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

Linear Temporal Logic (LTL)

Linear Temporal Logic (LTL)

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

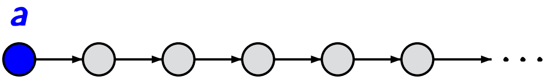
where $a \in AP$ $\qquad \bigcirc \;\widehat{=}\;$ next $\qquad \mathsf{U} \;\widehat{=}\;$ until

Linear Temporal Logic (LTL)

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

where $a \in AP$ $\qquad \bigcirc \mathrel{\widehat{=}}$ next $\qquad \mathsf{U} \mathrel{\widehat{=}}$ until

atomic proposition $a \in AP$

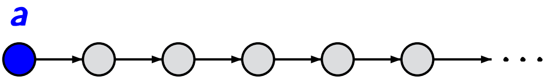


Linear Temporal Logic (LTL)

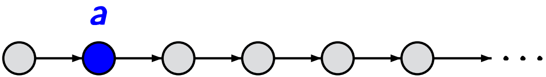
$$\varphi \;::=\; \mathit{true} \;\mid\; a \;\mid\; \varphi_1 \wedge \varphi_2 \;\mid\; \neg\varphi \;\mid\; \bigcirc\varphi \;\mid\; \varphi_1 \,\mathsf{U}\, \varphi_2$$

where $a \in AP$ $\qquad$ $\bigcirc \mathrel{\widehat{=}}$ next $\qquad$ $\mathsf{U} \mathrel{\widehat{=}}$ until

atomic proposition $a \in AP$



next operator $\bigcirc a$

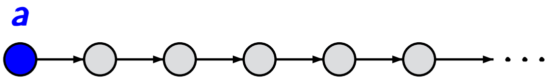


Linear Temporal Logic (LTL)

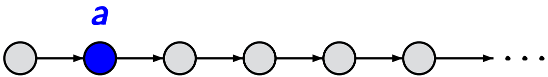
$$\boxed{\varphi \ ::= \ \textit{true} \ \big| \ a \ \big| \ \varphi_1 \wedge \varphi_2 \ \big| \ \neg\varphi \ \big| \ \bigcirc \varphi \ \big| \ \varphi_1 \, \mathsf{U} \, \varphi_2}$$

where $a \in AP$ $\quad\quad$ $\bigcirc \mathrel{\widehat{=}}$ next $\quad\quad$ $\mathsf{U} \mathrel{\widehat{=}}$ until

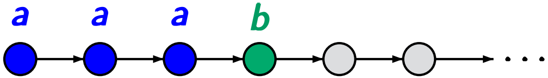
atomic proposition $a \in AP$



next operator $\bigcirc a$



until operator $a \, \mathsf{U} \, b$



Derived operators in LTL

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

derived operators:

$\vee, \rightarrow, \ldots$ as usual

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

derived operators:

$\vee, \rightarrow, \ldots$ as usual

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

Derived operators in LTL

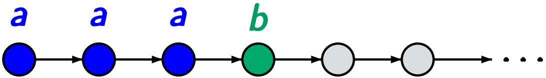
$$\varphi \ ::= \ \mathit{true} \ \big| \ a \ \big| \ \varphi_1 \wedge \varphi_2 \ \big| \ \neg\varphi \ \big| \ \bigcirc \varphi \ \big| \ \varphi_1 \,\mathsf{U}\, \varphi_2$$

derived operators:

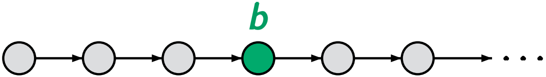
$\vee, \rightarrow, \ldots$ as usual

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

until operator
$a \,\mathsf{U}\, b$



eventually
$\Diamond b$



Derived operators in LTL

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

derived operators:

$\vee, \rightarrow, \ldots$ as usual

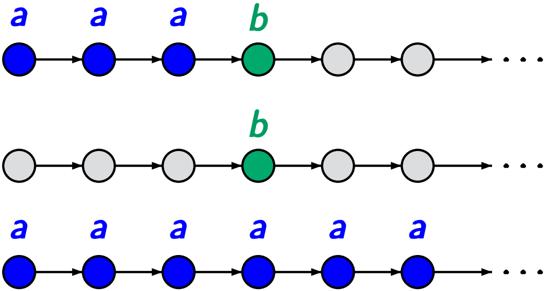
$$\Diamond\varphi \ \stackrel{\text{def}}{=} \ \mathit{true} \, \mathsf{U} \, \varphi \qquad \text{eventually}$$

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

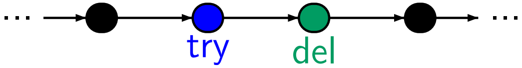
until operator $a \, \mathsf{U} \, b$

eventually $\Diamond b$

always $\Box a$

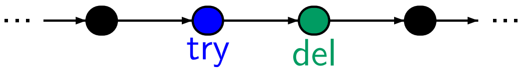


$\Box\,(\text{try\_to\_send} \rightarrow \bigcirc\ \text{delivered})$

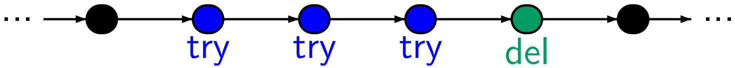


Next $\bigcirc$, until U and eventually $\Diamond$

$\Box\ (\text{try\_to\_send} \rightarrow \bigcirc\ \text{delivered})$

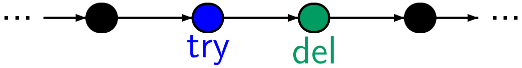


$\Box\ (\text{try\_to\_send} \rightarrow \text{try\_to\_send}\ \mathsf{U}\ \text{delivered})$

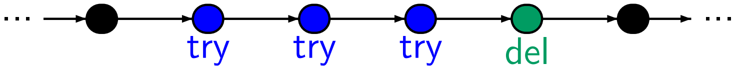


Next $\bigcirc$, until U and eventually $\Diamond$

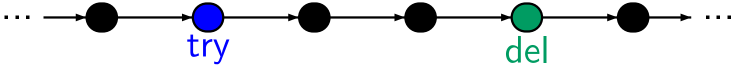
$$\Box\,(\text{try\_to\_send} \longrightarrow \bigcirc\ \text{delivered})$$



$$\Box\,(\text{try\_to\_send} \longrightarrow \text{try\_to\_send}\ \mathsf{U}\ \text{delivered})$$



$$\Box\,(\text{try\_to\_send} \longrightarrow \Diamond\ \text{delivered})$$



Examples for LTL formulas

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

eventually

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

always

$$\Box\varphi \overset{\text{def}}{=} \neg\Diamond\neg\varphi$$

Examples for LTL formulas

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

eventually

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

always

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

Examples for LTL formulas:

mutual exclusion: $\Box(\neg \mathit{crit}_1 \vee \neg \mathit{crit}_2)$

Examples for LTL formulas

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

eventually

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

always

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

Examples for LTL formulas:

mutual exclusion: $\Box(\neg \mathit{crit}_1 \vee \neg \mathit{crit}_2)$

railroad-crossing: $\Box(\mathit{train\_is\_near} \rightarrow \mathit{gate\_is\_closed})$

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

eventually

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

always

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

Examples for LTL formulas:

mutual exclusion: $\Box(\neg \mathit{crit}_1 \vee \neg \mathit{crit}_2)$

railroad-crossing: $\Box(\mathit{train\_is\_near} \rightarrow \mathit{gate\_is\_closed})$

progress property: $\Box(\mathit{request} \rightarrow \Diamond \mathit{response})$

Examples for LTL formulas

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

eventually

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

always

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

Examples for LTL formulas:

mutual exclusion: $\Box(\neg \textit{crit}_1 \vee \neg \textit{crit}_2)$

railroad-crossing: $\Box(\textit{train\_is\_near} \longrightarrow \textit{gate\_is\_closed})$

progress property: $\Box(\textit{request} \longrightarrow \Diamond \textit{response})$

traffic light: $\Box(\textit{yellow} \vee \bigcirc\neg \textit{red})$

Infinitely often and eventually forever

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

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

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

Infinitely often and eventually forever

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

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

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

infinitely often $\Box\Diamond\varphi$

Infinitely often and eventually forever

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

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

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

infinitely often $\Box\Diamond\varphi$

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

strong fairness $\Box\Diamond \textit{wait}_i \longrightarrow \Box\Diamond \textit{crit}_i$

Infinitely often and eventually forever

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

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-semantics

interpretation of **LTL** formulas over traces, i.e., infinite words over 2^{AP}

formalized by a satisfaction relation $\models$ for

- LTL formulas and
- infinite words $\sigma = A_0\, A_1\, A_2\, \ldots \in \left(2^{AP}\right)^{\omega}$

for $\sigma = A_0\, A_1\, A_2\, \ldots \in \left(2^{AP}\right)^{\omega}$:

Semantics of LTL over infinite words

for $\sigma = A_0 \, A_1 \, A_2 \, \ldots \in \left(2^{AP}\right)^{\omega}$:

$\sigma \models \mathit{true}$

Semantics of LTL over infinite words

for $\sigma = A_0\, A_1\, A_2 \ldots \in \left(2^{AP}\right)^{\omega}$:

$\sigma \models \mathit{true}$

$\sigma \models a$ iff $A_0 \models a$,i.e., $a \in A_0$

Semantics of LTL over infinite words

for $\sigma = A_0\, A_1\, A_2\, \ldots \in \left(2^{AP}\right)^{\omega}$:

$\sigma \models \mathit{true}$

$\sigma \models a$ iff $A_0 \models a$,i.e., $a \in A_0$

$\sigma \models \varphi_1 \wedge \varphi_2$ iff $\sigma \models \varphi_1$ and $\sigma \models \varphi_2$

Semantics of LTL over infinite words

for $\sigma = A_0\, A_1\, A_2\, \ldots \in \left(2^{AP}\right)^{\omega}$:

$$\sigma \models \mathit{true}$$

$$\sigma \models a \quad \text{iff} \quad A_0 \models a \text{ ,i.e., } a \in A_0$$

$$\sigma \models \varphi_1 \wedge \varphi_2 \quad \text{iff} \quad \sigma \models \varphi_1 \text{ and } \sigma \models \varphi_2$$

$$\sigma \models \neg\varphi \quad \text{iff} \quad \sigma \not\models \varphi$$

Semantics of LTL over infinite words

for $\sigma = A_0\, A_1\, A_2 \ldots \in \left(2^{AP}\right)^{\omega}$:

$\sigma \models \mathit{true}$		
$\sigma \models a$	iff	$A_0 \models a$,i.e., $a \in A_0$
$\sigma \models \varphi_1 \wedge \varphi_2$	iff	$\sigma \models \varphi_1$ and $\sigma \models \varphi_2$
$\sigma \models \neg\varphi$	iff	$\sigma \not\models \varphi$
$\sigma \models \bigcirc\varphi$	iff	$\mathit{suffix}(\sigma, 1) = A_1\, A_2\, A_3 \ldots \models \varphi$

Semantics of LTL over infinite words

for $\sigma = A_0\, A_1\, A_2 \ldots \in \left(2^{AP}\right)^{\omega}$:

$\sigma \models \mathit{true}$		
$\sigma \models a$	iff	$A_0 \models a$,i.e., $a \in A_0$
$\sigma \models \varphi_1 \wedge \varphi_2$	iff	$\sigma \models \varphi_1$ and $\sigma \models \varphi_2$
$\sigma \models \neg\varphi$	iff	$\sigma \not\models \varphi$
$\sigma \models \bigcirc\varphi$	iff	$\mathit{suffix}(\sigma, 1) = A_1\, A_2\, A_3 \ldots \models \varphi$
$\sigma \models \varphi_1 \mathsf{U}\, \varphi_2$	iff	there exists $j \geq 0$ such that

$\mathit{suffix}(\sigma, j) = A_j\, A_{j+1}\, A_{j+2} \ldots \models \varphi_2$ and

$\mathit{suffix}(\sigma, i) = A_i\, A_{i+1}\, A_{i+2} \ldots \models \varphi_1$ for $0 \leq i < j$

LT property of LTL formulas

LT property of LTL formulas

interpretation of **LTL** formulas over traces, i.e., infinite words over 2^{AP}

formalized by a satisfaction relation $\models$ for

- LTL formulas and
- infinite words $\sigma = A_0\, A_1\, A_2\, \ldots \in \left(2^{AP}\right)^{\omega}$

LT property of LTL formulas

interpretation of **LTL** formulas over traces, i.e.,
infinite words over 2^{AP}

formalized by a satisfaction relation $\models$ for

- LTL formulas and
- infinite words $\sigma = A_0\, A_1\, A_2\, \ldots \in \left(2^{AP}\right)^{\omega}$

LT property of formula φ:

$$Words(\varphi) \stackrel{\text{def}}{=} \left\{ \sigma \in \left(2^{AP}\right)^{\omega} : \sigma \models \varphi \right\}$$

LTL-semantics of derived operators $\Diamond$ and $\Box$

for $\sigma = A_0\, A_1\, A_2 \ldots \in \left(2^{AP}\right)^\omega$:

$$\vdots$$

$\sigma \models \varphi_1 \, \mathsf{U} \, \varphi_2$ iff there exists $j \geq 0$ such that

$A_j\, A_{j+1}\, A_{j+2} \ldots \models \varphi_2$ and

$A_i\, A_{i+1}\, A_{i+2} \ldots \models \varphi_1$ for $0 \leq i < j$

LTL-semantics of derived operators $\Diamond$ and $\Box$

for $\sigma = A_0\, A_1\, A_2\, \ldots \in \left(2^{AP}\right)^{\omega}$:

$$\vdots$$

$$
\begin{array}{lll}
\sigma \models \varphi_1 \,\mathsf{U}\, \varphi_2 & \text{iff} & \text{there exists } j \geq 0 \text{ such that} \\
 & & A_j\, A_{j+1}\, A_{j+2}\, \ldots \models \varphi_2 \quad \text{and} \\
 & & A_i\, A_{i+1}\, A_{i+2}\, \ldots \models \varphi_1 \quad \text{for } 0 \leq i < j \\
\sigma \models \Diamond \varphi & \text{iff} & \text{there exists } j \geq 0 \text{ such that} \\
 & & A_j\, A_{j+1}\, A_{j+2}\, \ldots \models \varphi
\end{array}
$$

LTL-semantics of derived operators $\Diamond$ and $\Box$

for $\sigma = A_0\, A_1\, A_2\, \ldots \in \left(2^{AP}\right)^{\omega}$:

$$
\begin{array}{lll}
 & \vdots & \\
\sigma \models \varphi_1 \,\mathsf{U}\, \varphi_2 & \text{iff} & \text{there exists } j \geq 0 \text{ such that} \\
 & & \quad A_j\, A_{j+1}\, A_{j+2}\, \ldots \models \varphi_2 \quad \text{and} \\
 & & \quad A_i\, A_{i+1}\, A_{i+2}\, \ldots \models \varphi_1 \quad \text{for } 0 \leq i < j \\
\sigma \models \Diamond\varphi & \text{iff} & \text{there exists } j \geq 0 \text{ such that} \\
 & & \quad A_j\, A_{j+1}\, A_{j+2}\, \ldots \models \varphi \\
\sigma \models \Box\varphi & \text{iff} & \text{for all } j \geq 0 \text{ we have:} \\
 & & \quad A_j\, A_{j+1}\, A_{j+2}\, \ldots \models \varphi
\end{array}
$$

LTL semantics over TS

given a TS $\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$

define satisfaction relation $\models$ for

- **LTL** formulas over AP
- the maximal path fragments and states of $\mathcal{T}$

assumption: $\mathcal{T}$ has no terminal states, i.e., all maximal path fragments in $\mathcal{T}$ are infinite

LTL semantics over paths of TS

LTL semantics over paths of TS

given: TS $\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$
without terminal states

LTL formula φ over AP

LTL semantics over paths of TS

given: TS $\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$
without terminal states
LTL formula φ over AP

interpretation of φ over infinite path fragments

$$\pi = s_0\, s_1\, s_2 \ldots \models \varphi \quad \text{iff} \quad trace(\pi) \models \varphi$$

LTL semantics over paths of TS

given: TS $\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$
without terminal states
LTL formula φ over AP

interpretation of φ over infinite path fragments

$$\boxed{\begin{array}{lll} \pi = s_0\, s_1\, s_2 \ldots \models \varphi & \text{iff} & trace(\pi) \models \varphi \\ & \text{iff} & trace(\pi) \in Words(\varphi) \end{array}}$$

LTL semantics over paths of TS

given: TS $\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$
without terminal states
LTL formula φ over AP

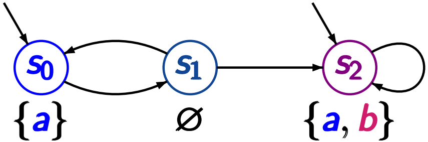
interpretation of φ over infinite path fragments

$$\pi = s_0\, s_1\, s_2 \ldots \models \varphi \quad \text{iff} \quad trace(\pi) \models \varphi$$
$$\text{iff} \quad trace(\pi) \in Words(\varphi)$$

remind: LT property of an LTL formula:

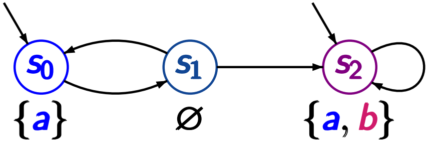
$$Words(\varphi) = \left\{ \sigma \in \left(2^{AP}\right)^{\omega} : \sigma \models \varphi \right\}$$

Example: LTL-semantics over paths



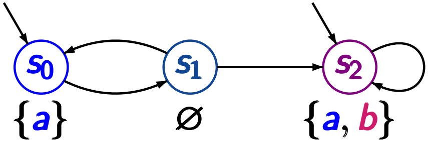
$AP = \{a, b\}$

Example: LTL-semantics over paths



$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_2\, s_2\, s_2\, s_2 \ldots$

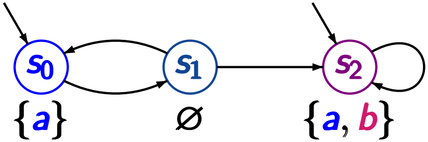


$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_2\, s_2\, s_2\, s_2 \ldots$ $\quad$ $trace(\pi) = \{a\}\, \varnothing\, \{a, b\}^\omega$

$\pi \models a$

Example: LTL-semantics over paths

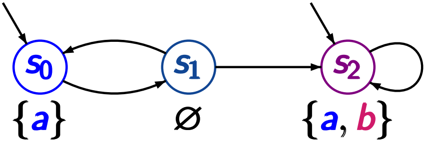


$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_2\, s_2\, s_2\, s_2 \ldots$ $\quad$ $trace(\pi) = \{a\}\, \varnothing\, \{a, b\}^\omega$

$\pi \models a$, but $\pi \not\models b$ $\qquad$ as $L(s_0) = \{a\}$

Example: LTL-semantics over paths



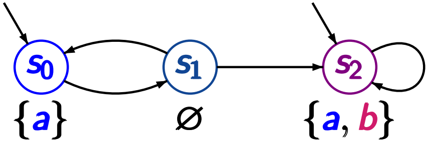
$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_2\, s_2\, s_2\, s_2 \ldots$ $\quad$ $\mathit{trace}(\pi) = \{a\}\, \varnothing\, \{a, b\}^\omega$

$\pi \models a$, but $\pi \not\models b$ $\quad$ as $L(s_0) = \{a\}$

$\pi \models \bigcirc(\neg a \wedge \neg b)$

Example: LTL-semantics over paths



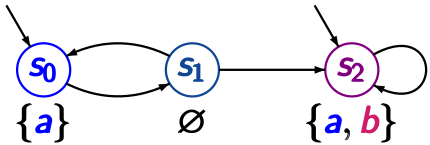
$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_2\, s_2\, s_2\, s_2 \ldots$ $\quad$ $\mathit{trace}(\pi) = \{a\}\,\varnothing\,\{a, b\}^\omega$

$\pi \models a$, but $\pi \not\models b$ $\quad$ as $L(s_0) = \{a\}$

$\pi \models \bigcirc(\neg a \wedge \neg b)$ $\quad$ as $L(s_1) = \varnothing$

Example: LTL-semantics over paths



$AP = \{a, b\}$

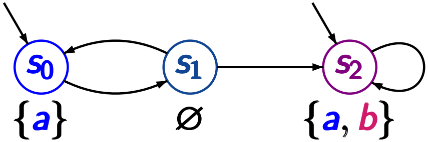
path $\pi = s_0\, s_1\, s_2\, s_2\, s_2\, s_2 \ldots$ $\quad$ $trace(\pi) = \{a\}\, \varnothing\, \{a, b\}^\omega$

$\pi \models a$, but $\pi \not\models b$ $\quad$ as $L(s_0) = \{a\}$

$\pi \models \bigcirc(\neg a \wedge \neg b)$ $\quad$ as $L(s_1) = \varnothing$

$\pi \models \bigcirc\bigcirc(a \wedge b)$

Example: LTL-semantics over paths



$AP = \{a, b\}$

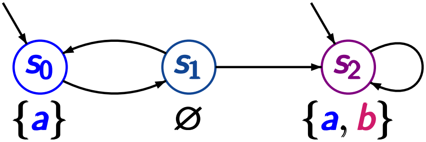
path $\pi = s_0\, s_1\, s_2\, s_2\, s_2\, s_2 \ldots$ $\qquad$ $trace(\pi) = \{a\}\, \varnothing\, \{a, b\}^{\omega}$

$\pi \models a$, but $\pi \not\models b$ $\qquad$ as $L(s_0) = \{a\}$

$\pi \models \bigcirc(\neg a \wedge \neg b)$ $\qquad$ as $L(s_1) = \varnothing$

$\pi \models \bigcirc \bigcirc (a \wedge b)$ $\qquad$ as $L(s_2) = \{a, b\}$

Example: LTL-semantics over paths



$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_2\, s_2\, s_2\, s_2 \ldots$ $\qquad$ $trace(\pi) = \{a\}\, \varnothing\, \{a, b\}^\omega$

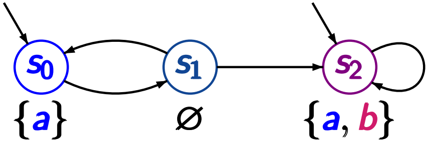
$\pi \models a$, but $\pi \not\models b$ $\qquad$ as $L(s_0) = \{a\}$

$\pi \models \bigcirc(\neg a \wedge \neg b)$ $\qquad$ as $L(s_1) = \varnothing$

$\pi \models \bigcirc\bigcirc(a \wedge b)$ $\qquad$ as $L(s_2) = \{a, b\}$

$\pi \models (\neg b) \,\mathsf{U}\, (a \wedge b)$

Example: LTL-semantics over paths

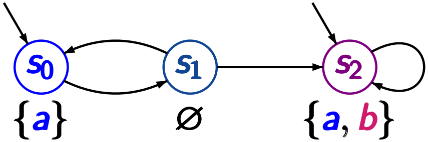


$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_2\, s_2\, s_2\, s_2 \ldots$ $\quad$ $trace(\pi) = \{a\}\, \varnothing\, \{a, b\}^\omega$

$\pi \models a$, but $\pi \not\models b$	as $L(s_0) = \{a\}$
$\pi \models \bigcirc(\neg a \wedge \neg b)$	as $L(s_1) = \varnothing$
$\pi \models \bigcirc\bigcirc(a \wedge b)$	as $L(s_2) = \{a, b\}$
$\pi \models (\neg b)\, \mathsf{U}\, (a \wedge b)$	as $s_0, s_1 \models \neg b$
	and $s_2 \models a \wedge b$

Example: LTL-semantics over paths

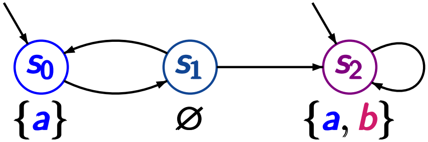


$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_2\, s_2\, s_2\, s_2 \ldots$ $\qquad$ $trace(\pi) = \{a\}\, \varnothing\, \{a, b\}^\omega$

$\pi \models a$, but $\pi \not\models b$	as $L(s_0) = \{a\}$
$\pi \models \bigcirc(\neg a \wedge \neg b)$	as $L(s_1) = \varnothing$
$\pi \models \bigcirc\bigcirc(a \wedge b)$	as $L(s_2) = \{a, b\}$
$\pi \models (\neg b)\, \mathsf{U}\, (a \wedge b)$	as $s_0, s_1 \models \neg b$
$\pi \models (\neg b)\, \mathsf{U}\, \Box(a \wedge b)$	and $s_2 \models a \wedge b$

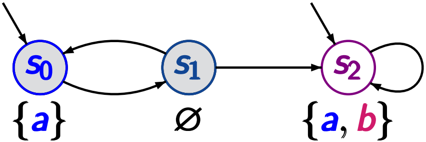
Correct or wrong ?



$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_0\, s_1\, s_0\, s_1\, \ldots$

Correct or wrong ?

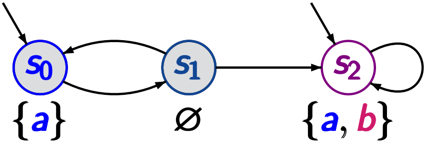


$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_0\, s_1\, s_0\, s_1 \ldots$

$trace(\pi) = (\{a\}\, \varnothing)^\omega$

Correct or wrong ?



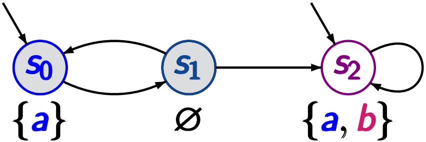
$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_0\, s_1\, s_0\, s_1 \ldots$

$trace(\pi) = (\{a\}\, \varnothing)^\omega$

$\pi \models a \,\mathsf{U}\, b$?

Correct or wrong ?

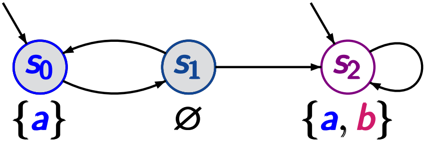


$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_0\, s_1\, s_0\, s_1 \ldots$ $\qquad$ $\mathit{trace}(\pi) = (\{a\}\,\varnothing)^\omega$

$\pi \not\models a \,\mathsf{U}\, b$ $\qquad$ as $s_0 \not\models b$ and $s_1 \not\models a \vee b$

Correct or wrong ?



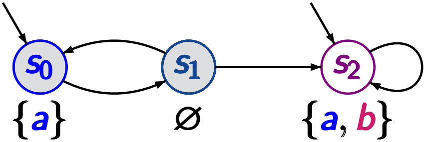
$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_0\, s_1\, s_0\, s_1\, \ldots$ $\qquad$ $\mathit{trace}(\pi) = (\{a\}\,\varnothing)^\omega$

$\pi \not\models a \,\mathsf{U}\, b$ $\qquad$ as $s_0 \not\models b$ and $s_1 \not\models a \vee b$

$\pi \models \Diamond b \rightarrow (a \,\mathsf{U}\, b)$?

Correct or wrong ?



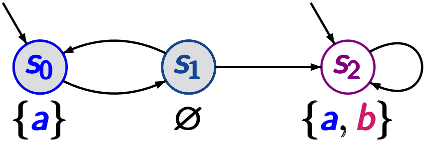
$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_0\, s_1\, s_0\, s_1 \ldots$ $\qquad$ $\mathit{trace}(\pi) = (\{a\}\, \varnothing)^\omega$

$\pi \not\models a \,\mathsf{U}\, b$ $\qquad$ as $s_0 \not\models b$ and $s_1 \not\models a \vee b$

$\pi \models \Diamond b \rightarrow (a \,\mathsf{U}\, b)$ $\qquad$ as $\pi \not\models \Diamond b$

Correct or wrong ?



$$AP = \{a, b\}$$

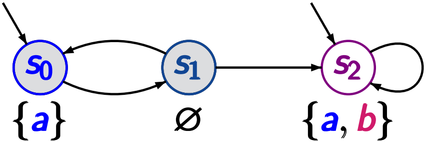
path $\pi = s_0\, s_1\, s_0\, s_1\, s_0\, s_1 \ldots$ $\qquad$ $trace(\pi) = (\{a\}\, \varnothing)^\omega$

$\pi \not\models a \,\mathsf{U}\, b$ $\qquad$ as $s_0 \not\models b$ and $s_1 \not\models a \vee b$

$\pi \models \Diamond b \rightarrow (a \,\mathsf{U}\, b)$ $\qquad$ as $\pi \not\models \Diamond b$

$\pi \models \bigcirc \bigcirc \neg b$?

Correct or wrong ?



$AP = \{a, b\}$

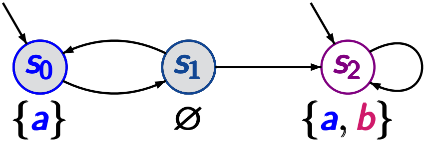
path $\pi = s_0\, s_1\, s_0\, s_1\, s_0\, s_1\, \ldots$ $\qquad$ $trace(\pi) = (\{a\}\, \varnothing)^\omega$

$\pi \not\models a \,\mathsf{U}\, b$ $\qquad$ as $s_0 \not\models b$ and $s_1 \not\models a \vee b$

$\pi \models \Diamond b \rightarrow (a \,\mathsf{U}\, b)$ $\qquad$ as $\pi \not\models \Diamond b$

$\pi \models \bigcirc \bigcirc \neg b$ $\qquad$ as $s_0 \models \neg b$

Correct or wrong ?



$AP = \{a, b\}$

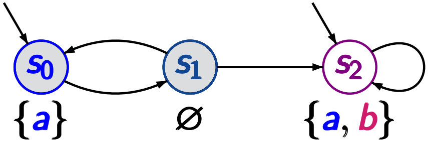
path $\pi = s_0\, s_1\, s_0\, s_1\, s_0\, s_1 \ldots$ $\qquad trace(\pi) = (\{a\}\, \varnothing)^\omega$

$\pi \not\models a \,\mathsf{U}\, b$ $\qquad$ as $s_0 \not\models b$ and $s_1 \not\models a \vee b$

$\pi \models \Diamond b \rightarrow (a \,\mathsf{U}\, b)$ $\qquad$ as $\pi \not\models \Diamond b$

$\pi \models \bigcirc \bigcirc \neg b$ $\qquad$ as $s_0 \models \neg b$

$\pi \models \Box a$?



$AP = \{a, b\}$

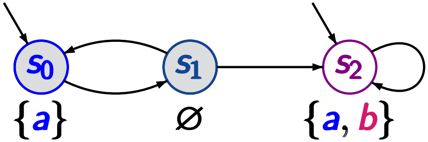
path $\pi = s_0\, s_1\, s_0\, s_1\, s_0\, s_1 \ldots$ $\qquad$ $trace(\pi) = (\{a\}\,\varnothing)^\omega$

$\pi \not\models a \,\mathsf{U}\, b$ $\qquad$ as $s_0 \not\models b$ and $s_1 \not\models a \vee b$

$\pi \models \Diamond b \rightarrow (a \,\mathsf{U}\, b)$ $\qquad$ as $\pi \not\models \Diamond b$

$\pi \models \bigcirc \bigcirc \neg b$ $\qquad$ as $s_0 \models \neg b$

$\pi \not\models \Box a$ $\qquad$ as $s_1 \not\models a$



$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_0\, s_1\, s_0\, s_1 \ldots$ $\qquad$ $trace(\pi) = (\{a\}\, \varnothing)^\omega$

$\pi \not\models a \,\mathsf{U}\, b$ $\qquad$ as $s_0 \not\models b$ and $s_1 \not\models a \vee b$

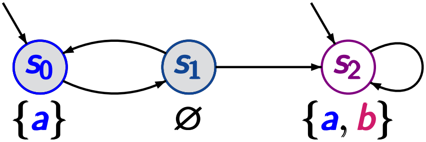
$\pi \models \lozenge b \to (a \,\mathsf{U}\, b)$ $\qquad$ as $\pi \not\models \lozenge b$

$\pi \models \bigcirc \bigcirc \neg b$ $\qquad$ as $s_0 \models \neg b$

$\pi \not\models \square a$ $\qquad$ as $s_1 \not\models a$

$\pi \models \square\lozenge a$?

Correct or wrong ?



$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_0\, s_1\, s_0\, s_1 \ldots$ $\qquad$ $trace(\pi) = (\{a\}\,\varnothing)^\omega$

$\pi \not\models a \,\mathsf{U}\, b$ $\qquad$ as $s_0 \not\models b$ and $s_1 \not\models a \vee b$

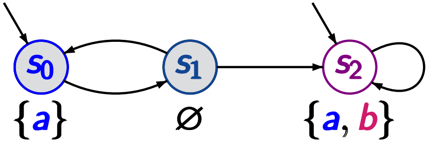
$\pi \models \Diamond b \rightarrow (a \,\mathsf{U}\, b)$ $\qquad$ as $\pi \not\models \Diamond b$

$\pi \models \bigcirc \bigcirc \neg b$ $\qquad$ as $s_0 \models \neg b$

$\pi \not\models \Box a$ $\qquad$ as $s_1 \not\models a$

$\pi \models \Box\Diamond a$ $\qquad$ as $\Box\Diamond \mathrel{\widehat{=}}$ infinitely often

Correct or wrong ?



$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_0\, s_1\, s_0\, s_1 \ldots$ $\qquad$ $trace(\pi) = (\{a\}\, \varnothing)^\omega$

$\pi \not\models a \,\mathsf{U}\, b$ $\qquad$ as $s_0 \not\models b$ and $s_1 \not\models a \vee b$

$\pi \models \Diamond b \rightarrow (a \,\mathsf{U}\, b)$ $\qquad$ as $\pi \not\models \Diamond b$

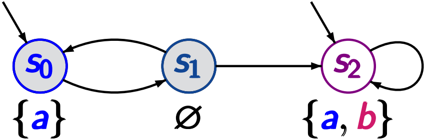
$\pi \models \bigcirc \bigcirc \neg b$ $\qquad$ as $s_0 \models \neg b$

$\pi \not\models \Box a$ $\qquad$ as $s_1 \not\models a$

$\pi \models \Box\Diamond a$ $\qquad$ as $\Box\Diamond \mathrel{\widehat{=}}$ infinitely often

$\pi \models \Diamond\Box a$?

Correct or wrong ?



$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_0\, s_1\, s_0\, s_1 \ldots$ $\qquad$ $\mathit{trace}(\pi) = (\{a\}\,\varnothing)^\omega$

$\pi \not\models a \,\mathsf{U}\, b$ $\qquad$ as $s_0 \not\models b$ and $s_1 \not\models a \vee b$

$\pi \models \Diamond b \rightarrow (a \,\mathsf{U}\, b)$ $\qquad$ as $\pi \not\models \Diamond b$

$\pi \models \bigcirc \bigcirc \neg b$ $\qquad$ as $s_0 \models \neg b$

$\pi \not\models \Box a$ $\qquad$ as $s_1 \not\models a$

$\pi \models \Box\Diamond a$ $\qquad$ as $\Box\Diamond \mathrel{\widehat{=}}$ infinitely often

$\pi \not\models \Diamond\Box a$ $\qquad$ as $\Diamond\Box \mathrel{\widehat{=}}$ eventually forever

LTL-semantics of derived operators

for $\sigma = A_0\, A_1\, A_2\, \ldots \in \left(2^{AP}\right)^{\omega}$:

LTL-semantics of derived operators

for $\sigma = A_0\, A_1\, A_2 \ldots \in \left(2^{AP}\right)^{\omega}$:

$\sigma \models \Diamond\varphi$	iff	there exists $j \geq 0$ such that $A_j\, A_{j+1}\, A_{j+2} \ldots \models \varphi$
$\sigma \models \Box\varphi$	iff	for all $j \geq 0$ we have: $A_j\, A_{j+1}\, A_{j+2} \ldots \models \varphi$

LTL-semantics of derived operators

for $\sigma = A_0\, A_1\, A_2 \ldots \in \left(2^{AP}\right)^{\omega}$:

$\sigma \models \Diamond\varphi$	iff	there exists $j \geq 0$ such that $A_j\, A_{j+1}\, A_{j+2} \ldots \models \varphi$
$\sigma \models \Box\varphi$	iff	for all $j \geq 0$ we have: $A_j\, A_{j+1}\, A_{j+2} \ldots \models \varphi$
$\sigma \models \Box\Diamond\varphi$	iff	there are infinitely many $j \geq 0$ s.t. $A_j\, A_{j+1}\, A_{j+2} \ldots \models \varphi$

LTL-semantics of derived operators

for $\sigma = A_0\, A_1\, A_2 \ldots \in \left(2^{AP}\right)^{\omega}$:

$\sigma \models \Diamond \varphi$	iff	there exists $j \geq 0$ such that $A_j\, A_{j+1}\, A_{j+2} \ldots \models \varphi$
$\sigma \models \Box \varphi$	iff	for all $j \geq 0$ we have: $A_j\, A_{j+1}\, A_{j+2} \ldots \models \varphi$
$\sigma \models \Box\Diamond \varphi$	iff	there are infinitely many $j \geq 0$ s.t. $A_j\, A_{j+1}\, A_{j+2} \ldots \models \varphi$
$\sigma \models \Diamond\Box \varphi$	iff	for almost all $j \geq 0$ we have: $A_j\, A_{j+1}\, A_{j+2} \ldots \models \varphi$

LTL semantics over the states of a TS

LTLSF3.1-SEM-STATES

LTL semantics over the states of a TS

given: TS $\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$
without terminal states

LTL formula φ over AP

interpretation of φ over infinite path fragments

$$\pi = s_0\, s_1\, s_2 \ldots \models \varphi \quad \text{iff} \quad trace(\pi) \models \varphi$$

interpretation of φ over states:

$$\boxed{s \models \varphi \quad \text{iff} \quad trace(\pi) \models \varphi \text{ for all } \pi \in Paths(s)}$$

LTL semantics over the states of a TS

given: TS $\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$
without terminal states

LTL formula φ over AP

interpretation of φ over infinite path fragments

$$\pi = s_0\, s_1\, s_2 \ldots \models \varphi \quad \text{iff} \quad trace(\pi) \models \varphi$$

interpretation of φ over states:

$$s \models \varphi \quad \text{iff} \quad trace(\pi) \models \varphi \text{ for all } \pi \in Paths(s)$$
$$\text{iff} \quad s \models Words(\varphi)$$

LTL semantics over the states of a TS

given: TS $\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$
without terminal states

LTL formula φ over AP

interpretation of φ over infinite path fragments

$$\pi = s_0\, s_1\, s_2 \ldots \models \varphi \quad \text{iff} \quad trace(\pi) \models \varphi$$

interpretation of φ over states:

$$\begin{aligned} s \models \varphi \quad & \text{iff} \quad trace(\pi) \models \varphi \text{ for all } \pi \in Paths(s) \\ & \text{iff} \quad s \models Words(\varphi) \end{aligned}$$

satisfaction relation for LT properties

LTL semantics over the states of a TS

given: TS $\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$
without terminal states

LTL formula φ over AP

interpretation of φ over infinite path fragments

$$\pi = s_0\, s_1\, s_2 \ldots \models \varphi \quad \text{iff} \quad trace(\pi) \models \varphi$$

interpretation of φ over states:

$$\begin{aligned} s \models \varphi \quad & \text{iff} \quad trace(\pi) \models \varphi \text{ for all } \pi \in Paths(s) \\ & \text{iff} \quad s \models Words(\varphi) \\ & \text{iff} \quad Traces(s) \subseteq Words(\varphi) \end{aligned}$$

Interpretation of LTL formulas over TS

Interpretation of LTL formulas over TS

given: TS $\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$
without terminal states

LTL formula φ over AP

$\mathcal{T} \models \varphi$ iff $s_0 \models \varphi$ for all $s_0 \in S_0$

Interpretation of LTL formulas over TS

given: TS $\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$
without terminal states

LTL formula φ over AP

$\mathcal{T} \models \varphi$ iff $s_0 \models \varphi$ for all $s_0 \in S_0$

iff $trace(\pi) \models \varphi$ for all $\pi \in Paths(\mathcal{T})$

Interpretation of LTL formulas over TS

given: TS $\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$
without terminal states

LTL formula φ over AP

$$\begin{aligned}
\mathcal{T} \models \varphi \quad & \text{iff} \quad s_0 \models \varphi \text{ for all } s_0 \in S_0 \\
& \text{iff} \quad trace(\pi) \models \varphi \text{ for all } \pi \in Paths(\mathcal{T}) \\
& \text{iff} \quad Traces(\mathcal{T}) \subseteq Words(\varphi)
\end{aligned}$$

Interpretation of LTL formulas over TS

given: TS $\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$
without terminal states

LTL formula φ over AP

$$
\begin{aligned}
\mathcal{T} \models \varphi \quad & \text{iff} \quad s_0 \models \varphi \text{ for all } s_0 \in S_0 \\
& \text{iff} \quad trace(\pi) \models \varphi \text{ for all } \pi \in Paths(\mathcal{T}) \\
& \text{iff} \quad Traces(\mathcal{T}) \subseteq Words(\varphi) \\
& \text{iff} \quad \mathcal{T} \models Words(\varphi)
\end{aligned}
$$

Interpretation of LTL formulas over TS

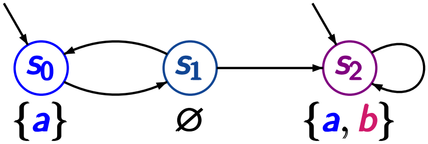
given: TS $\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$
without terminal states

LTL formula φ over AP

$$
\begin{array}{lll}
\mathcal{T} \models \varphi & \text{iff} & s_0 \models \varphi \text{ for all } s_0 \in S_0 \\
& \text{iff} & trace(\pi) \models \varphi \text{ for all } \pi \in Paths(\mathcal{T}) \\
& \text{iff} & Traces(\mathcal{T}) \subseteq Words(\varphi) \\
& \text{iff} & \mathcal{T} \models Words(\varphi)
\end{array}
$$

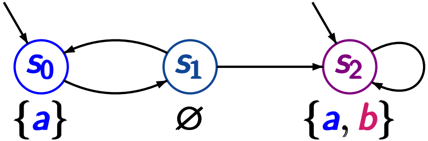
satisfaction relation for LT properties

Which formulas hold for $\mathcal{T}$?



$$AP = \{a, b\}$$

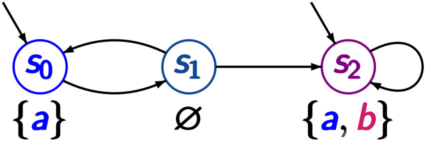
Which formulas hold for $\mathcal{T}$?



$AP = \{a, b\}$

$\mathcal{T} \models a$

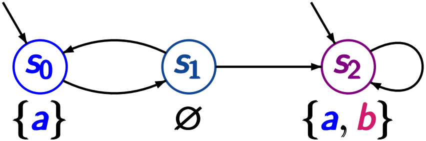
Which formulas hold for $\mathcal{T}$?



$AP = \{a, b\}$

$\mathcal{T} \models a$ as $s_0 \models a$ and $s_2 \models a$

Which formulas hold for $\mathcal{T}$?

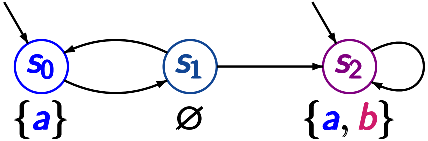


$AP = \{a, b\}$

$\mathcal{T} \models a$ as $s_0 \models a$ and $s_2 \models a$

$\mathcal{T} \models \Diamond\Box a$

Which formulas hold for $\mathcal{T}$?

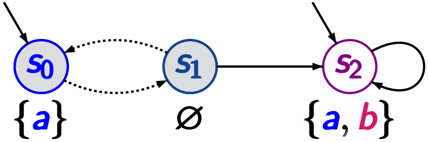


$AP = \{a, b\}$

$\mathcal{T} \models a$ as $s_0 \models a$ and $s_2 \models a$

$\mathcal{T} \not\models \Diamond\Box a$

Which formulas hold for $\mathcal{T}$?

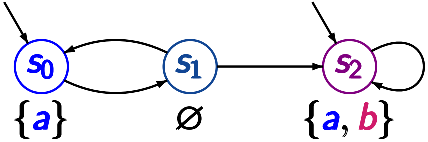


$AP = \{a, b\}$

$\mathcal{T} \models a$ as $s_0 \models a$ and $s_2 \models a$

$\mathcal{T} \not\models \Diamond\Box a$ as $s_0\, s_1\, s_0\, s_1 \ldots \not\models \Diamond\Box a$

Which formulas hold for $\mathcal{T}$?



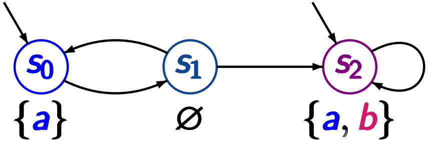
$AP = \{a, b\}$

$\mathcal{T} \models a$ as $s_0 \models a$ and $s_2 \models a$

$\mathcal{T} \not\models \Diamond\Box a$ as $s_0\, s_1\, s_0\, s_1 \ldots \not\models \Diamond\Box a$

$\mathcal{T} \models \Diamond\Box b \;\vee\; \Box\Diamond(\neg a \wedge \neg b)$

Which formulas hold for $\mathcal{T}$?



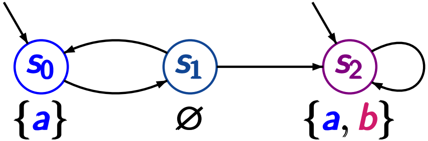
$AP = \{a, b\}$

$\mathcal{T} \models a$ as $s_0 \models a$ and $s_2 \models a$

$\mathcal{T} \not\models \Diamond\Box a$ as $s_0\, s_1\, s_0\, s_1 \ldots \not\models \Diamond\Box a$

$\mathcal{T} \models \Diamond\Box b \lor \Box\Diamond(\neg a \land \neg b)$ as $s_2 \models b$, $s_1 \not\models a, b$

Which formulas hold for $\mathcal{T}$?



$$AP = \{a, b\}$$

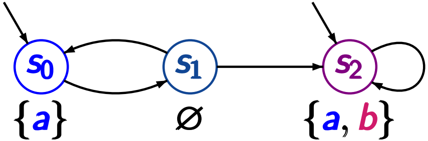
$\mathcal{T} \models a$ as $s_0 \models a$ and $s_2 \models a$

$\mathcal{T} \not\models \Diamond\Box a$ as $s_0\, s_1\, s_0\, s_1 \ldots \not\models \Diamond\Box a$

$\mathcal{T} \models \Diamond\Box b \vee \Box\Diamond(\neg a \wedge \neg b)$ as $s_2 \models b$, $s_1 \not\models a, b$

$\mathcal{T} \models \Box(a \rightarrow (\bigcirc\neg a \vee b))$

Which formulas hold for $\mathcal{T}$?



$AP = \{a, b\}$

$\mathcal{T} \models a$	as $s_0 \models a$ and $s_2 \models a$
$\mathcal{T} \not\models \Diamond\Box a$	as $s_0\, s_1\, s_0\, s_1 \ldots \not\models \Diamond\Box a$
$\mathcal{T} \models \Diamond\Box b \vee \Box\Diamond(\neg a \wedge \neg b)$	as $s_2 \models b$, $s_1 \not\models a, b$
$\mathcal{T} \models \Box(a \rightarrow (\bigcirc\neg a \vee b))$	as $s_2 \models b$, $s_0 \models \bigcirc\neg a$

Correct or wrong?

For each path π we have: $\pi \models \varphi$ or $\pi \models \neg\varphi$

Correct or wrong?

For each path π we have: $\pi \models \varphi$ or $\pi \models \neg\varphi$

correct, since $\pi \models \neg\varphi$ iff $\pi \not\models \varphi$

Correct or wrong?

For each path π we have: $\pi \models \varphi$ or $\pi \models \neg\varphi$

correct, since $\pi \models \neg\varphi$ iff $\pi \not\models \varphi$

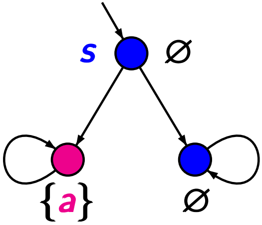
For each state s we have: $s \models \varphi$ or $s \models \neg\varphi$

For each path π we have: $\pi \models \varphi$ or $\pi \models \neg\varphi$

correct, since $\pi \models \neg\varphi$ iff $\pi \not\models \varphi$

For each state s we have: $s \models \varphi$ or $s \models \neg\varphi$

wrong.



$s \not\models \Diamond a$ and $s \not\models \neg\Diamond a$

LTL-formulas for MUTEX protocols

LTL-formulas for MUTEX protocols

LTL formulas over $AP = \{wait_1, crit_1, wait_2, crit_2\}$

- the mutual exclusion property

$$\varphi_{mutex} \;=\; ?$$

LTL-formulas for MUTEX protocols

LTL formulas over $AP = \{\mathsf{wait}_1, \mathsf{crit}_1, \mathsf{wait}_2, \mathsf{crit}_2\}$

- the mutual exclusion property

$$\varphi_{mutex} \;=\; \Box(\neg\mathsf{crit}_1 \vee \neg\mathsf{crit}_2)$$

LTL formulas over $AP = \{wait_1, crit_1, wait_2, crit_2\}$

- the mutual exclusion property

$$\varphi_{mutex} \;=\; \Box(\neg crit_1 \vee \neg crit_2)$$

- "every process enters the critical section infinitely often"

$$\varphi_{live} \;=\; ?$$

LTL-formulas for MUTEX protocols

LTL formulas over $AP = \{\mathsf{wait}_1, \mathsf{crit}_1, \mathsf{wait}_2, \mathsf{crit}_2\}$

- the mutual exclusion property

$$\varphi_{mutex} \;=\; \Box(\neg \mathsf{crit}_1 \vee \neg \mathsf{crit}_2)$$

- "every process enters the critical section infinitely often"

$$\varphi_{live} \;=\; \Box\Diamond \mathsf{crit}_1 \;\wedge\; \Box\Diamond \mathsf{crit}_2$$

LTL-formulas for MUTEX protocols

LTL formulas over $AP = \{\mathsf{wait}_1, \mathsf{crit}_1, \mathsf{wait}_2, \mathsf{crit}_2\}$

- the mutual exclusion property

$$\varphi_{mutex} \;=\; \Box(\neg \mathsf{crit}_1 \vee \neg \mathsf{crit}_2)$$

- "every process enters the critical section infinitely often"

$$\varphi_{live} \;=\; \Box\Diamond \mathsf{crit}_1 \;\wedge\; \Box\Diamond \mathsf{crit}_2$$

- starvation freedom
  "every waiting process finally enters its critical section"

$$\varphi_{sf} \;=\; ?$$

LTL-formulas for MUTEX protocols

LTL formulas over $AP = \{wait_1, crit_1, wait_2, crit_2\}$

- the mutual exclusion property

$$\varphi_{mutex} = \Box(\neg crit_1 \vee \neg crit_2)$$

- "every process enters the critical section infinitely often"

$$\varphi_{live} = \Box\Diamond crit_1 \wedge \Box\Diamond crit_2$$

- starvation freedom
  "every waiting process finally enters its critical section"

$$\varphi_{sf} = \Box(wait_1 \rightarrow \Diamond crit_1) \wedge \Box(wait_2 \rightarrow \Diamond crit_2)$$

Provide an LTL formula over $AP = \{a, b\}$ for ...

- set of all words $A_0 \, A_1 \, A_2 \, \ldots \in \left(2^{AP}\right)^{\omega}$ such that:

$$\forall i \geq 0. \left(\, a \in A_i \implies i \geq 1 \wedge b \in A_{i-1} \, \right)$$

Provide an LTL formula over $AP = \{a, b\}$ for ...

- set of all words $A_0\, A_1\, A_2 \ldots \in \left(2^{AP}\right)^{\omega}$ such that:

$$\forall i \geq 0.\ (\ a \in A_i \implies i \geq 1 \wedge b \in A_{i-1}\ )$$

$$\forall j \geq 0.\ (\ b \in A_j \ \vee\ a \notin A_{j+1})$$

Provide an LTL formula over $AP = \{a, b\}$ for ...

- set of all words $A_0\, A_1\, A_2 \ldots \in \left(2^{AP}\right)^{\omega}$ such that:

$$\forall i \geq 0.\ (\ a \in A_i \implies i \geq 1 \wedge b \in A_{i-1}\ )$$

$$\forall j \geq 0.\ (\ b \in A_j \vee a \notin A_{j+1})$$

$$\widehat{=}\ \ Words(\ \Box(b \vee \bigcirc \neg a)\ )$$

Provide an LTL formula over $AP = \{a, b\}$ for ...

- set of all words $A_0\, A_1\, A_2 \ldots \in \left(2^{AP}\right)^{\omega}$ such that:

$$\forall i \geq 0. \; (\; a \in A_i \implies i \geq 1 \wedge b \in A_{i-1} \;)$$

$$\forall j \geq 0. \; (\; b \in A_j \; \vee \; a \notin A_{j+1})$$

$$\widehat{=} \quad \mathit{Words}\big(\, \Box(b \vee \bigcirc\neg a) \,\big)$$

- set of all words of the form

$$\{b\}^{n_1}\,\{a\}\,\{b\}^{n_2}\,\{a\}\,\{b\}^{n_3}\,\{a\}\ldots$$

where $n_1, n_2, n_3, \ldots \geq 0$

Provide an LTL formula over $AP = \{a, b\}$ for ...

- set of all words $A_0\, A_1\, A_2 \ldots \in \left(2^{AP}\right)^\omega$ such that:

  $$\forall i \geq 0.\ (\ a \in A_i \implies i \geq 1 \land b \in A_{i-1}\ )$$

  $$\forall j \geq 0.\ (\ b \in A_j \ \lor\ a \notin A_{j+1})$$

  $$\widehat{=}\ \ \mathit{Words}\big(\ \Box(b \lor \bigcirc\neg a)\ \big)$$

- set of all words of the form

  $$\{b\}^{n_1}\,\{a\}\,\{b\}^{n_2}\,\{a\}\,\{b\}^{n_3}\,\{a\}\ldots$$

  where $n_1, n_2, n_3, \ldots \geq 0$

  $$\widehat{=}\ \ \mathit{Words}\big(\ \Box((b \land \neg a)\ \mathsf{U}\ (a \land \neg b))\ \big)$$

Equivalence of LTL formulas

$$\varphi_1 \equiv \varphi_2 \quad \text{iff} \quad Words(\varphi_1) = Words(\varphi_2)$$

Equivalence of LTL formulas

$$\varphi_1 \equiv \varphi_2 \quad \text{iff} \quad \mathit{Words}(\varphi_1) = \mathit{Words}(\varphi_2)$$

$$\text{iff} \quad \text{for all transition systems } \mathcal{T}:$$

$$\mathcal{T} \models \varphi_1 \iff \mathcal{T} \models \varphi_2$$

Equivalence of LTL formulas

$$\varphi_1 \equiv \varphi_2 \quad \text{iff} \quad \mathit{Words}(\varphi_1) = \mathit{Words}(\varphi_2)$$

iff for all transition systems $\mathcal{T}$:

$$\mathcal{T} \models \varphi_1 \iff \mathcal{T} \models \varphi_2$$

Examples:

$$\varphi_1 \vee \varphi_2 \equiv \varphi_2 \vee \varphi_1$$
$$\neg\neg\varphi \equiv \varphi$$
$$\vdots$$

all equivalences from propositional logic

Equivalence of LTL formulas

$$\varphi_1 \equiv \varphi_2 \quad \text{iff} \quad \mathit{Words}(\varphi_1) = \mathit{Words}(\varphi_2)$$

$$\text{iff} \quad \text{for all transition systems } \mathcal{T}\text{:}$$

$$\mathcal{T} \models \varphi_1 \iff \mathcal{T} \models \varphi_2$$

Examples:

$$\varphi_1 \vee \varphi_2 \equiv \varphi_2 \vee \varphi_1$$

$$\neg\neg\varphi \equiv \varphi$$

$$\vdots$$

$$\neg\bigcirc\varphi \equiv \bigcirc\neg\varphi$$

all equivalences from propositional logic

Self-duality of the next operator

$$\boxed{\varphi_1 \equiv \varphi_2 \quad \text{iff} \quad \mathit{Words}(\varphi_1) = \mathit{Words}(\varphi_2)}$$

Claim: $\neg \bigcirc \varphi \equiv \bigcirc \neg \varphi$ "self-duality of next"

Self-duality of the next operator

$$\boxed{\varphi_1 \equiv \varphi_2 \quad \text{iff} \quad \mathit{Words}(\varphi_1) = \mathit{Words}(\varphi_2)}$$

Claim: $\neg \bigcirc \varphi \equiv \bigcirc \neg \varphi$ "self-duality of next"

Proof: $A_0\, A_1\, A_2\, A_3 \ldots \models \neg \bigcirc \varphi$

$$\boxed{\varphi_1 \equiv \varphi_2 \quad \text{iff} \quad \mathit{Words}(\varphi_1) = \mathit{Words}(\varphi_2)}$$

Claim: $\neg\bigcirc\varphi \equiv \bigcirc\neg\varphi$ "self-duality of next"

Proof: $A_0\, A_1\, A_2\, A_3 \ldots \models \neg\bigcirc\varphi$

iff $A_0\, A_1\, A_2\, A_3 \ldots \not\models \bigcirc\varphi$

$$\boxed{\varphi_1 \equiv \varphi_2 \quad \text{iff} \quad \mathit{Words}(\varphi_1) = \mathit{Words}(\varphi_2)}$$

Claim: $\neg\bigcirc\varphi \equiv \bigcirc\neg\varphi$ "self-duality of next"

Proof:

$$
\begin{array}{lrcl}
 & A_0\,A_1\,A_2\,A_3\ldots & \models & \neg\bigcirc\varphi \\
\text{iff} & A_0\,A_1\,A_2\,A_3\ldots & \not\models & \bigcirc\varphi \\
\text{iff} & A_1\,A_2\,A_3\ldots & \not\models & \varphi
\end{array}
$$

Self-duality of the next operator

$$\boxed{\varphi_1 \equiv \varphi_2 \quad \text{iff} \quad \mathit{Words}(\varphi_1) = \mathit{Words}(\varphi_2)}$$

Claim: $\neg\bigcirc\varphi \equiv \bigcirc\neg\varphi$ "self-duality of next"

Proof:

$$\begin{array}{lrcl}
 & A_0\, A_1\, A_2\, A_3 \ldots & \models & \neg\bigcirc\varphi \\
\text{iff} & A_0\, A_1\, A_2\, A_3 \ldots & \not\models & \bigcirc\varphi \\
\text{iff} & A_1\, A_2\, A_3 \ldots & \not\models & \varphi \\
\text{iff} & A_1\, A_2\, A_3 \ldots & \models & \neg\varphi
\end{array}$$

$$\boxed{\varphi_1 \equiv \varphi_2 \quad \text{iff} \quad \mathit{Words}(\varphi_1) = \mathit{Words}(\varphi_2)}$$

Claim: $\neg\bigcirc\varphi \equiv \bigcirc\neg\varphi$ "self-duality of next"

Proof:

$$\begin{array}{lrcl}
 & A_0\,A_1\,A_2\,A_3\ldots & \models & \neg\bigcirc\varphi \\
\text{iff} & A_0\,A_1\,A_2\,A_3\ldots & \not\models & \bigcirc\varphi \\
\text{iff} & A_1\,A_2\,A_3\ldots & \not\models & \varphi \\
\text{iff} & A_1\,A_2\,A_3\ldots & \models & \neg\varphi \\
\text{iff} & A_0\,A_1\,A_2\,A_3\ldots & \models & \bigcirc\neg\varphi
\end{array}$$

Correct or wrong?

$$\Diamond(\varphi \vee \psi) \equiv \Diamond\varphi \vee \Diamond\psi$$

Correct or wrong?

$$\Diamond(\varphi \vee \psi) \;\equiv\; \Diamond\varphi \vee \Diamond\psi$$

correct

Correct or wrong?

$$\Diamond(\varphi \vee \psi) \equiv \Diamond\varphi \vee \Diamond\psi$$

correct

$$\Diamond(\varphi \wedge \psi) \equiv \Diamond\varphi \wedge \Diamond\psi$$

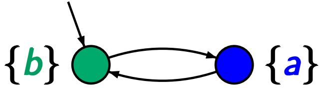
Correct or wrong?

$$\Diamond(\varphi \vee \psi) \;\equiv\; \Diamond\varphi \vee \Diamond\psi$$

correct

$$\Diamond(\varphi \wedge \psi) \;\equiv\; \Diamond\varphi \wedge \Diamond\psi$$

wrong,
e.g.,



$\models\ \Diamond b \wedge \Diamond a$

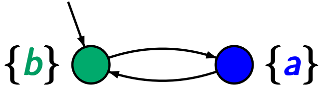
$\not\models\ \Diamond(b \wedge a)$

$$\Diamond(\varphi \vee \psi) \equiv \Diamond\varphi \vee \Diamond\psi$$

correct

$$\Diamond(\varphi \wedge \psi) \equiv \Diamond\varphi \wedge \Diamond\psi$$

wrong,
e.g.,



$\models \Diamond b \wedge \Diamond a$

$\not\models \Diamond(b \wedge a)$

---

similarly: $\Box(\varphi \wedge \psi) \equiv \Box\varphi \wedge \Box\psi$

$$\Box(\varphi \vee \psi) \not\equiv \Box\varphi \vee \Box\psi$$

Expansion laws

Expansion law for U

until: $\varphi \, \mathsf{U} \, \psi \;\equiv\; \psi \;\vee\; (\varphi \wedge \bigcirc(\varphi \, \mathsf{U} \, \psi))$

Expansion laws for U and $\Diamond$

until: $\varphi \,\mathsf{U}\, \psi \;\equiv\; \psi \;\vee\; (\varphi \wedge \bigcirc(\varphi \,\mathsf{U}\, \psi))$

eventually: $\Diamond\psi \;\equiv\; \psi \;\vee\; \bigcirc\Diamond\psi$

Expansion laws for U and $\Diamond$

until: $\varphi \mathsf{U} \psi \equiv \psi \vee (\varphi \wedge \bigcirc(\varphi \mathsf{U} \psi))$

eventually: $\Diamond\psi \equiv \psi \vee \bigcirc\Diamond\psi$

note: $\Diamond\psi = \textit{true}\, \mathsf{U}\, \psi$

Expansion laws for U and $\Diamond$

until: $\varphi \, \mathsf{U} \, \psi \;\equiv\; \psi \;\vee\; (\varphi \wedge \bigcirc(\varphi \, \mathsf{U} \, \psi))$

eventually: $\Diamond\psi \;\equiv\; \psi \;\vee\; \bigcirc\Diamond\psi$

note: $\Diamond\psi = \mathit{true} \, \mathsf{U} \, \psi$

$\equiv \psi \;\vee\; (\mathit{true} \;\wedge\; \bigcirc(\mathit{true} \, \mathsf{U} \, \psi))$

Expansion laws for U and $\Diamond$

until: $\varphi \,\mathsf{U}\, \psi \equiv \psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{U}\, \psi))$

eventually: $\Diamond\psi \equiv \psi \vee \bigcirc\Diamond\psi$

note: $\Diamond\psi = \mathit{true} \,\mathsf{U}\, \psi$

$$\equiv \psi \vee (\mathit{true} \wedge \bigcirc(\underbrace{\mathit{true} \,\mathsf{U}\, \psi}_{=\Diamond\psi}))$$

Expansion laws for U and $\Diamond$

until: $\varphi \,\mathsf{U}\, \psi \equiv \psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{U}\, \psi))$

eventually: $\Diamond\psi \equiv \psi \vee \bigcirc\Diamond\psi$

note:

$$\begin{aligned}\Diamond\psi &= \mathit{true} \,\mathsf{U}\, \psi \\ &\equiv \psi \vee (\mathit{true} \wedge \bigcirc(\underbrace{\mathit{true} \,\mathsf{U}\, \psi}_{=\Diamond\psi})) \\ &\equiv \psi \vee \bigcirc\Diamond\psi\end{aligned}$$

Expansion laws for U, $\Diamond$ and $\Box$

until: $\varphi \, \mathsf{U} \, \psi \equiv \psi \vee (\varphi \wedge \bigcirc(\varphi \, \mathsf{U} \, \psi))$

eventually: $\Diamond\psi \equiv \psi \vee \bigcirc\Diamond\psi$

always: $\Box\psi \equiv$ **?**

Expansion laws for U, $\Diamond$ and $\Box$

until: $\varphi \, \mathsf{U} \, \psi \equiv \psi \vee (\varphi \wedge \bigcirc(\varphi \, \mathsf{U} \, \psi))$

eventually: $\Diamond\psi \equiv \psi \vee \bigcirc\Diamond\psi$

always: $\Box\psi \equiv \psi \wedge \bigcirc\Box\psi$

Expansion laws for U, $\Diamond$ and $\Box$

until: $\varphi \, \mathsf{U} \, \psi \;\equiv\; \psi \;\vee\; (\varphi \wedge \bigcirc(\varphi \, \mathsf{U} \, \psi))$

eventually: $\Diamond\psi \;\equiv\; \psi \;\vee\; \bigcirc\Diamond\psi$

always: $\Box\psi \;\equiv\; \psi \;\wedge\; \bigcirc\Box\psi$

$\Box\psi \;=\; \neg\Diamond\neg\psi$

Expansion laws for U, $\Diamond$ and $\Box$

until: $\varphi \, \mathsf{U} \, \psi \equiv \psi \lor (\varphi \land \bigcirc(\varphi \, \mathsf{U} \, \psi))$

eventually: $\Diamond \psi \equiv \psi \lor \bigcirc \Diamond \psi$

always: $\Box \psi \equiv \psi \land \bigcirc \Box \psi$

$$\begin{aligned} \Box \psi &= \neg \Diamond \neg \psi \\ &\equiv \neg(\neg \psi \lor \bigcirc \Diamond \neg \psi) \longleftarrow \boxed{\text{expansion law for } \Diamond} \end{aligned}$$

Expansion laws for U, $\Diamond$ and $\Box$

until: $\varphi \mathbf{U} \psi \equiv \psi \vee (\varphi \wedge \bigcirc(\varphi \mathbf{U} \psi))$

eventually: $\Diamond\psi \equiv \psi \vee \bigcirc\Diamond\psi$

always: $\Box\psi \equiv \psi \wedge \bigcirc\Box\psi$

$$\begin{aligned}
\Box\psi &= \neg\Diamond\neg\psi \\
&\equiv \neg(\neg\psi \vee \bigcirc\Diamond\neg\psi) \\
&\equiv \neg\neg\psi \wedge \neg\bigcirc\Diamond\neg\psi \quad \longleftarrow \boxed{\text{de Morgan}}
\end{aligned}$$

Expansion laws for U, $\Diamond$ and $\Box$

until: $\varphi \,\mathsf{U}\, \psi \equiv \psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{U}\, \psi))$

eventually: $\Diamond\psi \equiv \psi \vee \bigcirc\Diamond\psi$

always: $\Box\psi \equiv \psi \wedge \bigcirc\Box\psi$

$$
\begin{aligned}
\Box\psi &= \neg\Diamond\neg\psi \\
&\equiv \neg(\neg\psi \vee \bigcirc\Diamond\neg\psi) \\
&\equiv \neg\neg\psi \wedge \neg\bigcirc\Diamond\neg\psi \\
&\equiv \psi \wedge \neg\bigcirc\Diamond\neg\psi \quad \longleftarrow \boxed{\text{double negation}}
\end{aligned}
$$

Expansion laws for U, $\Diamond$ and $\Box$

until: $\varphi \,\mathsf{U}\, \psi \equiv \psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{U}\, \psi))$

eventually: $\Diamond\psi \equiv \psi \vee \bigcirc\Diamond\psi$

always: $\Box\psi \equiv \psi \wedge \bigcirc\Box\psi$

$$
\begin{aligned}
\Box\psi &= \neg\Diamond\neg\psi \\
&\equiv \neg(\neg\psi \vee \bigcirc\Diamond\neg\psi) \\
&\equiv \neg\neg\psi \wedge \neg\bigcirc\Diamond\neg\psi \\
&\equiv \psi \wedge \bigcirc\neg\Diamond\neg\psi \quad \longleftarrow \boxed{\text{self duality of } \bigcirc}
\end{aligned}
$$

Expansion laws for U, $\Diamond$ and $\Box$

until: $\varphi \,\mathsf{U}\, \psi \equiv \psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{U}\, \psi))$

eventually: $\Diamond\psi \equiv \psi \vee \bigcirc\Diamond\psi$

always: $\Box\psi \equiv \psi \wedge \bigcirc\Box\psi$

$$
\begin{aligned}
\Box\psi &= \neg\Diamond\neg\psi \\
&\equiv \neg(\neg\psi \vee \bigcirc\Diamond\neg\psi) \\
&\equiv \neg\neg\psi \wedge \neg\bigcirc\Diamond\neg\psi \\
&\equiv \psi \wedge \bigcirc\neg\Diamond\neg\psi \\
&\equiv \psi \wedge \bigcirc\Box\psi \qquad \longleftarrow \boxed{\text{definition of } \Box}
\end{aligned}
$$

Expansion laws are fixed point equations

until: $\varphi \, \mathsf{U} \, \psi \equiv \psi \vee (\varphi \wedge \bigcirc(\varphi \, \mathsf{U} \, \psi))$

eventually: $\Diamond\psi \equiv \psi \vee \bigcirc\Diamond\psi$

always: $\Box\psi \equiv \psi \wedge \bigcirc\Box\psi$

Expansion laws are fixed point equations

until: $\boxed{\varphi \,\mathsf{U}\, \psi} \equiv \psi \vee (\varphi \wedge \bigcirc \boxed{\varphi \,\mathsf{U}\, \psi})$

eventually: $\boxed{\Diamond \psi} \equiv \psi \vee \bigcirc \boxed{\Diamond \psi}$

always: $\boxed{\Box \psi} \equiv \psi \wedge \bigcirc \boxed{\Box \psi}$

Expansion laws are fixed point equations

until: $\boxed{\varphi \mathsf{U} \psi} \equiv \psi \vee (\varphi \wedge \bigcirc \boxed{\varphi \mathsf{U} \psi})$

eventually: $\boxed{\Diamond \psi} \equiv \psi \vee \bigcirc \boxed{\Diamond \psi}$

always: $\boxed{\Box \psi} \equiv \psi \wedge \bigcirc \boxed{\Box \psi}$

...don't yield a complete characterization, e.g.,

$$\boxed{\begin{array}{lcl} \mathit{false} & \equiv & a \wedge \bigcirc \mathit{false} \\ \Box a & \equiv & a \wedge \bigcirc \Box a \end{array}}$$

consider $\psi = a$

Expansion laws are fixed point equations

until: $\boxed{\varphi \,\mathsf{U}\, \psi} \equiv \psi \vee (\varphi \wedge \bigcirc \boxed{\varphi \,\mathsf{U}\, \psi})$

eventually: $\boxed{\Diamond \psi} \equiv \psi \vee \bigcirc \boxed{\Diamond \psi}$

always: $\boxed{\Box \psi} \equiv \psi \wedge \bigcirc \boxed{\Box \psi}$

...don't yield a complete characterization, e.g.,

$$\boxed{\begin{array}{lcl} \mathit{false} & \equiv & a \wedge \bigcirc \mathit{false} \\ \Box a & \equiv & a \wedge \bigcirc \Box a \end{array}}$$

although

$\Box a \not\equiv \mathit{false}$

Expansion laws are fixed point equations

until: $\varphi \mathbf{U} \psi \equiv \psi \vee (\varphi \wedge \bigcirc(\varphi \mathbf{U} \psi))$

least fixed point

eventually: $\Diamond\psi \equiv \psi \vee \bigcirc\Diamond\psi$

least fixed point

always: $\Box\psi \equiv \psi \wedge \bigcirc\Box\psi$

...don't yield a complete characterization, e.g.,

$$\boxed{\begin{array}{lcl} \mathit{false} & \equiv & a \wedge \bigcirc \mathit{false} \\ \Box a & \equiv & a \wedge \bigcirc\Box a \end{array}}$$

although
$\Box a \not\equiv \mathit{false}$

Expansion laws are fixed point equations

until: $\varphi \, \mathsf{U} \, \psi \equiv \psi \vee (\varphi \wedge \bigcirc(\varphi \, \mathsf{U} \, \psi))$

least fixed point

eventually: $\Diamond \psi \equiv \psi \vee \bigcirc \Diamond \psi$

least fixed point

always: $\Box \psi \equiv \psi \wedge \bigcirc \Box \psi$

greatest fixed point

...don't yield a complete characterization, e.g.,

$$\boxed{\begin{array}{lcl} \mathit{false} & \equiv & a \wedge \bigcirc \mathit{false} \\ \Box a & \equiv & a \wedge \bigcirc \Box a \end{array}}$$

although
$\Box a \not\equiv \mathit{false}$

Expansion law for U

The LTL formula $\chi = \varphi \, \mathsf{U} \, \psi$ is the least solution of

$$\chi \equiv \psi \vee (\varphi \wedge \bigcirc \chi)$$

Expansion law for U

The LTL formula $\chi = \varphi \,\mathsf{U}\, \psi$ is the least solution of

$$\chi \equiv \psi \vee (\varphi \wedge \bigcirc \chi)$$

i.e., $\mathit{Words}(\varphi \,\mathsf{U}\, \psi)$ least LT-property E s.t.

$$E = \mathit{Words}(\psi) \cup \left\{ A_0 A_1 A_2 \ldots \in \mathit{Words}(\varphi) : A_1 A_2 \ldots \in E \right\}$$

The LTL formula $\chi = \varphi \, \mathsf{U} \, \psi$ is the least solution of

$$\chi \equiv \psi \vee (\varphi \wedge \bigcirc \chi)$$

i.e., $Words(\varphi \, \mathsf{U} \, \psi)$ least LT-property E s.t.

$$E = Words(\psi) \cup \left\{ A_0 A_1 A_2 \ldots \in Words(\varphi) : A_1 A_2 \ldots \in E \right\}$$

It even holds that $Words(\varphi \, \mathsf{U} \, \psi)$ least LT-property E s.t.

$$(1) \quad Words(\psi) \subseteq E$$

$$(2) \quad \left\{ A_0 A_1 A_2 \ldots \in Words(\varphi) : \; A_1 A_2 \ldots \in E \right\} \subseteq E$$

The weak until operator W

The weak until operator W

$$\boxed{\varphi \,\mathsf{W}\, \psi \stackrel{\mathsf{def}}{=} (\varphi \,\mathsf{U}\, \psi) \vee \Box\varphi}$$

The weak until operator W

$$\boxed{\varphi \,\mathsf{W}\, \psi \;\stackrel{\text{def}}{=}\; (\varphi \,\mathsf{U}\, \psi) \vee \Box\varphi}$$

deriving "always" and "until" from "weak until":

$$\Box\varphi \quad \equiv \quad ?$$

The weak until operator W

$$\boxed{\varphi \, \mathsf{W} \, \psi \;\stackrel{\text{def}}{=}\; (\varphi \, \mathsf{U} \, \psi) \vee \Box\varphi}$$

deriving "always" and "until" from "weak until":

$$\Box\varphi \quad \equiv \quad \varphi \, \mathsf{W} \, \mathit{false}$$

The weak until operator W

$$\boxed{\varphi \, \mathsf{W} \, \psi \ \stackrel{\text{def}}{=} \ (\varphi \, \mathsf{U} \, \psi) \vee \Box\varphi}$$

deriving "always" and "until" from "weak until":

$$\Box\varphi \equiv \varphi \, \mathsf{W} \, \mathit{false}$$

$$\varphi \, \mathsf{U} \, \psi \equiv \ ?$$

The weak until operator W

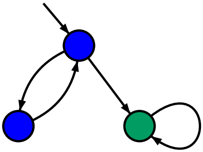
$$\boxed{\varphi \,\mathsf{W}\, \psi \;\stackrel{\text{def}}{=}\; (\varphi \,\mathsf{U}\, \psi) \vee \Box\varphi}$$

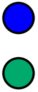
deriving "always" and "until" from "weak until":

$$\Box\varphi \equiv \varphi \,\mathsf{W}\, \mathit{false}$$

$$\varphi \,\mathsf{U}\, \psi \equiv (\varphi \,\mathsf{W}\, \psi) \wedge \Diamond\psi$$

Does $\mathcal{T} \models a \, \mathsf{W} \, b$ hold?

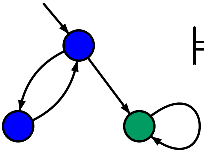




$\widehat{=} \ \{a\}$

$\widehat{=} \ \{b\}$

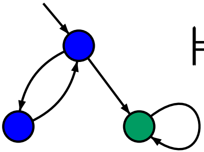
Does $\mathcal{T} \models a \, \mathsf{W} \, b$ hold?



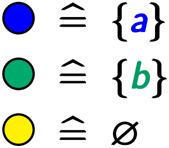
$\models a \, \mathsf{W} \, b$

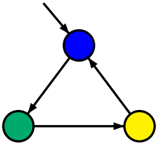
● $\widehat{=}$ $\{a\}$

● $\widehat{=}$ $\{b\}$

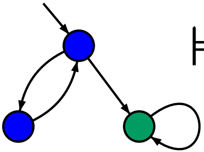


$\models a \,\mathsf{W}\, b$





Does $\mathcal{T} \models a \,\mathsf{W}\, b$ hold?

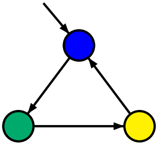


$\models a \,\mathsf{W}\, b$

$\widehat{=}$ $\{a\}$

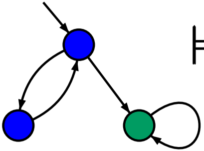
$\widehat{=}$ $\{b\}$

$\widehat{=}$ $\varnothing$



$\models\; a \,\mathsf{W}\, b \quad$ (even $a \,\mathsf{U}\, b$)

Does $\mathcal{T} \models a \,\mathsf{W}\, b$ hold?

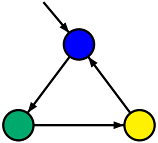


$\models a \,\mathsf{W}\, b$

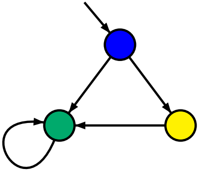
$\widehat{=} \ \{a\}$

$\widehat{=} \ \{b\}$

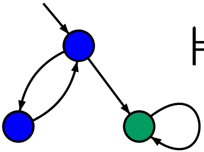
$\widehat{=} \ \varnothing$



$\models \ a \,\mathsf{W}\, b \quad$ (even $a \,\mathsf{U}\, b$)



Does $\mathcal{T} \models a \,\mathsf{W}\, b$ hold?

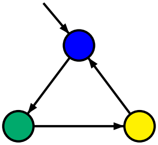


$\models a \,\mathsf{W}\, b$

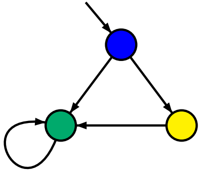
$\bullet_{\text{blue}} \mathrel{\widehat{=}} \{a\}$

$\bullet_{\text{green}} \mathrel{\widehat{=}} \{b\}$

$\bullet_{\text{yellow}} \mathrel{\widehat{=}} \varnothing$



$\models a \,\mathsf{W}\, b$ (even $a \,\mathsf{U}\, b$)



$\not\models a \,\mathsf{W}\, b$

Duality of U and W

$$\boxed{\varphi \, \mathsf{W} \, \psi \;\overset{\text{def}}{=}\; (\varphi \, \mathsf{U} \, \psi) \vee \Box\varphi}$$

goal: express $\neg(\varphi \, \mathsf{U} \, \psi)$ via **W**, and vice versa

Duality of U and W

$$\boxed{\varphi \,\mathsf{W}\, \psi \;\stackrel{\text{def}}{=}\; (\varphi \,\mathsf{U}\, \psi) \;\vee\; \Box\varphi}$$

$$\begin{aligned} &\neg(\varphi \,\mathsf{U}\, \psi) \\ \equiv\;\; &((\varphi \wedge \neg\psi) \;\mathsf{U}\; (\neg\varphi \wedge \neg\psi)) \;\vee\; \Box(\varphi \wedge \neg\psi) \end{aligned}$$

$$\boxed{\varphi \,\mathsf{W}\, \psi \;\overset{\text{def}}{=}\; (\varphi \,\mathsf{U}\, \psi) \vee \Box\varphi}$$

$$\begin{aligned}
& \neg(\varphi \,\mathsf{U}\, \psi) \\
\equiv\; & \big((\varphi \wedge \neg\psi) \;\mathsf{U}\; (\neg\varphi \wedge \neg\psi)\big) \vee \Box(\varphi \wedge \neg\psi) \\
\equiv\; & (\varphi \wedge \neg\psi) \,\mathsf{W}\, (\neg\varphi \wedge \neg\psi)
\end{aligned}$$

Duality of U and W

$$\boxed{\varphi \,\mathsf{W}\, \psi \overset{\text{def}}{=} (\varphi \,\mathsf{U}\, \psi) \vee \Box\varphi}$$

$$
\begin{aligned}
& \neg(\varphi \,\mathsf{U}\, \psi) \\
\equiv\ & ((\varphi \wedge \neg\psi) \ \mathsf{U}\ (\neg\varphi \wedge \neg\psi)) \vee \Box(\varphi \wedge \neg\psi) \\
\equiv\ & (\varphi \wedge \neg\psi) \,\mathsf{W}\, (\neg\varphi \wedge \neg\psi) \\
\equiv\ & (\neg\psi) \,\mathsf{W}\, (\neg\varphi \wedge \neg\psi)
\end{aligned}
$$

$$\boxed{\varphi \, \mathsf{W} \, \psi \;\overset{\text{def}}{=}\; (\varphi \, \mathsf{U} \, \psi) \vee \Box\varphi}$$

$$\begin{aligned}
&\neg(\varphi \, \mathsf{U} \, \psi) \\
\equiv\;& ((\varphi \wedge \neg\psi) \; \mathsf{U} \; (\neg\varphi \wedge \neg\psi)) \vee \Box(\varphi \wedge \neg\psi) \\
\equiv\;& (\varphi \wedge \neg\psi) \; \mathsf{W} \; (\neg\varphi \wedge \neg\psi) \\
\equiv\;& (\neg\psi) \; \mathsf{W} \; (\neg\varphi \wedge \neg\psi)
\end{aligned}$$

$$\neg(\varphi \, \mathsf{U} \, \psi) \equiv (\neg\psi) \, \mathsf{W} \, (\neg\varphi \wedge \neg\psi)$$

$$\neg(\varphi \, \mathsf{W} \, \psi) \equiv \; ?$$

$$\boxed{\varphi\, \mathsf{W}\, \psi \stackrel{\text{def}}{=} (\varphi\, \mathsf{U}\, \psi) \vee \Box\varphi}$$

$$\begin{aligned}
&\neg(\varphi\, \mathsf{U}\, \psi)\\
\equiv\;& ((\varphi \wedge \neg\psi)\ \mathsf{U}\ (\neg\varphi \wedge \neg\psi)) \vee \Box(\varphi \wedge \neg\psi)\\
\equiv\;& (\varphi \wedge \neg\psi)\ \mathsf{W}\ (\neg\varphi \wedge \neg\psi)\\
\equiv\;& (\neg\psi)\ \mathsf{W}\ (\neg\varphi \wedge \neg\psi)
\end{aligned}$$

$$\begin{aligned}
\neg(\varphi\, \mathsf{U}\, \psi) &\equiv (\neg\psi)\, \mathsf{W}\, (\neg\varphi \wedge \neg\psi)\\
\neg(\varphi\, \mathsf{W}\, \psi) &\equiv (\neg\psi)\, \mathsf{U}\, (\neg\varphi \wedge \neg\psi)
\end{aligned}$$

Expansion laws for U and W

Expansion laws for U and W

$$\varphi \,\mathsf{U}\, \psi \equiv \psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{U}\, \psi))$$

$$\varphi \,\mathsf{W}\, \psi \equiv \quad ?$$

Expansion laws for U and W

$$\varphi \,\mathsf{U}\, \psi \quad \equiv \quad \psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{U}\, \psi))$$

$$\varphi \,\mathsf{W}\, \psi \quad \equiv \quad \psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{W}\, \psi))$$

Expansion laws for U and W

$$\varphi \,\mathsf{U}\, \psi \quad \equiv \quad \psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{U}\, \psi))$$

smallest solution

$$\varphi \,\mathsf{W}\, \psi \quad \equiv \quad \psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{W}\, \psi))$$

Expansion laws for U and W

$\varphi \,\mathsf{U}\, \psi \equiv \psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{U}\, \psi))$	smallest solution
$\varphi \,\mathsf{W}\, \psi \equiv \psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{W}\, \psi))$	largest solution

Expansion laws for U and W

$\varphi \mathbf{U} \psi$	$\equiv$	$\psi \vee (\varphi \wedge \bigcirc(\varphi \mathbf{U} \psi))$	smallest solution
$\varphi \mathbf{W} \psi$	$\equiv$	$\psi \vee (\varphi \wedge \bigcirc(\varphi \mathbf{W} \psi))$	largest solution

Words$(\varphi \mathbf{U} \psi)$ smallest LT-property E s.t.

Expansion laws for U and W

$\varphi \,\mathsf{U}\, \psi$	$\equiv$	$\psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{U}\, \psi))$	smallest solution
$\varphi \,\mathsf{W}\, \psi$	$\equiv$	$\psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{W}\, \psi))$	largest solution

$Words(\varphi \,\mathsf{U}\, \psi)$ smallest LT-property E s.t.

$$\begin{array}{ll} (1) & Words(\psi) \subseteq E \\ (2) & \{A_0A_1A_2\ldots \in Words(\varphi) : A_1A_2\ldots \in E\} \subseteq E \end{array}$$

Expansion laws for U and W

$\varphi \,\mathsf{U}\, \psi \;\equiv\; \psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{U}\, \psi))$	smallest solution
$\varphi \,\mathsf{W}\, \psi \;\equiv\; \psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{W}\, \psi))$	largest solution

$Words(\varphi \,\mathsf{U}\, \psi)$ smallest LT-property E s.t.

$$(1) \quad Words(\psi) \subseteq E$$

$$(2) \quad \left\{ A_0 A_1 A_2 \ldots \in Words(\varphi) : \; A_1 A_2 \ldots \in E \right\} \subseteq E$$

$$\Updownarrow$$

$$Words(\psi) \cup \left\{ A_0 A_1 A_2 \ldots \in Words(\varphi) : \; A_1 A_2 \ldots \in E \right\} \subseteq E$$

Expansion laws for U and W

$\varphi \,\mathsf{U}\, \psi \quad \equiv \quad \psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{U}\, \psi))$	smallest solution
$\varphi \,\mathsf{W}\, \psi \quad \equiv \quad \psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{W}\, \psi))$	largest solution

$Words(\varphi \,\mathsf{U}\, \psi)$ smallest LT-property E s.t.

$$Words(\psi) \cup \{A_0 A_1 A_2 \ldots \in Words(\varphi) : A_1 A_2 \ldots \in E\} \subseteq E$$

$\varphi \, \mathsf{U} \, \psi$	$\equiv$	$\psi \vee (\varphi \wedge \bigcirc(\varphi \, \mathsf{U} \, \psi))$	smallest solution
$\varphi \, \mathsf{W} \, \psi$	$\equiv$	$\psi \vee (\varphi \wedge \bigcirc(\varphi \, \mathsf{W} \, \psi))$	largest solution

$Words(\varphi \, \mathsf{U} \, \psi)$ smallest LT-property E s.t.

$$Words(\psi) \cup \{A_0 A_1 A_2 \ldots \in Words(\varphi) : A_1 A_2 \ldots \in E\} \subseteq E$$

$Words(\varphi \, \mathsf{W} \, \psi)$ largest LT-property E s.t.

Expansion laws for U and W

$\varphi \, \mathsf{U} \, \psi$	$\equiv$	$\psi \vee (\varphi \wedge \bigcirc(\varphi \, \mathsf{U} \, \psi))$	smallest solution
$\varphi \, \mathsf{W} \, \psi$	$\equiv$	$\psi \vee (\varphi \wedge \bigcirc(\varphi \, \mathsf{W} \, \psi))$	largest solution

$Words(\varphi \, \mathsf{U} \, \psi)$ smallest LT-property E s.t.

$$Words(\psi) \cup \{A_0A_1A_2\ldots \in Words(\varphi) : A_1A_2\ldots \in E\} \subseteq E$$

$Words(\varphi \, \mathsf{W} \, \psi)$ largest LT-property E s.t.

$$Words(\psi) \cup \{A_0A_1A_2\ldots \in Words(\varphi) : A_1A_2\ldots \in E\} \supseteq E$$

Expansion laws for U and W

$\varphi \,\mathsf{U}\, \psi \;\equiv\; \psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{U}\, \psi))$	smallest solution
$\varphi \,\mathsf{W}\, \psi \;\equiv\; \psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{W}\, \psi))$	largest solution

$Words(\varphi \,\mathsf{U}\, \psi)$ smallest LT-property E s.t.

$$Words(\psi) \cup \{A_0A_1A_2\ldots \in Words(\varphi) : A_1A_2\ldots \in E\} \subseteq E$$

$Words(\varphi \,\mathsf{W}\, \psi)$ largest LT-property E s.t.

$$E \subseteq Words(\psi) \cup \{A_0A_1A_2\ldots \in Words(\varphi) : A_1A_2\ldots \in E\}$$

Expansion laws for U and W

$$\varphi \,\mathsf{U}\, \psi \quad \equiv \quad \psi \;\vee\; (\varphi \wedge \bigcirc(\varphi \,\mathsf{U}\, \psi))$$

smallest solution

$$\varphi \,\mathsf{W}\, \psi \quad \equiv \quad \psi \;\vee\; (\varphi \wedge \bigcirc(\varphi \,\mathsf{W}\, \psi))$$

largest solution

Expansion laws for U, W, $\Diamond$, and $\Box$

$$\varphi \,\mathsf{U}\, \psi \quad \equiv \quad \psi \;\vee\; (\varphi \wedge \bigcirc(\varphi \,\mathsf{U}\, \psi))$$

smallest solution

$$\Diamond\psi \quad \equiv \quad \psi \;\vee\; \bigcirc\Diamond\psi$$

smallest solution

$$\varphi \,\mathsf{W}\, \psi \quad \equiv \quad \psi \;\vee\; (\varphi \wedge \bigcirc(\varphi \,\mathsf{W}\, \psi))$$

largest solution

$$\Box\varphi \quad \equiv \quad \varphi \wedge \bigcirc\Box\varphi$$

largest solution

---

remind: $\Diamond\psi = \mathit{true}\,\mathsf{U}\,\psi$, $\quad \Box\varphi \equiv \varphi\,\mathsf{W}\,\mathit{false}$

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 $\wedge$

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

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

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

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

$$\bigcirc\varphi \longleftarrow$$ 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

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

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

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

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

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

$\Diamond$ 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:

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

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

$\neg \mathit{true}$	$\rightsquigarrow$	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 $\neg\vee$
$\neg \bigcirc \varphi$	$\rightsquigarrow$	$\bigcirc\neg\varphi$	
$\neg(\varphi_1 \,\mathsf{U}\, \varphi_2)$	$\rightsquigarrow$	$(\neg\varphi_2)\,\mathsf{W}(\neg\varphi_1 \wedge \neg\varphi_2)$	

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 $\neg\vee$
$\neg \bigcirc \varphi$	$\rightsquigarrow$	$\bigcirc\neg\varphi$	
$\neg(\varphi_1 \,\mathsf{U}\, \varphi_2)$	$\rightsquigarrow$	$(\neg\varphi_2)\,\mathsf{W}(\neg\varphi_1 \wedge \neg\varphi_2)$	
$\neg\Diamond\varphi$	$\rightsquigarrow$	$\Box\neg\varphi$	$\neg\Box\varphi \rightsquigarrow \Diamond\neg\varphi$

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

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

Example: LTL $\rightsquigarrow$ LTL-PNF

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

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

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

$\longleftarrow$ duality of $\Diamond$ and $\Box$

Example: LTL $\rightsquigarrow$ LTL-PNF

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

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

Example: LTL $\rightsquigarrow$ LTL-PNF

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

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

Example: LTL $\rightsquigarrow$ LTL-PNF

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

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

Example: LTL $\rightsquigarrow$ LTL-PNF

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

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

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

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

- 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 $\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$:

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

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 $A \in \mathcal{F}_{strong}$:

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

- 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 $\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$:

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

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

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

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

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

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

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

Process fairness is LTL-definable

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

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

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

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

LTL fairness assumptions

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

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

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

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

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

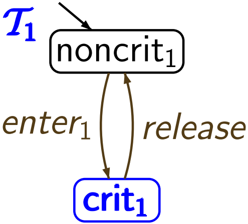
- unconditional fairness $\Box\Diamond\phi$
- strong fairness $\Box\Diamond\phi_1 \rightarrow \Box\Diamond\phi_2$
- weak fairness $\Diamond\Box\phi_1 \rightarrow \Box\Diamond\phi_2$

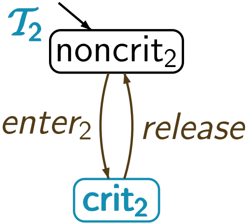
where ϕ_1, ϕ_2, ϕ are propositional formulas

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

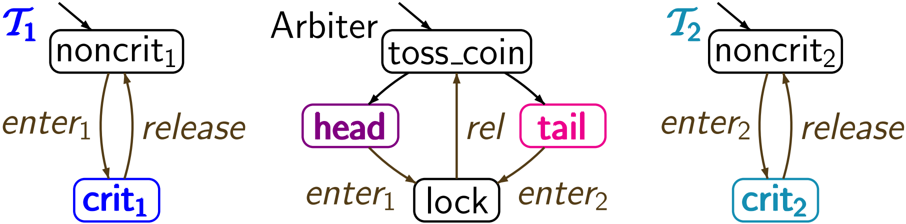
$$
\begin{aligned}
s \models_{fair} \varphi \quad & \text{iff} \quad \text{for all } \pi \in Paths(s): \\
& \qquad\quad \text{if } \pi \models fair \text{ then } \pi \models \varphi \\
& \text{iff} \quad s \models fair \rightarrow \varphi
\end{aligned}
$$

Randomized arbiter for MUTEX

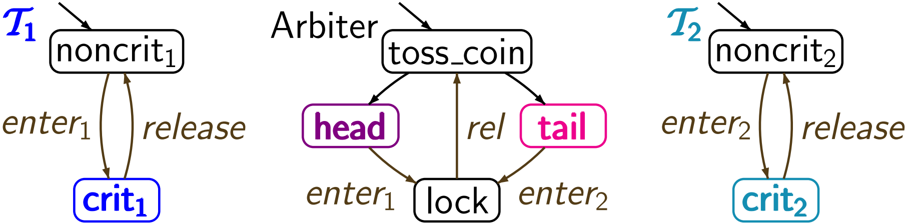




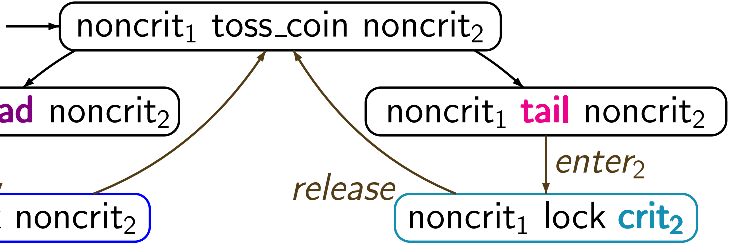
Randomized arbiter for MUTEX



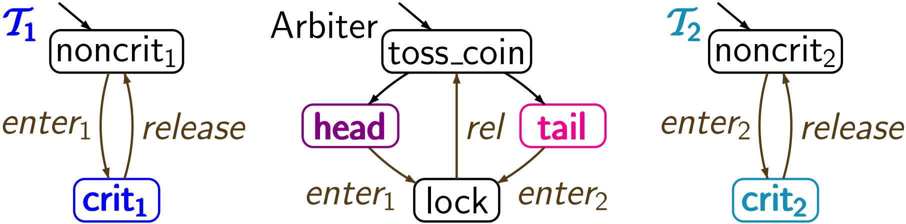
Randomized arbiter for MUTEX



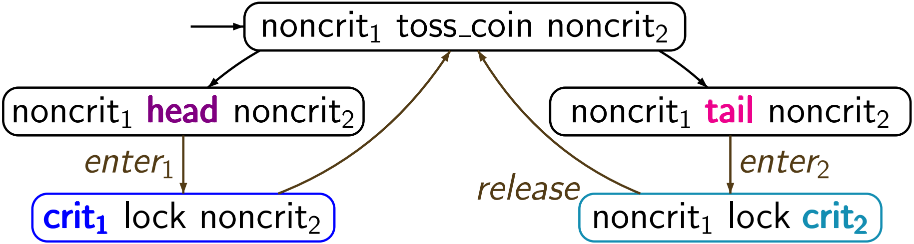
$(\mathcal{T}_1 \ ||| \ \mathcal{T}_2) \parallel Arbiter$



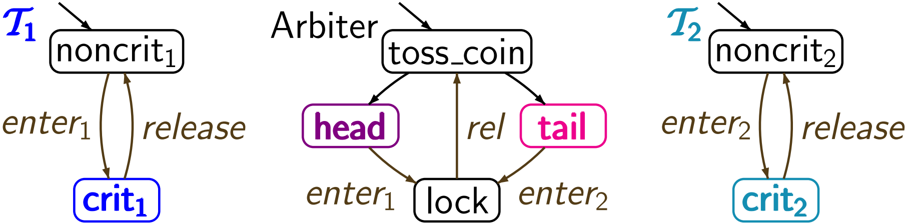
Randomized arbiter for MUTEX



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



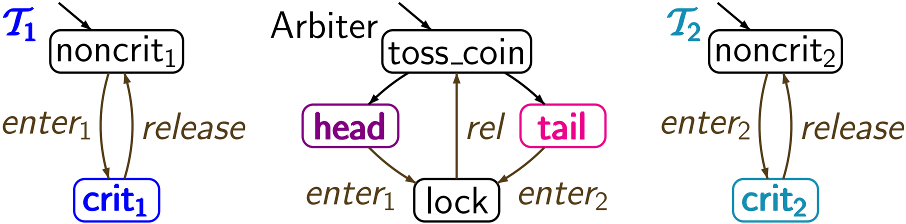
Randomized arbiter for MUTEX



unconditional LTL-fairness:

$$\mathit{fair} = \Box\Diamond\textbf{head} \wedge \Box\Diamond\textbf{tail}$$

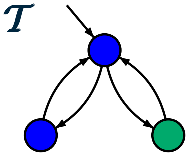
Randomized arbiter for MUTEX



unconditional LTL-fairness:

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

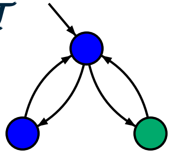
$$(\mathcal{T}_1 \;|||\; \mathcal{T}_2) \,\|\, Arbiter \;\models_{fair}\; \Box\Diamond \mathsf{crit}_1 \;\wedge\; \Box\Diamond \mathsf{crit}_2$$



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

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

$\mathcal{T}$



LTL fairness assumption

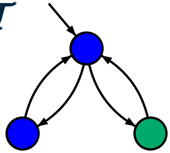
$fair = \Diamond\Box a \rightarrow \Box\Diamond b$

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

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

Correct or wrong?

$\mathcal{T}$



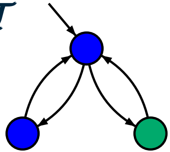
LTL fairness assumption
$fair = \Diamond\Box a \rightarrow \Box\Diamond b$

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

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

Correct or wrong?

$\mathcal{T}$



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

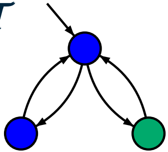
● $\widehat{=}\{a\}$ ● $\widehat{=}\{b\}$

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

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

Correct or wrong?

$\mathcal{T}$



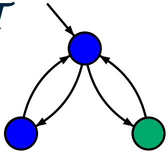
LTL fairness assumption
$fair = \Diamond\Box a \rightarrow \Box\Diamond b$

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

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

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

$\mathcal{T}$



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

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

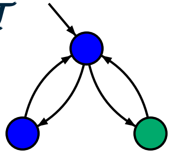
$\mathcal{T} \not\models_{fair} \bigcirc b$ as ●→●→●→●→●→●→ . . . is fair

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

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

Correct or wrong?

$\mathcal{T}$



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

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

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

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

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

as $\textcolor{blue}{\bullet} \to \textcolor{green}{\bullet} \to \textcolor{blue}{\bullet} \to \textcolor{blue}{\bullet} \to \textcolor{blue}{\bullet} \to \textcolor{green}{\bullet} \to \ldots$ 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.,

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

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

- 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 $AP = \{a, b, \ldots\}$.

Each strong **LTL** fairness assumption

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

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

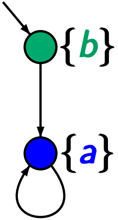
Correct or wrong?

Each strong **LTL** fairness assumption

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

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

wrong



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

is not 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:

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

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

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:

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

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

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:

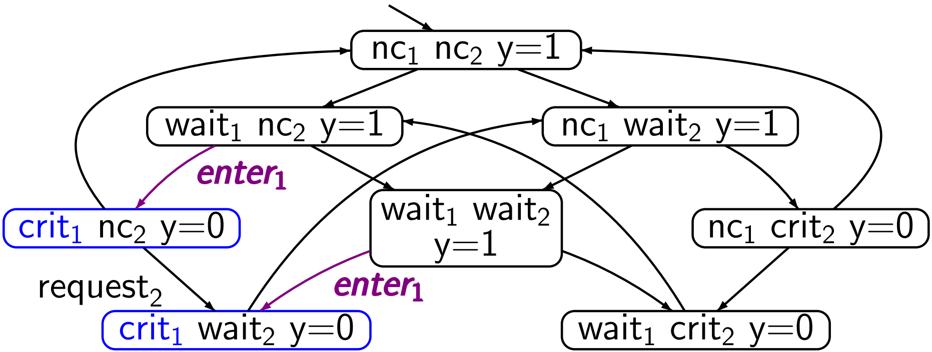
$$enabled(A) \in L(s) \quad \text{iff} \quad s \xrightarrow{\alpha} \ldots \text{ for some } \alpha \in A$$

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

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

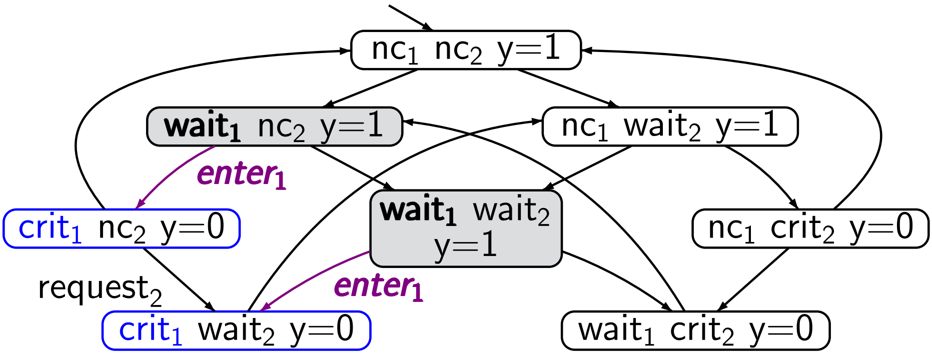
alternative 2: modify the given transition system by adding an action component to the states

Ad-hoc: action fairness ⇝ LTL-fairness



TS for mutual exclusion with semaphore

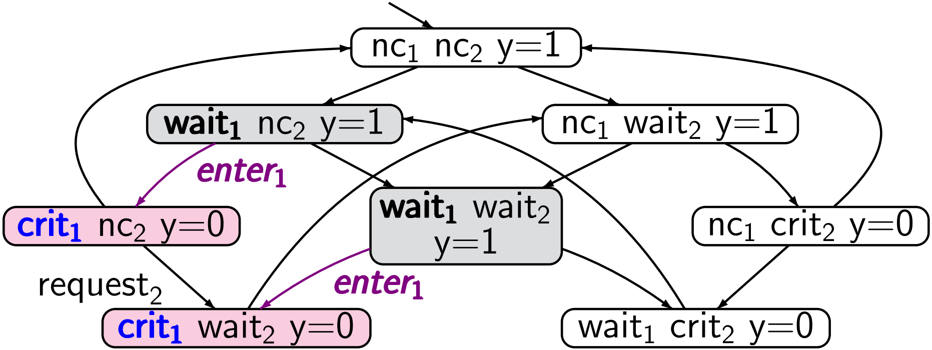
Ad-hoc: action fairness ⇝ LTL-fairness



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

TS for mutual exclusion with semaphore

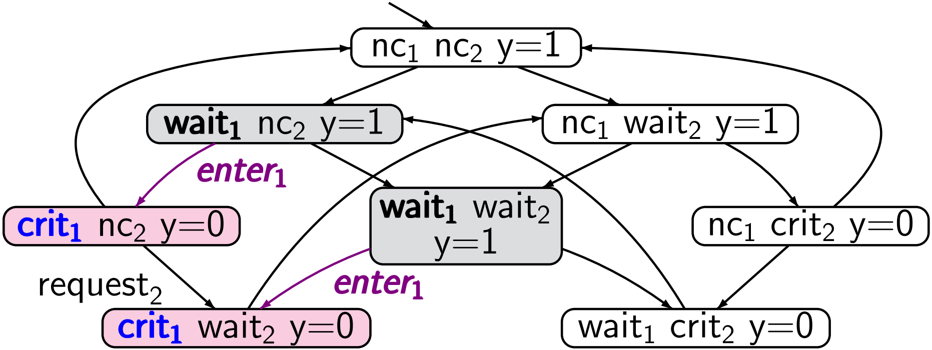
Ad-hoc: action fairness ⇝ LTL-fairness



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

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

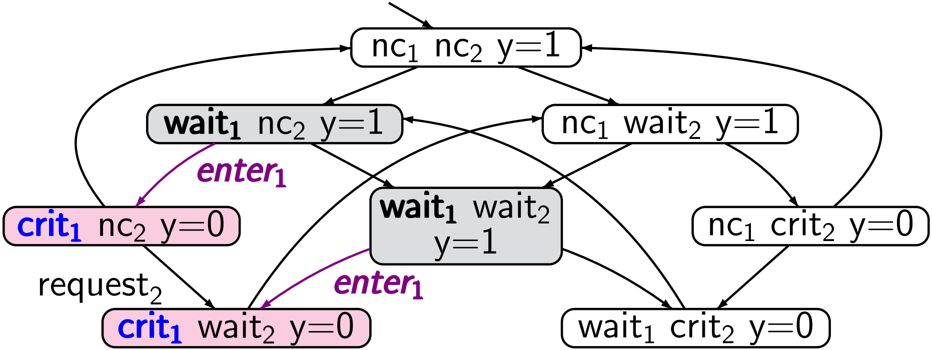
TS for mutual exclusion with semaphore



$\square$ (pink) $\widehat{=}$ $taken(\{enter_1\})$ $\widehat{=}$ $\mathbf{crit_1}$

$\square$ (grey) $\widehat{=}$ $enabled(\{enter_1\})$ $\widehat{=}$ $\mathbf{wait_1} \wedge \neg \mathbf{crit_2}$

Ad-hoc: action fairness $\rightsquigarrow$ LTL-fairness



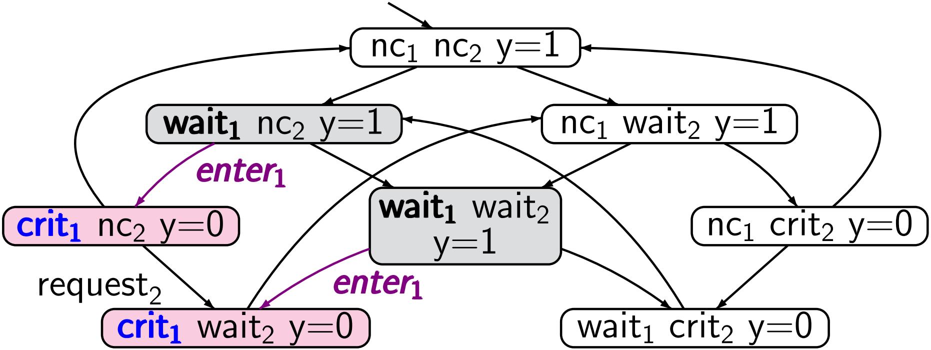
$\widehat{=}$ *taken*({*enter*$_1$}) $\widehat{=}$ **crit$_1$**

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

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

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

Ad-hoc: action fairness $\rightsquigarrow$ LTL-fairness



$\widehat{=}$ *taken*($\{$*enter*$_1\}$) $\widehat{=}$ $crit_1$

$\widehat{=}$ *enabled*($\{$*enter*$_1\}$) $\widehat{=}$ $wait_1 \wedge \neg crit_2$

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

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

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

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

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

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:

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

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

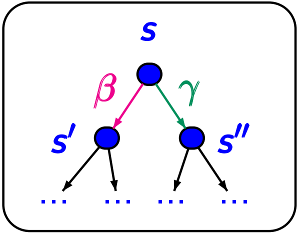
alternative 1: ad-hoc choice of "***taken***-predicate"

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

Action-based fairness $\rightsquigarrow$ LTL-fairness

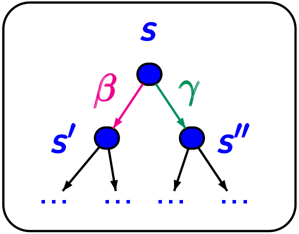
transition system

$\mathcal{T} = (S, Act, \to, \ldots)$

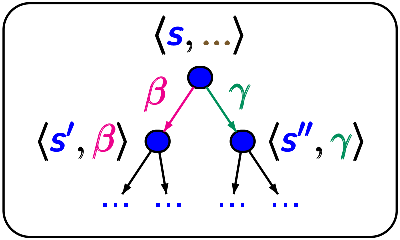


Action-based fairness $\rightsquigarrow$ LTL-fairness

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

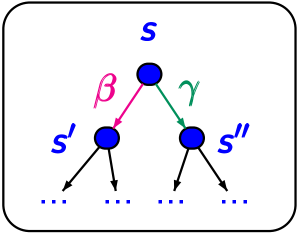


transition system $\mathcal{T}' = (S \times Act, \ldots, AP', L')$

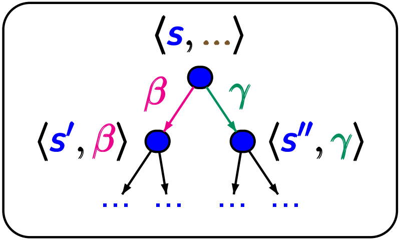


Action-based fairness $\rightsquigarrow$ LTL-fairness

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



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



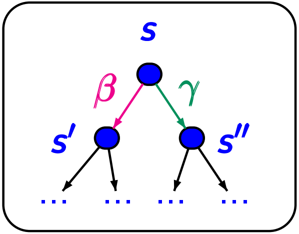
strong A-fairness
for $A \subseteq Act$

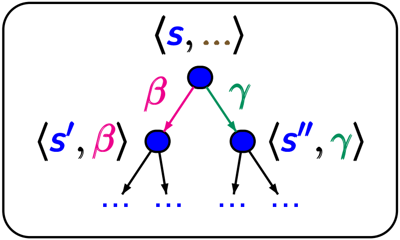
strong **LTL**-fairness
$\Box\Diamond enabled(A) \rightarrow \Box\Diamond taken(A)$

Action-based fairness $\rightsquigarrow$ LTL-fairness

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

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





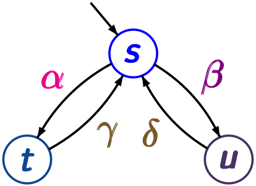
strong A-fairness
for $A \subseteq Act$

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

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

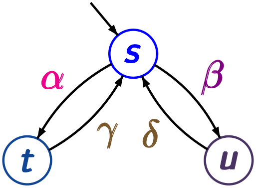
$$taken(A) \in L'(\langle s, \alpha \rangle) \quad \text{iff} \quad \alpha \in A$$

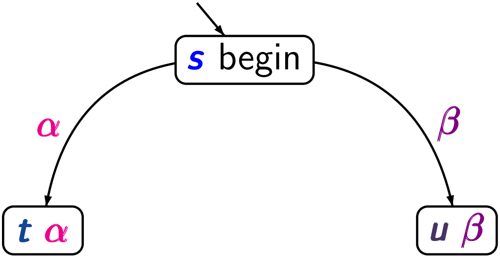
action-based fairness ⇝ LTL-fairness



Example: action fairness $\rightsquigarrow$ LTL-fairness

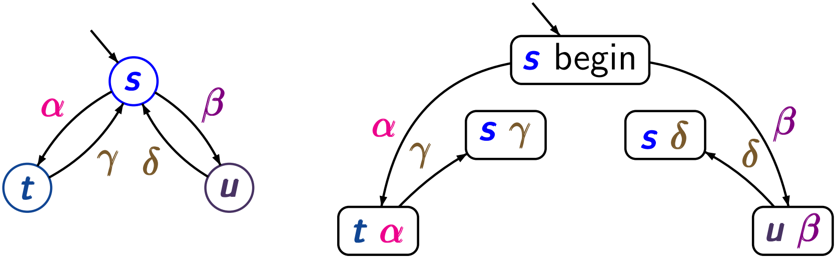
action-based fairness $\rightsquigarrow$ LTL-fairness



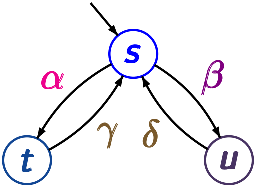


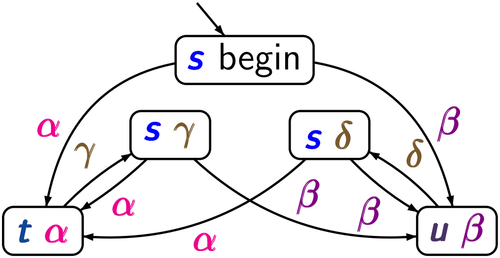
Example: action fairness ⇝ LTL-fairness

action-based fairness ⇝ LTL-fairness



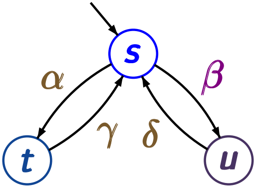
action-based fairness ⇝ LTL-fairness

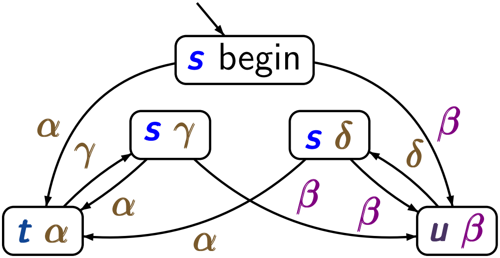




Example: action fairness ⇝ LTL-fairness

action-based fairness ⇝ LTL-fairness

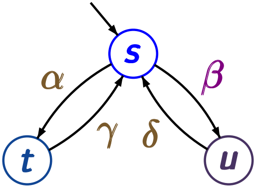


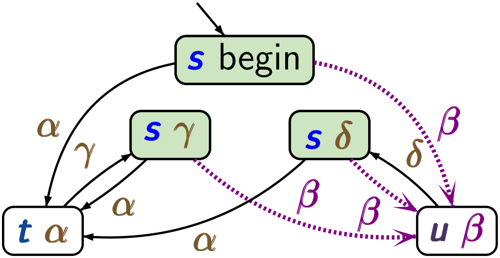


strong fairness for $\{\beta\}$:

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

action-based fairness $\rightsquigarrow$ LTL-fairness



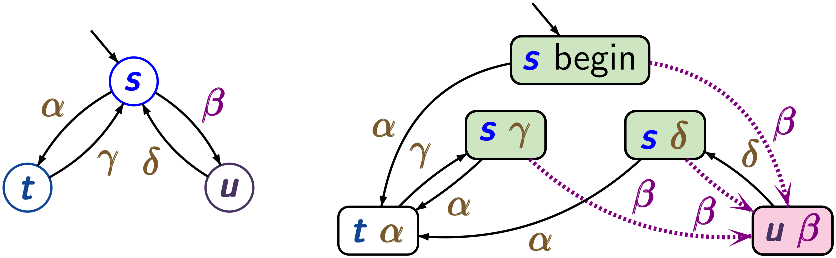


strong fairness for $\{\beta\}$:

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

Example: action fairness $\rightsquigarrow$ LTL-fairness

action-based fairness $\rightsquigarrow$ LTL-fairness

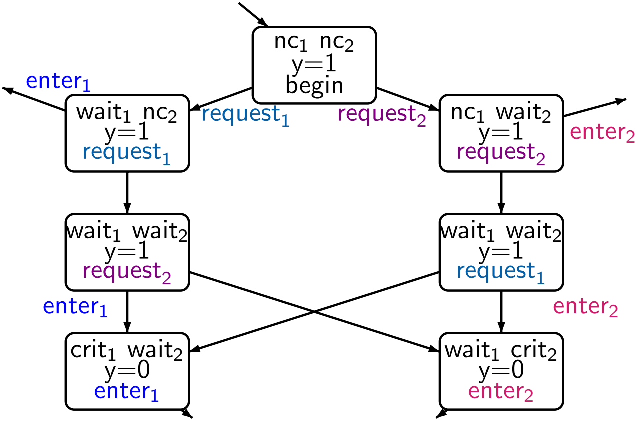


strong fairness for $\{\beta\}$:

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

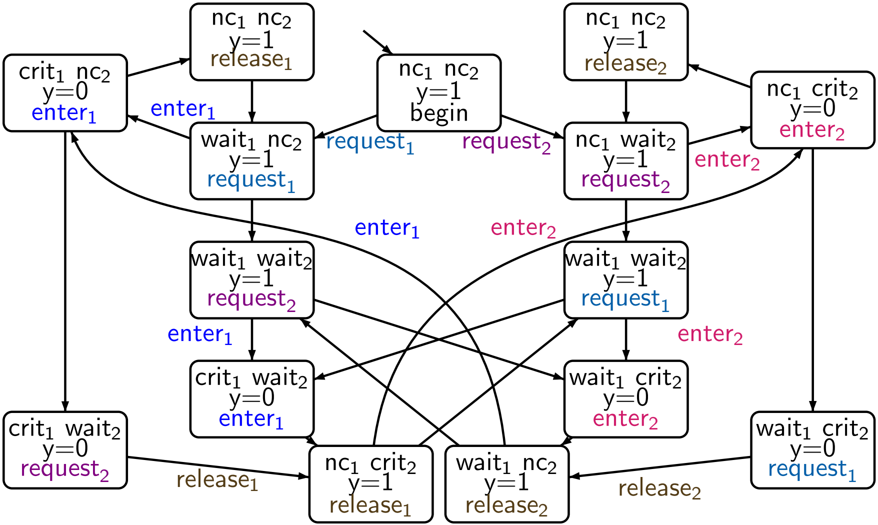
Example: mutual exclusion with semaphore

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 ∪ {begin}