Overview

Introduction
Modelling parallel systems

**Linear Time Properties**
state-based and linear time view
definition of linear time properties
invariants and safety
liveness and fairness

Regular Properties
Linear Temporal Logic
Computation-Tree Logic
Equivalences and Abstraction
“liveness: something good will happen.”
“liveness: something good will happen.”

“event a will occur eventually”
“liveness: something good will happen.”

“event a will occur eventually”

e.g., termination for sequential programs
Liveness

“liveness: something good will happen.”

“event \textit{a} will occur \textit{eventually}”

\textit{e.g.}, \textit{termination} for sequential programs

\textit{“event \textit{a} will occur infinitely many times”}

\textit{e.g.}, \textit{starvation freedom} for dining philosophers
“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”
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
which property type?

- Each philosopher thinks infinitely often.
which property type?

- Each philosopher thinks infinitely often.

liveness
which property type?

- Each philosopher thinks infinitely often.
- Two philosophers next to each other never eat at the same time.
which property type?

• Each philosopher thinks infinitely often. **liveness**

• Two philosophers next to each other never eat at the same time. **invariant**
which property type?

• 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.
Each philosopher thinks infinitely often. \textit{liveness}

Two philosophers next to each other never eat at the same time. \textit{invariant}

Whenever a philosopher eats then he has been thinking at some time \textit{before}. \textit{safety}
which property type?

• Each philosopher thinks infinitely often.  
  \textit{liveness}

• Two philosophers next to each other never eat at the same time.  
  \textit{invariant}

• Whenever a philosopher eats then he has been thinking at some time before.  
  \textit{safety}

• Whenever a philosopher eats then he will think some time afterwards.
Each philosopher thinks infinitely often.

Two philosophers next to each other never eat at the same time.

Whenever a philosopher eats then he has been thinking at some time before.

Whenever a philosopher eats then he will think some time afterwards.
which property type?

- Each philosopher thinks infinitely often.
  \[ \text{liveness} \]

- Two philosophers next to each other never eat at the same time.
  \[ \text{invariant} \]

- Whenever a philosopher eats then he has been thinking at some time before.
  \[ \text{safety} \]

- Whenever a philosopher eats then he will think some time afterwards.
  \[ \text{liveness} \]

- Between two eating phases of philosopher \( i \) lies at least one eating phase of philosopher \( i+1 \).
Each philosopher thinks infinitely often.  

Two philosophers next to each other never eat at the same time.  

Whenever a philosopher eats then he has been thinking at some time before.  

Whenever a philosopher eats then he will think some time afterwards.  

Between two eating phases of philosopher $i$ lies at least one eating phase of philosopher $i+1$.
many different formal definitions of liveness have been suggested in the literature
many different formal definitions of liveness have been suggested in the literature

here: one just example for a formal definition of liveness
Definition of liveness properties
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 \( E \).
Definition of liveness properties

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

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

recall: $\text{pref}(E) =$ set of all finite, nonempty prefixes of words in $E$
Definition of liveness properties

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

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

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
Examples for liveness properties

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

Examples for $AP = \{\text{crit}_i : i = 1, \ldots, n\}$:
Examples for liveness properties

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

Examples for $\text{AP} = \{\text{crit}_i : i = 1, \ldots, n\}$:

- each process will eventually enter its critical section
Examples for liveness properties

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

Examples for $AP = \{\text{crit}_i : i = 1, \ldots, n\}$:

- each process will eventually enter its critical section

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

$\forall i \in \{1, \ldots, n\} \exists k \geq 0. \text{crit}_i \in A_k$
An LT property $E$ over $AP$ is called a liveness property if $\text{pref}(E) = (2^{\text{AP}})^+$

Examples for $AP = \{\text{crit}_i : i = 1, \ldots, n\}$:

- each process will eventually enter its critical section
- each process will enter its critical section infinitely often
Examples for liveness properties

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

Examples for $AP = \{\text{crit}_i : i = 1, \ldots, n\}$:

- each process will eventually enter its critical section
- each process will enter its critical section infinitely often

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

$\forall i \in \{1, \ldots, n\} \ \exists \ k \geq 0. \ \text{crit}_i \in A_k$
Examples for liveness properties

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

Examples for $AP = \{\text{wait}_i, \text{crit}_i : i = 1, \ldots, n\}$:

- Each process will eventually enter its critical section
- Each process will enter its crit. section inf. often
- Whenever a process is waiting then it will eventually enter its critical section
Examples for liveness properties

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

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

- each process will eventually enter its critical section
- each process will enter its crit. section inf. often
- whenever a process is waiting then it will eventually enter its critical section

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

$\forall i \in \{1, \ldots, n\} \ \forall j \geq 0. \ \text{wait}_i \in A_j$ 

$\rightarrow \exists k > j. \ \text{crit}_i \in A_k$
Recall: safety properties, prefix closure

Let $E$ be an LT-property, i.e., $E \subseteq (2^{AP})^\omega$
Recall: safety properties, prefix closure

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

$E$ is a safety property

iff $\forall \sigma \in (2^{AP})^\omega \setminus E \ \exists A_0 A_1 \ldots A_n \in \text{pref}(\sigma) \ \text{s.t.}$

$$\{ \sigma' \in E : A_0 A_1 \ldots A_n \in \text{pref}(\sigma') \} = \emptyset$$
Recall: safety properties, prefix closure

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

$E$ is a safety property

iff $\forall \sigma \in (2^{\text{AP}})^\omega \setminus E \ \exists A_0 A_1 \ldots A_n \in \text{pref}(\sigma)$ s.t.

$$\{ \sigma' \in E : A_0 A_1 \ldots A_n \in \text{pref}(\sigma') \} = \emptyset$$

remind:

$$\text{pref}(\sigma) = \text{set of all finite, nonempty prefixes of } \sigma$$
$$\text{pref}(E) = \bigcup_{\sigma \in E} \text{pref}(\sigma)$$
Recall: safety properties, prefix closure

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

$E$ is a safety property

iff $\forall \sigma \in (2^{AP})^\omega \setminus E \exists A_0 A_1 \ldots A_n \in \text{pref}(\sigma) \text{ s.t.}$

$\{\sigma' \in E : A_0 A_1 \ldots A_n \in \text{pref}(\sigma')\} = \emptyset$

iff $cl(E) = E$

remind: $cl(E) = \{\sigma \in (2^{AP})^\omega : \text{pref}(\sigma) \subseteq \text{pref}(E)\}$

$\text{pref}(\sigma) =$ set of all finite, nonempty prefixes of $\sigma$

$\text{pref}(E) = \bigcup_{\sigma \in E} \text{pref}(\sigma)$
For each LT-property $E$, there exists a safety property $SAFE$ and a liveness property $LIVE$ s.t.

$$E = SAFE \cap LIVE$$
Decomposition theorem

For each LT-property $E$, there exists a safety property $SAFE$ and a liveness property $LIVE$ s.t.

$E = SAFE \cap LIVE$

Proof:
Decomposition theorem

For each LT-property $E$, there exists a safety property $SAFE$ and a liveness property $LIVE$ s.t.

$$E = SAFE \cap LIVE$$

Proof: Let $SAFE \overset{\text{def}}{=} cl(E)$
Decomposition theorem

For each LT-property $E$, there exists a safety property $SAFE$ and a liveness property $LIVE$ s.t.

$$E = SAFE \cap LIVE$$

Proof: Let $SAFE \overset{\text{def}}{=} cl(E)$

---

remind: $cl(E) = \{ \sigma \in (2^{AP})^\omega : \text{pref}(\sigma) \subseteq \text{pref}(E) \}$

$\text{pref}(\sigma) =$ set of all finite, nonempty prefixes of $\sigma$

$\text{pref}(E) = \bigcup_{\sigma \in E} \text{pref}(\sigma)$
Decomposition theorem

For each LT-property $E$, there exists a safety property $SAFE$ and a liveness property $LIVE$ s.t.

$$E = SAFE \cap LIVE$$

Proof: Let $SAFE \overset{\text{def}}{=} cl(E)$

$$LIVE \overset{\text{def}}{=} E \cup ((2^{AP})^\omega \setminus cl(E))$$

remind: $cl(E) = \{ \sigma \in (2^{AP})^\omega : \text{pref}(\sigma) \subseteq \text{pref}(E) \}$

$\text{pref}(\sigma) =$ set of all finite, nonempty prefixes of $\sigma$

$\text{pref}(E) = \bigcup_{\sigma \in E} \text{pref}(\sigma)$
Decomposition theorem

For each LT-property $E$, there exists a safety property $SAFE$ and a liveness property $LIVE$ s.t.

$$E = SAFE \cap LIVE$$

**Proof:** Let $SAFE \overset{\text{def}}{=} cl(E)$

$$LIVE \overset{\text{def}}{=} E \cup \left( (2^{AP})^{\omega} \setminus cl(E) \right)$$

Show that:

- $E = SAFE \cap LIVE$
- $SAFE$ is a safety property
- $LIVE$ is a liveness property
Decomposition theorem

For each LT-property $E$, there exists a safety property $SAFE$ and a liveness property $LIVE$ s.t.

$$E = SAFE \cap LIVE$$

**Proof:** Let

- $SAFE \overset{\text{def}}{=} cl(E)$
- $LIVE \overset{\text{def}}{=} E \cup (\,(2^{AP})^\omega \setminus cl(E))$

Show that:

- $E = SAFE \cap LIVE$ \checkmark
- $SAFE$ is a safety property
- $LIVE$ is a liveness property
Decomposition theorem

For each LT-property $E$, there exists a safety property $SAFE$ and a liveness property $LIVE$ s.t.

$$E = SAFE \cap LIVE$$

Proof: Let $SAFE \overset{def}{=} cl(E)$

$LIVE \overset{def}{=} E \cup ((2^{AP})^{\omega} \setminus cl(E))$

Show that:

- $E = SAFE \cap LIVE$ \checkmark
- $SAFE$ is a safety property as $cl(SAFE) = SAFE$
- $LIVE$ is a liveness property
Decomposition theorem

For each LT-property \( E \), there exists a safety property \( \text{SAFE} \) and a liveness property \( \text{LIVE} \) s.t.

\[
E = \text{SAFE} \cap \text{LIVE}
\]

Proof: Let \( \text{SAFE} \overset{\text{def}}{=} \text{cl}(E) \)

\[
\text{LIVE} \overset{\text{def}}{=} E \cup \left( (2^{AP})^\omega \setminus \text{cl}(E) \right)
\]

Show that:

- \( E = \text{SAFE} \cap \text{LIVE} \) \( \checkmark \)
- \( \text{SAFE} \) is a safety property as \( \text{cl}(\text{SAFE}) = \text{SAFE} \)
- \( \text{LIVE} \) is a liveness property, i.e., \( \text{pref}(\text{LIVE}) = (2^{AP})^+ \)
Which LT properties are both a safety and a liveness property?
Which LT properties are both a safety and a liveness property?

answer: The set $\left(2^{AP}\right)^\omega$ is the only LT property which is a safety property and a liveness property.
Which LT properties are both a safety and a liveness property?

answer: The set \((2^{AP})^\omega\) is the only LT property which is a safety property and a liveness property.

- \((2^{AP})^\omega\) is a safety and a liveness property: √
Which LT properties are both a safety and a liveness property?

answer: The set \((2^{AP})^\omega\) is the only LT property which is a safety property and a liveness property.

- \((2^{AP})^\omega\) is a safety and a liveness property: \(\checkmark\)
- If \(E\) is a liveness property then

\[\text{pref}(E) = (2^{AP})^+\]
Which LT properties are both a safety and a liveness property?

answer: The set $(2^{AP})^\omega$ is the only LT property which is a safety property and a liveness property:

- $(2^{AP})^\omega$ is a safety and a liveness property: √
- If $E$ is a liveness property then $\text{pref}(E) = (2^{AP})^+$
  $\implies \text{cl}(E) = (2^{AP})^\omega$
Which LT properties are both a safety and a liveness property?

*answer:* The set \((2^{AP})^\omega\) is the only LT property which is a safety property and a liveness property.

- \((2^{AP})^\omega\) is a safety and a liveness property: ✓
- If \(E\) is a liveness property then
  \[
  \text{pref}(E) = (2^{AP})^+
  \Rightarrow \quad \text{cl}(E) = (2^{AP})^\omega
  \]

  If \(E\) is a safety property too, then \(\text{cl}(E) = E\).
Being safe and live

Which LT properties are both a safety and a liveness property?

*answer*: The set \((2^{AP})^\omega\) is the only LT property which is a safety property and a liveness property

- \((2^{AP})^\omega\) is a safety and a liveness property:  ✓
- If \(E\) is a liveness property then 
  \[
  \text{pref}(E) = (2^{AP})^+
  \]
  \[
  \implies cl(E) = (2^{AP})^\omega
  \]

If \(E\) is a safety property too, then \(cl(E) = E\). Hence \(E = cl(E) = (2^{AP})^\omega\).
Observation

liveness properties are often violated although we expect them to hold
Two independent traffic lights

- - - - - - -

light 1

red_1

green_1

light 2

red_2

green_2
Two independent traffic lights

light 1

- red
- green

light 2

- red
- green

light 1 ||| light 2
Two independent traffic lights

light 1

red_1

green_1

light 2

red_2

green_2

light 1 ||| light 2

\[ \neg \text{“infinitely often } \text{green}_1 \]
Two independent traffic lights

light 1

red$_1$

green$_1$

light 2

red$_2$

green$_2$

light 1 \text{|||} light 2

\nottently often green$_1$
Two independent traffic lights

light 1

<table>
<thead>
<tr>
<th>red1</th>
</tr>
</thead>
<tbody>
<tr>
<td>green1</td>
</tr>
</tbody>
</table>

light 2

<table>
<thead>
<tr>
<th>red2</th>
</tr>
</thead>
<tbody>
<tr>
<td>green2</td>
</tr>
</tbody>
</table>

light 1 ||| light 2

light 1 ||| light 2 \not\models \text{“infinitely often } \text{green}_1 \text{”}

although light 1 \models \text{“infinitely often } \text{green}_1 \text{”}
Two independent traffic lights

light 1

- red
- green

light 2

- red
- green

light 1 ||| light 2

- red
- green

“infinitely often green_1”

interleaving is completely time abstract!
Mutual exclusion (semaphore)

\[ \mathcal{I}_{sem} \]

- **noncrit\_1 noncrit\_2**
  - \( y = 1 \)

- **wait\_1 noncrit\_2**
  - \( y = 1 \)

- **crit\_1 noncrit\_2**
  - \( y = 0 \)

- **wait\_1 wait\_2**
  - \( y = 1 \)

- **crit\_1 wait\_2**
  - \( y = 0 \)

- **noncrit\_1 wait\_2**
  - \( y = 1 \)

- **noncrit\_1 crit\_2**
  - \( y = 0 \)

- **wait\_1 crit\_2**
  - \( y = 0 \)
Mutual exclusion (semaphore)

Liveness property \( \equiv \) “each waiting process will eventually enter its critical section”
Mutual exclusion (semaphore)

\[ \mathcal{I}_{\text{sem}} \]

- \( \text{noncrit}_1 \) \( \text{noncrit}_2 \) \( y=1 \)
- \( \text{wait}_1 \) \( \text{noncrit}_2 \) \( y=1 \)
- \( \text{crit}_1 \) \( \text{noncrit}_2 \) \( y=0 \)
- \( \text{crit}_1 \) \( \text{wait}_2 \) \( y=0 \)
- \( \text{wait}_1 \) \( \text{wait}_2 \) \( y=1 \)
- \( \text{noncrit}_1 \) \( \text{crit}_2 \) \( y=0 \)
- \( \text{wait}_1 \) \( \text{crit}_2 \) \( y=0 \)

\[ \mathcal{I}_{\text{sem}} \not\models \text{“each waiting process will eventually enter its critical section”} \]
Mutual exclusion (semaphore)

$\mathcal{I}_{\text{sem}}$  

(noncrit$_1$ noncrit$_2$)  

$y = 1$  

wait$_1$ noncrit$_2$  

$y = 1$  

wait$_1$ wait$_2$  

noncrit$_1$ wait$_2$  

$y = 1$  

crit$_1$ noncrit$_2$  

$y = 0$  

wait$_1$ crit$_2$  

$y = 0$  

noncrit$_1$ crit$_2$  

$y = 0$  

$\mathcal{I}_{\text{sem}} \not\models$  

“each waiting process will eventually enter its critical section”
Mutual exclusion (semaphore)

\[ T_{sem} \]

noncrit\textsubscript{1} noncrit\textsubscript{2}
\[ y=1 \]

wait\textsubscript{1} noncrit\textsubscript{2}
\[ y=1 \]

noncrit\textsubscript{1} wait\textsubscript{2}
\[ y=1 \]

wait\textsubscript{1} wait\textsubscript{2}
\[ y=1 \]

noncrit\textsubscript{1} crit\textsubscript{2}
\[ y=0 \]

crit\textsubscript{1} wait\textsubscript{2}
\[ y=0 \]

crit\textsubscript{1} noncrit\textsubscript{2}
\[ y=0 \]

wait\textsubscript{1} crit\textsubscript{2}
\[ y=0 \]

wait\textsubscript{1} noncrit\textsubscript{2}
\[ y=1 \]

crit\textsubscript{1} wait\textsubscript{2}
\[ y=0 \]

\[ T_{sem} \not\models \text{“each waiting process will eventually enter its critical section”} \]

level of abstraction is too coarse!
Process fairness
Process fairness

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

possible interleavings:

$P_1 \ P_2 \  P_2 \ P_1 \ P_1 \ P_1 \ P_1 \ P_2 \ P_2 \ P_2 \ P_2 \ P_2 \ P_1 \ P_1 \ ...$

$P_1 \ P_1 \ P_2 \ P_1 \ P_1 \ P_2 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_2 \ P_1 \ P_2 \ P_1 \ ...$
Process fairness

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

possible interleavings:

$P_1 \ P_2 \ P_2 \ P_1 \ P_1 \ P_1 \ P_2 \ P_1 \ P_2 \ P_2 \ P_2 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1$ ...

$P_1 \ P_1 \ P_2 \ P_1 \ P_1 \ P_2 \ P_1 \ P_2 \ P_1 \ P_1 \ P_2 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1$ ...

$P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1$ ...
Process fairness

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

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

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

$P_1 P_1 P_1 P_1 P_1 P_1 P_1 P_1 P_1 P_1 P_1 P_1 \ldots$ unfair
Process fairness

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

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

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

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

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

- unconditional fairness
- strong fairness
- weak fairness
Nuances of fairness

- unconditional fairness, e.g., every process enters gets its turn infinitely often.

- strong fairness

- weak fairness
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
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
Fairness for action-set

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

$\rho = s_0 \xrightarrow{\alpha_0} s_1 \xrightarrow{\alpha_1} s_2 \xrightarrow{\alpha_2} \ldots$ infinite execution fragment
Let $\mathcal{T}$ be a TS with action-set $\text{Act}$, $A \subseteq \text{Act}$ 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 $\rho$
- strong $A$-fairness of $\rho$
- weak $A$-fairness of $\rho$
Let $\mathcal{T}$ be a TS with action-set $\text{Act}$, $A \subseteq \text{Act}$ and $
abla = 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 $\nabla$
- strong $A$-fairness of $\nabla$
- weak $A$-fairness of $\nabla$

using the following notations:

$$\text{Act}(s_i) = \{ \beta \in \text{Act} : \exists s' \text{ s.t. } s_i \xrightarrow{\beta} s' \}$$
Fairness for action-set

Let $\mathcal{T}$ be a TS with action-set $\textbf{Act}$, $A \subseteq \textbf{Act}$ 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 $\rho$
- strong $A$-fairness of $\rho$
- weak $A$-fairness of $\rho$

using the following notations:

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

$s \equiv \exists \text{ “there exists infinitely many ...”}$
Fairness for action-set

Let $\mathcal{T}$ be a TS with action-set $\text{Act}$, $A \subseteq \text{Act}$ 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 $\rho$
- strong $A$-fairness of $\rho$
- weak $A$-fairness of $\rho$

using the following notations:

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

$\exists^\infty \equiv \text{“there exists infinitely many ...”}$

$\forall^\infty \equiv \text{“for all, but finitely many ...”}$
Let $\mathcal{T}$ be a TS with action-set $\textbf{Act}$, $A \subseteq \textbf{Act}$ and 

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

- $\rho$ is unconditionally $A$-fair, if
Fairness for action-set

Let $\mathcal{T}$ be a TS with action-set $\textbf{Act}$, $A \subseteq \textbf{Act}$ and 
\[ \rho = s_0 \xrightarrow{\alpha_0} s_1 \xrightarrow{\alpha_1} s_2 \xrightarrow{\alpha_2} \ldots \] infinite execution fragment

- $\rho$ is unconditionally $A$-fair, if $\exists i \geq 0. \alpha_i \in A$

"actions in $A$ will be taken infinitely many times"
Fairness for action-set

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

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

• $\rho$ is unconditionally $A$-fair, if $\exists \ i \geq 0. \ \alpha_i \in A$

• $\rho$ is strongly $A$-fair, if
Fairness for action-set

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

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

- $\rho$ is unconditionally $A$-fair, if $\exists i \geq 0. \alpha_i \in A$
- $\rho$ is strongly $A$-fair, if

$$\exists i \geq 0. A \cap \text{Act}(s_i) \neq \emptyset \implies \exists i \geq 0. \alpha_i \in A$$

“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 $\text{Act}$, $A \subseteq \text{Act}$ and

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

- $\rho$ is unconditionally $A$-fair, if $\exists \ i \geq 0. \ \alpha_i \in A$

- $\rho$ is strongly $A$-fair, if

  $\exists \ i \geq 0. \ A \cap \text{Act}(s_i) \neq \emptyset \quad \Rightarrow \quad \exists \ i \geq 0. \ \alpha_i \in A$

- $\rho$ is weakly $A$-fair, if
Fairness for action-set

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

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

• $\rho$ is unconditionally $A$-fair, if $\exists i \geq 0. \alpha_i \in A$

• $\rho$ is strongly $A$-fair, if

$\exists i \geq 0. A \cap \text{Act}(s_i) \neq \emptyset \implies \exists i \geq 0. \alpha_i \in A$

• $\rho$ is weakly $A$-fair, if

$\forall i \geq 0. A \cap \text{Act}(s_i) \neq \emptyset \implies \exists i \geq 0. \alpha_i \in A$

“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 $\text{Act}$, $A \subseteq \text{Act}$ and

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

- $\rho$ is unconditionally $A$-fair, if $\exists \ i \geq 0. \ \alpha_i \in A$
- $\rho$ is strongly $A$-fair, if

\[ \exists \ i \geq 0. \ A \cap \text{Act}(s_i) \neq \emptyset \quad \Rightarrow \quad \exists \ i \geq 0. \ \alpha_i \in A \]

- $\rho$ is weakly $A$-fair, if

\[ \forall \ i \geq 0. \ A \cap \text{Act}(s_i) \neq \emptyset \quad \Rightarrow \quad \exists \ i \geq 0. \ \alpha_i \in A \]

unconditionally $A$-fair $\Rightarrow$ strongly $A$-fair

$\Rightarrow$ weakly $A$-fair
Let $\mathcal{T}$ be a TS with action-set $\textbf{Act}$, $A \subseteq \textbf{Act}$ and 
\[ \rho = s_0 \xrightarrow{\alpha_0} s_1 \xrightarrow{\alpha_1} s_2 \xrightarrow{\alpha_2} \ldots \] an infinite execution fragment

- $\rho$ is unconditionally $A$-fair, if $\exists i \geq 0. \, \alpha_i \in A$
- $\rho$ is strongly $A$-fair, if $\exists i \geq 0. \, A \cap \text{Act}(s_i) \neq \emptyset \implies \exists i \geq 0. \, \alpha_i \in A$
- $\rho$ is weakly $A$-fair, if $\forall i \geq 0. \, A \cap \text{Act}(s_i) \neq \emptyset \implies \exists i \geq 0. \, \alpha_i \in A$

<table>
<thead>
<tr>
<th>unconditionally $A$-fair</th>
<th>$\implies$</th>
<th>strongly $A$-fair</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\implies$</td>
<td></td>
<td>weakly $A$-fair</td>
</tr>
</tbody>
</table>
Strong and weak action fairness

strong $A$-fairness is \textit{violated} if

\begin{itemize}
  \item no $A$-actions are executed from a certain moment
  \item $A$-actions are enabled infinitely many times
\end{itemize}
Strong and weak action fairness

Strong \textbf{A}-fairness is \textit{violated} if

- no \textbf{A}-actions are executed from a certain moment
- \textbf{A}-actions are enabled infinitely many times

Weak \textbf{A}-fairness is \textit{violated} if

- no \textbf{A}-actions are executed from a certain moment
- \textbf{A}-actions are \textit{continuously} enabled from some moment on
Mutual exclusion with arbiter

$T_1$
- **noncrit$_1$**
  - **wait$_1$**
  - **request$_1$**
  - **enter$_1$**
  - **release**

$T_2$
- **noncrit$_2$**
  - **wait$_2$**
  - **request$_2$**
  - **enter$_2$**
  - **release**
Mutual exclusion with arbiter

\[ T_1 \]
- noncrit\(_1\) \rightarrow wait\(_1\) \rightarrow \text{request\(_1\)} \rightarrow \text{crit\(_1\)} \rightarrow \text{release} \rightarrow \text{unlock} \rightarrow \text{enter\(_1\)} \rightarrow \text{rel} \rightarrow \text{lock} \rightarrow \text{enter\(_1\)} \rightarrow \text{release}

Arbiter

\[ T_2 \]
- noncrit\(_2\) \rightarrow wait\(_2\) \rightarrow \text{request\(_2\)} \rightarrow \text{crit\(_2\)} \rightarrow \text{release} \rightarrow \text{unlock} \rightarrow \text{enter\(_2\)} \rightarrow \text{rel} \rightarrow \text{lock} \rightarrow \text{enter\(_2\)} \rightarrow \text{release}
Mutual exclusion with arbiter

\[ T_1 \]
- noncrit\(_1\)
- request\(_1\)
- wait\(_1\)
- enter\(_1\)
- crit\(_1\)

\[ T_2 \]
- noncrit\(_2\)
- request\(_2\)
- wait\(_2\)
- enter\(_2\)

\( \mathcal{T}_1 \parallel \text{Arbiter} \parallel \mathcal{T}_2 \)

Arbiter

- unlock
- rel
- lock
- enter\(_1\)
- enter\(_2\)

\( n_1 \cup n_2 \)
- release
- \( n_1 \cup w_2 \)
- \( w_1 \cup n_2 \)
- \( w_1 \cup w_2 \)
- \( n_1 \cup \text{crit}_2 \)
- \( w_1 \cup \text{crit}_2 \)

\( \text{crit}_1 \parallel n_2 \parallel \text{crit}_1 \parallel w_2 \)
Unconditional, strongly or weakly fair?

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

$\text{crit}_1 \quad / \quad n_2$

$\text{crit}_1 \quad / \quad w_2$

$\text{enter}_1$

$n_1 \quad u \quad n_2$

$\text{enter}_1$

$\text{enter}_2$

$n_1 \quad u \quad w_2$

$\text{enter}_2$

$n_1 \quad / \quad \text{crit}_2$

$\text{crit}_1 \quad / \quad w_2$

$w_1 \quad / \quad \text{crit}_2$

$w_1 \quad u \quad w_2$
Unconditional, strongly or weakly fair?

\[ T_1 \parallel \text{Arbiter} \parallel T_2 \]

\[ \langle n_1, u, n_2 \rangle \rightarrow \left( \langle n_1, u, w_2 \rangle \rightarrow \langle w_1, u, w_2 \rangle \rightarrow \langle \text{crit}_1, l, w_2 \rangle \right)^\omega \]

- unconditional \( A \)-fairness:
- strong \( A \)-fairness:
- weak \( A \)-fairness:
Unconditional, strongly or weakly fair?

\[ \mathcal{T}_1 \parallel \text{Arbiter} \parallel \mathcal{T}_2 \]

fairness for action set \( A = \{ \text{enter}_1 \} \):

\[
\langle n_1, u, n_2 \rangle \rightarrow \left( \langle n_1, u, w_2 \rangle \rightarrow \langle w_1, u, w_2 \rangle \rightarrow \langle \text{crit}_1, l, w_2 \rangle \right)^\omega
\]

- unconditional \( A \)-fairness: yes
- strong \( A \)-fairness: yes \( \leftrightarrow \) unconditionally fair
- weak \( A \)-fairness: yes \( \leftrightarrow \) unconditionally fair
Unconditional, strongly or weakly fair?

 fairness for action-set $A = \{\text{enter}_1\}$:

\[
\left( \langle n_1, u, n_2 \rangle \rightarrow \langle n_1, u, w_2 \rangle \rightarrow \langle n_1, l, \text{crit}_2 \rangle \right)^\omega
\]

- unconditional $A$-fairness:
- strong $A$-fairness:
- weak $A$-fairness:
Unconditional, strongly or weakly fair?

\( \mathcal{T}_1 \parallel \text{Arbiter} \parallel \mathcal{T}_2 \)

\[
\begin{align*}
\text{crit}_1 \& n_2 & \xrightarrow{\text{enter}_1} & \text{crit}_1 \& w_2 \\
& \xrightarrow{\text{enter}_1} & \text{crit}_1 \& w_2 & \xrightarrow{\text{enter}_2} & n_1 \& \text{crit}_2 \\
& \xrightarrow{\text{enter}_1 \text{ enter}_2} & \text{crit}_1 \& w_2 & \xrightarrow{\text{enter}_1 \text{ enter}_2} & w_1 \& \text{crit}_2
\end{align*}
\]

Fairness for action-set \( A = \{ \text{enter}_1 \} \):

\[
\left( \langle n_1, u, n_2 \rangle \rightarrow \langle n_1, u, w_2 \rangle \rightarrow \langle n_1, l, \text{crit}_2 \rangle \right) \omega
\]

- Unconditional \( A \)-fairness: no
- Strong \( A \)-fairness: yes \( \leftarrow A \) never enabled
- Weak \( A \)-fairness: yes \( \leftarrow \) strongly \( A \)-fair
Unconditional, strongly or weakly fair?

\[\mathcal{T}_1 \parallel \text{Arbiter} \parallel \mathcal{T}_2\]

Fairness for action-set \(A = \{\text{enter}_1\}\):

\[\langle n_1, u, n_2 \rangle \rightarrow (\langle w_1, u, n_2 \rangle \rightarrow \langle w_1, u, w_2 \rangle \rightarrow \langle n_1, l, \text{crit}_2 \rangle)^\omega\]

- unconditional \(A\)-fairness:
- strong \(A\)-fairness:
- weak \(A\)-fairness:
Unconditional, strongly or weakly fair?

\[ T_1 \parallel \text{Arbiter} \parallel T_2 \]

Fairness for action-set \( A = \{\text{enter}_1\} \):

\[ \langle n_1, u, n_2 \rangle \rightarrow \left( \langle w_1, u, n_2 \rangle \rightarrow \langle w_1, u, w_2 \rangle \rightarrow \langle n_1, l, \text{crit}_2 \rangle \right)^\omega \]

- unconditional \( A \)-fairness: no
- strong \( A \)-fairness: no
- weak \( A \)-fairness: yes
Unconditional, strongly or weakly fair?

\[ T_1 \parallel \text{Arbiter} \parallel T_2 \]

fairness for action set \( A = \{\text{enter}_1, \text{enter}_2\} \):

\[
\left( \langle n_1, u, n_2 \rangle \rightarrow \langle n_1, u, w_2 \rangle \rightarrow \langle n_1, u, \text{crit}_2 \rangle \right) ^ \omega
\]

- unconditional \( A \)-fairness:
- strong \( A \)-fairness:
- weak \( A \)-fairness:
Unconditional, strongly or weakly fair?

$T_1 \parallel \text{Arbiter} \parallel T_2$

fairness for action set $A = \{\text{enter}_1, \text{enter}_2\}$:

$$\left(\langle n_1, u, n_2 \rangle \rightarrow \langle n_1, u, w_2 \rangle \rightarrow \langle n_1, u, \text{crit}_2 \rangle\right)^\omega$$

- 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 $\text{Act}$. A fairness assumption for $\mathcal{T}$ is a triple

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

where $\mathcal{F}_{\text{ucond}}, \mathcal{F}_{\text{strong}}, \mathcal{F}_{\text{weak}} \subseteq 2^{\text{Act}}$. 
## Action-based fairness assumptions

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

$$F = (F_{\text{ucond}}, F_{\text{strong}}, F_{\text{weak}})$$

where $F_{\text{ucond}}, F_{\text{strong}}, F_{\text{weak}} \subseteq 2^{\text{Act}}$.

An execution $\rho$ is called $F$-fair iff

- $\rho$ is unconditionally $A$-fair for all $A \in F_{\text{ucond}}$
- $\rho$ is strongly $A$-fair for all $A \in F_{\text{strong}}$
- $\rho$ is weakly $A$-fair for all $A \in F_{\text{weak}}$
Let $\mathcal{T}$ be a transition system with action-set $\text{Act}$. A fairness assumption for $\mathcal{T}$ is a triple

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

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

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

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

$$\text{FairTraces}_\mathcal{F}(\mathcal{T}) \overset{\text{def}}{=} \{ \text{trace}(\rho) : \rho \text{ is a } \mathcal{F}\text{-fair execution of } \mathcal{T} \}$$
Fair satisfaction relation
A fairness assumption for $T$ 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 $\rho$ is called $\mathcal{F}$-fair iff

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

If $T$ is a TS and $E$ a LT property over $AP$ then:

$$T \models_{\mathcal{F}} E \iff \text{FairTraces}_{\mathcal{F}}(T) \subseteq E$$
Example: fair satisfaction relation

fairness assumption $\mathcal{F}$

- no unconditional fairness condition
- strong fairness for $\{\alpha, \beta\}$
- no weak fairness condition
Example: fair satisfaction relation

fairness assumption $\mathcal{F}$

- no unconditional fairness condition $\Rightarrow \mathcal{F}_{ucond} = \emptyset$
- strong fairness for $\{\alpha, \beta\}$ $\Rightarrow \mathcal{F}_{strong} = \{\{\alpha, \beta\}\}$
- no weak fairness condition $\Rightarrow \mathcal{F}_{weak} = \emptyset$
Example: fair satisfaction relation

\[ \mathcal{T} \models \mathcal{F} \quad \text{“infinitely often } b \text{”} ? \]

fairness assumption \( \mathcal{F} \)

- no unconditional fairness condition \( \leftarrow \mathcal{F}_{\text{ucond}} = \emptyset \)
- strong fairness for \( \{ \alpha, \beta \} \) \( \leftarrow \mathcal{F}_{\text{strong}} = \{ \{ \alpha, \beta \} \} \)
- no weak fairness condition \( \leftarrow \mathcal{F}_{\text{weak}} = \emptyset \)
Example: fair satisfaction relation

\[ \emptyset \xrightarrow{\alpha} \emptyset \xrightarrow{\beta} \{b\} \]

\[ \mathcal{T} \models \mathcal{F} \text{ “infinitely often } b \text{”?} \]

answer: no

fairness assumption \( \mathcal{F} \)

- no unconditional fairness condition \( \leftarrow \mathcal{F}_{\text{ucond}} = \emptyset \)
- strong fairness for \( \{\alpha, \beta\} \) \( \leftarrow \mathcal{F}_{\text{strong}} = \{\{\alpha, \beta\}\} \)
- no weak fairness condition \( \leftarrow \mathcal{F}_{\text{weak}} = \emptyset \)
Example: fair satisfaction relation

\[ \mathcal{T} \models \mathcal{F} \text{ “infinitely often } b\text{” ?} \]

answer: no

fairness assumption \( \mathcal{F} \):

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

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

\( \mathcal{F}\)-fair
Example: fair satisfaction relation

- strong fairness for $\alpha$ \[ F_{\text{strong}} = \{\{\alpha\}\} \]
- weak fairness for $\beta$ \[ F_{\text{weak}} = \{\{\beta\}\} \]
- no unconditional fairness assumption
Example: fair satisfaction relation

\[ \emptyset \rightarrow \{b\} \]

\[ \emptyset \quad \alpha \quad \beta \]

\[ \mathcal{T} \models \mathcal{F} \text{ “infinitely often } b \text{” ?} \]

fairness assumption \( \mathcal{F} \)

- strong fairness for \( \alpha \)
- weak fairness for \( \beta \)
- no unconditional fairness assumption

\[ \leftarrow \mathcal{F}_{\text{strong}} = \{\{\alpha\}\} \]
\[ \leftarrow \mathcal{F}_{\text{weak}} = \{\{\beta\}\} \]
Example: fair satisfaction relation

$\emptyset \xrightarrow{\alpha} \{b\} \xrightarrow{\beta} \emptyset$

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

answer: no

- fairness assumption $\mathcal{F}$
  - strong fairness for $\alpha$
    $\leftarrow \mathcal{F}_{\text{strong}} = \{\{\alpha\}\}$
  - weak fairness for $\beta$
    $\leftarrow \mathcal{F}_{\text{weak}} = \{\{\beta\}\}$
  - no unconditional fairness assumption
Example: fair satisfaction relation

\( \emptyset \xrightarrow{\alpha} \{b\} \xrightarrow{\beta} \emptyset \)

\[ \mathcal{T} \models \mathcal{F} \text{ “infinitely often } b \text{” ?} \]

answer: no

fairness assumption \( \mathcal{F} \)

- strong fairness for \( \alpha \)
  \[ \leftarrow \mathcal{F}_{\text{strong}} = \{\{\alpha\}\} \]

- weak fairness for \( \beta \)
  \[ \leftarrow \mathcal{F}_{\text{weak}} = \{\{\beta\}\} \]

- no unconditional fairness assumption

\[ \alpha \xrightarrow{\beta} \alpha \xrightarrow{\beta} \alpha \xrightarrow{\beta} \alpha \xrightarrow{\beta} \ldots \]

\( \mathcal{F} \)-fair
Example: fair satisfaction relation

\[ \emptyset \rightarrow \{b\} \]

\[ \emptyset \rightarrow \{b\} \]

\[ \emptyset \rightarrow \{b\} \]

fairness assumption \( F \)

- strong fairness for \( \beta \)
- no weak fairness assumption
- no unconditional fairness assumption

\[ \mathcal{T} \models_{F} \text{“infinitely often } b \text{”} \]

\[ \leftarrow F_{\text{strong}} = \{\{\beta\}\} \]
Example: fair satisfaction relation

\[ \emptyset \rightarrow \{b\} \]

\[ \emptyset \rightarrow \alpha \rightarrow \beta \rightarrow \{b\} \]

fairness assumption \( \mathcal{F} \)

- strong fairness for \( \beta \)
- no weak fairness assumption
- no unconditional fairness assumption

\[ \mathcal{T} \models_{\mathcal{F}} \text{ “infinitely often } b \text{”} \]

\[ \mathcal{T} \models_{\mathcal{F}_{\text{strong}}} = \{\{\beta\}\} \]

\[ \alpha \rightarrow \beta \rightarrow \alpha \rightarrow \beta \rightarrow \alpha \rightarrow \ldots \]

is not \( \mathcal{F} \)-fair
Which type of fairness?

LF2.6-13A
Which type of fairness?

fairness assumptions should be as weak as possible
Two independent traffic lights

light 1
- red
- green
- enter red
- enter green

light 2
- red
- green
- enter red
- enter green
Two independent traffic lights

fairness assumption \( \mathcal{F} \):

\[ \mathcal{F}_{ucond} = ? \]
\[ \mathcal{F}_{strong} = ? \]
\[ \mathcal{F}_{weak} = ? \]

\[ \text{light 1} \]
\[ \text{red} \quad \text{green} \]
\[ \text{enter red}_1 \quad \text{enter green}_1 \]

\[ \text{light 2} \]
\[ \text{red} \quad \text{green} \]
\[ \text{enter red}_2 \quad \text{enter green}_2 \]

\[ \text{red red} \]
\[ \text{green red} \]
\[ \text{green green} \]

\[ \text{red green} \]

light 1 \( \parallel \) light 2 \( \models_\mathcal{F} E \)

\[ E \equiv \text{“both lights are infinitely often green”} \]
Two independent traffic lights

\[ A_1 = \text{actions of light 1} \]
\[ A_2 = \text{actions of light 2} \]

Fairness assumption \( \mathcal{F} \):  
\[ \mathcal{F}_{ucond} = ? \]
\[ \mathcal{F}_{strong} = ? \]
\[ \mathcal{F}_{weak} = ? \]

\[ \text{light 1} \]
- red
- green

\[ \text{light 2} \]
- red
- green

Enter

\[ \text{light 1} \]
- green

\[ \text{light 2} \]
- red

\[ E \equiv \text{“both lights are infinitely often green”} \]
Two independent traffic lights

\[ A_1 = \text{actions of light 1} \]
\[ A_2 = \text{actions of light 2} \]

fairness assumption \( \mathcal{F} \):
\[ \mathcal{F}_{\text{ucond}} = \emptyset \]
\[ \mathcal{F}_{\text{strong}} = \emptyset \]
\[ \mathcal{F}_{\text{weak}} = \{A_1, A_2\} \]

light 1
- \( \text{red} \)
- \( \text{green} \)

light 2
- \( \text{red} \)
- \( \text{green} \)

\( \mathcal{F} \models E \)
\[ E \equiv \text{“both lights are infinitely often green”} \]
Example: MUTEX with fair arbiter

\[ T = T_1 \parallel \text{Arbiter} \parallel T_2 \]
Example: MUTEX with fair arbiter

\[ T = T_1 \parallel \text{Arbiter} \parallel T_2 \]
Example: MUTEX with fair arbiter

\[ \mathcal{T} = \mathcal{T}_1 \parallel \text{Arbiter} \parallel \mathcal{T}_2 \]

\[ \mathcal{T}_1 \]
- **noncrit**
  - **request**
  - **wait**
  - **crit**

\[ \mathcal{T}_2 \]
- **noncrit**
  - **request**
  - **wait**
  - **crit**

\[ \mathcal{T}_1 \] and \[ \mathcal{T}_2 \] compete to communicate with the arbiter by means of the actions \textit{enter}_1 and \textit{enter}_2, respectively.
LT property $E$: each waiting process eventually enters its critical section

$\mathcal{T} \not\models E$
Example: MUTEX with fair arbiter

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

fairness assumption $F$

$F_{ucond} = F_{strong} = \emptyset$

$F_{weak} = \{\{\text{enter}_1\}, \{\text{enter}_2\}\}$

does $T \models_F E$ hold?
Example: MUTEX with fair arbiter

$\mathcal{T}$

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

fairness assumption $\mathcal{F}$

$\mathcal{F}_{ucond} = \mathcal{F}_{strong} = \emptyset$
$\mathcal{F}_{weak} = \{\{\text{enter}_1\}, \{\text{enter}_2\}\}$

does $\mathcal{T} \models_{\mathcal{F}} E$ hold? answer: no
Example: MUTEX with fair arbiter

$T$

$\langle \text{crit}_1, l, n_2 \rangle \rightarrow n_1 \ u \ n_2 \rightarrow w_1 \ u \ n_2 \rightarrow n_1 \ u \ w_2 \rightarrow w_1 \ u \ w_2 \rightarrow n_1 \ l \ \text{crit}_2$

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

 fairness assumption $F$

$F_{\text{ucond}} = F_{\text{strong}} = \emptyset$
$F_{\text{weak}} = \{\{\text{enter}_1\}, \{\text{enter}_2\}\}$

$T \not \vDash_F E$

as $\text{enter}_2$ is not enabled in $\langle \text{crit}_1, l, w_2 \rangle$
Example: MUTEX with fair arbiter

\[ T \]

\[ n_1 \ u \ n_2 \]

\[ w_1 \ u \ n_2 \]

\[ n_1 \ u \ w_2 \]

\[ w_1 \ u \ w_2 \]

\[ n_1 \ l \ crit_2 \]

\[ crit_1 \ l \ n_2 \]

\[ crit_1 \ l \ w_2 \]

\[ w_1 \ l \ crit_2 \]

\[ enter_1 \]

\[ enter_2 \]

\[ E: \] each waiting process eventually enters its crit. section

\[ F_{ucond} = ? \]

\[ F_{strong} = ? \]

\[ F_{weak} = ? \]
Example: MUTEX with fair arbiter

\( \mathcal{T} \)

\( n_1 u n_2 \)

\( w_1 u n_2 \)

\( n_1 u w_2 \)

\( w_1 u w_2 \)

\( w_1 l \text{crit}_2 \)

\( n_1 l \text{crit}_2 \)

\( \text{crit}_1 l n_2 \)

\( \text{crit}_1 l w_2 \)

\( \text{enter}_1 \)

\( \text{enter}_2 \)

\( E: \) each waiting process eventually enters its crit. section

\( \mathcal{F}_{\text{ucond}} = \emptyset \)

\( \mathcal{F}_{\text{strong}} = \{\{\text{enter}_1\}, \{\text{enter}_2\}\} \)

\( \mathcal{F}_{\text{weak}} = \emptyset \)

\( \mathcal{T} \upharpoonright\not\models E, \)

but \( \mathcal{T} \models_{\mathcal{F}} E \)
Example: MUTEX with fair arbiter

$$T$$

$$E:$$ each waiting process eventually enters its crit. section

$$D:$$ each process enters its critical section infinitely often

$$\mathcal{F}_{ucond} = \emptyset$$

$$\mathcal{F}_{strong} = \left\{ \{enter_1\}, \{enter_2\} \right\}$$

$$\mathcal{F}_{weak} = \emptyset$$

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

$$\mathcal{T} \not\models_{\mathcal{F}} D$$
Example: MUTEX with fair arbiter

\[ T \]

\[ n_1 \cup n_2 \]

\[ w_1 \cup n_2 \]

\[ n_1 \cup w_2 \]

\[ w_1 \cup w_2 \]

\[ n_1 \cup \text{crit}_2 \]

\[ \text{crit}_1 \cup n_2 \]

\[ \text{crit}_1 \cup w_2 \]

\[ w_1 \cup \text{crit}_2 \]

\[ \text{enter}_1 \]

\[ \text{enter}_2 \]

\[ E: \] each waiting process eventually enters its crit. section

\[ D: \] each process enters its critical section infinitely often

\[ \mathcal{F}_{ucond} = \emptyset \]

\[ \mathcal{F}_{strong} = \{ \{\text{enter}_1\}, \{\text{enter}_2\} \} \]

\[ \mathcal{F}_{weak} = \emptyset \]

\[ \mathcal{T} \models \mathcal{F} E, \]

\[ \mathcal{T} \not\models \mathcal{F} D \]
Example: MUTEX with fair arbiter

\[ T \]

\[ \begin{align*}
T & \rightarrow n_1 u n_2 \\
T & \rightarrow w_1 u n_2 \\
T & \rightarrow n_1 u w_2 \\
T & \rightarrow w_1 u w_2 \\
T & \rightarrow n_1 l \text{crit}_2 \\
T & \rightarrow w_1 l \text{crit}_2 \\
T & \rightarrow \text{crit}_1 l n_2 \\
T & \rightarrow \text{crit}_1 l w_2 \\
\end{align*} \]

\[ E: \text{each waiting process eventually enters its crit. section} \]

\[ D: \text{each process enters its critical section infinitely often} \]

\[ F_{\text{ucond}} = \emptyset \]

\[ F_{\text{strong}} = \{ \{ \text{enter}_1 \}, \{ \text{enter}_2 \} \} \]

\[ F_{\text{weak}} = \{ \{ \text{req}_1 \}, \{ \text{req}_2 \} \} \]

\[ T \models F E, \]

\[ T \models F D \]
Process fairness
Process fairness

For asynchronous systems:

\[
\text{parallelism} = \text{interleaving} + \text{fairness}
\]
For asynchronous systems:

\[
\text{parallelism} = \text{interleaving} + \text{fairness}
\]

should be as weak as possible
Process fairness

For asynchronous systems:

parallelism = interleaving + fairness

should be as weak as possible

rule of thumb:

- **strong fairness** for the
  - choice between dependent actions
  - resolution of competitions
Process fairness

For asynchronous systems:

\[
\text{parallelism} = \text{interleaving} + \text{fairness}
\]

should be as weak as possible

rule of thumb:

- **strong fairness** for the
  - choice between dependent actions
  - resolution of competitions
- **weak fairness** for the nondeterminism obtained from
  the interleaving of independent actions
Process fairness

For asynchronous systems:

\[ \text{parallelism} = \text{interleaving} + \text{fairness} \]

should be as weak as possible

rule of thumb:

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

Parallelism = interleaving + 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
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
Fairness

\[\mathcal{T} \rightarrow \{a\} \] \[\alpha \]

\[\emptyset \]

Fairness assumption \(\mathcal{F}\): unconditional fairness for action set \(\{\alpha\}\)

Does \(\mathcal{T} \models \mathcal{F}\) “infinitely often \(a\)” hold?
fairness assumption $\mathcal{F}$: unconditional fairness for action set $\{\alpha\}$

does $\mathcal{T} \models_{\mathcal{F}} \text{“infinitely often } \alpha \text{” }$ hold?

answer: yes as there is no fair path
fairness assumption $\mathcal{F}$: unconditional fairness for action set $\{\alpha\}$

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

answer: yes as there is no fair path
Realizability of fairness assumptions

\[ \mathcal{T} \rightarrow \{a\} \]

\[ \alpha \]

\[ \emptyset \]

Fairness assumption \( \mathcal{F} \): unconditional fairness for action set \( \{\alpha\} \)

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

**Does \( \mathcal{T} \models_{\mathcal{F}} \) “infinitely often \( a \)” hold?**

**Answer:** Yes as there is no fair path
Realizability of fairness assumptions

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

$\mathcal{T}$

$\{a\}$

$\alpha$

$\emptyset$

Does $\mathcal{T} \models_{\mathcal{F}} \text{“infinitely often } a \text{”} \text{ hold?}$

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 $s$. 
Realizability of fairness assumptions
Realizability of fairness assumptions

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

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

- unconditional fairness for $A \in \mathcal{F}_{\text{ucond}}$
- strong fairness for $A \in \mathcal{F}_{\text{strong}}$
- weak fairness for $A \in \mathcal{F}_{\text{weak}}$
Realizability of fairness assumptions

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

- unconditional fairness for $A \in F_{ucond}$
  $\leadsto$ might not be realizable

- strong fairness for $A \in F_{strong}$

- weak fairness for $A \in F_{weak}$
Realizability of fairness assumptions

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

- unconditional fairness for $A \in \mathcal{F}_{ucond}$
  - 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 $F$ is a realizable fairness assumption for TS $T$ and $E$ a safety property then:

$T \models E$ iff $T \models_{\mathcal{F}} E$
Safety and realizable fairness

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
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:

$$\mathcal{T} \models E \iff \mathcal{T} \models_{\mathcal{F}} E$$

... wrong for non-realizable fairness assumptions

$\alpha \in \{a\}$

$\emptyset$

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

$\alpha \xrightarrow{\{a\}} \{a\}$

$\emptyset$

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

$E = \text{invariant \text{ "always a"}}$

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