

Introduction

Modelling parallel systems

Linear Time Properties

Regular Properties

**Linear Temporal Logic (LTL)**

Computation-Tree Logic

Equivalences and Abstraction

extend propositional or predicate logic by  
temporal modalities

extend propositional or predicate logic by  
temporal modalities, e.g.

$\Box\varphi$  “ $\varphi$  holds **always**”, i.e., now and forever  
in the future

$\Diamond\varphi$  “ $\varphi$  holds now or **eventually** in the future”

extend propositional or predicate logic by  
temporal modalities, e.g.

$\Box\varphi$  “ $\varphi$  holds **always**”, i.e., now and forever  
in the future

$\Diamond\varphi$  “ $\varphi$  holds now or **eventually** in the future”

*here:* two propositional temporal logics:

**LTL:** linear temporal logic

**CTL:** computation tree logic

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





$$\varphi ::= \text{true} \mid a \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi$$

where  $a \in AP$

$$\varphi ::= \text{true} \mid a \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \bigcirc\varphi$$

where  $a \in AP$        $\bigcirc \hat{=} \text{next}$



$$\varphi ::= \text{true} \mid a \mid \varphi_1 \wedge \varphi_2 \mid \neg \varphi \mid \bigcirc \varphi \mid \varphi_1 \mathbf{U} \varphi_2$$

where  $a \in AP$

$\bigcirc \hat{=}$  next

$\mathbf{U} \hat{=}$  until

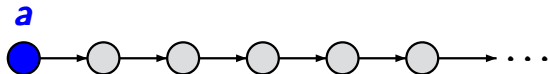
$$\varphi ::= \text{true} \mid a \mid \varphi_1 \wedge \varphi_2 \mid \neg \varphi \mid \bigcirc \varphi \mid \varphi_1 \mathbf{U} \varphi_2$$

where  $a \in AP$

$\bigcirc \hat{=}$  next

$\mathbf{U} \hat{=}$  until

atomic  
proposition  
 $a \in AP$



$$\varphi ::= \text{true} \mid a \mid \varphi_1 \wedge \varphi_2 \mid \neg \varphi \mid \bigcirc \varphi \mid \varphi_1 \mathbf{U} \varphi_2$$

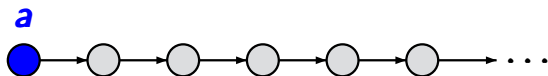
where  $a \in AP$

$\bigcirc \hat{=}$  next

$\mathbf{U} \hat{=}$  until

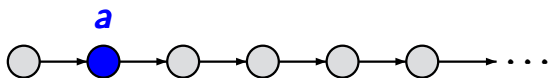
atomic  
proposition

$a \in AP$



next operator

$\bigcirc a$



$$\varphi ::= \text{true} \mid a \mid \varphi_1 \wedge \varphi_2 \mid \neg \varphi \mid \bigcirc \varphi \mid \varphi_1 \mathbf{U} \varphi_2$$

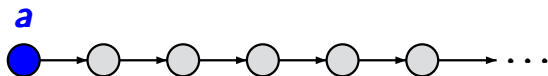
where  $a \in AP$

$\bigcirc \hat{=}$  next

$\mathbf{U} \hat{=}$  until

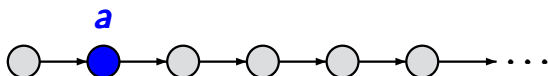
atomic  
proposition

$a \in AP$



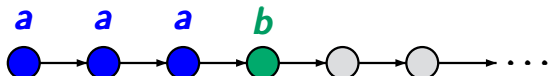
next operator

$\bigcirc a$



until operator

$a \mathbf{U} b$



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

derived operators:

$\forall, \rightarrow, \dots$  as usual

$$\varphi ::= \text{true} \mid a \mid \varphi_1 \wedge \varphi_2 \mid \neg \varphi \mid \bigcirc \varphi \mid \varphi_1 \mathbf{U} \varphi_2$$

derived operators:

$\forall, \rightarrow, \dots$  as usual

$$\diamond \varphi \stackrel{\text{def}}{=} \text{true} \mathbf{U} \varphi \quad \text{eventually}$$

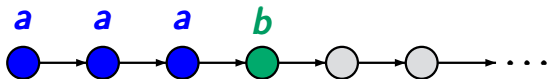
$$\varphi ::= \mathit{true} \mid a \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \bigcirc\varphi \mid \varphi_1 \mathbf{U} \varphi_2$$

derived operators:

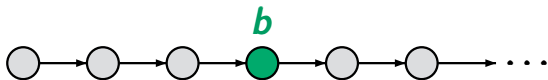
$\forall, \rightarrow, \dots$  as usual

$$\diamond\varphi \stackrel{\text{def}}{=} \mathit{true} \mathbf{U} \varphi \quad \text{eventually}$$

until operator

$$a \mathbf{U} b$$


eventually

$$\diamond b$$


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

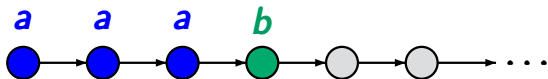
derived operators:

$\forall, \rightarrow, \dots$  as usual

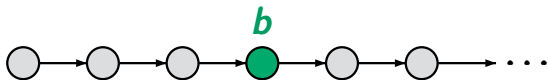
$$\diamond \varphi \stackrel{\text{def}}{=} \mathbf{true} \mathbf{U} \varphi \quad \text{eventually}$$

$$\square \varphi \stackrel{\text{def}}{=} \neg \diamond \neg \varphi \quad \text{always}$$

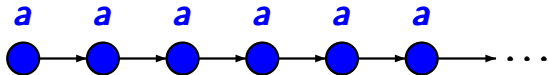
until operator  
 $\mathbf{a} \mathbf{U} \mathbf{b}$



eventually  
 $\diamond \mathbf{b}$

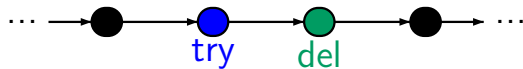


always  
 $\square \mathbf{a}$

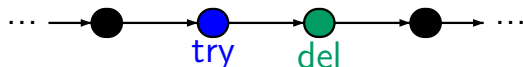




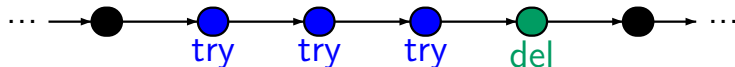
□ (try\_to\_send → ○ delivered)



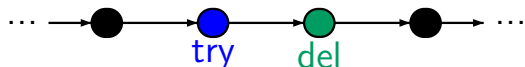
$\square$  (try\_to\_send  $\rightarrow$   $\bigcirc$  delivered)



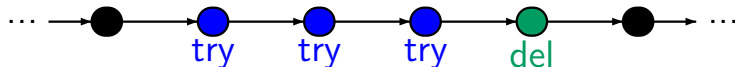
$\square$  (try\_to\_send  $\rightarrow$  try\_to\_send **U** delivered)



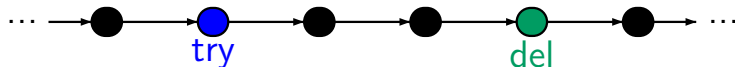
$\square$  ( $\text{try\_to\_send} \rightarrow \bigcirc \text{delivered}$ )



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



$\square$  ( $\text{try\_to\_send} \rightarrow \blacklozenge \text{delivered}$ )



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

eventually

$$\diamond \varphi \stackrel{\text{def}}{=} \mathit{true} \mathbf{U} \varphi$$

always

$$\square \varphi \stackrel{\text{def}}{=} \neg \diamond \neg \varphi$$

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

eventually

$$\diamond \varphi \stackrel{\text{def}}{=} \mathit{true} \mathbf{U} \varphi$$

always

$$\square \varphi \stackrel{\text{def}}{=} \neg \diamond \neg \varphi$$

*Examples* for LTL formulas:

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

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

eventually

$$\diamond\varphi \stackrel{\text{def}}{=} \mathit{true} \mathbf{U}\varphi$$

always

$$\square\varphi \stackrel{\text{def}}{=} \neg\diamond\neg\varphi$$

Examples for LTL formulas:

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

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

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

eventually

$$\diamond\varphi \stackrel{\text{def}}{=} \mathit{true} \mathbf{U} \varphi$$

always

$$\square\varphi \stackrel{\text{def}}{=} \neg\diamond\neg\varphi$$

Examples for LTL formulas:

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

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

progress property:  $\square(\mathit{request} \rightarrow \diamond\mathit{response})$

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

eventually

$$\diamond \varphi \stackrel{\text{def}}{=} \mathbf{true} \mathbf{U} \varphi$$

always

$$\square \varphi \stackrel{\text{def}}{=} \neg \diamond \neg \varphi$$

Examples for LTL formulas:

mutual exclusion:  $\square(\neg \mathbf{crit}_1 \vee \neg \mathbf{crit}_2)$

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

progress property:  $\square(\mathbf{request} \rightarrow \diamond \mathbf{response})$

traffic light:  $\square(\mathbf{yellow} \vee \bigcirc \neg \mathbf{red})$



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

eventually  $\diamond \varphi \stackrel{\text{def}}{=} \mathit{true} \mathbf{U} \varphi$

always  $\square \varphi \stackrel{\text{def}}{=} \neg \diamond \neg \varphi$

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

eventually  $\diamond \varphi \stackrel{\text{def}}{=} \mathit{true} \mathbf{U} \varphi$

always  $\square \varphi \stackrel{\text{def}}{=} \neg \diamond \neg \varphi$

infinitely often  $\square \diamond \varphi$

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

eventually  $\diamond\varphi \stackrel{\text{def}}{=} \mathit{true} \mathbf{U} \varphi$

always  $\square\varphi \stackrel{\text{def}}{=} \neg\diamond\neg\varphi$

infinitely often  $\square\diamond\varphi$

e.g., unconditional fairness  $\square\diamond\mathit{crit}_i$

strong fairness  $\square\diamond\mathit{wait}_i \rightarrow \square\diamond\mathit{crit}_i$

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

eventually  $\diamond\varphi \stackrel{\text{def}}{=} \mathbf{true} \mathbf{U} \varphi$

always  $\square\varphi \stackrel{\text{def}}{=} \neg\diamond\neg\varphi$

infinitely often  $\square\diamond\varphi$

eventually forever  $\diamond\square\varphi$

e.g., unconditional fairness  $\square\diamond\mathbf{crit}_i$

strong fairness  $\square\diamond\mathbf{wait}_i \rightarrow \square\diamond\mathbf{crit}_i$

weak fairness  $\diamond\square\mathbf{wait}_i \rightarrow \square\diamond\mathbf{crit}_i$



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

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  $\sigma = A_0 A_1 A_2 \dots \in (2^{AP})^\omega$

for  $\sigma = A_0 A_1 A_2 \dots \in (2^{AP})^\omega$ :



for  $\sigma = A_0 A_1 A_2 \dots \in (2^{AP})^\omega$ :

$\sigma \models \text{true}$

for  $\sigma = A_0 A_1 A_2 \dots \in (2^{AP})^\omega$ :

$\sigma \models \text{true}$

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

for  $\sigma = A_0 A_1 A_2 \dots \in (2^{AP})^\omega$ :

$\sigma \models \text{true}$

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

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

for  $\sigma = A_0 A_1 A_2 \dots \in (2^{AP})^\omega$ :

$\sigma \models \text{true}$

$\sigma \models a$       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  $\sigma \not\models \varphi$

for  $\sigma = A_0 A_1 A_2 \dots \in (2^{AP})^\omega$ :

$\sigma \models \text{true}$

$\sigma \models a$  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  $\text{suffix}(\sigma, 1) = A_1 A_2 A_3 \dots \models \varphi$

for  $\sigma = A_0 A_1 A_2 \dots \in (2^{AP})^\omega$ :

$\sigma \models \text{true}$

$\sigma \models a$  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  $\text{suffix}(\sigma, 1) = A_1 A_2 A_3 \dots \models \varphi$

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

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

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

for  $\sigma = A_0 A_1 A_2 \dots \in (2^{AP})^\omega$ :

$\sigma \models \text{true}$

$\sigma \models a$  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  $\text{suffix}(\sigma, 1) = A_1 A_2 A_3 \dots \models \varphi$

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

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

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





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  $\sigma = A_0 A_1 A_2 \dots \in (2^{AP})^\omega$

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  $\sigma = A_0 A_1 A_2 \dots \in (2^{AP})^\omega$

**LT property** of formula  $\varphi$ :

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



for  $\sigma = A_0 A_1 A_2 \dots \in (2^{AP})^\omega$ :

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

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

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

for  $\sigma = A_0 A_1 A_2 \dots \in (2^{AP})^\omega$ :

$\sigma \models \varphi_1 \mathbf{U} \varphi_2$  iff there exists  $j \geq 0$  such that  
 $A_j A_{j+1} A_{j+2} \dots \models \varphi_2$  and  
 $A_i A_{i+1} A_{i+2} \dots \models \varphi_1$  for  $0 \leq i < j$

$\sigma \models \diamond \varphi$  iff there exists  $j \geq 0$  such that  
 $A_j A_{j+1} A_{j+2} \dots \models \varphi$

for  $\sigma = A_0 A_1 A_2 \dots \in (2^{AP})^\omega$ :

	$\vdots$	
$\sigma \models \varphi_1 \mathbf{U} \varphi_2$	iff	there exists $j \geq 0$ such that $A_j A_{j+1} A_{j+2} \dots \models \varphi_2$ and $A_i A_{i+1} A_{i+2} \dots \models \varphi_1$ for $0 \leq i < j$
$\sigma \models \diamond \varphi$	iff	there exists $j \geq 0$ such that $A_j A_{j+1} A_{j+2} \dots \models \varphi$
$\sigma \models \square \varphi$	iff	for all $j \geq 0$ we have: $A_j A_{j+1} A_{j+2} \dots \models \varphi$



given a TS  $\mathcal{T} = (\mathcal{S}, Act, \rightarrow, \mathcal{S}_0, AP, L)$

define satisfaction relation  $\models$  for

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



given a TS  $\mathcal{T} = (\mathcal{S}, Act, \rightarrow, \mathcal{S}_0, AP, L)$

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



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

without terminal states

LTL formula  $\varphi$  over  $AP$

given: TS  $\mathcal{T} = (\mathcal{S}, Act, \rightarrow, s_0, AP, L)$

without terminal states

LTL formula  $\varphi$  over  $AP$

interpretation of  $\varphi$  over infinite path fragments

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

given: TS  $\mathcal{T} = (\mathcal{S}, Act, \rightarrow, s_0, AP, L)$

without terminal states

LTL formula  $\varphi$  over  $AP$

interpretation of  $\varphi$  over infinite path fragments

$$\begin{aligned} \pi = s_0 s_1 s_2 \dots \models \varphi & \text{ iff } \text{trace}(\pi) \models \varphi \\ & \text{ iff } \text{trace}(\pi) \in \text{Words}(\varphi) \end{aligned}$$

given: TS  $\mathcal{T} = (\mathcal{S}, Act, \rightarrow, s_0, AP, L)$   
without terminal states

LTL formula  $\varphi$  over  $AP$

interpretation of  $\varphi$  over infinite path fragments

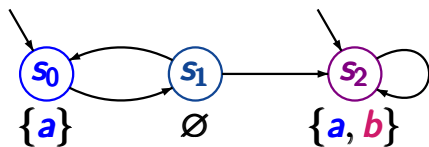
$$\begin{aligned} \pi = s_0 s_1 s_2 \dots \models \varphi & \text{ iff } \text{trace}(\pi) \models \varphi \\ & \text{ iff } \text{trace}(\pi) \in \text{Words}(\varphi) \end{aligned}$$

remind: LT property of an LTL formula:

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

# Example: LTL-semantics over paths

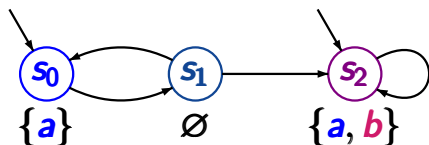
LTLSF3.1-9



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

# Example: LTL-semantics over paths

LTLSF3.1-9



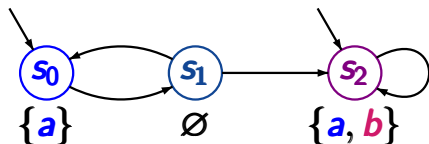
$$AP = \{a, b\}$$

path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$



# Example: LTL-semantics over paths

LTLSF3.1-9



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

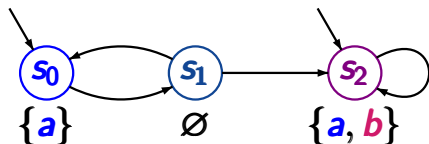
path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$

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

$$\pi \models a$$

# Example: LTL-semantics over paths

LTLSF3.1-9



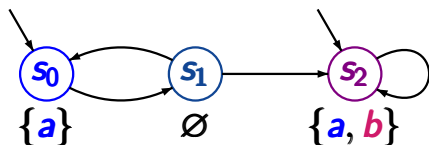
$$AP = \{a, b\}$$

path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$

$$\text{trace}(\pi) = \{a\} \emptyset \{a, b\}^\omega$$

$\pi \models a$ , but  $\pi \not\models b$

as  $L(s_0) = \{a\}$



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

path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$

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

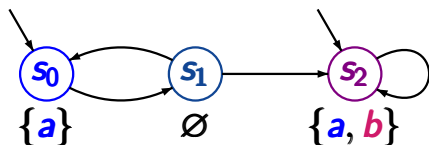
$\pi \models a$ , but  $\pi \not\models b$

as  $L(s_0) = \{a\}$

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

# Example: LTL-semantics over paths

LTLSF3.1-9



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

path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$

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

$\pi \models a$ , but  $\pi \not\models b$

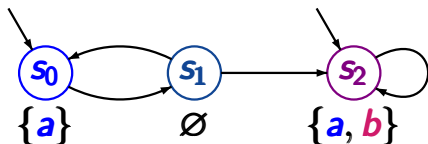
as  $L(s_0) = \{a\}$

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

as  $L(s_1) = \emptyset$

# Example: LTL-semantics over paths

LTLSF3.1-9



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

path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$

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

$\pi \models a$ , but  $\pi \not\models b$

as  $L(s_0) = \{a\}$

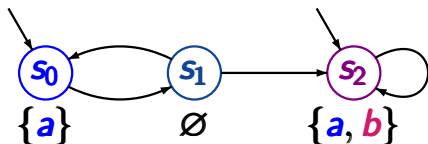
$\pi \models \bigcirc(\neg a \wedge \neg b)$

as  $L(s_1) = \emptyset$

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

# Example: LTL-semantics over paths

LTLSF3.1-9



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

path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$

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

$\pi \models a$ , but  $\pi \not\models b$

as  $L(s_0) = \{a\}$

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

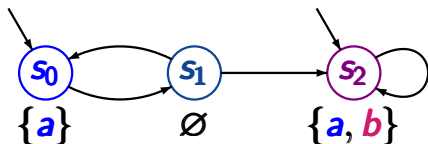
as  $L(s_1) = \emptyset$

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

as  $L(s_2) = \{a, b\}$

# Example: LTL-semantics over paths

LTLSF3.1-9



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

path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$

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

$\pi \models a$ , but  $\pi \not\models b$

as  $L(s_0) = \{a\}$

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

as  $L(s_1) = \emptyset$

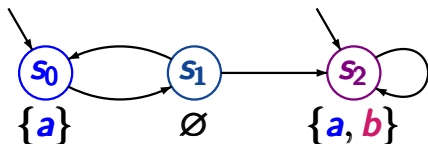
$\pi \models \bigcirc \bigcirc (a \wedge b)$

as  $L(s_2) = \{a, b\}$

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

# Example: LTL-semantics over paths

LTLSF3.1-9



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

path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$

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

$\pi \models a$ , but  $\pi \not\models b$

as  $L(s_0) = \{a\}$

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

as  $L(s_1) = \emptyset$

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

as  $L(s_2) = \{a, b\}$

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

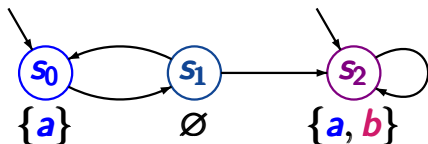
as  $s_0, s_1 \models \neg b$

and  $s_2 \models a \wedge b$



# Example: LTL-semantics over paths

LTLSF3.1-9



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

path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$

$$\text{trace}(\pi) = \{a\} \emptyset \{a, b\}^\omega$$

$\pi \models a$ , but  $\pi \not\models b$

as  $L(s_0) = \{a\}$

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

as  $L(s_1) = \emptyset$

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

as  $L(s_2) = \{a, b\}$

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

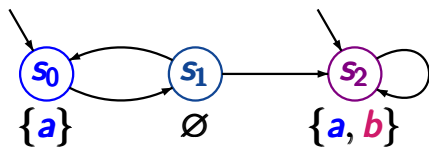
as  $s_0, s_1 \models \neg b$

$\pi \models (\neg b) \cup \square(a \wedge b)$

and  $s_2 \models a \wedge b$

# Correct or wrong ?

LTLSF3.1-7

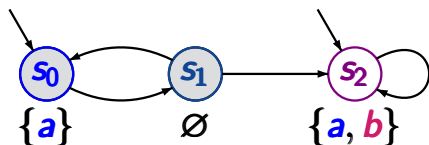


$$AP = \{a, b\}$$

path  $\pi = s_0 s_1 s_0 s_1 s_0 s_1 \dots$

# Correct or wrong ?

LTLSF3.1-7



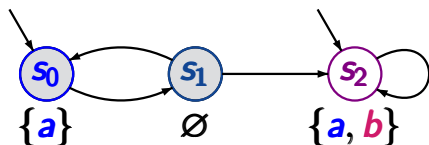
path  $\pi = s_0 s_1 s_0 s_1 s_0 s_1 \dots$

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

$$\text{trace}(\pi) = (\{a\} \emptyset)^\omega$$

# Correct or wrong ?

LTLSF3.1-7



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

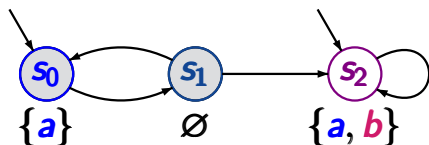
path  $\pi = s_0 s_1 s_0 s_1 s_0 s_1 \dots$

$$\text{trace}(\pi) = (\{a\} \emptyset)^\omega$$

$\pi \models a \cup b$  ?

# Correct or wrong ?

LTLSF3.1-7



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

path  $\pi = s_0 s_1 s_0 s_1 s_0 s_1 \dots$

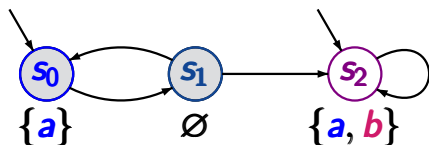
$$\text{trace}(\pi) = (\{a\} \emptyset)^\omega$$

$\pi \not\models a \cup b$

as  $s_0 \not\models b$  and  $s_1 \not\models a \vee b$

# Correct or wrong ?

LTLSF3.1-7



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

path  $\pi = s_0 s_1 s_0 s_1 s_0 s_1 \dots$

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

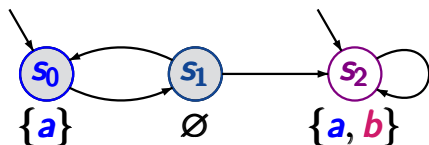
$$\pi \not\models a \cup b$$

as  $s_0 \not\models b$  and  $s_1 \not\models a \vee b$

$$\pi \models \diamond b \rightarrow (a \cup b) ?$$

# Correct or wrong ?

LTLSF3.1-7



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

path  $\pi = s_0 s_1 s_0 s_1 s_0 s_1 \dots$

$$\text{trace}(\pi) = (\{a\} \emptyset)^\omega$$

$$\pi \not\models a \cup b$$

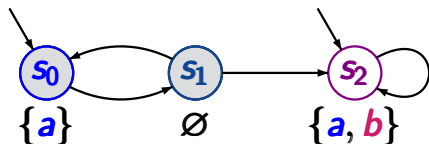
as  $s_0 \not\models b$  and  $s_1 \not\models a \vee b$

$$\pi \models \diamond b \rightarrow (a \cup b)$$

as  $\pi \not\models \diamond b$

# Correct or wrong ?

LTLSF3.1-7



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

path  $\pi = s_0 s_1 s_0 s_1 s_0 s_1 \dots$

$$\text{trace}(\pi) = (\{a\} \emptyset)^\omega$$

$$\pi \not\models a \cup b$$

as  $s_0 \not\models b$  and  $s_1 \not\models a \vee b$

$$\pi \models \diamond b \rightarrow (a \cup b)$$

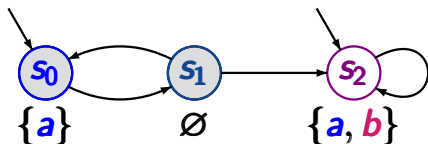
as  $\pi \not\models \diamond b$

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



# Correct or wrong ?

LTLSF3.1-7



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

path  $\pi = s_0 s_1 s_0 s_1 s_0 s_1 \dots$

$$\text{trace}(\pi) = (\{a\} \emptyset)^\omega$$

$$\pi \not\models a \cup b$$

as  $s_0 \not\models b$  and  $s_1 \not\models a \vee b$

$$\pi \models \diamond b \rightarrow (a \cup b)$$

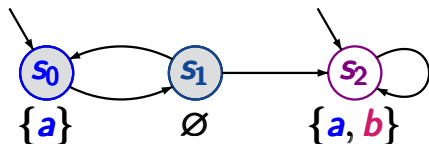
as  $\pi \not\models \diamond b$

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

as  $s_0 \models \neg b$

# Correct or wrong ?

LTLSF3.1-7



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

path  $\pi = s_0 s_1 s_0 s_1 s_0 s_1 \dots$

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

$$\pi \not\models a \cup b$$

as  $s_0 \not\models b$  and  $s_1 \not\models a \vee b$

$$\pi \models \diamond b \rightarrow (a \cup b)$$

as  $\pi \not\models \diamond b$

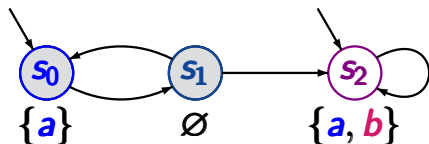
$$\pi \models \bigcirc \bigcirc \neg b$$

as  $s_0 \models \neg b$

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

# Correct or wrong ?

LTLSF3.1-7



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

path  $\pi = s_0 s_1 s_0 s_1 s_0 s_1 \dots$

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

$$\pi \not\models a \cup b$$

as  $s_0 \not\models b$  and  $s_1 \not\models a \vee b$

$$\pi \models \diamond b \rightarrow (a \cup b)$$

as  $\pi \not\models \diamond b$

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

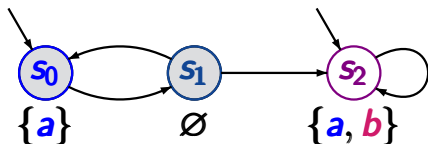
as  $s_0 \models \neg b$

$$\pi \not\models \square a$$

as  $s_1 \not\models a$

# Correct or wrong ?

LTLSF3.1-7



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

path  $\pi = s_0 s_1 s_0 s_1 s_0 s_1 \dots$

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

$$\pi \not\models a \cup b$$

as  $s_0 \not\models b$  and  $s_1 \not\models a \vee b$

$$\pi \models \diamond b \rightarrow (a \cup b)$$

as  $\pi \not\models \diamond b$

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

as  $s_0 \models \neg b$

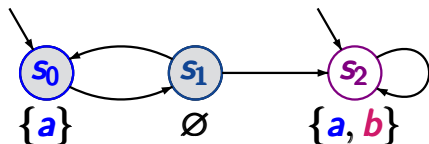
$$\pi \not\models \square a$$

as  $s_1 \not\models a$

$$\pi \models \square \diamond a ?$$

# Correct or wrong ?

LTLSF3.1-7



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

path  $\pi = s_0 s_1 s_0 s_1 s_0 s_1 \dots$

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

$$\pi \not\models a \cup b$$

as  $s_0 \not\models b$  and  $s_1 \not\models a \vee b$

$$\pi \models \diamond b \rightarrow (a \cup b)$$

as  $\pi \not\models \diamond b$

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

as  $s_0 \models \neg b$

$$\pi \not\models \square a$$

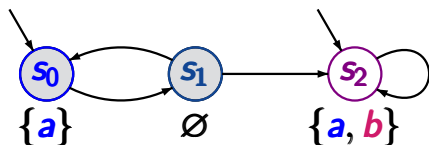
as  $s_1 \not\models a$

$$\pi \models \square \diamond a$$

as  $\square \diamond \hat{=}$  infinitely often

# Correct or wrong ?

LTLSF3.1-7



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

path  $\pi = s_0 s_1 s_0 s_1 s_0 s_1 \dots$

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

$$\pi \not\models a \cup b$$

as  $s_0 \not\models b$  and  $s_1 \not\models a \vee b$

$$\pi \models \diamond b \rightarrow (a \cup b)$$

as  $\pi \not\models \diamond b$

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

as  $s_0 \models \neg b$

$$\pi \not\models \square a$$

as  $s_1 \not\models a$

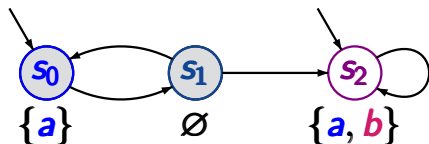
$$\pi \models \square \diamond a$$

as  $\square \diamond \hat{=}$  infinitely often

$$\pi \models \diamond \square a ?$$

# Correct or wrong ?

LTLSF3.1-7



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

path  $\pi = s_0 s_1 s_0 s_1 s_0 s_1 \dots$

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

$$\pi \not\models a \cup b$$

as  $s_0 \not\models b$  and  $s_1 \not\models a \vee b$

$$\pi \models \diamond b \rightarrow (a \cup b)$$

as  $\pi \not\models \diamond b$

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

as  $s_0 \models \neg b$

$$\pi \not\models \square a$$

as  $s_1 \not\models a$

$$\pi \models \square \diamond a$$

as  $\square \diamond \hat{=}$  infinitely often

$$\pi \not\models \diamond \square a$$

as  $\diamond \square \hat{=}$  eventually forever

for  $\sigma = A_0 A_1 A_2 \dots \in (2^{AP})^\omega$ :



for  $\sigma = A_0 A_1 A_2 \dots \in (2^{AP})^\omega$ :

$\sigma \models \Diamond \varphi$  iff there exists  $j \geq 0$  such that

$$A_j A_{j+1} A_{j+2} \dots \models \varphi$$

$\sigma \models \Box \varphi$  iff for all  $j \geq 0$  we have:

$$A_j A_{j+1} A_{j+2} \dots \models \varphi$$

for  $\sigma = A_0 A_1 A_2 \dots \in (2^{AP})^\omega$ :

$\sigma \models \Diamond \varphi$  iff there exists  $j \geq 0$  such that

$$A_j A_{j+1} A_{j+2} \dots \models \varphi$$

$\sigma \models \Box \varphi$  iff for all  $j \geq 0$  we have:

$$A_j A_{j+1} A_{j+2} \dots \models \varphi$$

$\sigma \models \Box \Diamond \varphi$  iff there are infinitely many  $j \geq 0$  s.t.

$$A_j A_{j+1} A_{j+2} \dots \models \varphi$$

for  $\sigma = A_0 A_1 A_2 \dots \in (2^{AP})^\omega$ :

$\sigma \models \Diamond \varphi$  iff there exists  $j \geq 0$  such that

$$A_j A_{j+1} A_{j+2} \dots \models \varphi$$

$\sigma \models \Box \varphi$  iff for all  $j \geq 0$  we have:

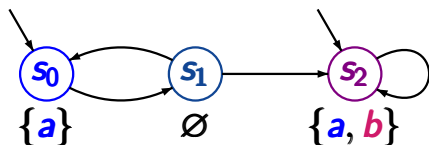
$$A_j A_{j+1} A_{j+2} \dots \models \varphi$$

$\sigma \models \Box \Diamond \varphi$  iff there are infinitely many  $j \geq 0$  s.t.

$$A_j A_{j+1} A_{j+2} \dots \models \varphi$$

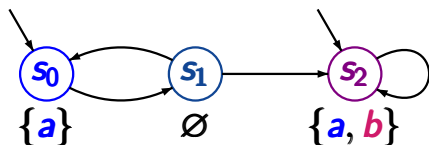
$\sigma \models \Diamond \Box \varphi$  iff for almost all  $j \geq 0$  we have:

$$A_j A_{j+1} A_{j+2} \dots \models \varphi$$



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

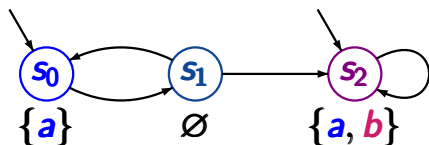
path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$



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

path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$

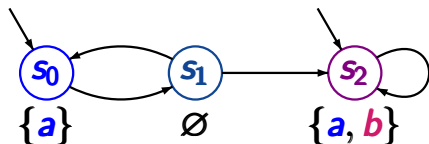
$$trace(\pi) = \{a\} \emptyset \{a, b\}^\omega$$



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

path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$        $trace(\pi) = \{a\} \emptyset \{a, b\}^\omega$

$$\pi \models O((\neg a \wedge \neg b) \cup (a \wedge b)) \quad ?$$



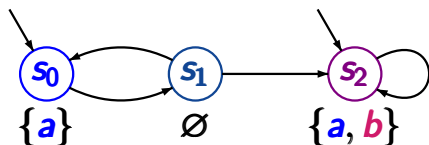
$$AP = \{a, b\}$$

path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$

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

$$\pi \models O((\neg a \wedge \neg b) \cup (a \wedge b)) \quad \text{as } s_1 \models \neg a \wedge \neg b$$

$$s_2 \models a \wedge b$$



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

path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$

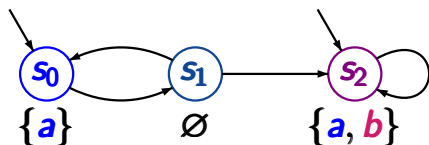
$trace(\pi) = \{a\} \emptyset \{a, b\}^\omega$

$$\pi \models \bigcirc((\neg a \wedge \neg b) \cup (a \wedge b)) \quad \text{as } s_1 \models \neg a \wedge \neg b$$

$$s_2 \models a \wedge b$$

$$\pi \models \bigcirc \square (a \leftrightarrow b) ?$$





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

path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$

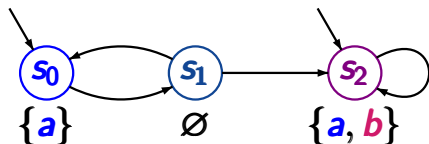
$trace(\pi) = \{a\} \emptyset \{a, b\}^\omega$

$\pi \models \bigcirc((\neg a \wedge \neg b) \cup (a \wedge b))$  as  $s_1 \models \neg a \wedge \neg b$

$s_2 \models a \wedge b$

$\pi \models \bigcirc \square(a \leftrightarrow b)$

as  $s_1, s_2 \models a \leftrightarrow b$



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

path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$

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

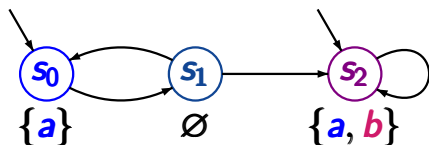
$\pi \models \bigcirc((\neg a \wedge \neg b) \cup (a \wedge b))$  as  $s_1 \models \neg a \wedge \neg b$

$s_2 \models a \wedge b$

$\pi \models \bigcirc \square(a \leftrightarrow b)$

as  $s_1, s_2 \models a \leftrightarrow b$

$\pi \models a \cup (\neg b \cup a) ?$



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

path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$

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

$\pi \models \bigcirc((\neg a \wedge \neg b) \cup (a \wedge b))$  as  $s_1 \models \neg a \wedge \neg b$

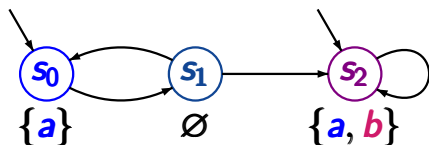
$s_2 \models a \wedge b$

$\pi \models \bigcirc \square (a \leftrightarrow b)$

as  $s_1, s_2 \models a \leftrightarrow b$

$\pi \models a \cup (\neg b \cup a)$

as  $s_0, s_2 \models a, s_1 \models \neg b$



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

path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$

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

$\pi \models \bigcirc((\neg a \wedge \neg b) \cup (a \wedge b))$  as  $s_1 \models \neg a \wedge \neg b$

$s_2 \models a \wedge b$

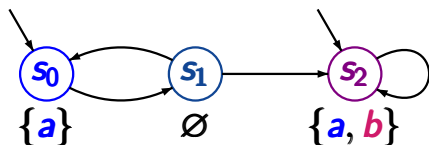
$\pi \models \bigcirc \square(a \leftrightarrow b)$

as  $s_1, s_2 \models a \leftrightarrow b$

$\pi \models a \cup (\neg b \cup a)$

as  $s_0, s_2 \models a, s_1 \models \neg b$

$\pi \models \diamond \square(\neg a \rightarrow \diamond \neg b) ?$



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

path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$

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

$$\pi \models \bigcirc((\neg a \wedge \neg b) \cup (a \wedge b)) \quad \text{as } s_1 \models \neg a \wedge \neg b$$

$$s_2 \models a \wedge b$$

$$\pi \models \bigcirc \square(a \leftrightarrow b)$$

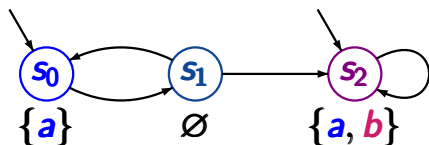
$$\text{as } s_1, s_2 \models a \leftrightarrow b$$

$$\pi \models a \cup (\neg b \cup a)$$

$$\text{as } s_0, s_2 \models a, s_1 \models \neg b$$

$$\pi \models \diamond \square(\neg a \rightarrow \diamond \neg b)$$

$$\text{as } s_2 s_2 s_2 \dots \models \neg a \rightarrow \diamond \neg b$$



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

path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$

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

$$\pi \models \bigcirc((\neg a \wedge \neg b) \cup (a \wedge b)) \quad \text{as } s_1 \models \neg a \wedge \neg b$$

$$s_2 \models a \wedge b$$

$$\pi \models \bigcirc \square (a \leftrightarrow b)$$

$$\text{as } s_1, s_2 \models a \leftrightarrow b$$

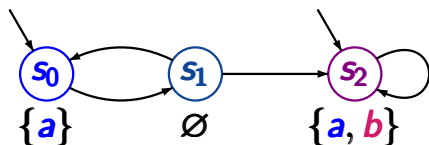
$$\pi \models a \cup (\neg b \cup a)$$

$$\text{as } s_0, s_2 \models a, s_1 \models \neg b$$

$$\pi \models \diamond \square (\neg a \rightarrow \diamond \neg b)$$

$$\text{as } s_2 s_2 s_2 \dots \models \neg a \rightarrow \diamond \neg b$$

$$\pi \models \square (\neg b \rightarrow \bigcirc a) ?$$



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

path  $\pi = s_0 s_1 s_2 s_2 s_2 s_2 \dots$

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

$\pi \models \bigcirc((\neg a \wedge \neg b) \cup (a \wedge b))$  as  $s_1 \models \neg a \wedge \neg b$

$s_2 \models a \wedge b$

$\pi \models \bigcirc \square(a \leftrightarrow b)$

as  $s_1, s_2 \models a \leftrightarrow b$

$\pi \models a \cup (\neg b \cup a)$

as  $s_0, s_2 \models a, s_1 \models \neg b$

$\pi \models \diamond \square(\neg a \rightarrow \diamond \neg b)$

as  $s_2 s_2 s_2 \dots \models \neg a \rightarrow \diamond \neg b$

$\pi \not\models \square(\neg b \rightarrow \bigcirc a)$

as  $s_0 \models \neg b, s_1 \not\models a$

# LTL semantics over the states of a TS

LTLSF3.1-SEM-STATES



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

LTL formula  $\varphi$  over  $AP$

interpretation of  $\varphi$  over infinite path fragments

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

interpretation of  $\varphi$  over states:

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

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

LTL formula  $\varphi$  over  $AP$

interpretation of  $\varphi$  over infinite path fragments

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

interpretation of  $\varphi$  over states:

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

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

LTL formula  $\varphi$  over  $AP$

interpretation of  $\varphi$  over infinite path fragments

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

interpretation of  $\varphi$  over states:

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

↑  
satisfaction relation for LT properties

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

without terminal states

LTL formula  $\varphi$  over  $AP$

interpretation of  $\varphi$  over infinite path fragments

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

interpretation of  $\varphi$  over states:

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

$$\text{iff} \quad s \models \text{Words}(\varphi)$$

$$\text{iff} \quad \text{Traces}(s) \subseteq \text{Words}(\varphi)$$



given: TS  $\mathcal{T} = (\mathcal{S}, Act, \rightarrow, \mathcal{S}_0, AP, L)$

without terminal states

LTL formula  $\varphi$  over  $AP$

$\mathcal{T} \models \varphi$  iff  $s_0 \models \varphi$  for all  $s_0 \in \mathcal{S}_0$

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

without terminal states

LTL formula  $\varphi$  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  $\pi \in Paths(\mathcal{T})$

given: TS  $\mathcal{T} = (\mathcal{S}, Act, \rightarrow, \mathcal{S}_0, AP, L)$

without terminal states

LTL formula  $\varphi$  over  $AP$

$\mathcal{T} \models \varphi$  iff  $s_0 \models \varphi$  for all  $s_0 \in \mathcal{S}_0$   
iff  $trace(\pi) \models \varphi$  for all  $\pi \in Paths(\mathcal{T})$   
iff  $Traces(\mathcal{T}) \subseteq Words(\varphi)$



given: TS  $\mathcal{T} = (\mathcal{S}, Act, \rightarrow, \mathcal{S}_0, AP, L)$   
without terminal states

LTL formula  $\varphi$  over  $AP$

$\mathcal{T} \models \varphi$  iff  $s_0 \models \varphi$  for all  $s_0 \in \mathcal{S}_0$   
iff  $trace(\pi) \models \varphi$  for all  $\pi \in Paths(\mathcal{T})$   
iff  $Traces(\mathcal{T}) \subseteq Words(\varphi)$   
iff  $\mathcal{T} \models Words(\varphi)$

given: TS  $\mathcal{T} = (\mathcal{S}, Act, \rightarrow, \mathcal{S}_0, AP, L)$

without terminal states

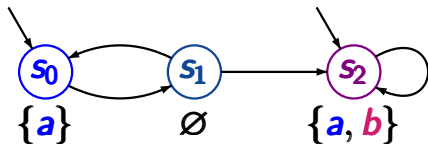
LTL formula  $\varphi$  over  $AP$

$\mathcal{T} \models \varphi$  iff  $s_0 \models \varphi$  for all  $s_0 \in \mathcal{S}_0$   
iff  $trace(\pi) \models \varphi$  for all  $\pi \in Paths(\mathcal{T})$   
iff  $Traces(\mathcal{T}) \subseteq Words(\varphi)$   
iff  $\mathcal{T} \models Words(\varphi)$

↑  
satisfaction relation for LT properties

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

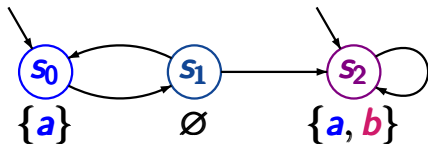
LTLSF3.1-11



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

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

LTLSF3.1-11

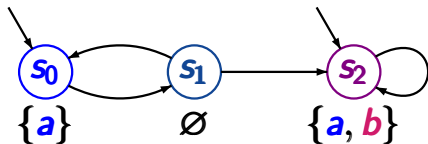


$$AP = \{a, b\}$$

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

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

LTLSF3.1-11



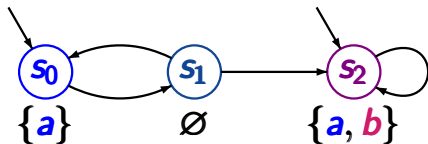
$$AP = \{a, b\}$$

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

$$\text{as } s_0 \models a \text{ and } s_2 \models a$$

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

LTLSF3.1-11



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

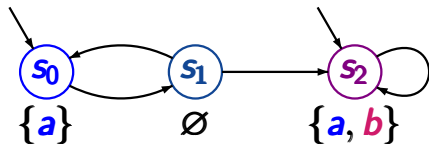
$$\mathcal{T} \models a$$

$$\text{as } s_0 \models a \text{ and } s_2 \models a$$

$$\mathcal{T} \models \diamond \square a$$

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

LTLSF3.1-11



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

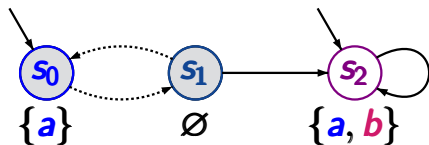
$$\mathcal{T} \models a$$

$$\text{as } s_0 \models a \text{ and } s_2 \models a$$

$$\mathcal{T} \not\models \diamond \square a$$

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

LTLSF3.1-11



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

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

$$\text{as } s_0 \models a \text{ and } s_2 \models a$$

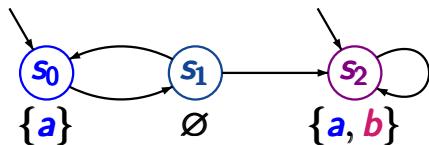
$$\mathcal{T} \not\models \diamond \square a$$

$$\text{as } s_0 s_1 s_0 s_1 \dots \not\models \diamond \square a$$



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

LTLSF3.1-11



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

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

$$\text{as } s_0 \models a \text{ and } s_2 \models a$$

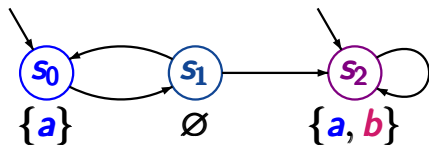
$$\mathcal{T} \not\models \diamond \Box a$$

$$\text{as } s_0 s_1 s_0 s_1 \dots \not\models \diamond \Box a$$

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

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

LTLSF3.1-11



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

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

$$\text{as } s_0 \models a \text{ and } s_2 \models a$$

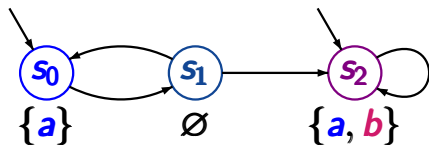
$$\mathcal{T} \not\models \diamond \Box a$$

$$\text{as } s_0 s_1 s_0 s_1 \dots \not\models \diamond \Box a$$

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

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

LTLSF3.1-11



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

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

$$\text{as } s_0 \models a \text{ and } s_2 \models a$$

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

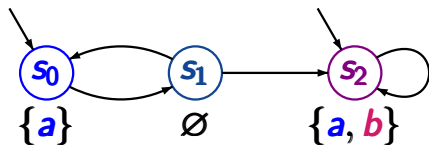
$$\text{as } s_0 s_1 s_0 s_1 \dots \not\models \diamond \Box a$$

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

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

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

LTLSF3.1-11



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

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

as  $s_0 \models a$  and  $s_2 \models a$

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

as  $s_0 s_1 s_0 s_1 \dots \not\models \diamond \Box a$

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

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?

LTLSF3.1-12

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

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

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

# Correct or wrong?

LTLSF3.1-12

For each path  $\pi$  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  $s \models \neg\varphi$

# Correct or wrong?

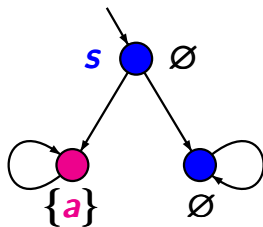
LTLSF3.1-12

For each path  $\pi$  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 over  $AP = \{\text{wait}_1, \text{crit}_1, \text{wait}_2, \text{crit}_2\}$

- the mutual exclusion property

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

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

- the mutual exclusion property

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

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

- the mutual exclusion property

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

- “every process enters the critical section infinitely often”

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

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

- the mutual exclusion property

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

- “every process enters the critical section infinitely often”

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

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

- the mutual exclusion property

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

- “every process enters the critical section infinitely often”

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

- starvation freedom

“every waiting process finally enters its critical section”

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

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

- the mutual exclusion property

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

- “every process enters the critical section infinitely often”

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

- starvation freedom

“every waiting process finally enters its critical section”

$$\varphi_{\text{sf}} = \Box(\text{wait}_1 \rightarrow \Diamond \text{crit}_1) \wedge \Box(\text{wait}_2 \rightarrow \Diamond \text{crit}_2)$$

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

LTLSF3.1-17

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

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



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

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

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

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

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

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

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

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

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

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

$$\cong \text{Words}( \Box(b \vee \bigcirc \neg a) )$$

- set of all words of the form

$$\{b\}^{n_1} \{a\} \{b\}^{n_2} \{a\} \{b\}^{n_3} \{a\} \dots$$

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

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

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

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

$$\cong \text{Words}( \Box( b \vee \bigcirc \neg a ) )$$

- set of all words of the form

$$\{b\}^{n_1} \{a\} \{b\}^{n_2} \{a\} \{b\}^{n_3} \{a\} \dots$$

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

$$\cong \text{Words}( \Box( ( b \wedge \neg a ) \cup ( a \wedge \neg b ) ) )$$



$\varphi_1 \equiv \varphi_2$  iff  $Words(\varphi_1) = Words(\varphi_2)$

$\varphi_1 \equiv \varphi_2$  iff  $Words(\varphi_1) = Words(\varphi_2)$

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

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

$$\begin{aligned} \varphi_1 \equiv \varphi_2 \quad \text{iff} \quad & \mathbf{Words}(\varphi_1) = \mathbf{Words}(\varphi_2) \\ \text{iff for all transition systems } \mathcal{T}: & \\ & \mathcal{T} \models \varphi_1 \iff \mathcal{T} \models \varphi_2 \end{aligned}$$

Examples:

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

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

⋮

all equivalences  
from propositional logic



$$\begin{aligned} \varphi_1 \equiv \varphi_2 \quad \text{iff} \quad & \mathbf{Words}(\varphi_1) = \mathbf{Words}(\varphi_2) \\ \text{iff for all transition systems } \mathcal{T}: & \\ & \mathcal{T} \models \varphi_1 \iff \mathcal{T} \models \varphi_2 \end{aligned}$$

Examples:

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

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

⋮

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

all equivalences  
from propositional logic

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

*Claim:*  $\neg \bigcirc \varphi \equiv \bigcirc \neg \varphi$  “self-duality of next”

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

*Claim:*  $\neg \bigcirc \varphi \equiv \bigcirc \neg \varphi$  “self-duality of next”

*Proof:*  $A_0 A_1 A_2 A_3 \dots \models \neg \bigcirc \varphi$

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

*Claim:*  $\neg \bigcirc \varphi \equiv \bigcirc \neg \varphi$  “self-duality of next”

*Proof:*  $A_0 A_1 A_2 A_3 \dots \models \neg \bigcirc \varphi$

iff  $A_0 A_1 A_2 A_3 \dots \not\models \bigcirc \varphi$

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

*Claim:*  $\neg \bigcirc \varphi \equiv \bigcirc \neg \varphi$  “self-duality of next”

*Proof:*  $A_0 A_1 A_2 A_3 \dots \models \neg \bigcirc \varphi$

iff  $A_0 A_1 A_2 A_3 \dots \not\models \bigcirc \varphi$

iff  $A_1 A_2 A_3 \dots \not\models \varphi$

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

*Claim:*  $\neg \bigcirc \varphi \equiv \bigcirc \neg \varphi$  “self-duality of next”

*Proof:*  $A_0 A_1 A_2 A_3 \dots \models \neg \bigcirc \varphi$

iff  $A_0 A_1 A_2 A_3 \dots \not\models \bigcirc \varphi$

iff  $A_1 A_2 A_3 \dots \not\models \varphi$

iff  $A_1 A_2 A_3 \dots \models \neg \varphi$

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

*Claim:*  $\neg \bigcirc \varphi \equiv \bigcirc \neg \varphi$  “self-duality of next”

*Proof:*

	$A_0 A_1 A_2 A_3 \dots$	$\models$	$\neg \bigcirc \varphi$
iff	$A_0 A_1 A_2 A_3 \dots$	$\not\models$	$\bigcirc \varphi$
iff	$A_1 A_2 A_3 \dots$	$\not\models$	$\varphi$
iff	$A_1 A_2 A_3 \dots$	$\models$	$\neg \varphi$
iff	$A_0 A_1 A_2 A_3 \dots$	$\models$	$\bigcirc \neg \varphi$

# Correct or wrong?

LTLSF3.1-26

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



# Correct or wrong?

LTLSF3.1-26

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

correct

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

correct

---

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

# Correct or wrong?

LTLSF3.1-26

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

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

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

# Correct or wrong?

LTLSF3.1-27

$$\diamond\diamond\psi \equiv \diamond\psi$$

# Correct or wrong?

LTLSF3.1-27

$$\diamond\diamond\varphi \equiv \diamond\varphi$$

**correct**    Analogous:  $\square\square\varphi \equiv \square\varphi$

# Correct or wrong?

LTLSF3.1-27

$$\diamond\diamond\varphi \equiv \diamond\varphi$$

**correct**    Analogous:  $\square\square\varphi \equiv \square\varphi$

---

$$\circ\square\varphi \equiv \square\circ\varphi$$

# Correct or wrong?

LTLSF3.1-27

$$\diamond\diamond\varphi \equiv \diamond\varphi$$

**correct**    Analogous:  $\square\square\varphi \equiv \square\varphi$

---

$$\bigcirc\square\varphi \equiv \square\bigcirc\varphi$$

**correct**



$$\diamond\diamond\varphi \equiv \diamond\varphi$$

correct    Analogous:  $\square\square\varphi \equiv \square\varphi$

---

$$\bigcirc\square\varphi \equiv \square\bigcirc\varphi \stackrel{\text{def}}{=} \psi$$

correct

note that:

$A_0 A_1 A_2 \dots \models \psi$  iff  $A_i A_{i+1} \dots \models \varphi$  for all  $i \geq 1$

# Correct or wrong?

LTLSF3.1-27

$$\diamond\diamond\varphi \equiv \diamond\varphi$$

**correct**    Analogous:  $\square\square\varphi \equiv \square\varphi$

---

$$\bigcirc\square\varphi \equiv \square\bigcirc\varphi$$

**correct**

---

$$\diamond\square\varphi \equiv \square\diamond\varphi$$

# Correct or wrong?

LTLSF3.1-27

$$\diamond\diamond\varphi \equiv \diamond\varphi$$

**correct**    Analogous:  $\square\square\varphi \equiv \square\varphi$

---

$$\bigcirc\square\varphi \equiv \square\bigcirc\varphi$$

**correct**

---

$$\diamond\square\varphi \equiv \square\diamond\varphi$$

$\square\diamond \hat{=}$  infinitely often  
 $\diamond\square \hat{=}$  eventually forever

# Correct or wrong?

LTLSF3.1-27

$$\diamond\diamond\varphi \equiv \diamond\varphi$$

**correct** Analogous:  $\square\square\varphi \equiv \square\varphi$

---

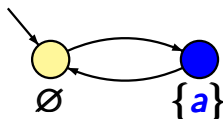
$$\bigcirc\square\varphi \equiv \square\bigcirc\varphi$$

**correct**

---

$$\diamond\square\varphi \equiv \square\diamond\varphi$$

**wrong**



$\square\diamond \hat{=} \text{infinitely often}$

$\diamond\square \hat{=} \text{eventually forever}$

$\models \square\diamond a$

$\not\models \diamond\square a$



until:

$$\varphi \mathbf{U} \psi \equiv \psi \vee (\varphi \wedge \mathbf{O}(\varphi \mathbf{U} \psi))$$

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

eventually:  $\diamond \psi \equiv \psi \vee \mathbf{O} \diamond \psi$

# Expansion laws for U and $\diamond$

LTLSF3.1-28

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

eventually:  $\diamond\psi \equiv \psi \vee \mathbf{O}\diamond\psi$

note:  $\diamond\psi = \mathbf{true} \mathbf{U} \psi$



# Expansion laws for U and $\diamond$

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

eventually:  $\diamond\psi \equiv \psi \vee \mathbf{O}\diamond\psi$

note:  $\diamond\psi = \mathbf{true} \mathbf{U} \psi$   
 $\equiv \psi \vee (\mathbf{true} \wedge \mathbf{O}(\mathbf{true} \mathbf{U} \psi))$

# Expansion laws for U and $\diamond$

LTLSF3.1-28

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

eventually:  $\diamond\psi \equiv \psi \vee \mathbf{O}\diamond\psi$

note:  $\diamond\psi = \mathbf{true} \mathbf{U} \psi$   
 $\equiv \psi \vee (\mathbf{true} \wedge \mathbf{O}(\underbrace{\mathbf{true} \mathbf{U} \psi}_{= \diamond\psi}))$

# Expansion laws for U and $\diamond$

LTLSF3.1-28

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

eventually:  $\diamond\psi \equiv \psi \vee \mathbf{O}\diamond\psi$

note:  $\diamond\psi = \mathbf{true} \mathbf{U} \psi$   
 $\equiv \psi \vee (\mathbf{true} \wedge \mathbf{O}(\underbrace{\mathbf{true} \mathbf{U} \psi}_{= \diamond\psi}))$   
 $\equiv \psi \vee \mathbf{O}\diamond\psi$

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

eventually:  $\diamond \psi \equiv \psi \vee \mathbf{O} \diamond \psi$

always:  $\square \psi \equiv ?$

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

eventually:  $\diamond \psi \equiv \psi \vee \mathbf{O} \diamond \psi$

always:  $\square \psi \equiv \psi \wedge \mathbf{O} \square \psi$

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

eventually:  $\diamond \psi \equiv \psi \vee \mathbf{O} \diamond \psi$

always:  $\square \psi \equiv \psi \wedge \mathbf{O} \square \psi$

$$\square \psi = \neg \diamond \neg \psi$$

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

eventually:  $\diamond \psi \equiv \psi \vee \mathbf{O} \diamond \psi$

always:  $\square \psi \equiv \psi \wedge \mathbf{O} \square \psi$

$$\square \psi = \neg \diamond \neg \psi$$

$$\equiv \neg (\neg \psi \vee \mathbf{O} \diamond \neg \psi) \leftarrow \text{expansion law for } \diamond$$

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

eventually:  $\diamond \psi \equiv \psi \vee \mathbf{O} \diamond \psi$

always:  $\square \psi \equiv \psi \wedge \mathbf{O} \square \psi$

$$\square \psi = \neg \diamond \neg \psi$$

$$\equiv \neg (\neg \psi \vee \mathbf{O} \diamond \neg \psi)$$

$$\equiv \neg \neg \psi \wedge \neg \mathbf{O} \diamond \neg \psi \quad \leftarrow \text{de Morgan}$$



# Expansion laws for U, $\diamond$ and $\square$

LTLSF3.1-29

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

eventually:  $\diamond \psi \equiv \psi \vee \mathbf{O} \diamond \psi$

always:  $\square \psi \equiv \psi \wedge \mathbf{O} \square \psi$

$$\square \psi = \neg \diamond \neg \psi$$

$$\equiv \neg (\neg \psi \vee \mathbf{O} \diamond \neg \psi)$$

$$\equiv \neg \neg \psi \wedge \neg \mathbf{O} \diamond \neg \psi$$

$$\equiv \psi \wedge \neg \mathbf{O} \diamond \neg \psi \quad \leftarrow \text{double negation}$$

# Expansion laws for U, $\diamond$ and $\square$

LTLSF3.1-29

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

eventually:  $\diamond \psi \equiv \psi \vee \mathbf{O} \diamond \psi$

always:  $\square \psi \equiv \psi \wedge \mathbf{O} \square \psi$

$$\square \psi = \neg \diamond \neg \psi$$

$$\equiv \neg (\neg \psi \vee \mathbf{O} \diamond \neg \psi)$$

$$\equiv \neg \neg \psi \wedge \neg \mathbf{O} \diamond \neg \psi$$

$$\equiv \psi \wedge \mathbf{O} \neg \diamond \neg \psi \quad \leftarrow \text{self duality of } \mathbf{O}$$

# Expansion laws for U, $\diamond$ and $\square$

LTLSF3.1-29

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

eventually:  $\diamond \psi \equiv \psi \vee \mathbf{O} \diamond \psi$

always:  $\square \psi \equiv \psi \wedge \mathbf{O} \square \psi$

$$\square \psi = \neg \diamond \neg \psi$$

$$\equiv \neg (\neg \psi \vee \mathbf{O} \diamond \neg \psi)$$

$$\equiv \neg \neg \psi \wedge \neg \mathbf{O} \diamond \neg \psi$$

$$\equiv \psi \wedge \mathbf{O} \neg \diamond \neg \psi$$

$$\equiv \psi \wedge \mathbf{O} \square \psi \quad \leftarrow \text{definition of } \square$$

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

eventually:  $\mathbf{\diamond} \psi \equiv \psi \vee \mathbf{O} \mathbf{\diamond} \psi$

always:  $\mathbf{\square} \psi \equiv \psi \wedge \mathbf{O} \mathbf{\square} \psi$

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

eventually:  $\boxed{\diamond \psi} \equiv \psi \vee \mathbf{O} \boxed{\diamond \psi}$

always:  $\boxed{\square \psi} \equiv \psi \wedge \mathbf{O} \boxed{\square \psi}$

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

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

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

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

$$\mathbf{false} \equiv a \wedge \bigcirc \mathbf{false}$$

$$\boxed{a} \equiv a \wedge \bigcirc \boxed{a}$$

consider

$$\psi = a$$

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

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

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

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

$$\begin{array}{l} \mathbf{false} \equiv a \wedge \bigcirc \mathbf{false} \\ \square a \equiv a \wedge \bigcirc \square a \end{array}$$

although  $\square a \not\equiv \mathbf{false}$

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

least fixed point

eventually:  $\mathbf{\Diamond} \psi \equiv \psi \vee \mathbf{O} \mathbf{\Diamond} \psi$

least fixed point

always:  $\mathbf{\Box} \psi \equiv \psi \wedge \mathbf{O} \mathbf{\Box} \psi$

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

$$\begin{aligned} \mathbf{false} &\equiv a \wedge \mathbf{O} \mathbf{false} \\ \mathbf{\Box} a &\equiv a \wedge \mathbf{O} \mathbf{\Box} a \end{aligned}$$

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



until:  $\varphi \mathbf{U} \psi \equiv \psi \vee (\varphi \wedge \mathbf{O}(\varphi \mathbf{U} \psi))$   
least fixed point

eventually:  $\mathbf{\diamond} \psi \equiv \psi \vee \mathbf{O} \mathbf{\diamond} \psi$   
least fixed point

always:  $\mathbf{\square} \psi \equiv \psi \wedge \mathbf{O} \mathbf{\square} \psi$   
greatest fixed point

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

$$\begin{aligned} \mathbf{false} &\equiv a \wedge \mathbf{O} \mathbf{false} \\ \mathbf{\square} a &\equiv a \wedge \mathbf{O} \mathbf{\square} a \end{aligned}$$

although  
 $\mathbf{\square} a \not\equiv \mathbf{false}$

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

$$\chi \equiv \psi \vee (\varphi \wedge \mathbf{O}\chi)$$

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

$$\chi \equiv \psi \vee (\varphi \wedge \mathbf{O}\chi)$$

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

$$E = \mathbf{Words}(\psi) \cup \{A_0 A_1 A_2 \dots \in \mathbf{Words}(\varphi) : A_1 A_2 \dots \in E\}$$

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

$$\chi \equiv \psi \vee (\varphi \wedge \mathbf{O}\chi)$$

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

$$E = \mathbf{Words}(\psi) \cup \{A_0A_1A_2\dots \in \mathbf{Words}(\varphi) : A_1A_2\dots \in E\}$$

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

$$(1) \quad \mathbf{Words}(\psi) \subseteq E$$

$$(2) \quad \{A_0A_1A_2\dots \in \mathbf{Words}(\varphi) : A_1A_2\dots \in E\} \subseteq E$$

# The weak until operator $W$

LTLSF3.1-WEAKUNTIL

# The weak until operator W

$$\varphi \text{ W } \psi \stackrel{\text{def}}{=} (\varphi \text{ U } \psi) \vee \square \varphi$$

# The weak until operator W

$$\varphi \text{ W } \psi \stackrel{\text{def}}{=} (\varphi \text{ U } \psi) \vee \square\varphi$$

deriving “always” and “until” from “weak until”:

$$\square\varphi \equiv ?$$

# The weak until operator W

$$\varphi \mathbf{W} \psi \stackrel{\text{def}}{=} (\varphi \mathbf{U} \psi) \vee \square\varphi$$

deriving “always” and “until” from “weak until”:

$$\square\varphi \equiv \varphi \mathbf{W} \textit{false}$$



# The weak until operator W

$$\varphi \mathbf{W} \psi \stackrel{\text{def}}{=} (\varphi \mathbf{U} \psi) \vee \square\varphi$$

deriving “always” and “until” from “weak until”:

$$\square\varphi \equiv \varphi \mathbf{W} \textit{false}$$

$$\varphi \mathbf{U} \psi \equiv ?$$

# The weak until operator W

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

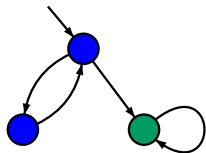
deriving “always” and “until” from “weak until”:

$$\Box \varphi \equiv \varphi \mathbf{W} \textit{false}$$

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

Does  $\mathcal{T} \models aWb$  hold?

LTLSF3.1-32

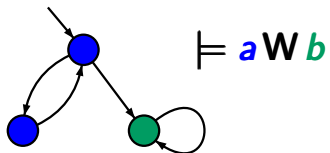


●  $\hat{=} \{a\}$

●  $\hat{=} \{b\}$

Does  $\mathcal{T} \models aWb$  hold?

LTLSF3.1-32

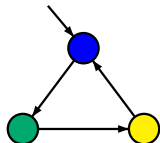
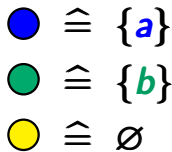
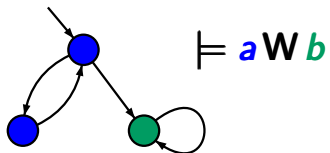


●  $\hat{=} \{a\}$

●  $\hat{=} \{b\}$

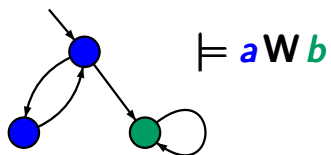
Does  $\mathcal{T} \models aWb$  hold?

LTLSF3.1-32



Does  $\mathcal{T} \models aWb$  hold?

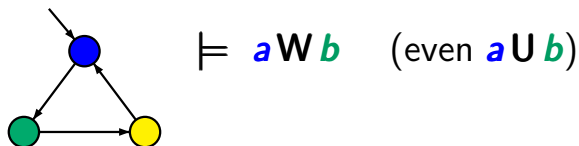
LTLSF3.1-32



●  $\hat{=} \{a\}$

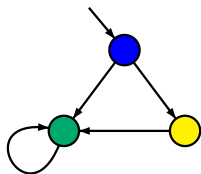
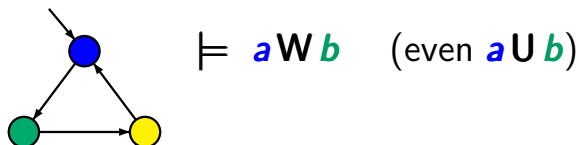
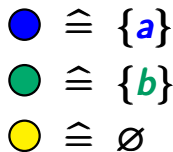
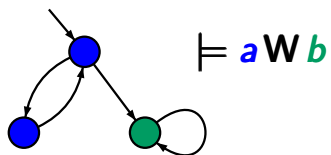
●  $\hat{=} \{b\}$

●  $\hat{=} \emptyset$



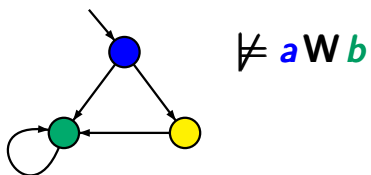
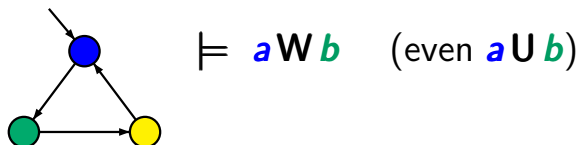
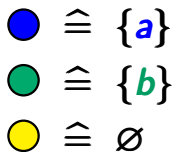
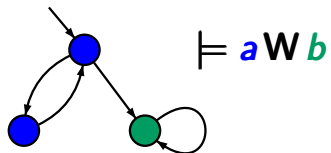
Does  $\mathcal{T} \models aWb$  hold?

LTLSF3.1-32



# Does $\mathcal{T} \models aWb$ hold?

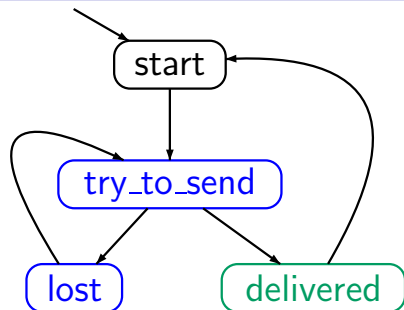
LTLSF3.1-32





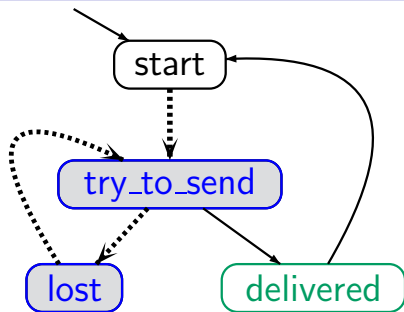
# Example: simple communication protocol

LTLSF3.1-33



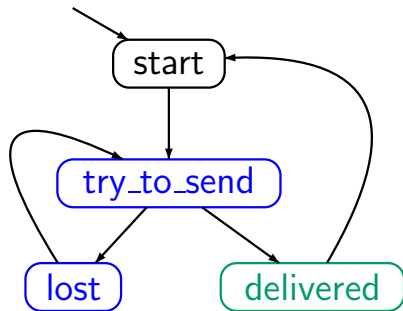
# Example: simple communication protocol

LTLSF3.1-33


$$\mathcal{T} \not\models \square(\text{blue} \longrightarrow \text{blue} \cup \text{delivered})$$

# Example: until versus weak until

LTLSF3.1-33

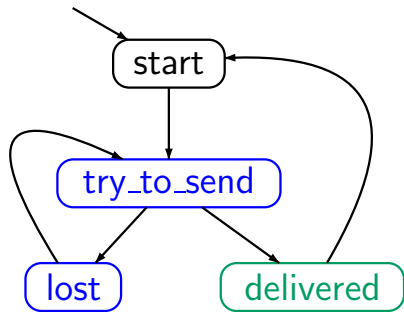


$\mathcal{T} \not\models \square(\text{blue} \longrightarrow \text{blue} \cup \text{delivered})$

$\mathcal{T} \models \square(\text{blue} \longrightarrow \text{blue} \text{W} \text{delivered})$

# Example: until versus weak until

LTLSF3.1-33



constrained liveness:

$$\mathcal{T} \not\models \square(\text{blue} \longrightarrow \text{blue} \cup \text{delivered})$$

safety:

$$\mathcal{T} \models \square(\text{blue} \longrightarrow \text{blue} \text{W} \text{delivered})$$

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

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

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

$$\neg(\varphi \text{ U } \psi)$$

$$\equiv ((\varphi \wedge \neg \psi) \text{ U } (\neg \varphi \wedge \neg \psi)) \vee \Box(\varphi \wedge \neg \psi)$$

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

$$\neg(\varphi \mathbf{U} \psi)$$

$$\equiv ((\varphi \wedge \neg\psi) \mathbf{U} (\neg\varphi \wedge \neg\psi)) \vee \Box(\varphi \wedge \neg\psi)$$

$$\equiv (\varphi \wedge \neg\psi) \mathbf{W} (\neg\varphi \wedge \neg\psi)$$

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

$$\neg(\varphi \mathbf{U} \psi)$$

$$\equiv ((\varphi \wedge \neg\psi) \mathbf{U} (\neg\varphi \wedge \neg\psi)) \vee \Box(\varphi \wedge \neg\psi)$$

$$\equiv (\varphi \wedge \neg\psi) \mathbf{W} (\neg\varphi \wedge \neg\psi)$$

$$\equiv (\neg\psi) \mathbf{W} (\neg\varphi \wedge \neg\psi)$$



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

$$\neg(\varphi \text{ U } \psi)$$

$$\equiv ((\varphi \wedge \neg\psi) \text{ U } (\neg\varphi \wedge \neg\psi)) \vee \Box(\varphi \wedge \neg\psi)$$

$$\equiv (\varphi \wedge \neg\psi) \text{ W } (\neg\varphi \wedge \neg\psi)$$

$$\equiv (\neg\psi) \text{ W } (\neg\varphi \wedge \neg\psi)$$

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

$$\neg(\varphi \text{ W } \psi) \equiv ?$$

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

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

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

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

# Expansion laws for U and W

LTLSF3.1-34

$$\varphi \text{ U } \psi \equiv \psi \vee (\varphi \wedge \text{O}(\varphi \text{ U } \psi))$$

$$\varphi \text{ W } \psi \equiv ?$$

# Expansion laws for U and W

LTLSF3.1-34

$$\varphi \text{ U } \psi \equiv \psi \vee (\varphi \wedge \text{O}(\varphi \text{ U } \psi))$$

$$\varphi \text{ W } \psi \equiv \psi \vee (\varphi \wedge \text{O}(\varphi \text{ W } \psi))$$

# Expansion laws for U and W

LTLSF3.1-34

$$\varphi \text{ U } \psi \equiv \psi \vee (\varphi \wedge \text{O}(\varphi \text{ U } \psi))$$

smallest  
solution

$$\varphi \text{ W } \psi \equiv \psi \vee (\varphi \wedge \text{O}(\varphi \text{ W } \psi))$$

# Expansion laws for U and W

LTLSF3.1-34

$$\varphi \text{ U } \psi \equiv \psi \vee (\varphi \wedge \text{O}(\varphi \text{ U } \psi))$$

smallest  
solution

$$\varphi \text{ W } \psi \equiv \psi \vee (\varphi \wedge \text{O}(\varphi \text{ W } \psi))$$

largest  
solution

$$\varphi \text{ U } \psi \equiv \psi \vee (\varphi \wedge \text{O}(\varphi \text{ U } \psi))$$

smallest  
solution

$$\varphi \text{ W } \psi \equiv \psi \vee (\varphi \wedge \text{O}(\varphi \text{ W } \psi))$$

largest  
solution

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



$$\varphi \text{ U } \psi \equiv \psi \vee (\varphi \wedge \text{O}(\varphi \text{ U } \psi))$$

smallest  
solution

$$\varphi \text{ W } \psi \equiv \psi \vee (\varphi \wedge \text{O}(\varphi \text{ W } \psi))$$

largest  
solution

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

$$(1) \quad \text{Words}(\psi) \subseteq E$$

$$(2) \quad \{A_0 A_1 A_2 \dots \in \text{Words}(\varphi) : A_1 A_2 \dots \in E\} \subseteq E$$

$$\varphi \text{ U } \psi \equiv \psi \vee (\varphi \wedge \text{O}(\varphi \text{ U } \psi))$$

smallest  
solution

$$\varphi \text{ W } \psi \equiv \psi \vee (\varphi \wedge \text{O}(\varphi \text{ W } \psi))$$

largest  
solution

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

$$(1) \quad \text{Words}(\psi) \subseteq E$$

$$(2) \quad \{A_0 A_1 A_2 \dots \in \text{Words}(\varphi) : A_1 A_2 \dots \in E\} \subseteq E$$



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

$$\varphi \text{ U } \psi \equiv \psi \vee (\varphi \wedge \text{O}(\varphi \text{ U } \psi))$$

smallest  
solution

$$\varphi \text{ W } \psi \equiv \psi \vee (\varphi \wedge \text{O}(\varphi \text{ W } \psi))$$

largest  
solution

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

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

$$\varphi \text{ U } \psi \equiv \psi \vee (\varphi \wedge \text{O}(\varphi \text{ U } \psi)) \quad \text{smallest solution}$$

$$\varphi \text{ W } \psi \equiv \psi \vee (\varphi \wedge \text{O}(\varphi \text{ W } \psi)) \quad \text{largest solution}$$

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

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

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

$$\varphi \text{ U } \psi \equiv \psi \vee (\varphi \wedge \text{O}(\varphi \text{ U } \psi)) \quad \text{smallest solution}$$

$$\varphi \text{ W } \psi \equiv \psi \vee (\varphi \wedge \text{O}(\varphi \text{ W } \psi)) \quad \text{largest solution}$$

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

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

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

$$\text{Words}(\psi) \cup \{A_0 A_1 A_2 \dots \in \text{Words}(\varphi) : A_1 A_2 \dots \in E\} \supseteq E$$

$$\varphi \text{ U } \psi \equiv \psi \vee (\varphi \wedge \text{O}(\varphi \text{ U } \psi)) \quad \text{smallest solution}$$

$$\varphi \text{ W } \psi \equiv \psi \vee (\varphi \wedge \text{O}(\varphi \text{ W } \psi)) \quad \text{largest solution}$$

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

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

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

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

$$\varphi \mathbf{U} \psi \equiv \psi \vee (\varphi \wedge \mathbf{O}(\varphi \mathbf{U} \psi))$$

smallest solution

---

$$\varphi \mathbf{W} \psi \equiv \psi \vee (\varphi \wedge \mathbf{O}(\varphi \mathbf{W} \psi))$$

largest solution

$$\varphi \mathbf{U} \psi \equiv \psi \vee (\varphi \wedge \mathbf{O}(\varphi \mathbf{U} \psi))$$

smallest solution

$$\diamond \psi \equiv \psi \vee \mathbf{O} \diamond \psi$$

smallest solution

$$\varphi \mathbf{W} \psi \equiv \psi \vee (\varphi \wedge \mathbf{O}(\varphi \mathbf{W} \psi))$$

largest solution

$$\square \varphi \equiv \varphi \wedge \mathbf{O} \square \varphi$$

largest solution

remind:  $\diamond \psi = \mathbf{true} \mathbf{U} \psi$ ,  $\square \varphi \equiv \varphi \mathbf{W} \mathbf{false}$





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

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

syntax of propositional formulas in PNF:

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

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

syntax of propositional formulas in PNF:

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

$$\neg \text{true} \equiv \text{false}$$

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)

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

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

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

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

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

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

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

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

$$\varphi ::= \text{true} \mid \text{false} \mid a \mid \neg a \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid$$
$$\bigcirc \varphi \leftarrow \text{no new operator needed for } \neg \bigcirc$$

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

$$\neg \bigcirc \varphi \equiv \bigcirc \neg \varphi \quad \text{self-duality of the next operator}$$



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

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

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

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

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

$$\varphi ::= \text{true} \mid \text{false} \mid a \mid \neg a \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \\ \bigcirc \varphi \mid \varphi_1 \mathbf{U} \varphi_2 \mid \varphi_1 \mathbf{W} \varphi_2$$

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

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

$\neg(\varphi_1 \mathbf{U} \varphi_2) \equiv (\neg \varphi_2) \mathbf{W}(\neg \varphi_1 \wedge \neg \varphi_2)$

duality of  $\mathbf{U}$  and  $\mathbf{W}$

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

$$\varphi ::= \text{true} \mid \text{false} \mid a \mid \neg a \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \\ \bigcirc \varphi \mid \varphi_1 \text{ U } \varphi_2 \mid \varphi_1 \text{ W } \varphi_2 \mid \diamond \varphi \mid \square \varphi$$

$\diamond$  and  $\square$  can (still) be derived:

$$\diamond \varphi \stackrel{\text{def}}{=} \text{true U } \varphi$$

$$\square \varphi \stackrel{\text{def}}{=} \varphi \text{ W } \text{false}$$



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  $\varphi'$   
by successive application of the following rules:

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

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

$$\begin{array}{ll} \neg \text{true} & \rightsquigarrow \text{false} \\ \neg \neg \varphi & \rightsquigarrow \varphi \\ \neg(\varphi_1 \wedge \varphi_2) & \rightsquigarrow \neg \varphi_1 \vee \neg \varphi_2 \\ \neg \bigcirc \varphi & \rightsquigarrow \bigcirc \neg \varphi \\ \neg(\varphi_1 \text{ U } \varphi_2) & \rightsquigarrow (\neg \varphi_2) \text{ W } (\neg \varphi_1 \wedge \neg \varphi_2) \end{array}$$



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

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

$$\begin{aligned}\neg \mathit{true} &\rightsquigarrow \mathit{false} \\ \neg \neg \varphi &\rightsquigarrow \varphi \\ \neg(\varphi_1 \wedge \varphi_2) &\rightsquigarrow \neg \varphi_1 \vee \neg \varphi_2 \\ \neg \bigcirc \varphi &\rightsquigarrow \bigcirc \neg \varphi \\ \neg(\varphi_1 \mathbf{U} \varphi_2) &\rightsquigarrow (\neg \varphi_2) \mathbf{W}(\neg \varphi_1 \wedge \neg \varphi_2)\end{aligned}$$

exponential-blow up is possible

$\neg \text{true}$	$\rightsquigarrow$	$\text{false}$
$\neg \neg \varphi$	$\rightsquigarrow$	$\varphi$
$\neg(\varphi_1 \wedge \varphi_2)$	$\rightsquigarrow$	$\neg \varphi_1 \vee \neg \varphi_2$
$\neg \bigcirc \varphi$	$\rightsquigarrow$	$\bigcirc \neg \varphi$
$\neg(\varphi_1 \text{ U } \varphi_2)$	$\rightsquigarrow$	$(\neg \varphi_2) \text{ W } (\neg \varphi_1 \wedge \neg \varphi_2)$

$\neg \text{true}$	$\rightsquigarrow$	$\text{false}$	+ analogue rule for $\neg \text{false}$
$\neg \neg \varphi$	$\rightsquigarrow$	$\varphi$	
$\neg(\varphi_1 \wedge \varphi_2)$	$\rightsquigarrow$	$\neg \varphi_1 \vee \neg \varphi_2$	+ analogue rule for $\neg \vee$
$\neg \bigcirc \varphi$	$\rightsquigarrow$	$\bigcirc \neg \varphi$	
$\neg(\varphi_1 \text{ U } \varphi_2)$	$\rightsquigarrow$	$(\neg \varphi_2) \text{ W } (\neg \varphi_1 \wedge \neg \varphi_2)$	

$\neg \text{true}$	$\rightsquigarrow$	$\text{false}$	+ analogue rule for $\neg \text{false}$
$\neg \neg \varphi$	$\rightsquigarrow$	$\varphi$	
$\neg(\varphi_1 \wedge \varphi_2)$	$\rightsquigarrow$	$\neg \varphi_1 \vee \neg \varphi_2$	+ analogue rule for $\neg \vee$
$\neg \bigcirc \varphi$	$\rightsquigarrow$	$\bigcirc \neg \varphi$	
$\neg(\varphi_1 \text{ U } \varphi_2)$	$\rightsquigarrow$	$(\neg \varphi_2) \text{ W } (\neg \varphi_1 \wedge \neg \varphi_2)$	
$\neg \diamond \varphi$	$\rightsquigarrow$	$\square \neg \varphi$	$\neg \square \varphi \rightsquigarrow \diamond \neg \varphi$

$\neg \text{true}$	$\rightsquigarrow$	$\text{false}$	+ analogue rule for $\neg \text{false}$
$\neg \neg \varphi$	$\rightsquigarrow$	$\varphi$	
$\neg(\varphi_1 \wedge \varphi_2)$	$\rightsquigarrow$	$\neg \varphi_1 \vee \neg \varphi_2$	+ analogue rule for $\neg \vee$
$\neg \bigcirc \varphi$	$\rightsquigarrow$	$\bigcirc \neg \varphi$	
$\neg(\varphi_1 \text{U} \varphi_2)$	$\rightsquigarrow$	$(\neg \varphi_2) \text{W}(\neg \varphi_1 \wedge \neg \varphi_2)$	
$\neg \diamond \varphi$	$\rightsquigarrow$	$\square \neg \varphi$	$\neg \square \varphi \rightsquigarrow \diamond \neg \varphi$

$$\neg \square((a \text{U} b) \vee \bigcirc c)$$

$\neg \text{true}$	$\rightsquigarrow$	$\text{false}$	+ analogue rule for $\neg \text{false}$
$\neg \neg \varphi$	$\rightsquigarrow$	$\varphi$	
$\neg(\varphi_1 \wedge \varphi_2)$	$\rightsquigarrow$	$\neg \varphi_1 \vee \neg \varphi_2$	+ analogue rule for $\neg \vee$
$\neg \bigcirc \varphi$	$\rightsquigarrow$	$\bigcirc \neg \varphi$	
$\neg(\varphi_1 \text{U} \varphi_2)$	$\rightsquigarrow$	$(\neg \varphi_2) \text{W}(\neg \varphi_1 \wedge \neg \varphi_2)$	
$\neg \diamond \varphi$	$\rightsquigarrow$	$\square \neg \varphi$	$\neg \square \varphi \rightsquigarrow \diamond \neg \varphi$

$$\neg \square((a \text{U} b) \vee \bigcirc c)$$

$$\equiv \diamond \neg((a \text{U} b) \vee \bigcirc c)$$

← duality of  $\diamond$  and  $\square$

$\neg \text{true}$	$\rightsquigarrow$	$\text{false}$	+ analogue rule for $\neg \text{false}$
$\neg \neg \varphi$	$\rightsquigarrow$	$\varphi$	
$\neg(\varphi_1 \wedge \varphi_2)$	$\rightsquigarrow$	$\neg \varphi_1 \vee \neg \varphi_2$	+ analogue rule for $\neg \vee$
$\neg \bigcirc \varphi$	$\rightsquigarrow$	$\bigcirc \neg \varphi$	
$\neg(\varphi_1 \text{U} \varphi_2)$	$\rightsquigarrow$	$(\neg \varphi_2) \text{W}(\neg \varphi_1 \wedge \neg \varphi_2)$	
$\neg \diamond \varphi$	$\rightsquigarrow$	$\square \neg \varphi$	$\neg \square \varphi \rightsquigarrow \diamond \neg \varphi$

$$\neg \square((a \text{U} b) \vee \bigcirc c)$$

$$\equiv \diamond \neg((a \text{U} b) \vee \bigcirc c)$$

$$\equiv \diamond(\neg(a \text{U} b) \wedge \neg \bigcirc c)$$

← duality of  $\diamond$  and  $\square$

← duality of  $\wedge$  and  $\vee$

$\neg \text{true}$	$\rightsquigarrow$	$\text{false}$	+ analogue rule for $\neg \text{false}$
$\neg \neg \varphi$	$\rightsquigarrow$	$\varphi$	
$\neg(\varphi_1 \wedge \varphi_2)$	$\rightsquigarrow$	$\neg \varphi_1 \vee \neg \varphi_2$	+ analogue rule for $\neg \vee$
$\neg \bigcirc \varphi$	$\rightsquigarrow$	$\bigcirc \neg \varphi$	
$\neg(\varphi_1 \text{U} \varphi_2)$	$\rightsquigarrow$	$(\neg \varphi_2) \text{W}(\neg \varphi_1 \wedge \neg \varphi_2)$	
$\neg \diamond \varphi$	$\rightsquigarrow$	$\square \neg \varphi$	$\neg \square \varphi \rightsquigarrow \diamond \neg \varphi$

$$\neg \square((a \text{U} b) \vee \bigcirc c)$$

$$\equiv \diamond \neg((a \text{U} b) \vee \bigcirc c)$$

$$\equiv \diamond(\neg(a \text{U} b) \wedge \neg \bigcirc c)$$

$$\equiv \diamond(\neg(a \text{U} b) \wedge \bigcirc \neg c)$$

← duality of  $\diamond$  and  $\square$

← duality of  $\wedge$  and  $\vee$

← self-duality of  $\bigcirc$



$\neg \text{true}$	$\rightsquigarrow$	$\text{false}$	+ analogue rule for $\neg \text{false}$
$\neg \neg \varphi$	$\rightsquigarrow$	$\varphi$	
$\neg(\varphi_1 \wedge \varphi_2)$	$\rightsquigarrow$	$\neg \varphi_1 \vee \neg \varphi_2$	+ analogue rule for $\neg \vee$
$\neg \bigcirc \varphi$	$\rightsquigarrow$	$\bigcirc \neg \varphi$	
$\neg(\varphi_1 \text{U} \varphi_2)$	$\rightsquigarrow$	$(\neg \varphi_2) \text{W}(\neg \varphi_1 \wedge \neg \varphi_2)$	
$\neg \diamond \varphi$	$\rightsquigarrow$	$\square \neg \varphi$	$\neg \square \varphi \rightsquigarrow \diamond \neg \varphi$

$$\neg \square((a \text{U} b) \vee \bigcirc c)$$

$$\equiv \diamond \neg((a \text{U} b) \vee \bigcirc c)$$

← duality of  $\diamond$  and  $\square$

$$\equiv \diamond(\neg(a \text{U} b) \wedge \neg \bigcirc c)$$

← duality of  $\wedge$  and  $\vee$

$$\equiv \diamond((\neg b) \text{W}(\neg a \wedge \neg b) \wedge \bigcirc \neg c)$$

← duality of **U** and **W**

$\neg \text{true}$	$\rightsquigarrow$	$\text{false}$	+ analogue rule for $\neg \text{false}$
$\neg \neg \varphi$	$\rightsquigarrow$	$\varphi$	
$\neg(\varphi_1 \wedge \varphi_2)$	$\rightsquigarrow$	$\neg \varphi_1 \vee \neg \varphi_2$	+ analogue rule for $\neg \vee$
$\neg \bigcirc \varphi$	$\rightsquigarrow$	$\bigcirc \neg \varphi$	
$\neg(\varphi_1 \text{U} \varphi_2)$	$\rightsquigarrow$	$(\neg \varphi_2) \text{W}(\neg \varphi_1 \wedge \neg \varphi_2)$	
$\neg \diamond \varphi$	$\rightsquigarrow$	$\square \neg \varphi$	$\neg \square \varphi \rightsquigarrow \diamond \neg \varphi$

$$\neg \square((a \text{U} b) \vee \bigcirc c)$$

$$\equiv \diamond \neg((a \text{U} b) \vee \bigcirc c)$$

$$\equiv \diamond(\neg(a \text{U} b) \wedge \neg \bigcirc c)$$

$$\equiv \diamond((\neg b) \text{W}(\neg a \wedge \neg b) \wedge \bigcirc \neg c) \longleftarrow \text{PNF}$$



# Recall: action-based fairness

LTLSF3.1-38

fairness assumption for TS  $\mathcal{T} = (\mathcal{S}, \text{Act}, \rightarrow, \mathcal{S}_0, \text{AP}, L)$ :

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

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

$\mathcal{F}_{ucond}$  unconditional fairness assumption

$\mathcal{F}_{strong}$  strong fairness assumption

$\mathcal{F}_{weak}$  weak fairness assumption

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

fairness assumption for TS  $\mathcal{T} = (\mathcal{S}, \text{Act}, \rightarrow, \mathcal{S}_0, \text{AP}, L)$ :

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

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

execution  $\mathcal{S}_0 \xrightarrow{\alpha_1} \mathcal{S}_1 \xrightarrow{\alpha_2} \mathcal{S}_2 \xrightarrow{\alpha_3} \dots$   $\mathcal{F}$ -fair if

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

fairness assumption for TS  $\mathcal{T} = (\mathcal{S}, \text{Act}, \rightarrow, \mathcal{S}_0, \text{AP}, L)$ :

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

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

execution  $\mathcal{S}_0 \xrightarrow{\alpha_1} \mathcal{S}_1 \xrightarrow{\alpha_2} \mathcal{S}_2 \xrightarrow{\alpha_3} \dots$   $\mathcal{F}$ -fair if

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

$$\exists^{\infty} i \geq 1. A \cap \text{Act}(\mathcal{S}_i) \neq \emptyset \implies \exists^{\infty} i \geq 1. \alpha_i \in A$$



fairness assumption for TS  $\mathcal{T} = (\mathcal{S}, \text{Act}, \rightarrow, \mathcal{S}_0, AP, L)$ :

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

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

execution  $\mathcal{S}_0 \xrightarrow{\alpha_1} \mathcal{S}_1 \xrightarrow{\alpha_2} \mathcal{S}_2 \xrightarrow{\alpha_3} \dots$   $\mathcal{F}$ -fair if

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

$$\exists i \geq 1. A \cap \text{Act}(\mathcal{S}_i) \neq \emptyset \implies \exists i \geq 1. \alpha_i \in A$$
- for all  $A \in \mathcal{F}_{\text{weak}}$ :  

$$\forall i \geq 1. A \cap \text{Act}(\mathcal{S}_i) \neq \emptyset \implies \exists i \geq 1. \alpha_i \in A$$

fairness assumption for TS  $\mathcal{T} = (\mathcal{S}, \text{Act}, \rightarrow, \mathcal{S}_0, AP, L)$ :

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

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

satisfaction relation for LT-properties under fairness:

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



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

eventually  $\diamond\varphi \stackrel{\text{def}}{=} \mathit{true} \mathbf{U}\varphi$

always  $\square\varphi \stackrel{\text{def}}{=} \neg\diamond\neg\varphi$

infinitely often  $\square\diamond\varphi$

eventually forever  $\diamond\square\varphi$

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

eventually  $\diamond \varphi \stackrel{\text{def}}{=} \mathbf{true} \mathbf{U} \varphi$

always  $\square \varphi \stackrel{\text{def}}{=} \neg \diamond \neg \varphi$

infinitely often  $\square \diamond \varphi$

eventually forever  $\diamond \square \varphi$

e.g., unconditional fairness  $\square \diamond \mathbf{crit}_i$

strong fairness  $\square \diamond \mathbf{wait}_i \rightarrow \square \diamond \mathbf{crit}_i$

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

eventually  $\diamond \varphi \stackrel{\text{def}}{=} \mathbf{true} \mathbf{U} \varphi$

always  $\square \varphi \stackrel{\text{def}}{=} \neg \diamond \neg \varphi$

infinitely often  $\square \diamond \varphi$

eventually forever  $\diamond \square \varphi$

e.g., unconditional fairness  $\square \diamond \mathbf{crit}_i$

strong fairness  $\square \diamond \mathbf{wait}_i \rightarrow \square \diamond \mathbf{crit}_i$

weak fairness  $\diamond \square \mathbf{wait}_i \rightarrow \square \diamond \mathbf{crit}_i$



... 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  $\phi_1, \phi_2, \phi$  are propositional formulas



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

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

where  $\phi_1, \phi_2, \phi$  are propositional formulas

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

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

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

where  $\phi_1, \phi_2, \phi$  are propositional formulas

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

$s \models_{\text{fair}} \varphi$  iff for all  $\pi \in \text{Paths}(s)$ :  
if  $\pi \models_{\text{fair}}$  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  $\Diamond\Box\phi_1 \rightarrow \Box\Diamond\phi_2$

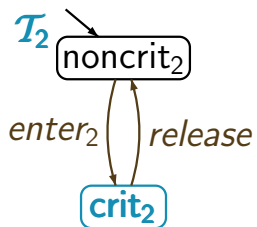
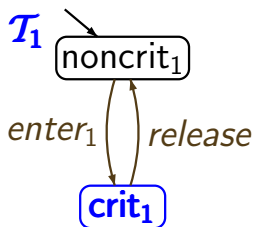
where  $\phi_1, \phi_2, \phi$  are propositional formulas

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

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

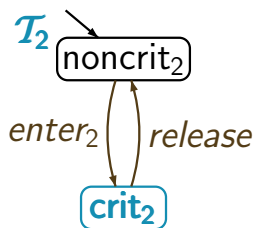
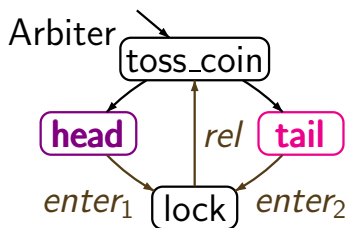
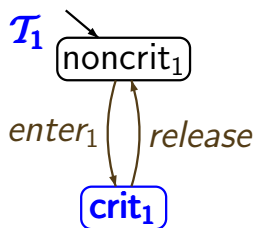
# Randomized arbiter for MUTEX

LTLSF3.1-40



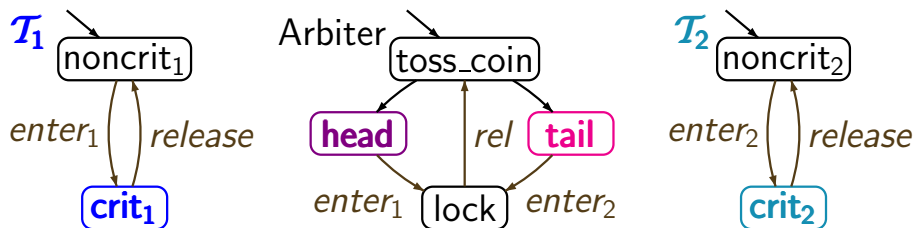
# Randomized arbiter for MUTEX

LTLSF3.1-40

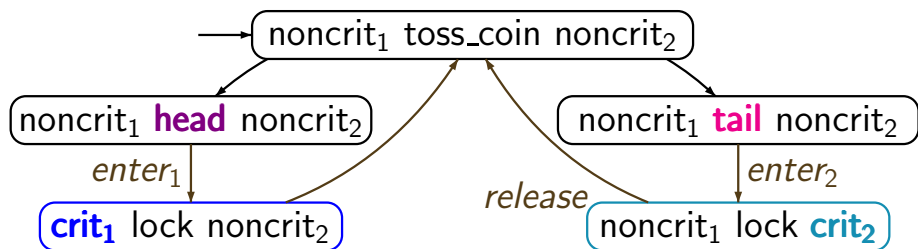


# Randomized arbiter for MUTEX

LTLSF3.1-40

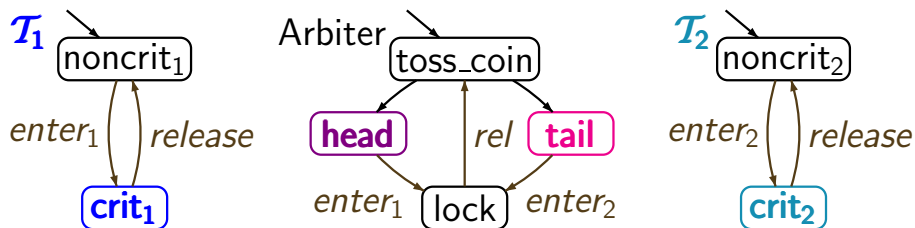


$(\mathcal{T}_1 \parallel \mathcal{T}_2) \parallel \text{Arbiter}$

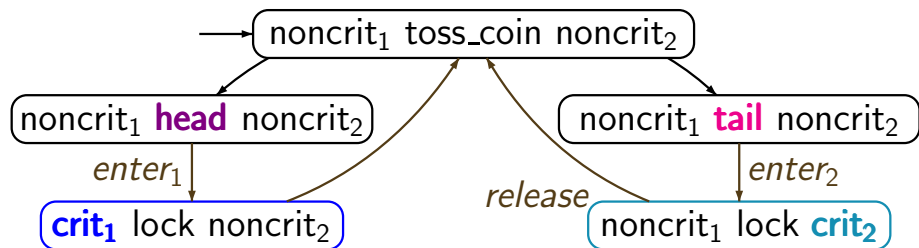


# Randomized arbiter for MUTEX

LTLSF3.1-40

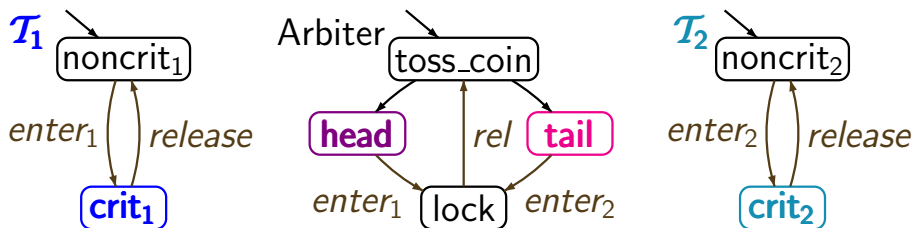


$$(\mathcal{T}_1 \parallel \mathcal{T}_2) \parallel \text{Arbiter} \not\models \square \diamond \text{crit}_1 \wedge \square \diamond \text{crit}_2$$



# Randomized arbiter for MUTEX

LTLSF3.1-40



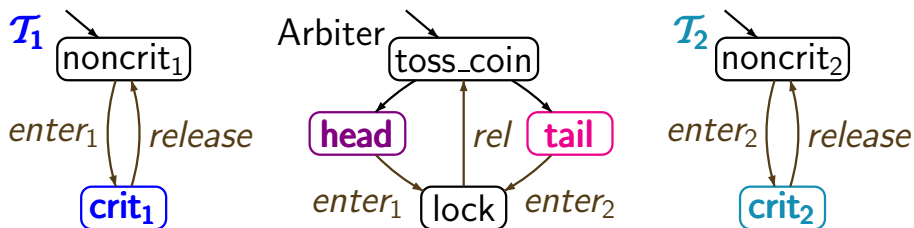
unconditional LTL-fairness:

$$\text{fair} = \square \diamond \text{head} \wedge \square \diamond \text{tail}$$



# Randomized arbiter for MUTEX

LTLSF3.1-40



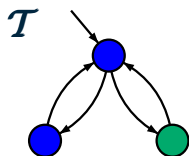
unconditional LTL-fairness:

$$fair = \square \diamond head \wedge \square \diamond tail$$

$$(\mathcal{T}_1 \parallel \mathcal{T}_2) \parallel Arbiter \models_{fair} \square \diamond crit_1 \wedge \square \diamond crit_2$$

# Correct or wrong?

LTLSF3.1-41

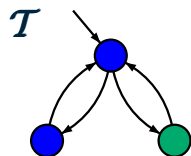


LTL fairness assumption  
*fair* =  $\diamond \Box a \rightarrow \Box \diamond b$

●  $\hat{=}\{a\}$  ●  $\hat{=}\{b\}$

# Correct or wrong?

LTLSF3.1-41



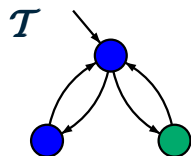
LTL fairness assumption  
 $fair = \diamond \Box a \rightarrow \Box \diamond b$

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

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

# Correct or wrong?

LTLSF3.1-41



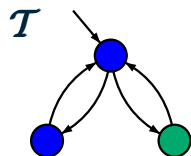
LTL fairness assumption  
*fair* =  $\diamond \Box a \rightarrow \Box \diamond b$

$\bullet \hat{=} \{a\}$     $\bullet \hat{=} \{b\}$

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

# Correct or wrong?

LTLSF3.1-41



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

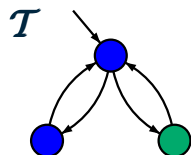
$\bullet \hat{=} \{a\}$     $\bullet \hat{=} \{b\}$

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

$\mathcal{T} \models_{fair} a \cup b$  ?

# Correct or wrong?

LTLSF3.1-41



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

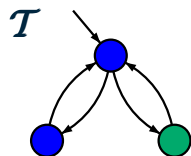
●  $\hat{=} \{a\}$    ●  $\hat{=} \{b\}$

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

$\mathcal{T} \models_{fair} a \cup b$  ✓

# Correct or wrong?

LTLSF3.1-41



LTL fairness assumption  
*fair* =  $\diamond \Box a \rightarrow \Box \diamond b$

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

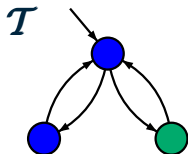
$\mathcal{T} \not\models_{\text{fair}} \bigcirc b$  as ●  $\rightarrow$  ●  $\rightarrow$  ●  $\rightarrow$  ●  $\rightarrow$  ●  $\rightarrow$  ●  $\rightarrow$  ... is fair

$\mathcal{T} \models_{\text{fair}} a \cup b$  ✓

$\mathcal{T} \models_{\text{fair}} a \cup \Box (b \leftrightarrow \bigcirc a)$  ?

# Correct or wrong?

LTLSF3.1-41



LTL fairness assumption  
*fair* =  $\diamond \Box a \rightarrow \Box \diamond b$

$\bullet \hat{=} \{a\}$     $\bullet \hat{=} \{b\}$

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

$\mathcal{T} \models_{\text{fair}} a \cup b$   $\checkmark$

$\mathcal{T} \not\models_{\text{fair}} a \cup \Box (b \leftrightarrow \bigcirc a)$

as  $\bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \dots$  is fair



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

$$\mathcal{I}_{sem} \not\models \square \diamond crit_1 \wedge \square \diamond crit_2$$

$$\mathcal{I}_{sem} \models_{fair} \square \diamond crit_1 \wedge \square \diamond crit_2$$

for appropriate fairness condition

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

$$\mathcal{T}_{sem} \not\models \square \diamond crit_1 \wedge \square \diamond crit_2$$

$$\mathcal{T}_{sem} \models_{fair} \square \diamond crit_1 \wedge \square \diamond crit_2$$

for appropriate fairness condition, e.g.,

$$fair = \bigwedge_{i=1,2} ((\square \diamond wait_i \rightarrow \square \diamond crit_i) \wedge (\diamond \square noncrit_i \rightarrow \square \diamond wait_i))$$

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

$$\mathcal{T}_{sem} \not\models \square \diamond crit_1 \wedge \square \diamond crit_2$$

$$\mathcal{T}_{sem} \models_{fair} \square \diamond crit_1 \wedge \square \diamond crit_2$$

for appropriate fairness condition

- can be verifiable system properties

e.g., Peterson algorithm guarantees strong fairness

$$\mathcal{T}_{Pet} \models \square \diamond wait_1 \rightarrow \square \diamond crit_1$$

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

$$\mathcal{T}_{sem} \not\models \square\lozenge crit_1 \wedge \square\lozenge crit_2$$

$$\mathcal{T}_{sem} \models_{fair} \square\lozenge crit_1 \wedge \square\lozenge crit_2$$

for appropriate fairness condition

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

$$\mathcal{T}_{Pet} \models \square\lozenge wait_1 \rightarrow \square\lozenge crit_1$$

- 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

Each strong **LTL** fairness assumption

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

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

Each strong **LTL** fairness assumption

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

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

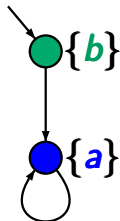
*recall:* a fairness condition is called **realizable**  
if for each reachable state **s** there exists  
a fair path starting in **s**

Each strong **LTL** fairness assumption

$$\textit{fair} = \Box\Diamond a \rightarrow \Box\Diamond b$$

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

**wrong**



$$\textit{fair} = \Box\Diamond a \rightarrow \Box\Diamond b$$

is not realizable

# Action-based fairness $\rightsquigarrow$ LTL-fairness

LTLSF3.1-43



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

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

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

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

$$\begin{aligned} \mathit{enabled}(A) \in L(s) & \text{ iff } s \xrightarrow{\alpha} \dots \text{ for some } \alpha \in A \\ \mathit{taken}(A) \in L(s) & \text{ iff for all transitions } \dots \xrightarrow{\alpha} s: \\ & \alpha \in A \end{aligned}$$

- 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:  $\Diamond \Box \mathit{enabled}(A) \rightarrow \Box \Diamond \mathit{taken}(A)$

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

$$\begin{aligned} \text{enabled}(A) \in L(s) & \text{ iff } s \xrightarrow{\alpha} \dots \text{ for some } \alpha \in A \\ \text{taken}(A) \in L(s) & \text{ iff for } \boxed{\text{all}} \text{ transitions } \dots \xrightarrow{\alpha} s: \\ & \alpha \in A \end{aligned}$$

**problem:** each state **s** can have several incoming transitions

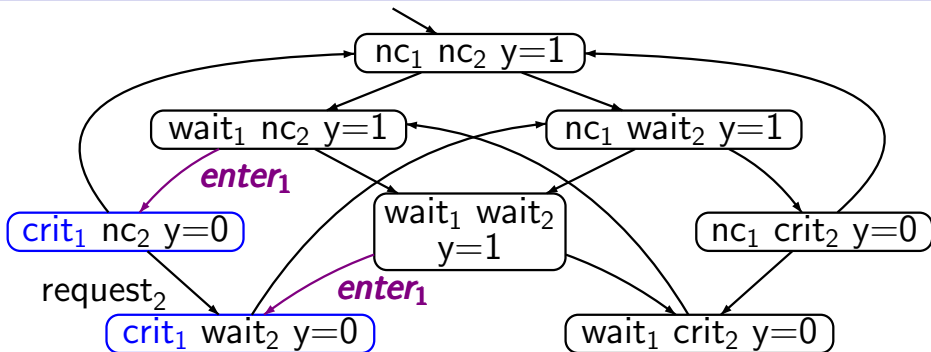
$$t \xrightarrow{\alpha} s, \quad u \xrightarrow{\beta} s, \quad \dots$$

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

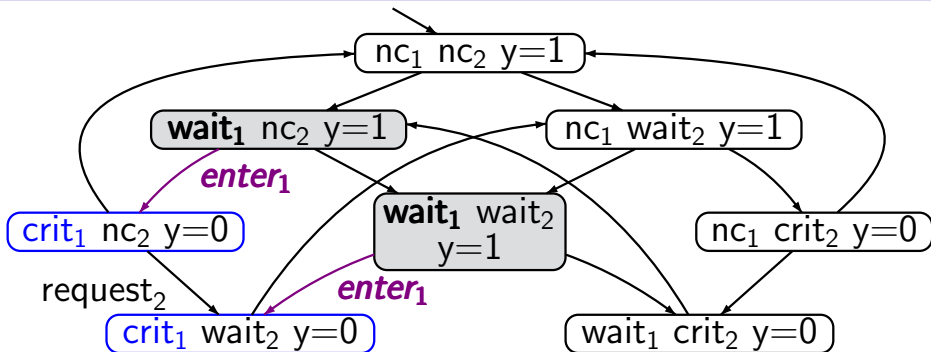
**enabled(A)**  $\in L(s)$  iff  $s \xrightarrow{\alpha} \dots$  for some  $\alpha \in A$   
**taken(A)**  $\in L(s)$  iff for **all** transitions  $\dots \xrightarrow{\alpha} s$ :  
 $\alpha \in A$

*alternative 1:* ad-hoc choice of “**taken**-predicate”

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

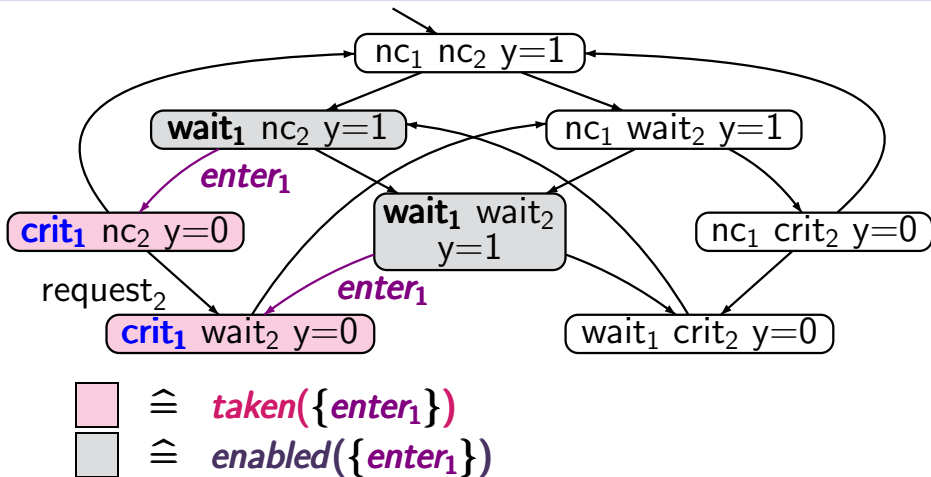


TS for mutual exclusion with semaphore

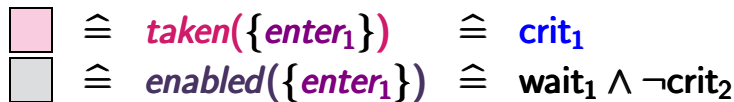
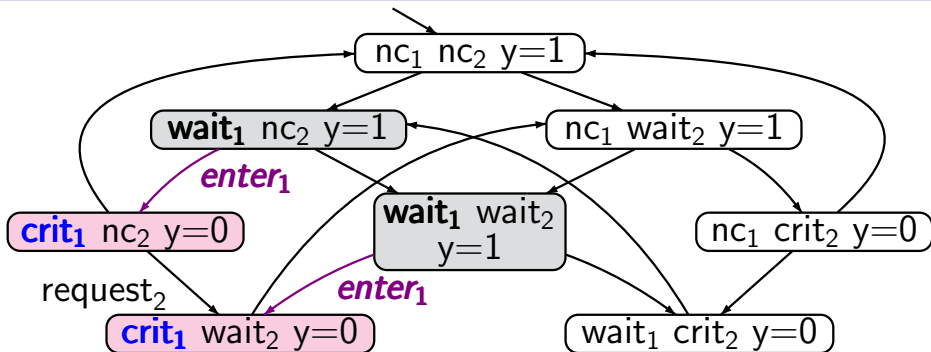


$\square \hat{=} \text{enabled}(\{enter_1\})$

TS for mutual exclusion with semaphore

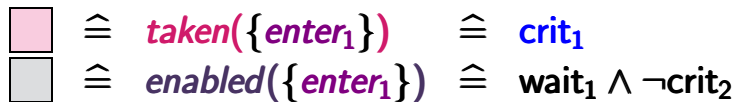
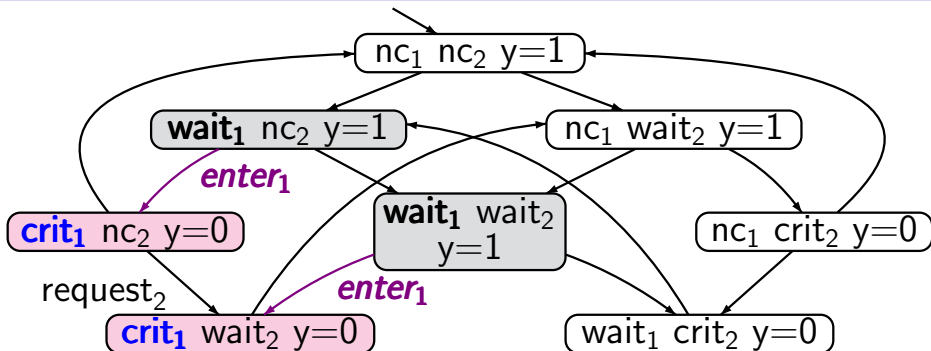


TS for mutual exclusion with semaphore



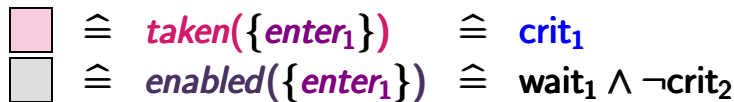
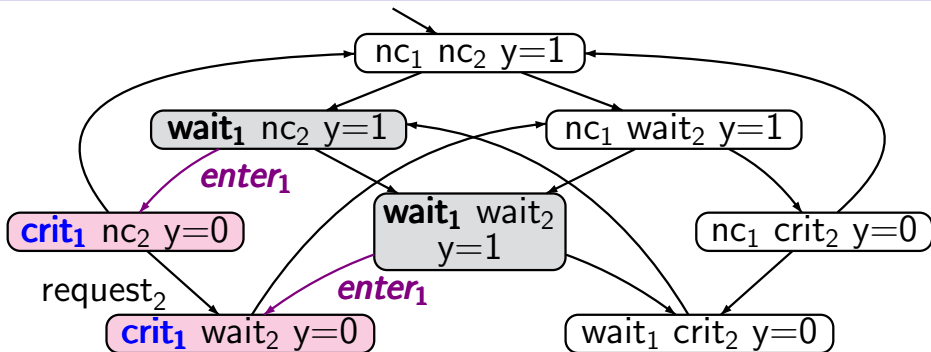


# Ad-hoc: action fairness $\rightsquigarrow$ LTL-fairness



strong  $\{enter_1\}$ -fairness: LTL formula

$$\square \diamond enabled(\{enter_1\}) \rightarrow \square \diamond taken(\{enter_1\})$$



$\square \diamond enabled(\{enter_1\}) \rightarrow \square \diamond taken(\{enter_1\})$

$\hat{=} \square \diamond (wait_1 \wedge \neg crit_2) \rightarrow \square \diamond crit_1$

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

$$\begin{aligned} \text{enabled}(A) \in L(s) & \text{ iff } s \xrightarrow{\alpha} \dots \text{ for some } \alpha \in A \\ \text{taken}(A) \in L(s) & \text{ iff for all transitions } \dots \xrightarrow{\alpha} s: \\ & \alpha \in A \end{aligned}$$

*alternative 1:* **ad-hoc choice** of “**taken**-predicate”

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

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

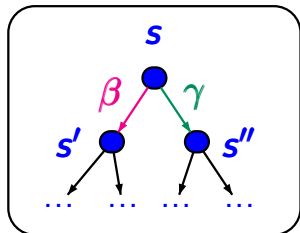
$$\begin{aligned} \mathit{enabled}(A) \in L(s) & \text{ iff } s \xrightarrow{\alpha} \dots \text{ for some } \alpha \in A \\ \mathit{taken}(A) \in L(s) & \text{ iff for all transitions } \dots \xrightarrow{\alpha} s: \\ & \alpha \in A \end{aligned}$$

*alternative 1:* ad-hoc choice of “**taken**-predicate”

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

transition system

$$\mathcal{T} = (\mathcal{S}, \text{Act}, \rightarrow, \dots)$$

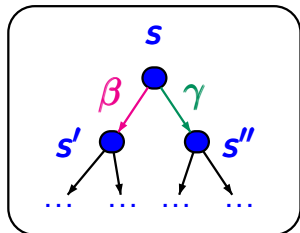


# Action-based fairness $\rightsquigarrow$ LTL-fairness

LTLSP3.1-47

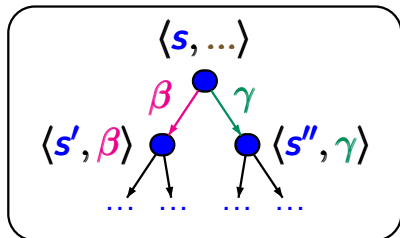
transition system

$$\mathcal{T} = (\mathcal{S}, \text{Act}, \rightarrow, \dots)$$



transition system

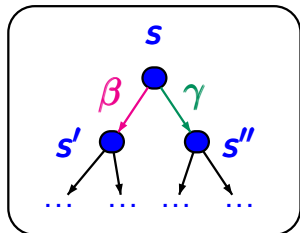
$$\mathcal{T}' = (\mathcal{S} \times \text{Act}, \dots, \text{AP}', L')$$



# Action-based fairness $\rightsquigarrow$ LTL-fairness

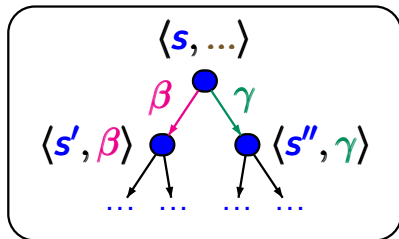
LTLSP3.1-47

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



strong **A**-fairness  
 for  $A \subseteq \mathbf{Act}$

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

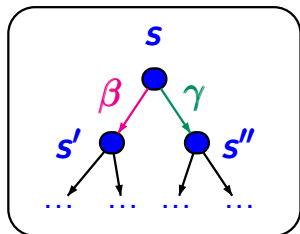


strong **LTL**-fairness  
 $\Box \Diamond \mathbf{enabled}(A) \rightarrow \Box \Diamond \mathbf{taken}(A)$

# Action-based fairness $\rightsquigarrow$ LTL-fairness

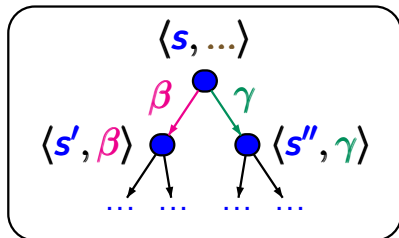
LTLSP3.1-47

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



strong **A**-fairness  
 for  $A \subseteq \mathbf{Act}$

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



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

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

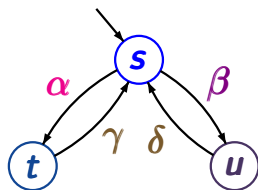
$\mathbf{taken}(A) \in L'(\langle s, \alpha \rangle)$  iff  $\alpha \in A$



# Example: action fairness $\rightsquigarrow$ LTL-fairness

LTLSF3.1-48

action-based fairness  $\rightsquigarrow$  LTL-fairness

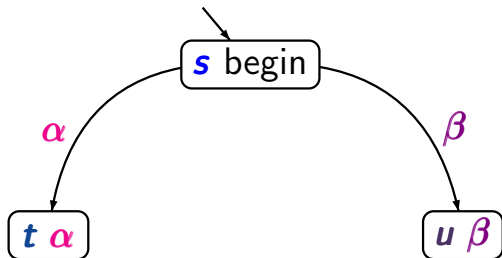
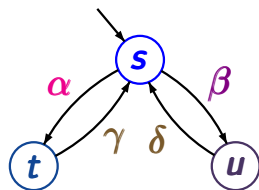


# Example: action fairness $\rightsquigarrow$ LTL-fairness

LTLSF3.1-48

action-based fairness  $\rightsquigarrow$

LTL-fairness

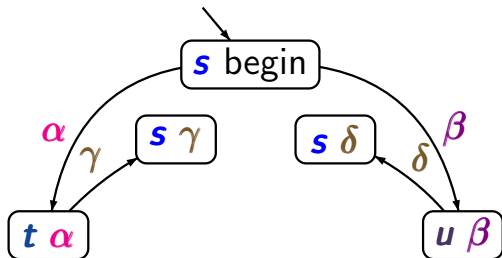
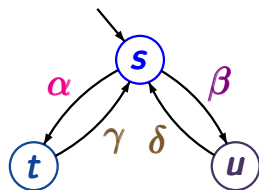


# Example: action fairness $\rightsquigarrow$ LTL-fairness

LTLSF3.1-48

action-based fairness  $\rightsquigarrow$

LTL-fairness

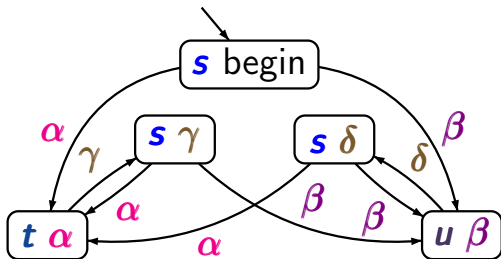
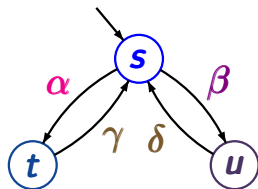


# Example: action fairness $\rightsquigarrow$ LTL-fairness

LTLSF3.1-48

action-based fairness  $\rightsquigarrow$

LTL-fairness

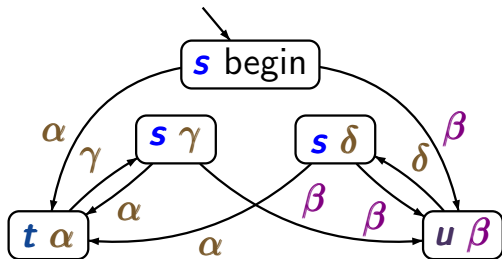
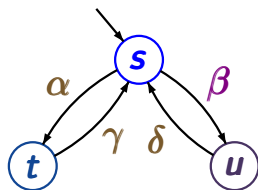


# Example: action fairness $\rightsquigarrow$ LTL-fairness

LTLSF3.1-48

action-based fairness  $\rightsquigarrow$ 

LTL-fairness

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

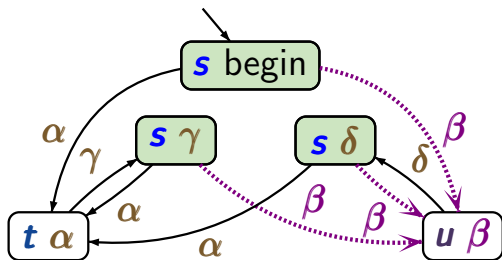
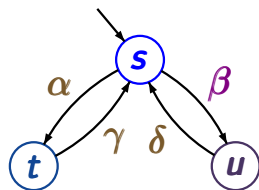
$$\square \diamond \textit{enabled}(\beta) \rightarrow \square \diamond \textit{taken}(\beta)$$

# Example: action fairness $\rightsquigarrow$ LTL-fairness

LTLSF3.1-48

action-based fairness  $\rightsquigarrow$ 

LTL-fairness

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

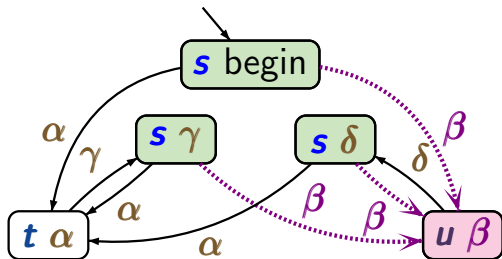
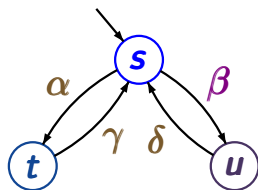
$$\square \diamond \text{enabled}(\beta) \rightarrow \square \diamond \text{taken}(\beta)$$

# Example: action fairness $\rightsquigarrow$ LTL-fairness

LTLSF3.1-48

action-based fairness  $\rightsquigarrow$ 

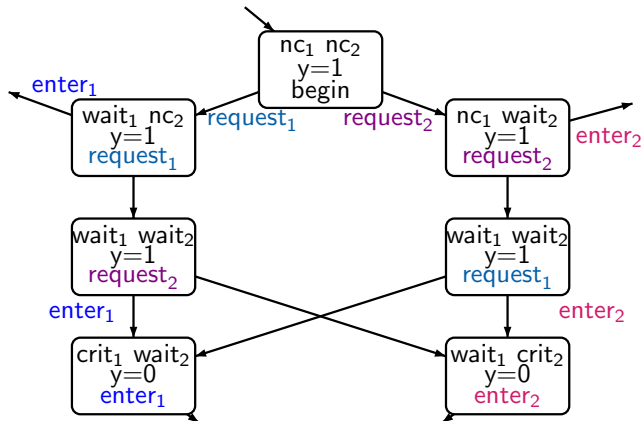
LTL-fairness

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

$$\square \diamond \text{enabled}(\beta) \rightarrow \square \diamond \text{taken}(\beta)$$

# Example: mutual exclusion with semaphore

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

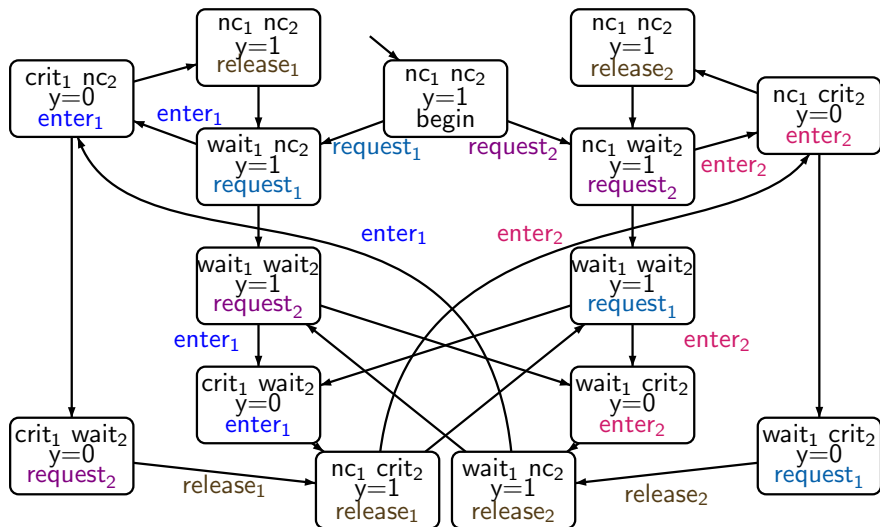




# Example: mutual exclusion with semaphore

LTLSF3.1-49

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



# Example: mutual exclusion with semaphore

LTL3.1-49

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

