigning values to tokens

- In contains 3 tokens with the values 4, 6 and 7
- C contains one token with the value 2



This week: verification of Petri Nets

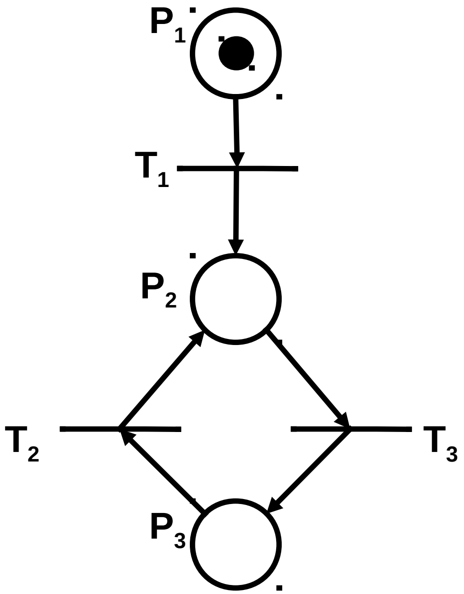
- Verification of properties
  - Behavioural
    - Depend on the initial marking
  - Structural
    - Depend on the structure of the PN (topology)

Which properties do Petri Nets have?

- Behavioural properties
  - Reachability
  - Boundedness
  - Liveness
  - Conservativeness
- Structural properties
  - Structural liveness
  - Controllability
  - Structural boundedness

Behavioural properties: reachability

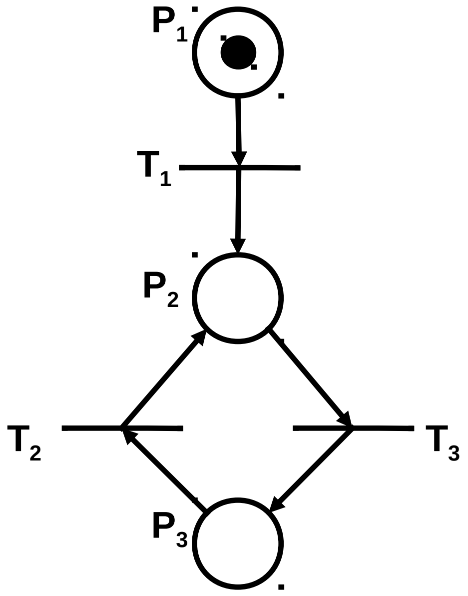
- Marking M is reachable from M_0 if there exists a firing sequence s = < T_1 T_2 T_3 ... > that transforms M_0 to M
- M_0 = (1,0,0)
- Can we reach M = (0,1,0)?
  - s = < T1 >
- And what about M = (1,1,0)?
  - No



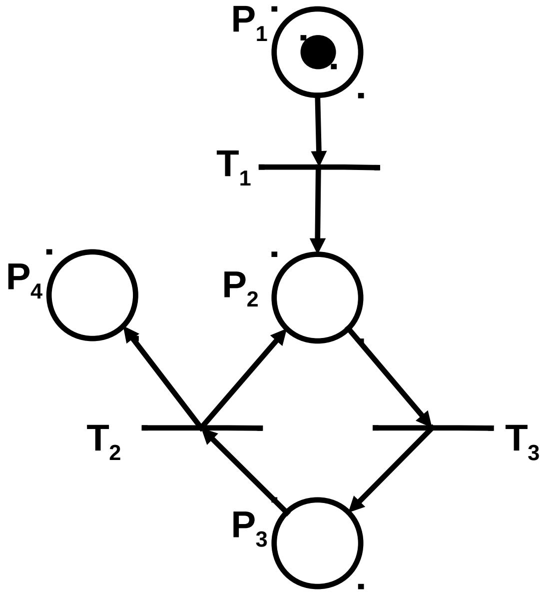
Behavioural properties: Boundedness

- A place is *k*-bounded if the number of tokens in that place does not exceed *k* for any marking reachable from M_0

Behavioural properties: Boundedness 2/2



P_1, P_2 and P_3 are 1-bounded

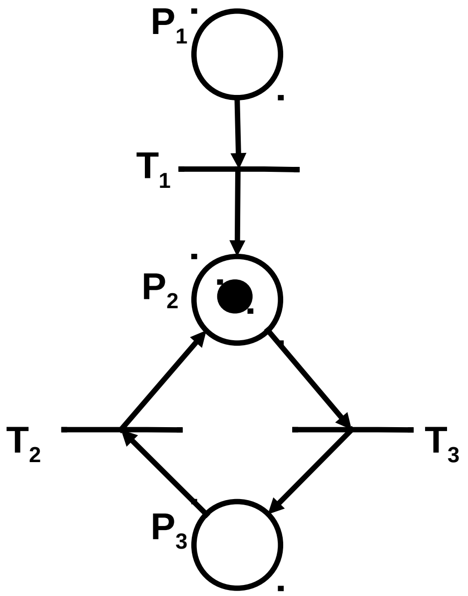


How about now? **P_4 is unbounded**

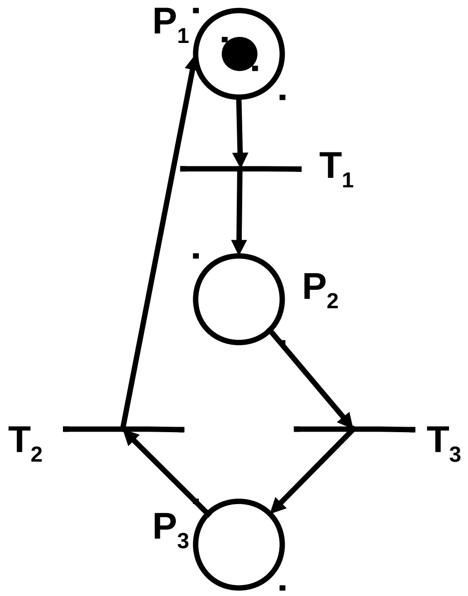
Behavioural properties: Liveness 1/2

- A transition t is live, if there exists a marking M that is reachable from every M_0 from which t is enabled
  - i.e., there is always a firing sequence from M_0 that enables t

Behavioural properties: Liveness 2/2



T_1 is not live; T_2 and T_3 are live

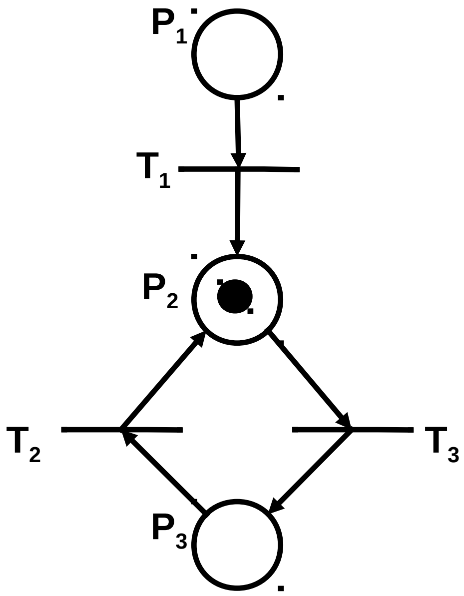


All transitions are live

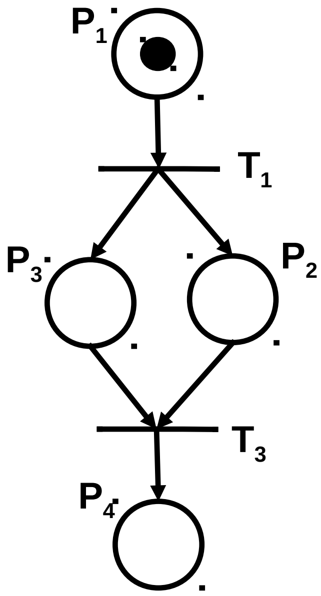
Behavioural properties: Conservativeness 1/2

- The total number of tokens in the PN is constant

Behavioural properties: Conservativeness 2/2



Conservative PN



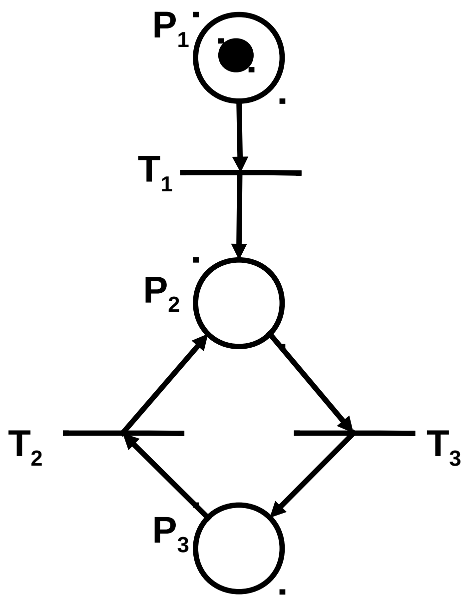
Non-conservative PN

Which properties do Petri Nets have?

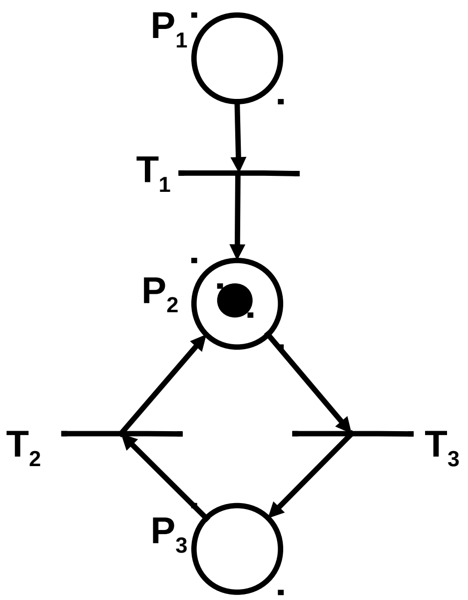
- Behavioural properties
  - Reachability
  - Boundedness
  - Liveness
  - Conservativeness
- **Structural properties**
  - **Structural liveness**
  - **Controllability**
  - **Structural boundedness**

Structural properties: Structural liveness 1/2

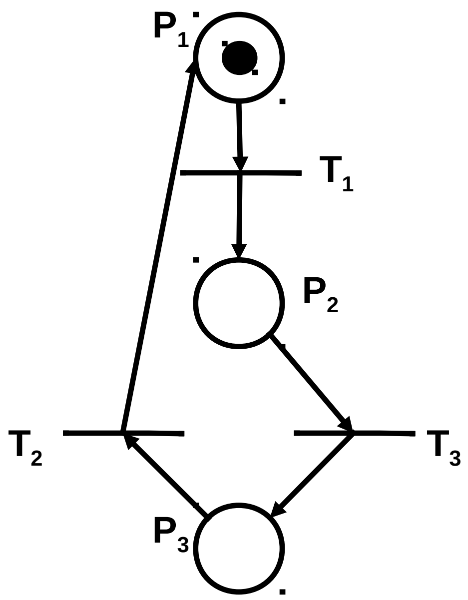
- A live Petri Net has only live transitions
- Liveness implies deadlock-free
- Deadlock-free does not imply liveness



Structural properties: Structural liveness 2/2



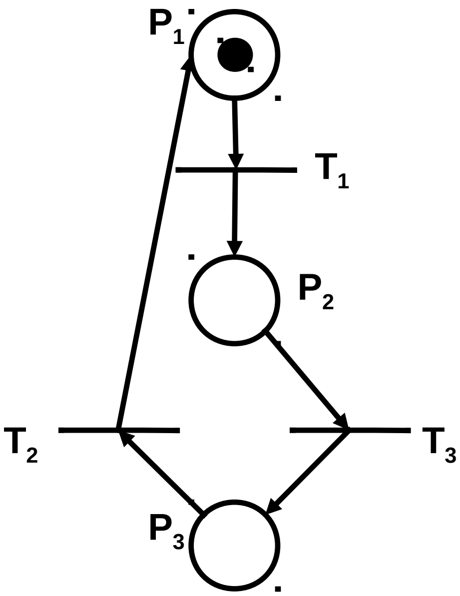
T_1 is not live; PN is deadlock free



PN is live

Structural properties: Controllability

- Any marking is reachable from any other marking



Structural properties: Structural boundedness

- PN is structurally bounded if it is bounded for any initial marking M_0
- 1-bounded PNs are called *safe*
  - Safeness can be important in e.g., storage system to prevent buffer overflow

Dynamic and static analysis

- Dynamic analysis
  - Involves experimentation using models
  - Targets to show correct/incorrect behaviour
- Static analysis
  - Applies analysis to the model
  - Targets proving theorems about properties

Dynamic analysis of Petri Nets 1/2

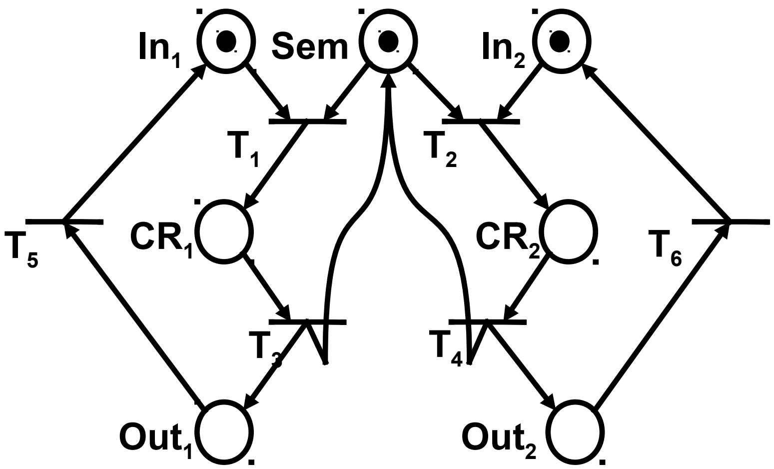
- Uses graphs or trees
  - Reachability graphs
    - Graph representation of all possible firing sequences
    - Shows possible behaviours of the system
    - Graph is analyzed by searching for a particular node or path
      - Node = particular state of the system (marking)
      - Created from the initial state/marking
      - If the node/path is found, the behaviour is possible

Dynamic analysis of Petri Nets 2/2

- Experimentation to show (in)correct behaviour
  - Usually used to show incorrect behaviour
  - e.g., show that deadlock is possible
- An experiment is a single behaviour (particular situation)
- To prove that behaviour is correct we need to execute all possible experiments

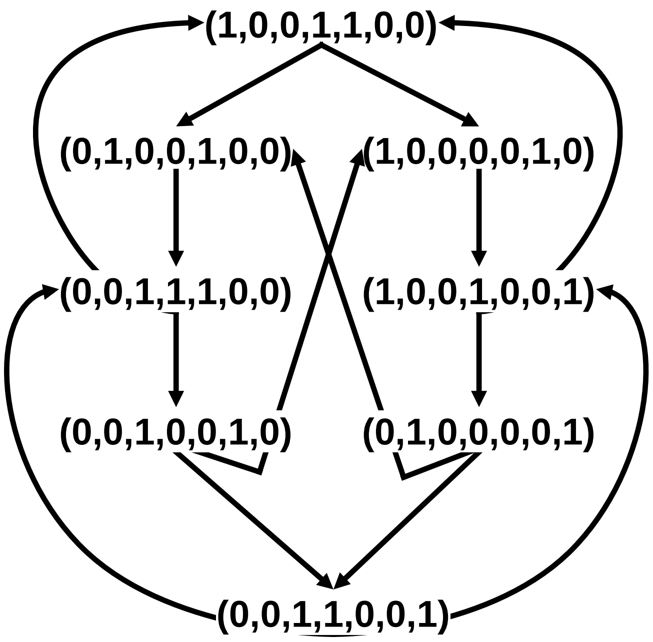
Dynamic analysis of the semaphore

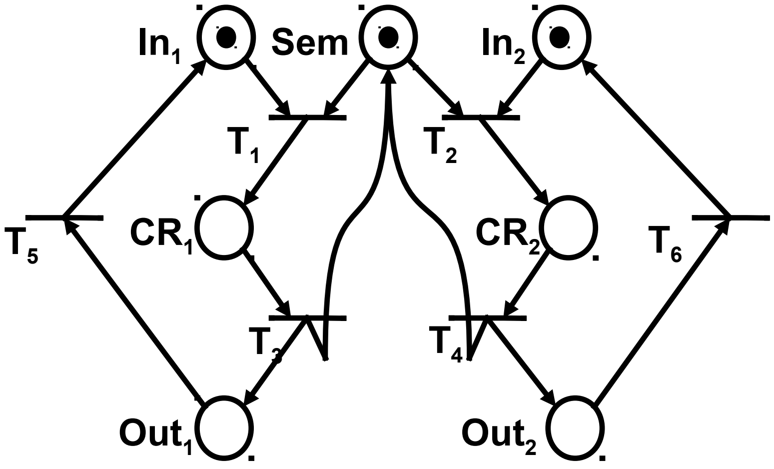
- Marking vector:
  - $M = (In_1, CR_1, Sem, In_2, CR_2, Out_2)$
  - Shown marking is (1,0,0,1,1,0,0)
- Let's draw the reachability graph!



Reachability graph of the semaphore

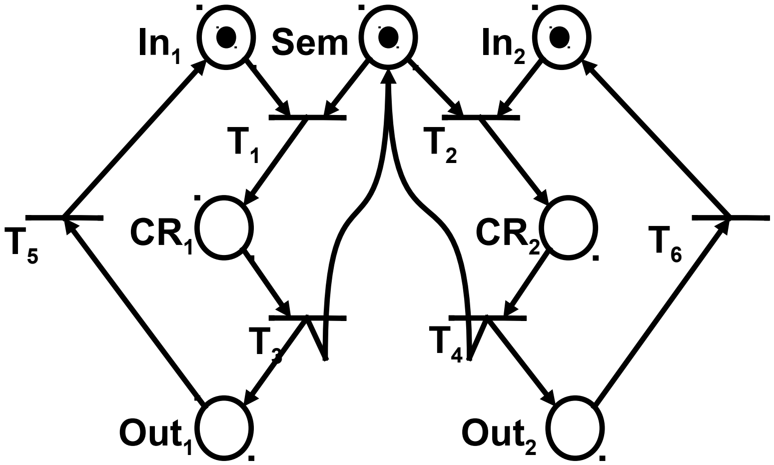
- M = (In$_1$, CR$_1$, Sem, In$_2$, CR$_2$, Out$_2$)





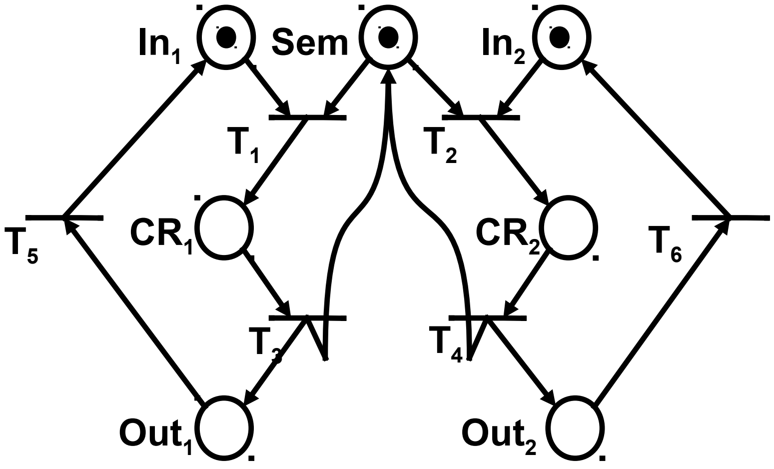
Questions answered using the reachability graph

- Can both processes access the critical resource at the same time?
- Can one process access the critical resource, while the other process waits?



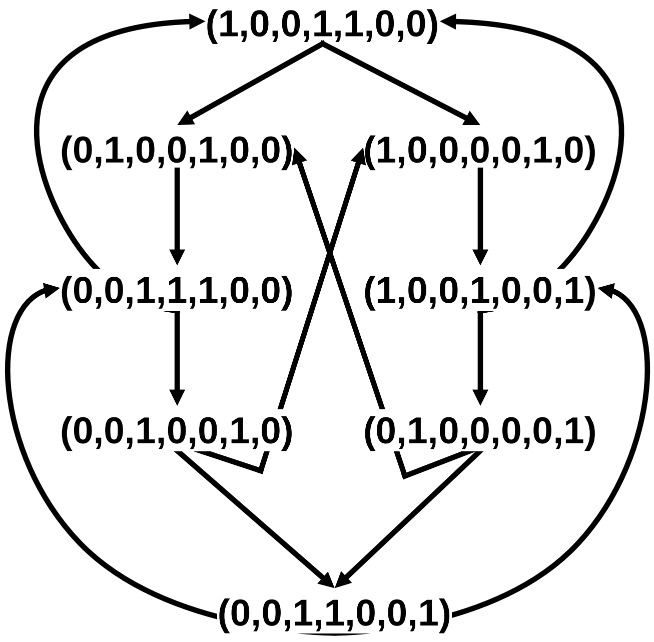
Questions answered using the reachability graph

- Can both processes access the critical resource at the same time?
  - Look for (0,1,0,0,0,1,0)
- Can one process access the critical resource, while the other process waits?
  - Look for (1,0,0,0,0,1,0) or (0,1,0,0,1,0,0)



Dynamic analysis of the semaphore

- Analysis is dynamic because we enumerate all possible behaviours
- Although the system runs forever, the graph can still model it



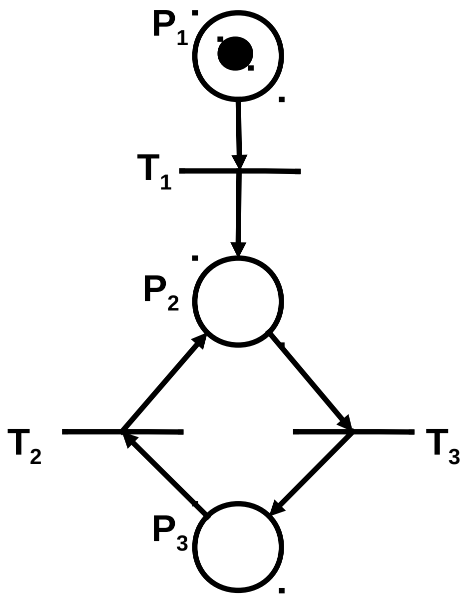
Static analysis of Petri Nets

- Reachability graph can become HUGE
  - Static analysis does not require the graph
- Analyse the structure of the PN using
  - State equation and incidence matrix
  - Invariants
    - Properties that hold in all markings of PN
- Uses linear algebra to prove properties
  - Matrix equations

Incidence matrix A 1/3

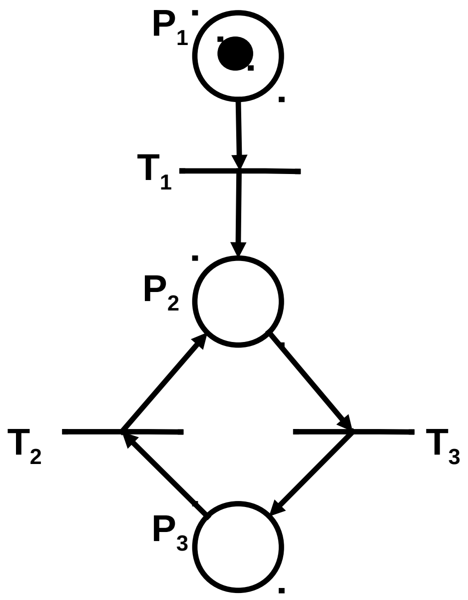
- I = matrix of input places
  - Rows are transitions
  - Columns are places

$$I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$



Incidence matrix A 2/3

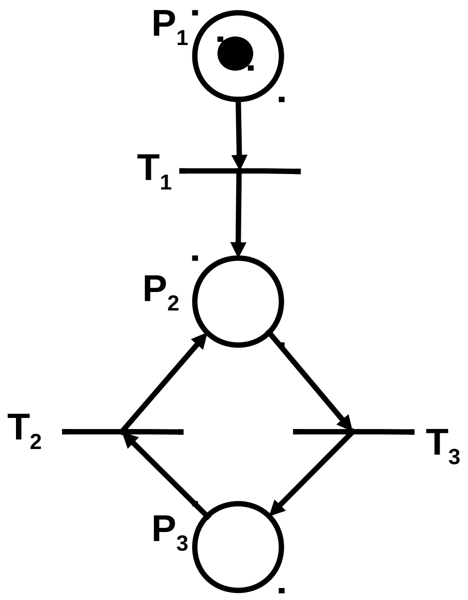
- O = matrix of output places
  - Rows are transitions
  - Columns are places



$$I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \qquad O = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Incidence matrix A 3/3

- Incidence matrix A
  - $A = O - I$
  - What does this matrix show?
    - The net result of each transition on each place

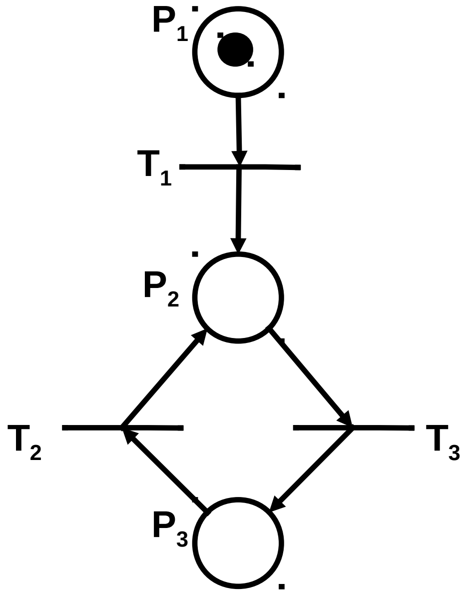


$$I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \qquad O = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad A = O - I = \begin{bmatrix} -1 & 1 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{bmatrix}$$

A vector representation of firing transitions

- $M = M_0 + t$
  - t is the input/output vector of an enabled transition

$$M = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} + \begin{bmatrix} -1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix}$$



State equation

- $M = M_0 + vA$
  - There exists a firing vector v such that M_0 is transformed into M
    - M is reachable from M_0
  - v contains t-elements (one for each transition)

An example of the state equation

- Given: $M = M_0 + vA$, $M_0 = (1,0,0)$, $M = (0,0,1)$, $t = 3$
- How can we reach M from M_0?

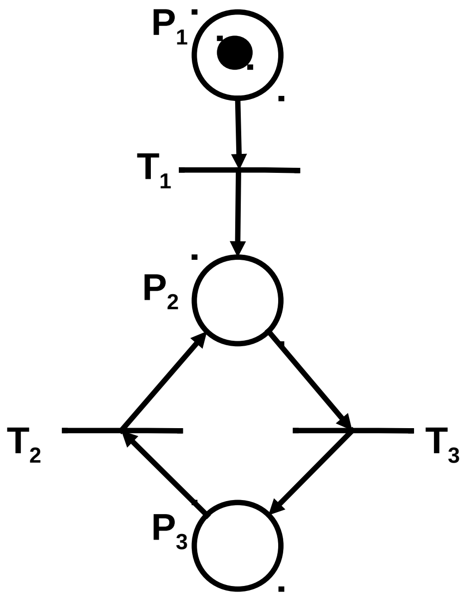
$$\begin{bmatrix}0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 0\end{bmatrix} + \begin{bmatrix}v_1 & v_2 & v_3\end{bmatrix}\begin{bmatrix}-1 & 1 & 0\\ 0 & 1 & -1\\ 0 & -1 & 1\end{bmatrix}$$

$$\begin{bmatrix}0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 0\end{bmatrix} + \begin{bmatrix}-v_1 & v_1+v_2-v_3 & -v_2+v_3\end{bmatrix}$$

$$\begin{bmatrix}0 & 0 & 1\end{bmatrix} = \begin{bmatrix}-v_1+1 & v_1+v_2-v_3 & -v_2+v_3\end{bmatrix}$$

$$v_1 = 1, v_2 = v_3 - 1$$

So M is reachable from M_0 by firing (1,0,1), or (1,k,k+1)



Invariants

- T-invariant (transition-invariant)
  - Firing sequence that brings PN back to the marking it starts in
- P-invariant (place-invariant)
  - Indicate places in which sum of tokens is constant for any reachable marking

The t-invariant 1/2

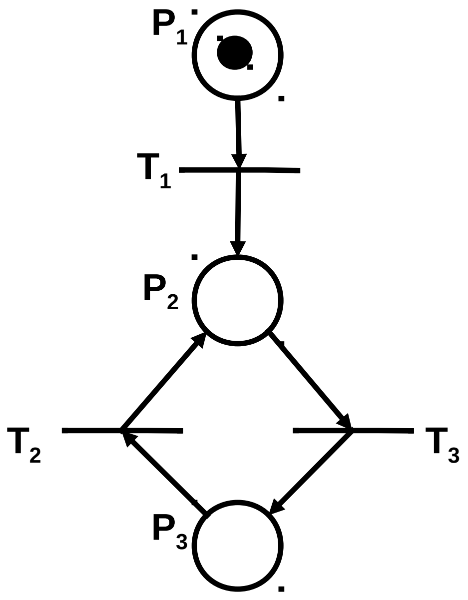
- The sequence of transitions that bring back PN to the marking it starts in
- Basically, a sequence of markings of which the net effect is zero

$$M = M_0 + yA$$

$$M = M_0 + 0$$

$$M = M_0$$

- Let's solve yA = 0

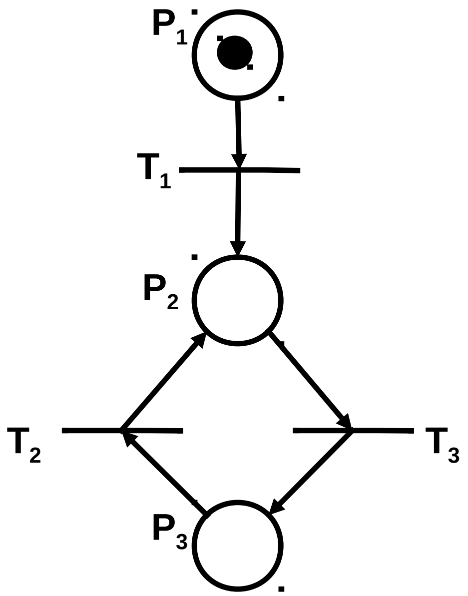


The t-invariant 2/2

$$yA = 0 \rightarrow \begin{bmatrix} y_1 & y_2 & y_3 \end{bmatrix} \begin{bmatrix} -1 & 1 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$$

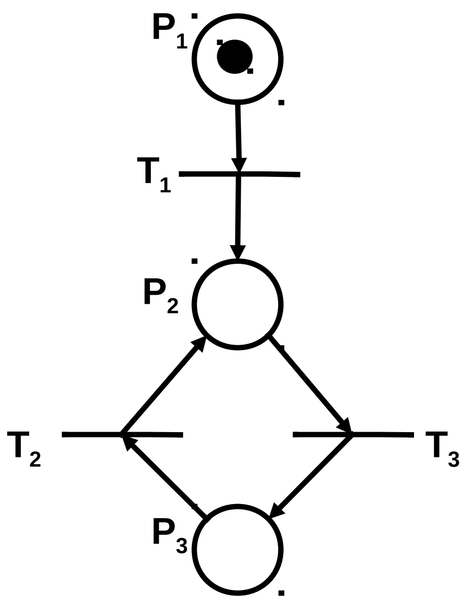
$$y_1 = 0, y_2 = y_3$$

General form of y = (0,k,k)



The number of tokens in M

- M(p) is the number of tokens in place p for marking M
- So, the total number of tokens in marking M is:
  - $M(P_1) + M(P_2) + M(P_3) + M(P_{...}) + M(P_n)$
  - Note: we can also write Mx where x is a vector with an element for each place



The p-invariant

- Indicate places in which sum of tokens is constant for any reachable marking

$$M = M_0 + yA$$

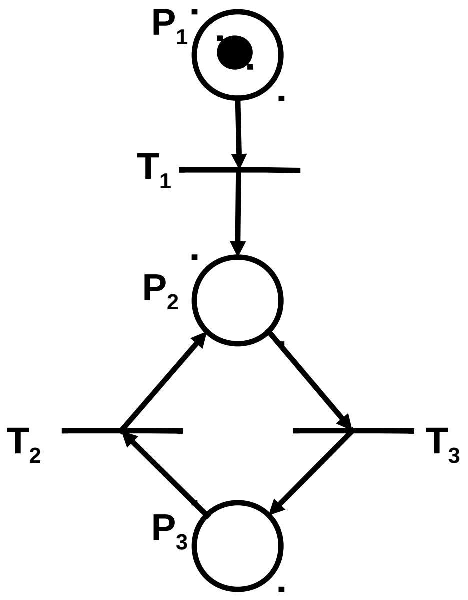
- To get the number of tokens, we use the vector x:

$$Mx = (M_0 + yA)x$$

$$Mx = M_0x + yAx$$

$$\text{if } Ax = 0 \text{ then } Mx = M_0x$$

- x is called a p-invariant



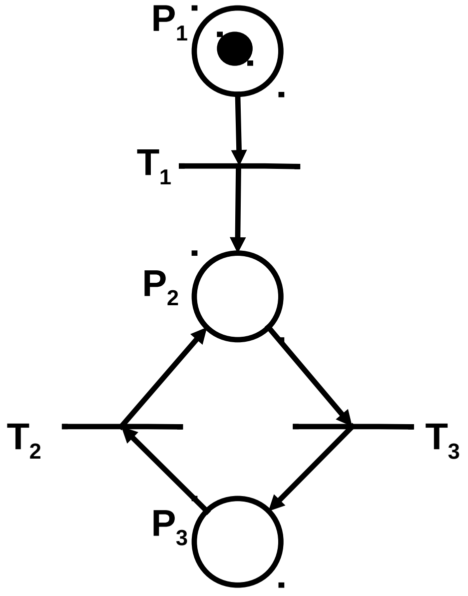
The p-invariant

- Indicate places in which sum of tokens is constant for any reachable marking
- What is Ax = 0?

$$Ax = 0 \rightarrow \begin{bmatrix} -1 & 1 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$x_1 = x_2 = x_3$$

General form of x = (k,k,k)
(sum of tokens is constant for any marking that we can reach)

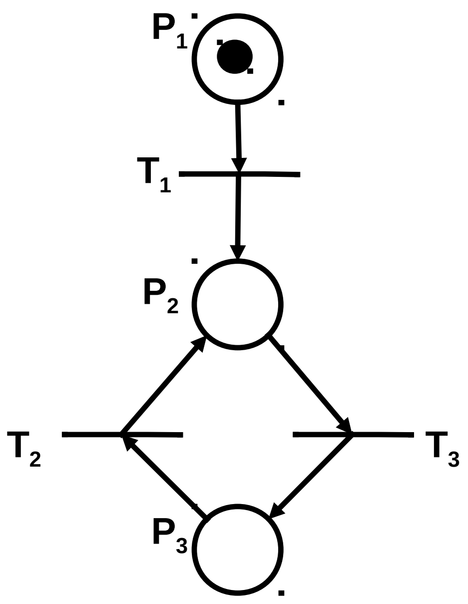


The p-invariant equation

- We know that all places are in the invariant
- We know that $Mx = M_0x$, and $x = (1,1,1)$ so:

$$M(P_1) + M(P_2) + M(P_3) =$$

$$M_0(P_1) + M_0(P_2) + M_0(P_3) = ?$$



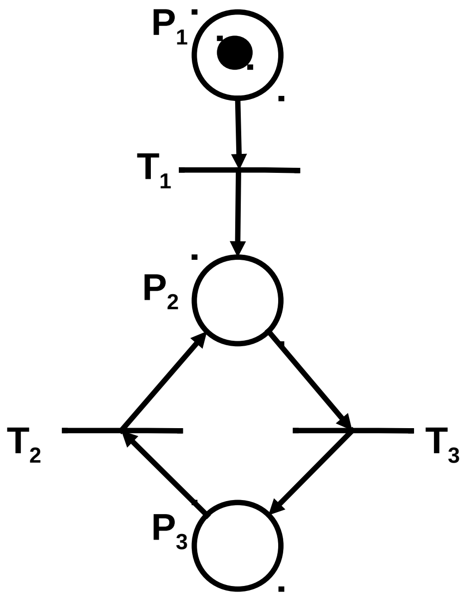
The p-invariant equation

- We know that all places are in the invariant
- We know that $Mx = M_0x$, and $x = (1,1,1)$ so:

  $M(P_1) + M(P_2) + M(P_3) =$

  $M_0(P_1) + M_0(P_2) + M_0(p_3) = \mathbf{1}$

  – Because the total number of tokens in M_0 is 1
- What is this invariant useful for?



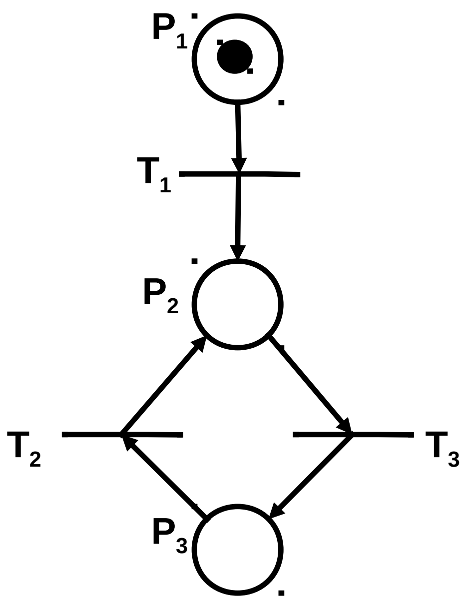
The p-invariant equation

- We know that all places are in the invariant
- We know that $Mx = M_0x$, and $x = (1,1,1)$ so:

  $M(P_1) + M(P_2) + M(P_3) =$

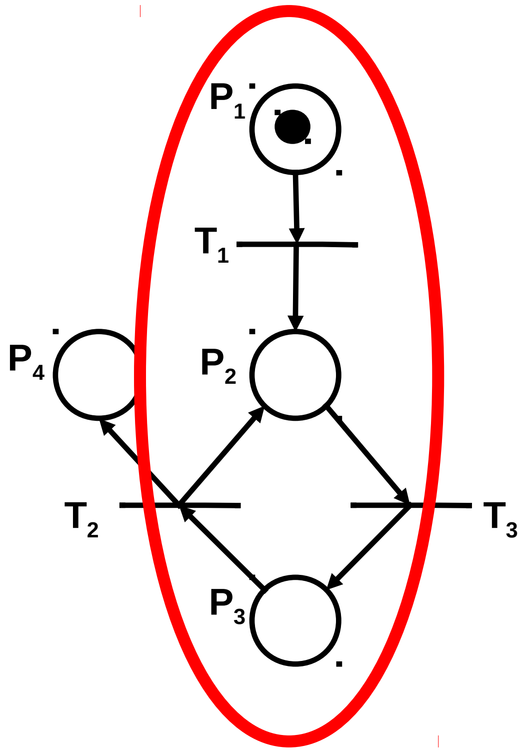
  $M_0(P_1) + M_0(P_2) + M_0(p_3) = \mathbf{1}$

  – Because the total number of tokens in M_0 is 1
- What is this invariant useful for?
  – Proves mutual exclusiveness between the places



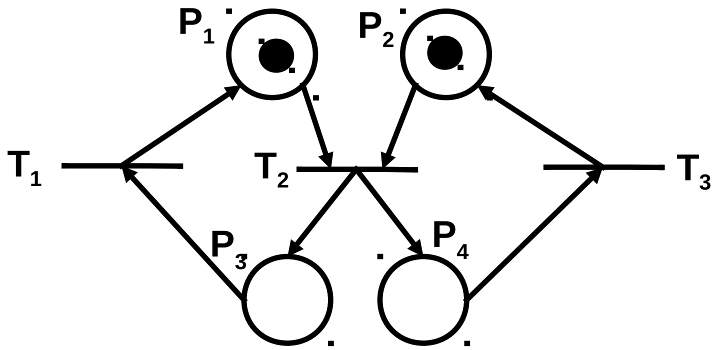
The p-invariant equation

- What is the p-invariant now?
  - (1, 1, 1, 0)



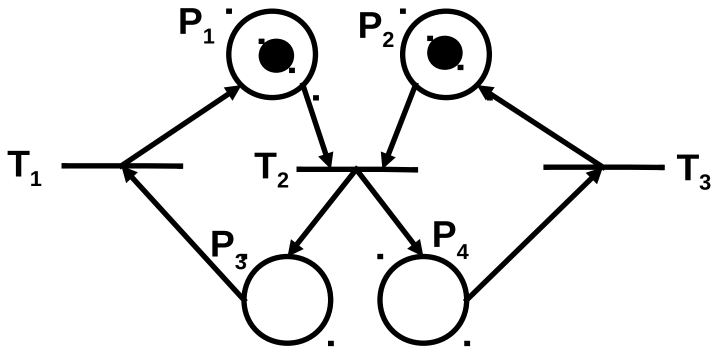
Can you calculate the invariants?

- T-invariant (yA = 0)
- P-invariant (Ax = 0)
- P-invariant equation



Can you calculate the invariants?

- T-invariant (yA = 0)
  - y = (k, k, k)
- P-invariant (Ax = 0)
  - x = (a,b,a,b)
- P-invariant equation
  - For a=1: $M(P_1) + M(P_3) = 1$
  - For b=1: $M(P_2) + M(P_4) = 1$



Examples of invariant analysis

- Invariants are useful for analysis of properties such as liveness and boundedness
- For example, we can use a p-invariant to prove mutual exclusiveness
  - e.g., $M(P_1) + M(P_2) + M(P_3) = 1$
- Advantage: much less computationally intensive than dynamic analysis

Next week

- Reading week
  - So no lecture
- Office hours as usual