Overview

Introduction

Modelling parallel systems

Linear Time Properties

Regular Properties

Linear Temporal Logic (LTL)

- syntax and semantics of LTL ⟵
- automata-based LTL model checking
- complexity of LTL model checking

Computation-Tree Logic

Equivalences and Abstraction

Positive normal form (PNF)

Positive normal form (PNF)

- negation only on the level of literals
- uses for each operator its dual

PNF for propositional logic

- negation only on the level of literals
- uses for each operator its dual

syntax of propositional formulas in PNF:

$$\varphi \ ::= \ \mathit{true} \mid \mathit{false} \mid a \mid \neg a \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2$$

PNF for propositional logic

- negation only on the level of literals
- uses for each operator its dual

syntax of propositional formulas in PNF:

$$\varphi \ ::= \ \mathit{true} \mid \mathit{false} \mid a \mid \neg a \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2$$

$\neg \mathit{true} \ \equiv \ \mathit{false}$	duality of the constant truth values
$\neg(\varphi_1 \wedge \varphi_2) \ \equiv \ \neg\varphi_1 \vee \neg\varphi_2$	duality of $\vee$ and $\wedge$ (de Morgan's law)

LTL in positive normal form (PNF)

- negation only on the level of literals
- uses for each operator its dual

LTL in positive normal form (PNF)

- negation only on the level of literals
- uses for each operator its dual

$$\varphi \ ::= \ \mathit{true} \mid \mathit{false} \mid a \mid \neg a \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2$$

using duality of constants and duality of $\vee$ and $\wedge$

LTL in positive normal form (PNF)

- negation only on the level of literals
- uses for each operator its dual

$$\varphi \;::=\; \mathit{true} \mid \mathit{false} \mid a \mid \neg a \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid$$

$\bigcirc\varphi$ + dual operator for $\bigcirc$

using duality of constants and duality of $\vee$ and $\wedge$

LTL in positive normal form (PNF)

- negation only on the level of literals
- uses for each operator its dual

$$\varphi \;::=\; \mathit{true} \mid \mathit{false} \mid a \mid \neg a \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid$$

$$\bigcirc\varphi \longleftarrow \boxed{\text{no new operator needed for } \neg\bigcirc}$$

using duality of constants and duality of $\vee$ and $\wedge$

$\neg\bigcirc\varphi \;\equiv\; \bigcirc\neg\varphi$ self-duality of the next operator

LTL in positive normal form (PNF)

- negation only on the level of literals
- uses for each operator its dual

$$\varphi \ ::= \ \mathit{true} \mid \mathit{false} \mid a \mid \neg a \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \bigcirc\varphi \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \ + \text{dual operator for } \mathsf{U}$$

using duality of constants and duality of $\vee$ and $\wedge$

$\neg \bigcirc \varphi \ \equiv \ \bigcirc \neg \varphi$ self-duality of the next operator

LTL in positive normal form (PNF)

- negation only on the level of literals
- uses for each operator its dual

$$\boxed{\begin{array}{l} \varphi \;::=\; \mathit{true} \mid \mathit{false} \mid a \mid \neg a \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \\ \qquad\qquad \bigcirc\varphi \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \mid \varphi_1 \,\mathsf{W}\, \varphi_2 \end{array}}$$

using duality of constants and duality of $\vee$ and $\wedge$

$\neg\bigcirc\varphi \;\equiv\; \bigcirc\neg\varphi$ self-duality of the next operator

$\neg(\varphi_1 \,\mathsf{U}\, \varphi_2) \;\equiv\; (\neg\varphi_2)\,\mathsf{W}(\neg\varphi_1 \wedge \neg\varphi_2)$

duality of **U** and **W**

Derivation of $\Diamond$ and $\Box$ in LTL-PNF

$$\varphi \quad ::= \quad \mathit{true} \mid \mathit{false} \mid a \mid \neg a \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \bigcirc\varphi \mid \varphi_1 \mathsf{U} \varphi_2 \mid \varphi_1 \mathsf{W} \varphi_2$$

Derivation of $\Diamond$ and $\Box$ in LTL-PNF

$$\begin{array}{rcl} \varphi & ::= & \mathit{true} \mid \mathit{false} \mid a \mid \neg a \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \\ & & \bigcirc \varphi \mid \varphi_1 \, \mathsf{U} \, \varphi_2 \mid \varphi_1 \, \mathsf{W} \, \varphi_2 \mid \Diamond \varphi \mid \Box \varphi \end{array}$$

$\Diamond$ and $\Box$ can (still) be derived:

$$\Diamond \varphi \stackrel{\text{def}}{=} \mathit{true} \, \mathsf{U} \, \varphi$$

$$\Box \varphi \stackrel{\text{def}}{=} \varphi \, \mathsf{W} \, \mathit{false}$$

Universality of LTL-PNF

Universality of LTL-PNF

Each LTL formula can be transformed into an equivalent LTL formula in **PNF**

Each LTL formula can be transformed into an equivalent LTL formula in **PNF**

LTL formula $\varphi \rightsquigarrow$ LTL formula in PNF φ'
by successive application of the following rules:

Universality of LTL-PNF

> Each LTL formula can be transformed into an equivalent LTL formula in **PNF**

LTL formula $\varphi \rightsquigarrow$ LTL formula in PNF φ'
by successive application of the following rules:

$$
\begin{array}{lll}
\neg \mathit{true} & \rightsquigarrow & \mathit{false} \\
\neg\neg\varphi & \rightsquigarrow & \varphi \\
\neg(\varphi_1 \wedge \varphi_2) & \rightsquigarrow & \neg\varphi_1 \ \vee \ \neg\varphi_2 \\
\neg \bigcirc \varphi & \rightsquigarrow & \bigcirc\neg\varphi \\
\neg(\varphi_1 \, \mathsf{U} \, \varphi_2) & \rightsquigarrow & (\neg\varphi_2) \, \mathsf{W} (\neg\varphi_1 \wedge \neg\varphi_2)
\end{array}
$$

> Each LTL formula can be transformed into an equivalent LTL formula in **PNF**

LTL formula $\varphi \rightsquigarrow$ LTL formula in PNF φ'
by successive application of the following rules:

$$
\begin{array}{lcl}
\neg \mathit{true} & \rightsquigarrow & \mathit{false} \\
\neg\neg\varphi & \rightsquigarrow & \varphi \\
\neg(\varphi_1 \wedge \varphi_2) & \rightsquigarrow & \neg\varphi_1 \ \vee \ \neg\varphi_2 \\
\neg \bigcirc \varphi & \rightsquigarrow & \bigcirc\neg\varphi \\
\neg(\varphi_1 \,\mathsf{U}\, \varphi_2) & \rightsquigarrow & (\neg\varphi_2)\,\mathsf{W}(\neg\varphi_1 \wedge \neg\varphi_2)
\end{array}
$$

exponential-blow up is possible

Example: LTL $\rightsquigarrow$ LTL-PNF

$$
\begin{array}{lcl}
\neg \mathit{true} & \rightsquigarrow & \mathit{false} \\
\neg\neg\varphi & \rightsquigarrow & \varphi \\
\neg(\varphi_1 \wedge \varphi_2) & \rightsquigarrow & \neg\varphi_1 \vee \neg\varphi_2 \\
\neg \bigcirc \varphi & \rightsquigarrow & \bigcirc\neg\varphi \\
\neg(\varphi_1 \,\mathsf{U}\, \varphi_2) & \rightsquigarrow & (\neg\varphi_2)\,\mathsf{W}(\neg\varphi_1 \wedge \neg\varphi_2)
\end{array}
$$

Example: LTL $\rightsquigarrow$ LTL-PNF

$$\neg \mathit{true} \rightsquigarrow \mathit{false} \quad + \text{ analogue rule for } \neg \mathit{false}$$

$$\neg\neg\varphi \rightsquigarrow \varphi$$

$$\neg(\varphi_1 \wedge \varphi_2) \rightsquigarrow \neg\varphi_1 \vee \neg\varphi_2 \quad + \text{ analogue rule for } \neg\vee$$

$$\neg \bigcirc \varphi \rightsquigarrow \bigcirc\neg\varphi$$

$$\neg(\varphi_1 \,\mathsf{U}\, \varphi_2) \rightsquigarrow (\neg\varphi_2)\,\mathsf{W}(\neg\varphi_1 \wedge \neg\varphi_2)$$

Example: LTL $\rightsquigarrow$ LTL-PNF

$\neg \mathit{true}$	$\rightsquigarrow$	false	+ analogue rule for $\neg \mathit{false}$
$\neg\neg\varphi$	$\rightsquigarrow$	φ	
$\neg(\varphi_1 \wedge \varphi_2)$	$\rightsquigarrow$	$\neg\varphi_1 \vee \neg\varphi_2$	+ analogue rule for $\neg\vee$
$\neg \bigcirc \varphi$	$\rightsquigarrow$	$\bigcirc\neg\varphi$	
$\neg(\varphi_1 \, \mathsf{U} \, \varphi_2)$	$\rightsquigarrow$	$(\neg\varphi_2) \, \mathsf{W} (\neg\varphi_1 \wedge \neg\varphi_2)$	
$\neg\Diamond\varphi$	$\rightsquigarrow$	$\Box\neg\varphi$	$\neg\Box\varphi \rightsquigarrow \Diamond\neg\varphi$

Example: LTL $\rightsquigarrow$ LTL-PNF

$$
\begin{array}{lll}
\neg \mathit{true} & \rightsquigarrow & \mathit{false} \quad + \text{ analogue rule for } \neg \mathit{false} \\
\neg\neg\varphi & \rightsquigarrow & \varphi \\
\neg(\varphi_1 \wedge \varphi_2) & \rightsquigarrow & \neg\varphi_1 \vee \neg\varphi_2 \quad + \text{ analogue rule for } \neg\vee \\
\neg \bigcirc \varphi & \rightsquigarrow & \bigcirc\neg\varphi \\
\neg(\varphi_1 \,\mathsf{U}\, \varphi_2) & \rightsquigarrow & (\neg\varphi_2)\,\mathsf{W}(\neg\varphi_1 \wedge \neg\varphi_2) \\
\neg\Diamond\varphi & \rightsquigarrow & \Box\neg\varphi \qquad \neg\Box\varphi \rightsquigarrow \Diamond\neg\varphi
\end{array}
$$

$$\neg\Box((a \,\mathsf{U}\, b) \vee \bigcirc c)$$

Example: LTL $\rightsquigarrow$ LTL-PNF

$$\begin{array}{lll}
\neg \mathit{true} & \rightsquigarrow & \mathit{false} \quad + \text{ analogue rule for } \neg \mathit{false} \\
\neg\neg\varphi & \rightsquigarrow & \varphi \\
\neg(\varphi_1 \wedge \varphi_2) & \rightsquigarrow & \neg\varphi_1 \vee \neg\varphi_2 \quad + \text{ analogue rule for } \neg\vee \\
\neg \bigcirc \varphi & \rightsquigarrow & \bigcirc\neg\varphi \\
\neg(\varphi_1 \,\mathsf{U}\, \varphi_2) & \rightsquigarrow & (\neg\varphi_2)\,\mathsf{W}(\neg\varphi_1 \wedge \neg\varphi_2) \\
\neg\Diamond\varphi & \rightsquigarrow & \Box\neg\varphi \qquad \neg\Box\varphi \;\rightsquigarrow\; \Diamond\neg\varphi
\end{array}$$

$$\neg\Box((a \,\mathsf{U}\, b) \;\vee\; \bigcirc c)$$

$$\equiv \;\Diamond\neg((a \,\mathsf{U}\, b) \;\vee\; \bigcirc c) \qquad \longleftarrow \boxed{\text{duality of } \Diamond \text{ and } \Box}$$

$\neg \mathit{true}$	$\rightsquigarrow$	false	+ analogue rule for $\neg \mathit{false}$
$\neg\neg\varphi$	$\rightsquigarrow$	φ	
$\neg(\varphi_1 \wedge \varphi_2)$	$\rightsquigarrow$	$\neg\varphi_1 \vee \neg\varphi_2$	+ analogue rule for $\neg\vee$
$\neg \bigcirc \varphi$	$\rightsquigarrow$	$\bigcirc\neg\varphi$	
$\neg(\varphi_1 \, \mathsf{U} \, \varphi_2)$	$\rightsquigarrow$	$(\neg\varphi_2) \, \mathsf{W} (\neg\varphi_1 \wedge \neg\varphi_2)$	
$\neg\Diamond\varphi$	$\rightsquigarrow$	$\Box\neg\varphi$	$\neg\Box\varphi \rightsquigarrow \Diamond\neg\varphi$

$$\neg\Box((a \, \mathsf{U} \, b) \;\vee\; \bigcirc c)$$

$$\equiv \; \Diamond\neg((a \, \mathsf{U} \, b) \;\vee\; \bigcirc c) \qquad \longleftarrow \boxed{\text{duality of } \Diamond \text{ and } \Box}$$

$$\equiv \; \Diamond(\neg(a \, \mathsf{U} \, b) \;\wedge\; \neg\bigcirc c) \qquad \longleftarrow \boxed{\text{duality of } \wedge \text{ and } \vee}$$

Example: LTL $\rightsquigarrow$ LTL-PNF

$$\begin{array}{lcll}
\neg \mathit{true} & \rightsquigarrow & \mathit{false} & + \text{ analogue rule for } \neg \mathit{false} \\
\neg\neg\varphi & \rightsquigarrow & \varphi & \\
\neg(\varphi_1 \wedge \varphi_2) & \rightsquigarrow & \neg\varphi_1 \vee \neg\varphi_2 & + \text{ analogue rule for } \neg\vee \\
\neg \bigcirc \varphi & \rightsquigarrow & \bigcirc\neg\varphi & \\
\neg(\varphi_1 \,\mathsf{U}\, \varphi_2) & \rightsquigarrow & (\neg\varphi_2) \,\mathsf{W}\, (\neg\varphi_1 \wedge \neg\varphi_2) & \\
\neg\Diamond\varphi & \rightsquigarrow & \Box\neg\varphi & \neg\Box\varphi \rightsquigarrow \Diamond\neg\varphi
\end{array}$$

$$\begin{array}{lll}
 & \neg\Box((a \,\mathsf{U}\, b) \vee \bigcirc c) & \\
\equiv & \Diamond\neg((a \,\mathsf{U}\, b) \vee \bigcirc c) & \longleftarrow \boxed{\text{duality of } \Diamond \text{ and } \Box} \\
\equiv & \Diamond(\neg(a \,\mathsf{U}\, b) \wedge \neg\bigcirc c) & \longleftarrow \boxed{\text{duality of } \wedge \text{ and } \vee} \\
\equiv & \Diamond(\neg(a \,\mathsf{U}\, b) \wedge \bigcirc\neg c) & \longleftarrow \boxed{\text{self-duality of } \bigcirc}
\end{array}$$

$$\begin{array}{lll}
\neg \mathit{true} & \rightsquigarrow & \mathit{false} \quad + \text{ analogue rule for } \neg \mathit{false} \\
\neg\neg\varphi & \rightsquigarrow & \varphi \\
\neg(\varphi_1 \wedge \varphi_2) & \rightsquigarrow & \neg\varphi_1 \vee \neg\varphi_2 \quad + \text{ analogue rule for } \neg\vee \\
\neg \bigcirc \varphi & \rightsquigarrow & \bigcirc\neg\varphi \\
\neg(\varphi_1 \,\mathsf{U}\, \varphi_2) & \rightsquigarrow & (\neg\varphi_2)\,\mathsf{W}(\neg\varphi_1 \wedge \neg\varphi_2) \\
\neg\Diamond\varphi & \rightsquigarrow & \Box\neg\varphi \qquad \neg\Box\varphi \rightsquigarrow \Diamond\neg\varphi
\end{array}$$

$$\begin{array}{ll}
& \neg\Box((a \,\mathsf{U}\, b) \vee \bigcirc c) \\
\equiv & \Diamond\neg((a \,\mathsf{U}\, b) \vee \bigcirc c) \quad \longleftarrow \boxed{\text{duality of } \Diamond \text{ and } \Box} \\
\equiv & \Diamond(\neg(a \,\mathsf{U}\, b) \wedge \neg\bigcirc c) \quad \longleftarrow \boxed{\text{duality of } \wedge \text{ and } \vee} \\
\equiv & \Diamond((\neg b)\,\mathsf{W}(\neg a \wedge \neg b) \wedge \bigcirc\neg c) \longleftarrow \boxed{\text{duality of } \mathsf{U} \text{ and } \mathsf{W}}
\end{array}$$

Example: LTL $\rightsquigarrow$ LTL-PNF

$$
\begin{array}{lll}
\neg \mathit{true} & \rightsquigarrow & \mathit{false} \quad + \text{ analogue rule for } \neg \mathit{false} \\
\neg\neg\varphi & \rightsquigarrow & \varphi \\
\neg(\varphi_1 \wedge \varphi_2) & \rightsquigarrow & \neg\varphi_1 \vee \neg\varphi_2 \quad + \text{ analogue rule for } \neg\vee \\
\neg \bigcirc \varphi & \rightsquigarrow & \bigcirc\neg\varphi \\
\neg(\varphi_1 \,\mathsf{U}\, \varphi_2) & \rightsquigarrow & (\neg\varphi_2)\,\mathsf{W}(\neg\varphi_1 \wedge \neg\varphi_2) \\
\neg\Diamond\varphi & \rightsquigarrow & \Box\neg\varphi \qquad \neg\Box\varphi \rightsquigarrow \Diamond\neg\varphi
\end{array}
$$

$$
\begin{array}{ll}
 & \neg\Box\big((a \,\mathsf{U}\, b) \vee \bigcirc c\big) \\
\equiv & \Diamond\neg\big((a \,\mathsf{U}\, b) \vee \bigcirc c\big) \\
\equiv & \Diamond\big(\neg(a \,\mathsf{U}\, b) \wedge \neg\bigcirc c\big) \\
\equiv & \Diamond\big((\neg b)\,\mathsf{W}(\neg a \wedge \neg b) \wedge \bigcirc\neg c\big) \longleftarrow \boxed{\textbf{PNF}}
\end{array}
$$

Fairness in LTL

Recall: action-based fairness

Recall: action-based fairness

fairness assumption for TS $\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$:

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

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

- $\mathcal{F}_{ucond}$ unconditional fairness assumption
- $\mathcal{F}_{strong}$ strong fairness assumption
- $\mathcal{F}_{weak}$ weak fairness assumption

Recall: action-based fairness

fairness assumption for TS $\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$:

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

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

execution $s_0 \xrightarrow{\alpha_1} s_1 \xrightarrow{\alpha_2} s_2 \xrightarrow{\alpha_3} \ldots$ $\mathcal{F}$-fair if fairness assumption for TS $\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$:

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

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

execution $s_0 \xrightarrow{\alpha_1} s_1 \xrightarrow{\alpha_2} s_2 \xrightarrow{\alpha_3} \ldots$ $\mathcal{F}$-fair if

- for all $A \in \mathcal{F}_{ucond}$: $\stackrel{\infty}{\exists} i \geq 1.\, \alpha_i \in A$

fairness assumption for TS $\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$:

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

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

execution $s_0 \xrightarrow{\alpha_1} s_1 \xrightarrow{\alpha_2} s_2 \xrightarrow{\alpha_3} \ldots$ $\mathcal{F}$-fair if

- for all $A \in \mathcal{F}_{ucond}$: $\overset{\infty}{\exists}\, i \geq 1.\, \alpha_i \in A$
- for all $A \in \mathcal{F}_{strong}$:

$$\overset{\infty}{\exists}\, i \geq 1.\, A \cap Act(s_i) \neq \varnothing \implies \overset{\infty}{\exists}\, i \geq 1.\, \alpha_i \in A$$

Recall: action-based fairness

fairness assumption for TS $\mathcal{T} = (S, Act, \to, S_0, AP, L)$:

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

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

execution $s_0 \xrightarrow{\alpha_1} s_1 \xrightarrow{\alpha_2} s_2 \xrightarrow{\alpha_3} \ldots$ $\mathcal{F}$-fair if

- for all $A \in \mathcal{F}_{ucond}$: $\overset{\infty}{\exists}\, i \geq 1.\, \alpha_i \in A$
- for all $A \in \mathcal{F}_{strong}$:
  $$\overset{\infty}{\exists}\, i \geq 1.\, A \cap Act(s_i) \neq \varnothing \implies \overset{\infty}{\exists}\, i \geq 1.\, \alpha_i \in A$$
- for all $A \in \mathcal{F}_{weak}$:
  $$\overset{\infty}{\forall}\, i \geq 1.\, A \cap Act(s_i) \neq \varnothing \implies \overset{\infty}{\exists}\, i \geq 1.\, \alpha_i \in A$$

Recall: action-based fairness

fairness assumption for TS $\mathcal{T} = (S, Act, \to, S_0, AP, L)$:

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

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

satisfaction relation for LT-properties under fairness:

$\mathcal{T} \models_{\mathcal{F}} E$ iff for all $\mathcal{F}$-fair paths π of $\mathcal{T}$:
$trace(\pi) \in E$

Process fairness is LTL-definable

Process fairness is LTL-definable

$$\boxed{\varphi \ ::= \ \mathit{true} \mid a \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \bigcirc \varphi \mid \varphi_1 \,\mathsf{U}\, \varphi_2}$$

eventually $\Diamond\varphi \stackrel{\text{def}}{=} \mathit{true} \,\mathsf{U}\, \varphi$

always $\Box\varphi \stackrel{\text{def}}{=} \neg\Diamond\neg\varphi$

infinitely often $\Box\Diamond\varphi$

eventually forever $\Diamond\Box\varphi$

Process fairness is LTL-definable

$$\varphi \ ::= \ \mathit{true} \ \big| \ a \ \big| \ \varphi_1 \wedge \varphi_2 \ \big| \ \neg\varphi \ \big| \ \bigcirc \varphi \ \big| \ \varphi_1 \, \mathsf{U} \, \varphi_2$$

eventually	$\Diamond\varphi$	$\stackrel{\text{def}}{=}$	$\mathit{true}\,\mathsf{U}\,\varphi$
always	$\Box\varphi$	$\stackrel{\text{def}}{=}$	$\neg\Diamond\neg\varphi$
infinitely often		$\Box\Diamond\,\varphi$	
eventually forever		$\Diamond\Box\,\varphi$	

e.g., unconditional fairness $\Box\Diamond \mathit{crit}_i$

strong fairness $\Box\Diamond \mathit{wait}_i \rightarrow \Box\Diamond \mathit{crit}_i$

$$\varphi \ ::= \ \mathit{true} \mid a \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \bigcirc\varphi \mid \varphi_1 \,\mathsf{U}\, \varphi_2$$

eventually	$\Diamond\varphi$	$\stackrel{\text{def}}{=}$	$\mathit{true}\,\mathsf{U}\,\varphi$
always	$\Box\varphi$	$\stackrel{\text{def}}{=}$	$\neg\Diamond\neg\varphi$
infinitely often		$\Box\Diamond\varphi$	
eventually forever		$\Diamond\Box\varphi$	

e.g.,	unconditional fairness	$\Box\Diamond \mathit{crit}_i$
	strong fairness	$\Box\Diamond \mathit{wait}_i \longrightarrow \Box\Diamond \mathit{crit}_i$
	weak fairness	$\Diamond\Box \mathit{wait}_i \longrightarrow \Box\Diamond \mathit{crit}_i$

LTL fairness assumptions

LTL fairness assumptions

... are conjunctions of LTL formulas of the form:

- unconditional fairness $\Box\Diamond\phi$
- strong fairness $\Box\Diamond\phi_1 \rightarrow \Box\Diamond\phi_2$
- weak fairness $\Diamond\Box\phi_1 \rightarrow \Box\Diamond\phi_2$

where ϕ_1, ϕ_2, ϕ are propositional formulas

... are conjunctions of LTL formulas of the form:

- unconditional fairness $\Box\Diamond\phi$
- strong fairness $\Box\Diamond\phi_1 \rightarrow \Box\Diamond\phi_2$
- weak fairness $\Diamond\Box\phi_1 \rightarrow \Box\Diamond\phi_2$

where ϕ_1, ϕ_2, ϕ are propositional formulas

If *fair* is a LTL fairness assumption, s a state in a TS, and φ an LTL formula then

... are conjunctions of LTL formulas of the form:

- unconditional fairness $\Box\Diamond\phi$
- strong fairness $\Box\Diamond\phi_1 \rightarrow \Box\Diamond\phi_2$
- weak fairness $\Diamond\Box\phi_1 \rightarrow \Box\Diamond\phi_2$

where ϕ_1, ϕ_2, ϕ are propositional formulas

If *fair* is a LTL fairness assumption, s a state in a TS, and φ an LTL formula then

$$s \models_{fair} \varphi \quad \text{iff} \quad \text{for all } \pi \in \mathit{Paths}(s)\text{:}$$
$$\text{if } \pi \models \mathit{fair} \text{ then } \pi \models \varphi$$

LTL fairness assumptions

... are conjunctions of **LTL formulas** of the form:

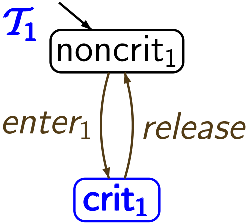
- unconditional fairness $\Box\Diamond\phi$
- strong fairness $\Box\Diamond\phi_1 \rightarrow \Box\Diamond\phi_2$
- weak fairness $\Diamond\Box\phi_1 \rightarrow \Box\Diamond\phi_2$

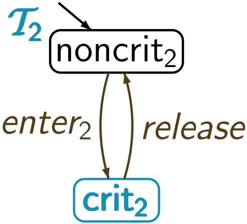
where ϕ_1, ϕ_2, ϕ are propositional formulas

If *fair* is a LTL fairness assumption, s a state in a TS, and φ an LTL formula then

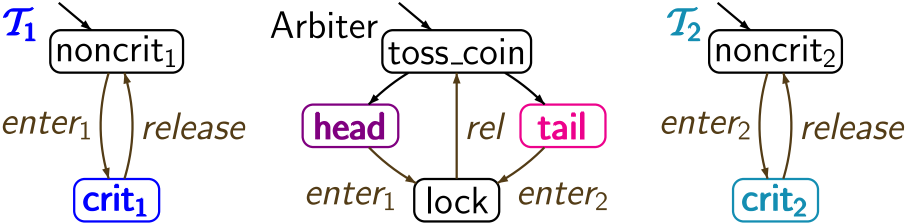
$$\begin{array}{lll} s \models_{fair} \varphi & \text{iff} & \text{for all } \pi \in Paths(s): \\ & & \quad \text{if } \pi \models fair \text{ then } \pi \models \varphi \\ & \text{iff} & s \models fair \rightarrow \varphi \end{array}$$

Randomized arbiter for MUTEX

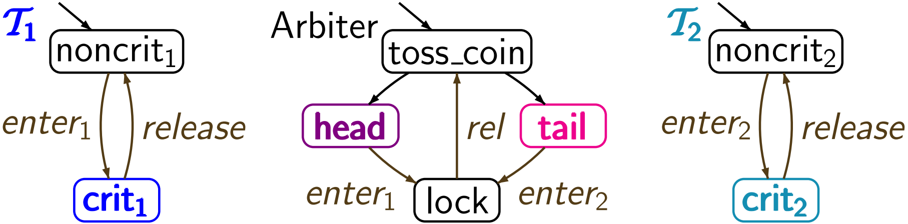




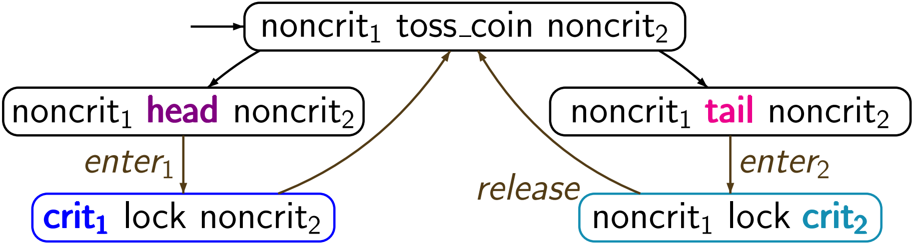
Randomized arbiter for MUTEX



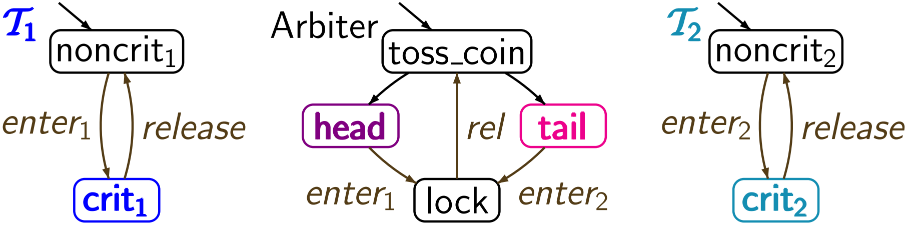
Randomized arbiter for MUTEX



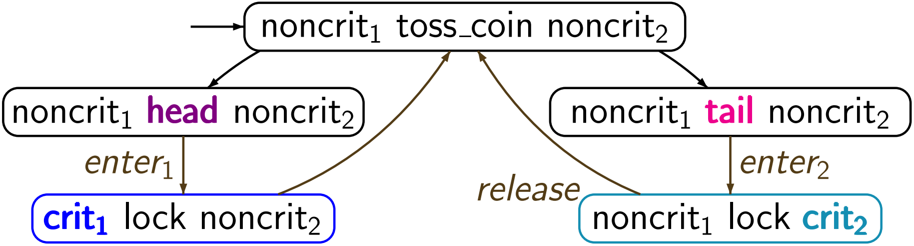
$(\mathcal{T}_1 \mid\mid\mid \mathcal{T}_2) \parallel \mathit{Arbiter}$



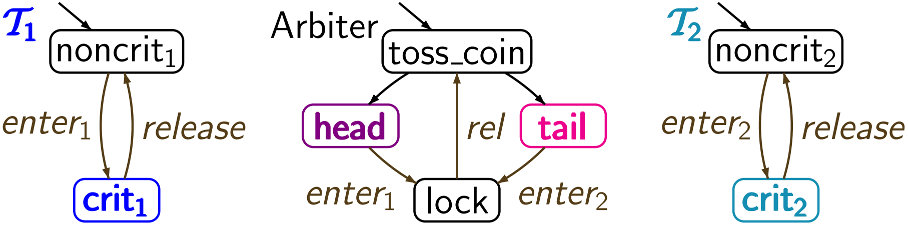
Randomized arbiter for MUTEX



$$(\mathcal{T}_1 \,|||\, \mathcal{T}_2) \,\|\, \textit{Arbiter} \not\models \Box\Diamond \textbf{crit}_1 \wedge \Box\Diamond \textbf{crit}_2$$



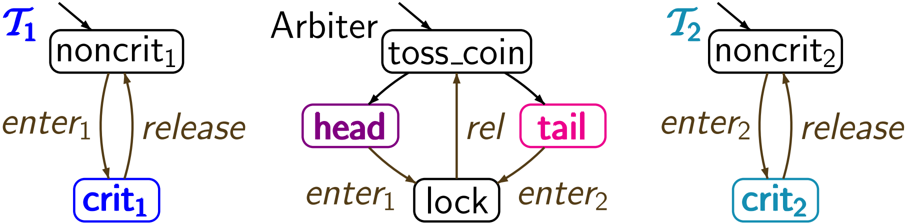
Randomized arbiter for MUTEX



unconditional LTL-fairness:

$$fair = \Box\Diamond \mathbf{head} \wedge \Box\Diamond \mathbf{tail}$$

Randomized arbiter for MUTEX

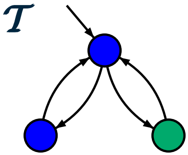


unconditional LTL-fairness:

$$fair \; = \; \Box\Diamond \mathsf{head} \;\wedge\; \Box\Diamond \mathsf{tail}$$

$$(\mathcal{T}_1 \;|||\; \mathcal{T}_2) \,\|\, \mathit{Arbiter} \;\models_{fair}\; \Box\Diamond \mathsf{crit}_1 \;\wedge\; \Box\Diamond \mathsf{crit}_2$$

Correct or wrong?

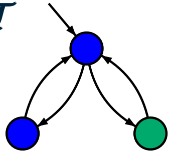


LTL fairness assumption
$fair = \Diamond\Box a \rightarrow \Box\Diamond b$

● $\widehat{=}\{a\}$ ● $\widehat{=}\{b\}$

Correct or wrong?

$\mathcal{T}$

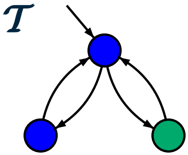


LTL fairness assumption
$fair = \Diamond\Box a \rightarrow \Box\Diamond b$

● $\widehat{=} \{a\}$ ● $\widehat{=} \{b\}$

$\mathcal{T} \models_{fair} \bigcirc b$ **?**

Correct or wrong?



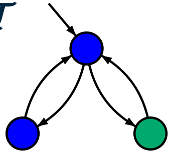
LTL fairness assumption

$fair = \Diamond\Box a \rightarrow \Box\Diamond b$

● $\widehat{=}\{a\}$ ● $\widehat{=}\{b\}$

$\mathcal{T} \not\models_{fair} \bigcirc b$ as ● → ● → ● → ● → ● → ● → … is fair

$\mathcal{T}$



LTL fairness assumption

$fair = \Diamond\Box a \rightarrow \Box\Diamond b$

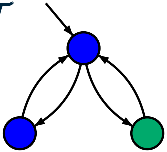
$\bullet \;\widehat{=}\{a\}$ $\bullet \;\widehat{=}\{b\}$

$\mathcal{T} \not\models_{fair} \bigcirc b$ as $\bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \ldots$ is fair

$\mathcal{T} \models_{fair} a \,\mathsf{U}\, b$ **?**

Correct or wrong?

$\mathcal{T}$



LTL fairness assumption

$fair = \Diamond\Box a \rightarrow \Box\Diamond b$

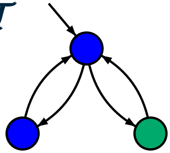
● $\widehat{=} \{a\}$ ● $\widehat{=} \{b\}$

$\mathcal{T} \not\models_{fair} \bigcirc b$ as ●→●→●→●→●→●→ … is fair

$\mathcal{T} \models_{fair} a \,\mathsf{U}\, b$ $\surd$

Correct or wrong?

$\mathcal{T}$



LTL fairness assumption

$$fair = \Diamond\Box a \rightarrow \Box\Diamond b$$

${\color{blue}\bullet} \,\widehat{=}\, \{a\} \quad {\color{green}\bullet} \,\widehat{=}\, \{b\}$

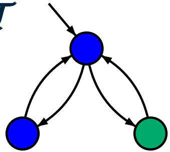
$\mathcal{T} \not\models_{fair} \bigcirc b$ as ${\color{blue}\bullet} \longrightarrow {\color{blue}\bullet} \longrightarrow {\color{blue}\bullet} \longrightarrow {\color{green}\bullet} \longrightarrow {\color{blue}\bullet} \longrightarrow {\color{green}\bullet} \longrightarrow \ldots$ is fair

$\mathcal{T} \models_{fair} a \,\mathsf{U}\, b$ $\surd$

$\mathcal{T} \models_{fair} a \,\mathsf{U}\, \Box(b \leftrightarrow \bigcirc a)$ **?**

Correct or wrong?

$\mathcal{T}$



LTL fairness assumption

$fair = \Diamond\Box a \rightarrow \Box\Diamond b$

$\textcolor{blue}{\bullet} \mathrel{\widehat{=}} \{a\} \quad \textcolor{green}{\bullet} \mathrel{\widehat{=}} \{b\}$

$\mathcal{T} \not\models_{fair} \bigcirc b$ as $\textcolor{blue}{\bullet} \rightarrow \textcolor{blue}{\bullet} \rightarrow \textcolor{blue}{\bullet} \rightarrow \textcolor{green}{\bullet} \rightarrow \textcolor{blue}{\bullet} \rightarrow \textcolor{green}{\bullet} \rightarrow \ldots$ is fair

$\mathcal{T} \models_{fair} a \,\mathsf{U}\, b$ $\surd$

$\mathcal{T} \not\models_{fair} a \,\mathsf{U}\, \Box(b \leftrightarrow \bigcirc a)$

as $\textcolor{blue}{\bullet} \rightarrow \textcolor{green}{\bullet} \rightarrow \textcolor{blue}{\bullet} \rightarrow \textcolor{blue}{\bullet} \rightarrow \textcolor{blue}{\bullet} \rightarrow \textcolor{green}{\bullet} \rightarrow \ldots$ is fair

LTL-fairness assumptions

- can be necessary to prove liveness properties, e.g., mutual exclusion with arbiter/semaphore

$$\mathcal{T}_{sem} \not\models \Box\Diamond crit_1 \wedge \Box\Diamond crit_2$$

$$\mathcal{T}_{sem} \models_{fair} \Box\Diamond crit_1 \wedge \Box\Diamond crit_2$$

for appropriate fairness condition

LTL-fairness assumptions

- can be necessary to prove liveness properties, e.g., mutual exclusion with arbiter/semaphore

$$\mathcal{T}_{sem} \not\models \Box\Diamond crit_1 \wedge \Box\Diamond crit_2$$
$$\mathcal{T}_{sem} \models_{fair} \Box\Diamond crit_1 \wedge \Box\Diamond crit_2$$

for appropriate fairness condition, e.g.,

$$fair = \bigwedge_{i=1,2} \big((\Box\Diamond wait_i \rightarrow \Box\Diamond crit_i) \wedge (\Diamond\Box noncrit_i \rightarrow \Box\Diamond wait_i) \big)$$

- can be necessary to prove liveness properties, e.g., mutual exclusion with arbiter/semaphore

$$\mathcal{T}_{sem} \not\models \Box\Diamond crit_1 \wedge \Box\Diamond crit_2$$

$$\mathcal{T}_{sem} \models_{fair} \Box\Diamond crit_1 \wedge \Box\Diamond crit_2$$

for appropriate fairness condition

- can be verifiable system properties

e.g., Peterson algorithm guarantees strong fairness

$$\mathcal{T}_{Pet} \models \Box\Diamond wait_1 \rightarrow \Box\Diamond crit_1$$

LTL-fairness assumptions

- can be necessary to prove liveness properties, e.g.,

$$\mathcal{T}_{sem} \not\models \Box\Diamond crit_1 \wedge \Box\Diamond crit_2$$
$$\mathcal{T}_{sem} \models_{fair} \Box\Diamond crit_1 \wedge \Box\Diamond crit_2$$

  for appropriate fairness condition

- can be verifiable system properties, e.g.,

$$\mathcal{T}_{Pet} \models \Box\Diamond wait_1 \rightarrow \Box\Diamond crit_1$$

- are irrelevant for verifying safety properties

$$\mathcal{T} \models \varphi_{safe} \quad \text{iff} \quad \mathcal{T} \models_{fair} \varphi_{safe}$$

if *fair* is realizable

Correct or wrong?

Each strong **LTL** fairness assumption

$$fair \;=\; \Box\Diamond a \rightarrow \Box\Diamond b$$

is realizable for each TS over $AP = \{a, b, \ldots\}$.

Correct or wrong?

Each strong **LTL** fairness assumption

$$\mathit{fair} \;=\; \Box\Diamond a \rightarrow \Box\Diamond b$$

is realizable for each TS over $AP = \{a, b, \ldots\}$.

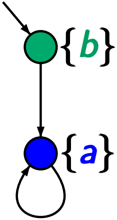
recall: a fairness condition is called realizable
if for each reachable state s there exists
a fair path starting in s

Each strong **LTL** fairness assumption

$$fair \;=\; \Box\Diamond a \rightarrow \Box\Diamond b$$

is realizable for each TS over $AP = \{a, b, \ldots\}$.

wrong



$fair = \Box\Diamond a \rightarrow \Box\Diamond b$

is <u>not</u> realizable

Action-based fairness $\rightsquigarrow$ LTL-fairness

Action-based fairness $\rightsquigarrow$ LTL-fairness

idea: use new atomic propositions ***enabled*(A)** and ***taken*(A)** and extend the labeling function:

$$\mathit{enabled}(A) \in L(s) \quad \text{iff} \quad s \xrightarrow{\alpha} \ldots \text{ for some } \alpha \in A$$

$$\mathit{taken}(A) \in L(s) \quad \text{iff} \quad \text{for all transitions } \ldots \xrightarrow{\alpha} s\text{:} \quad \alpha \in A$$

Action-based fairness $\rightsquigarrow$ LTL-fairness

idea: use new atomic propositions $\mathit{enabled}(A)$ and $\mathit{taken}(A)$ and extend the labeling function:

$$\mathit{enabled}(A) \in L(s) \quad \text{iff} \quad s \xrightarrow{\alpha} \ldots \text{ for some } \alpha \in A$$

$$\mathit{taken}(A) \in L(s) \quad \text{iff} \quad \text{for all transitions } \ldots \xrightarrow{\alpha} s\text{: } \alpha \in A$$

- unconditional A-fairness: $\Box\Diamond \mathit{taken}(A)$
- strong A-fairness: $\Box\Diamond \mathit{enabled}(A) \rightarrow \Box\Diamond \mathit{taken}(A)$
- weak A-fairness: $\Diamond\Box \mathit{enabled}(A) \rightarrow \Box\Diamond \mathit{taken}(A)$

Action-based fairness $\rightsquigarrow$ LTL-fairness

idea: use new atomic propositions ***enabled***(A) and ***taken***(A) and extend the labeling function:

$$\begin{array}{lcl} \mathit{enabled}(A) \in L(s) & \text{iff} & s \xrightarrow{\alpha} \ldots \text{ for some } \alpha \in A \\ \mathit{taken}(A) \in L(s) & \text{iff} & \text{for } \boxed{\text{all}} \text{ transitions } \ldots \xrightarrow{\alpha} s\text{:} \\ & & \qquad\qquad \alpha \in A \end{array}$$

problem: each state s can have several incoming transitions

$$t \xrightarrow{\alpha} s, \quad u \xrightarrow{\beta} s, \ \ldots$$

Action-based fairness $\rightsquigarrow$ LTL-fairness

idea: use new atomic propositions ***enabled***(A) and ***taken***(A) and extend the labeling function:

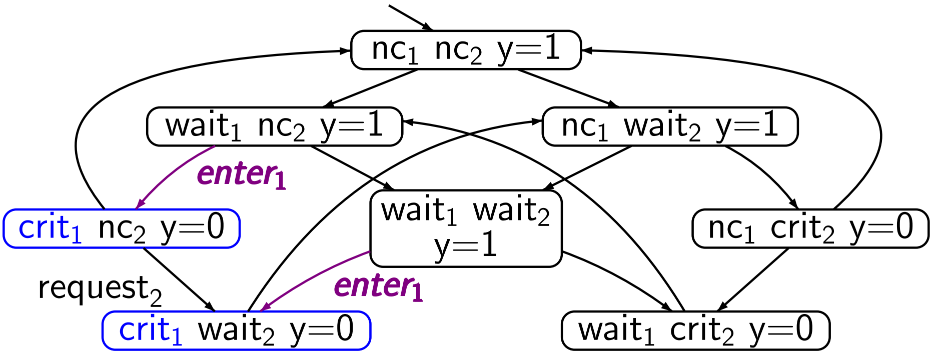
$$\textit{enabled}(A) \in L(s) \quad \text{iff} \quad s \xrightarrow{\alpha} \ldots \text{ for some } \alpha \in A$$

$$\textit{taken}(A) \in L(s) \quad \text{iff} \quad \text{for } \boxed{\text{all}} \text{ transitions } \ldots \xrightarrow{\alpha} s\text{: } \alpha \in A$$

alternative 1: ad-hoc choice of "***taken***-predicate"

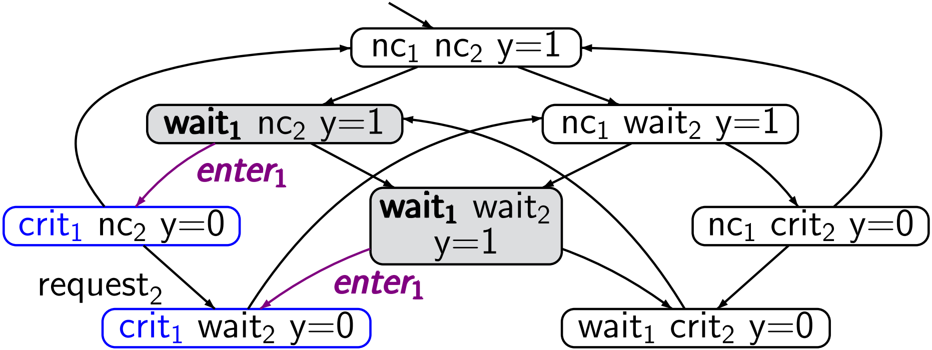
alternative 2: modify the given transition system by adding an action component to the states

Ad-hoc: action fairness ⇝ LTL-fairness



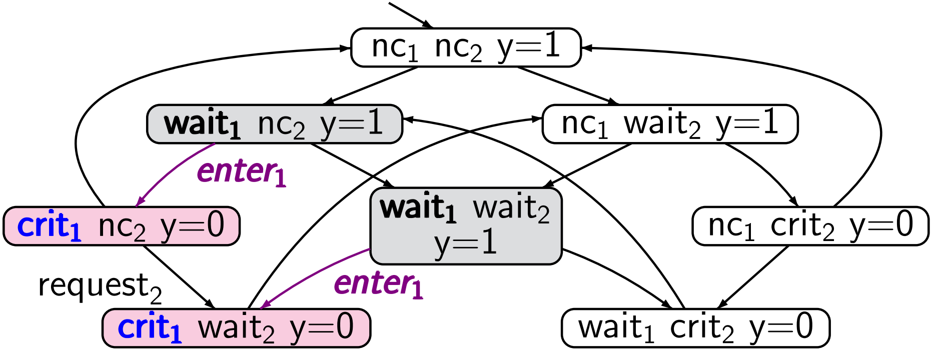
TS for mutual exclusion with semaphore

Ad-hoc: action fairness ⇝ LTL-fairness



$\square \;\widehat{=}\;$ *enabled*({*enter*$_1$})

TS for mutual exclusion with semaphore

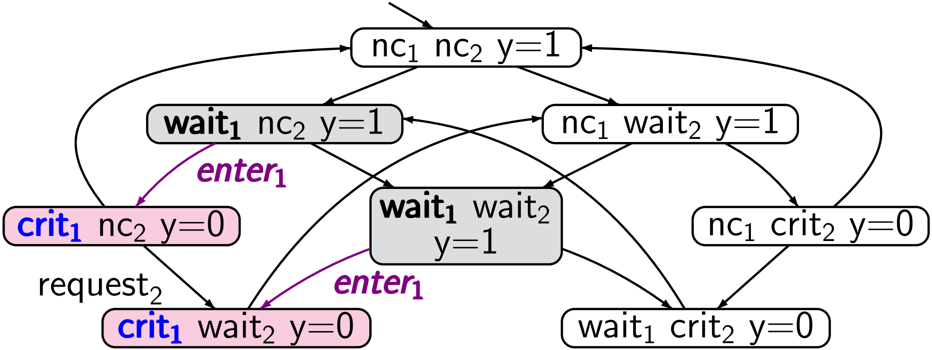


 $\widehat{=}$ *taken*({*enter*$_1$})

 $\widehat{=}$ *enabled*({*enter*$_1$})

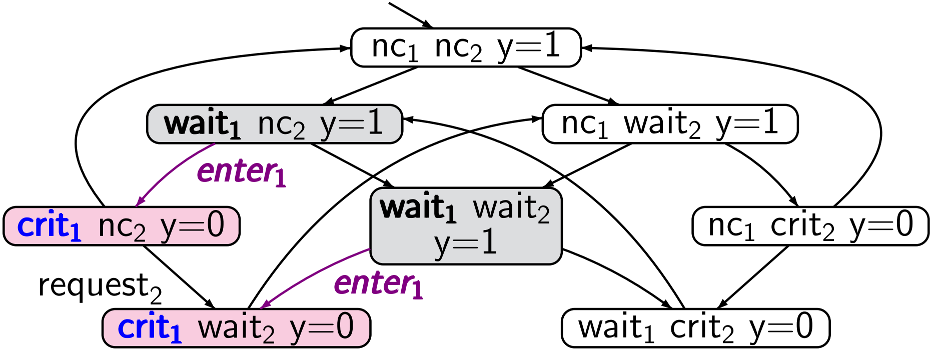
TS for mutual exclusion with semaphore

Ad-hoc: action fairness ⇝ LTL-fairness



(pink box)	$\widehat{=}$	*taken*({*enter*$_1$})	$\widehat{=}$	$crit_1$
(grey box)	$\widehat{=}$	*enabled*({*enter*$_1$})	$\widehat{=}$	$wait_1 \wedge \neg crit_2$

Ad-hoc: action fairness ⇝ LTL-fairness

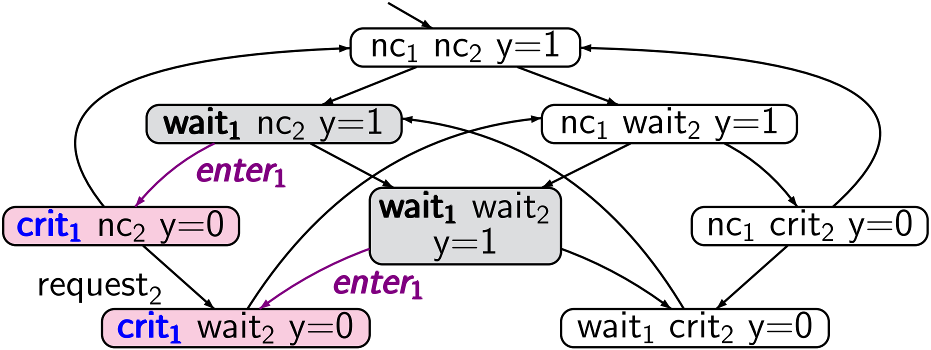


(pink box)	$\widehat{=}$	*taken*({*enter*$_1$})	$\widehat{=}$	**crit$_1$**
(grey box)	$\widehat{=}$	*enabled*({*enter*$_1$})	$\widehat{=}$	**wait$_1$** $\wedge$ $\neg$**crit$_2$**

strong {*enter*$_1$}-fairness: LTL formula

$$\Box\Diamond\, \mathit{enabled}(\{\mathit{enter}_1\}) \rightarrow \Box\Diamond\, \mathit{taken}(\{\mathit{enter}_1\})$$

Ad-hoc: action fairness ⇝ LTL-fairness



(pink)	$\widehat{=}$	*taken*({*enter*$_1$})	$\widehat{=}$	**crit$_1$**
(grey)	$\widehat{=}$	*enabled*({*enter*$_1$})	$\widehat{=}$	**wait$_1$ $\wedge$ ¬crit$_2$**

$$\Box\Diamond\, enabled(\{enter_1\}) \;\rightarrow\; \Box\Diamond\, taken(\{enter_1\})$$

$$\widehat{=}\;\; \Box\Diamond\,(wait_1 \wedge \neg crit_2) \;\rightarrow\; \Box\Diamond\, crit_1$$

Action-based fairness $\rightsquigarrow$ LTL-fairness

idea: use new atomic propositions $\mathit{enabled}(A)$ and $\mathit{taken}(A)$ and extend the labeling function:

$$\mathit{enabled}(A) \in L(s) \quad \text{iff} \quad s \xrightarrow{\alpha} \dots \text{ for some } \alpha \in A$$

$$\mathit{taken}(A) \in L(s) \quad \text{iff} \quad \text{for all transitions } \dots \xrightarrow{\alpha} s\text{:} \ \alpha \in A$$

alternative 1: **ad-hoc choice** of "***taken***-predicate"

alternative 2: modify the given transition system by adding an action component to the states

Action-based fairness $\rightsquigarrow$ LTL-fairness

idea: use new atomic propositions ***enabled***(A) and ***taken***(A) and extend the labeling function:

$$enabled(A) \in L(s) \quad \text{iff} \quad s \xrightarrow{\alpha} \dots \text{ for some } \alpha \in A$$

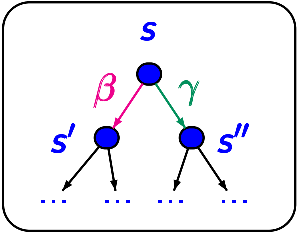
$$taken(A) \in L(s) \quad \text{iff} \quad \text{for all transitions } \dots \xrightarrow{\alpha} s\text{:} \ \alpha \in A$$

alternative 1: ad-hoc choice of "***taken***-predicate"

alternative 2: modify the given transition system by **adding an action component** to the states

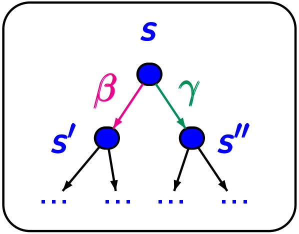
Action-based fairness $\leadsto$ LTL-fairness

transition system
$$\mathcal{T} = (S, Act, \rightarrow, \ldots)$$

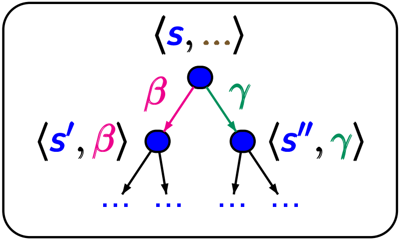


Action-based fairness $\rightsquigarrow$ LTL-fairness

transition system
$\mathcal{T} = (S, Act, \rightarrow, \ldots)$

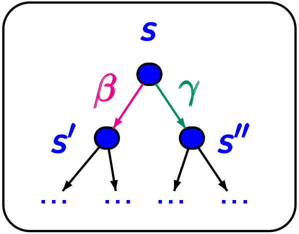


transition system
$\mathcal{T}' = (S \times Act, \ldots, AP', L')$

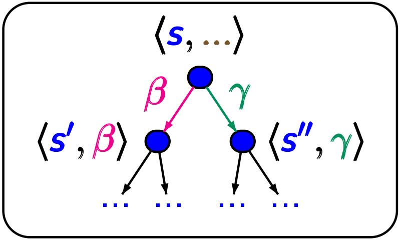


Action-based fairness $\rightsquigarrow$ LTL-fairness

transition system
$\mathcal{T} = (S, Act, \rightarrow, \ldots)$



transition system
$\mathcal{T}' = (S \times Act, \ldots, AP', L')$

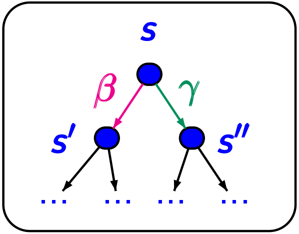


strong A-fairness
for $A \subseteq Act$

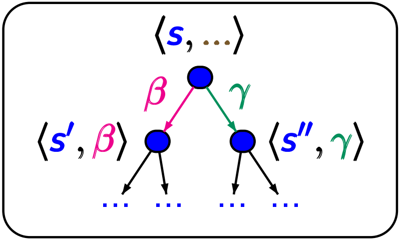
strong **LTL**-fairness
$\Box\Diamond enabled(A) \rightarrow \Box\Diamond taken(A)$

Action-based fairness $\rightsquigarrow$ LTL-fairness

transition system
$\mathcal{T} = (S, Act, \rightarrow, \ldots)$



transition system
$\mathcal{T}' = (S \times Act, \ldots, AP', L')$



strong A-fairness
for $A \subseteq Act$

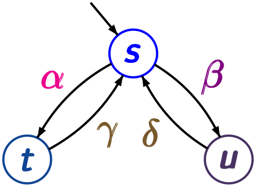
strong **LTL**-fairness
$\Box\Diamond enabled(A) \rightarrow \Box\Diamond taken(A)$

$enabled(A) \in L'(\langle s, \alpha \rangle)$ iff $s \xrightarrow{\beta} \ldots$ for some $\beta \in A$

$taken(A) \in L'(\langle s, \alpha \rangle)$ iff $\alpha \in A$

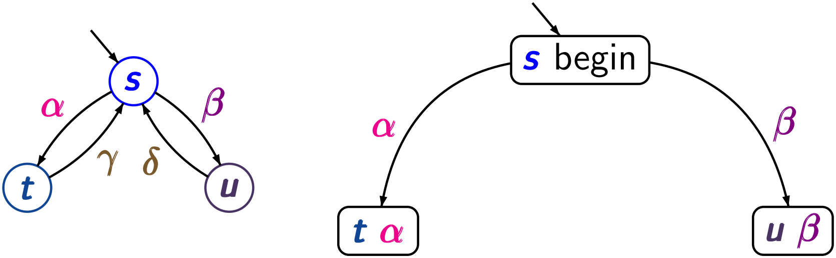
Example: action fairness $\rightsquigarrow$ LTL-fairness

action-based fairness $\rightsquigarrow$ LTL-fairness



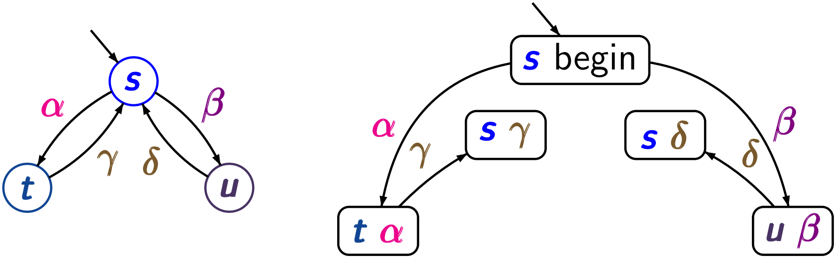
Example: action fairness ⇝ LTL-fairness

action-based fairness ⇝ LTL-fairness



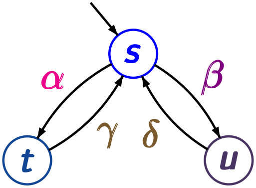
Example: action fairness $\rightsquigarrow$ LTL-fairness

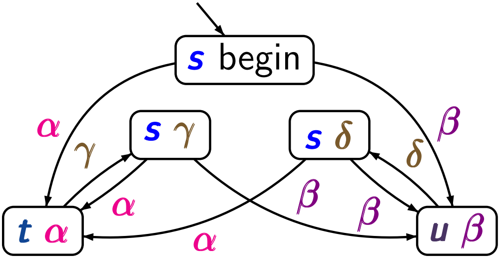
action-based fairness $\rightsquigarrow$ LTL-fairness



Example: action fairness ⇝ LTL-fairness

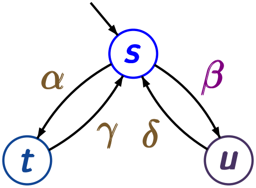
action-based fairness ⇝ LTL-fairness

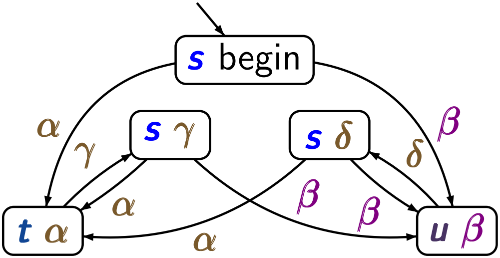




Example: action fairness ⇝ LTL-fairness

action-based fairness ⇝ LTL-fairness



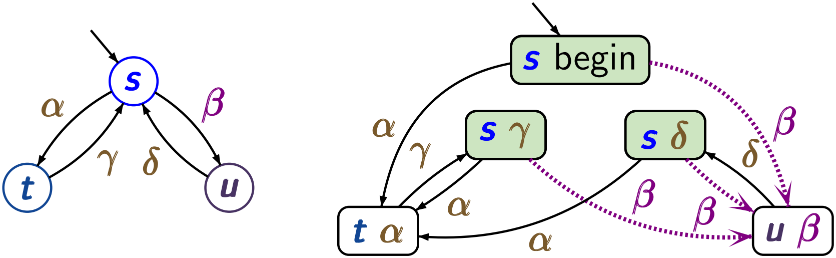


strong fairness for $\{\beta\}$:

$$\Box\Diamond\, \mathit{enabled}(\beta) \rightarrow \Box\Diamond\, \mathit{taken}(\beta)$$

Example: action fairness ⇝ LTL-fairness

action-based fairness ⇝ LTL-fairness

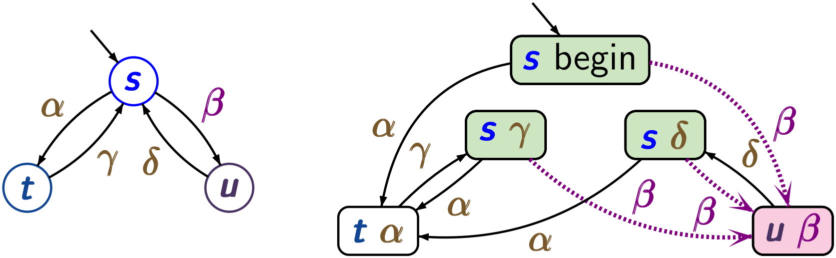


strong fairness for $\{\beta\}$:

$$\Box\Diamond\, \mathit{enabled}(\beta) \rightarrow \Box\Diamond\, \mathit{taken}(\beta)$$

Example: action fairness $\rightsquigarrow$ LTL-fairness

action-based fairness $\rightsquigarrow$ LTL-fairness

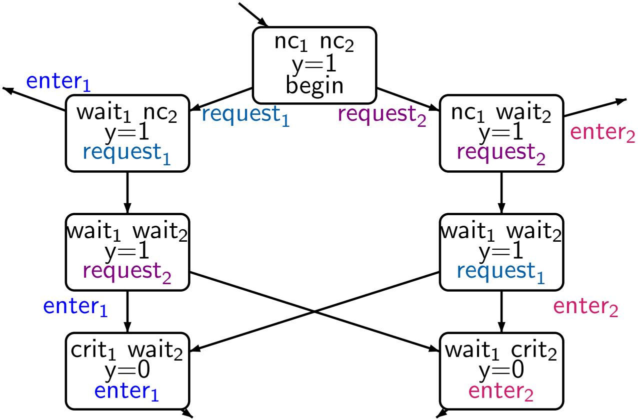


strong fairness for $\{\beta\}$:

$$\Box\Diamond\, enabled(\beta) \rightarrow \Box\Diamond\, taken(\beta)$$

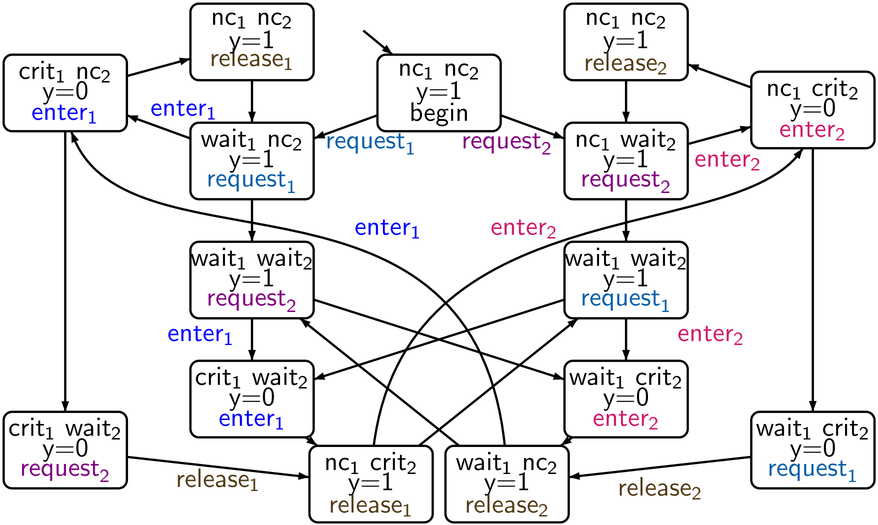
Example: mutual exclusion with semaphore

add additional variable last_action with domain Act ∪ {begin}



Example: mutual exclusion with semaphore

add additional variable last_action with domain Act ∪ {begin}



Example: mutual exclusion with semaphore

add additional variable last_action with domain Act $\cup$ {begin}