

Introduction

Modelling parallel systems

Linear Time Properties

Regular Properties

**Linear Temporal Logic (LTL)**

Computation-Tree Logic

Equivalences and Abstraction



# Expansion law for U

LTLSF3.1-28

until:

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

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 $\diamond$

LTLSP3.1-28

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 $\diamond$

LTLSP3.1-28

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

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

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

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

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

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

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

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

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

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

$$\boxed{\square a} \equiv a \wedge \mathbf{O} \boxed{\square a}$$

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.,

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

although  $\boxed{\square a} \not\equiv \mathit{false}$

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

least fixed point

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

least fixed point

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

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

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

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

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.,

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

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

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.

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



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

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

# 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”:

$$\square\varphi \equiv ?$$

# 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

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

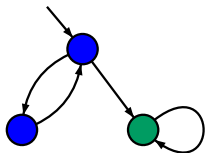
deriving “always” and “until” from “weak until”:

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

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

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

LTLSF3.1-32



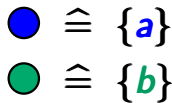
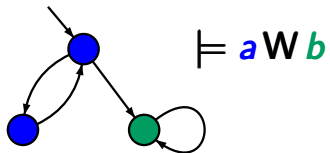
●  $\hat{=} \{a\}$

●  $\hat{=} \{b\}$



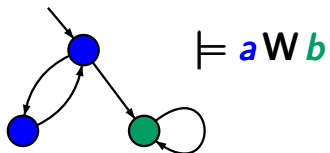
Does  $\mathcal{T} \models aWb$  hold?

LTLSF3.1-32



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

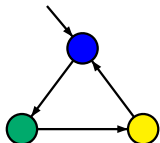
LTLSF3.1-32



●  $\hat{=} \{a\}$

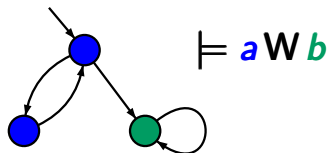
●  $\hat{=} \{b\}$

●  $\hat{=} \emptyset$



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

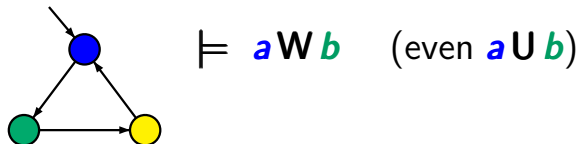
LTLSF3.1-32



●  $\hat{=} \{a\}$

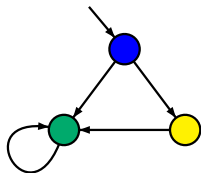
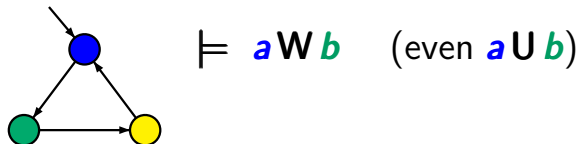
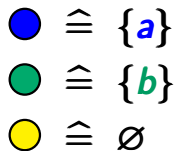
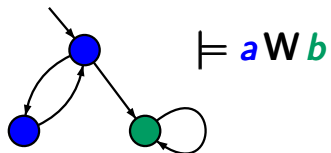
●  $\hat{=} \{b\}$

●  $\hat{=} \emptyset$



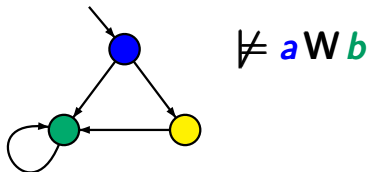
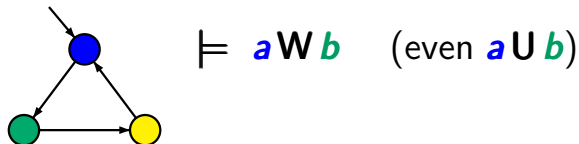
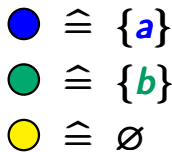
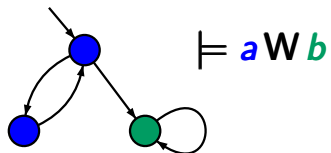
Does  $\mathcal{T} \models aWb$  hold?

LTLSF3.1-32



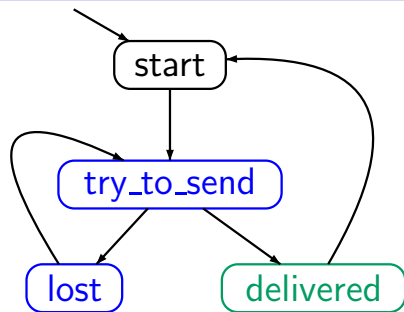
Does  $\mathcal{T} \models aWb$  hold?

LTLSF3.1-32



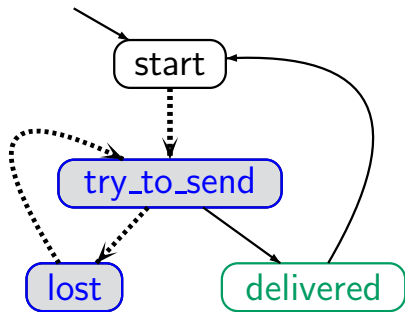
# Example: simple communication protocol

LTLSF3.1-33



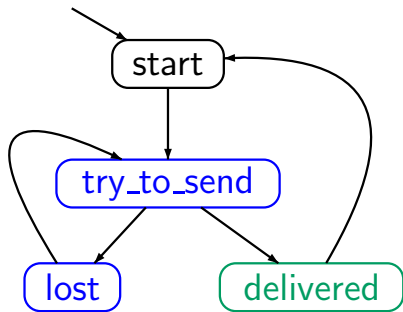
# Example: simple communication protocol

LTLSF3.1-33


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

# Example: until versus weak until

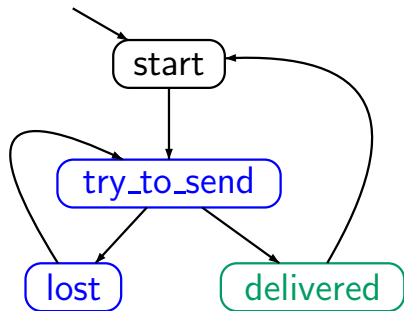
LTLSP3.1-33


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



# Example: until versus weak until

LTLSP3.1-33



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# Expansion laws for U and W

LTLSF3.1-34



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

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

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

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

# 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.

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

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

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

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

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

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

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



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

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

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.

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



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

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

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

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

$\mathbf{Words}(\varphi \mathbf{W} \psi)$  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.

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

$$\varphi U \psi \equiv \psi \vee (\varphi \wedge O(\varphi U \psi))$$

smallest solution

---

$$\varphi W \psi \equiv \psi \vee (\varphi \wedge O(\varphi W \psi))$$

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

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

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

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

$\neg(\varphi_1 \text{U} \varphi_2) \equiv (\neg \varphi_2) \text{W}(\neg \varphi_1 \wedge \neg \varphi_2)$

duality of **U** and **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:

$$\begin{aligned}\neg \text{true} &\rightsquigarrow \text{false} \\ \neg \neg \varphi &\rightsquigarrow \varphi \\ \neg(\varphi_1 \wedge \varphi_2) &\rightsquigarrow \neg \varphi_1 \vee \neg \varphi_2 \\ \neg \bigcirc \varphi &\rightsquigarrow \bigcirc \neg \varphi \\ \neg(\varphi_1 \text{ U } \varphi_2) &\rightsquigarrow (\neg \varphi_2) \text{ W } (\neg \varphi_1 \wedge \neg \varphi_2)\end{aligned}$$

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 $\neg \vee$
$\neg \bigcirc \varphi$	$\rightsquigarrow$	$\bigcirc \neg \varphi$	
$\neg(\varphi_1 \text{U} \varphi_2)$	$\rightsquigarrow$	$(\neg \varphi_2) \text{W}(\neg \varphi_1 \wedge \neg \varphi_2)$	
$\neg \diamond \varphi$	$\rightsquigarrow$	$\square \neg \varphi$	$\neg \square \varphi \rightsquigarrow \diamond \neg \varphi$

$$\neg \square((a \text{U} b) \vee \bigcirc c)$$

$$\equiv \diamond \neg((a \text{U} b) \vee \bigcirc c)$$

← duality of  $\diamond$  and  $\square$

$$\equiv \diamond(\neg(a \text{U} b) \wedge \neg \bigcirc c)$$

← duality of  $\wedge$  and  $\vee$

# Example: LTL $\rightsquigarrow$ LTL-PNF

LTLSP3.1-37

$\neg \text{true}$	$\rightsquigarrow$	$\text{false}$	+ 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 $\neg \vee$
$\neg \bigcirc \varphi$	$\rightsquigarrow$	$\bigcirc \neg \varphi$	
$\neg(\varphi_1 \text{U} \varphi_2)$	$\rightsquigarrow$	$(\neg \varphi_2) \text{W}(\neg \varphi_1 \wedge \neg \varphi_2)$	
$\neg \diamond \varphi$	$\rightsquigarrow$	$\square \neg \varphi$	$\neg \square \varphi \rightsquigarrow \diamond \neg \varphi$

$$\neg \square((a \text{U} b) \vee \bigcirc c)$$

$$\equiv \diamond \neg((a \text{U} b) \vee \bigcirc c) \quad \leftarrow \text{duality of } \diamond \text{ and } \square$$

$$\equiv \diamond(\neg(a \text{U} b) \wedge \neg \bigcirc c) \quad \leftarrow \text{duality of } \wedge \text{ and } \vee$$

$$\equiv \diamond((\neg b) \text{W}(\neg a \wedge \neg b) \wedge \bigcirc \neg c) \quad \leftarrow \text{duality of } \text{U} \text{ and } \text{W}$$

$\neg \text{true}$	$\rightsquigarrow$	$\text{false}$	+ 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 $\neg \vee$
$\neg \bigcirc \varphi$	$\rightsquigarrow$	$\bigcirc \neg \varphi$	
$\neg(\varphi_1 \text{U} \varphi_2)$	$\rightsquigarrow$	$(\neg \varphi_2) \text{W}(\neg \varphi_1 \wedge \neg \varphi_2)$	
$\neg \diamond \varphi$	$\rightsquigarrow$	$\square \neg \varphi$	$\neg \square \varphi \rightsquigarrow \diamond \neg \varphi$

$$\neg \square((a \text{U} b) \vee \bigcirc c)$$

$$\equiv \diamond \neg((a \text{U} b) \vee \bigcirc c)$$

$$\equiv \diamond(\neg(a \text{U} b) \wedge \neg \bigcirc c)$$

$$\equiv \diamond((\neg b) \text{W}(\neg a \wedge \neg b) \wedge \bigcirc \neg c) \leftarrow \text{PNF}$$





# Recall: action-based fairness

LTLSF3.1-38

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

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

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

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

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

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

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

$$\exists i \geq 1. A \cap \text{Act}(\mathcal{S}_i) \neq \emptyset \implies \exists i \geq 1. \alpha_i \in A$$
- for all  $A \in \mathcal{F}_{weak}$ :  

$$\forall i \geq 1. A \cap \text{Act}(\mathcal{S}_i) \neq \emptyset \implies \exists i \geq 1. \alpha_i \in A$$

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

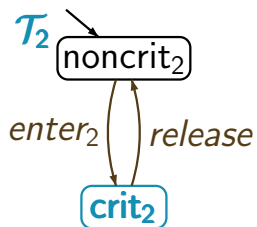
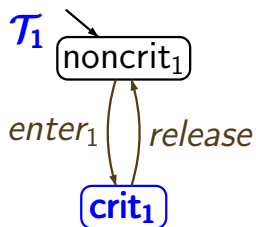
If **fair** is a LTL fairness assumption, **s** a state in a TS, and  $\varphi$  an LTL formula then

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



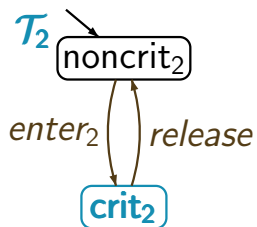
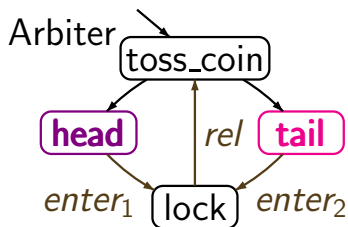
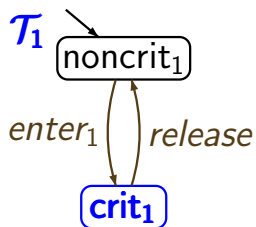
# Randomized arbiter for MUTEX

LTLSF3.1-40



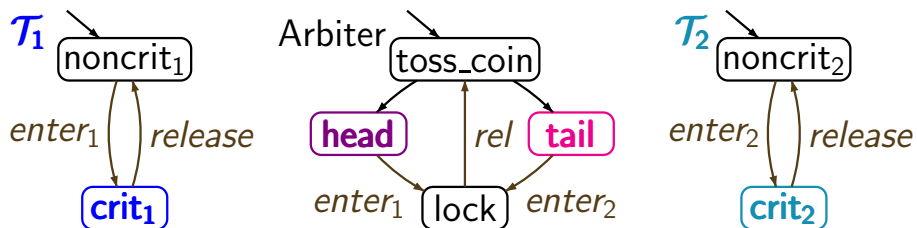
# Randomized arbiter for MUTEX

LTLSF3.1-40

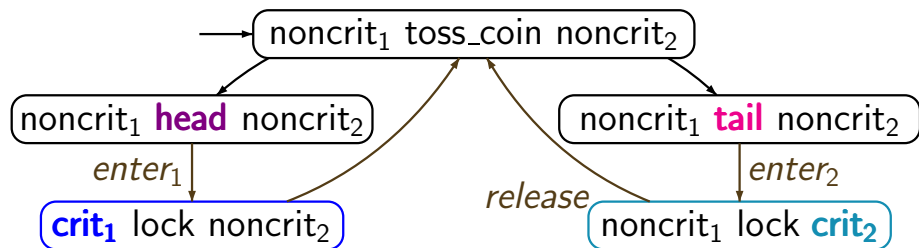


# Randomized arbiter for MUTEX

LTLSF3.1-40

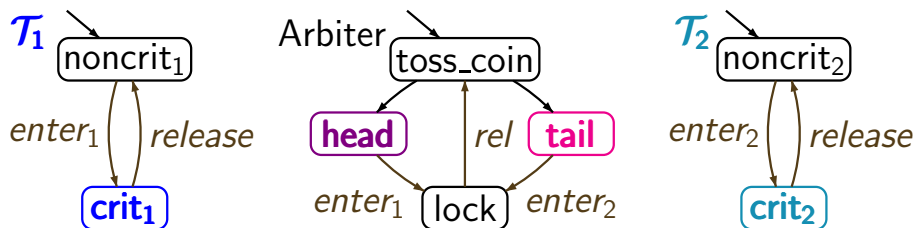


$(\mathcal{T}_1 \parallel \mathcal{T}_2) \parallel \text{Arbiter}$

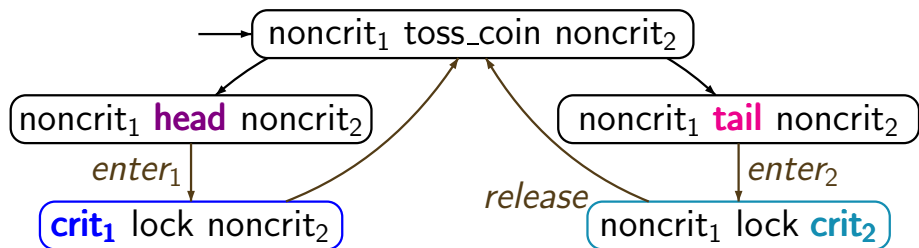


# Randomized arbiter for MUTEX

LTLSF3.1-40

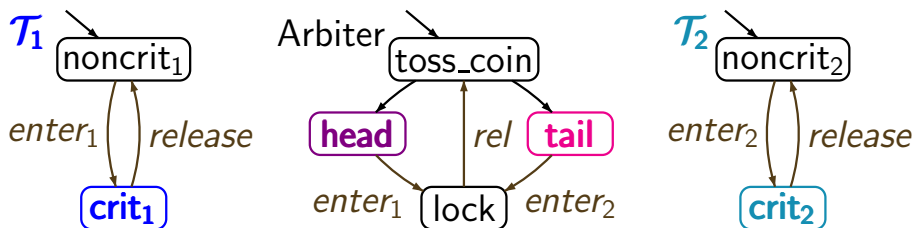


$$(\mathcal{T}_1 \parallel \mathcal{T}_2) \parallel \text{Arbiter} \not\models \square \diamond \text{crit}_1 \wedge \square \diamond \text{crit}_2$$



# Randomized arbiter for MUTEX

LTLSF3.1-40

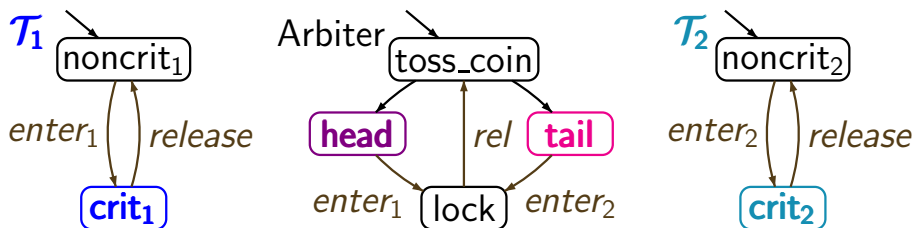


unconditional LTL-fairness:

$$fair = \square \diamond head \wedge \square \diamond tail$$

# Randomized arbiter for MUTEX

LTLSF3.1-40



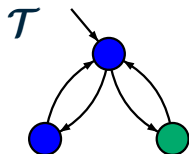
unconditional LTL-fairness:

$$\text{fair} = \square \diamond \text{head} \wedge \square \diamond \text{tail}$$

$$(\mathcal{T}_1 \parallel \mathcal{T}_2) \parallel \text{Arbiter} \models_{\text{fair}} \square \diamond \text{crit}_1 \wedge \square \diamond \text{crit}_2$$

# Correct or wrong?

LTLSF3.1-41

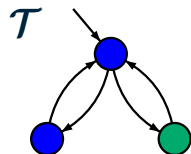


LTL fairness assumption  
*fair* =  $\diamond \Box a \rightarrow \Box \diamond b$

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

# Correct or wrong?

LTLSF3.1-41



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

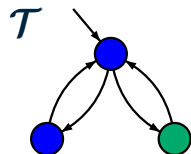
●  $\hat{=} \{a\}$  ●  $\hat{=} \{b\}$

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



# Correct or wrong?

LTLSF3.1-41



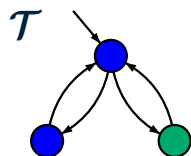
LTL fairness assumption  
 $fair = \diamond \Box a \rightarrow \Box \diamond b$

$\bullet \hat{=} \{a\}$     $\bullet \hat{=} \{b\}$

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

# Correct or wrong?

LTLSF3.1-41



LTL fairness assumption  
*fair* =  $\diamond \Box a \rightarrow \Box \diamond b$

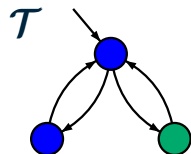
$\bullet \hat{=} \{a\}$     $\bullet \hat{=} \{b\}$

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

$\mathcal{T} \models_{\text{fair}} a \cup b$  ?

# Correct or wrong?

LTLSF3.1-41



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

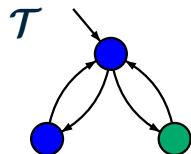
$\bullet \hat{=} \{a\}$     $\bullet \hat{=} \{b\}$

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

$\mathcal{T} \models_{fair} a \cup b$   $\checkmark$

# Correct or wrong?

LTLSP3.1-41



LTL fairness assumption  
*fair* =  $\diamond \Box a \rightarrow \Box \diamond b$

$\bullet \hat{=} \{a\}$     $\bullet \hat{=} \{b\}$

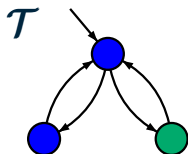
$\mathcal{T} \not\models_{\text{fair}} \bigcirc b$  as  $\bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \dots$  is fair

$\mathcal{T} \models_{\text{fair}} a \cup b$  ✓

$\mathcal{T} \models_{\text{fair}} a \cup \Box (b \leftrightarrow \bigcirc a)$  ?

# 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

$$\mathcal{T}_{sem} \not\models \square \diamond crit_1 \wedge \square \diamond crit_2$$

$$\mathcal{T}_{sem} \models_{fair} \square \diamond crit_1 \wedge \square \diamond crit_2$$

for appropriate fairness condition

- can be 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.,

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

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

for appropriate fairness condition

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

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

- are irrelevant for verifying safety properties

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

if *fair* is realizable

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

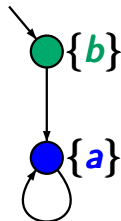
*recall:* a fairness condition is called **realizable**  
if for each reachable state **s** there exists  
a fair path starting in **s**

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:

$$\begin{aligned} \text{enabled}(A) \in L(s) & \text{ iff } s \xrightarrow{\alpha} \dots \text{ for some } \alpha \in A \\ \text{taken}(A) \in L(s) & \text{ iff for all transitions } \dots \xrightarrow{\alpha} s: \\ & \alpha \in A \end{aligned}$$

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

*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

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

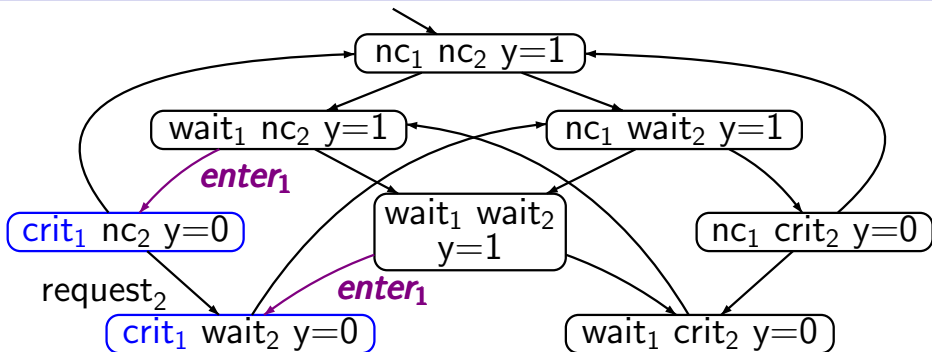


*idea:* use new atomic propositions **enabled(A)** and **taken(A)** and extend the labeling function:

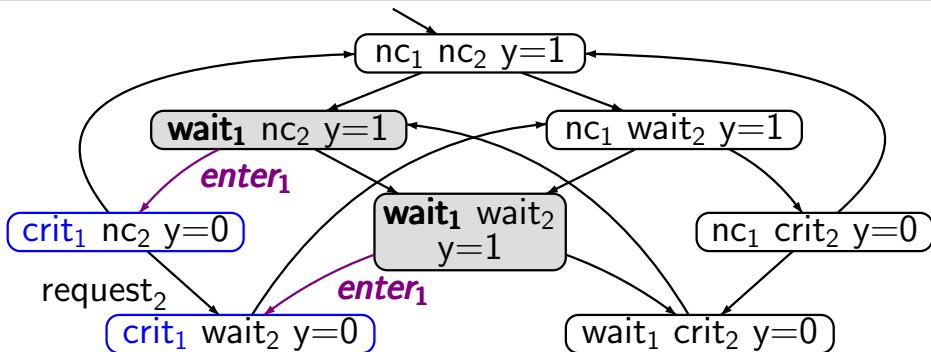
$$\begin{aligned} \text{enabled}(A) \in L(s) & \text{ iff } s \xrightarrow{\alpha} \dots \text{ for some } \alpha \in A \\ \text{taken}(A) \in L(s) & \text{ iff for } \boxed{\text{all}} \text{ transitions } \dots \xrightarrow{\alpha} s: \\ & \alpha \in A \end{aligned}$$

*alternative 1:* ad-hoc choice of “**taken**-predicate”

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

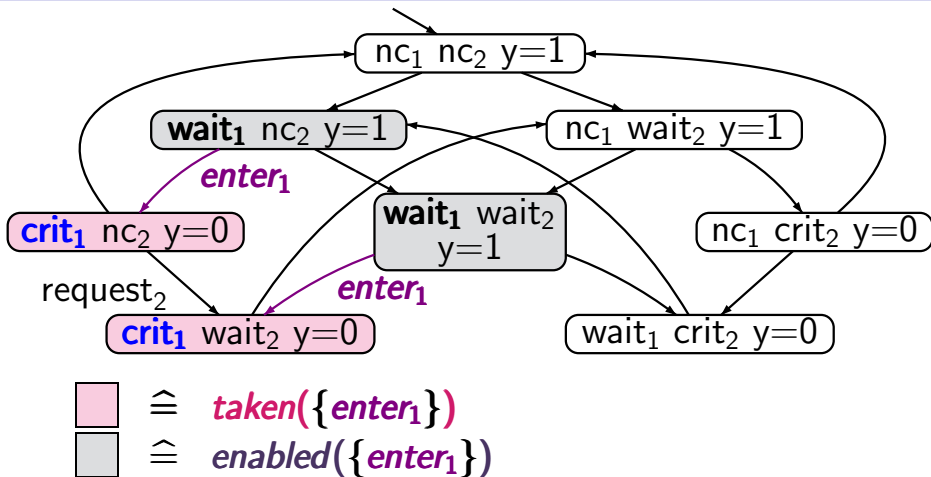


TS for mutual exclusion with semaphore

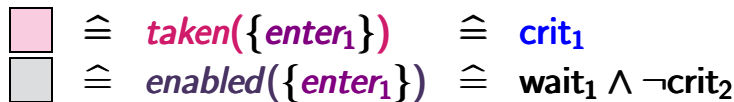
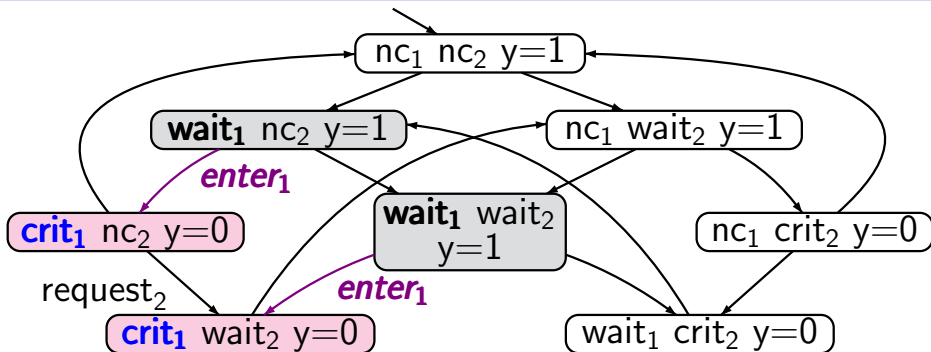


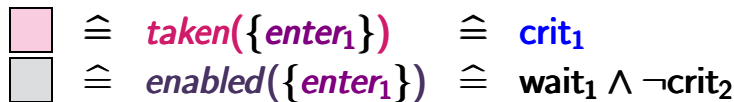
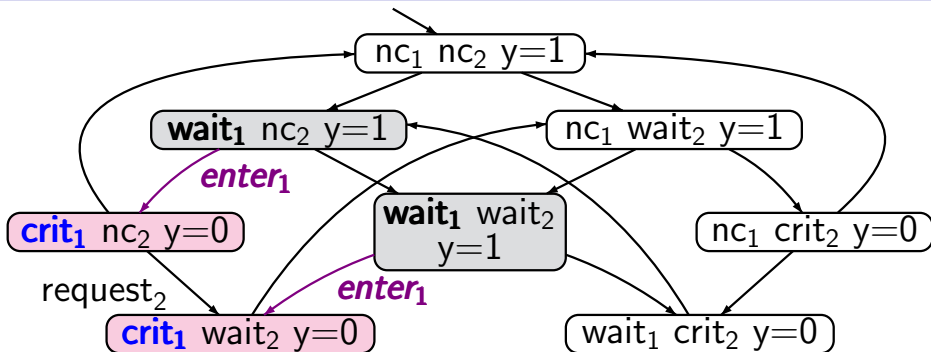
□  $\hat{=}$  *enabled*(*{enter<sub>1</sub>}*)

TS for mutual exclusion with semaphore



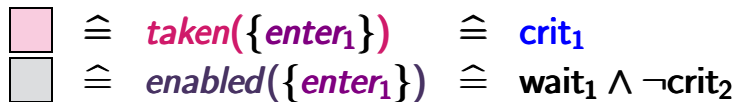
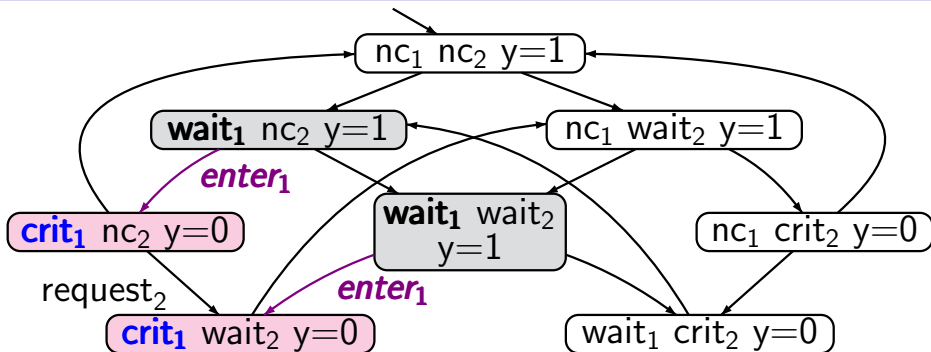
TS for mutual exclusion with semaphore





strong *{enter<sub>1</sub>}*-fairness: LTL formula

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



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

$\hat{=} \Box \Diamond (wait_1 \wedge \neg crit_2) \rightarrow \Box \Diamond crit_1$

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

$$\begin{aligned} \mathit{enabled}(A) \in L(s) & \text{ iff } s \xrightarrow{\alpha} \dots \text{ for some } \alpha \in A \\ \mathit{taken}(A) \in L(s) & \text{ iff for all transitions } \dots \xrightarrow{\alpha} s: \\ & \alpha \in A \end{aligned}$$

*alternative 1:* **ad-hoc choice** of “**taken**-predicate”

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



*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  $\alpha \in A$

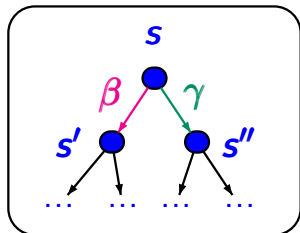
**taken(A)**  $\in L(s)$  iff for all transitions  $\dots \xrightarrow{\alpha} s$ :  
 $\alpha \in A$

*alternative 1:* ad-hoc choice of “**taken**-predicate”

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

transition system

$$\mathcal{T} = (\mathcal{S}, \mathbf{Act}, \rightarrow, \dots)$$

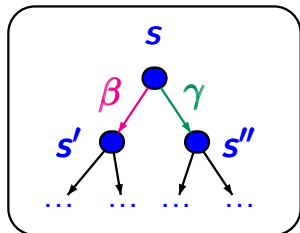


# Action-based fairness $\rightsquigarrow$ LTL-fairness

LTLSP3.1-47

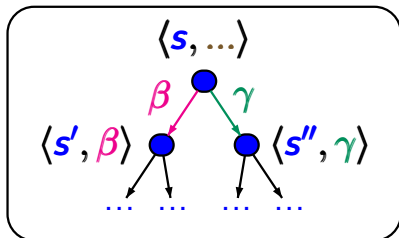
transition system

$$\mathcal{T} = (\mathcal{S}, \text{Act}, \rightarrow, \dots)$$



transition system

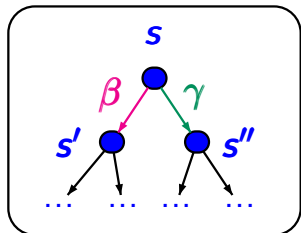
$$\mathcal{T}' = (\mathcal{S} \times \text{Act}, \dots, \text{AP}', L')$$



# Action-based fairness $\rightsquigarrow$ LTL-fairness

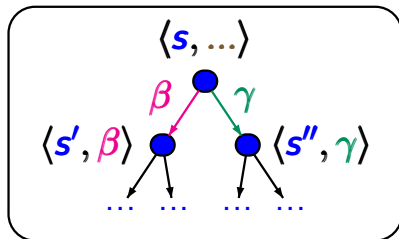
LTLSP3.1-47

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



strong **A**-fairness  
for  $A \subseteq \mathbf{Act}$

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

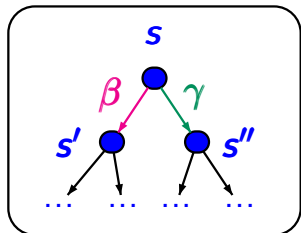


strong **LTL**-fairness  
 $\Box \Diamond \mathbf{enabled}(A) \rightarrow \Box \Diamond \mathbf{taken}(A)$

# Action-based fairness $\rightsquigarrow$ LTL-fairness

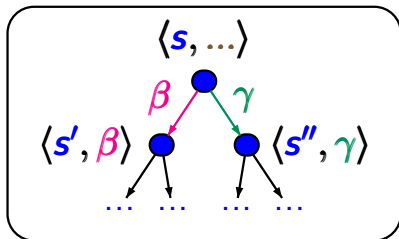
LTLSP3.1-47

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  
 $\Box \Diamond \mathbf{enabled}(A) \rightarrow \Box \Diamond \mathbf{taken}(A)$

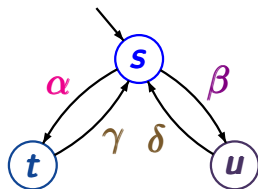
$\mathbf{enabled}(A) \in L'(\langle s, \alpha \rangle)$  iff  $s \xrightarrow{\beta} \dots$  for some  $\beta \in A$

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

# Example: action fairness $\rightsquigarrow$ LTL-fairness

LTLSF3.1-48

action-based fairness  $\rightsquigarrow$  LTL-fairness

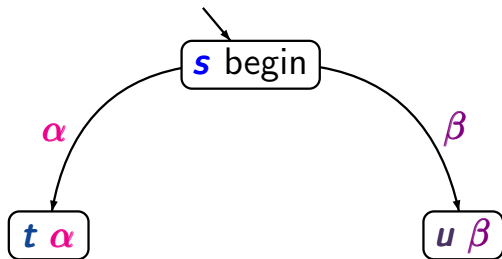
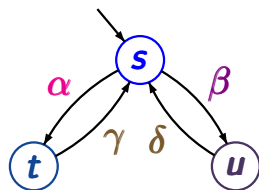


# Example: action fairness $\rightsquigarrow$ LTL-fairness

LTLSF3.1-48

action-based fairness  $\rightsquigarrow$

LTL-fairness

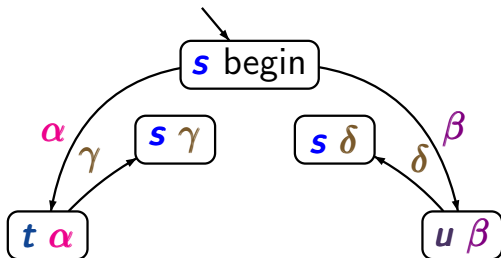
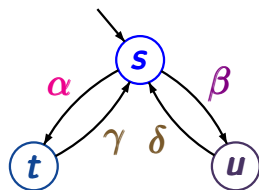


# Example: action fairness $\rightsquigarrow$ LTL-fairness

LTLSF3.1-48

action-based fairness  $\rightsquigarrow$

LTL-fairness



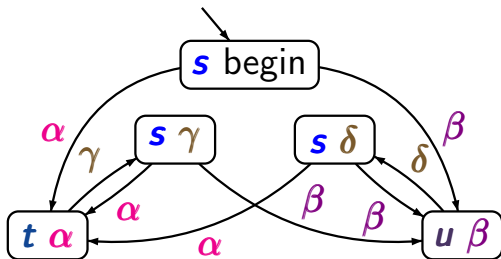
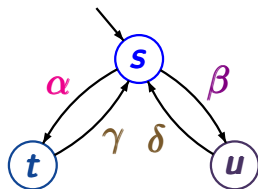


# Example: action fairness $\rightsquigarrow$ LTL-fairness

LTLSF3.1-48

action-based fairness  $\rightsquigarrow$

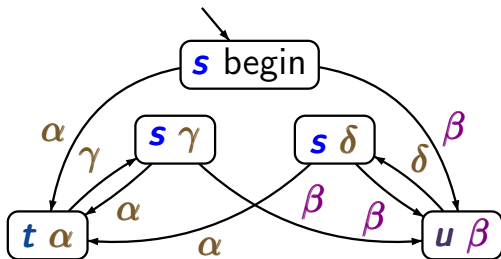
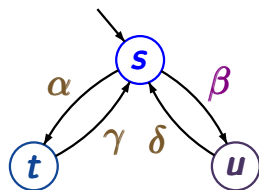
LTL-fairness



# Example: action fairness $\rightsquigarrow$ LTL-fairness

LTLSF3.1-48

action-based fairness  $\rightsquigarrow$  LTL-fairness



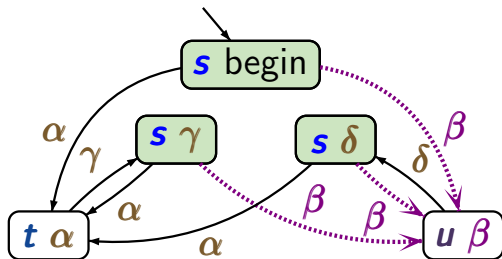
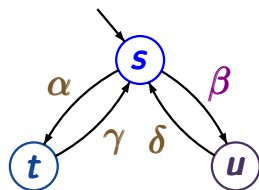
strong fairness for  $\{\beta\}$ :

$$\square \diamond \textit{enabled}(\beta) \rightarrow \square \diamond \textit{taken}(\beta)$$

# Example: action fairness $\rightsquigarrow$ LTL-fairness

LTLSF3.1-48

action-based fairness  $\rightsquigarrow$  LTL-fairness



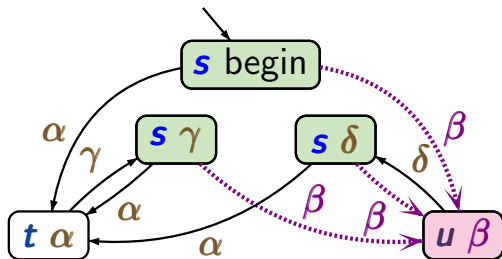
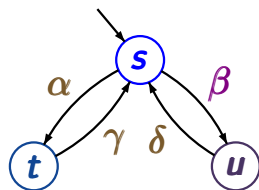
strong fairness for  $\{\beta\}$ :

$$\square \diamond \text{enabled}(\beta) \rightarrow \square \diamond \text{taken}(\beta)$$

# Example: action fairness $\rightsquigarrow$ LTL-fairness

LTLSF3.1-48

action-based fairness  $\rightsquigarrow$  LTL-fairness

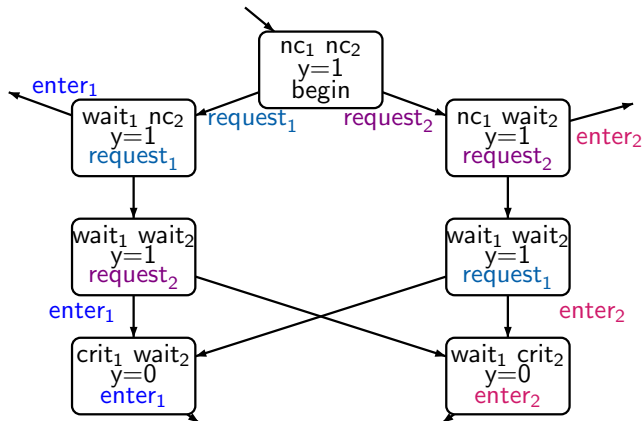


strong fairness for  $\{\beta\}$ :

$$\square \diamond \text{enabled}(\beta) \rightarrow \square \diamond \text{taken}(\beta)$$

# Example: mutual exclusion with semaphore

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



# Example: mutual exclusion with semaphore

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

