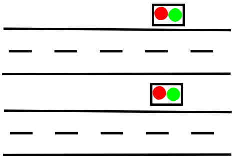
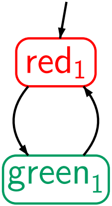
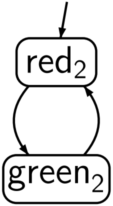
Two independent traffic lights



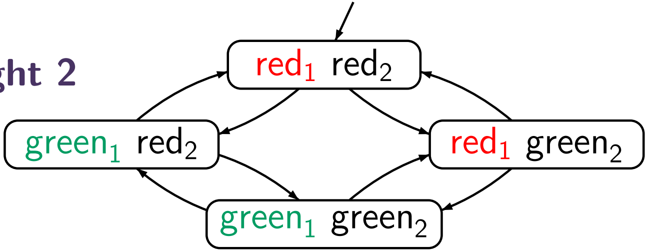
light 1



light 2



light 1 ||| light 2

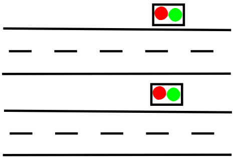


light 1 ||| light 2 $\not\models$ "infinitely often ***green$_1$***"

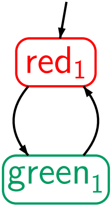
although **light 1** $\models$ "infinitely often ***green$_1$***"

Two independent traffic lights

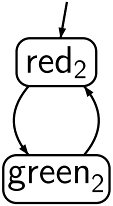
LF2.6-3



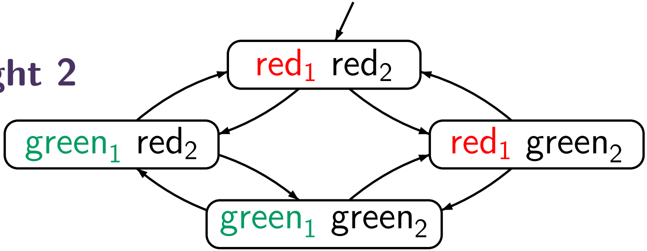
light 1



light 2



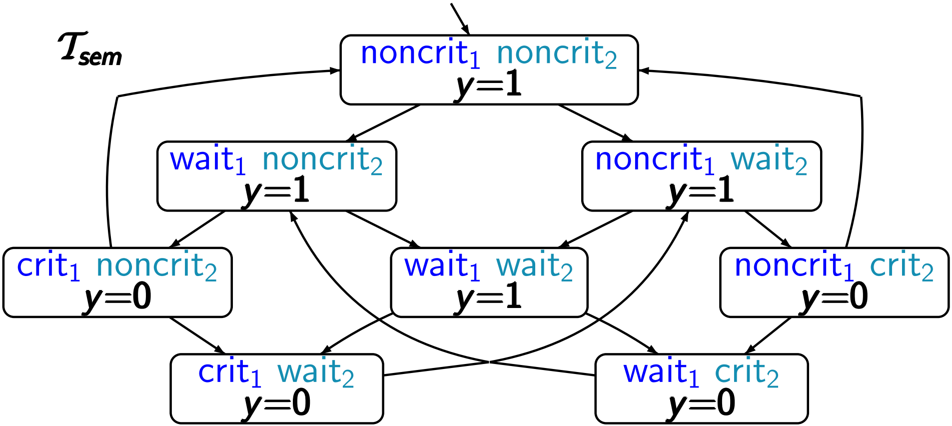
light 1 ||| light 2



light 1 ||| light 2 $\not\models$ "infinitely often ***green$_1$***"

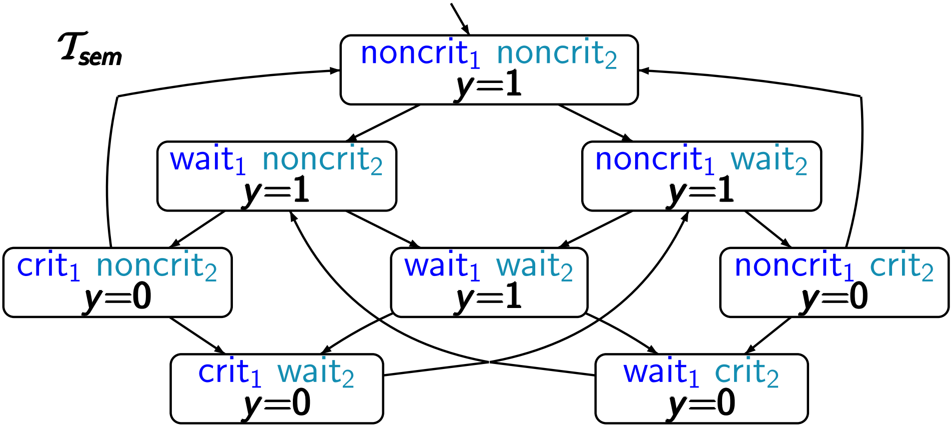
interleaving is completely time abstract !

Mutual exclusion (semaphore)



liveness property $\widehat{=}$ "each waiting process will eventually enter its critical section"

Mutual exclusion (semaphore)

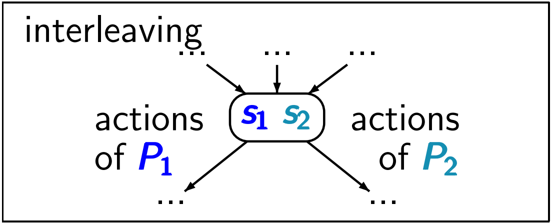


$\mathcal{T}_{sem} \not\models$ "each waiting process will eventually enter its critical section"

level of abstraction is too coarse !

Process fairness

two independent non-communicating processes $P_1 \mid\mid\mid P_2$



possible interleavings:

$P_1\ P_2\ P_2\ P_1\ P_1\ P_1\ P_2\ P_1\ P_2\ P_2\ P_2\ P_1\ P_1\ \ldots$ fair

$P_1\ P_1\ P_2\ P_1\ P_1\ P_2\ P_1\ P_1\ P_2\ P_1\ P_1\ P_2\ P_1\ \ldots$ fair

$P_1\ P_1\ P_1\ P_1\ P_1\ P_1\ P_1\ P_1\ P_1\ P_1\ P_1\ P_1\ P_1\ \ldots$ unfair

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

Nuances of 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.

Fairness for action-set

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 $\overset{\infty}{\exists}\, i \geq 0.\, \alpha_i \in A$

$\boxed{\text{“actions in } A \text{ will be taken infinitely many times”}}$

Fairness for action-set

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."

Fairness for action-set

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."

Fairness for action-set

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

$\rho = s_0 \xrightarrow{\alpha_0} s_1 \xrightarrow{\alpha_1} s_2 \xrightarrow{\alpha_2} \ldots$ an 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

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

$$\boxed{\begin{array}{lcl} \text{unconditionally } A\text{-fair} & \Longrightarrow & \text{strongly } A\text{-fair} \\ & \Longrightarrow & \text{weakly } A\text{-fair} \end{array}}$$

Strong and weak action fairness

LF2.6-8

strong A-fairness is *violated* if

$$s_0 \longrightarrow s_1 \dashrightarrow s_2 \longrightarrow s_3 \longrightarrow s_4 \longrightarrow s_5 \longrightarrow s_6 \longrightarrow s_7 \longrightarrow s_8 \longrightarrow s_9 \longrightarrow \ldots$$

- no A-actions are executed from a certain moment
- A-actions are enabled infinitely many times

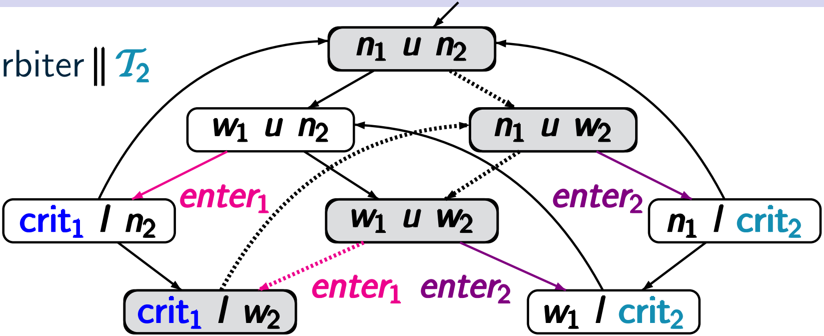
weak A-fairness is *violated* if

$$s_0 \longrightarrow s_1 \dashrightarrow s_2 \longrightarrow s_3 \longrightarrow s_4 \longrightarrow s_5 \longrightarrow s_6 \longrightarrow s_7 \longrightarrow s_8 \longrightarrow s_9 \longrightarrow \ldots$$

- no A-actions are executed from a certain moment
- A-actions are continuously enabled from some moment on

Unconditional, strongly or weakly fair?

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



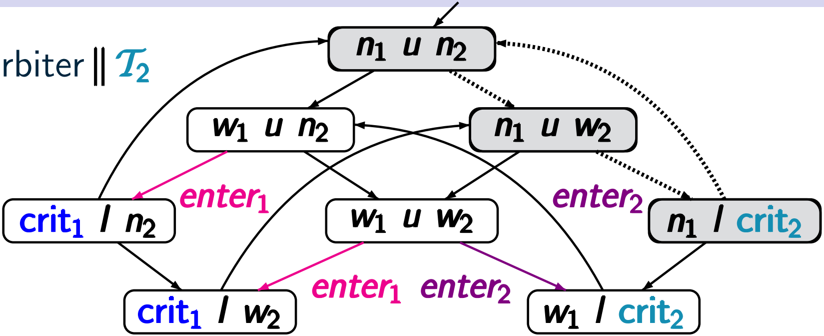
fairness for action set $A = \{enter_1\}$:

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

- unconditional A-fairness: **yes**
- strong A-fairness: **yes** $\leftarrow$ unconditionally fair
- weak A-fairness: **yes** $\leftarrow$ unconditionally fair

Unconditional, strongly or weakly fair?

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



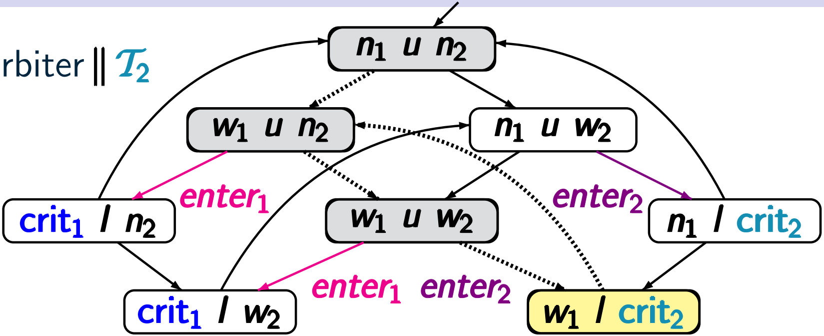
fairness for action-set $A = \{enter_1\}$:

$$\Big(\langle n_1, u, n_2\rangle \longrightarrow \langle n_1, u, w_2\rangle \longrightarrow \langle n_1, l, crit_2\rangle\Big)^{\omega}$$

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

Unconditional, strongly or weakly fair?

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



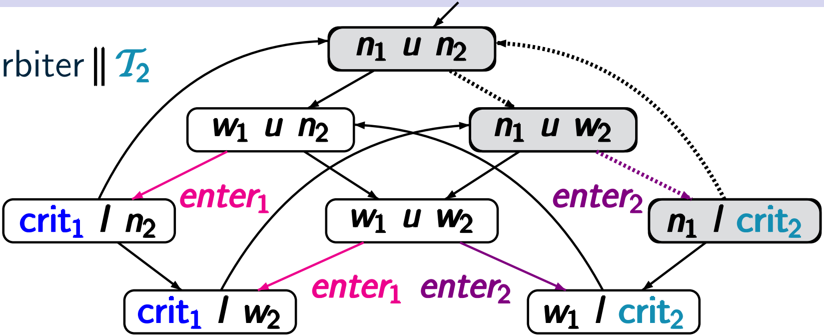
fairness for action-set $A = \{enter_1\}$:

$$\langle n_1, u, n_2\rangle \to \Big(\langle w_1, u, n_2\rangle \to \langle w_1, u, w_2\rangle \to \langle n_1, l, crit_2\rangle\Big)^{\omega}$$

- unconditional A-fairness: **no**
- strong A-fairness: **no**
- weak A-fairness: **yes**

Unconditional, strongly or weakly fair?

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



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

$$\Big(\langle n_1, u, n_2\rangle \longrightarrow \langle n_1, u, w_2\rangle \longrightarrow \langle n_1, u, crit_2\rangle\Big)^\omega$$

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

Action-based fairness assumptions

Let $\mathcal{T}$ be a transition system with action-set Act.
A fairness assumption for $\mathcal{T}$ is a triple

$$\mathcal{F} = (\mathcal{F}_{ucond}, \mathcal{F}_{strong}, \mathcal{F}_{weak})$$

where $\mathcal{F}_{ucond}$, $\mathcal{F}_{strong}$, $\mathcal{F}_{weak} \subseteq 2^{Act}$.

An execution ρ is called $\mathcal{F}$-fair iff

- ρ is unconditionally A-fair for all $A \in \mathcal{F}_{ucond}$
- ρ is strongly A-fair for all $A \in \mathcal{F}_{strong}$
- ρ is weakly A-fair for all $A \in \mathcal{F}_{weak}$

$$FairTraces_{\mathcal{F}}(\mathcal{T}) \stackrel{\text{def}}{=} \{trace(\rho) : \rho \text{ is a } \mathcal{F}\text{-fair execution of } \mathcal{T}\}$$

Fair satisfaction relation

A fairness assumption for $\mathcal{T}$ is a triple

$$\mathcal{F} = (\mathcal{F}_{ucond}, \mathcal{F}_{strong}, \mathcal{F}_{weak})$$

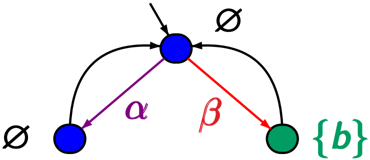
where $\mathcal{F}_{ucond}, \mathcal{F}_{strong}, \mathcal{F}_{weak} \subseteq 2^{Act}$.

An execution ρ is called $\mathcal{F}$-fair iff

- ρ is unconditionally A-fair for all $A \in \mathcal{F}_{ucond}$
- ρ is strongly A-fair for all $A \in \mathcal{F}_{strong}$
- ρ is weakly A-fair for all $A \in \mathcal{F}_{weak}$

If $\mathcal{T}$ is a TS and E a LT property over AP then:

$$\mathcal{T} \models_{\mathcal{F}} E \quad \overset{\text{def}}{\iff} \quad FairTraces_{\mathcal{F}}(\mathcal{T}) \subseteq E$$



$\mathcal{T} \models_{\mathcal{F}}$ "infinitely often b" ?

answer: **no**

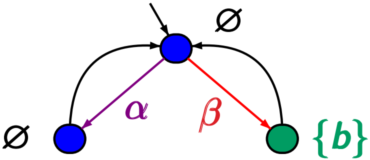
fairness assumption $\mathcal{F}$

- no unconditional fairness condition $\leftarrow \mathcal{F}_{ucond} = \varnothing$
- strong fairness for $\{\alpha, \beta\}$ $\leftarrow \mathcal{F}_{strong} = \{\{\alpha, \beta\}\}$
- no weak fairness condition $\leftarrow \mathcal{F}_{weak} = \varnothing$

$\bullet \xrightarrow{\alpha} \bullet \longrightarrow \bullet \xrightarrow{\alpha} \bullet \longrightarrow \bullet \xrightarrow{\alpha} \bullet \longrightarrow \cdots$ $\mathcal{F}$-fair

actions in $\{\alpha, \beta\}$ are executed infinitely many times

Example: fair satisfaction relation

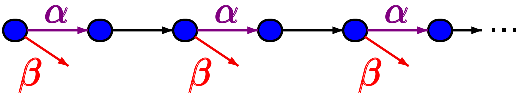


$\mathcal{T} \models_{\mathcal{F}}$ "infinitely often b" ?

answer: **no**

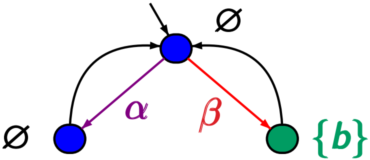
fairness assumption $\mathcal{F}$

- strong fairness for α $\leftarrow \mathcal{F}_{strong} = \{\{\alpha\}\}$
- weak fairness for β $\leftarrow \mathcal{F}_{weak} = \{\{\beta\}\}$
- no unconditional fairness assumption



$\mathcal{F}$-fair

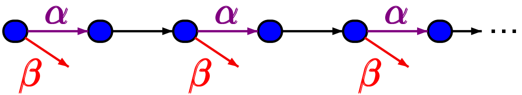
Example: fair satisfaction relation



$\mathcal{T} \models_{\mathcal{F}}$ "infinitely often b"

fairness assumption $\mathcal{F}$

- strong fairness for β $\leftarrow \mathcal{F}_{strong} = \{\{\beta\}\}$
- no weak fairness assumption
- no unconditional fairness assumption

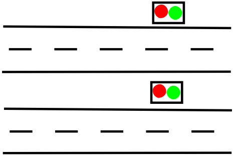


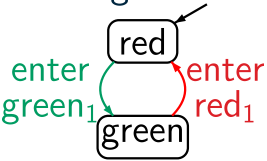
is not $\mathcal{F}$-fair

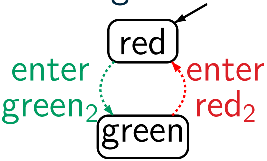
Which type of fairness?

fairness assumptions should be
as weak as possible

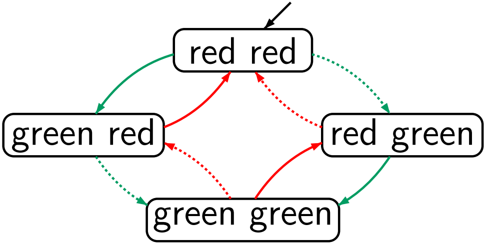
Two independent traffic lights







A_1 = actions of light 1
A_2 = actions of light 2



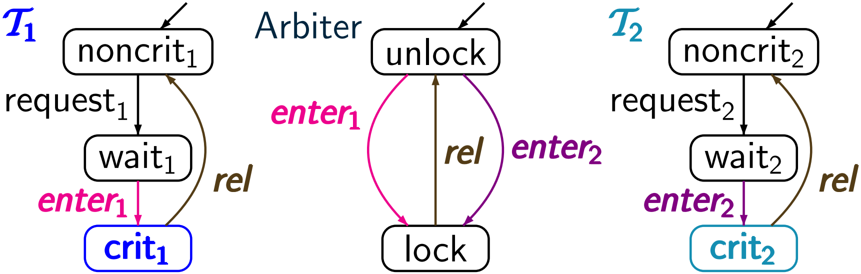
fairness assumption $\mathcal{F}$:
$\mathcal{F}_{ucond} = \varnothing$
$\mathcal{F}_{strong} = \varnothing$
$\mathcal{F}_{weak} = \{A_1, A_2\}$

light 1 $|||$ light 2 $\models_{\mathcal{F}} E$

$E \;\widehat{=}\;$ "both lights are infinitely often green"

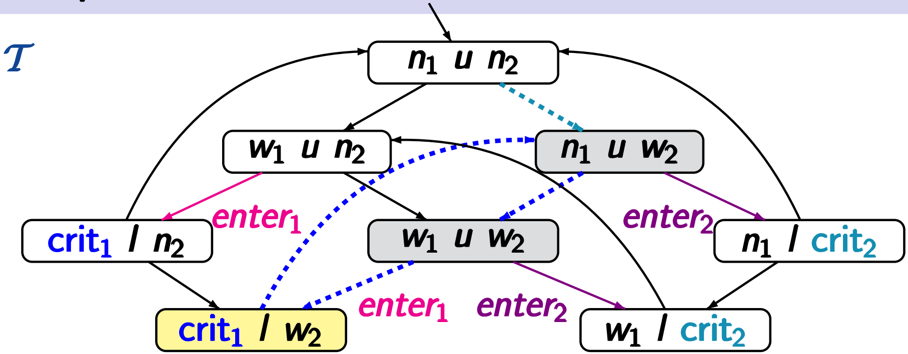
Example: MUTEX with fair arbiter

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



$\mathcal{T}_1$ and $\mathcal{T}_2$ compete to communicate with the arbiter by means of the actions ***enter$_1$*** and ***enter$_2$***, respectively

Example: MUTEX with fair arbiter



LT property E: each waiting process eventually enters its critical section

fairness assumption $\mathcal{F}$

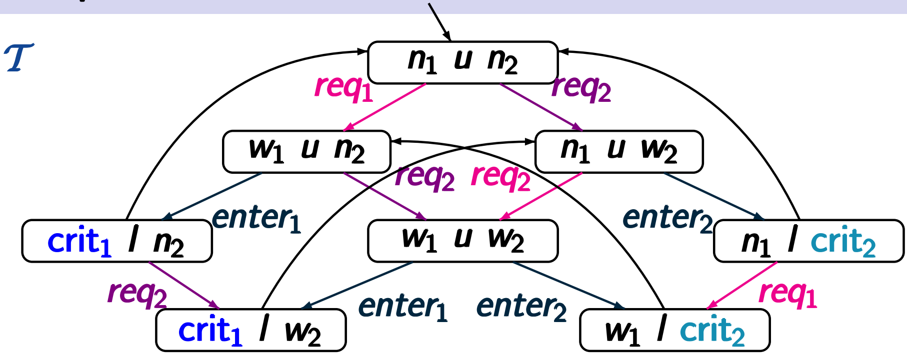
$\mathcal{F}_{ucond} = \mathcal{F}_{strong} = \varnothing$

$\mathcal{F}_{weak} = \{\{enter_1\}, \{enter_2\}\}$

$\mathcal{T} \not\models_{\mathcal{F}} E$

as $enter_2$ is not enabled in $\langle crit_1, l, w_2 \rangle$

Example: MUTEX with fair arbiter



E: each waiting process eventually enters its crit. section

D: each process enters its critical section infinitely often

$$\mathcal{F}_{ucond} = \varnothing$$
$$\mathcal{F}_{strong} = \{\{enter_1\}, \{enter_2\}\}$$
$$\mathcal{F}_{weak} = \{\{req_1\}, \{req_2\}\}$$

$$\mathcal{T} \models_{\mathcal{F}} E,$$
$$\mathcal{T} \models_{\mathcal{F}} D$$

For asynchronous systems:

$$\boxed{\text{parallelism} \;=\; \text{interleaving} + \text{fairness}}$$

should be as weak as possible

rule of thumb:

- strong fairness for the
  - choice between dependent actions
  - resolution of competitions
- weak fairness for the nondetermism obtained from the interleaving of independent actions
- unconditional fairness: only of theoretical interest

Purpose of fairness conditions

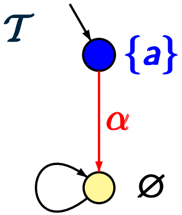
$$\boxed{\text{parallelism} \;=\; \text{interleaving} + \text{fairness}}$$

Process fairness and other fairness conditions

- can compensate information loss due to interleaving
  or rule out other unrealistic pathological cases
- can be requirements for a scheduler
  or requirements for environment
- can be verifiable system properties

liveness properties:	fairness can be essential
safety properties:	fairness is irrelevant

Realizability of fairness assumptions



fairness assumption $\mathcal{F}$:
unconditional fairness for action set $\{\alpha\}$

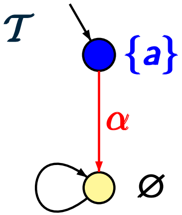
↑

not realizable

does $\mathcal{T} \models_{\mathcal{F}}$ "infinitely often a" hold ?

answer: **yes** as there is no fair path

Realizability requires that each initial finite path fragment can be extended to a $\mathcal{F}$-fair path



fairness assumption $\mathcal{F}$:
unconditional fairness
for action set $\{\alpha\}$

not realizable

does $\mathcal{T} \models_{\mathcal{F}}$ "infinitely often a" hold ?

answer: **yes** as there is no fair path

Fairness assumption $\mathcal{F}$ is said to be realizable for a transition system $\mathcal{T}$ if for each reachable state s in $\mathcal{T}$ there exists a $\mathcal{F}$-fair path starting in s

fairness assumption $\mathcal{F} = (\mathcal{F}_{ucond}, \mathcal{F}_{strong}, \mathcal{F}_{weak})$ for TS $\mathcal{T}$

- unconditional fairness for $A \in \mathcal{F}_{ucond}$

  $\leadsto$ might not be realizable

- strong fairness for $A \in \mathcal{F}_{strong}$
- weak fairness for $A \in \mathcal{F}_{weak}$

↑

can always be guaranteed by a scheduler, i.e.,
an instance that resolves the nondeterminism in $\mathcal{T}$

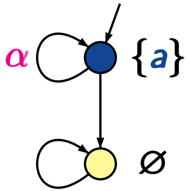
Safety and realizable fairness

Realizable fairness assumptions are irrelevant for safety properties

Realizable fairness assumptions are irrelevant for safety properties

> If $\mathcal{F}$ is a realizable fairness assumption for TS $\mathcal{T}$ and E a safety property then:
>
> $$\mathcal{T} \models E \quad \text{iff} \quad \mathcal{T} \models_{\mathcal{F}} E$$

... wrong for non-realizable fairness assumptions



$\mathcal{F}$: unconditional fairness for $\{\alpha\}$

E = invariant "always a"

$\mathcal{T} \not\models E$, but $\mathcal{T} \models_{\mathcal{F}} E$