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: something good will happen.”

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

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

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

e.g., \texttt{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: 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
• Each philosopher thinks infinitely often.
which property type?

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

- 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.
• 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**
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.  **safety**

- Whenever a philosopher eats then he will think some time afterwards.
• 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.
  \textit{liveness}
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. \textit{liveness}
- Between two eating phases of philosopher $i$ lies at least one eating phase of philosopher $i+1$. 

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.  
  **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**
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: $\text{pref}(E) = \text{set of all finite, nonempty prefixes of words in } E$
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
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 $\text{pref}(E) = (2^AP)^+$

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

- 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

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

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

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

$$\forall i \in \{1, \ldots, n\} \quad \exists k \geq 0. \quad \text{crit}_i \in A_k$$
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 infinitely 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 $AP = \{\text{wait}_i, \text{crit}_i : i = 1, \ldots, n\}$:

- 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

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

$\forall i \in \{1, \ldots, n\} \forall j \geq 0. \text{wait}_i \in A_j$  $\rightarrow$  $\exists k > j. \text{crit}_i \in A_k$
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 $\forall \sigma \in (2^{AP})^\omega \setminus E \exists A_0 A_1 \ldots A_n \in \text{pref}(\sigma)$ 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., $E \subseteq (2^{AP})^\omega$

$E$ is a safety property

iff \hspace{1cm} \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

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 \hspace{1cm} \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 \hspace{1cm} \text{cl}(E) = E

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

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

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

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

$$E = \textit{SAFE} \cap \textit{LIVE}$$
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 $SAFE \overset{\text{def}}{=} \text{cl}(E)$
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: $cl(E) = \{\sigma \in (2^{AP})^\omega : pref(\sigma) \subseteq pref(E)\}$

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

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

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

$$ E = \textit{SAFE} \cap \textit{LIVE} $$

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

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

Show that:

- $E = \textit{SAFE} \cap \textit{LIVE}$
- $\textit{SAFE}$ is a safety property
- $\textit{LIVE}$ 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 $SAFE \overset{\text{def}}{=} \text{cl}(E)$

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

Show that:

- $E = SAFE \cap LIVE$ \qquad \checkmark
- $SAFE$ is a safety property as $\text{cl}(SAFE) = SAFE$
- $LIVE$ 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 $SAFE \overset{\text{def}}{=} \text{cl}(E)$

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

Show that:

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

- $\left(2^{AP}\right)^\omega$ is a safety and a liveness property: $\checkmark$
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
  \[
  \text{pref}(E) = (2^{AP})^+
  \]
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
  \[
  \text{pref}(E) = (2^{AP})^+
  \]
  \[\implies \text{cl}(E) = (2^{AP})^\omega\]
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

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

\[\implies \text{cl}(E) = (2^{AP})^\omega\]

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

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

\[
\Rightarrow \quad \text{cl}(E) = (2^{AP})^\omega
\]

If \(E\) is a safety property too, then \(\text{cl}(E) = E\). Hence \(E = \text{cl}(E) = (2^{AP})^\omega\).
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
Two independent traffic lights

light 1

red₁

green₁

light 2

red₂

green₂

light 1 ||| light 2

\[ \text{light 1} \ ||| \ \text{light 2} \quad \nRightarrow \quad \text{“infinitely often green}_1 \]
Two independent traffic lights

\begin{center}
\begin{tikzpicture}

\node [draw] at (0,0) (light1) {light 1};
\node [draw] at (3,0) (light2) {light 2};

\node [draw] at (0,-1) (red1) {red$_1$};
\node [draw] at (0,-2) (green1) {green$_1$};
\node [draw] at (3,-1) (red2) {red$_2$};
\node [draw] at (3,-2) (green2) {green$_2$};

\draw [->, thick] (red1) -- (green1);
\draw [->, thick] (red2) -- (green2);
\draw [->, thick] (green1) -- (red2);
\draw [->, thick] (green2) -- (red1);
\end{tikzpicture}
\end{center}

light 1 \parallel light 2

\[ \not \equiv \text{“infinitely often green$_1$”} \]
Two independent traffic lights

light 1

red₁

green₁

red₁ red₂

red₂

light 2

green₂

red₁ green₂

light 1 ||| light 2

light 1 ||| light 2 ⊮ “infinitely often green₁”

although light 1 ⊧ “infinitely often green₁”
Two independent traffic lights

light 1
- - - - - - -
- - - - - - -
- - - - - - -

light 2
- - - - - - -
- - - - - - -

light 1 ||| light 2

light 1 ||| light 2 ⊭ “infinitely often green$_1$”

interleaving is completely time abstract!
Mutual exclusion (semaphore)

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

- \text{noncrit}_{1} \text{ noncrit}_{2} \quad y=1
- \text{wait}_{1} \text{ noncrit}_{2} \quad y=1
- \text{crit}_{1} \text{ noncrit}_{2} \quad y=0
- \text{wait}_{1} \text{ wait}_{2} \quad y=1
- \text{crit}_{1} \text{ wait}_{2} \quad y=0
- \text{noncrit}_{1} \text{ wait}_{2} \quad y=1
- \text{noncrit}_{1} \text{ crit}_{2} \quad y=0
- \text{wait}_{1} \text{ crit}_{2} \quad y=0
Mutual exclusion (semaphore)

\[ I_{sem} \]

\[ \text{noncrit}_1 \text{ noncrit}_2 \]

\[ y=1 \]

\[ \text{wait}_1 \text{ noncrit}_2 \]

\[ y=1 \]

\[ \text{crit}_1 \text{ noncrit}_2 \]

\[ y=0 \]

\[ \text{wait}_1 \text{ wait}_2 \]

\[ y=1 \]

\[ \text{crit}_1 \text{ wait}_2 \]

\[ y=0 \]

\[ \text{wait}_1 \text{ crit}_2 \]

\[ y=0 \]

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

\[ I_{sem} \]

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

\[ I_{sem} \not

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

\[ T_{sem} \]

\begin{align*}
\text{noncrit}_1 & \Rightarrow \text{noncrit}_2 \\
y = 1 & \\
\text{wait}_1 & \Rightarrow \text{noncrit}_2 \\
y = 1 & \\
\text{crit}_1 & \Rightarrow \text{noncrit}_2 \\
y = 0 & \\
\text{wait}_1 & \Rightarrow \text{wait}_2 \\
y = 1 & \\
\text{noncrit}_1 & \Rightarrow \text{wait}_2 \\
y = 1 & \\
\text{noncrit}_1 & \Rightarrow \text{crit}_2 \\
y = 0 & \\
\text{wait}_1 & \Rightarrow \text{crit}_2 \\
y = 0 & \\
\text{wait}_1 & \Rightarrow \text{wait}_2 \\
y = 1 & \\
\end{align*}

\[ T_{sem} \neq \quad \text{“each waiting process will eventually enter its critical section”} \]
Mutual exclusion (semaphore)

\[ I_{sem} \]

\[ \text{noncrit}_1 \text{ noncrit}_2 \]
\[ y = 1 \]

\[ \text{wait}_1 \text{ noncrit}_2 \]
\[ y = 1 \]

\[ \text{crit}_1 \text{ noncrit}_2 \]
\[ y = 0 \]

\[ \text{crit}_1 \text{ wait}_2 \]
\[ y = 0 \]

\[ \text{wait}_1 \text{ wait}_2 \]
\[ y = 1 \]

\[ \text{noncrit}_1 \text{ wait}_2 \]
\[ y = 1 \]

\[ \text{noncrit}_1 \text{ crit}_2 \]
\[ y = 0 \]

\[ \text{wait}_1 \text{ crit}_2 \]
\[ y = 0 \]

\[ I_{sem} \not\models \]

"each waiting process will eventually enter its critical section"

level of abstraction is too coarse!
Process fairness

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

possible interleavings:

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

$P_1\ P_1\ P_2\ P_1\ P_1\ P_2\ P_1\ P_1\ P_2\ P_1\ P_1\ P_2\ P_1\ P_1 \ldots$
Process fairness

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

possible interleavings:

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

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

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

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

possible interleavings:

\[
\begin{align*}
& P_1 \ P_2 \ P_2 \ P_1 \ P_1 \ P_1 \ P_2 \ P_1 \ P_2 \ P_2 \ P_2 \ P_1 \ P_1 \ \cdots \ \text{fair} \\
& P_1 \ P_1 \ P_2 \ P_1 \ P_1 \ P_2 \ P_1 \ P_2 \ P_1 \ P_2 \ P_1 \ \cdots \ \text{fair} \\
& P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ \cdots \ \text{unfair}
\end{align*}
\]
Process 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

$P_1 P_1 P_2 P_1 P_1 P_2 P_1 P_2 P_1 P_2 P_1 P_1 ...$  fair

$P_1 P_1 P_1 P_1 P_1 P_1 P_1 P_1 P_1 P_1 P_1 P_1 ...$  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 $\text{Act}$, $A \subseteq \text{Act}$ and

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

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

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

we will provide conditions for

- unconditional $A$-fairness of $\rho$
- strong $A$-fairness of $\rho$
- weak $A$-fairness of $\rho$

using the following notations:

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

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

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

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

$\forall^\infty \equiv \text{“for all, but finitely many ...”}$
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
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 $\exists \ i \geq 0. \hspace{1em} \alpha_i \in A$

“actions in $A$ will be taken infinitely many times”
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 $\mathcal{T}$ 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

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

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

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

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

unconditionally $A$-fair $\implies$ strongly $A$-fair $\implies$ weakly $A$-fair
Fairness for action-set

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

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

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

\[
\begin{array}{c}
\text{unconditionally } A\text{-fair} \implies \text{strongly } A\text{-fair} \\
\implies \text{weakly } A\text{-fair}
\end{array}
\]
Strong and weak action fairness

**Strong $A$-fairness is violated if**

- no $A$-actions are executed from a certain moment
- $A$-actions are enabled infinitely many times
Strong and weak action fairness

**Strong A-fairness** is violated if

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

**Weak A-fairness** is violated if

• no A-actions are executed from a certain moment
• A-actions are continuously enabled from some moment on
Mutual exclusion with arbiter

\[ T_1 \]

noncrit\(_1\) → request\(_1\) → wait\(_1\) → enter\(_1\) → \text{release} → \text{crit}\(_1\) → \text{release}

\[ T_2 \]

noncrit\(_2\) → request\(_2\) → wait\(_2\) → enter\(_2\) → \text{release} → \text{crit}\(_2\) → \text{release}

LF2.6-9
Mutual exclusion with arbiter

\( T_1 \)

\( \text{noncrit}_1 \) 

\( \text{wait}_1 \) 

\( \text{request}_1 \) 

\( \text{enter}_1 \) 

\( \text{release} \) 

\( \text{crit}_1 \) 

\( \text{Arbiter} \)

\( \text{unlock} \) 

\( \text{rel} \) 

\( \text{enter}_1 \) 

\( \text{enter}_2 \) 

\( \text{release} \) 

\( \text{crit}_2 \) 

\( \text{Arbiter} \)

\( \text{lock} \) 

\( \text{request}_2 \) 

\( \text{enter}_2 \) 

\( \text{enter}_2 \) 

\( \text{release} \) 

\( \text{wait}_2 \) 

\( \text{noncrit}_2 \)
**Mutual exclusion with arbiter**

\[ \mathcal{T}_1 \]
- `noncrit_1` → `wait_1`
- `request_1` → `wait_1`
- `enter_1` → `crit_1`

\[ \mathcal{T}_2 \]
- `noncrit_2` → `wait_2`
- `request_2` → `wait_2`
- `enter_2` → `crit_2`

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

- `n_1 \cup n_2`
  - `enter_1`
  - `enter_2`
  - `release`
- `n_1 \cup w_2`
- `w_1 \cup n_2`
- `w_1 \cup w_2`
- `crit_1 \cup n_2`
- `crit_1 \cup w_2`
- `w_1 \cup crit_2`
- `n_1 \cup crit_2`
Unconditional, strongly or weakly fair?

$\mathcal{T}_1 \parallel \text{Arbiter} \parallel \mathcal{T}_2$
Unconditional, strongly or weakly fair?

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

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

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

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

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

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

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

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

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?

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

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: \( \text{no} \)
- Strong \( A \)-fairness: \( \text{yes} \) \( \leftarrow A \) never enabled
- Weak \( A \)-fairness: \( \text{yes} \) \( \leftarrow \) strongly \( A \)-fair
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:
- 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 \( A = \{\text{enter}_1\} \):

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

- 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 \( A = \{ \text{enter}_1, \text{enter}_2 \} \):

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

- 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 $\mathcal{A}$. A fairness assumption for $\mathcal{T}$ is a triple $\mathcal{F} = (\mathcal{F}_{ucond}, \mathcal{F}_{strong}, \mathcal{F}_{weak})$ where $\mathcal{F}_{ucond}, \mathcal{F}_{strong}, \mathcal{F}_{weak} \subseteq 2^{\mathcal{A}}$. 
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 $A \in \mathcal{F}_{\text{weak}}$
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 $\mathcal{T}$ is a triple

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

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

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

1. $\rho$ is unconditionally $A$-fair for all $A \in \mathcal{F}_{ucond}$
2. $\rho$ is strongly $A$-fair for all $A \in \mathcal{F}_{strong}$
3. $\rho$ 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:

$$\mathcal{T} \models_{\mathcal{F}} E \iff \text{FairTraces}_{\mathcal{F}}(\mathcal{T}) \subseteq E$$
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 $\leftarrow \mathcal{F}_{ucond} = \emptyset$
- strong fairness for $\{\alpha, \beta\} \leftarrow \mathcal{F}_{strong} = \{\{\alpha, \beta\}\}$
- no weak fairness condition $\leftarrow \mathcal{F}_{weak} = \emptyset$
Example: fair satisfaction relation

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

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

fairness assumption \( \mathcal{F} \)

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

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

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

\( \mathcal{T} \models \mathcal{F} \) “infinitely often b”?

answer: no

Fairness assumption \( \mathcal{F} \)

- no unconditional fairness condition \( \leftarrow \mathcal{F}_{u\text{cond}} = \emptyset \)
- 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 \( \leftarrow \mathcal{F}_{ucond} = \emptyset \)
- 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
Example: fair satisfaction relation

fairness assumption $\mathcal{F}$

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

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

fairness assumption \( \mathcal{F} \)

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

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

- no unconditional fairness assumption

\( \mathcal{T} \models \mathcal{F} \) “infinitely often \( b \)” ?
Example: fair satisfaction relation

\[ T \models \mathcal{F} \text{ “infinitely often } b \text{” ?} \]
answer: no

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

- strong fairness for \( \alpha \)
  \[ \mathcal{F}_{\text{strong}} = \{\{\alpha}\} \]
- weak fairness for \( \beta \)
  \[ \mathcal{F}_{\text{weak}} = \{\{\beta}\} \]
- no unconditional fairness assumption
Example: fair satisfaction relation

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

answer: no

fairness assumption \( \mathcal{F} \)

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

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

fairness assumption $\mathcal{F}$

- strong fairness for $\beta$
- no weak fairness assumption
- no unconditional fairness assumption

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

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

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

fairness assumption $\mathcal{F}$

- strong fairness for $\beta$
- no weak fairness assumption
- no unconditional fairness assumption

\[ \mathcal{T} \not\models_{\mathcal{F}} \text{ is not } \mathcal{F}\text{-fair} \]
Which type of fairness?
Which type of fairness?

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

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

light 2
- red
- green
- enter
  - red
  - green

red red
- green red
- green green

red green
- green green
Two independent traffic lights

fairness assumption $\mathcal{F}$:

$F_{u\text{cond}} = ?$

$F_{\text{strong}} = ?$

$F_{\text{weak}} = ?$

light 1

red

green

enter red

1

Enter green

2

light 2

red

green

enter red

1

Enter green

2

$\vdash_{\mathcal{F}} E$

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

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

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

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

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

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

light 1 \( ||| \) 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 \( \mathcal{F} \):
\[ \mathcal{F}_{\text{ucond}} = \emptyset \]
\[ \mathcal{F}_{\text{strong}} = \emptyset \]
\[ \mathcal{F}_{\text{weak}} = \{A_1, A_2\} \]

\[ \text{light 1} \quad \text{green} \quad \text{red} \]
\[ \text{light 2} \quad \text{red} \quad \text{green} \]

\[ \text{enter red}_1 \quad \text{enter red}_2 \]

\[ \text{green}_1 \quad \text{green}_2 \]

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

\[ \text{light 1} \parallel \parallel \text{light 2} \models_\mathcal{F} E \]

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

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

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

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

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

\[ \text{Arbiter} \]
- unlock
  - enter
  - rel

\[ \mathcal{T}_2 \]
- noncrit
  - request
    - wait
      - enter
        - crit
Example: MUTEX with fair arbiter

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

\[ \mathcal{T}_1 \]
- noncrit\(_1\)
  - request\(_1\) → wait\(_1\)
    - enter\(_1\) → crit\(_1\)
      - rel
        - enter\(_1\) → wait\(_1\)
          - enter\(_1\) → crit\(_1\)

\[ \mathcal{T}_2 \]
- noncrit\(_2\)
  - request\(_2\) → wait\(_2\)
    - enter\(_2\) → crit\(_2\)
      - rel
        - enter\(_2\) → wait\(_2\)
          - enter\(_2\) → crit\(_2\)

\[ \mathcal{T}_1 \] 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

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

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

fairness assumption $\mathcal{F}$

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

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

does $\mathcal{T} \models_{\mathcal{F}} E$ hold?
Example: MUTEX with fair arbiter

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

fairness assumption $\mathcal{F}$

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

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

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

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

fairness assumption $\mathcal{F}$

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

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

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

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

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

$F_{ucond} = ?$

$F_{strong} = ?$

$F_{weak} = ?$

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

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

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

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

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

\[ T \]

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

\[ \begin{align*}
\text{crit}_1 \cup w_2 &\rightarrow \text{enter}_1 \\
\text{crit}_1 \cup n_2 &\rightarrow \text{enter}_2 \\
\end{align*} \]

\[ \begin{align*}
w_1 \cup \text{crit}_2 &\rightarrow \text{enter}_2 \\
w_1 \cup w_2 &\rightarrow \text{enter}_1 \\
crit_1 \cup \text{crit}_2 &\rightarrow \text{enter}_1 \\
crit_1 \cup n_2 &\rightarrow \text{enter}_2
\end{align*} \]

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

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

\[ \begin{align*}
\mathcal{F}_{\text{ucond}} &\rightarrow \emptyset \\
\mathcal{F}_{\text{strong}} &\rightarrow \{\{\text{enter}_1\}, \{\text{enter}_2\}\} \\
\mathcal{F}_{\text{weak}} &\rightarrow \emptyset
\end{align*} \]

\[ \begin{align*}
T \vdash_{\mathcal{F}} E, \\
T \not\vdash_{\mathcal{F}} D
\end{align*} \]
Example: MUTEX with fair arbiter

\( T \)

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

\( D: \) each process enters its critical section infinitely often

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

\( \mathcal{F}_{strong} = \{ \{ enter_1 \} , \{ enter_2 \} \} \)

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

\( T \models_{\mathcal{F}} E \)

\( T \not\models_{\mathcal{F}} D \)
**Example: MUTEX with fair arbiter**

\[ \mathcal{T} \]

\[ n_1 \ u \ n_2 \]

\[ w_1 \ u \ n_2 \]

\[ w_1 \ u \ w_2 \]

\[ n_1 \ u \ w_2 \]

\[ n_1 \ / \ crit_2 \]

\[ crit_1 \ / \ n_2 \]

\[ crit_1 \ / \ w_2 \]

\[ w_1 \ / \ crit_2 \]

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

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

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

\[ \mathcal{F}_{strong} = \{ \{ enter_1 \}, \{ enter_2 \} \} \]

\[ \mathcal{F}_{weak} = \{ \{ req_1 \}, \{ req_2 \} \} \]

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

\[ \mathcal{T} \models_{\mathcal{F}} D \]
Process fairness

LF2.6-19
Process fairness

For asynchronous systems:

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

For asynchronous systems:

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

should be as weak as possible
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
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
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

liveness properties: fairness can be essential

safety properties: fairness is irrelevant
Fairness

\[ \mathcal{T} \]

\[ \{a\} \]

\[ \alpha \]

\[ \emptyset \]

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

does \( \mathcal{T} \models \mathcal{F} \) “infinitely often \( a \)” hold?
Fairness

\[ \mathcal{T} \]

\( \{a\} \)

\( \alpha \)

\( \emptyset \)

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

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

answer: yes as there is no fair path
Fairness assumption $\mathcal{F}$: unconditional fairness for action set \{a\} is not realizable.

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

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

\[ \mathcal{T} \quad \{a\} \quad \alpha \quad \emptyset \]

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

\( \text{not realizable} \)

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
Realizability of fairness assumptions

\[ T \]

\[ \alpha \]

\[ \emptyset \]

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

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

Answer: Yes as there is no fair path

Fairness assumption \( F \) is said to be realizable for a transition system \( T \) if for each reachable state \( s \) in \( T \) there exists a \( F \)-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 $\mathcal{T}$
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 $\mathcal{F} = (\mathcal{F}_{ucond}, \mathcal{F}_{strong}, \mathcal{F}_{weak})$ 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 $A \in \mathcal{F}_{weak}$
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 $A \in \mathcal{F}_\text{ucond}$
  \[ \rightsquigarrow \text{might not be realizable} \]
- strong fairness for $A \in \mathcal{F}_\text{strong}$
- weak fairness for $A \in \mathcal{F}_\text{weak}$

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:

$$\mathcal{T} \models E \iff \mathcal{T} \models^{\mathcal{F}} E$$
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:

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

... 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.

$\alpha \subseteq \{a\}$

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

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

... wrong for non-realizable fairness assumptions

$\alpha \xleftarrow{} \{a\}$

$\emptyset$

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

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

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