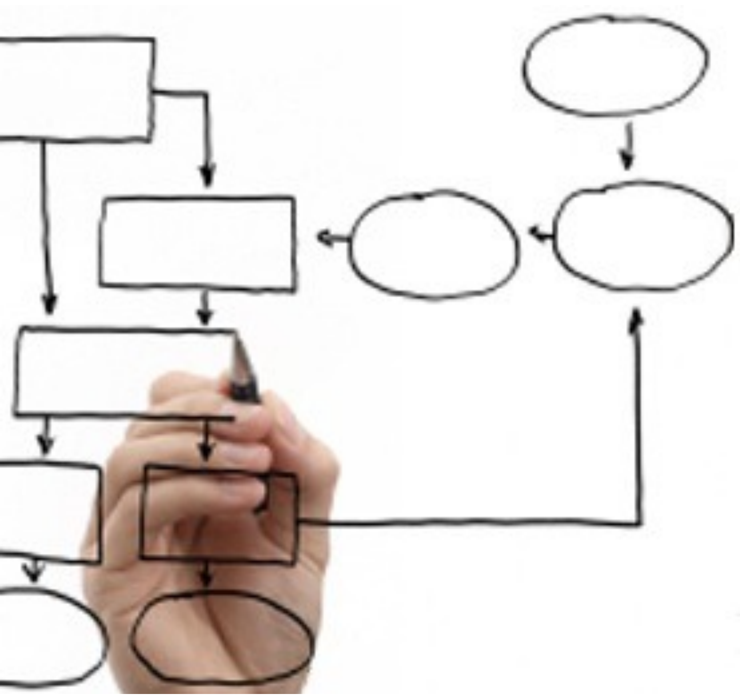
Methods for the specification and verification of business processes

MPB (6 cfu, 295AA)

Roberto Bruni
http://www.di.unipi.it/~bruni



15 - S-systems, T-systems

Before we start...

Two theorems on strong connectedness whose proofs we omit

Strong connectedness theorem

Theorem: If a weakly connected system is live and bounded then it is strongly connected

(the proof requires a few technical lemmas that we prefer to omit)

Strong connectedness via invariants

Theorem: If a weakly connected net has a positive S-invariant and a positive T-invariant then it is strongly connected

(the proof exploits requires a few technical lemmas that we prefer to omit)

Object

We study some “good” properties of S-systems and T-systems

Notation: token count

$$M(P) = \sum_{p \in P} M(p)$$

Example

$P = \{p_1, p_2, p_3\}$ $\qquad M = 2p_1 + 3p_2 \qquad M(P) = 2 + 3 + 0 = 5$

S-systems

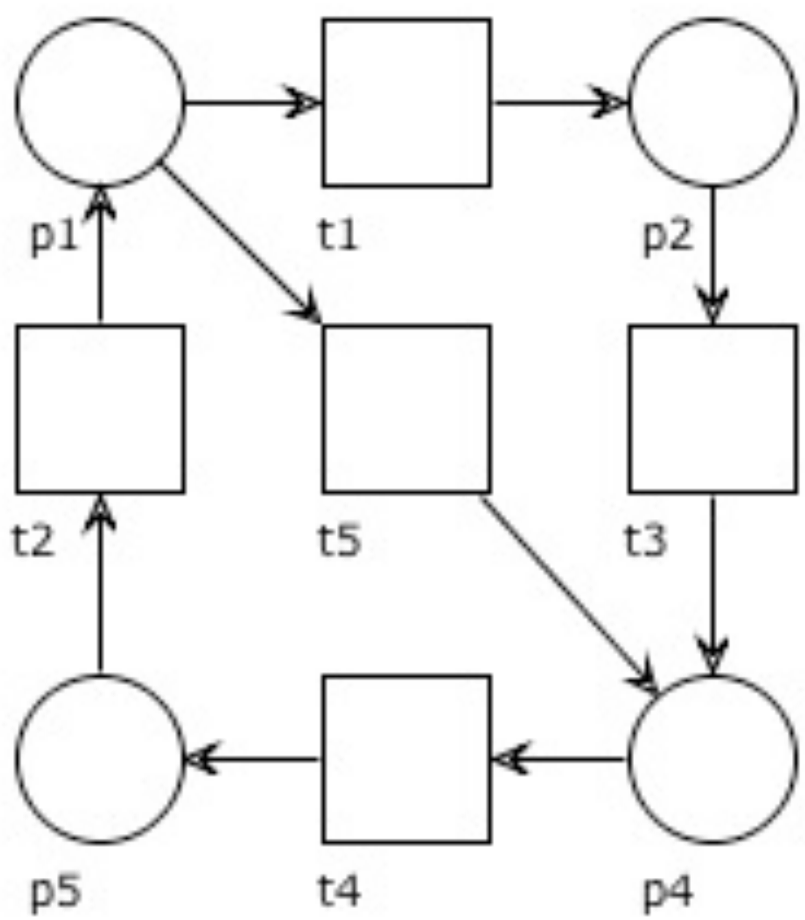
S-system

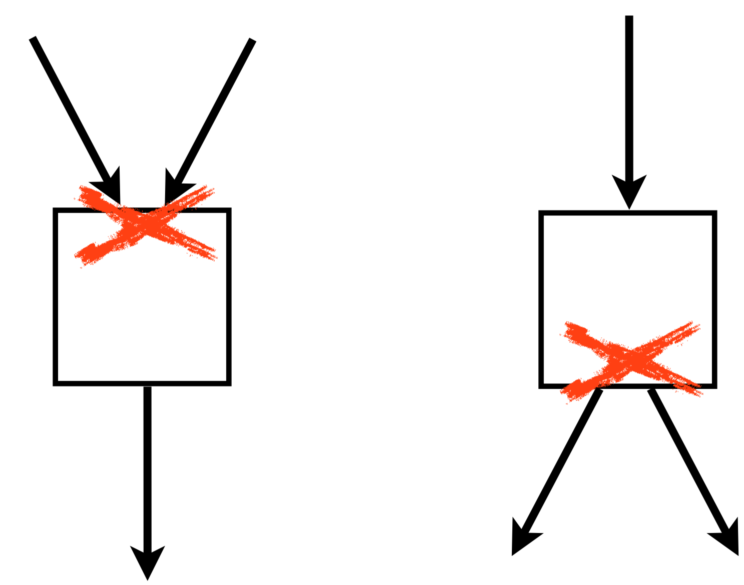
Definition: We recall that a net N is an **S-net** if each transition has exactly one input place and exactly one output place

$$\forall t \in T, \qquad |\bullet t| = 1 = |t \bullet|$$

A system (N,M_0) is an **S-system** if N is an S-net

S-system: example





Fundamental property of S-systems

Observation: each transition t that fires removes exactly one token from some place p and inserts exactly one token in some place p’ (p and p’ can also coincide)

Thus, **the overall number of tokens in the net is an invariant** under any firing.

Fundamental property of S-systems

Proposition: Let (P,T,F,M_0) be an S-system.
If M is a reachable marking, then $M(P) = M_0(P)$

We show that for any $M \xrightarrow{\sigma} M'$ we have $M'(P) = M(P)$

$\textbf{base } (\sigma = \epsilon)\textbf{:}$ trivial $(M' = M)$

$\textbf{induction } (\sigma = \sigma' t \textbf{ for some } \sigma' \in T^* \textbf{ and } t \in T)\textbf{:}$

Let $M \xrightarrow{\sigma'} M'' \xrightarrow{t} M'$.

By inductive hypothesis: $M''(P) = M(P)$

By definition of T-system: $|\bullet t| = |t \bullet| = 1$

Thus, $M'(P) = M''(P) - |\bullet \ t| + |t \bullet| = M(P) - 1 + 1 = M(P)$

A consequence of the fundamental property

Corollary: Any S-system is bounded

Let $M \in [\, M_0 \,\rangle$.

By the fundamental property of S-systems: $M(P) = M_0(P)$.

Then, for any $p \in P$ we have $M(p) \leq M(P) = M_0(P)$.

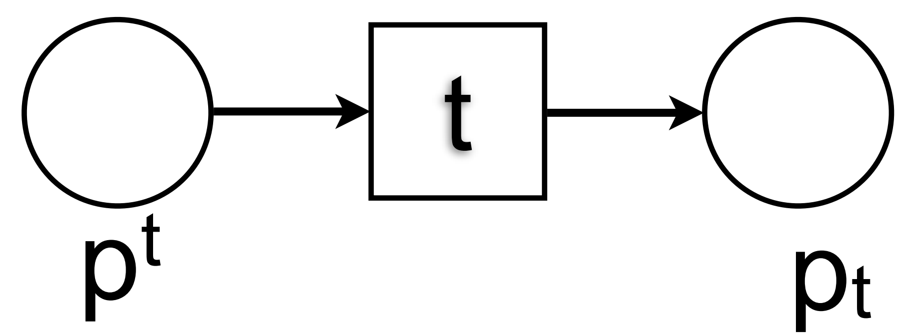
Thus the S-system is k-bounded for any $k \geq M_0(P)$.

S-invariants of S-nets

Proposition: Let N=(P,T,F) be a connected S-net.
I is a rational-valued S-invariant of N iff **I**=[x ... x]
for some rational value x

S-invariance $$\forall t \in T,\ \sum_{p \in \bullet t} \mathbf{I}(p) = \sum_{p \in t \bullet} \mathbf{I}(p)$$

S-nets $$\forall t \in T,\ |\bullet t| = |t \bullet| = 1$$

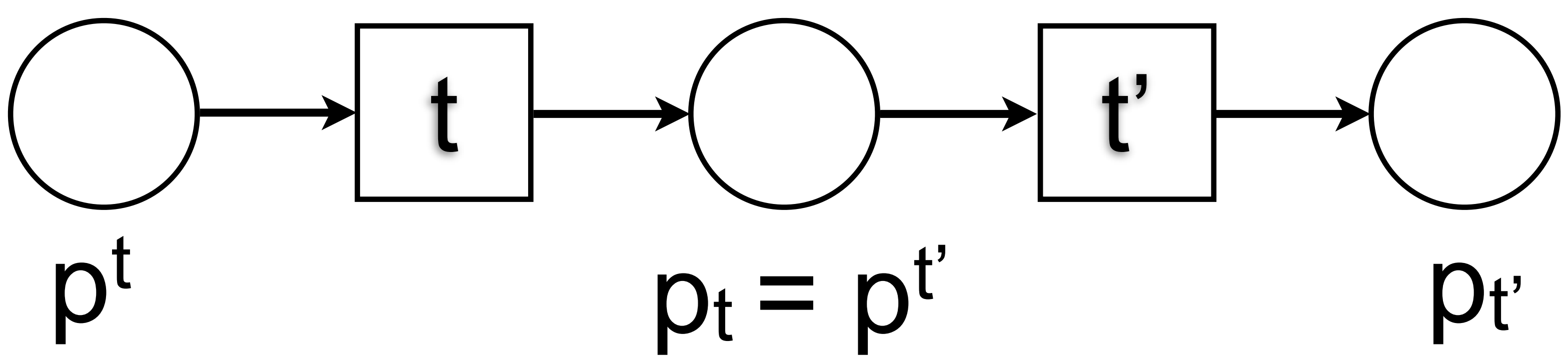


Let $\bullet t = \{p^t\}$ and $t\bullet = \{p_t\}$

$$\forall t \in T,\ \mathbf{I}(p^t) = \mathbf{I}(p_t)$$

S-invariants of S-nets

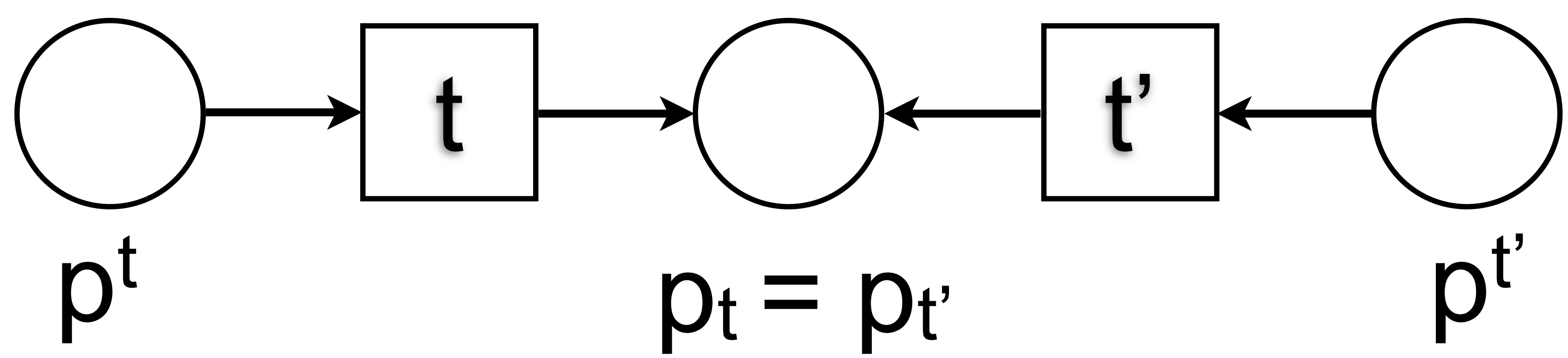
Proposition: Let N=(P,T,F) be a connected S-net.
I is a rational-valued S-invariant of N iff **I**=[x ... x]
for some rational value x



$$\mathbf{I}(p^t) = \mathbf{I}(p_t) = \mathbf{I}(p^{t'}) = \mathbf{I}(p_{t'})$$

S-invariants of S-nets

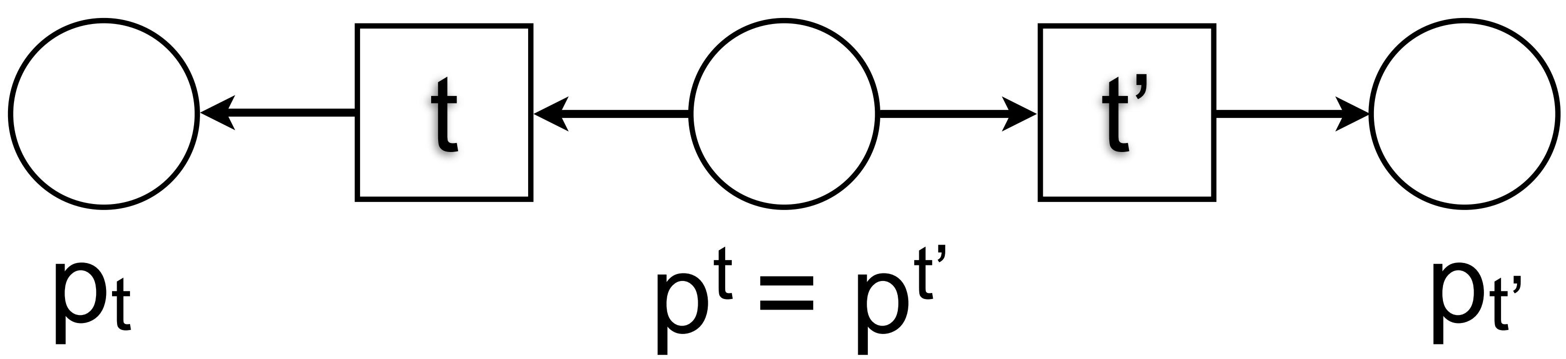
Proposition: Let N=(P,T,F) be a connected S-net.
I is a rational-valued S-invariant of N iff **I**=[x ... x]
for some rational value x



$$\mathbf{I}(p^t) = \mathbf{I}(p_t) = \mathbf{I}(p_{t'}) = \mathbf{I}(p^{t'})$$

S-invariants of S-nets

Proposition: Let N=(P,T,F) be a connected S-net.
I is a rational-valued S-invariant of N iff **I**=[x ... x]
for some rational value x



$$\mathbf{I}(p_t) = \mathbf{I}(p^t) = \mathbf{I}(p^{t'}) = \mathbf{I}(p_{t'})$$

S-invariants of S-nets

Proposition: Let N=(P,T,F) be a connected S-net.
I is a rational-valued S-invariant of N iff **I**=[x ... x]
for some rational value x

weak connectivity

$$\forall p_0, p_n \in P, \quad p_0\, t_1\, p_1\, t_2\, p_2\, t_3\, p_3 \dots t_n\, p_n$$

$$(\forall t_i, \text{ either } (p_i, t_i)(t_i, p_{i+1}) \text{ or } (t_i, p_i)(p_{i+1}, t_i))$$

$$\forall p_0, p_n \in P, \mathbf{I}(p_0) = \mathbf{I}(p_n)$$

A note on S-invariants and S-nets

S-invariance $$\forall M \in [\, M_0 \,\rangle, \quad \mathbf{I} \cdot M = \mathbf{I} \cdot M_0$$

S-invariant of S-nets $$\mathbf{I} = [\, 1\ 1\ ...\ 1 \,]$$

consequence $$\forall M, \quad \mathbf{I} \cdot M = \sum_{p \in P} 1 \cdot M(p) = \sum_{p \in P} M(p) = M(P)$$

We recover the Fundamental property of S-nets $$\forall M \in [\, M_0 \,\rangle, \quad M(P) = \mathbf{I} \cdot M = \mathbf{I} \cdot M_0 = M_0(P)$$

Reachability lemma for S-nets

Lemma: Let (P,T,F) be a strongly connected S-net.
If M(P) = M'(P), then M' is reachable from M

We proceed by induction on $M(P)$

base $(M(P) = M'(P) = 0)$**:** trivial $(M' = M)$

induction $(M(P) = M'(P) > 0)$**:**

Let $p, p' \in P$ be such that $M(p) > 0$ and $M'(p') > 0$.

Let $K = M - p$ and $K' = M' - p'$.

Clearly $K'(P) = K(P) < M(P) = M'(P)$.

By inductive hypothesis: $\exists \sigma,\ K \stackrel{\sigma}{\longrightarrow} K'$

By strong connectedness: there is a path from $p_0 = p$ to $p_n = p'$

$(p_0, t_1)(t_1, p_1)(p_1, t_2)...(t_n, p_n)$

By definition of S-system: $\bullet t_i = \{p_{i-1}\}$ and $t_i \bullet = \{p_i\}$.

Thus, $p = p_0 \stackrel{\sigma'}{\longrightarrow} p_n = p'$ for $\sigma' = t_1 t_2 ... t_n$.

By the monotonicity lemma: $M = K + p \stackrel{\sigma}{\longrightarrow} K' + p \stackrel{\sigma'}{\longrightarrow} K' + p' = M'$

Liveness theorem for S-systems

Theorem: An S-system (N,M_0) is live iff N is strongly connected and M_0 marks at least one place

$\Rightarrow$) (quite obvious)
(N, M_0) is live by hypothesis and bounded (because S-system).
By the strong connectedness theorem, N is strongly connected.

Since (N, M_0) is live, then $M_0 \xrightarrow{t}$ for some t.

Assume $\bullet t = \{p\}$. Thus, $M_0(p) \geq 1$.

Liveness theorem for S-systems

Theorem: An S-system (N,M_0) is live iff N is strongly connected and M_0 marks at least one place

$\Leftarrow$) (more interesting)
Take any $M \in [\, M_0 \,\rangle$ and $t \in T$.
We want to find $M' \in [\, M \,\rangle$ such that $M' \stackrel{t}{\longrightarrow}$.

Take $p_1 \in P$ such that $M(p_1) \geq 1$ (it exists, because $M(P) = M_0(P) \geq 1$).
By strong connectedness: there is a path from p_1 to $t_n = t$
$(p_1, t_1)(t_1, p_2)(p_2, t_2)...(p_n, t_n)$

By definition of S-system: $\bullet t_i = \{p_i\}$ and $t_i \bullet = \{p_{i+1}\}$.
Thus, $M \stackrel{\sigma}{\longrightarrow} M' \stackrel{t}{\longrightarrow}$ for $\sigma = t_1 t_2 ... t_{n-1}$.

Reachability Theorem for S-systems

Theorem: Let (P,T,F,M_0) be a live S-system.
A marking M is reachable **iff** $M(P)=M_0(P)$

=>) Follows from the fundamental property of S-systems

<=) By the liveness theorem, the S-net is strongly connected. Then we conclude by applying the reachability lemma.

S-systems: recap

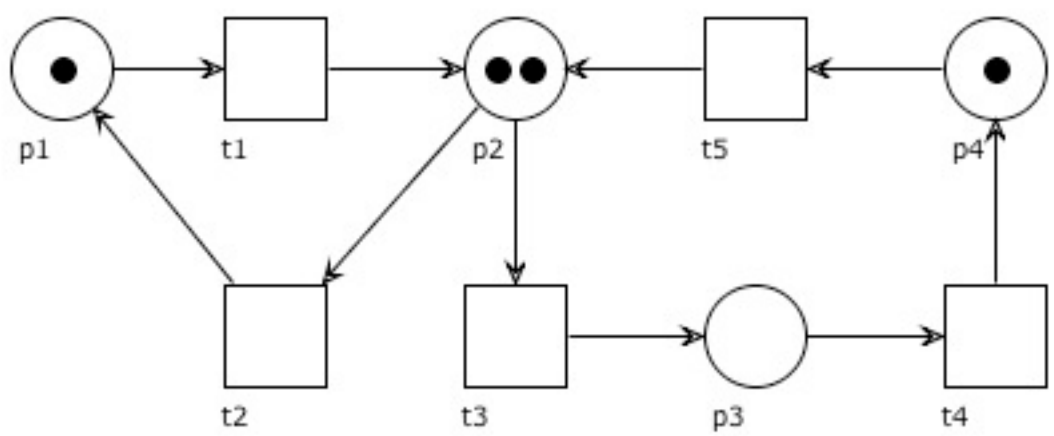
S-system => bounded
S-system: str. conn. + $M_0(P)>0$ <=> liveness

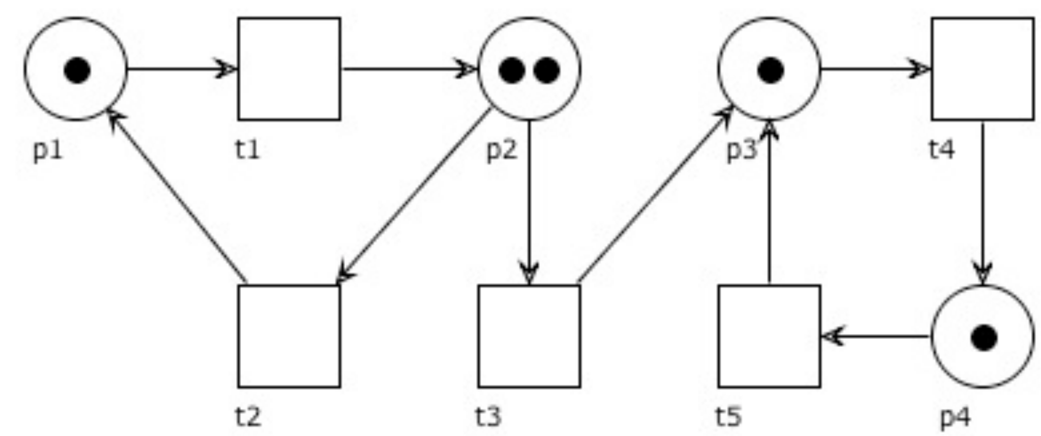
S-system + M reachable => $M(P) = M_0(P)$
S-system + str. conn.: $M(P)=M_0(P)$ <=> M reachable
S-system + liveness: $M(P)=M_0(P)$ <=> M reachable

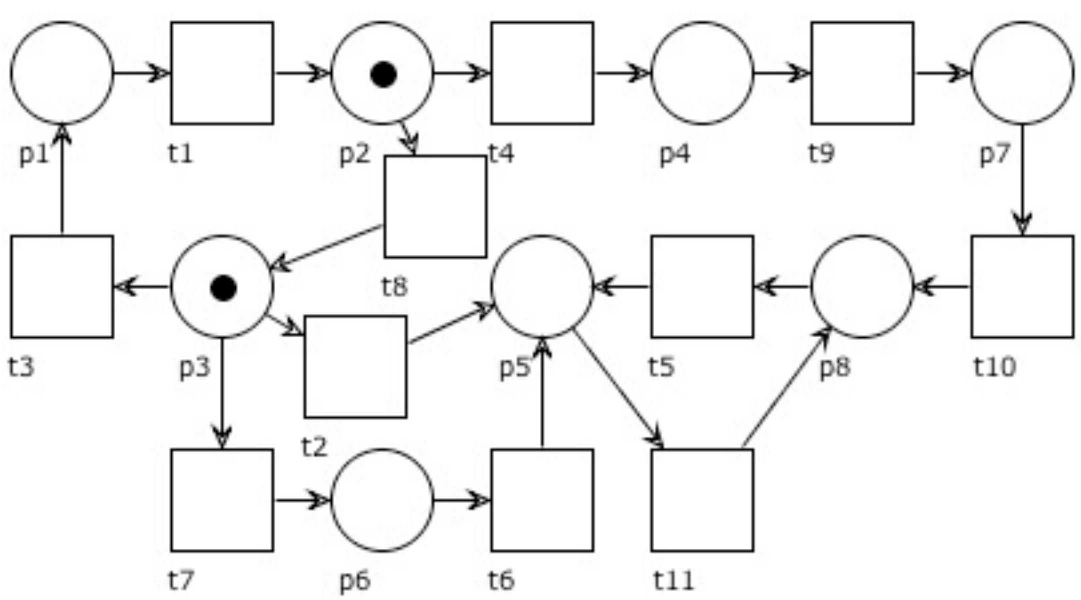
S-invariant **I** => **I** = [x x ... x]

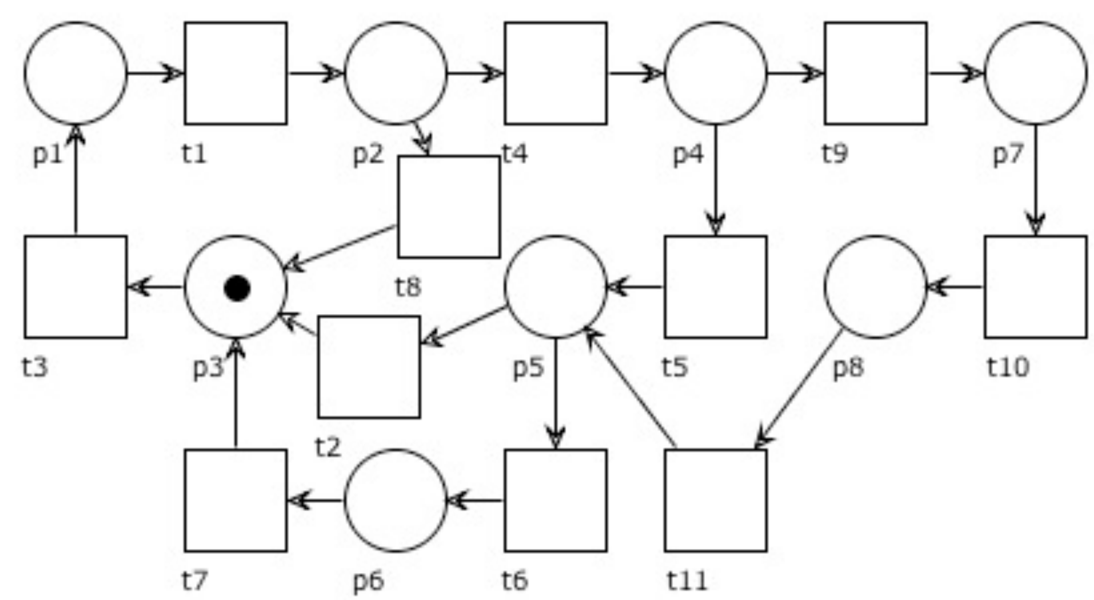
Exercises

Which of the following S-systems are live? (why?)



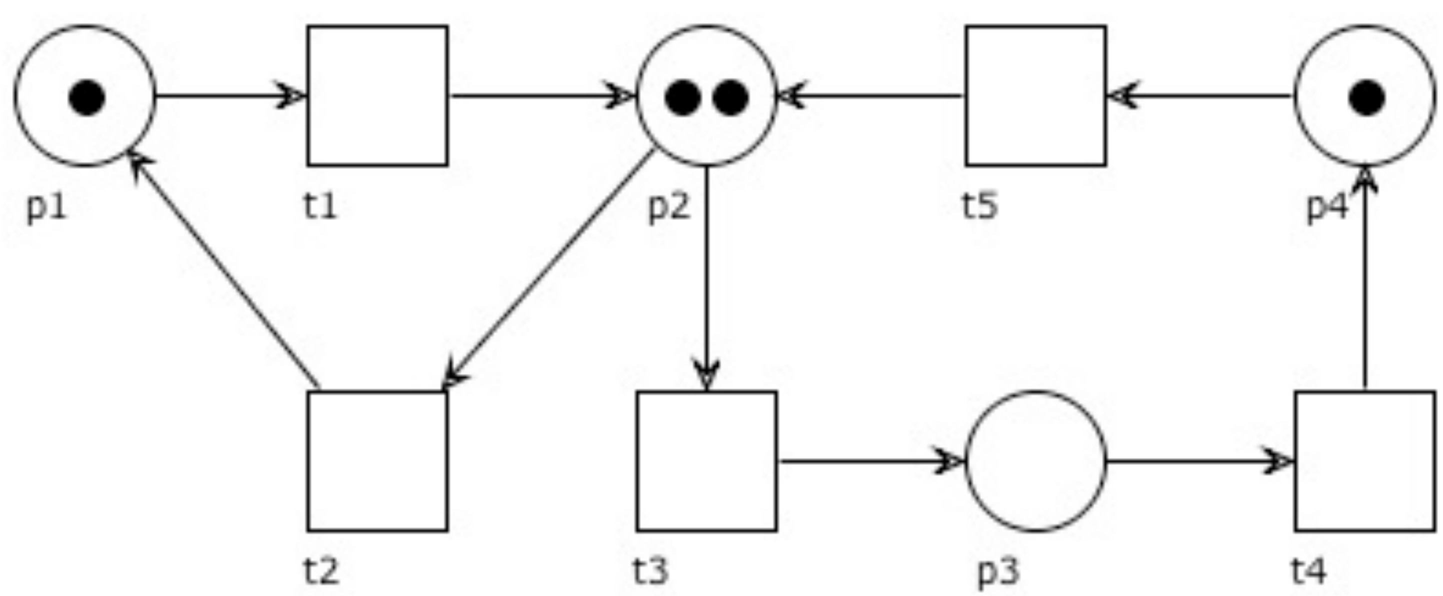






Exercises

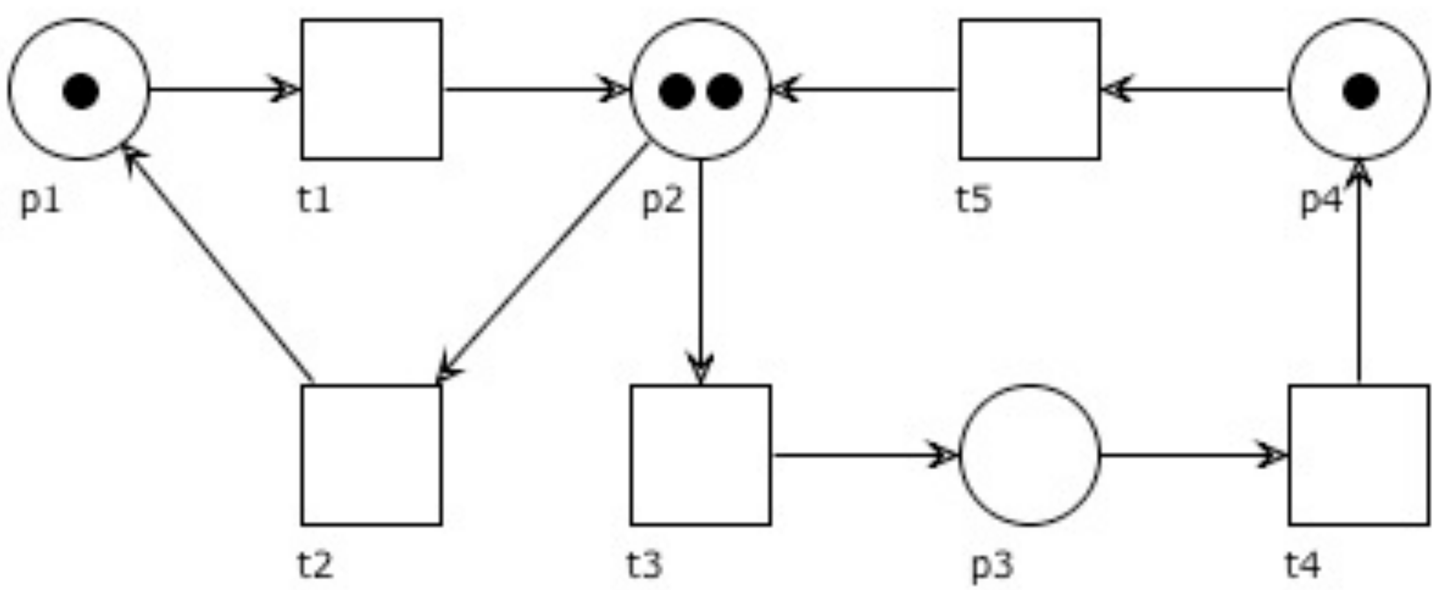
Which of the following markings are reachable? (why?)



[1 1 1 1]
[2 0 2 0]
[1 2 1 2]
[4 0 0 0]
[0 4 0 4]
[0 3 2 1]
[0 0 4 0]
[0 3 0 0]
[0 3 0 1]

Exercises

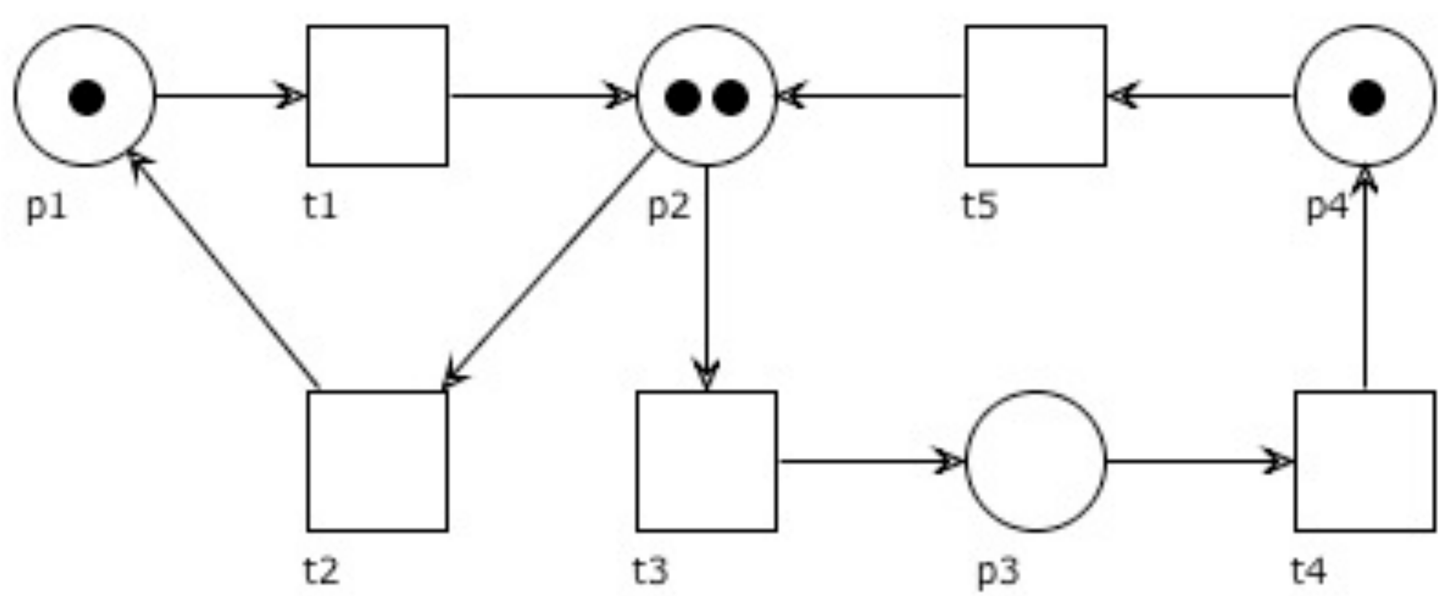
Which of the following markings are reachable? (why?)



[1 1 1 1]
[2 0 2 0]
[1 2 1 2]
[4 0 0 0]
[0 4 0 4]
[0 3 2 1]
[0 0 4 0]
[0 3 0 0]
[0 3 0 1]

Exercise

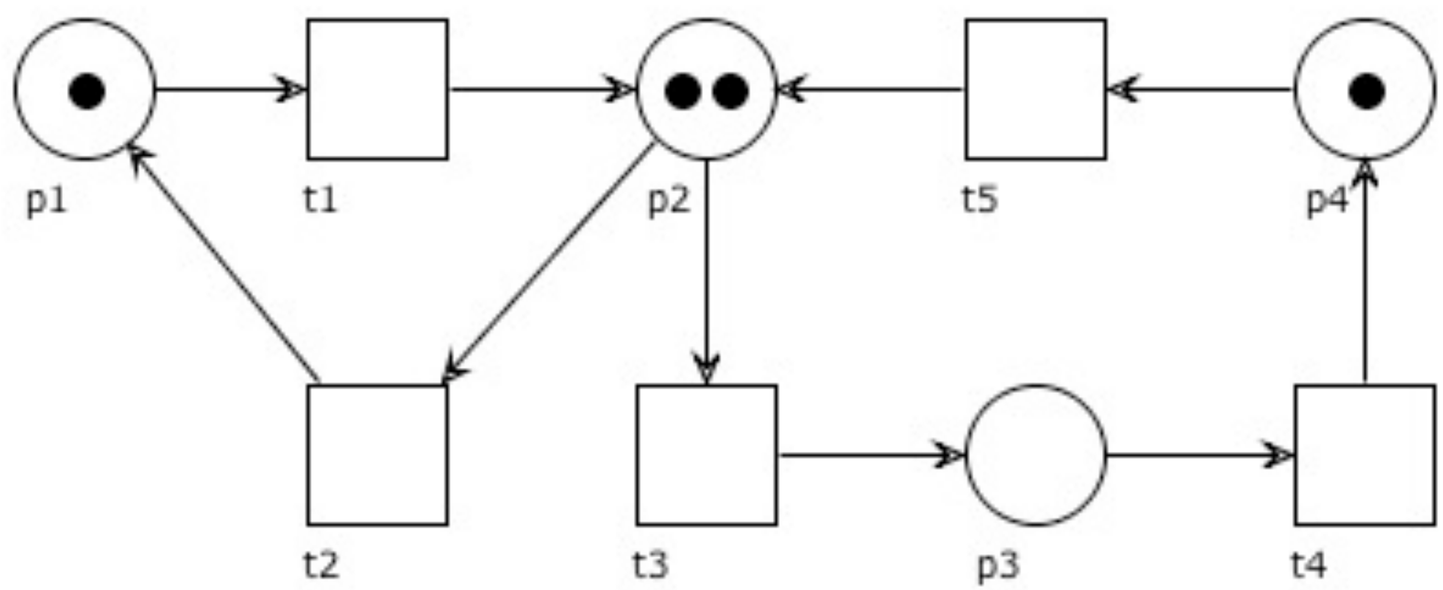
Which of the following are S-invariants? (why?)



[1 1 0 0]
[0 0 2 2]
[1 1 1 1]
[2 2 1 1]
[2 2 2 2]
[1 2 2 1]

Exercise

Which of the following are S-invariants? (why?)



[1 1 0 0]
[0 0 2 2]
[1 1 1 1]
[2 2 1 1]
[2 2 2 2]
[1 2 2 1]

Boundedness Theorem for S-systems

Theorem:
A live S-system (P, T, F, M_0) is k-bounded iff $M_0(P) \leq k$

Exercise

Prove the boundedness theorem for live S-systems

T-systems

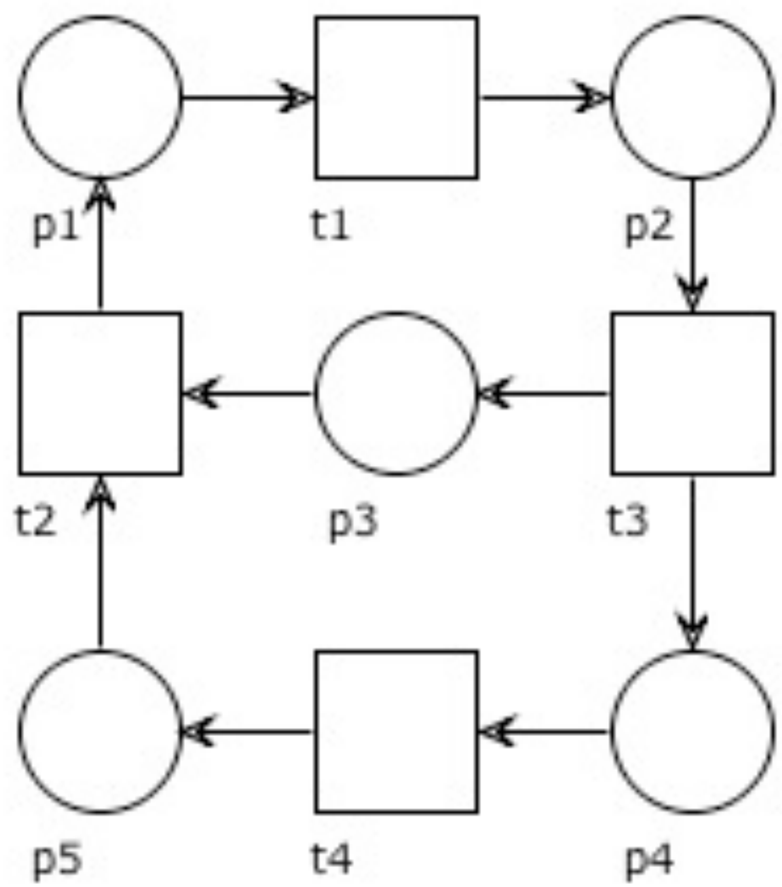
T-system

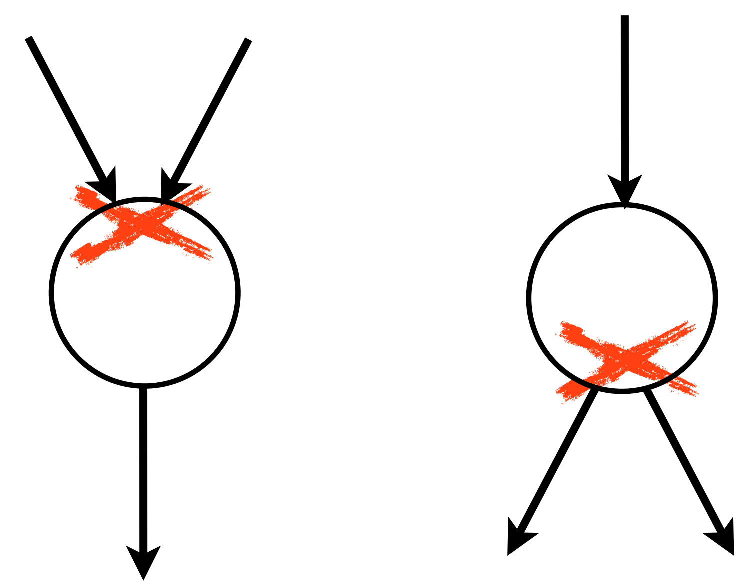
Definition: We recall that a net N is a **T-net** if each place has exactly one input transition and exactly one output transition

$$\forall p \in P, \qquad |\bullet p| = 1 = |p \bullet|$$

A system (N,M_0) is a **T-system** if N is a T-net

T-system: example





T-systems: an observation

Notably, computation in T-systems is concurrent, but essentially deterministic:

the firing of a transition t in M cannot disable another transition t' enabled at M

T-systems: another observation

Determination of control:

the transitions responsible for enabling t are one for each input place of t

Notation: token count of a circuit

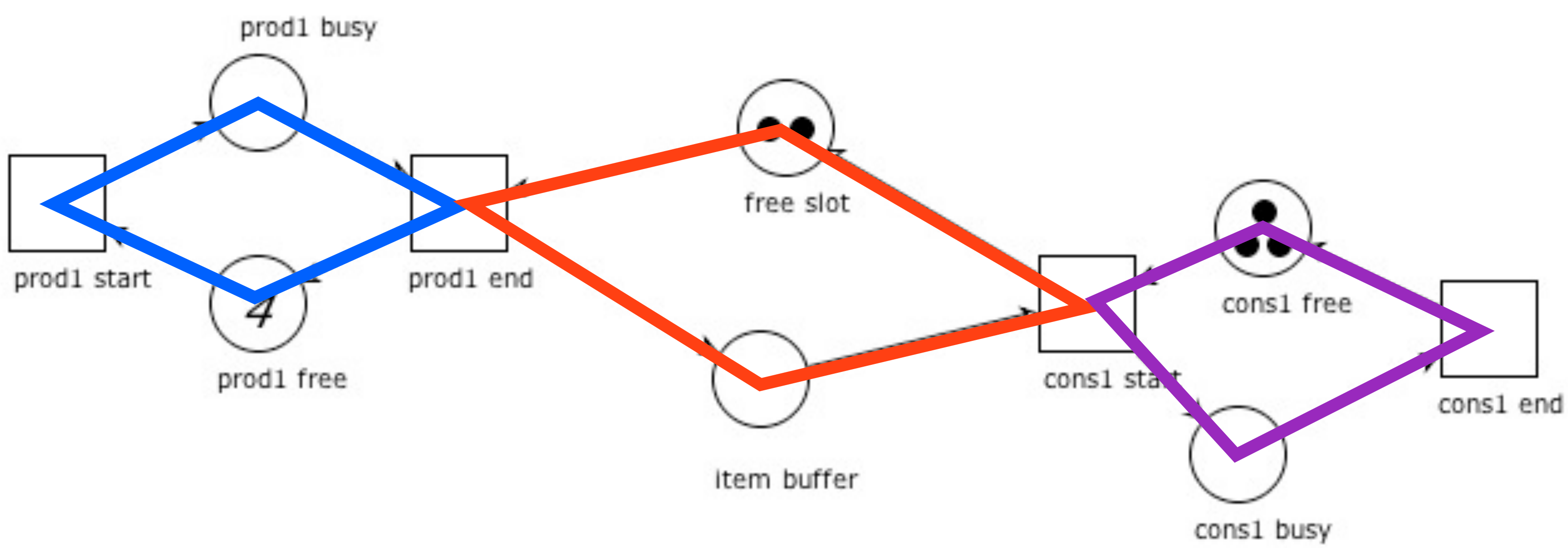
Let $\gamma = (x_1, y_1)(y_1, x_2)(x_2, y_2)...(x_n, y_n)$ be a circuit.

Let $P_{|\gamma} \subseteq P$ be the set of places in γ.

$$M(\gamma) = M(P_{|\gamma}) = \sum_{p \in P_{|\gamma}} M(p)$$

We say that γ is **marked at** M if $M(\gamma) > 0$

Example



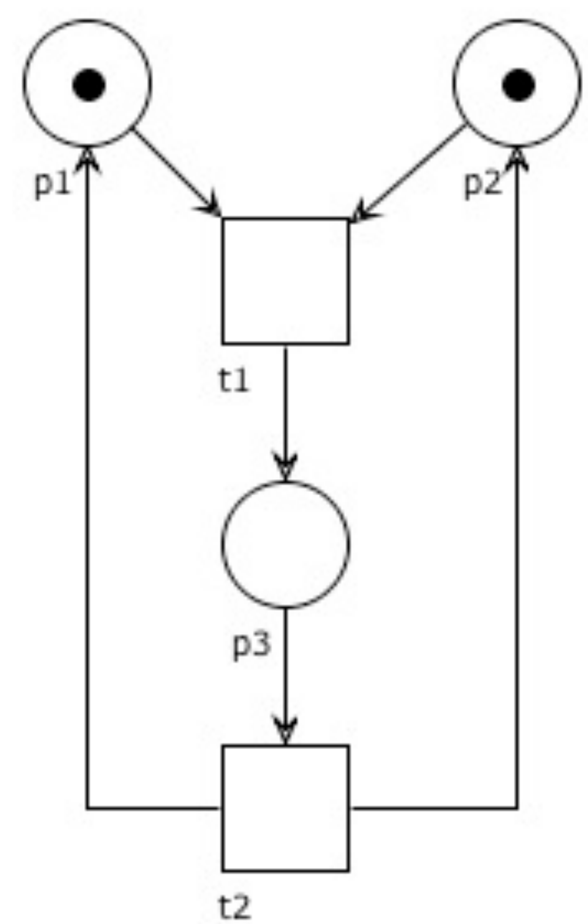
$$M(\gamma_1) = 4$$

$$M(\gamma_2) = 2$$

$$M(\gamma_3) = 3$$

Example

Trace two circuits over the T-system below



Fundamental property of T-systems

The token count of a circuit is invariant under any firing.

Fundamental property of T-systems

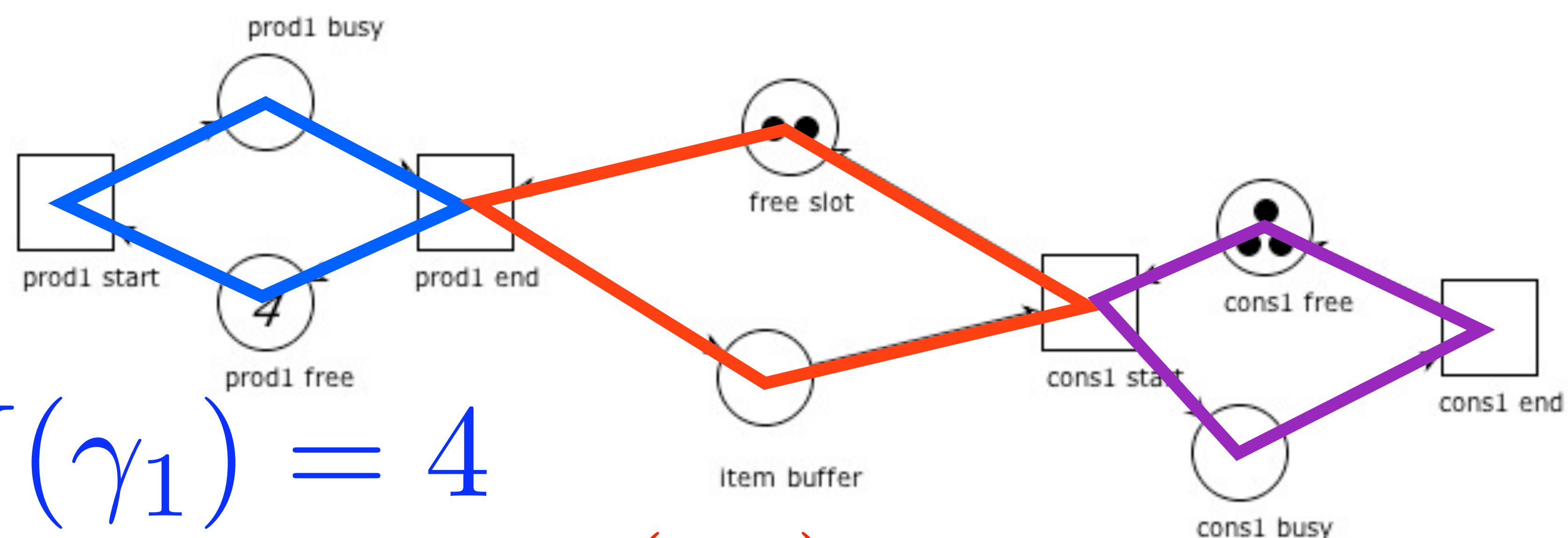
Proposition: Let γ be a circuit of a T-system (P, T, F, M_0). If M is a reachable marking, then $M(\gamma) = M_0(\gamma)$

Take any $t \in T$: either $t \notin \gamma$ or $t \in \gamma$.

If $t \notin \gamma$, then no place in $\bullet t \cup t \bullet$ is in γ
(otherwise, by definition of T-nets, t would be in γ).
Then, an occurrence of t does not change the token count of γ.

If $t \in \gamma$, then exactly one place in $\bullet t$ and one place in $t \bullet$ are in γ.
Then, an occurrence of t does not change the token count of γ.

Example



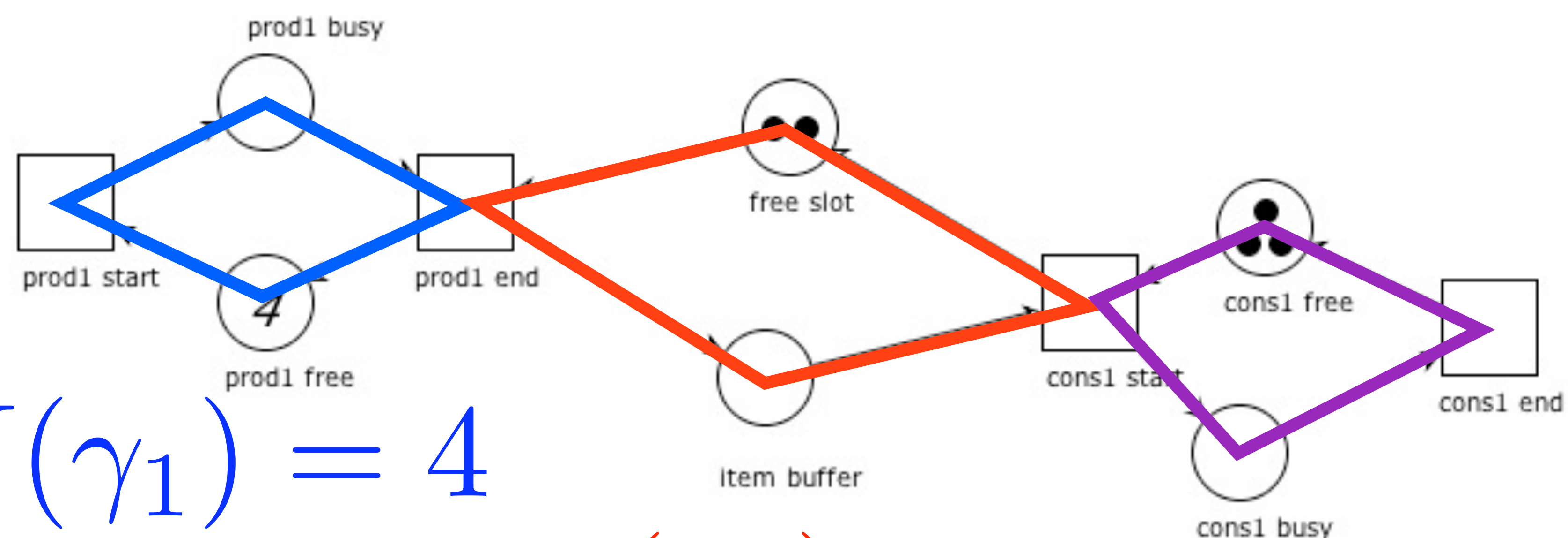
$$M(\gamma_1) = 4$$

$$M(\gamma_2) = 2$$

$$M(\gamma_3) = 3$$

M_0 = [0 4 2 0 3 0]
M = [2 2 1 2 2 1]
M' = [2 1 1 1 2 2]

Example



$M(\gamma_1) = 4$

$M(\gamma_2) = 2$

$M(\gamma_3) = 3$

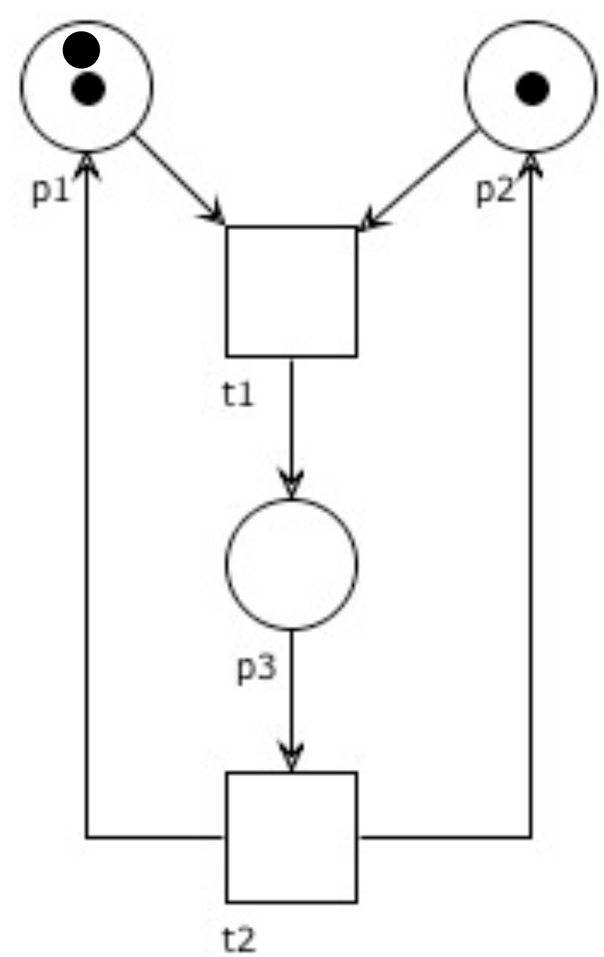
M_0 = [0 4 2 0 3 0]

M = [2 2 1 2 2 1] Not reachable!

M' = [2 1 1 1 2 2] Not reachable!

Example

Is the marking $p_1 + 2p_2$ reachable? (why?)



T-invariants of T-nets

Proposition: Let N=(P,T,F) be a connected T-net.
J is a rational-valued T-invariant of N iff **J**=[x ... x]
for some rational value x

(the proof is dual to the analogous proposition for
S-invariants of S-nets)

Liveness theorem for T-systems

Theorem: A T-system (N,M_0) is live iff every circuit of N is marked at M_0

$\Rightarrow$) (quite obvious)
By contradiction, let γ be a circuit with $M_0(\gamma) = 0$.
By the fundamental property of T-systems: $\forall M \in [\, M_0 \,\rangle,\ M(\gamma) = 0$.

Take any $t \in T_{|\gamma}$ and $p \in P_{|\gamma} \cap \bullet t$.

For any $M \in [\, M_0 \,\rangle$, we have $M(p) = 0$.
Hence t is never enabled and the T-system is not live.

Liveness theorem for T-systems

Theorem: A T-system (N,M_0) is live iff every circuit of N is marked at M_0

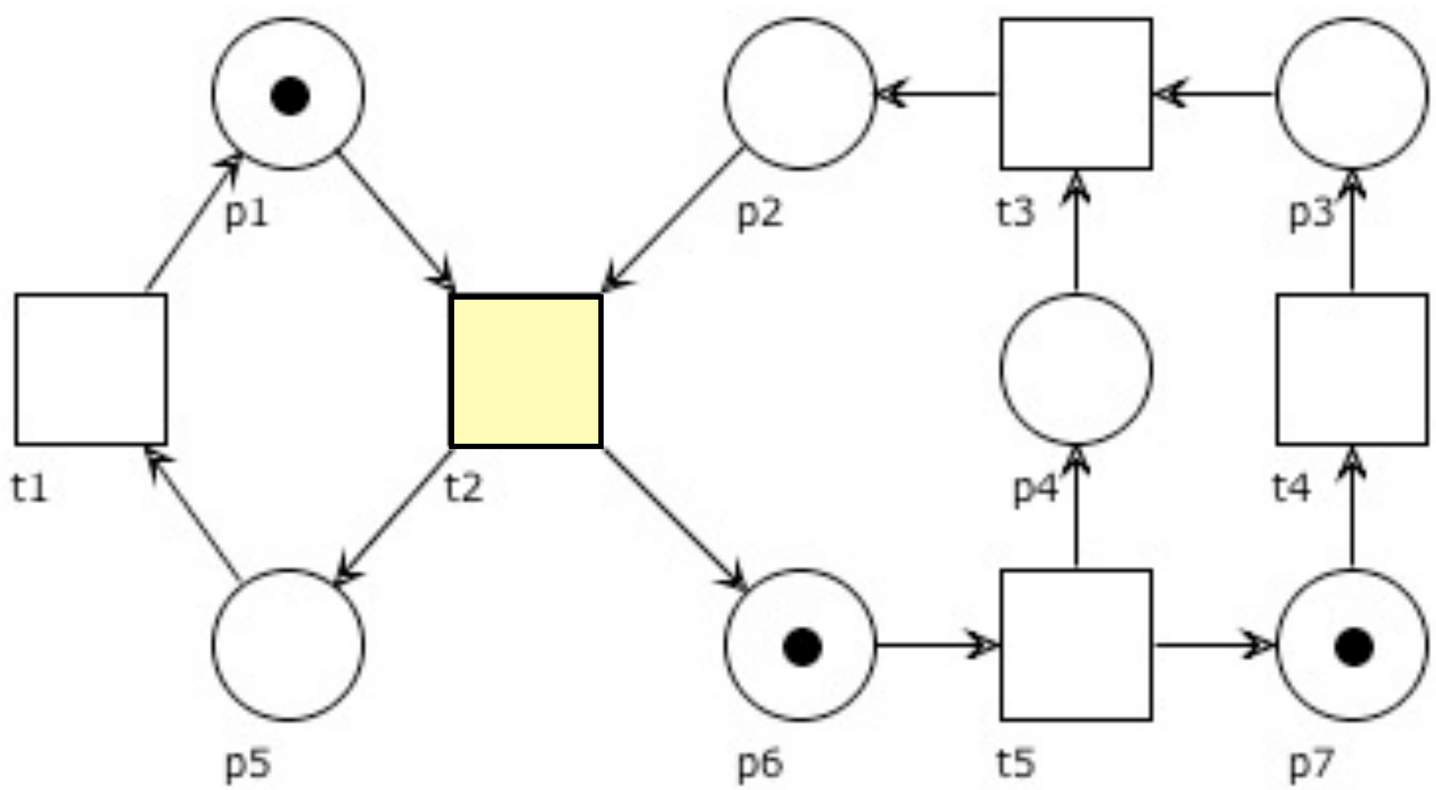
$\Leftarrow$) (more involved)
Take any $t \in T$ and $M \in [\, M_0 \,\rangle$.
We need to show that some marking M' reachable from M enables t.

The key idea is to collect the places that control the firing of t:
$p \in P_{M,t}$ if there is a path from p to t through places unmarked at M.
We then proceed by induction on the size of $P_{M,t}$.

We just sketch the key idea of the proof over a T-system.

Liveness theorem for T-systems

Theorem: A T-system (N,M_0) is live iff every circuit of N is marked at M_0

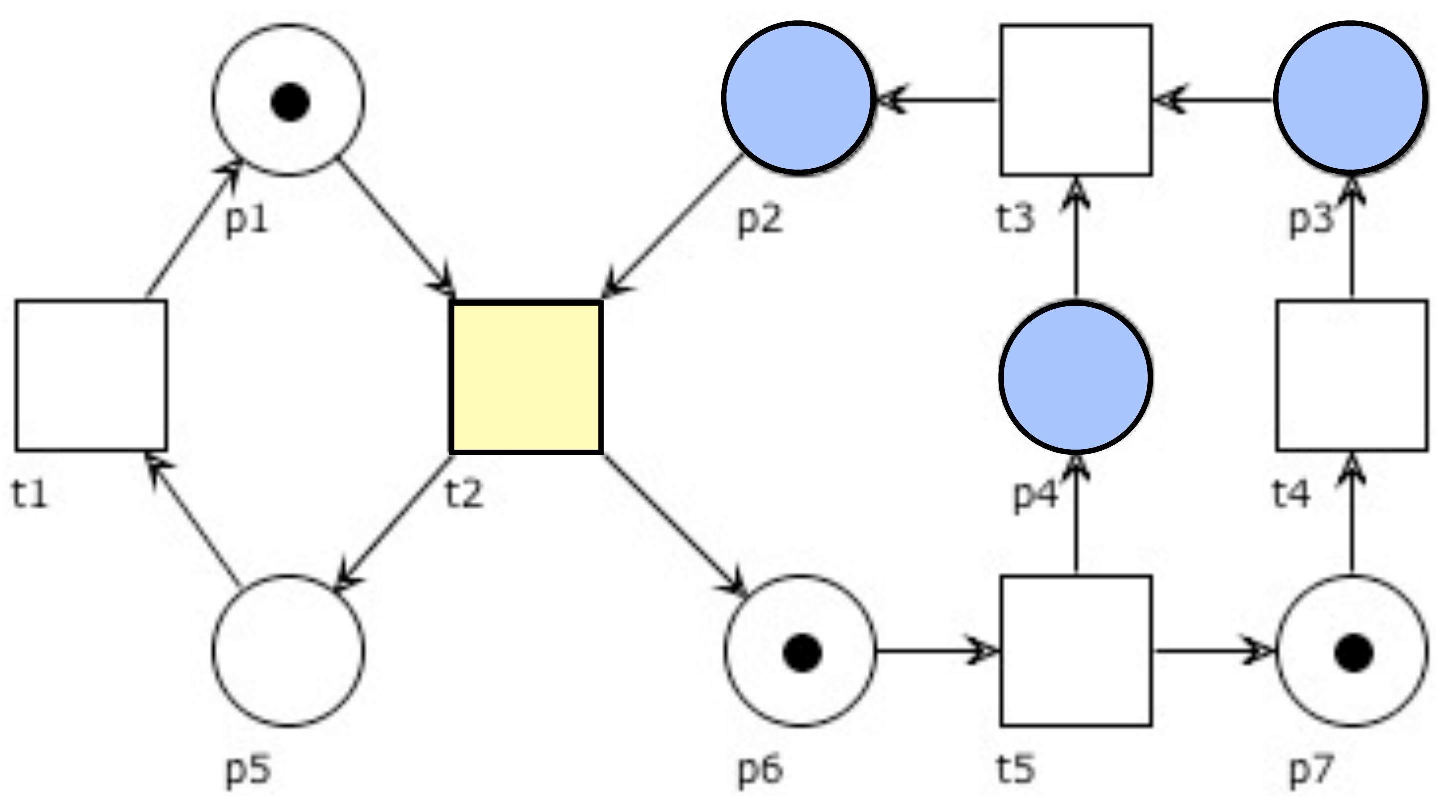


$M = p_1 + p_6 + p_7$

M' enabling t_2?

Liveness theorem for T-systems

Theorem: A T-system (N,M_0) is live iff every circuit of N is marked at M_0



$P_{M,t2} = \{ p_2, p_3, p_4 \}$

Liveness theorem for T-systems

Theorem: A T-system (N,M_0) is live iff every circuit of N is marked at M_0

$\Leftarrow$) (continued proof sketch)

Base case: $|P_{M,t}| = 0$.

Every place in $\bullet t$ is already marked at M.

Hence t is enabled at M.

Liveness theorem for T-systems

Theorem: A T-system (N,M_0) is live iff every circuit of N is marked at M_0

$\Leftarrow$) (continued proof sketch)

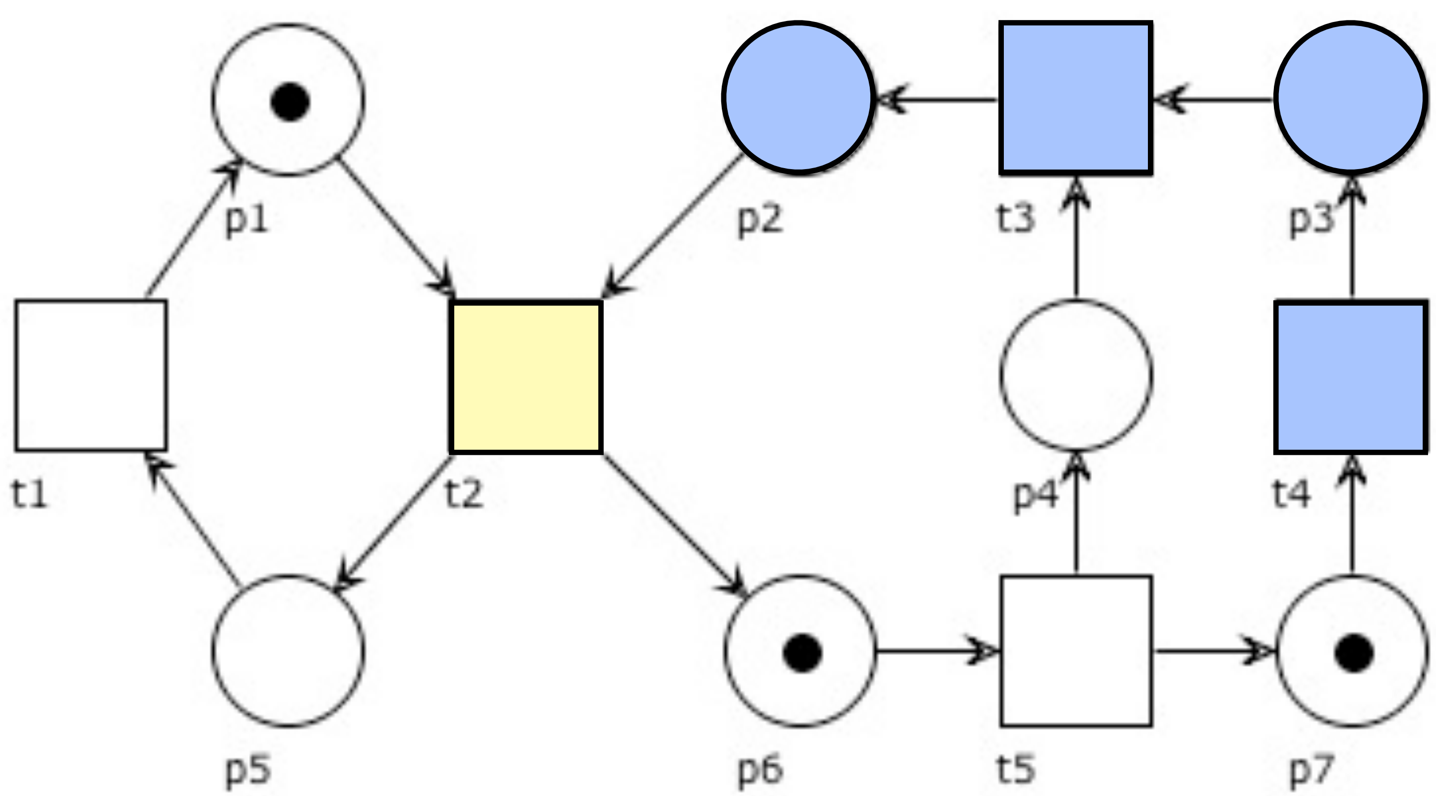
Inductive case: $|P_{M,t}| > 0$.
Therefore t is not enabled at M.

We look for a path π of maximal length necessary for firing t.
π must contain only places unmarked at M.

By the fundamental property of T-systems: all circuits are marked at M.
π is not necessarily unique, but exists (no cycle in it).

Liveness theorem for T-systems

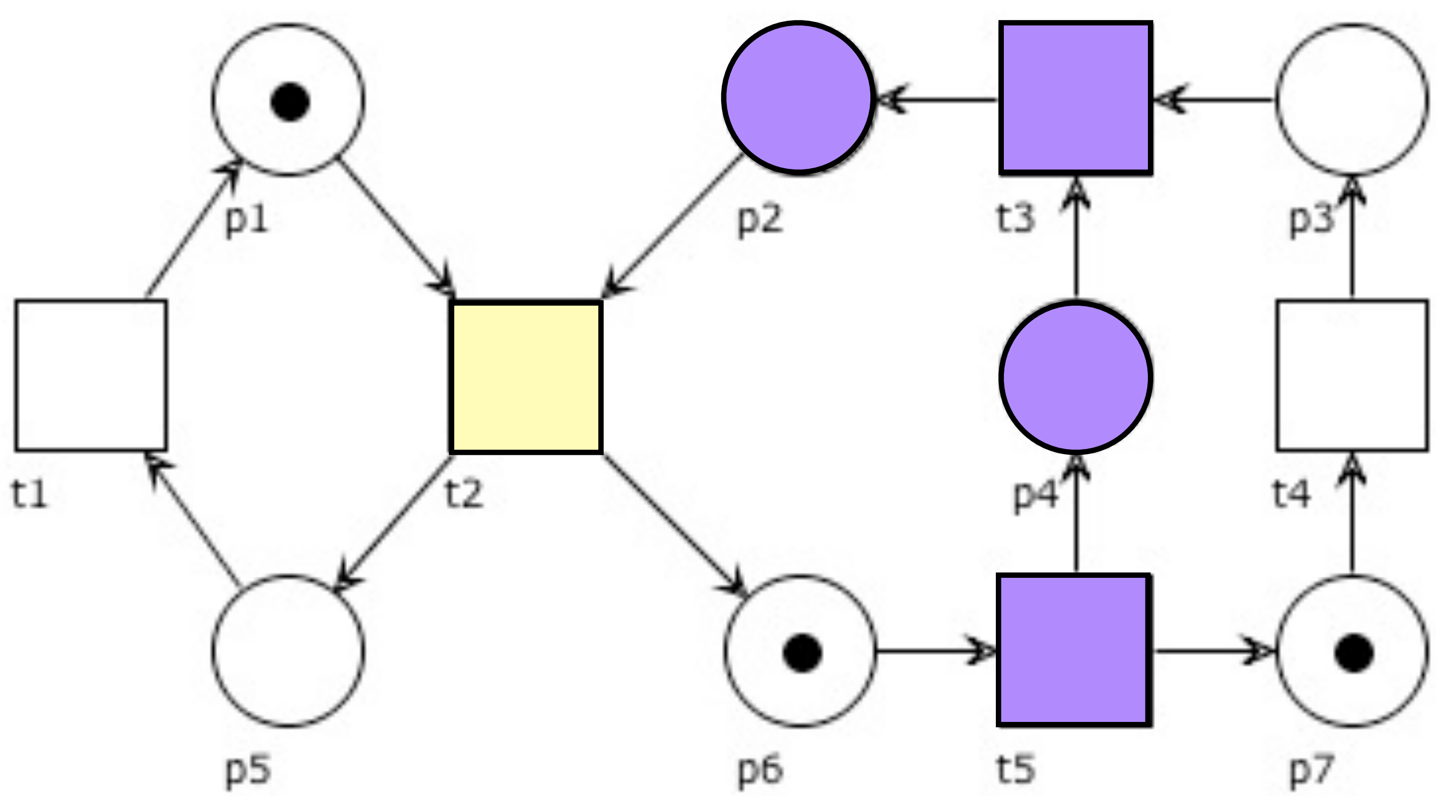
Theorem: A T-system (N,M_0) is live iff every circuit of N is marked at M_0



$$\pi = t_4\, p_3\, t_3\, p_2\, t_2$$

Liveness theorem for T-systems

Theorem: A T-system (N,M_0) is live iff every circuit of N is marked at M_0



$$\pi = t_5\, p_4\, t_3\, p_2\, t_2$$

Liveness theorem for T-systems

Theorem: A T-system (N,M_0) is live
iff every circuit of N is marked at M_0

$\Leftarrow$) (Inductive case: $|P_{M,t}| > 0$, continued proof sketch)

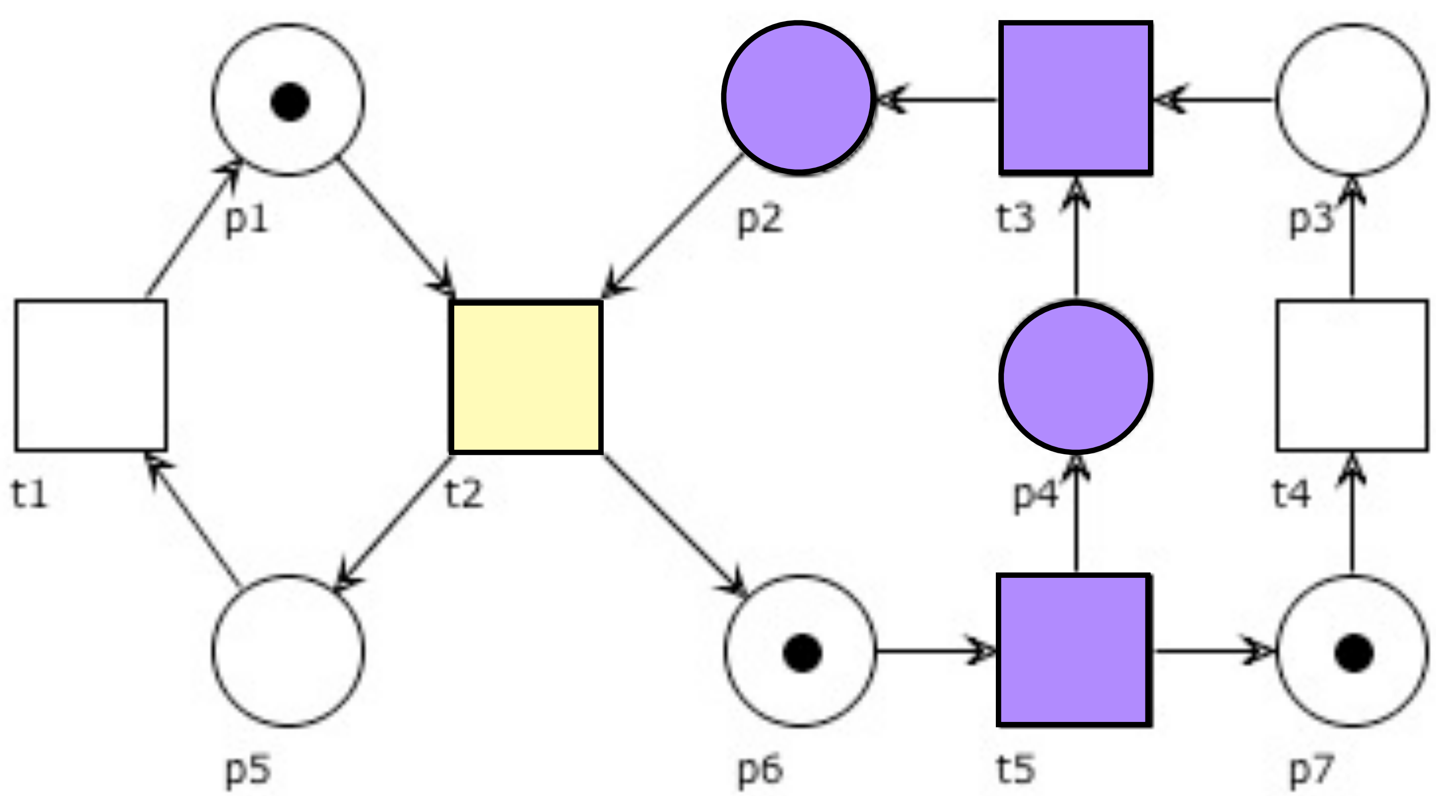
π begins with a transition t' enabled at M.
(otherwise a longer path could be found).

By firing t' we reach a marking M'' such that $P_{M'',t} \subset P_{M,t}$.

Hence $|P_{M'',t}| < |P_{M,t}|$ and we conclude by inductive hypothesis.

Liveness theorem for T-systems

Theorem: A T-system (N,M_0) is live iff every circuit of N is marked at M_0

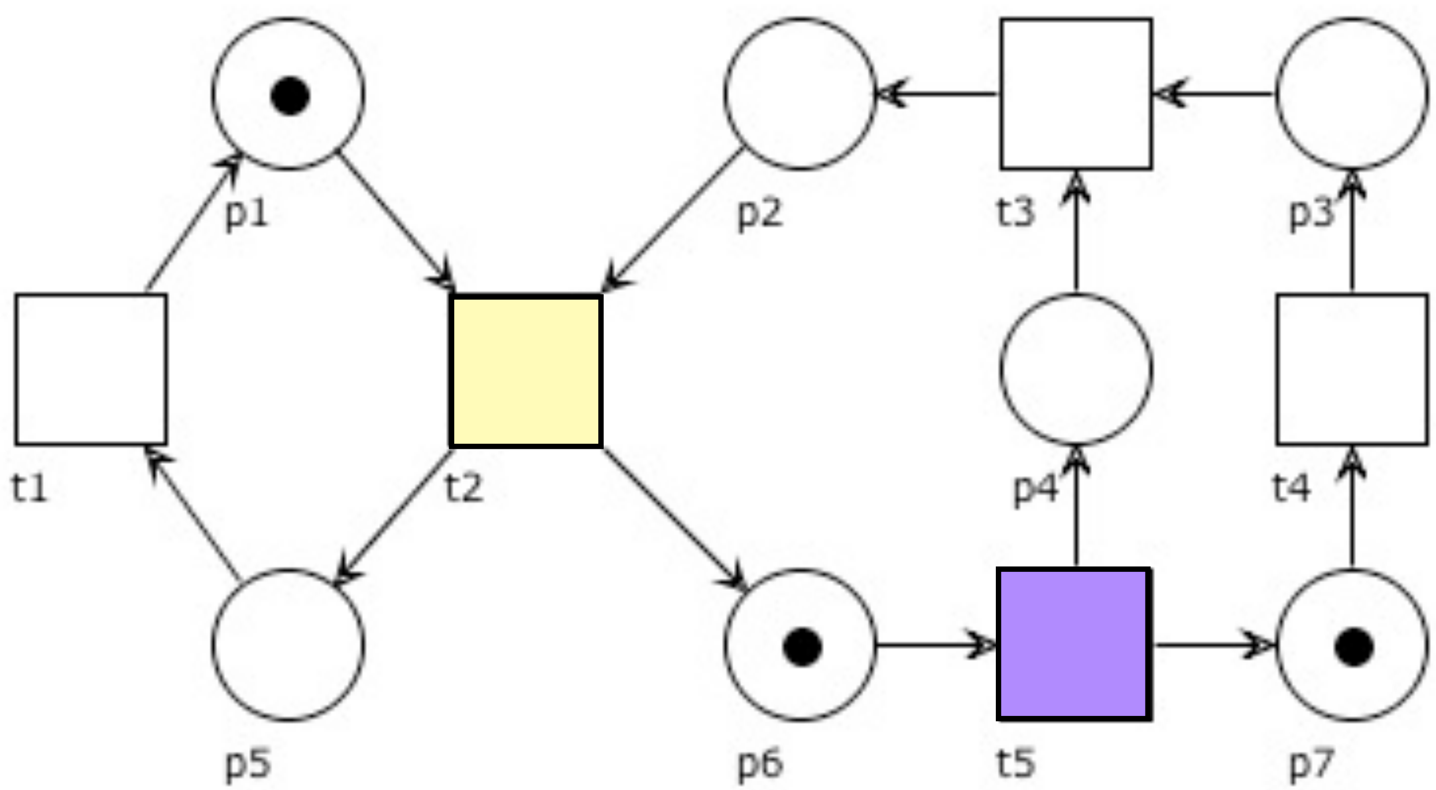


$P_{M,t2} = \{ p_2, p_3, p_4 \}$

$$\pi = t_5\, p_4\, t_3\, p_2\, t_2$$

Liveness theorem for T-systems

Theorem: A T-system (N,M_0) is live iff every circuit of N is marked at M_0

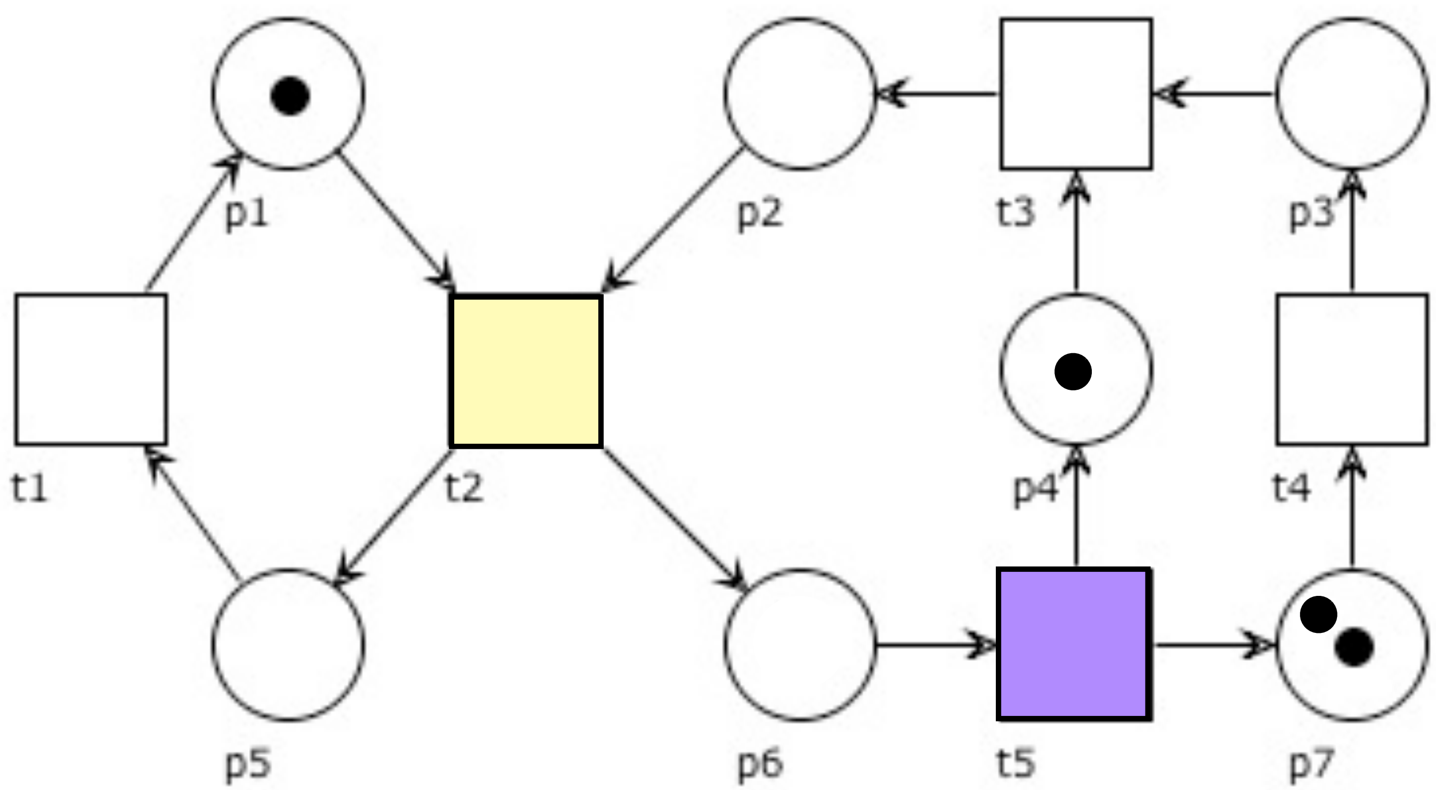


$P_{M,t2} = \{ p_2, p_3, p_4 \}$

$$\pi \ = \ t_5\, p_4\, t_3\, p_2\, t_2$$

Liveness theorem for T-systems

Theorem: A T-system (N,M_0) is live iff every circuit of N is marked at M_0

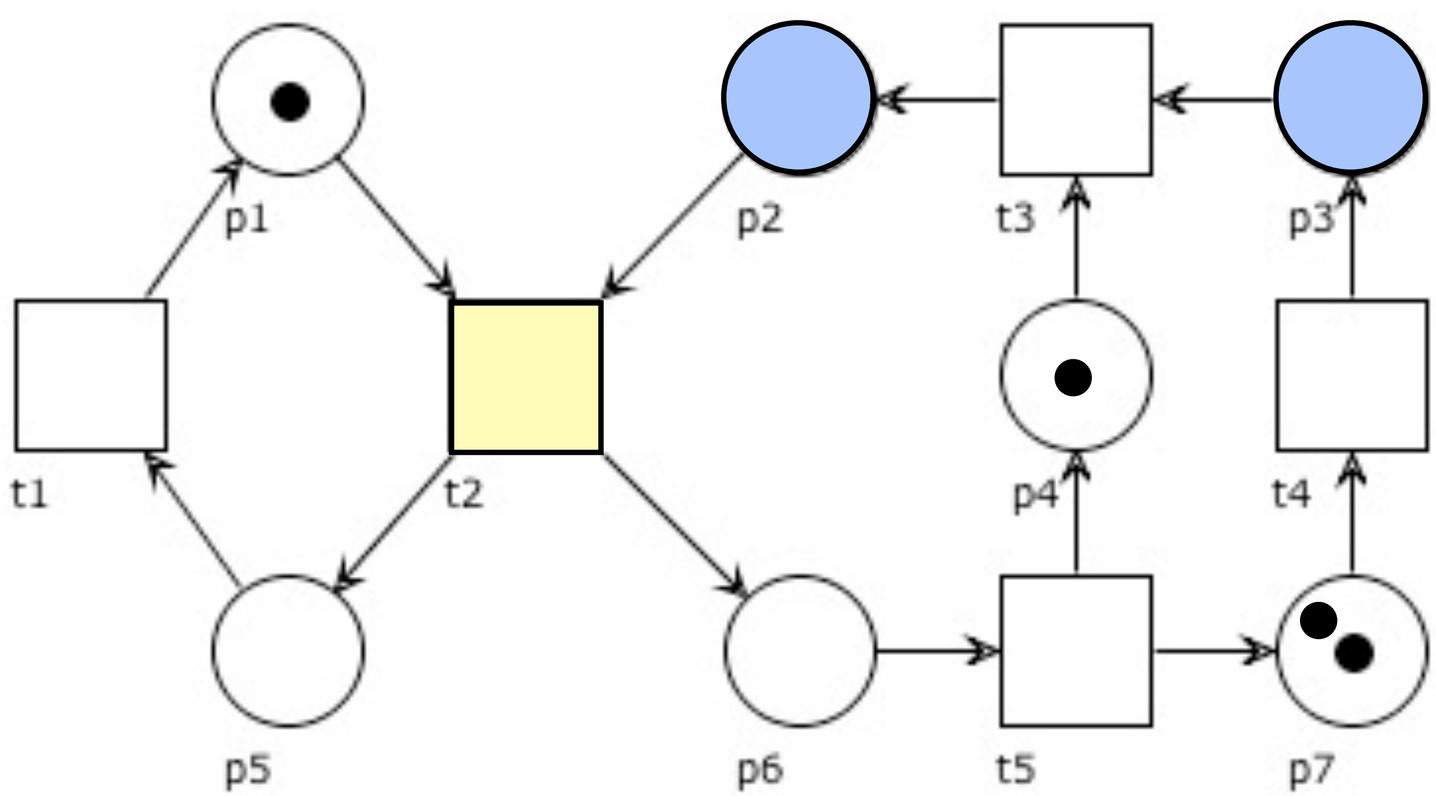


$P_{M,t2} = \{ p_2, p_3, p_4 \}$

$$\pi = t_5\, p_4\, t_3\, p_2\, t_2$$

Liveness theorem for T-systems

Theorem: A T-system (N,M_0) is live iff every circuit of N is marked at M_0

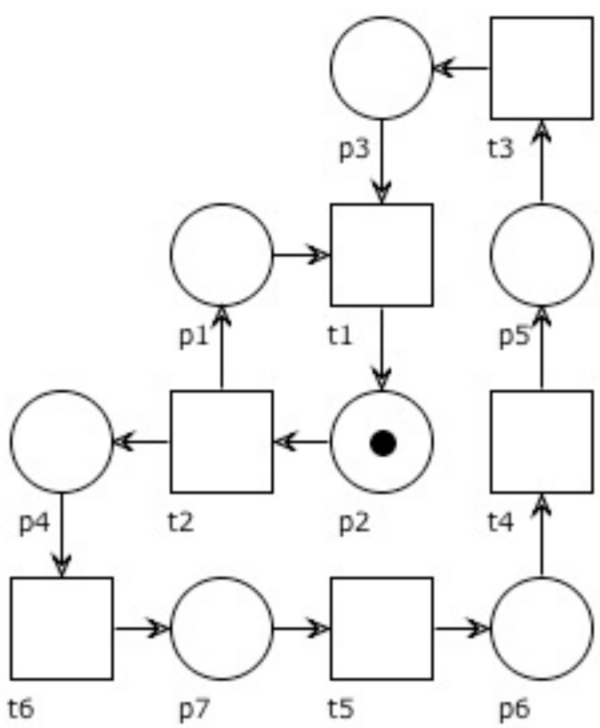


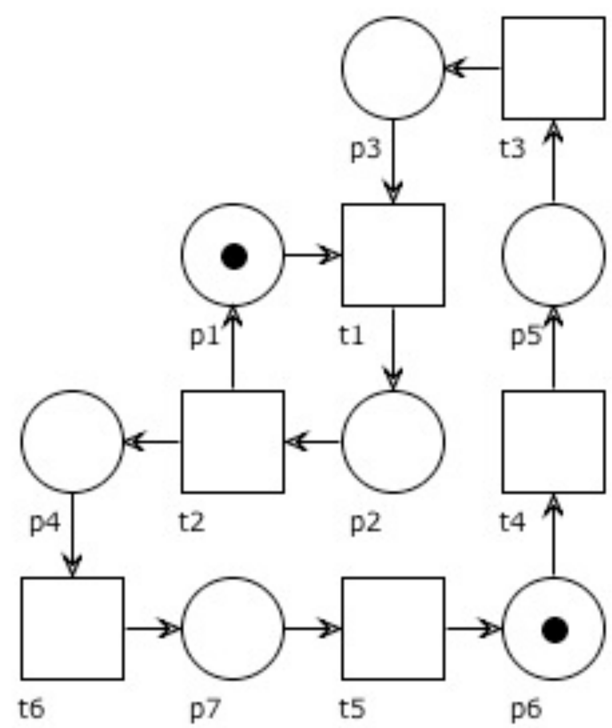
$P_{M,t2} = \{ p_2, p_3, p_4 \}$

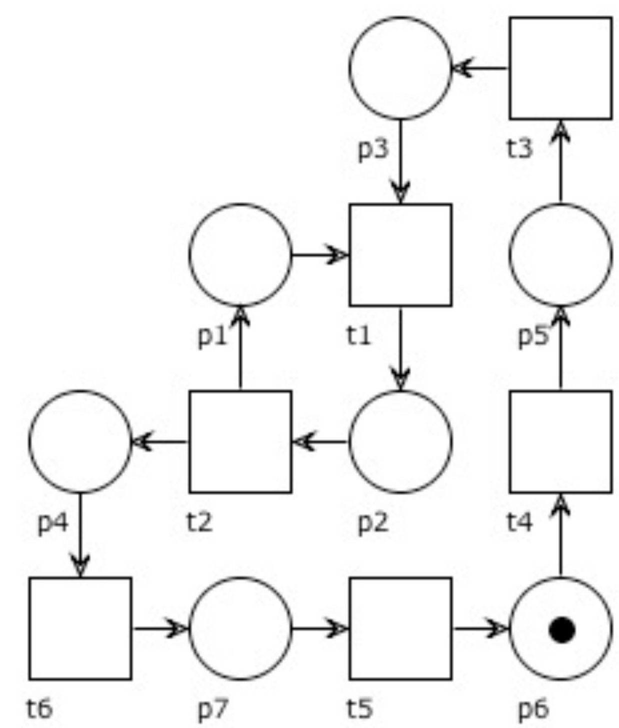
$P_{M'',t2} = \{ p_2, p_3 \}$

Example

Which of the T-systems below is live? (why?)







Boundedness theorem for live T-systems

Theorem: A live T-system (P, T, F, M_0) is k-bounded iff every place $p \in P$ belongs to a circuit γ_p with $M_0(\gamma_p) \leq k$.

$\Rightarrow$) Let $k_p \leq k$ be the bound of p.
Take $M \in [\, M_0 \,\rangle$ with $M(p) = k_p$.

Define $L = M - k_p p$ and note that the T-system (N, L) is not live.
(otherwise $L \xrightarrow{\sigma} L'$ with $L'(p) > 0$ for enabling $t \in p\bullet$. But then:
$M = L + k_p p \xrightarrow{\sigma} L' + k_p p = M'$ with $M'(p) = L'(p) + k_p > k_p$!)

By the liveness theorem: some circuit γ is not marked at L.
Since (N, M) is live, the circuit γ is marked at $M \supset L$.
Since $M - L = k_p p$, the circuit γ contains p and
$M_0(\gamma) = M(\gamma) = M(p) = k_p \leq k$.

Boundedness theorem for live T-systems

Theorem: A live T-system (P, T, F, M_0) is k-bounded iff every place $p \in P$ belongs to a circuit γ_p with $M_0(\gamma_p) \leq k$.

$\Leftarrow$) Let $M \in [\, M_0 \,\rangle$ and take any $p \in P$.

By the fundamental property of T-systems:
$M(p) \leq M(\gamma_p) = M_0(\gamma_p) \leq k$

Boundedness in strongly connected T-systems

Lemma: If a T-system (N,M_0) is strongly connected, then it is bounded

Let Γ be the set of the circuits of N and let $k = \max_{\gamma \in \Gamma} M_0(\gamma)$.

Since N is strongly connected, every place p belongs to some circuit γ_p.

By the fundamental property of T-systems: token count of γ_p is invariant.

Thus, for any reachable marking M, we have $M(p) \leq M(\gamma_p) = M_0(\gamma_p) \leq k$.
Hence the net is k-bounded.

Liveness in strongly connected T-systems

Lemma: If a T-system (N,M_0) is strongly connected, then it is live iff it is deadlock-free iff it has an infinite run

$\Longrightarrow$ $\Longrightarrow$

It is obvious that (for any net):
Liveness implies deadlock freedom.
Deadlock freedom implies the existence of an infinite run.

We show that (for strongly connected T-systems):
The existence of an infinite run implies liveness.

Liveness in strongly connected T-systems

Lemma: Let (N, M_0) be a strongly connected T-system. If it has an infinite run, then it is live

Since the T-system is strongly connected then it is bounded.

By the Reproduction lemma (holding for any bounded net):
There is a semi-positive T-invariant $\mathbf{J}$.
The support of $\mathbf{J}$ is included in the set of transitions of the infinite run σ.

By T-invariance in T-systems: $\langle \mathbf{J} \rangle = T$
(σ is an infinite run that contains all transitions).

Hence every transition can occur from M_0.
Hence every place can become marked.
Hence every circuit can become marked.

By the fundamental property of T-systems: every circuit is marked at M_0.

By the liveness theorem, (N, M_0) is live.

Place bounds in live T-systems

Let (P, T, F, M_0) be a live T-system.
We can draw some easy consequences of the above results:

1) If $p \in P$ is bounded, then it belongs to some circuit.
(see part $\Rightarrow$ of the proof of the boundedness theorem)

2) If $p \in P$ belongs to some circuit, then it is bounded.
(by the fundamental property of T-systems)

3) If (N, M_0) is bounded, then it is strongly connected.
(by strong connectedness theorem, holding for any system)

4) If N is strongly connected, then (N, M_0) is bounded.
(by 1, since any $p \in P$ belongs to a circuit by strong connectdness)

Place bounds in live T-systems

Let (P, T, F, M_0) be a live T-system.
We can draw some easy consequences of the above results:

1+2) $p \in P$ is bounded iff it belongs to some circuit.

3+4) (N, M_0) is bounded iff it is strongly connected.

T-systems: recap

T-system + M reachable + c circuit => $M(c) = M_0(c)$

T-system + $c_1 ... c_n$ circuits: $\exists i.\ p \in c_i$ <=> p bounded

T-system: $M(c)>0$ for all circuits c <=> live

T-system: strongly connected <=> bounded

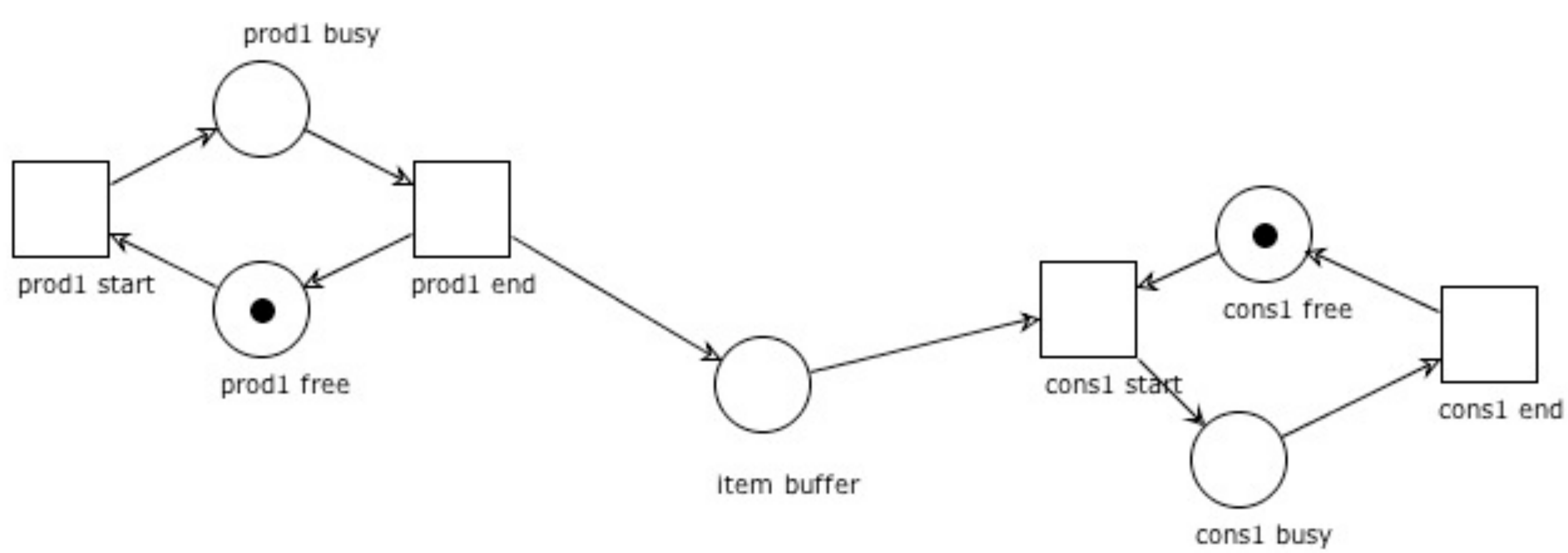
T-system + str. conn.: deadlock-free <=> live

T-system + str. conn.: infinite run <=> live

T-invariant **J** => **J** = [x x ... x]

Exercises

Which are the circuits of the T-system below?
Is the T-system below live? (why?)
Which places are bounded? (why?)
Assign a bound to each bounded place.



Exercises

Which are the circuits of the T-systems below?
Are the T-systems below live? (why?)
Which places are bounded? (why?)
Assign a bound to each bounded place.