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
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 → red₁

light 2

red₂ → green₂ → red₂

light 1 \|\| light 2

\[\text{light 1} \|\| \text{light 2} \not\Rightarrow \text{“infinitely often green}_1\]
Two independent traffic lights

light 1

\[
\begin{align*}
\text{red}_1 & \\
\text{green}_1 & \\
\text{red}_2 & \\
\end{align*}
\]

light 2

\[
\begin{align*}
\text{red}_2 & \\
\text{green}_2 & \\
\end{align*}
\]

light 1 ||| light 2

\[\text{light 1} \|\|\| \text{light 2} \]
Two independent traffic lights

light 1

\[
\begin{align*}
\text{red}_1 & \quad \text{green}_1 \\
\text{red}_2 & \quad \text{green}_2
\end{align*}
\]

light 2

\[
\begin{align*}
\text{red}_2 & \quad \text{green}_2
\end{align*}
\]

light 1 ||| light 2

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

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

light 1

red_1

green_1

red_1 red_2

green_1 red_2

red_1 green_2

light 2

red_2

green_2

red_1 red_2

light 1 \parallel|\parallel light 2

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

interleaving is completely time abstract!
Mutual exclusion (semaphore)

\[ T_{sem} \]

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

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

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

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

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

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

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

\[ \text{wait}_1 \text{ crit}_2 \]
\[ y = 0 \]
Mutual exclusion (semaphore)

\( \mathcal{T}_{sem} \)

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

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

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

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

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

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

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

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

**liveness property**: “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

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

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

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

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

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

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

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

```
noncrit_1 noncrit_2
y=1
```

```
wait_1 noncrit_2
y=1
```

```
oncrit_1 wait_2
y=1
```

```
crit_1 noncrit_2
y=0
```

```
wait_1 wait_2
y=1
```

```
crit_1 wait_2
y=0
```

```
noncrit_1 crit_2
y=0
```

```
wait_1 crit_2
y=0
```

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

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

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

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

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

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

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

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

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

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

\[ \mathcal{I}_{sem} \not\models \]

“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:

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

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

Two independent non-communicating processes $P_1 ||| P_2$

Possible interleavings:

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

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

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

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

possible interleavings:

$P_1 \ P_2 \ P_2 \ P_1 \ P_1 \ P_1 \ P_2 \ P_1 \ P_2 \ P_2 \ P_2 \ P_1 \ P_1 \ ... \ \text{fair}$

$P_1 \ P_1 \ P_2 \ P_1 \ P_1 \ P_2 \ P_1 \ P_1 \ P_2 \ P_1 \ P_1 \ P_2 \ P_1 \ ... \ \text{fair}$

$P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ P_1 \ ... \ \text{unfair}$
Process fairness

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

possible interleavings:

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

LF 2.6-7
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
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
we will provide conditions for
- unconditional $A$-fairness of $\rho$
- strong $A$-fairness of $\rho$
- weak $A$-fairness of $\rho$
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

we will provide conditions for

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

using the following notations:

$$\text{Act}(s_i) = \{ \beta \in \text{Act} : \exists s' \text{ s.t. } s_i \xrightarrow{\beta} s' \}$$
Let $T$ be a TS with action-set $\text{Act}$, $A \subseteq \text{Act}$ and
$\rho = s_0 \xrightarrow{\alpha_0} s_1 \xrightarrow{\alpha_1} s_2 \xrightarrow{\alpha_2} ...$ 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:
\[
\text{Act}(s_i) = \{ \beta \in \text{Act} : \exists s' \text{ s.t. } s_i \xrightarrow{\beta} s' \}
\]
\[\exists \equiv \text{“there exists infinitely many ...”}\]
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

we will provide conditions for

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

using the following notations:

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

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

$\forall \equiv \text{“for all, but finitely many ...”}$
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

- $\rho$ 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 $\exists i \geq 0. \alpha_i \in A$

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

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

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

- $\rho$ 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

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

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

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

\[ \text{unconditionally } A\text{-fair} \implies \text{strongly } A\text{-fair} \implies \text{weakly } A\text{-fair} \]
Fairness for action-set

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

$\rho = s_0 \xrightarrow{\alpha_0} s_1 \xrightarrow{\alpha_1} s_2 \xrightarrow{\alpha_2} \ldots$ 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>Strongly $A$-fair</th>
<th>Weakly $A$-fair</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\implies$</td>
<td>$\implies$</td>
<td>$\implies$</td>
</tr>
</tbody>
</table>
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

\( T_1 \)

\text{noncrit}_1 \rightarrow \text{wait}_1 \rightarrow \text{request}_1 \rightarrow \text{enter}_1 \rightarrow \text{release} \rightarrow \text{crit}_1

\( T_2 \)

\text{noncrit}_2 \rightarrow \text{wait}_2 \rightarrow \text{request}_2 \rightarrow \text{enter}_2 \rightarrow \text{release} \rightarrow \text{crit}_2
Mutual exclusion with arbiter

\( T_1 \)

- **request\(_1\)**
- **wait\(_1\)**
- **enter\(_1\)**
- **release**
- **crit\(_1\)**

**Arbiter**

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

\( T_2 \)

- **request\(_2\)**
- **wait\(_2\)**
- **enter\(_2\)**
- **enter\(_2\)**
- **release**
- **crit\(_2\)**
Mutual exclusion with arbiter

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

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

\[ \mathcal{T}_1 \parallel \text{Arbiter} \parallel \mathcal{T}_2 \]
- enter\(_1\)
- enter\(_2\)

- enter\(_1\)
- enter\(_2\)

- enter\(_1\)
- enter\(_2\)

- enter\(_1\)
- enter\(_2\)
Unconditional, strongly or weakly fair?

$T_1 \parallel$ Arbiter $\parallel T_2$
Unconditional, strongly or weakly fair?

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

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

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

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

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

- 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: no
- strong $A$-fairness: yes $\leftarrow A$ never enabled
- weak $A$-fairness: yes $\leftarrow$ strongly $A$-fair
Unconditional, strongly or weakly fair?

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

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

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

Unconditional, strongly or weakly fair?

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

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

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

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

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

Unconditional, strongly or weakly fair:

- unconditional \( A \)-fairness:
- strong \( A \)-fairness:
- weak \( A \)-fairness:

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, strongly or weakly fair?

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

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

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

- 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

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

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

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

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

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 $A \in \mathcal{F}_{\text{weak}}$

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

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

\[ \{b\} \]

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

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

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

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

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

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

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

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

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

\(\mathcal{F}\)-fair actions in \(\{\alpha, \beta\}\) are executed infinitely many times
Example: fair satisfaction relation

- **fair satisfaction relation**

\[ \emptyset \]

- \( \{ b \} \)

*fairness assumption* \( F \)

- strong fairness for \( \alpha \) \[ F_{\text{strong}} = \{ \{ \alpha \} \} \]

- weak fairness for \( \beta \) \[ F_{\text{weak}} = \{ \{ \beta \} \} \]

- no unconditional fairness assumption
Example: fair satisfaction relation

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

fairness assumption \( \mathcal{F} \)

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

\[ \mathcal{F}_{\text{strong}} = \{ \{ \alpha \} \} \]
\[ \mathcal{F}_{\text{weak}} = \{ \{ \beta \} \} \]
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

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

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

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

answer: **no**

Fairness assumption \( \mathcal{F} \)

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

\[ \mathcal{F}_{\text{strong}} = \{\{\alpha\}\} \]

\[ \mathcal{F}_{\text{weak}} = \{\{\beta\}\} \]

\[ \mathcal{F} \text{-fair} \]
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

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

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

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

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

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

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

Diagram showing a sequence of states and transitions that is not \( \mathcal{F} \)-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
- enter green

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

red red
- green red
- green green
- red green
Two independent traffic lights

Fairness assumption $\mathcal{F}$:

$\mathcal{F}_{ucond} = ?$
$\mathcal{F}_{strong} = ?$
$\mathcal{F}_{weak} = ?$

light 1

- red
- green

enter

green$_1$

= $E$

light 2

- red
- green

enter

green$_2$

= $E$

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

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

fairness assumption $F$:
$F_{\text{ucond}} = ?$
$F_{\text{strong}} = ?$
$F_{\text{weak}} = ?$

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

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

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

\[ \mathcal{F}_{ucond} = \emptyset \]
\[ \mathcal{F}_{strong} = \emptyset \]
\[ \mathcal{F}_{weak} = \{A_1, A_2\} \]

light 1

- red
- green

light 2

- red
- green

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

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

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

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

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

Arbiter
- unlock
- rel
- enter\(_1\)
- enter\(_2\)
Example: MUTEX with fair arbiter

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

\( \mathcal{T}_1 \) and \( \mathcal{T}_2 \) compete to communicate with the arbiter by means of the actions \( \text{enter}_1 \) and \( \text{enter}_2 \), respectively.
Example: MUTEX with fair arbiter

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 $\mathcal{F}$

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

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

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

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

Fairness assumption $F$

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

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

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

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

fairness assumption \( \mathcal{F} \)

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

\( \mathcal{T} \not\models_{\mathcal{F}} E \)
as \text{enter}_2 \text{ is not enabled in } \langle \text{crit}_1, l, w_2 \rangle
Example: MUTEX with fair arbiter

$\mathcal{T}$

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

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

$\mathcal{F}_{strong} = ?$

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

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

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

\[ T \]

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

\[ \begin{aligned}
    \text{enter}_1 & \quad \text{enter}_2 \\
    \text{enter}_1 & \quad \text{enter}_2
\end{aligned} \]

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

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

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

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

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

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

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

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

$\mathcal{T}$

$\mathcal{E}$: each waiting process eventually enters its crit. section

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

$F_{ucond} = \emptyset$

$F_{strong} = \{\{enter_1\}, \{enter_2\}\}$

$F_{weak} = \emptyset$

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

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

\[ T \]

\[ F_{ucond} = \emptyset \]
\[ F_{strong} = \{ \{ enter_1 \}, \{ enter_2 \} \} \]
\[ F_{weak} = \{ \{ req_1 \}, \{ req_2 \} \} \]

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

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

does $\mathcal{T} \models_{\mathcal{F}} \text{“infinitely often } a\text{” hold?}$
Fairness assumption \( \mathcal{F} \): unconditional fairness for action set \( \{a\} \)

\( \mathcal{T} \)

\( \{a\} \)

\( \alpha \)

\( \emptyset \)

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

answer: yes as there is no fair path
Fairness

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

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

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

not realizable

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

answer: yes as there is no fair path

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

$$\mathcal{T} \xrightarrow{\alpha} \{a\} \xrightarrow{} \emptyset$$

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

not realizable

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

answer: yes as there is no fair path

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

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

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

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

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

- unconditional fairness for \( A \in \mathcal{F}_{ucond} \)
  \( \rightsquigarrow \) 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 $\mathcal{F} = (\mathcal{F}_{ucond}, \mathcal{F}_{strong}, \mathcal{F}_{weak})$ for TS $\mathcal{T}$

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

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

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

  can always be guaranteed by a scheduler, i.e., an instance that resolves the nondeterminism in $\mathcal{T}$
Safety and realizable fairness
Realizable fairness assumptions are irrelevant for safety properties
Realizable fairness assumptions are irrelevant for safety properties

If $\mathcal{F}$ is a realizable fairness assumption for TS $\mathcal{T}$ and $E$ a safety property then:

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

$\alpha$: unconditional fairness for $\{a\}$

$\mathcal{F}$: 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:

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

... wrong for non-realizable fairness assumptions.

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

$E = \text{invariant “always } a\text{”}$

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