Overview: Linear time behavior and property

Linear Time Properties

- state-based and linear time view
- definition of linear time properties
- invariants and safety
- liveness and fairness

State-based view of TS

transition system $\mathcal{T} = (S, Act, \longrightarrow, S_0, AP, L)$

$\downarrow$ abstraction from actions

state graph $G_{\mathcal{T}}$

- set of nodes = state space S
- edges = transitions without action label

Act for modeling interactions/communication

AP, L for specifying properties

State-based view of TS

transition system $\mathcal{T} = (S, Act, \longrightarrow, S_0, AP, L)$

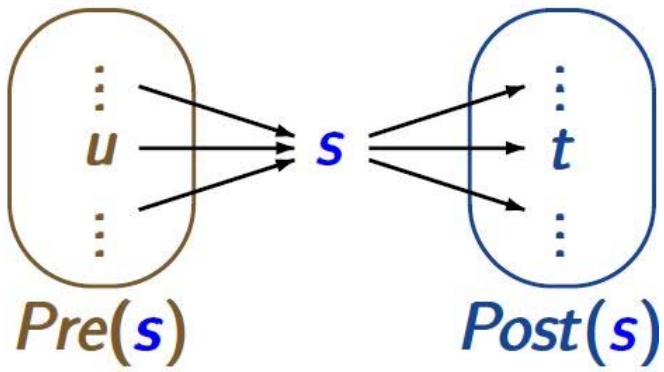
$\downarrow$ abstraction from actions

state graph $G_{\mathcal{T}}$

- set of nodes = state space S
- edges = transitions without action label

use standard notations
for graphs, e.g.,

$$Post(s) = \{t \in S : s \to t\}$$
$$Pre(s) = \{u \in S : u \to s\}$$



Execution and path fragments

execution fragment: sequence of consecutive transitions

$s_0 \xrightarrow{\alpha_0} s_1 \xrightarrow{\alpha_1} \ldots$ infinite or

$s_0 \xrightarrow{\alpha_0} s_1 \xrightarrow{\alpha_1} \ldots \xrightarrow{\alpha_{n-1}} s_n$ finite

path fragment: sequence of states arising from the projection of an execution fragment to the states

$\pi = s_0\, s_1\, s_2 \ldots$ infinite or $\pi = s_0\, s_1 \ldots s_n$ finite

such that $s_{i+1} \in Post(s_i)$ for all $i < |\pi|$

initial: if $s_0 \in S_0$ = set of initial states

maximal: if infinite or ending in a terminal state

Notations for paths

path fragment: sequence of states

$\pi = s_0\, s_1\, s_2 \ldots$ infinite or $\pi = s_0\, s_1 \ldots s_n$ finite

s.t. $s_{i+1} \in Post(s_i)$ for all $i < |\pi|$

initial: if $s_0 \in S_0$ = set of initial states

maximal: if infinite or ending in terminal state

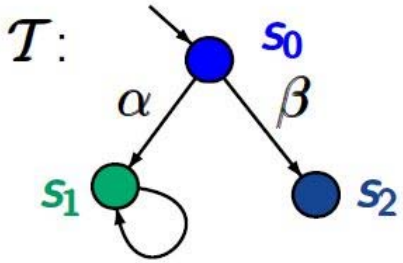
path of TS $\mathcal{T}$ $\widehat{=}$ initial, maximal path fragment

path of state s $\widehat{=}$ maximal path fragment starting in state s

$Paths(\mathcal{T})$ = set of all initial, maximal path fragments

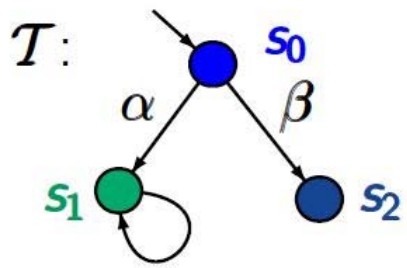
$Paths(s)$ = set of all maximal path fragments starting in state s

Paths of a TS



How many paths are there in $\mathcal{T}$?

Paths of a TS and its states

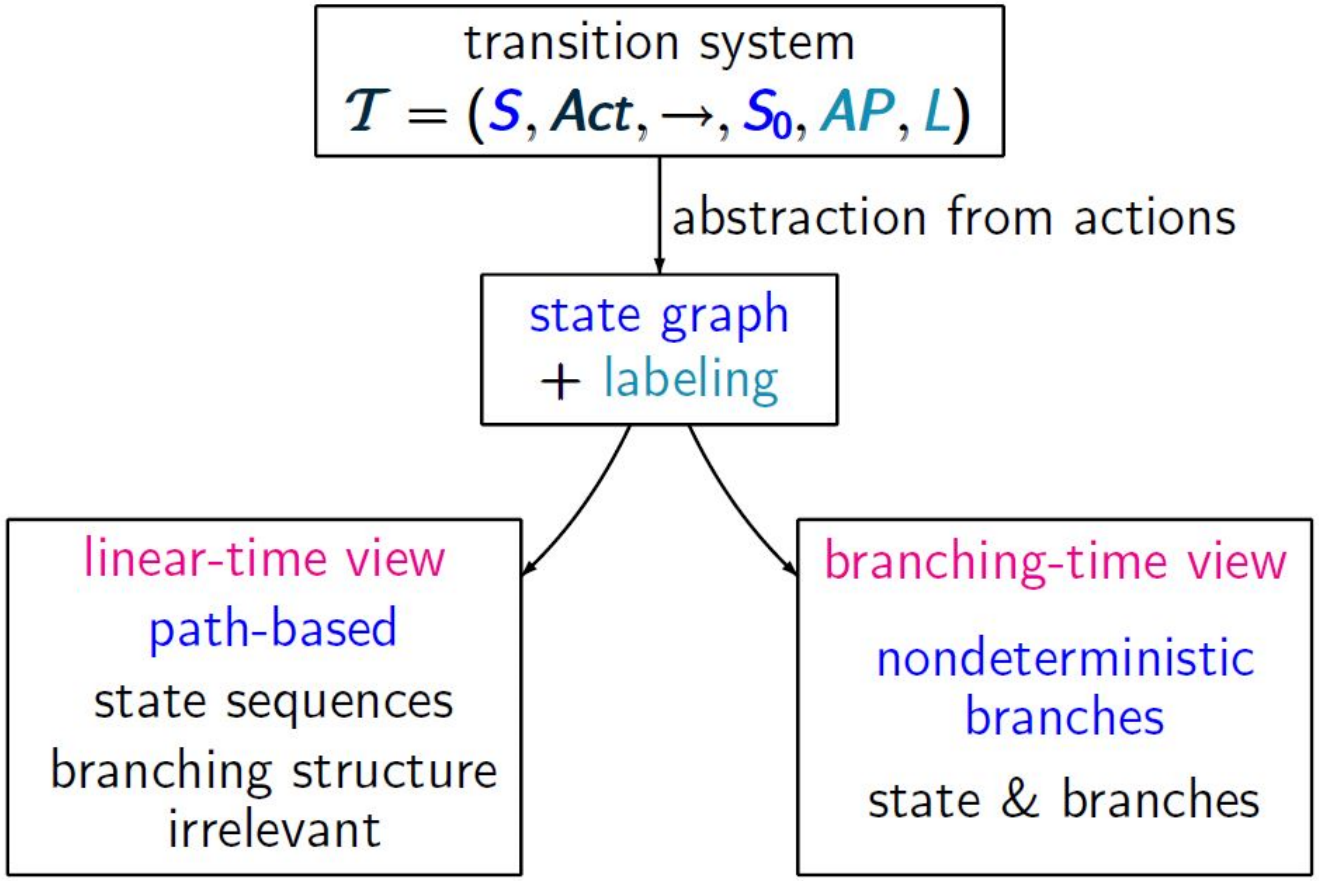


How many paths are there in $\mathcal{T}$?

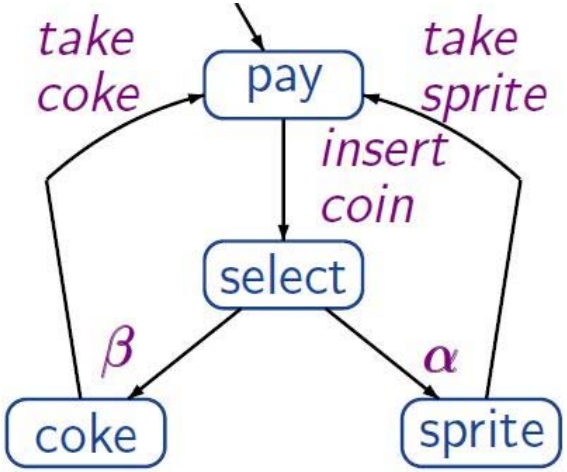
answer: 2, namely $s_0\, s_1\, s_1\, s_1 \ldots$ and $s_0\, s_2$

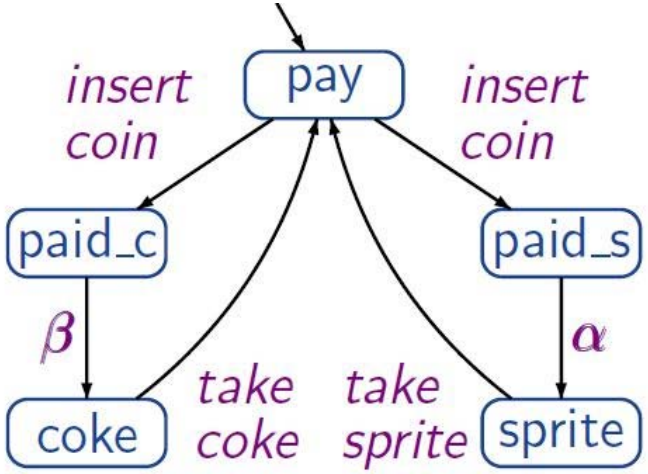
$Paths(s_1)$	$=$ set of all maximal paths fragments starting in s_1 $= \{s_1^\omega\}$ where $s_1^\omega = s_1\, s_1\, s_1\, s_1\, \ldots$
$Paths_{fin}(s_1)$	$=$ set of all finite path fragments starting in s_1 $= \{s_1^n : n \in \mathbb{N}, n \geq 1\}$

Linear-time vs branching-time



Example: vending machine

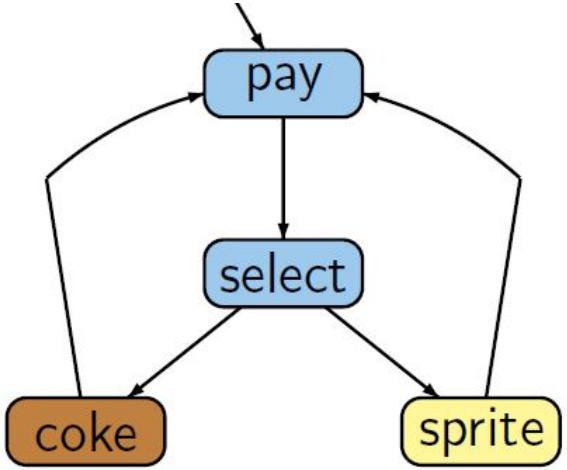


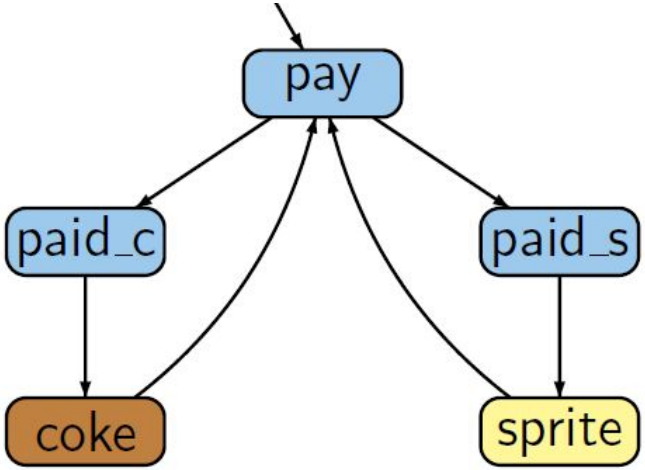


vending machine with
1 coin deposit
select drink after
having paid

vending machine with
2 coin deposits
select drink by inserting
the coin

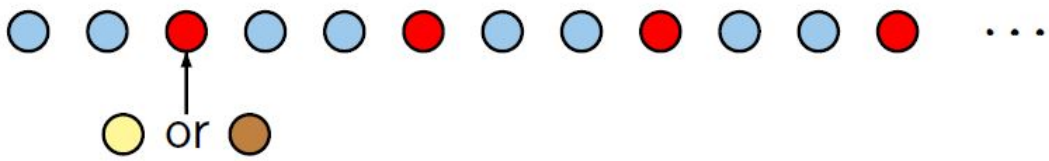
Example: vending machine



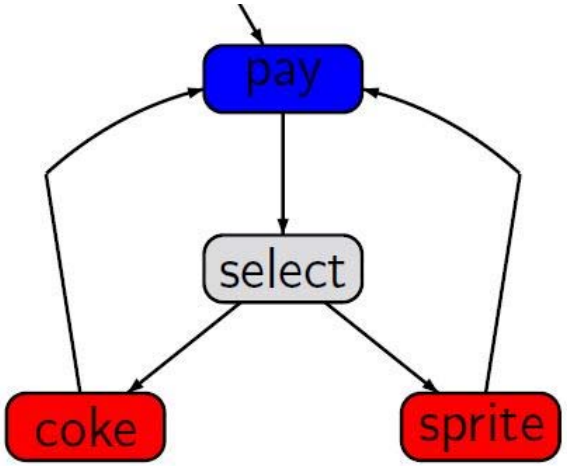


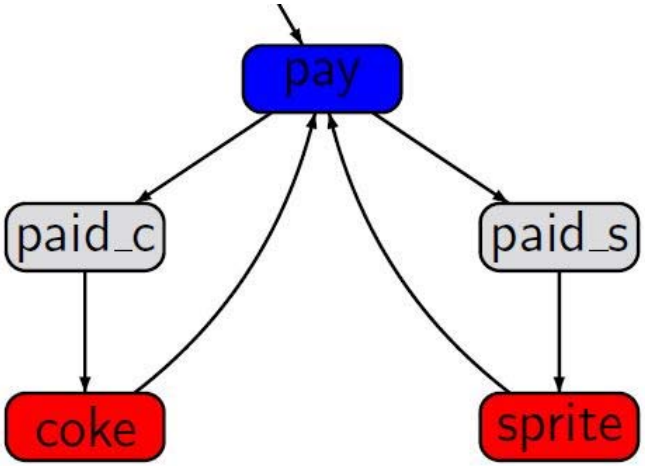
state based view: abstracts from actions and projects onto atomic propositions, e.g. $AP = \{coke, sprite\}$

linear time: all observable behaviors are of the form



Example: vending machine



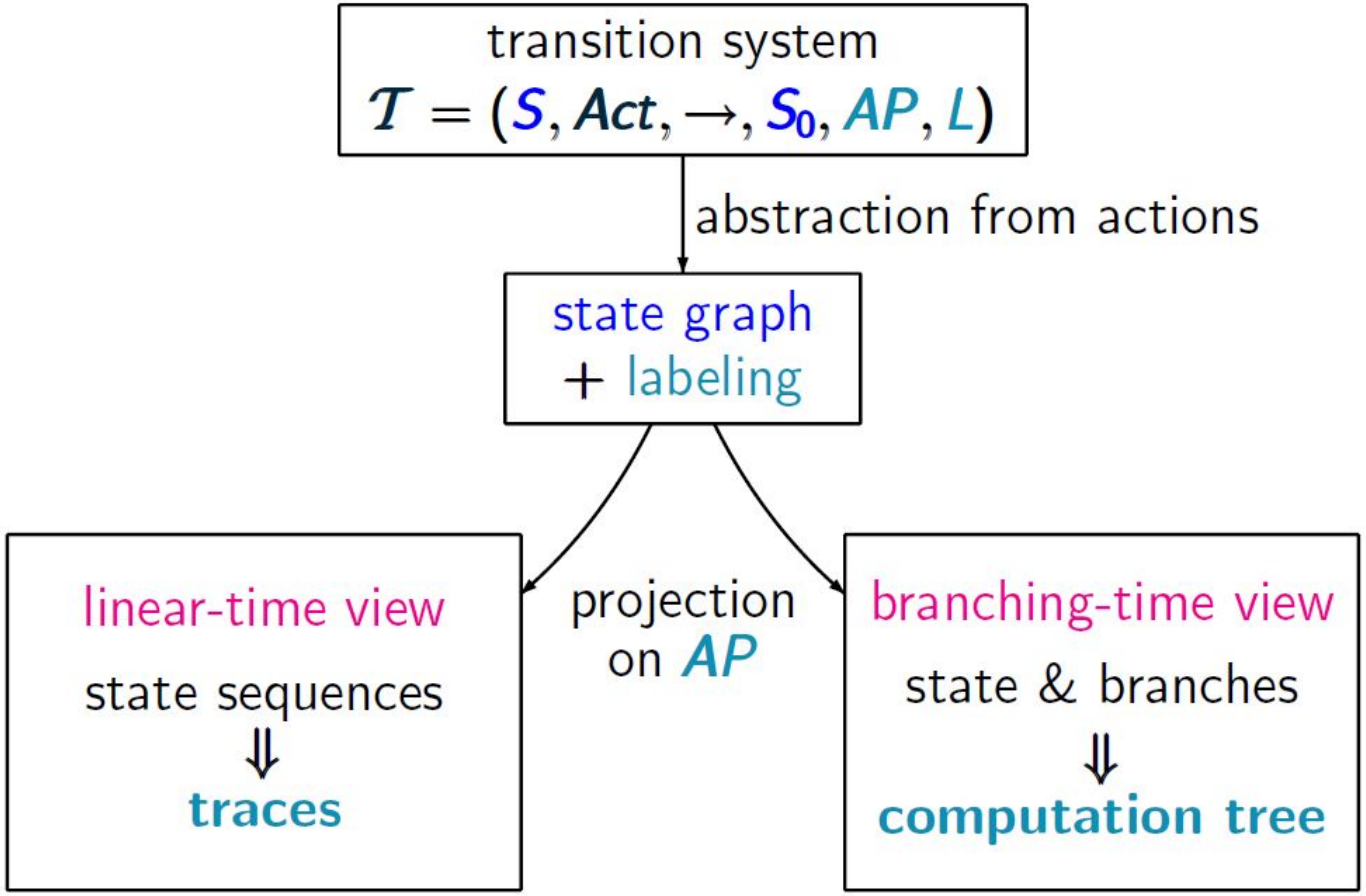


state based view: abstracts from actions and projects on atomc propositions, e.g., $AP = \{pay, drink\}$

linear & branching time:

all observable behaviors have the form

Linear-time vs branching-time



Traces

for TS with labeling function $L : S \to 2^{AP}$

execution: states + actions

$s_0 \xrightarrow{\alpha_1} s_1 \xrightarrow{\alpha_2} s_2 \xrightarrow{\alpha_3} \ldots$ infinite or finite

↓

paths: sequences of states

$s_0\, s_1\, s_2 \ldots$ infinite or $s_0\, s_1 \ldots s_n$ finite

↓

traces: sequences of sets of atomic propositions

$L(s_0)\, L(s_1)\, L(s_2) \ldots \quad \in (2^{AP})^\omega \cup (2^{AP})^+$

for simplicity: we often assume that the given TS has **no terminal states**

Traces

for TS with labeling function $L : S \to 2^{AP}$

execution: states + actions

$s_0 \xrightarrow{\alpha_1} s_1 \xrightarrow{\alpha_2} s_2 \xrightarrow{\alpha_3} \ldots$ infinite or ~~finite~~

paths: sequences of states

$s_0\, s_1\, s_2 \ldots$ infinite or ~~$s_0\, s_1 \ldots s_n$ finite~~

traces: sequences of sets of atomic propositions

$L(s_0)\, L(s_1)\, L(s_2) \ldots \in (2^{AP})^\omega \cup \cancel{(2^{AP})^+}$

for simplicity: we often assume that the given TS has **no terminal states**

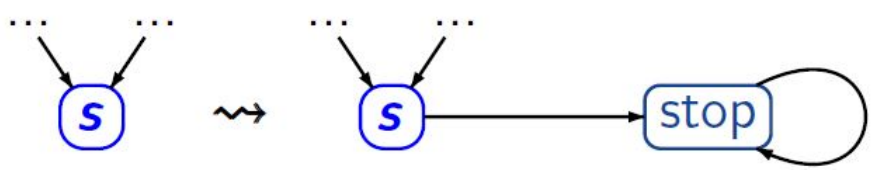
Treatment of terminal states

perform standard graph algorithms to compute the reachable fragment of the given TS

$$\mathit{Reach}(\mathcal{T}) = \left\{ \begin{array}{c} \text{set of states that are reachable} \\ \text{from some initial state} \end{array} \right.$$

for each reachable terminal state s:

- if s stands for an intended halting configuration then add a transition from s to a trap state:



- if s stands for system fault, e.g., deadlock then correct the design before checking further properties

Traces of a TS

Let $\mathcal{T}$ be a TS $\longleftarrow$ *without* terminal states

$$\mathit{Traces}(\mathcal{T}) \stackrel{\text{def}}{=} \{\mathit{trace}(\pi) : \pi \in \mathit{Paths}(\mathcal{T})\} \subseteq (2^{AP})^{\omega}$$

initial, infinite path fragment

$$\mathit{Traces}_{fin}(\mathcal{T}) \stackrel{\text{def}}{=} \{\mathit{trace}(\widehat{\pi}) : \widehat{\pi} \in \mathit{Paths}_{fin}(\mathcal{T})\} \subseteq (2^{AP})^{*}$$

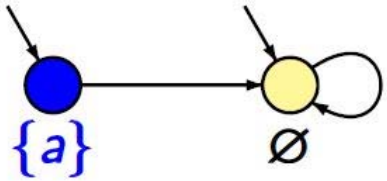
initial, finite path fragment

Example: traces

Let $\mathcal{T}$ be a TS without terminal states.

$$\mathit{Traces}(\mathcal{T}) \stackrel{\text{def}}{=} \{\mathit{trace}(\pi) : \pi \in \mathit{Paths}(\mathcal{T})\} \subseteq (2^{AP})^\omega$$

$$\mathit{Traces}_{fin}(\mathcal{T}) \stackrel{\text{def}}{=} \{\mathit{trace}(\widehat{\pi}) : \widehat{\pi} \in \mathit{Paths}_{fin}(\mathcal{T})\} \subseteq (2^{AP})^*$$

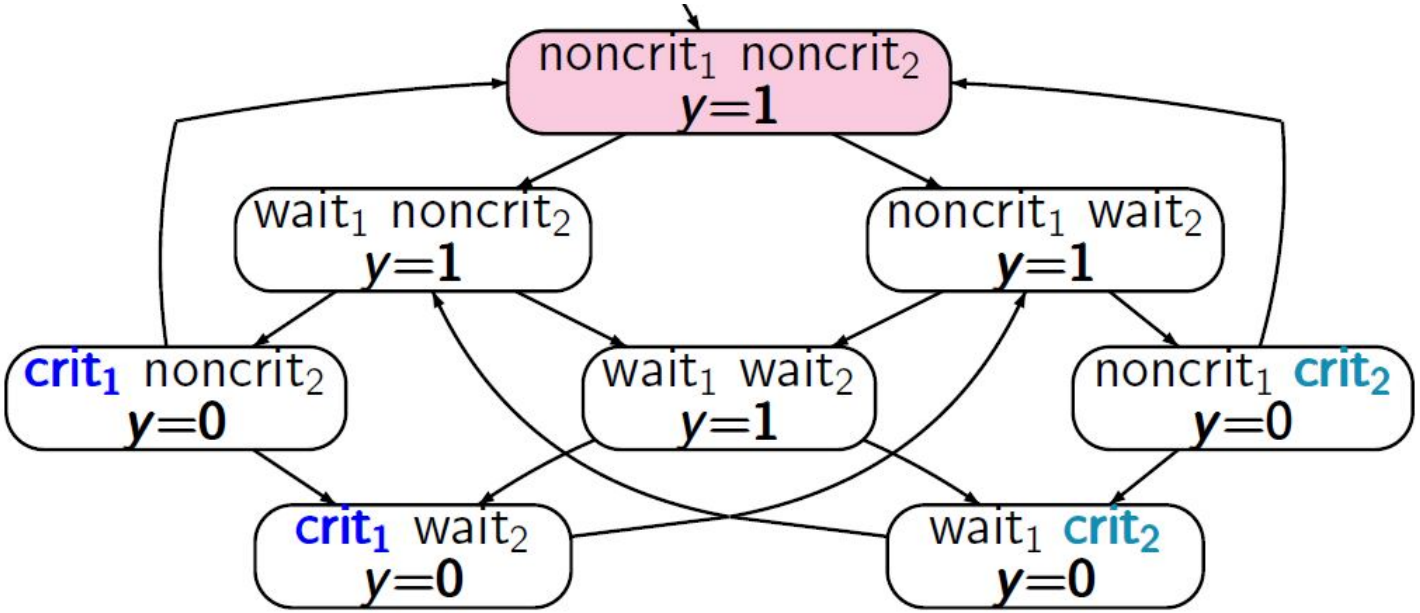


TS $\mathcal{T}$ with a single atomic proposition a

$$\mathit{Traces}(\mathcal{T}) = \{\, \{a\}\varnothing^\omega, \varnothing^\omega \,\}$$

$$\mathit{Traces}_{fin}(\mathcal{T}) = \{\{a\}\varnothing^n : n \geq 0\} \cup \{\varnothing^m : m \geq 1\}$$

Mutual exclusion with semaphore

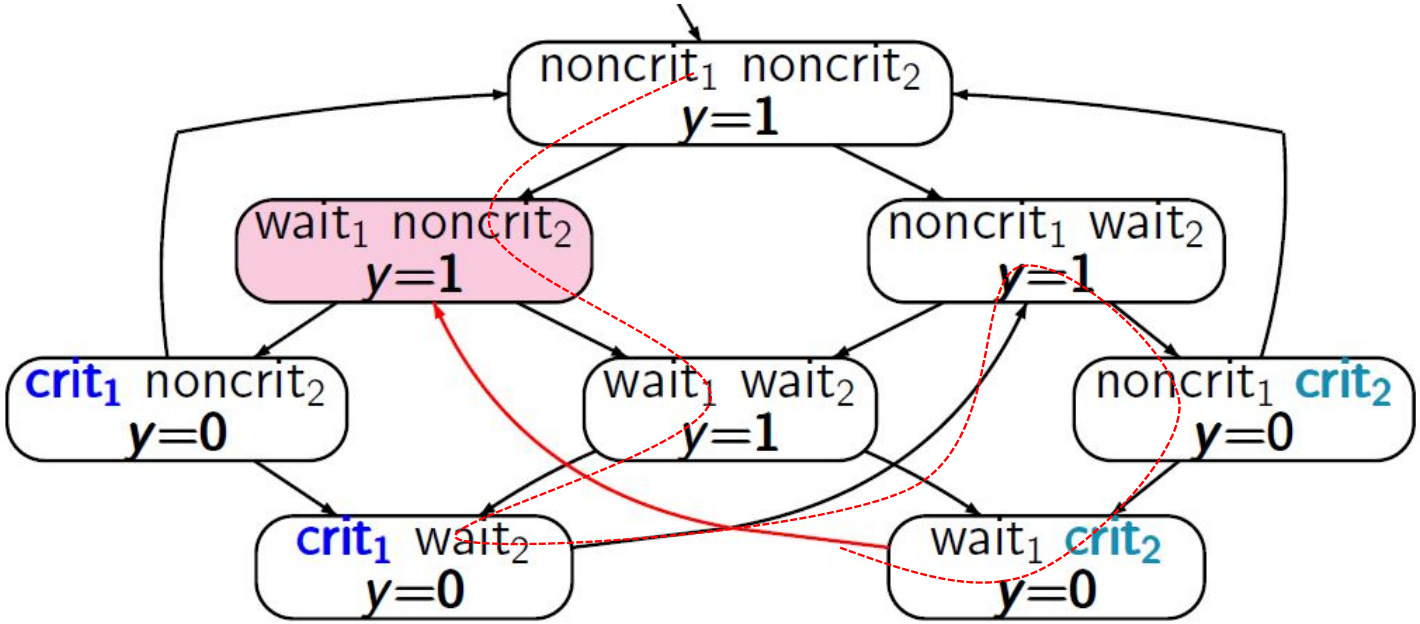


set of atomic propositions $AP = \{\text{crit}_1, \text{crit}_2\}$

traces, e.g., $\varnothing\ \varnothing\ \{\text{crit}_1\}\ \varnothing\ \varnothing\ \{\text{crit}_1\}\ \varnothing\ \varnothing\ \{\text{crit}_1\} \ldots$

$\varnothing\ \varnothing\ \varnothing\ \{\text{crit}_1\}\ \varnothing\ \{\text{crit}_2\}\ \{\text{crit}_2\}\ \varnothing \ldots$

Mutual exclusion with semaphore

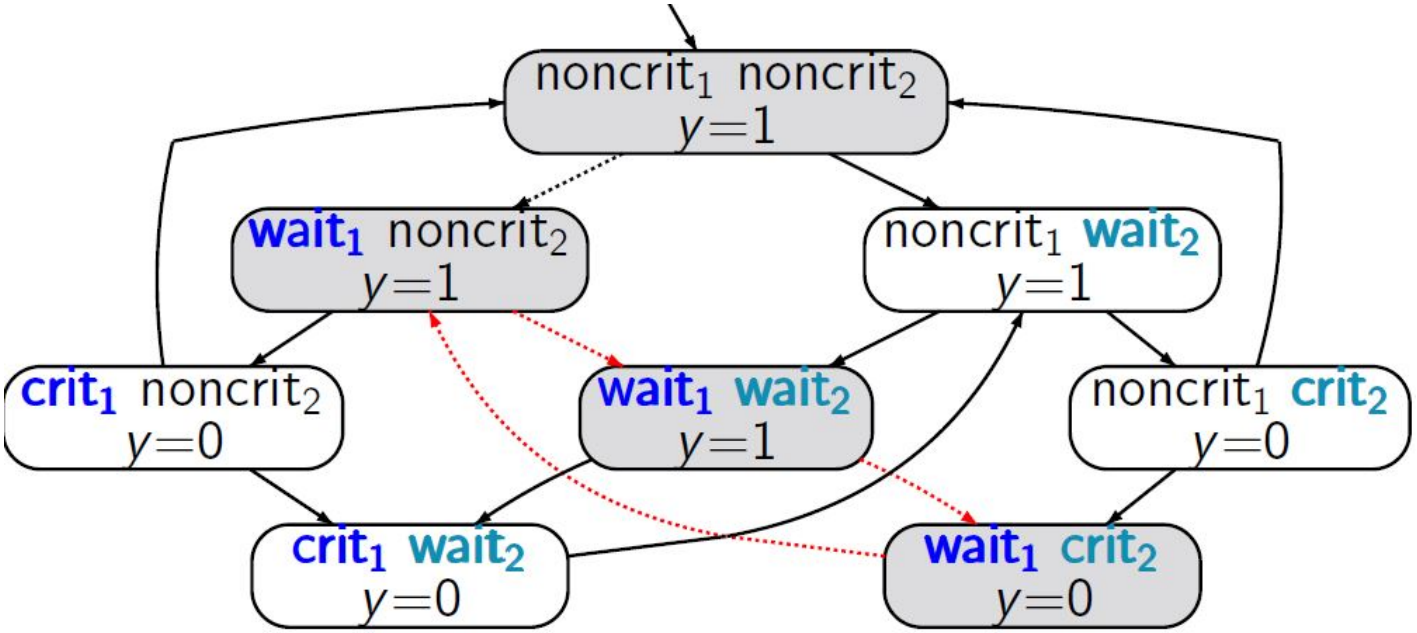


set of atomic propositions $AP = \{\text{crit}_1, \text{crit}_2\}$

traces, e.g., $\varnothing\ \varnothing\ \{\text{crit}_1\}\ \varnothing\ \varnothing\ \{\text{crit}_1\}\ \varnothing\ \varnothing\ \{\text{crit}_1\}\ \ldots$

$\varnothing\ \varnothing\ \varnothing\ \{\text{crit}_1\}\ \varnothing\ \{\text{crit}_2\}\ \{\text{crit}_2\}\ \varnothing\ \ldots$

Mutual exclusion with semaphore



set of propositions $AP = \{\text{wait}_1, \text{crit}_1, \text{wait}_2, \text{crit}_2\}$

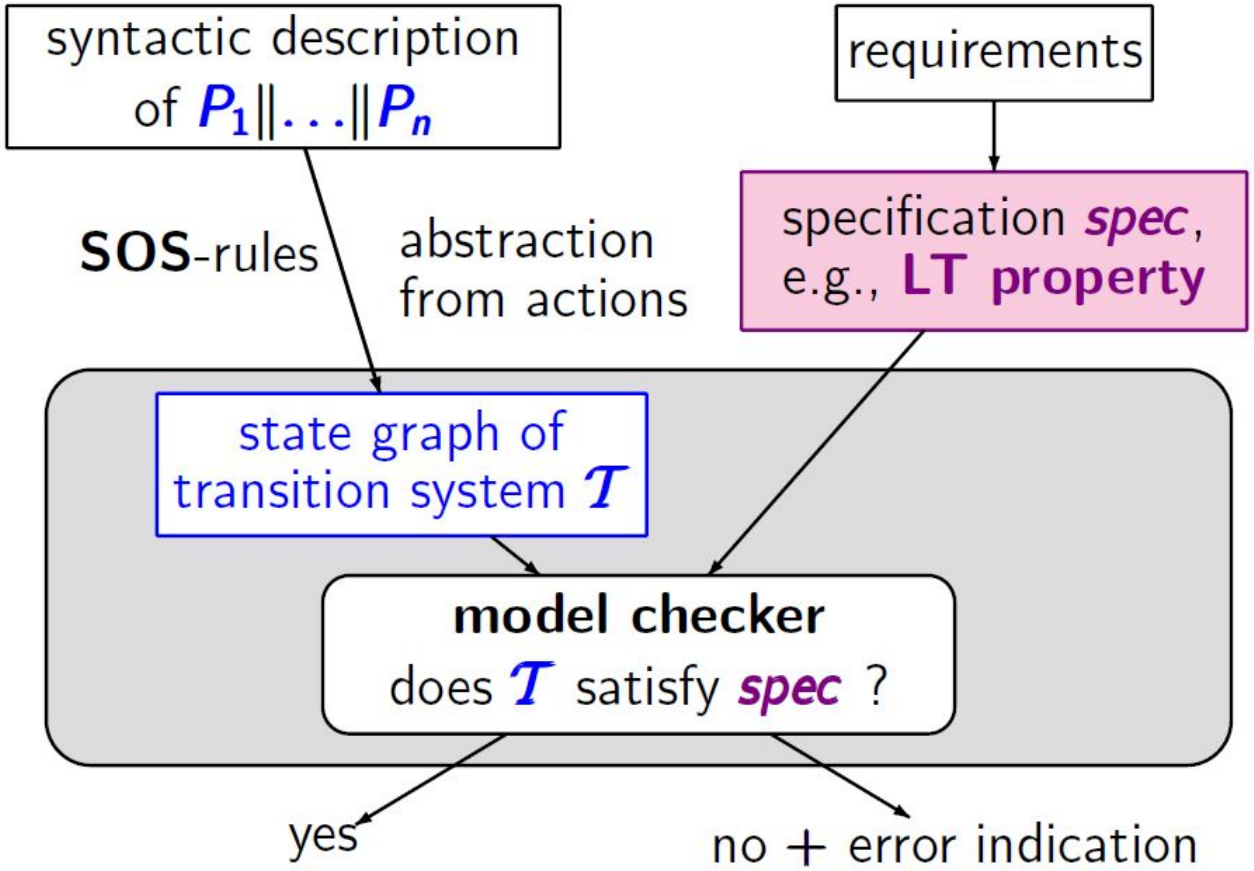
traces, e.g.,

$$\varnothing \left(\{\text{wait}_1\}\,\{\text{wait}_1, \text{wait}_2\}\,\{\text{wait}_1, \text{crit}_2\}\right)^{\omega}$$

Linear Time Properties

- state-based and linear time view
- definition of linear time properties
- invariants and safety
- liveness and fairness

Model checking



Linear-time properties (LT properties)

for TS over AP without terminal states

An LT property over AP is a language E of infinite words over the alphabet $\Sigma = 2^{AP}$, i.e., $E \subseteq \left(2^{AP}\right)^{\omega}$.

E.g., for mutual exclusion problems and
$AP = \{\mathrm{crit}_1, \mathrm{crit}_2, \ldots\}$

safety:

$$MUTEX = \begin{array}{l} \text{set of all infinite words } A_0\, A_1\, A_2 \ldots \\ \text{over } 2^{AP} \text{ such that for all } i \in \mathbb{N}: \\ \quad \mathrm{crit}_1 \notin A_i \;\text{ or }\; \mathrm{crit}_2 \notin A_i \end{array}$$

LP properties for MUTEX

$AP = \{\mathbf{wait}_1, \mathbf{crit}_1, \mathbf{wait}_2, \mathbf{crit}_2\}$

safety:

$$MUTEX = \begin{array}{l} \text{set of all infinite words } A_0\, A_1\, A_2 \ldots \\ \text{over } 2^{AP} \text{ such that for all } i \in \mathbb{N}: \\ \quad \mathbf{crit}_1 \notin A_i \;\text{ or }\; \mathbf{crit}_2 \notin A_i \end{array}$$

$\varnothing\ \{\mathbf{wait}_1\}\ \{\mathbf{crit}_1\}\ \varnothing\ \{\mathbf{wait}_1\}\ \{\mathbf{crit}_1\}\ \ldots \quad \in MUTEX$

$\varnothing\ \{\mathbf{wait}_1\}\ \{\mathbf{crit}_1\}\ \{\mathbf{crit}_1, \mathbf{wait}_2\}\ \{\mathbf{crit}_1, \mathbf{crit}_2\}\ \ldots \quad \notin MUTEX$

$\varnothing\ \varnothing\ \{\mathbf{wait}_1, \mathbf{crit}_1, \mathbf{crit}_2\}\ \ldots \quad \notin MUTEX$

LP properties for MUTEX

$AP = \{\mathbf{wait}_1, \mathbf{crit}_1, \mathbf{wait}_2, \mathbf{crit}_2\}$

safety:

$$MUTEX = \begin{array}{l} \text{set of all infinite words } A_0\, A_1\, A_2 \ldots \\ \text{over } 2^{AP} \text{ such that for all } i \in \mathbb{N}: \\ \quad \mathbf{crit}_1 \notin A_i \;\text{ or }\; \mathbf{crit}_2 \notin A_i \end{array}$$

liveness (starvation freedom):

$$LIVE = \begin{array}{l} \text{set of all infinite words } A_0\, A_1\, A_2 \ldots \text{ s.t.} \\ \quad \overset{\infty}{\exists}\, i \in \mathbb{N}.\mathbf{wait}_1 \in A_i \implies \overset{\infty}{\exists}\, i \in \mathbb{N}.\mathbf{crit}_1 \in A_i \\ \wedge\; \overset{\infty}{\exists}\, i \in \mathbb{N}.\mathbf{wait}_2 \in A_i \implies \overset{\infty}{\exists}\, i \in \mathbb{N}.\mathbf{crit}_2 \in A_i \end{array}$$

Satisfaction relation for LT properties

An LT property over AP is a language E of infinite words over the alphabet $\Sigma = 2^{AP}$, i.e., $E \subseteq (2^{AP})^{\omega}$.

Satisfaction relation $\models$ for TS and states:

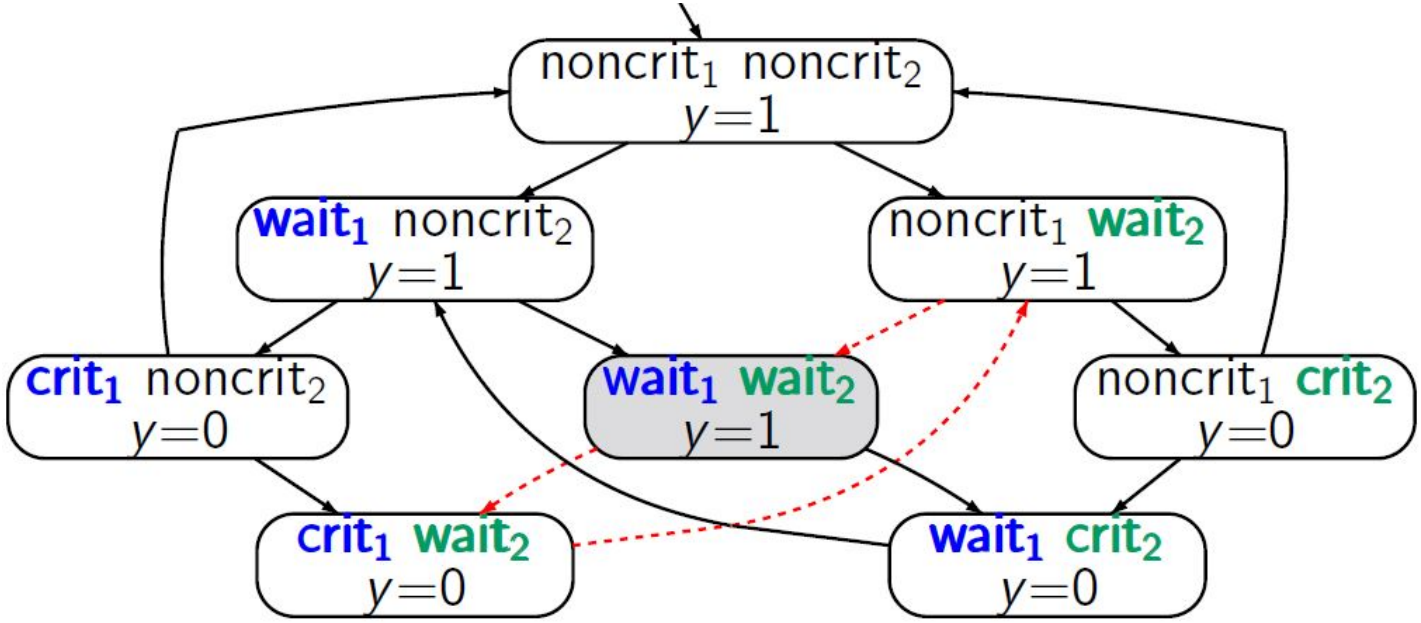
If $\mathcal{T}$ is a TS (without terminal states) over AP and E an LT property over AP then

$$\mathcal{T} \models E \quad \text{iff} \quad \mathit{Traces}(\mathcal{T}) \subseteq E$$

If s is a state in $\mathcal{T}$ then

$$s \models E \quad \text{iff} \quad \mathit{Traces}(s) \subseteq E$$

MUTEX with semaphore



$$\mathcal{T}_{Sem} \models \mathit{MUTEX}, \quad \mathcal{T}_{Sem} \not\models \mathit{LIVE}$$

$$\varnothing \, \{\mathrm{wait}_1\} \, \big(\{\mathrm{wait}_1, \mathrm{wait}_2\} \, \{\mathrm{crit}_1, \mathrm{wait}_2\} \{\mathrm{wait}_2\} \big)^{\omega} \notin \mathit{LIVE}$$

LP properties and trace inclusion

An LT property over AP is a language E of infinite words over the alphabet $\Sigma = 2^{AP}$, i.e., $E \subseteq (2^{AP})^{\omega}$.

If $\mathcal{T}$ is a TS over AP then $\mathcal{T} \models E$ iff $Traces(\mathcal{T}) \subseteq E$.

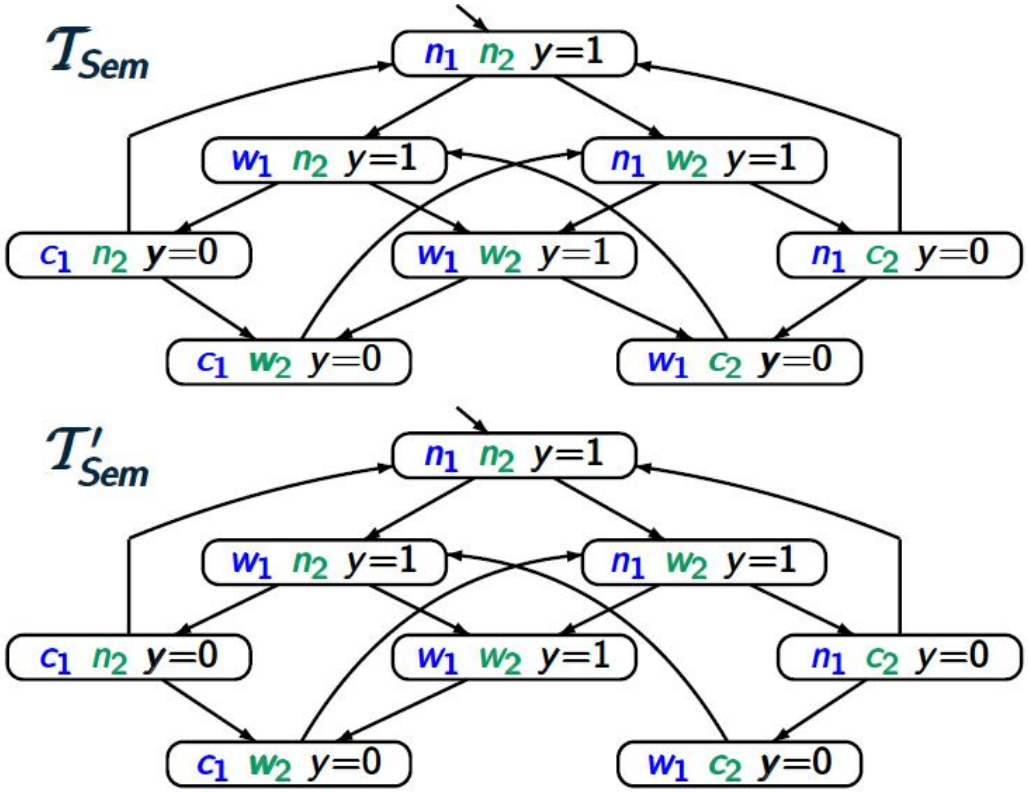
Consequence of these definitions:

If $\mathcal{T}_1$ and $\mathcal{T}_2$ are TS over AP then for all LT properties E over AP:

$$Traces(\mathcal{T}_1) \subseteq Traces(\mathcal{T}_2) \wedge \mathcal{T}_2 \models E \Longrightarrow \mathcal{T}_1 \models E$$

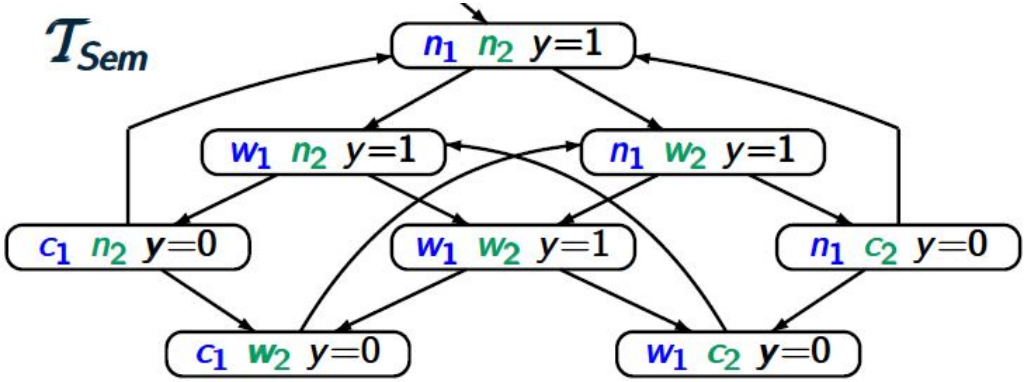
note: $Traces(\mathcal{T}_1) \subseteq Traces(\mathcal{T}_2) \subseteq E$

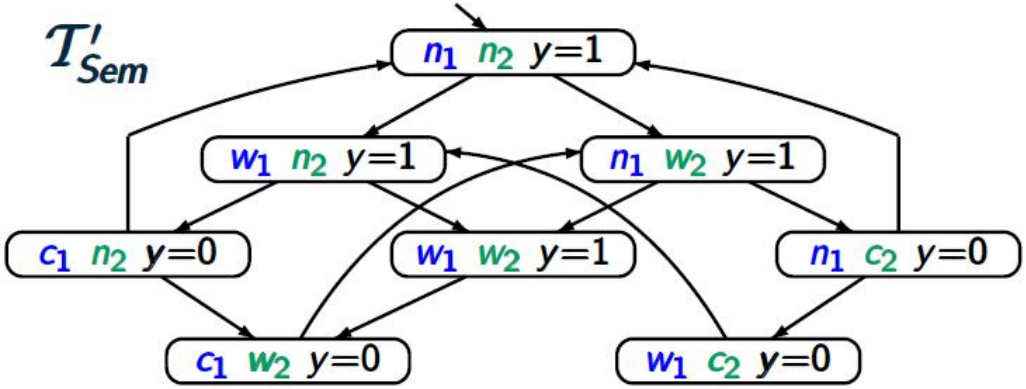
MUTEX with semaphore



$$Paths(\mathcal{T}'_{Sem}) \subseteq Paths(\mathcal{T}_{Sem})$$

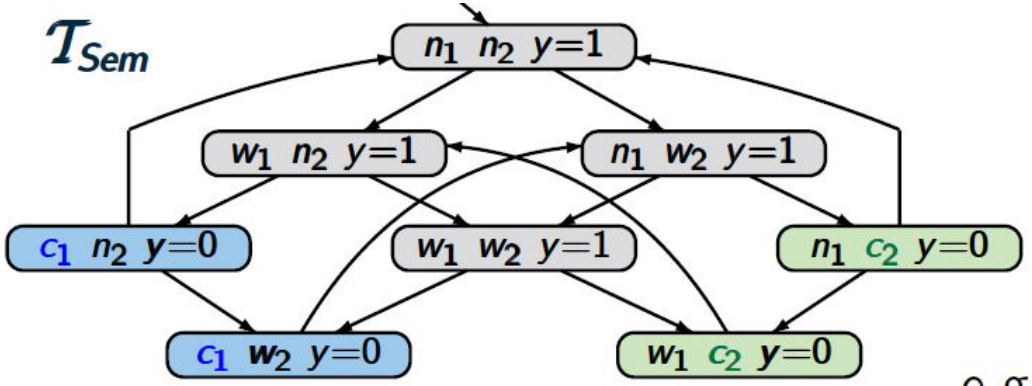
MUTEX with semaphore



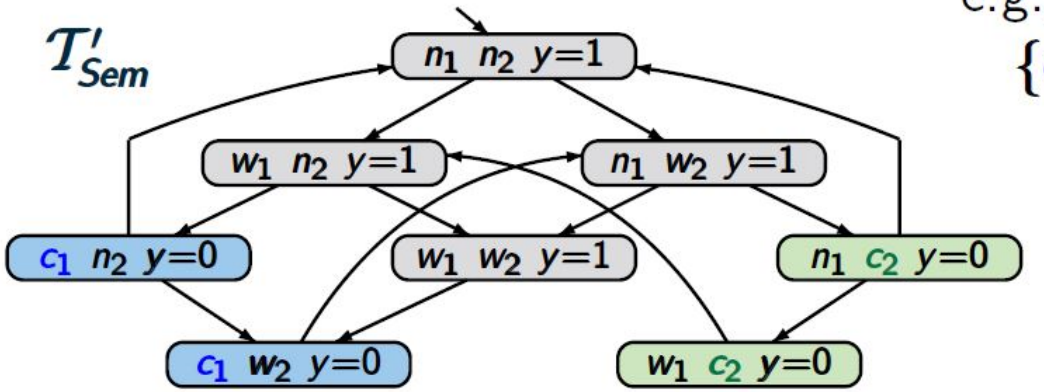


$Traces(\mathcal{T}'_{Sem}) \subseteq Traces(\mathcal{T}_{Sem})$ for any AP

MUTEX with semaphore



e.g., for $AP = \{\mathrm{crit}_1, \mathrm{crit}_2\}$



$Traces(\mathcal{T}_{Sem}) \models E$ implies $Traces(\mathcal{T}'_{Sem}) \models E$ for any E

Trace equivalence

Transition systems $\mathcal{T}_1$ and $\mathcal{T}_2$ over the same set AP of atomic propositions are called trace equivalent iff

$$Traces(\mathcal{T}_1) = Traces(\mathcal{T}_2)$$

i.e., trace equivalence requires trace inclusion in both directions

Trace equivalent TS satisfy the **same LT properties**

LP properties and trace relations

Let $\mathcal{T}_1$ and $\mathcal{T}_2$ be TS over AP.

The following statements are equivalent:

(1) $Traces(\mathcal{T}_1) \subseteq Traces(\mathcal{T}_2)$

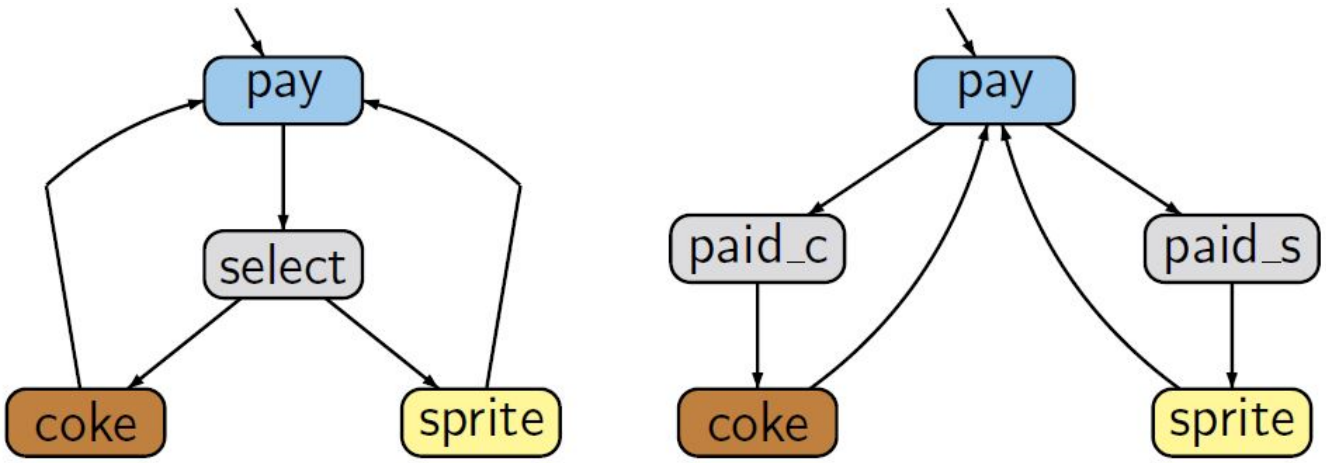
(2) for all LT-properties E: $\mathcal{T}_2 \models E \Longrightarrow \mathcal{T}_1 \models E$

The following statements are equivalent:

(1) $Traces(\mathcal{T}_1) = Traces(\mathcal{T}_2)$

(2) for all LT-properties E: $\mathcal{T}_1 \models E$ iff $\mathcal{T}_2 \models E$

Trace equivalent beverage machines



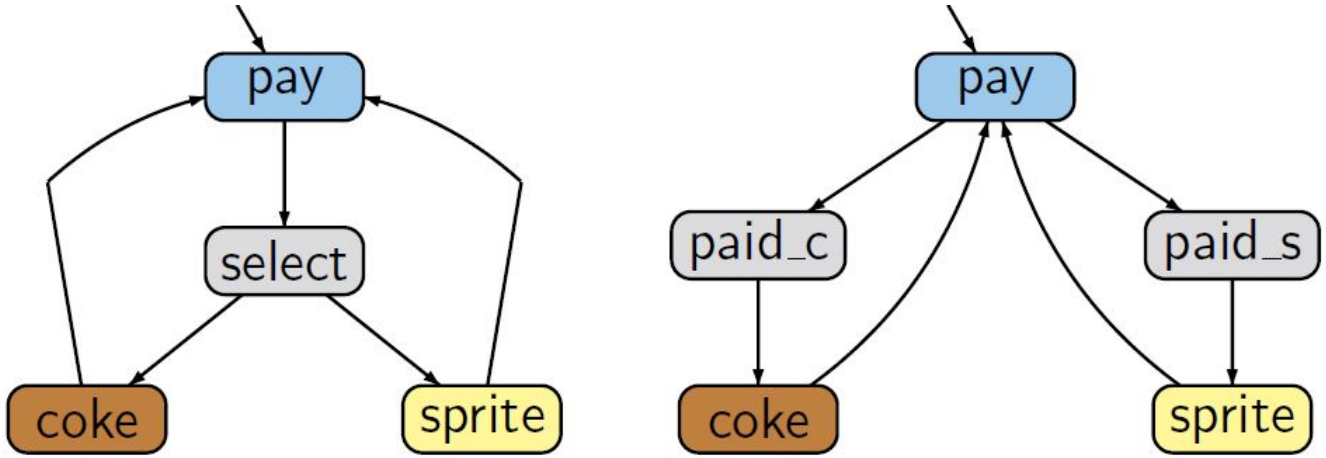
set of atomic propositions $AP = \{pay, coke, sprite\}$

$Traces(\mathcal{T}_1) = Traces(\mathcal{T}_2) =$ set of all infinite words

$\{pay\}\,\varnothing\,\{drink_1\}\,\{pay\}\,\varnothing\,\{drink_2\}\,\ldots$

where $drink_1, drink_2, \ldots \in \{coke, sprite\}$

Trace equivalent beverage machines



set of atomic propositions $AP = \{pay, coke, sprite\}$

$Traces(\mathcal{T}_1) = Traces(\mathcal{T}_2) =$ set of all infinite words

$\{pay\}\,\varnothing\,\{drink_1\}\,\{pay\}\,\varnothing\,\{drink_2\}\ \ldots$

$\mathcal{T}_1$ and $\mathcal{T}_2$ satisfy the same LT-properties over AP

Linear Time Properties

- state-based and linear time view
- definition of linear time properties
- invariants and safety
- liveness and fairness