به نام خدا

روش‌های رسمی در مهندسی نرم‌افزار

مرجان عظیمی
Azimi.marjan@gmail.com

خصوصیات زمان خطی

- برای هدف verification باید سیستم گذار ویژگی‌های مورد نظر را برآورده کند. این ویژگی‌ها به صورت فرمال بیان می‌شوند و یکسری الگوریتم‌های مدل چک بیان می‌شود تا این ویژگی‌ها را به صورت اتوماتیک بررسی نماید.

خصوصیات زمان خطی

- برای تحلیل یک سیستم گذار دو رویکرد action-based و state-based داریم. رویکرد مبتنی بر حالت خلاصه‌ای از عمل‌هاست و فقط ترتیب حالت‌ها در نظر گرفته می‌شود. در رویکرد مبتنی بر عمل فقط به گذار عمل‌ها توجه می‌کند.

تبدیل سیستم گذار به گراف حالت

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

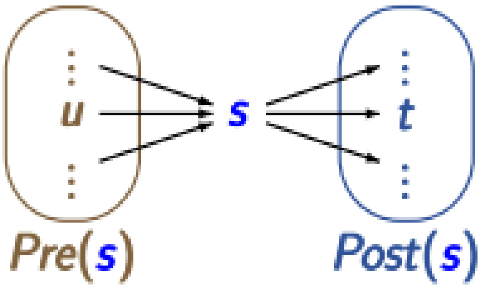
↓ abstraction from actions

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

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

use standard notations for graphs, e.g.,

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



path

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

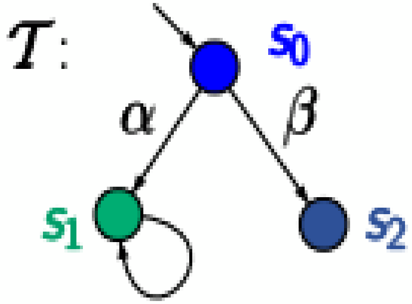
$\pi = s_0\, s_1\, s_2 \ldots$ infinite or $\pi = s_0\, s_1 \ldots s_n$ finite

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

مثال: path



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

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

trace

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

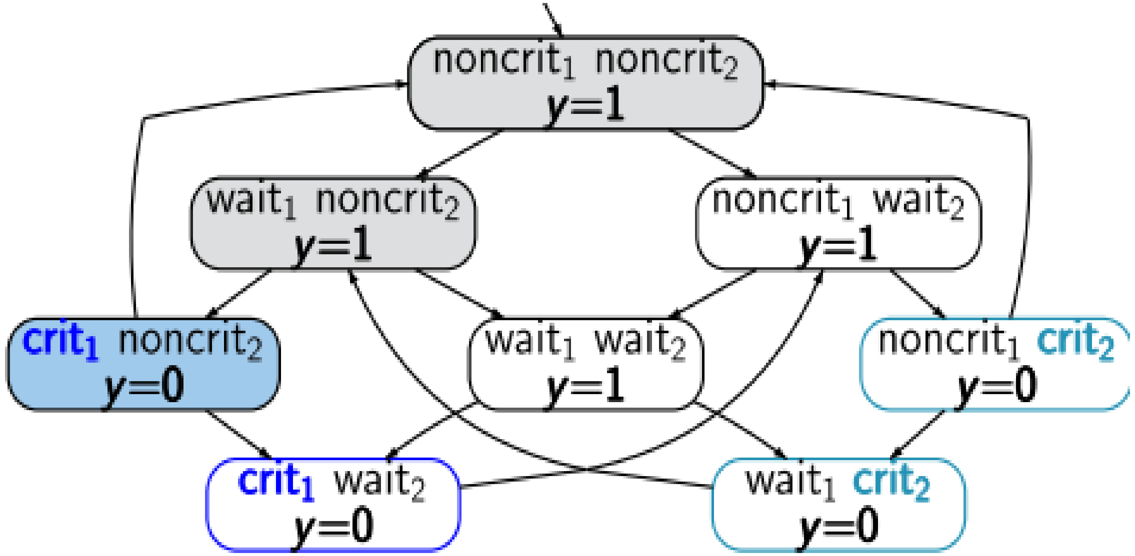
paths: sequences of states

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

traces: sequences of sets of atomic propositions

$L(s_0)\, L(s_1)\, L(s_2)\, \ldots$

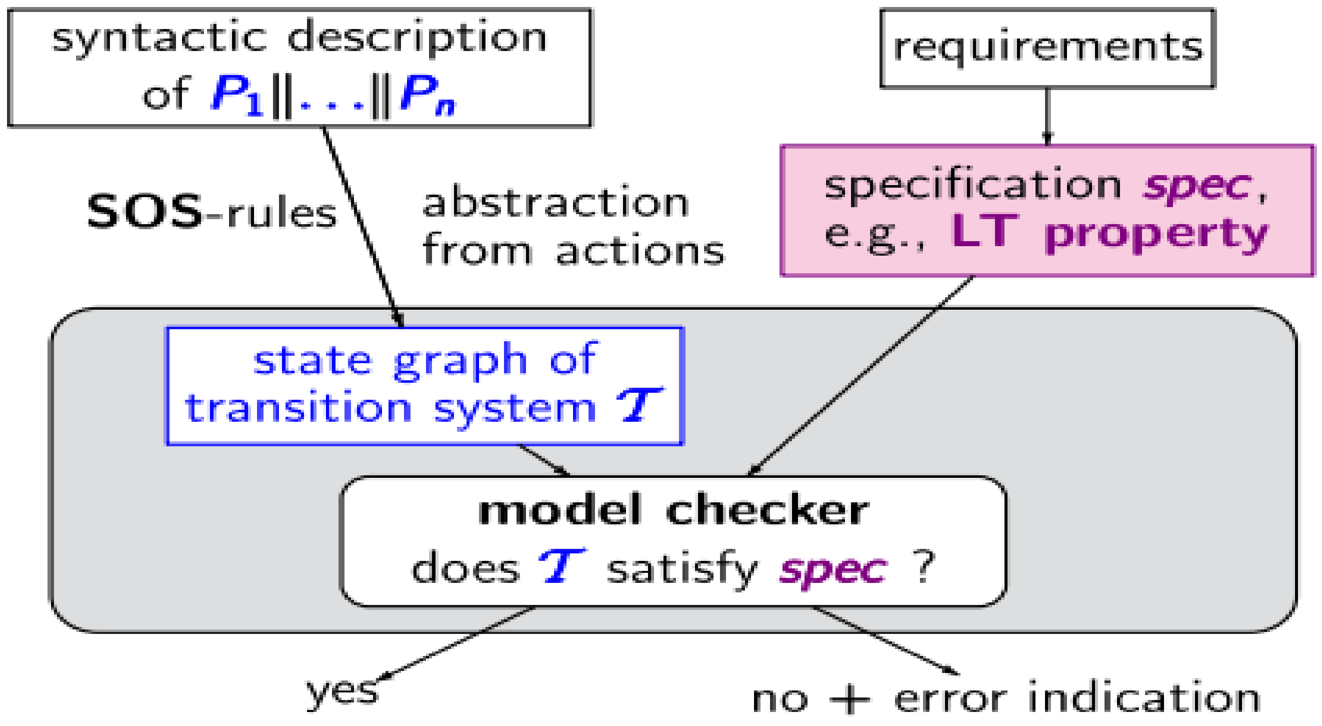
مثال: trace



set of atomic propositions $AP = \{crit_1, crit_2\}$

traces, e.g., $\varnothing\, \varnothing\, \{crit_1\}\, \varnothing\, \varnothing\, \{crit_1\}\, \varnothing\, \varnothing\, \{crit_1\} \ldots$

مدل چک



syntactic description of $P_1 \| \ldots \| P_n$
requirements
SOS-rules
abstraction from actions
specification spec, e.g., LT property
state graph of transition system $\mathcal{T}$
model checker
does $\mathcal{T}$ satisfy spec ?
yes
no + error indication

خصوصیات زمان خطی

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:

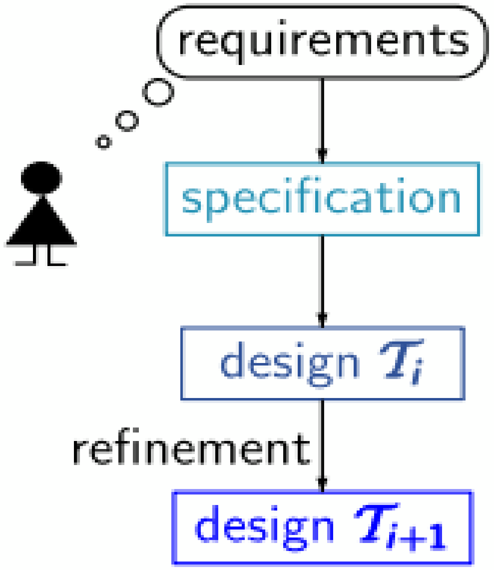
If $\mathcal{T}$ is a TS (without terminal states) over AP and E an LT property over AP then

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

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

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

هم‌ارزی trace ها



trace inclusion

$\mathcal{T}_{i+1} \sqsubseteq \mathcal{T}_i$ iff $Traces(\mathcal{T}_{i+1}) \subseteq Traces(\mathcal{T}_i)$

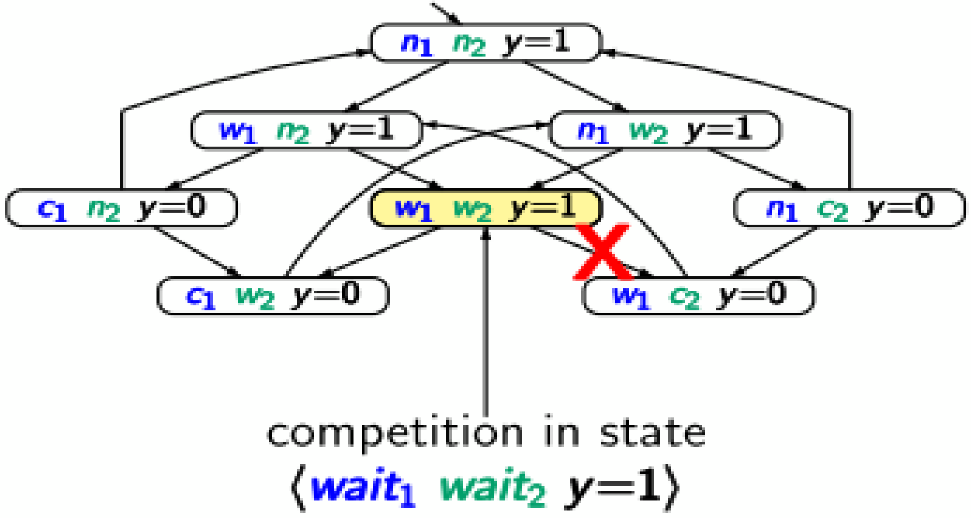
$\longleftarrow \mathcal{T}_i \models E$

$\longleftarrow \mathcal{T}_{i+1} \sqsubseteq \mathcal{T}_i$ implies $\mathcal{T}_{i+1} \models E$

implementation/refinement relation $\sqsubseteq$:

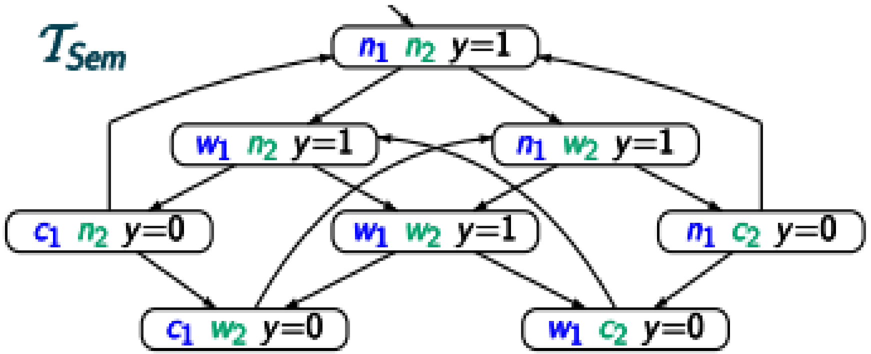
$\mathcal{T}_{i+1} \sqsubseteq \mathcal{T}_i$ iff "$\mathcal{T}_{i+1}$ correctly implements $\mathcal{T}_i$"

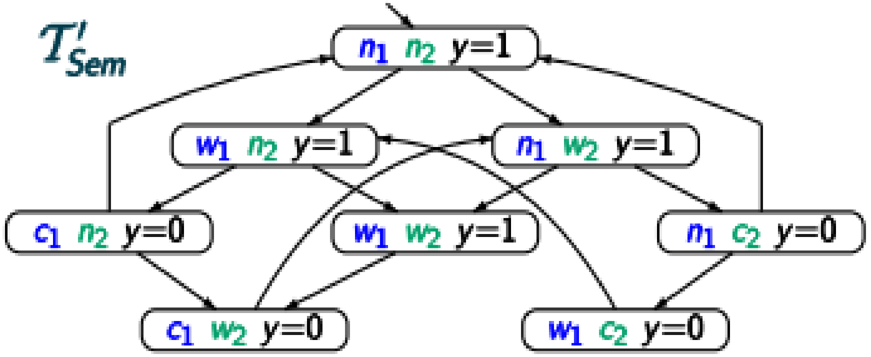
مثال



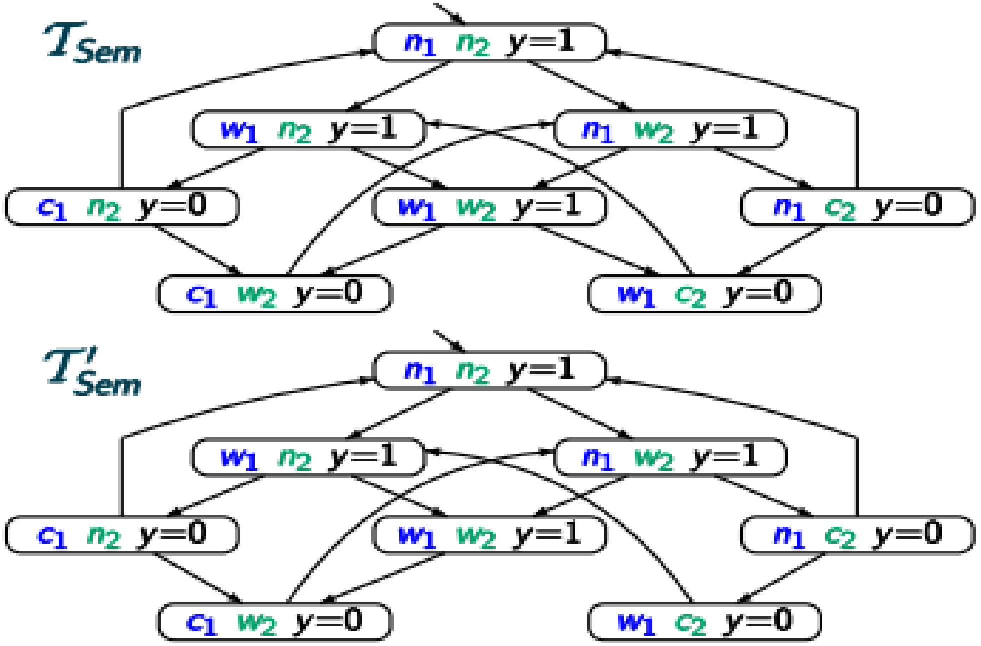
resolve the nondeterminism by giving priority to process P_1

مثال


$\mathcal{T}_{Sem}$
n1 n2 y=1
w1 n2 y=1
n1 w2 y=1
c1 n2 y=0
w1 w2 y=1
n1 c2 y=0
c1 w2 y=0
w1 c2 y=0

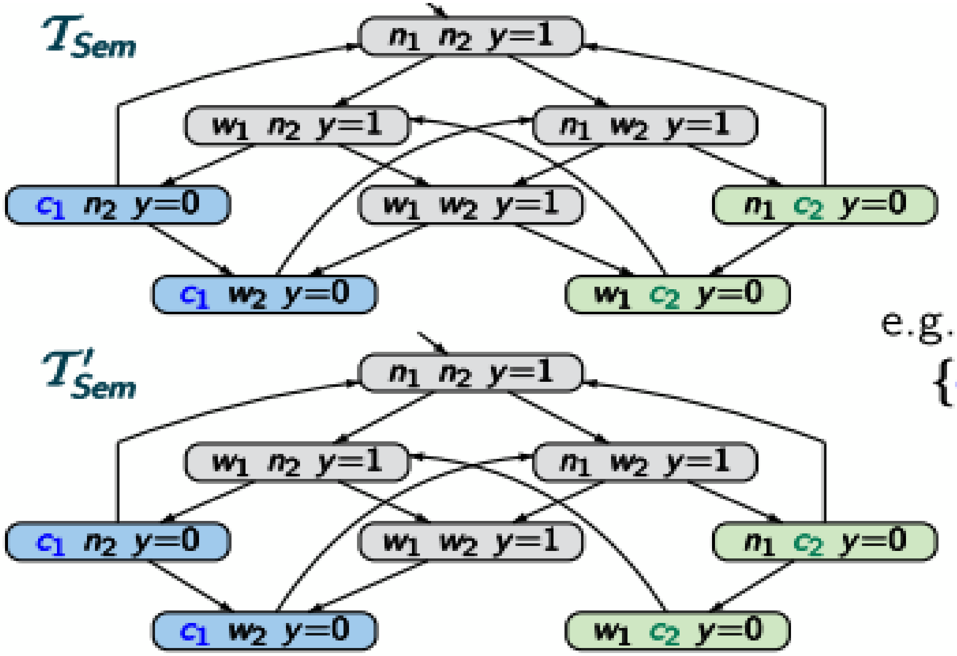

$\mathcal{T}'_{Sem}$
n1 n2 y=1
w1 n2 y=1
n1 w2 y=1
c1 n2 y=0
w1 w2 y=1
n1 c2 y=0
c1 w2 y=0
w1 c2 y=0

مثال



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

مثال



e.g., for $AP = \{crit_1, crit_2\}$

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

خصوصیات زمان خطی

safety properties *"nothing bad will happen"*

liveness properties *"something good will happen"*

خصوصیات زمان خطی

safety properties *"nothing bad will happen"*

examples:

- mutual exclusion
- deadlock freedom

} special case: **invariants** *"no bad state will be reached"*

- "every red phase is preceded by a yellow phase"

liveness properties *"something good will happen"*

examples:

- "each waiting process will eventually enter its critical section"
- "each philosopher will eat infinitely often"

invariant

Let E be an LT property over AP.

E is called an invariant if there exists a propositional formula Φ over AP such that

$$E = \{ A_0 A_1 A_2 \ldots \in (2^{AP})^{\omega} : \forall i \geq 0. A_i \models \Phi \}$$

Φ is called the invariant condition of E.

invariant

mutual exclusion (safety):

$$MUTEX = \begin{array}{l} \text{set of all infinite words } A_0\, A_1\, A_2 \ldots \text{ s.t.} \\ \forall i \in \mathbb{N}.\ \ crit_1 \notin A_i \ \text{ or } \ crit_2 \notin A_i \end{array}$$

invariant condition: $\Phi = \neg crit_1 \vee \neg crit_2$

here: $AP = \{crit_1, crit_2, \ldots\}$

invariant

mutual exclusion (safety):

$$MUTEX = \begin{array}{l}\text{set of all infinite words } A_0\, A_1\, A_2 \ldots \text{ s.t.} \\ \forall i \in \mathbb{N}.\ \ \text{crit}_1 \notin A_i \ \text{ or } \ \text{crit}_2 \notin A_i\end{array}$$

invariant condition: $\Phi = \neg \text{crit}_1 \vee \neg \text{crit}_2$

deadlock freedom for 5 dining philosophers:

$$DF = \begin{array}{l}\text{set of all infinite words } A_0\, A_1\, A_2 \ldots \text{ s.t.} \\ \forall i \in \mathbb{N}\ \exists j \in \{0,1,2,3,4\}.\ \text{wait}_j \notin A_i\end{array}$$

invariant condition:

$$\Phi = \neg \text{wait}_0 \vee \neg \text{wait}_1 \vee \neg \text{wait}_2 \vee \neg \text{wait}_3 \vee \neg \text{wait}_4$$

here: $AP = \{\text{wait}_j : 0 \leq j \leq 4\} \cup \{\ldots\}$

invariant

Let E be an LT property over AP. E is called an invariant if there exists a propositional formula Φ s.t.

$$E = \{ A_0 A_1 A_2 \ldots \in (2^{AP})^\omega : \forall i \geq 0. A_i \models \Phi \}$$

Let $\mathcal{T}$ be a TS over AP without terminal states. Then:

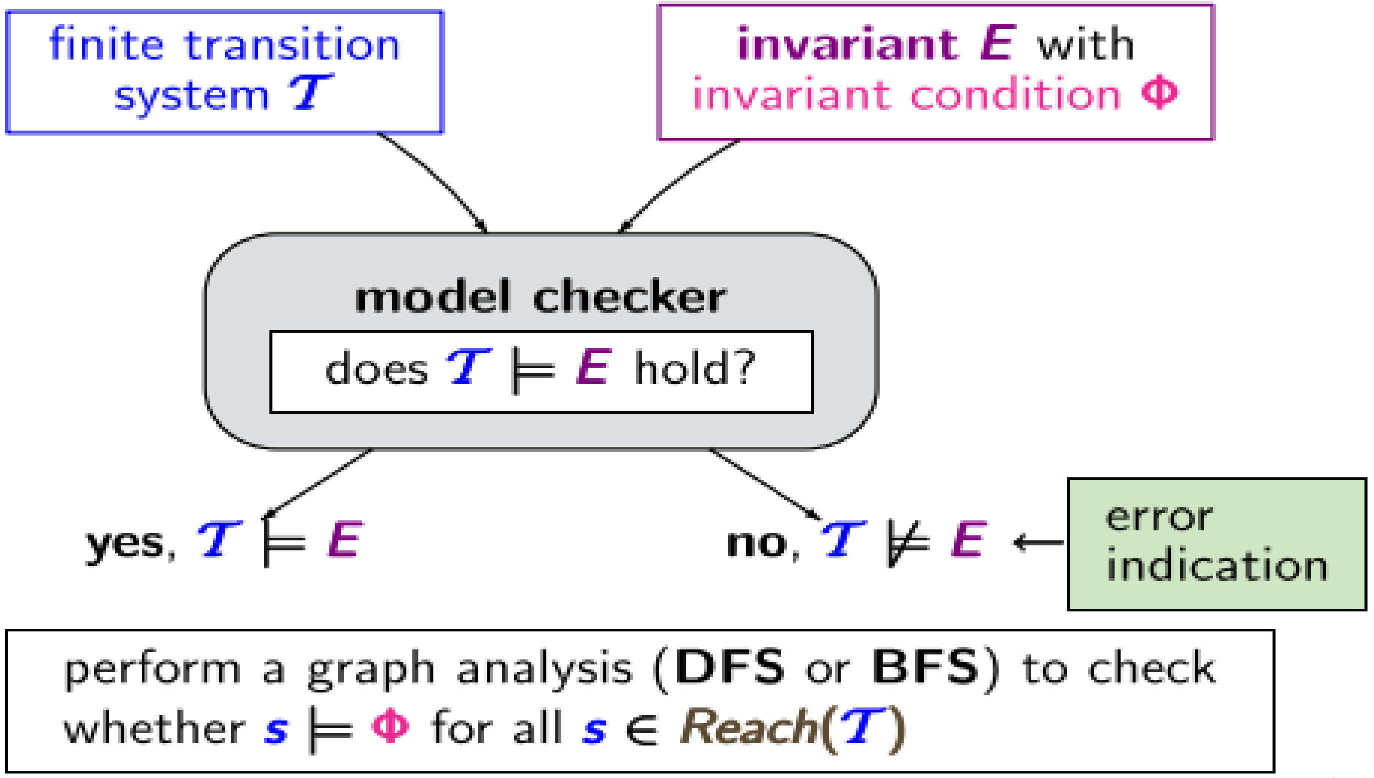
$\mathcal{T} \models E$ iff $trace(\pi) \in E$ for all $\pi \in Paths(\mathcal{T})$

iff $s \models \Phi$ for all states s on a path of $\mathcal{T}$

iff $s \models \Phi$ for all states $s \in Reach(\mathcal{T})$

i.e., Φ holds in all initial states and is invariant under all transitions

Invariant check



خصوصیت safety

state that "nothing bad will happen"

invariants: ⟵ "no **bad state** will be reached"

- mutual exclusion: *never* $crit_1 \wedge crit_2$
- deadlock freedom: *never* $\bigwedge_{0 \leq i < n} wait_i$

---

other safety properties: ⟵ "no **bad prefix**"

- German traffic lights:
  every red phase is preceded by a yellow phase
- beverage machine:
  the total number of entered coins is never less than the total number of released drinks

Bad prefix

- traffic lights:

  every red phase is preceded by a yellow phase

  ↑

  bad prefix: finite trace fragment where a red phase appears without being preceded by a yellow phase
  e.g., . . . {●} {●}

- beverage machine:

  the total number of entered coins is never less than the total number of released drinks

  ↑

  bad prefix, e.g., {*pay*} {*drink*} {*drink*}

safety

Let E be a LT property over AP, i.e., $E \subseteq (2^{AP})^\omega$.

E is called a safety property if for all words

$$\sigma = A_0 A_1 A_2 \ldots \in (2^{AP})^\omega \setminus E$$

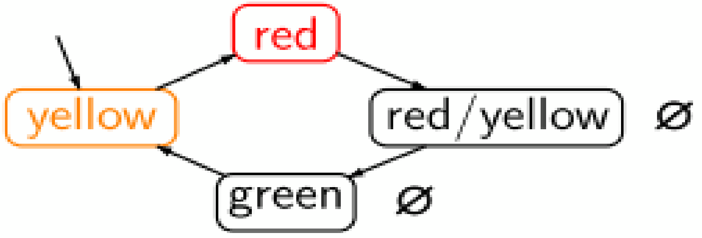
there exists a finite prefix $A_0 A_1 \ldots A_n$ of σ such that *none* of the words $A_0 A_1 \ldots A_n B_{n+1} B_{n+2} B_{n+3} \ldots$ belongs to E, i.e.,

$$E \cap \{\sigma' \in (2^{AP})^\omega : A_0 \ldots A_n \text{ is a prefix of } \sigma'\} = \varnothing$$

Such words $A_0 A_1 \ldots A_n$ are called bad prefixes for E.

$$BadPref_E \overset{\text{def}}{=} \text{set of bad prefixes for } E$$

مثال

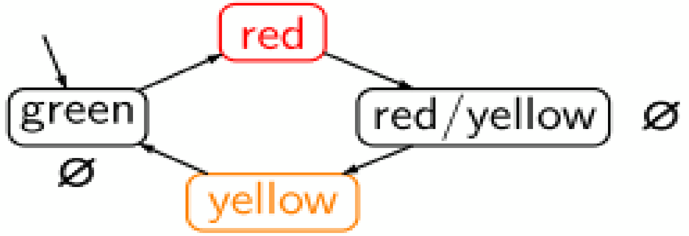


"every red phase is preceded by a yellow phase"

hence: $\mathcal{T} \models E$

E = set of all infinite words $A_0\, A_1\, A_2 \ldots$ over 2^{AP} such that for all $i \in \mathbb{N}$:

$$red \in A_i \implies i \geq 1 \text{ and } yellow \in A_{i-1}$$



$\mathcal{T} \not\models E$

minimal bad prefix:

$\varnothing\,\{red\}$

safety

Let $E \subseteq (2^{AP})^\omega$ be a safety property, $\mathcal{T}$ a TS over AP.

$$\begin{aligned} \mathcal{T} \models E \quad & \text{iff} \quad Traces(\mathcal{T}) \subseteq E \\ & \text{iff} \quad Traces_{fin}(\mathcal{T}) \cap BadPref = \varnothing \\ & \text{iff} \quad Traces_{fin}(\mathcal{T}) \cap MinBadPref = \varnothing \end{aligned}$$

$BadPref$ = set of all bad prefixes of E
$MinBadPref$ = set of all minimal bad prefixes of E
$Traces(\mathcal{T})$ = set of traces of $\mathcal{T}$
$Traces_{fin}(\mathcal{T})$ = set of finite traces of $\mathcal{T}$
$= \{ \, trace(\widehat{\pi}) : \widehat{\pi}$ is an initial, finite path fragment of $\mathcal{T} \}$

liveness

"liveness: something good will happen."

"event *a* will occur eventually"

e.g., termination for sequential programs

"event *a* will occur infinitely many times"

e.g., starvation freedom for dining philosophers

"whenever event *b* occurs then event *a* will occur sometimes in the future"

e.g., every waiting process enters eventually its critical section

مثال

- Each philosopher thinks infinitely often.
  liveness
- Two philosophers next to each other never eat at the same time.
  invariant
- Whenever a philosopher eats then he has been thinking at some time before.
  safety
- Whenever a philosopher eats then he will think some time afterwards.
  liveness
- Between two eating phases of philosopher i lies at least one eating phase of philosopher $i+1$.
  safety

liveness

Let E be an LT property over AP, i.e., $E \subseteq (2^{AP})^{\omega}$.

E is called a liveness property if each finite word over AP can be extended to an infinite word in E, i.e., if

$$pref(E) = (2^{AP})^{+}$$

Examples:

- each process will eventually enter its critical section
- each process will enter its critical section infinitely often
- whenever a process has requested its critical section then it will eventually enter its critical section

مثال

An LT property E over AP is called a liveness property if $pref(E) = (2^{AP})^+$

Examples for $AP = \{crit_i : i = 1, \ldots, n\}$:

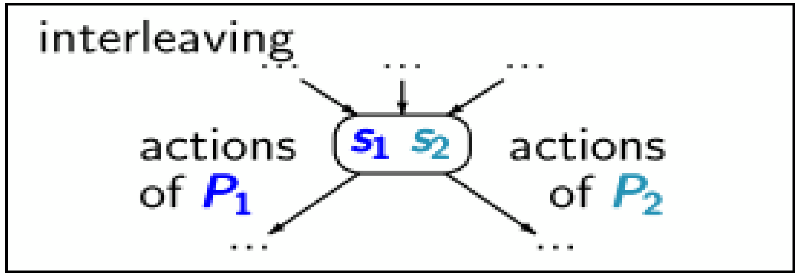
- each process will eventually enter its critical section

E = set of all infinite words $A_0 A_1 A_2 \ldots$ s.t.

$$\forall i \in \{1, \ldots, n\} \; \exists k \geq 0. \; crit_i \in A_k$$

fairness

two independent non-communicating processes P_1 ||| P_2



possible interleavings:

P_1 P_2 P_2 P_1 P_1 P_1 P_2 P_1 P_2 P_2 P_2 P_1 P_1 … fair
P_1 P_1 P_2 P_1 P_1 P_2 P_1 P_1 P_2 P_1 P_1 P_2 P_1 … fair
P_1 P_1 P_1 P_1 P_1 P_1 P_1 P_1 P_1 P_1 P_1 P_1 P_1 … unfair

> process fairness assumes an appropriate resolution of the nondeterminism resulting from interleaving and competitions

68 / 189

انواع fairness

- unconditional fairness, e.g.,

  every process enters gets its turn infinitely often.

- strong fairness, e.g.,

  every process that is enabled infinitely often
  gets its turn infinitely often.

- weak fairness, e.g.,

  every process that is continuously enabled
  from a certain time instance on,
  gets its turn infinitely often.

انواع fairness

Let $\mathcal{T}$ be a TS with action-set Act, $A \subseteq Act$ and

$\rho = s_0 \xrightarrow{\alpha_0} s_1 \xrightarrow{\alpha_1} s_2 \xrightarrow{\alpha_2} \ldots$ infinite execution fragment

we will provide conditions for

- unconditional A-fairness of ρ
- strong A-fairness of ρ
- weak A-fairness of ρ

using the following notations:

$$Act(s_i) = \{\beta \in Act : \exists s' \text{ s.t. } s_i \xrightarrow{\beta} s'\}$$

$$\overset{\infty}{\exists} \;\widehat{=}\; \text{“there exists infinitely many ...”}$$

$$\overset{\infty}{\forall} \;\widehat{=}\; \text{“for all, but finitely many ...”}$$

انواع fairness

Let $\mathcal{T}$ be a TS with action-set Act, $A \subseteq Act$ and

$\rho = s_0 \xrightarrow{\alpha_0} s_1 \xrightarrow{\alpha_1} s_2 \xrightarrow{\alpha_2} \ldots$ infinite execution fragment

- ρ is unconditionally A-fair, if $\overset{\infty}{\exists}\, i \geq 0.\, \alpha_i \in A$

"actions in A will be taken infinitely many times"

انواع fairness

Let $\mathcal{T}$ be a TS with action-set Act, $A \subseteq Act$ and

$\rho = s_0 \xrightarrow{\alpha_0} s_1 \xrightarrow{\alpha_1} s_2 \xrightarrow{\alpha_2} \ldots$ infinite execution fragment

- ρ is unconditionally A-fair, if $\overset{\infty}{\exists} i \geq 0.\, \alpha_i \in A$
- ρ is strongly A-fair, if

$$\overset{\infty}{\exists} i \geq 0.\, A \cap Act(s_i) \neq \varnothing \quad \Longrightarrow \quad \overset{\infty}{\exists} i \geq 0.\, \alpha_i \in A$$

"If infinitely many times some action in A is enabled, then actions in A will be taken infinitely many times."

انواع fairness

Let $\mathcal{T}$ be a TS with action-set Act, $A \subseteq Act$ and

$\rho = s_0 \xrightarrow{\alpha_0} s_1 \xrightarrow{\alpha_1} s_2 \xrightarrow{\alpha_2} \ldots$ infinite execution fragment

- ρ is unconditionally A-fair, if $\overset{\infty}{\exists}\, i \geq 0.\, \alpha_i \in A$
- ρ is strongly A-fair, if

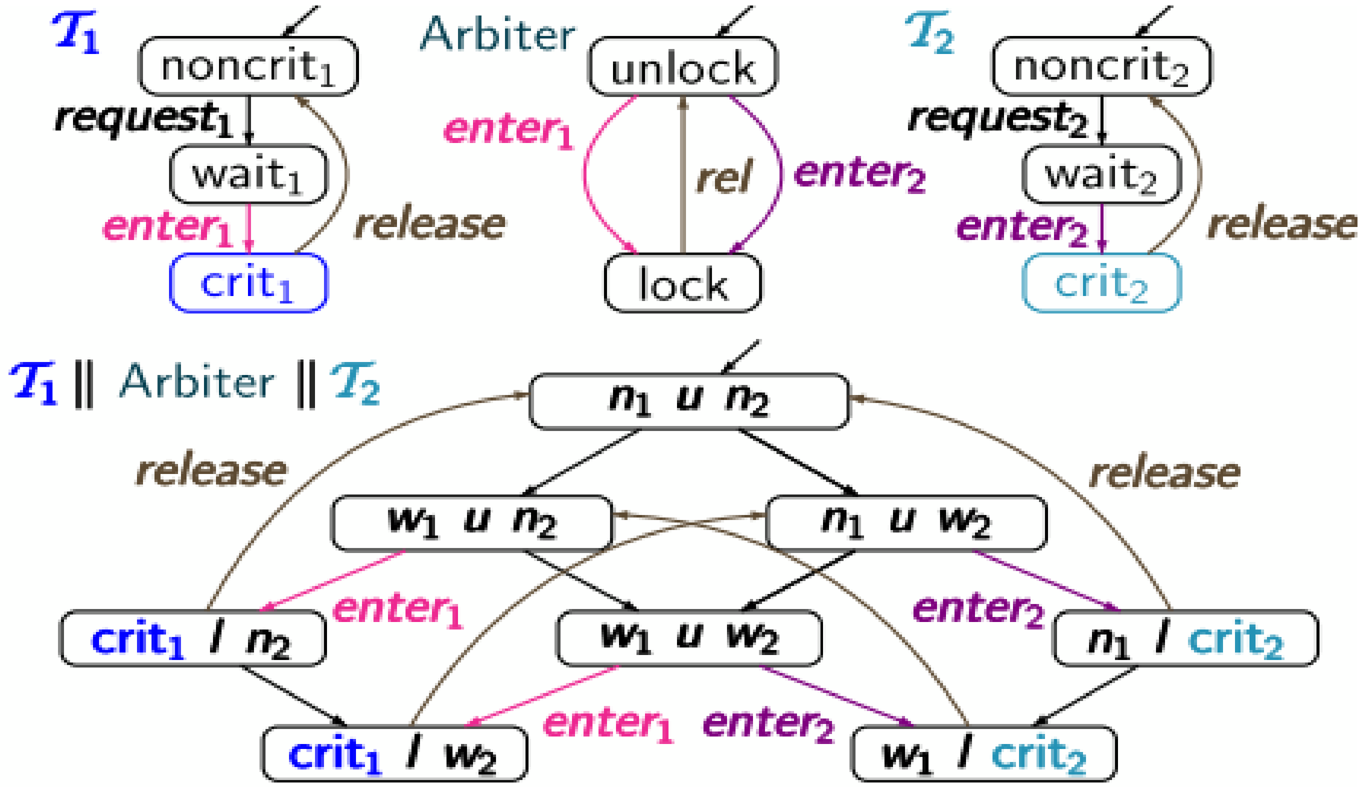
$$\overset{\infty}{\exists}\, i \geq 0.\, A \cap Act(s_i) \neq \varnothing \quad \Longrightarrow \quad \overset{\infty}{\exists}\, i \geq 0.\, \alpha_i \in A$$

- ρ is weakly A-fair, if

$$\overset{\infty}{\forall}\, i \geq 0.\, A \cap Act(s_i) \neq \varnothing \quad \Longrightarrow \quad \overset{\infty}{\exists}\, i \geq 0.\, \alpha_i \in A$$

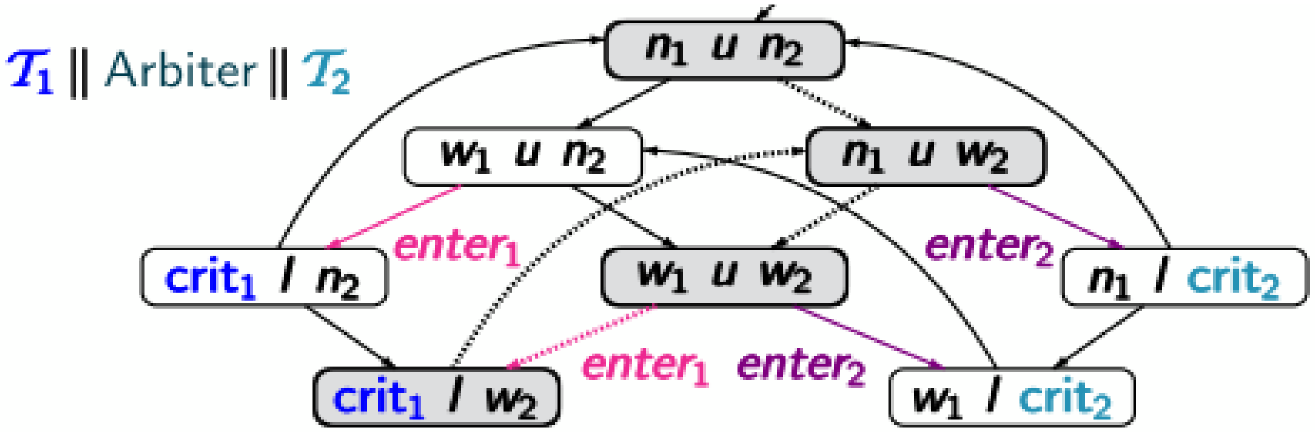
"If from some moment, actions in A are enabled, then actions in A will be taken infinitely many times."

مثال



$\mathcal{T}_1$
noncrit₁
request₁
wait₁
enter₁
crit₁
release
Arbiter
unlock
enter₁
rel
enter₂
lock
$\mathcal{T}_2$
noncrit₂
request₂
wait₂
enter₂
crit₂
release
$\mathcal{T}_1$ ∥ Arbiter ∥ $\mathcal{T}_2$
n₁ u n₂
release
release
w₁ u n₂
n₁ u w₂
enter₁
enter₂
crit₁ l n₂
w₁ u w₂
n₁ l crit₂
enter₁
enter₂
crit₁ l w₂
w₁ l crit₂

مثال



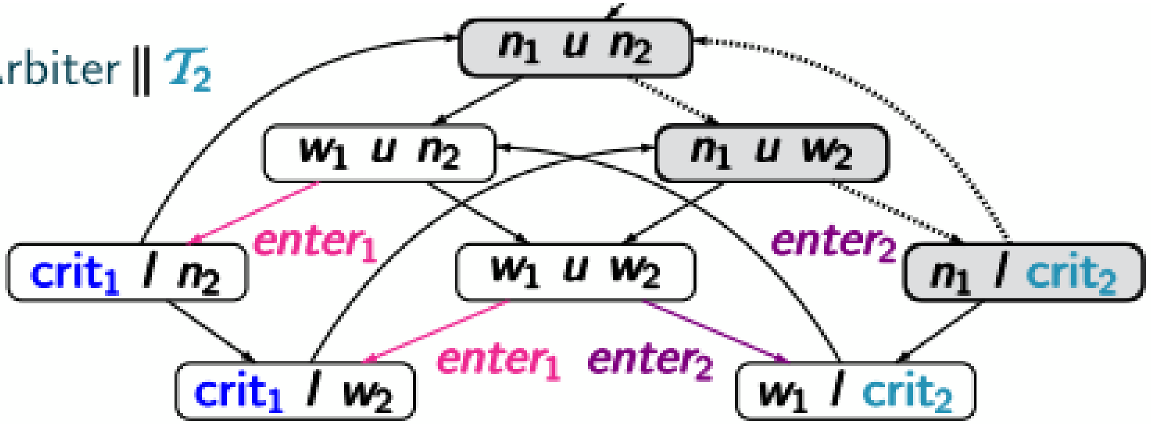
fairness for action set $A = \{enter_1\}$:

$$\langle n_1, u, n_2 \rangle \rightarrow \Big(\langle n_1, u, w_2 \rangle \rightarrow \langle w_1, u, w_2 \rangle \rightarrow \langle crit_1, l, w_2 \rangle \Big)^\omega$$

- unconditional A-fairness: **yes**
- strong A-fairness: **yes** ← unconditionally fair
- weak A-fairness: **yes** ← unconditionally fair

مثال

$\mathcal{T}_1 \parallel \text{Arbiter} \parallel \mathcal{T}_2$



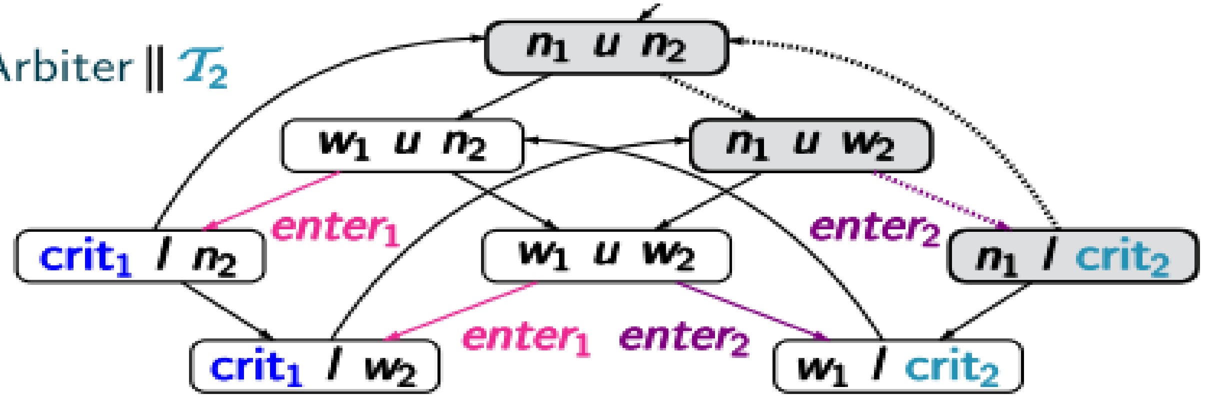
fairness for action-set $A = \{enter_1\}$:

$$\left(\langle n_1, u, n_2 \rangle \rightarrow \langle n_1, u, w_2 \rangle \rightarrow \langle n_1, l, crit_2 \rangle \right)^{\omega}$$

- unconditional A-fairness: **no**
- strong A-fairness: **yes** $\leftarrow$ A never enabled
- weak A-fairness: **yes** $\leftarrow$ strongly A-fair

مثال

$\mathcal{T}_1 \parallel \text{Arbiter} \parallel \mathcal{T}_2$



fairness for action set $A = \{enter_1, enter_2\}$:

$$\left(\langle n_1, u, n_2 \rangle \rightarrow \langle n_1, u, w_2 \rangle \rightarrow \langle n_1, u, crit_2 \rangle \right)^{\omega}$$

- unconditional A-fairness: yes
- strong A-fairness: yes
- weak A-fairness: yes

؟