

Introduction

Modelling parallel systems

Linear Time Properties

Regular Properties

Linear Temporal Logic (LTL)

**Computation Tree Logic**

    syntax and semantics of CTL

    expressiveness of CTL and LTL

    CTL model checking

    CTL with fairness



    counterexamples/witnesses, CTL<sup>+</sup> and CTL\*

Equivalences and Abstraction



**LTL** model checking problem:

PSPACE-complete and solvable in time

$$\mathcal{O}(\text{size}(\mathcal{T}) \cdot \exp(|\varphi|))$$

---

**CTL** model checking problem:

solvable in polynomial time

$$\mathcal{O}(\text{size}(\mathcal{T}) \cdot |\Phi|)$$

**LTL** model checking problem:

PSPACE-complete and solvable in time

$$\mathcal{O}(\text{size}(\mathcal{T}) \cdot \exp(|\varphi|))$$

---

**CTL** model checking problem:

solvable in polynomial time (even PTIME-complete)

$$\mathcal{O}(\text{size}(\mathcal{T}) \cdot |\Phi|)$$

**LTL** model checking problem:

PSPACE-complete and solvable in time

$$\mathcal{O}(\text{size}(\mathcal{T}) \cdot \exp(|\varphi|))$$

**LTL** with fairness:  $\mathcal{O}(\text{size}(\mathcal{T}) \cdot \exp(|\varphi| + |\text{fair}|))$

---

**CTL** model checking problem:

solvable in polynomial time (even PTIME-complete)

$$\mathcal{O}(\text{size}(\mathcal{T}) \cdot |\Phi|)$$

**LTL** model checking problem:

PSPACE-complete and solvable in time

$$\mathcal{O}(\text{size}(\mathcal{T}) \cdot \exp(|\varphi|))$$

**LTL** with fairness:  $\mathcal{O}(\text{size}(\mathcal{T}) \cdot \exp(|\varphi| + |\text{fair}|))$

---

**CTL** model checking problem:

solvable in polynomial time (even PTIME-complete)

$$\mathcal{O}(\text{size}(\mathcal{T}) \cdot |\Phi|)$$

**CTL** with fairness:  $\mathcal{O}(\text{size}(\mathcal{T}) \cdot |\Phi| \cdot |\text{fair}|)$

# Recall: LTL fairness assumptions

CTLFAIR4.4-2

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

- unconditional fairness  $\Box\Diamond\phi$
- strong fairness  $\Box\Diamond\psi \rightarrow \Box\Diamond\phi$
- weak fairness  $\Diamond\Box\psi \rightarrow \Box\Diamond\phi$

where  $\phi, \psi$  are propositional formulas



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

- unconditional fairness  $\Box\Diamond\phi$
- strong fairness  $\Box\Diamond\psi \rightarrow \Box\Diamond\phi$
- weak fairness  $\Diamond\Box\psi \rightarrow \Box\Diamond\phi$

where  $\phi, \psi$  are propositional formulas

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

- unconditional fairness  $\Box\Diamond\phi$
- strong fairness  $\Box\Diamond\psi \rightarrow \Box\Diamond\phi$
- weak fairness  $\Diamond\Box\psi \rightarrow \Box\Diamond\phi$

where  $\phi, \psi$  are propositional formulas

Reduction of  $\models_{\text{fair}}$  to  $\models$

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

- unconditional fairness  $\Box\Diamond\phi$
- strong fairness  $\Box\Diamond\psi \rightarrow \Box\Diamond\phi$
- weak fairness  $\Diamond\Box\psi \rightarrow \Box\Diamond\phi$

where  $\phi, \psi$  are propositional formulas

Reduction of  $\models_{\text{fair}}$  to  $\models$

$\mathcal{T} \models_{\text{fair}} \varphi$  iff  $\pi \models \varphi$  for all fair paths  $\pi$  in  $\mathcal{T}$

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

- unconditional fairness  $\Box\Diamond\phi$
- strong fairness  $\Box\Diamond\psi \rightarrow \Box\Diamond\phi$
- weak fairness  $\Diamond\Box\psi \rightarrow \Box\Diamond\phi$

where  $\phi, \psi$  are propositional formulas

Reduction of  $\models_{\text{fair}}$  to  $\models$

$$\begin{aligned} \mathcal{T} \models_{\text{fair}} \varphi & \text{ iff } \pi \models \varphi \text{ for all fair paths } \pi \text{ in } \mathcal{T} \\ & \text{ iff for all paths } \pi \text{ in } \mathcal{T}: \\ & \quad \pi \models \text{fair} \rightarrow \varphi \end{aligned}$$

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

- unconditional fairness  $\Box\Diamond\phi$
- strong fairness  $\Box\Diamond\psi \rightarrow \Box\Diamond\phi$
- weak fairness  $\Diamond\Box\psi \rightarrow \Box\Diamond\phi$

where  $\phi, \psi$  are propositional formulas

Reduction of  $\models_{\text{fair}}$  to  $\models$ , e.g., for  $\text{fair} = \Box\Diamond a$

$\mathcal{T} \models_{\text{fair}} \varphi$  iff  $\pi \models \varphi$  for all fair paths  $\pi$  in  $\mathcal{T}$

iff for all paths  $\pi$  in  $\mathcal{T}$ :

$\pi \models \text{fair} \rightarrow \varphi$

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

- unconditional fairness  $\Box\Diamond\phi$
- strong fairness  $\Box\Diamond\psi \rightarrow \Box\Diamond\phi$
- weak fairness  $\Diamond\Box\psi \rightarrow \Box\Diamond\phi$

where  $\phi, \psi$  are propositional formulas

Reduction of  $\models_{\text{fair}}$  to  $\models$ , e.g., for  $\text{fair} = \Box\Diamond a$

$\mathcal{T} \models_{\text{fair}} \varphi$  iff  $\pi \models \varphi$  for all fair paths  $\pi$  in  $\mathcal{T}$

iff for all paths  $\pi$  in  $\mathcal{T}$ :

$$\pi \models \text{fair} \rightarrow \varphi \equiv \Diamond\Box\neg a \vee \varphi$$



conjunctions of “formulas” of the type

- unconditional fairness:  $\Box\Diamond\Phi$
- strong fairness:  $\Box\Diamond\Psi \rightarrow \Box\Diamond\Phi$
- weak fairness:  $\Diamond\Box\Psi \rightarrow \Box\Diamond\Phi$

where  $\Psi$ ,  $\Phi$  are CTL state formulas



conjunctions of “formulas” of the type

- unconditional fairness:  $\Box\Diamond\Phi$
- strong fairness:  $\Box\Diamond\Psi \rightarrow \Box\Diamond\Phi$
- weak fairness:  $\Diamond\Box\Psi \rightarrow \Box\Diamond\Phi$

where  $\Psi$ ,  $\Phi$  are CTL state formulas

*note:* CTL fairness assumptions

- are not CTL (state or path) formulas
- just a syntactic formalism to specify fairness assumptions

conjunctions of “formulas” of the type

- unconditional fairness:  $\Box\Diamond\Phi$
- strong fairness:  $\Box\Diamond\Psi \rightarrow \Box\Diamond\Phi$
- weak fairness:  $\Diamond\Box\Psi \rightarrow \Box\Diamond\Phi$

where  $\Psi$ ,  $\Phi$  are CTL state formulas

e.g., a strong CTL fairness assumption has the form:

$$\mathit{fair} = \bigwedge_{1 \leq j \leq k} (\Box\Diamond\Psi_j \rightarrow \Box\Diamond\Phi_j)$$

where  $\Psi_j$ ,  $\Phi_j$  are CTL state formulas



$s \models_{\text{fair}} \text{true}$  $s \models_{\text{fair}} a$  iff  $a \in L(s)$  $s \models_{\text{fair}} \neg\Phi$  iff  $s \not\models_{\text{fair}} \Phi$  $s \models_{\text{fair}} \Phi_1 \wedge \Phi_2$  iff  $s \models_{\text{fair}} \Phi_1$  and  $s \models_{\text{fair}} \Phi_2$

$s \models_{\text{fair}} \text{true}$  $s \models_{\text{fair}} a$  iff  $a \in L(s)$  $s \models_{\text{fair}} \neg\Phi$  iff  $s \not\models_{\text{fair}} \Phi$  $s \models_{\text{fair}} \Phi_1 \wedge \Phi_2$  iff  $s \models_{\text{fair}} \Phi_1$  and  $s \models_{\text{fair}} \Phi_2$  $s \models_{\text{fair}} \exists\varphi$  iff there exists  $\pi \in \text{Paths}(s)$  with  
 $\pi \models_{\text{fair}}$  and  $\pi \models_{\text{fair}} \varphi$

$s \models_{\text{fair}} \text{true}$  $s \models_{\text{fair}} a$  iff  $a \in L(s)$  $s \models_{\text{fair}} \neg\Phi$  iff  $s \not\models_{\text{fair}} \Phi$  $s \models_{\text{fair}} \Phi_1 \wedge \Phi_2$  iff  $s \models_{\text{fair}} \Phi_1$  and  $s \models_{\text{fair}} \Phi_2$  $s \models_{\text{fair}} \exists\varphi$  iff there exists  $\pi \in \text{Paths}(s)$  with  
 $\pi \models_{\text{fair}}$  and  $\pi \models_{\text{fair}} \varphi$  $s \models_{\text{fair}} \forall\varphi$  iff for all  $\pi \in \text{Paths}(s)$ :  
 $\pi \models_{\text{fair}}$  implies  $\pi \models_{\text{fair}} \varphi$

$$s \models_{\text{fair}} \text{true}$$

$$s \models_{\text{fair}} a \quad \text{iff} \quad a \in L(s)$$

$$s \models_{\text{fair}} \neg\Phi \quad \text{iff} \quad s \not\models_{\text{fair}} \Phi$$

$$s \models_{\text{fair}} \Phi_1 \wedge \Phi_2 \quad \text{iff} \quad s \models_{\text{fair}} \Phi_1 \text{ and } s \models_{\text{fair}} \Phi_2$$

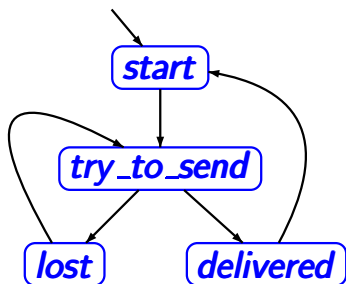
$$s \models_{\text{fair}} \exists\varphi \quad \text{iff} \quad \text{there exists } \pi \in \text{Paths}(s) \text{ with}$$

$$\boxed{\pi \models_{\text{fair}}} \text{ and } \pi \models_{\text{fair}} \varphi$$

$$s \models_{\text{fair}} \forall\varphi \quad \text{iff} \quad \text{for all } \pi \in \text{Paths}(s):$$

$$\boxed{\pi \models_{\text{fair}}} \text{ implies } \pi \models_{\text{fair}} \varphi$$

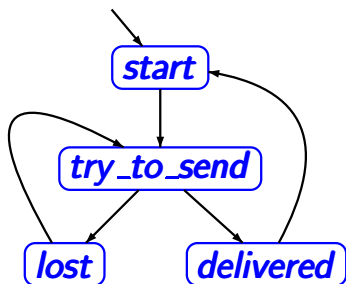
e.g.,  $s_0 s_1 s_2 \dots \models \square\Diamond\Phi$  iff  $\exists i \geq 0$  s.t.  $s_i \models \Phi$



CTL formula

$$\Phi = \forall \square \forall \diamond \textit{start}$$

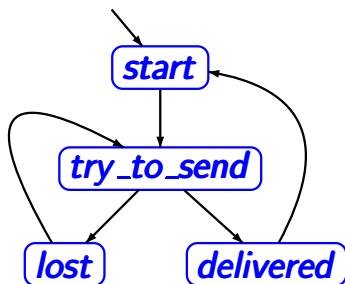




CTL formula

$$\Phi = \forall \square \forall \diamond \textit{start}$$

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



CTL formula

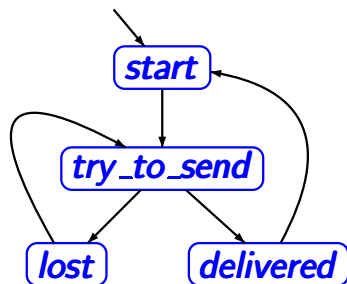
$$\Phi = \forall \square \forall \diamond \text{start}$$

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

$$\mathcal{T} \models_{\text{ufair}} \Phi$$

unconditional CTL fairness assumption:

$$\text{ufair} = \square \diamond \text{delivered}$$



CTL formula

$$\Phi = \forall \square \forall \diamond \text{start}$$

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

$$\mathcal{T} \models_{\text{ufair}} \Phi$$

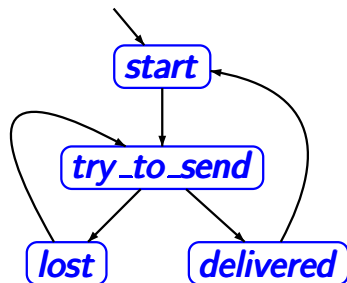
$$\mathcal{T} \models_{\text{sfair}} \Phi$$

unconditional CTL fairness assumption:

$$\text{ufair} = \square \diamond \text{delivered}$$

strong CTL fairness assumption:

$$\text{sfair} = \square \diamond \text{try\_to\_send} \rightarrow \square \diamond \text{delivered}$$



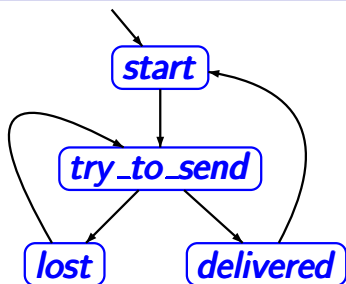
$$\phi = \forall \square \forall \diamond \text{start}$$

$$\mathcal{T} \models_{\text{ufair}} \phi \quad ?$$

unconditional fairness:  $\text{ufair} = \square \diamond \exists \bigcirc \text{start}$

# Simple communication protocol

CTLFAIR4.4-6

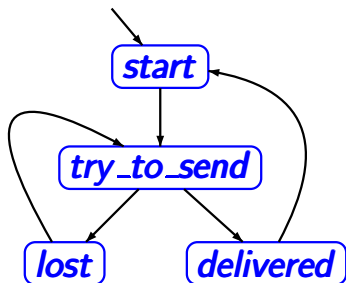


$$\phi = \forall \square \forall \diamond \text{start}$$

$$\mathcal{T} \models_{\text{ufair}} \phi \quad ?$$

unconditional fairness:  $\text{ufair} = \square \diamond \boxed{\exists \bigcirc \text{start}}$

$$\text{Sat}(\exists \bigcirc \text{start}) = \{\text{delivered}\}$$



$$\phi = \forall \square \forall \diamond \text{start}$$

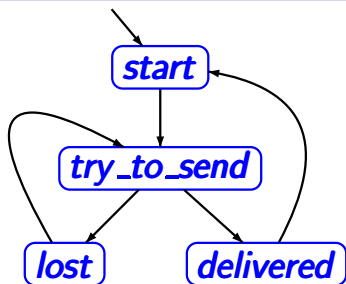
$$\mathcal{T} \models_{\text{fair}} \phi \quad ?$$

unconditional fairness:  $\text{fair} = \square \diamond \boxed{\exists \bigcirc \text{start}}$



$$\text{Sat}(\exists \bigcirc \text{start}) = \{\text{delivered}\}$$

$$\text{fair} \hat{=} \square \diamond \text{delivered}$$



$$\phi = \forall \square \forall \diamond \text{start}$$

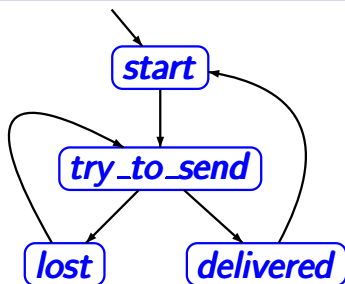
$$\mathcal{T} \models_{\text{ufair}} \phi \quad \checkmark$$

unconditional fairness:  $\text{ufair} = \square \diamond \exists \bigcirc \text{start}$



$$\text{Sat}(\exists \bigcirc \text{start}) = \{\text{delivered}\}$$

$$\text{ufair} \hat{=} \square \diamond \text{delivered}$$



$$\Phi = \forall \square \forall \diamond \text{start}$$

$$\mathcal{T} \models_{\text{ufair}} \Phi \quad \checkmark$$

$$\mathcal{T} \models_{\text{wfair}} \Phi \quad ?$$

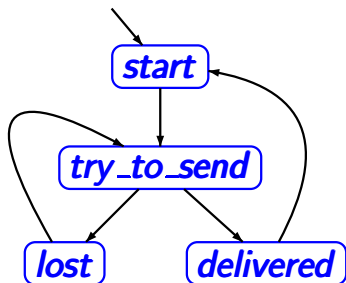
unconditional fairness:  $\text{ufair} = \square \diamond \exists \bigcirc \text{start}$

weak fairness:  $\text{wfair} = \diamond \square \exists \bigcirc \text{delivered} \rightarrow \square \diamond \text{delivered}$



# Simple communication protocol

CTLFAIR4.4-6



$$\Phi = \forall \square \forall \diamond \text{start}$$

$$\mathcal{T} \models_{\text{ufair}} \Phi \quad \checkmark$$

$$\mathcal{T} \models_{\text{wfair}} \Phi \quad ?$$

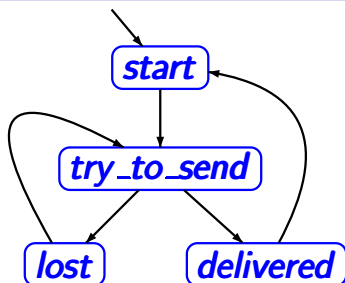
unconditional fairness:  $\text{ufair} = \square \diamond \exists \bigcirc \text{start}$

weak fairness:  $\text{wfair} = \diamond \square \boxed{\exists \bigcirc \text{delivered}} \rightarrow \square \diamond \text{delivered}$

$$\text{Sat}(\exists \bigcirc \text{delivered}) = \{\text{try\_to\_send}\}$$

# Simple communication protocol

CTLFAIR4.4-6



$$\Phi = \forall \square \forall \diamond \text{start}$$

$$\mathcal{T} \models_{\text{ufair}} \Phi \quad \checkmark$$

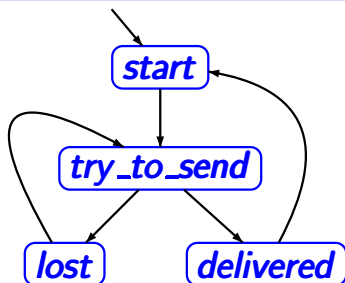
$$\mathcal{T} \models_{\text{wfair}} \Phi \quad ?$$

unconditional fairness:  $\text{ufair} = \square \diamond \exists \bigcirc \text{start}$

weak fairness:  $\text{wfair} = \diamond \square \exists \bigcirc \text{delivered} \rightarrow \square \diamond \text{delivered}$

$$\text{Sat}(\exists \bigcirc \text{delivered}) = \{\text{try\_to\_send}\}$$

$$\text{wfair} \hat{=} \diamond \square \text{try\_to\_send} \rightarrow \square \diamond \text{delivered}$$



$$\Phi = \forall \square \forall \diamond \text{start}$$

$$\mathcal{T} \models_{\text{ufair}} \Phi \quad \checkmark$$

$$\mathcal{T} \not\models_{\text{wfair}} \Phi \quad \text{wrong}$$

unconditional fairness:  $\text{ufair} = \square \diamond \exists \bigcirc \text{start}$

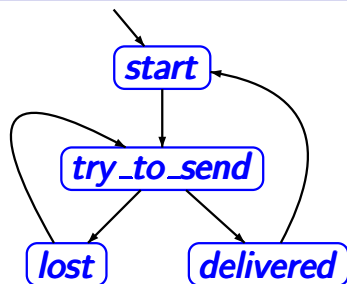
weak fairness:  $\text{wfair} = \diamond \square \exists \bigcirc \text{delivered} \rightarrow \square \diamond \text{delivered}$

$$\text{Sat}(\exists \bigcirc \text{delivered}) = \{\text{try\_to\_send}\}$$

$$\text{wfair} \hat{=} \diamond \square \text{try\_to\_send} \rightarrow \square \diamond \text{delivered}$$

# Simple communication protocol

CTLFAIR4.4-6



$$\Phi = \forall \square \forall \diamond \text{start}$$

$$\mathcal{T} \models_{\text{ufair}} \Phi \quad \checkmark$$

$$\mathcal{T} \not\models_{\text{wfair}} \Phi$$

$$\mathcal{T} \models_{\text{sfair}} \Phi \quad ?$$

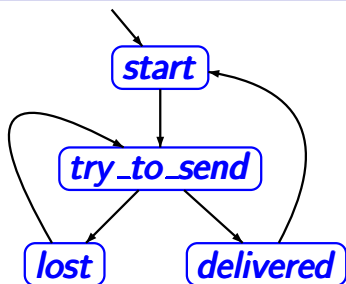
unconditional fairness:  $\text{ufair} = \square \diamond \exists \bigcirc \text{start}$

weak fairness:  $\text{wfair} = \diamond \square \exists \bigcirc \text{delivered} \rightarrow \square \diamond \text{delivered}$

strong fairness:  $\text{sfair} = \square \diamond \exists \bigcirc \text{delivered} \rightarrow \square \diamond \text{delivered}$

# Simple communication protocol

CTLFair4.4-6



$$\Phi = \forall \square \forall \diamond \text{start}$$

$$\mathcal{T} \models_{\text{ufair}} \Phi \quad \checkmark$$

$$\mathcal{T} \not\models_{\text{wfair}} \Phi$$

$$\mathcal{T} \models_{\text{sfair}} \Phi \quad ?$$

unconditional fairness:  $\text{ufair} = \square \diamond \exists \bigcirc \text{start}$

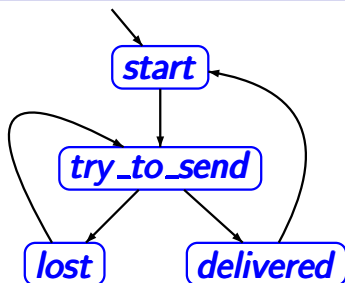
weak fairness:  $\text{wfair} = \diamond \square \exists \bigcirc \text{delivered} \rightarrow \square \diamond \text{delivered}$

strong fairness:  $\text{sfair} = \square \diamond \boxed{\exists \bigcirc \text{delivered}} \rightarrow \square \diamond \text{delivered}$

$$\text{Sat}(\exists \bigcirc \text{delivered}) = \{\text{try\_to\_send}\}$$

# Simple communication protocol

CTLFair4.4-6



$$\Phi = \forall \square \forall \diamond \text{start}$$

$$\mathcal{T} \models_{\text{ufair}} \Phi \quad \checkmark$$

$$\mathcal{T} \not\models_{\text{wfair}} \Phi$$

$$\mathcal{T} \models_{\text{sfair}} \Phi$$

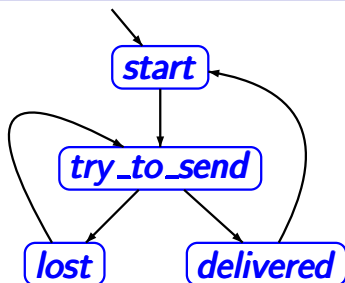
unconditional fairness:  $\text{ufair} = \square \diamond \exists \bigcirc \text{start}$

weak fairness:  $\text{wfair} = \diamond \square \exists \bigcirc \text{delivered} \rightarrow \square \diamond \text{delivered}$

strong fairness:  $\text{sfair} = \square \diamond \boxed{\exists \bigcirc \text{delivered}} \rightarrow \square \diamond \text{delivered}$

$$\text{Sat}(\exists \bigcirc \text{delivered}) = \{\text{try\_to\_send}\}$$

$$\text{sfair} \hat{=} \square \diamond \text{try\_to\_send} \rightarrow \square \diamond \text{delivered}$$



$$\Phi = \forall \square \forall \diamond \text{start}$$

$$\mathcal{T} \models_{\text{ufair}} \Phi \quad \checkmark$$

$$\mathcal{T} \not\models_{\text{wfair}} \Phi$$

$$\mathcal{T} \models_{\text{sfair}} \Phi \quad \checkmark$$

unconditional fairness:  $\text{ufair} = \square \diamond \exists \bigcirc \text{start}$

weak fairness:  $\text{wfair} = \diamond \square \exists \bigcirc \text{delivered} \rightarrow \square \diamond \text{delivered}$

strong fairness:  $\text{sfair} = \square \diamond \exists \bigcirc \text{delivered} \rightarrow \square \diamond \text{delivered}$

$$\text{Sat}(\exists \bigcirc \text{delivered}) = \{\text{try\_to\_send}\}$$

$$\text{sfair} \hat{=} \square \diamond \text{try\_to\_send} \rightarrow \square \diamond \text{delivered}$$

# Correct or wrong?

CTLFAIR4.4-7

If  $s \models \forall \diamond a$  where  $a \in AP$  then  $s \models_{fair} \forall \diamond a$



# Correct or wrong?

CTLFAIR4.4-7

If  $s \models \forall \diamond a$  where  $a \in AP$  then  $s \models_{fair} \forall \diamond a$

correct.

If  $s \models \forall \diamond a$  where  $a \in AP$  then  $s \models_{fair} \forall \diamond a$

**correct.** Note that:

$s \models \forall \varphi \implies$  for all  $\pi \in Paths(s)$ :  $\pi \models \varphi$

If  $s \models \forall \Diamond a$  where  $a \in AP$  then  $s \models_{fair} \forall \Diamond a$

**correct.** Note that:

$s \models \forall \varphi \implies$  for all  $\pi \in Paths(s)$ :  $\pi \models \varphi$

$\implies$  for all  $\pi \in Paths(s)$ :  
 $\pi \models_{fair}$  implies  $\pi \models \varphi$

If  $s \models \forall \Diamond a$  where  $a \in AP$  then  $s \models_{fair} \forall \Diamond a$

**correct.** Note that:

$s \models \forall \varphi \implies$  for all  $\pi \in Paths(s)$ :  $\pi \models \varphi$

$\implies$  for all  $\pi \in Paths(s)$ :  
 $\pi \models_{fair}$  implies  $\pi \models \varphi$

$\implies s \models_{fair} \forall \varphi$

# Correct or wrong?

CTLFAIR4.4-7

If  $s \models \forall \diamond a$  where  $a \in AP$  then  $s \models_{fair} \forall \diamond a$

correct.

If  $s \models \exists \diamond a$  where  $a \in AP$  then  $s \models_{fair} \exists \diamond a$

# Correct or wrong?

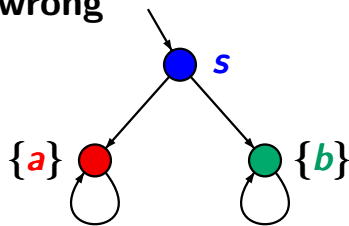
CTLFAIR4.4-7

If  $s \models \forall \diamond a$  where  $a \in AP$  then  $s \models_{fair} \forall \diamond a$

correct.

If  $s \models \exists \diamond a$  where  $a \in AP$  then  $s \models_{fair} \exists \diamond a$

wrong



$fair = \square \diamond b$

# Correct or wrong?

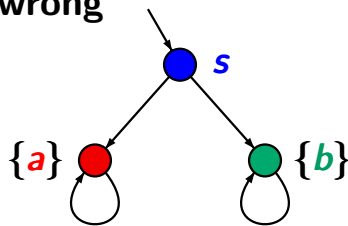
CTLFAIR4.4-7

If  $s \models \forall \diamond a$  where  $a \in AP$  then  $s \models_{fair} \forall \diamond a$

correct.

If  $s \models \exists \diamond a$  where  $a \in AP$  then  $s \models_{fair} \exists \diamond a$

wrong



$fair = \square \diamond b$

just one fair path ● ● ● . . .

# Correct or wrong?

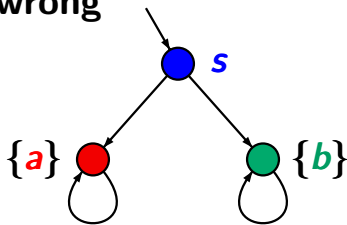
CTLFAIR4.4-7

If  $s \models \forall \diamond a$  where  $a \in AP$  then  $s \models_{fair} \forall \diamond a$

correct.

If  $s \models \exists \diamond a$  where  $a \in AP$  then  $s \models_{fair} \exists \diamond a$

wrong



$fair = \square \diamond b$

$s \not\models_{fair} \exists \diamond a$

just one fair path ● ● ● ● . . .



# Correct or wrong?

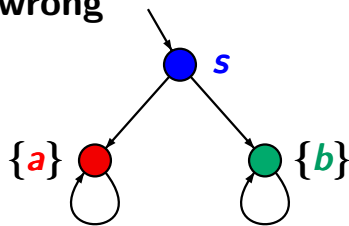
CTLFAIR4.4-7

If  $s \models \forall \diamond a$  where  $a \in AP$  then  $s \models_{fair} \forall \diamond a$

correct.

If  $s \models \exists \diamond a$  where  $a \in AP$  then  $s \models_{fair} \exists \diamond a$

wrong



$fair = \square \diamond b$

$s \not\models_{fair} \exists \diamond a$

$s \models \exists \diamond a$

just one fair path ● ● ● ● . . .

If  $s \models \forall \diamond a$  where  $a \in AP$  then  $s \models_{fair} \forall \diamond a$

**correct.**

Does the same condition hold if  $a$  is replaced with an arbitrary state formula ?

# Correct or wrong?

CTLFAIR4.4-8

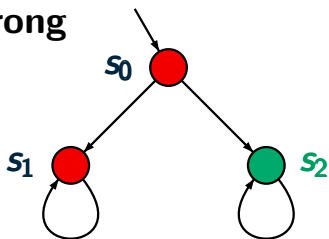
If  $s \models \forall \Diamond \exists \Box a$  then  $s \models_{\text{fair}} \forall \Diamond \exists \Box a$

# Correct or wrong?

CTLFAIR4.4-8

If  $s \models \forall \diamond \exists \square a$  then  $s \models_{\text{fair}} \forall \diamond \exists \square a$

wrong



● = {*b*}

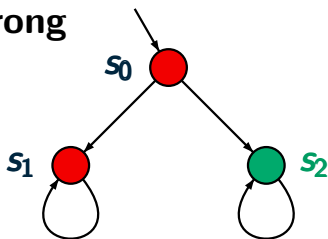
● = {*a*}

# Correct or wrong?

CTLFAIR4.4-8

If  $s \models \forall \diamond \exists \square a$  then  $s \models_{\text{fair}} \forall \diamond \exists \square a$

wrong



● = {*b*}

● = {*a*}

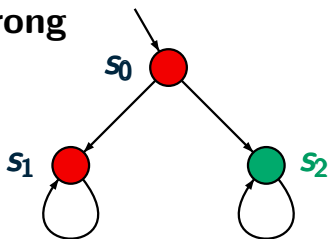
$Sat(\exists \square a) = \{s_0, s_1\}$

# Correct or wrong?

CTLFAIR4.4-8

If  $s \models \forall \diamond \exists \square a$  then  $s \models_{\text{fair}} \forall \diamond \exists \square a$

wrong



● = {*b*}

● = {*a*}

$$\text{Sat}(\exists \square a) = \{s_0, s_1\}$$

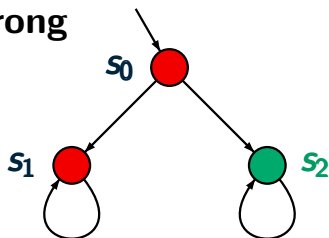
$$\text{Sat}(\forall \diamond \exists \square a) = \{s_0, s_1\}$$

# Correct or wrong?

CTLFAIR4.4-8

If  $s \models \forall \diamond \exists \square a$  then  $s \models_{\text{fair}} \forall \diamond \exists \square a$

wrong



● = {b}

● = {a}

$\text{fair} = \square \diamond b$

$\text{Sat}(\exists \square a) = \{s_0, s_1\}$

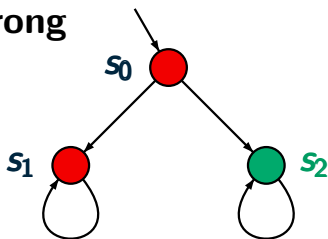
$\text{Sat}(\forall \diamond \exists \square a) = \{s_0, s_1\}$

# Correct or wrong?

CTLFAIR4.4-8

If  $s \models \forall \diamond \exists \square a$  then  $s \models_{\text{fair}} \forall \diamond \exists \square a$

wrong



● = {*b*}

● = {*a*}

$\text{fair} = \square \diamond b$

$\text{Sat}(\exists \square a) = \{s_0, s_1\}$

$\text{Sat}_{\text{fair}}(\exists \square a) = \emptyset$

$\text{Sat}(\forall \diamond \exists \square a) = \{s_0, s_1\}$

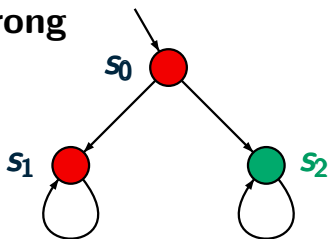


# Correct or wrong?

CTLFAIR4.4-8

If  $s \models \forall \diamond \exists \square a$  then  $s \models_{\text{fair}} \forall \diamond \exists \square a$

wrong



● = {*b*}

● = {*a*}

$\text{fair} = \square \diamond b$

$\text{Sat}(\exists \square a) = \{s_0, s_1\}$

$\text{Sat}_{\text{fair}}(\exists \square a) = \emptyset$

$\text{Sat}(\forall \diamond \exists \square a) = \{s_0, s_1\}$

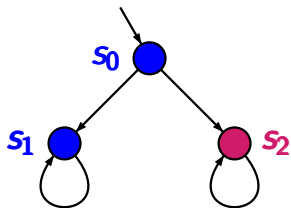
$\text{Sat}_{\text{fair}}(\forall \diamond \exists \square a) = \emptyset$

***Sat<sub>fair</sub>*( $\exists \square true$ ) = ?**

CTLFAIR4.4-11

$Sat_{fair}(\exists \square true) = ?$

CTLFAIR4.4-11



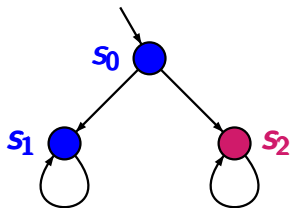
● = {*a*}

● = ∅

*fair* =  $\square \diamond a$

$Sat_{fair}(\exists \square true) = ?$

CTLFAIR4.4-11



● = {a}

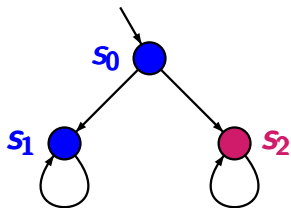
● = ∅

*fair* =  $\square \diamond a$

$Sat_{fair}(\exists \square true) = ?$

$Sat_{fair}(\exists \square true) = ?$

CTLFAIR4.4-11



● = {*a*}

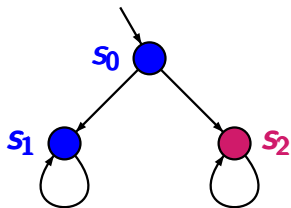
● = ∅

*fair* =  $\square \diamond a$

$Sat_{fair}(\exists \square true) = \{s_0, s_2\}$

$Sat_{fair}(\exists \square true) = ?$

CTLFair4.4-11



● = {*a*}

● = ∅

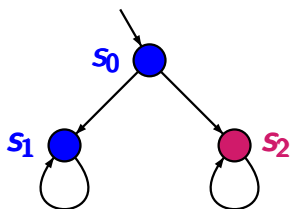
*fair* =  $\square \diamond a$

$Sat_{fair}(\exists \square true) = \{s_0, s_2\}$

$Sat_{fair}(\exists \square true) =$  set of states *s* that have at least one fair path

$Sat_{fair}(\exists \square true) = ?$

CTLFair4.4-11



● = {*a*}

● = ∅

*fair* =  $\square \diamond a$

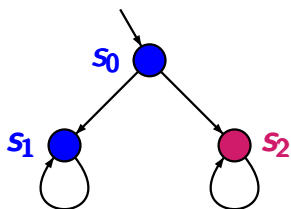
$Sat_{fair}(\exists \square true) = \{s_0, s_2\}$

$Sat_{fair}(\exists \square true) =$  set of states *s* that have at least one fair path

$= \{s : \exists \pi \in Paths(s) \text{ s.t. } \pi \models fair\}$

$Sat_{fair}(\exists \square true) = ?$

CTLFAIR4.4-11



● = {*a*}

● = ∅

*fair* =  $\square \diamond a$

$Sat_{fair}(\exists \square true) = \{s_0, s_2\}$

$Sat_{fair}(\exists \square true) =$  set of states *s* that have at least one fair path

$= \{s : \exists \pi \in Paths(s) \text{ s.t. } \pi \models fair\}$

*fair* is realizable iff

$Sat_{fair}(\exists \square true) \supseteq$  set of all reachable states





*given:*      finite transition system  $\mathcal{T}$   
                 CTL formula  $\Phi$   
                 CTL fairness assumption *fair*

*question:*    does  $\mathcal{T} \models_{\text{fair}} \Phi$  hold ?

*given:* finite transition system  $\mathcal{T}$   
CTL formula  $\Phi$   
CTL fairness assumption *fair*, e.g.,

$$\mathit{fair} = \bigwedge_{1 \leq i \leq k} \Box \Diamond \Psi_{i,1} \rightarrow \Box \Diamond \Psi_{i,2}$$

*question:* does  $\mathcal{T} \models_{\mathit{fair}} \Phi$  hold ?

*given:* finite transition system  $\mathcal{T}$   
CTL formula  $\Phi$   
CTL fairness assumption *fair*, e.g.,

$$\textit{fair} = \bigwedge_{1 \leq i \leq k} \Box \Diamond \Psi_{i,1} \rightarrow \Box \Diamond \Psi_{i,2}$$

*question:* does  $\mathcal{T} \models_{\textit{fair}} \Phi$  hold ?

*for simplicity:*

we suppose that  $\Phi$  is in **existential normal form**,  
i.e., a  $\forall$ -free CTL formula with temporal modalities

$$\exists \bigcirc, \exists \bigcup, \exists \Box$$

*given:* finite transition system  $\mathcal{T}$   
CTL formula  $\Phi$  in  $\exists$ -normal form  
CTL fairness assumption *fair*, e.g.,

$$\mathit{fair} = \bigwedge_{1 \leq i \leq k} \Box \Diamond \Psi_{i,1} \rightarrow \Box \Diamond \Psi_{i,2}$$

*question:* does  $\mathcal{T} \models_{\mathit{fair}} \Phi$  hold ?

*given:* finite transition system  $\mathcal{T}$   
CTL formula  $\Phi$  in  $\exists$ -normal form  
CTL fairness assumption *fair*, e.g.,

$$\mathit{fair} = \bigwedge_{1 \leq i \leq k} \Box \Diamond \Psi_{i,1} \rightarrow \Box \Diamond \Psi_{i,2}$$

*question:* does  $\mathcal{T} \models_{\mathit{fair}} \Phi$  hold ?

*preprocessing:* apply a standard CTL model checker to evaluate the CTL state subformulas of *fair*

*given:* finite transition system  $\mathcal{T}$   
CTL formula  $\Phi$  in  $\exists$ -normal form  
CTL fairness assumption *fair*, e.g.,

$$\mathit{fair} = \bigwedge_{1 \leq i \leq k} \Box \Diamond \Psi_{i,1} \rightarrow \Box \Diamond \Psi_{i,2}$$

*question:* does  $\mathcal{T} \models_{\mathit{fair}} \Phi$  hold ?

*preprocessing:* apply a standard CTL model checker to evaluate the CTL state subformulas of *fair*

- compute  $\mathit{Sat}(\Psi_{i,1})$  and  $\mathit{Sat}(\Psi_{i,2})$

*given:* finite transition system  $\mathcal{T}$   
CTL formula  $\Phi$  in  $\exists$ -normal form  
CTL fairness assumption *fair*, e.g.,

$$\text{fair} = \bigwedge_{1 \leq i \leq k} \square \diamond \Psi_{i,1} \rightarrow \square \diamond \Psi_{i,2}$$

*question:* does  $\mathcal{T} \models_{\text{fair}} \Phi$  hold ?

*preprocessing:* apply a standard CTL model checker to evaluate the CTL state subformulas of *fair*

- compute  $\text{Sat}(\Psi_{i,1})$  and  $\text{Sat}(\Psi_{i,2})$
- replace  $\Psi_{i,1}$  and  $\Psi_{i,2}$  with fresh atomic propositions  $b_i$  and  $c_i$ , respectively



*given:* finite transition system  $\mathcal{T}$   
CTL formula  $\Phi$  in  $\exists$ -normal form  
CTL fairness assumption *fair*, e.g.,

$$\mathit{fair} = \bigwedge_{1 \leq i \leq k} \square \diamond b_i \rightarrow \square \diamond c_i \text{ with } b_i, c_i \in AP$$

*question:* does  $\mathcal{T} \models_{\mathit{fair}} \Phi$  hold ?

*preprocessing:* apply a standard CTL model checker to evaluate the CTL state subformulas of *fair*

- compute  $\mathit{Sat}(\Psi_{i,1})$  and  $\mathit{Sat}(\Psi_{i,2})$
- replace  $\Psi_{i,1}$  and  $\Psi_{i,2}$  with fresh atomic propositions  $b_i$  and  $c_i$ , respectively

*given:*        finite transition system  $\mathcal{T}$   
                 CTL formula  $\Phi$  in  $\exists$ -normal form  
                 CTL fairness assumption *fair*  
*question:*    does  $\mathcal{T} \models_{\text{fair}} \Phi$  hold ?

1. ... preprocessing ...

*given:* finite transition system  $\mathcal{T}$   
CTL formula  $\Phi$  in  $\exists$ -normal form  
CTL fairness assumption *fair*

*question:* does  $\mathcal{T} \models_{\text{fair}} \Phi$  hold ?

1. ... preprocessing ...
2. Build the parse tree of  $\Phi$  and process it in bottom-up-manner.

*given:* finite transition system  $\mathcal{T}$   
CTL formula  $\Phi$  in  $\exists$ -normal form  
CTL fairness assumption *fair*

*question:* does  $\mathcal{T} \models_{\text{fair}} \Phi$  hold ?

1. ... preprocessing ...
2. Build the parse tree of  $\Phi$  and process it in bottom-up-manner. Treatment of:
  - *true*,  $a \in AP$ ,  $\wedge$ ,  $\neg$ : as for **standard CTL**

*given:*        finite transition system  $\mathcal{T}$   
                  CTL formula  $\Phi$  in  $\exists$ -normal form  
                  CTL fairness assumption *fair*

*question:*    does  $\mathcal{T} \models_{\text{fair}} \Phi$  hold ?

1. ... preprocessing ...
2. Build the parse tree of  $\Phi$  and process it in bottom-up-manner. Treatment of:
  - *true*,  $a \in AP$ ,  $\wedge$ ,  $\neg$ : as for **standard CTL**
  - $\exists O$ ,  $\exists U$ : via **standard CTL** model checking

*given:* finite transition system  $\mathcal{T}$   
CTL formula  $\Phi$  in  $\exists$ -normal form  
CTL fairness assumption *fair*

*question:* does  $\mathcal{T} \models_{\text{fair}} \Phi$  hold ?

1. ... preprocessing ...
2. Build the parse tree of  $\Phi$  and process it in bottom-up-manner. Treatment of:
  - *true*,  $a \in AP$ ,  $\wedge$ ,  $\neg$ : as for **standard CTL**
  - $\exists O$ ,  $\exists U$ : via **standard CTL** model checking
  - $\exists \square$ : via analysis of **SCCs**

recursive computation of the fair satisfaction sets:

$$Sat_{fair}(\Psi) = \{s \in S : s \models_{fair} \Psi\}$$

recursive computation of the fair satisfaction sets:

$$Sat_{fair}(\Psi) = \{s \in S : s \models_{fair} \Psi\}$$

*simple cases:*  $\Psi = true$  or  $\Psi = a \in AP$  or the outer most operator of  $\Psi$  is a negation or conjunction:



recursive computation of the fair satisfaction sets:

$$Sat_{fair}(\Psi) = \{s \in S : s \models_{fair} \Psi\}$$

simple cases:  $\Psi = true$  or  $\Psi = a \in AP$  or the outer most operator of  $\Psi$  is a negation or conjunction:

$$Sat_{fair}(true) = S$$

$$Sat_{fair}(a) = \{s \in S : a \in L(s)\}$$

$$Sat_{fair}(\neg\Psi) = S \setminus Sat_{fair}(\Psi)$$

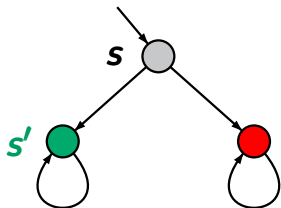
$$Sat_{fair}(\Psi_1 \wedge \Psi_2) = Sat_{fair}(\Psi_1) \cap Sat_{fair}(\Psi_2)$$

*given:* finite transition system  $\mathcal{T}$   
CTL formula  $\Phi$  in  $\exists$ -normal form  
CTL fairness assumption *fair*

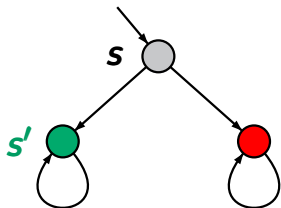
*question:* does  $\mathcal{T} \models_{\text{fair}} \Phi$  hold ?

1. ... preprocessing ...
2. Build the parse tree of  $\Phi$  and process it in bottom-up-manner. Treatment of:
  - *true*,  $a \in AP$ ,  $\wedge$ ,  $\neg$ : as for standard CTL
  - $\exists O$ ,  $\exists U$ : via **standard CTL model checking**
  - $\exists \square$ : via analysis of SCCs



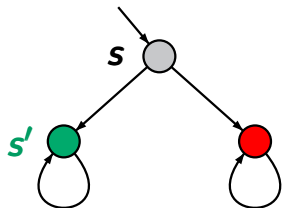


$$\text{fair} = \square\blacklozenge \text{red}$$



$fair = \square\lozenge red$

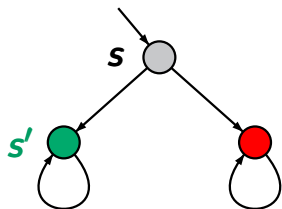
$s \not\models_{fair} \exists\bigcirc green$



$$fair = \square\lozenge red$$

$$s \not\models_{fair} \exists\bigcirc green$$

$$as\ s' \not\models_{fair} \exists\square true$$



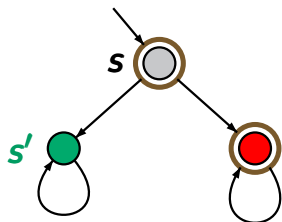
$$fair = \square\lozenge red$$

$$s \not\models_{fair} \exists\bigcirc green$$

$$\text{as } s' \not\models_{fair} \exists\square true$$

introduce an additional atomic proposition  $a_{fair}$   
 s.t. for all states  $s$ :

$$a_{fair} \in L(s) \text{ iff } s \models_{fair} \exists\square true$$



$$fair = \Box\Diamond red$$

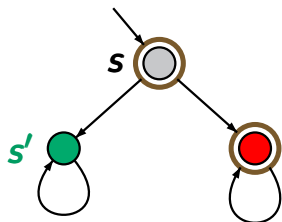
$$s \not\models_{fair} \exists\bigcirc green$$

$$\text{as } s' \not\models_{fair} \exists\Box true$$

introduce an additional atomic proposition  $a_{fair}$   
 s.t. for all states  $s$ :

$$a_{fair} \in L(s) \text{ iff } s \models_{fair} \exists\Box true$$





$$fair = \square\lozenge red$$

$$s \not\models_{fair} \exists\bigcirc green$$

$$\text{as } s' \not\models_{fair} \exists\square true$$

introduce an additional atomic proposition  $a_{fair}$   
s.t. for all states  $s$ :

$$a_{fair} \in L(s) \text{ iff } s \models_{fair} \exists\square true$$

This yields that for all  $b \in AP$  and all states  $s$ :

$$s \models_{fair} \exists\bigcirc b \text{ iff } s \models \exists\bigcirc (b \wedge a_{fair})$$

introduce an additional atomic proposition  $a_{fair}$  s.t.

$$a_{fair} \in L(s) \text{ iff } s \models_{fair} \exists\Box true$$

This yields that for all  $b, c \in AP$  and all states  $s$ :

$$s \models_{fair} \exists\bigcirc b \quad \text{iff} \quad s \models \exists\bigcirc(b \wedge a_{fair})$$

$$s \models_{fair} \exists(c \bigcup b) \quad \text{iff} \quad ?$$

introduce an additional atomic proposition  $a_{fair}$  s.t.

$$a_{fair} \in L(s) \text{ iff } s \models_{fair} \exists\Box true$$

This yields that for all  $b, c \in AP$  and all states  $s$ :

$$s \models_{fair} \exists\bigcirc b \quad \text{iff} \quad s \models \exists\bigcirc(b \wedge a_{fair})$$

$$s \models_{fair} \exists(c \mathbf{U} b) \quad \text{iff} \quad s \models \exists(c \mathbf{U}(b \wedge a_{fair}))$$

introduce an additional atomic proposition  $a_{fair}$  s.t.

$$a_{fair} \in L(s) \text{ iff } s \models_{fair} \exists\Box true$$

This yields that for all  $b, c \in AP$  and all states  $s$ :

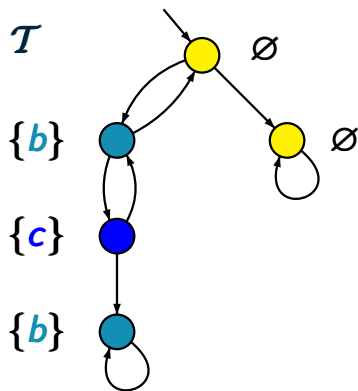
$$\begin{aligned} s \models_{fair} \exists\bigcirc b & \quad \text{iff} \quad s \models \exists\bigcirc(b \wedge a_{fair}) \\ s \models_{fair} \exists(c \mathbf{U} b) & \quad \text{iff} \quad s \models \exists(c \mathbf{U}(b \wedge a_{fair})) \end{aligned}$$

hence: treatment of  $\exists\bigcirc$  and  $\exists\mathbf{U}$  for FairCTL via

- special methods to compute  $Sat_{fair}(\exists\Box true)$
- standard CTL model checking for  $\exists\bigcirc$  and  $\exists\mathbf{U}$

# Example: treatment of $\exists\Diamond$

CTLFAIR4.4-15

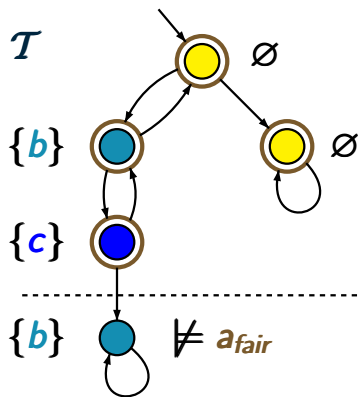


CTL formula  $\exists\Diamond c$

strong fairness assumption:  $fair = \Box\Diamond b \rightarrow \Box\Diamond c$

# Example: treatment of $\exists\Diamond$

CTLFAIR4.4-15



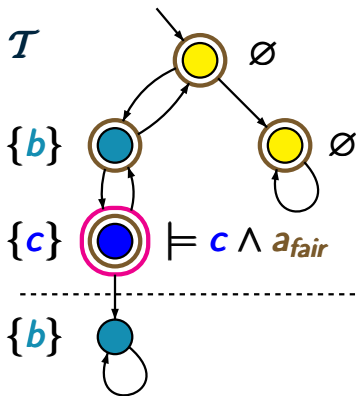
CTL formula  $\exists\Diamond c$

$\downarrow$   
 $\exists\Diamond (c \wedge a_{fair})$

strong fairness assumption:  $fair = \Box\Diamond b \rightarrow \Box\Diamond c$

# Example: treatment of $\exists\Diamond$

CTLFAIR4.4-15

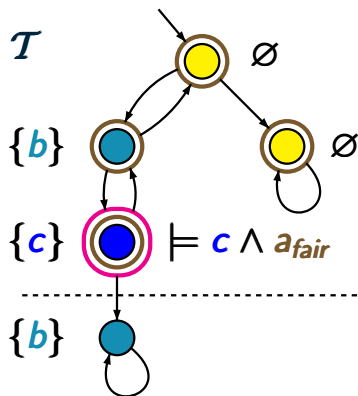


CTL formula  $\exists\Diamond c$

$\downarrow$

$\exists\Diamond (c \wedge a_{fair})$

strong fairness assumption:  $fair = \Box\Diamond b \rightarrow \Box\Diamond c$



CTL formula  $\exists\Diamond c$

$\downarrow$

$\exists\Diamond (c \wedge a_{fair})$

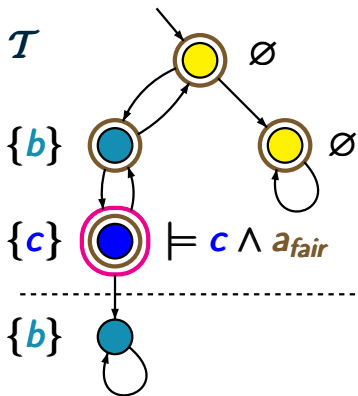
strong fairness assumption:  $fair = \Box\Diamond b \rightarrow \Box\Diamond c$

$\mathcal{T} \models \exists\Diamond (c \wedge a_{fair})$



# Example: treatment of $\exists\Diamond$

CTLFAIR4.4-15

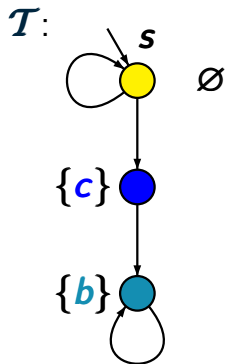


CTL formula  $\exists\Diamond c$

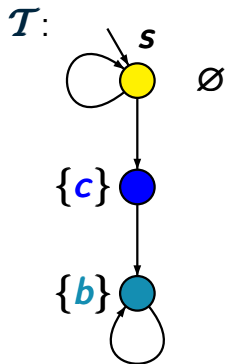
$\exists\Diamond (c \wedge a_{fair})$

strong fairness assumption:  $fair = \Box\Diamond b \rightarrow \Box\Diamond c$

$\mathcal{T} \models \exists\Diamond (c \wedge a_{fair}) \implies \mathcal{T} \models_{fair} \exists\Diamond c$



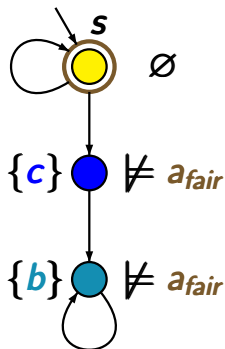
$$\mathcal{T} \models \exists(\neg b U c)$$



strong fairness assumption:  $fair = \Box \Diamond b \rightarrow \Box \Diamond c$

$$\mathcal{T} \models \exists(\neg b U c)$$

$\mathcal{T}$ :



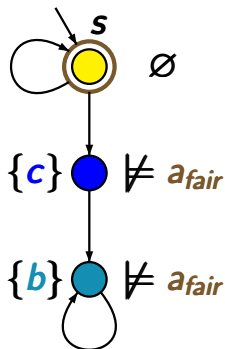
strong fairness assumption:  $fair = \Box \Diamond b \rightarrow \Box \Diamond c$

$$\mathcal{T} \models \exists(\neg b U c)$$

# Example: treatment of $\exists U$

CTLFAIR4.4-17

$\mathcal{T}$ :



$$\text{Sat}(c \wedge a_{fair}) = \emptyset$$

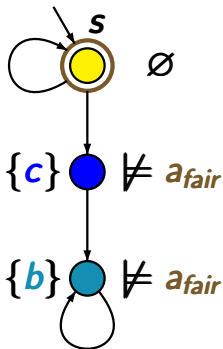
strong fairness assumption:  $fair = \Box \Diamond b \rightarrow \Box \Diamond c$

$$\mathcal{T} \models \exists(\neg b U c)$$

# Example: treatment of $\exists U$

CTLFAIR4.4-17

$\mathcal{T}$ :



$$s \not\models \exists(\neg b U (c \wedge a_{fair}))$$

$\Uparrow$

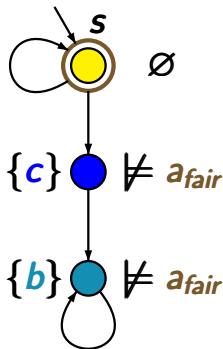
$$Sat(c \wedge a_{fair}) = \emptyset$$

strong fairness assumption:  $fair = \Box \Diamond b \rightarrow \Box \Diamond c$

$$\mathcal{T} \models \exists(\neg b U c)$$

# Example: treatment of $\exists U$

CTLFAIR4.4-17

 $\mathcal{T}$ :

$$s \not\models_{\text{fair}} \exists(\neg b U c)$$

 $\uparrow$ 

$$s \not\models \exists(\neg b U (c \wedge a_{\text{fair}}))$$

 $\uparrow$ 

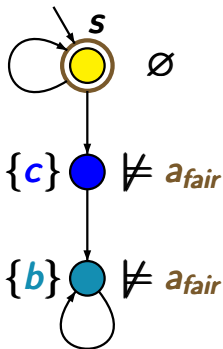
$$\text{Sat}(c \wedge a_{\text{fair}}) = \emptyset$$

strong fairness assumption:  $\text{fair} = \Box \Diamond b \rightarrow \Box \Diamond c$

$$\boxed{\mathcal{T} \models \exists(\neg b U c)}$$

# Example: treatment of $\exists U$

CTLFAIR4.4-17

 $\mathcal{T}$ :

$$s \not\models_{fair} \exists(\neg b U c)$$

 $\uparrow$ 

$$s \not\models \exists(\neg b U (c \wedge a_{fair}))$$

 $\uparrow$ 

$$Sat(c \wedge a_{fair}) = \emptyset$$

strong fairness assumption:  $fair = \Box \Diamond b \rightarrow \Box \Diamond c$

$$\mathcal{T} \models \exists(\neg b U c), \quad \text{but } \mathcal{T} \not\models_{fair} \exists(\neg b U c)$$



# Correct or wrong?

CTLFAIR4.4-16

$$s \models_{\text{fair}} \exists \bigcirc \exists (c \text{ U } b) \quad \text{iff} \quad s \models \exists \bigcirc \exists (c \text{ U } (b \wedge a_{\text{fair}}))$$

# Correct or wrong?

CTLFAIR4.4-16

$$s \models_{\text{fair}} \exists \bigcirc \exists (c \text{ U } b) \quad \text{iff} \quad s \models \exists \bigcirc \exists (c \text{ U } (b \wedge a_{\text{fair}}))$$

correct.

$$s \models_{\text{fair}} \exists \bigcirc \exists (c \text{ U } b) \quad \text{iff} \quad s \models \exists \bigcirc \exists (c \text{ U } (b \wedge a_{\text{fair}}))$$

correct. Note that:

if  $s_0 s_1 \dots s_{n-1} s_n$  is a path fragment from  $s_0 = s$  s.t.  
 $s_n \models a_{\text{fair}}$  then  $s_0, s_1, \dots, s_{n-1} \models a_{\text{fair}}$ .

$$s \models_{\text{fair}} \exists \bigcirc \exists (c \text{ U } b) \quad \text{iff} \quad s \models \exists \bigcirc \exists (c \text{ U } (b \wedge a_{\text{fair}}))$$

**correct.** Note that:

if  $s_0 s_1 \dots s_{n-1} s_n$  is a path fragment from  $s_0 = s$  s.t.  
 $s_n \models a_{\text{fair}}$  then  $s_0, s_1, \dots, s_{n-1} \models a_{\text{fair}}$ . Hence:

$$s \models \exists \bigcirc \exists (c \text{ U } (b \wedge a_{\text{fair}}))$$

$$\iff s \models \exists \bigcirc \exists ((c \wedge a_{\text{fair}}) \text{ U } (b \wedge a_{\text{fair}}))$$

$$s \models_{\text{fair}} \exists \bigcirc \exists (c \text{ U } b) \quad \text{iff} \quad s \models \exists \bigcirc \exists (c \text{ U } (b \wedge a_{\text{fair}}))$$

**correct.** Note that:

if  $s_0 s_1 \dots s_{n-1} s_n$  is a path fragment from  $s_0 = s$  s.t.  
 $s_n \models a_{\text{fair}}$  then  $s_0, s_1, \dots, s_{n-1} \models a_{\text{fair}}$ . Hence:

$$s \models \exists \bigcirc \exists (c \text{ U } (b \wedge a_{\text{fair}}))$$

$$\iff s \models \exists \bigcirc \exists ((c \wedge a_{\text{fair}}) \text{ U } (b \wedge a_{\text{fair}}))$$

$$\iff s \models \exists \bigcirc (\exists (c \text{ U } (b \wedge a_{\text{fair}})) \wedge a_{\text{fair}})$$

$$s \models_{\text{fair}} \exists \bigcirc \exists (c \text{ U } b) \quad \text{iff} \quad s \models \exists \bigcirc \exists (c \text{ U } (b \wedge a_{\text{fair}}))$$

correct. Note that:

if  $s_0 s_1 \dots s_{n-1} s_n$  is a path fragment from  $s_0 = s$  s.t.  
 $s_n \models a_{\text{fair}}$  then  $s_0, s_1, \dots, s_{n-1} \models a_{\text{fair}}$ . Hence:

$$s \models \exists \bigcirc \exists (c \text{ U } (b \wedge a_{\text{fair}}))$$

$$\iff s \models \exists \bigcirc \exists ((c \wedge a_{\text{fair}}) \text{ U } (b \wedge a_{\text{fair}}))$$

$$\iff s \models \exists \bigcirc (\exists (c \text{ U } (b \wedge a_{\text{fair}})) \wedge a_{\text{fair}})$$

$$\iff s \models_{\text{fair}} \exists \bigcirc \exists (c \text{ U } b)$$

# Correct or wrong?

CTLFAIR4.4-16

$$s \models_{\text{fair}} \exists \bigcirc \exists (c \text{ U } b) \quad \text{iff} \quad s \models \exists \bigcirc \exists (c \text{ U } (b \wedge a_{\text{fair}}))$$

correct.

$$s \models_{\text{fair}} \exists \bigcirc \exists (c \text{ U } b) \quad \text{iff} \quad s \models \exists \bigcirc (\exists (c \text{ U } b) \wedge a_{\text{fair}})$$

# Correct or wrong?

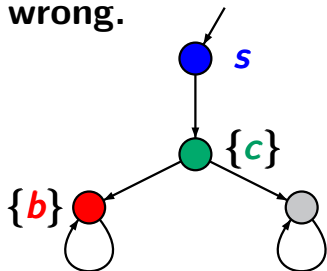
CTLFAIR4.4-16

$$s \models_{\text{fair}} \exists \bigcirc \exists (c \text{ U } b) \quad \text{iff} \quad s \models \exists \bigcirc \exists (c \text{ U } (b \wedge a_{\text{fair}}))$$

correct.

$$s \models_{\text{fair}} \exists \bigcirc \exists (c \text{ U } b) \quad \text{iff} \quad s \models \exists \bigcirc (\exists (c \text{ U } b) \wedge a_{\text{fair}})$$

wrong.



$$\text{fair} = \square \diamond \text{gray}$$



# Correct or wrong?

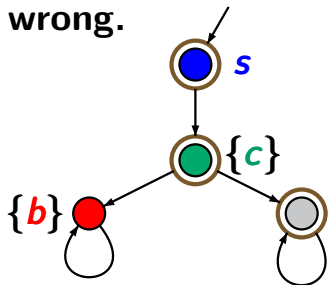
CTLFAIR4.4-16

$$s \models_{\text{fair}} \exists \bigcirc \exists (c \text{ U } b) \quad \text{iff} \quad s \models \exists \bigcirc \exists (c \text{ U } (b \wedge a_{\text{fair}}))$$

correct.

$$s \models_{\text{fair}} \exists \bigcirc \exists (c \text{ U } b) \quad \text{iff} \quad s \models \exists \bigcirc (\exists (c \text{ U } b) \wedge a_{\text{fair}})$$

wrong.



$$\text{fair} = \square \diamond \text{gray}$$

# Correct or wrong?

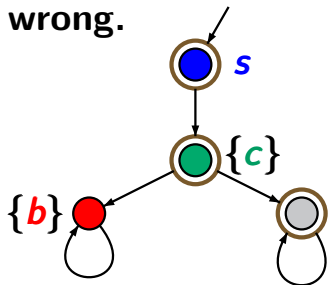
CTLFAIR4.4-16

$$s \models_{\text{fair}} \exists \bigcirc \exists (c \cup b) \quad \text{iff} \quad s \models \exists \bigcirc \exists (c \cup (b \wedge a_{\text{fair}}))$$

correct.

$$s \models_{\text{fair}} \exists \bigcirc \exists (c \cup b) \quad \text{iff} \quad s \models \exists \bigcirc (\exists (c \cup b) \wedge a_{\text{fair}})$$

wrong.



$$\text{fair} = \square \diamond \text{gray}$$

$$\text{Sat}_{\text{fair}}(\exists (c \cup b)) = \emptyset$$

# Correct or wrong?

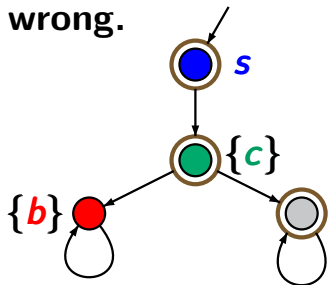
CTLFAIR4.4-16

$$s \models_{\text{fair}} \exists \bigcirc \exists (c \text{ U } b) \quad \text{iff} \quad s \models \exists \bigcirc \exists (c \text{ U } (b \wedge a_{\text{fair}}))$$

correct.

$$s \models_{\text{fair}} \exists \bigcirc \exists (c \text{ U } b) \quad \text{iff} \quad s \models \exists \bigcirc (\exists (c \text{ U } b) \wedge a_{\text{fair}})$$

wrong.



$$\text{fair} = \square \diamond \text{gray}$$

$$\text{Sat}_{\text{fair}}(\exists (c \text{ U } b)) = \emptyset$$

$$s \not\models_{\text{fair}} \exists \bigcirc \exists (c \text{ U } b)$$

# Correct or wrong?

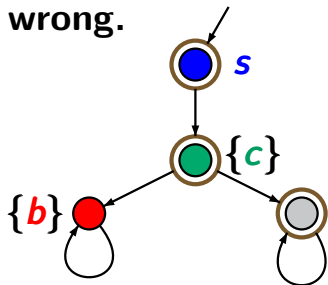
CTLFAIR4.4-16

$$s \models_{\text{fair}} \exists \bigcirc \exists (c \cup b) \quad \text{iff} \quad s \models \exists \bigcirc \exists (c \cup (b \wedge a_{\text{fair}}))$$

correct.

$$s \models_{\text{fair}} \exists \bigcirc \exists (c \cup b) \quad \text{iff} \quad s \models \exists \bigcirc (\exists (c \cup b) \wedge a_{\text{fair}})$$

wrong.



$$\text{fair} = \square \diamond \text{gray}$$

$$\text{Sat}_{\text{fair}}(\exists (c \cup b)) = \emptyset$$

$$s \not\models_{\text{fair}} \exists \bigcirc \exists (c \cup b)$$

$$s \models \exists \bigcirc (\exists (c \cup b) \wedge a_{\text{fair}})$$

# Correct or wrong?

CTLFAIR4.4-23

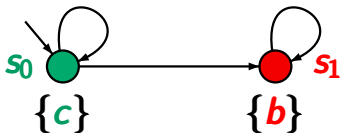
$$s \models_{fair} \exists \square c \quad \text{iff} \quad s \models \exists \square (c \wedge a_{fair})$$

# Correct or wrong?

CTLFAIR4.4-23

$$s \models_{\text{fair}} \exists \square c \text{ iff } s \models \exists \square (c \wedge a_{\text{fair}})$$

wrong.



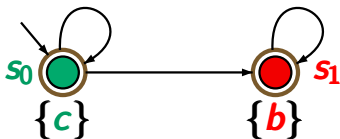
$$\text{fair} = \square \diamond b$$

# Correct or wrong?

CTLFAIR4.4-23

$$s \models_{\text{fair}} \exists \square c \quad \text{iff} \quad s \models \exists \square (c \wedge a_{\text{fair}})$$

wrong.



$$\text{fair} = \square \diamond b$$

$$s_0 \models a_{\text{fair}}$$

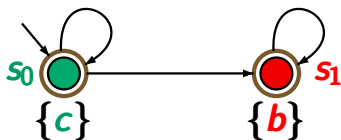
$$s_1 \models a_{\text{fair}}$$

# Correct or wrong?

CTLFAIR4.4-23

$$s \models_{\text{fair}} \exists \square c \quad \text{iff} \quad s \models \exists \square (c \wedge a_{\text{fair}})$$

wrong.



$$\text{fair} = \square \diamond b$$

$$s_0 \models a_{\text{fair}}$$

$$s_1 \models a_{\text{fair}}$$

regard state  $s = s_0$ :

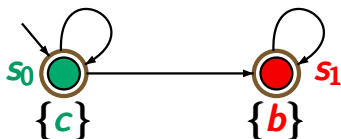


# Correct or wrong?

CTLFAIR4.4-23

$$s \models_{fair} \exists \square c \text{ iff } s \models \exists \square (c \wedge a_{fair})$$

wrong.



$$fair = \square \diamond b$$

$$s_0 \models a_{fair}$$

$$s_1 \models a_{fair}$$

regard state  $s = s_0$ :

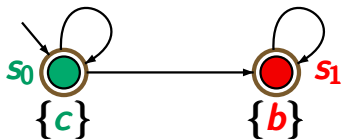
$$s \models \exists \square (c \wedge a_{fair}),$$

# Correct or wrong?

CTLFAIR4.4-23

$$s \models_{fair} \exists \square c \text{ iff } s \models \exists \square (c \wedge a_{fair})$$

wrong.



$$fair = \square \diamond b$$

$$s_0 \models a_{fair}$$

$$s_1 \models a_{fair}$$

regard state  $s = s_0$ :

$$s \models \exists \square (c \wedge a_{fair}),$$

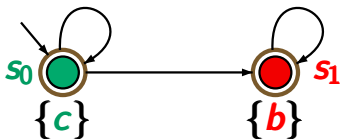
$$\uparrow$$
$$\text{path } \pi = s_0 s_0 s_0 s_0 \dots \models \square (c \wedge a_{fair})$$

# Correct or wrong?

CTLFAIR4.4-23

$$s \models_{fair} \exists \square c \text{ iff } s \models \exists \square (c \wedge a_{fair})$$

wrong.



$$fair = \square \diamond b$$

$$s_0 \models a_{fair}$$

$$s_1 \models a_{fair}$$

regard state  $s = s_0$ :

$$s \models \exists \square (c \wedge a_{fair}), \text{ but } s \not\models_{fair} \exists \square c$$

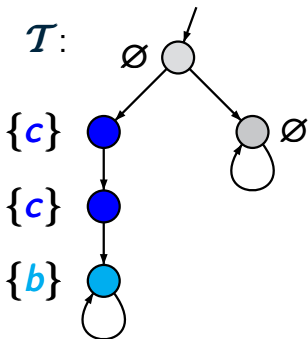
$$\begin{array}{c} \uparrow \\ \text{path } \pi = s_0 s_0 s_0 s_0 \dots \models \square (c \wedge a_{fair}) \end{array}$$

*given:* finite transition system  $\mathcal{T}$   
CTL formula  $\Phi$  in  $\exists$ -normal form  
CTL fairness assumption *fair*

*question:* does  $\mathcal{T} \models_{\text{fair}} \Phi$  hold ?

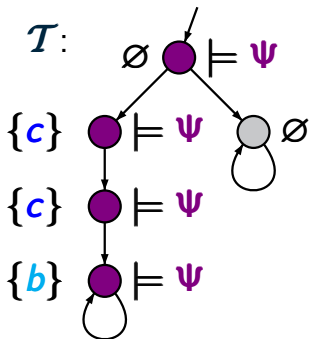
1. ... preprocessing ...
2. Build the parse tree of  $\Phi$  and process it in bottom-up-manner. Treatment of:
  - *true*,  $a \in AP$ ,  $\wedge$ ,  $\neg$ : as for standard CTL
  - $\exists O$ ,  $\exists U$ : via standard CTL model checking
  - $\exists \square$ : via analysis of **SCCs**

*fair* =  $\square \diamond b \rightarrow \square \diamond c$ , CTL state formula  $\Psi$



$\mathcal{T} \models_{\text{fair}} \exists \square \Psi$  ?

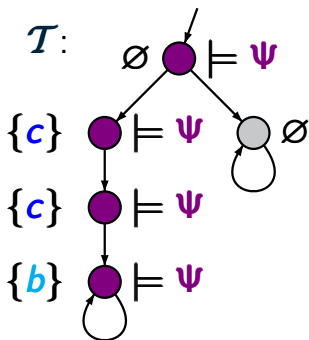
*fair* =  $\square \diamond b \rightarrow \square \diamond c$ , CTL state formula  $\Psi$



$\mathcal{T} \models_{\text{fair}} \exists \square \Psi$  ?

1. calculate  $\text{Sat}_{\text{fair}}(\Psi)$

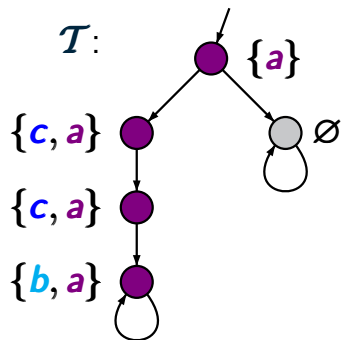
*fair* =  $\square \diamond b \rightarrow \square \diamond c$ , CTL state formula  $\Psi$



$\mathcal{T} \models_{\text{fair}} \exists \square \Psi$  ?

1. calculate  $\text{Sat}_{\text{fair}}(\Psi)$
2. replace  $\Psi$  with a fresh atomic proposition  $a = a_{\Psi}$

*fair* =  $\square \diamond b \rightarrow \square \diamond c$ , CTL state formula  $\Psi$

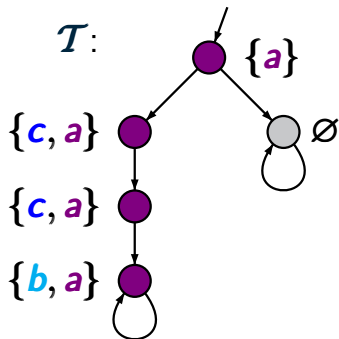


$\mathcal{T} \models_{\text{fair}} \exists \square \Psi$  ?

1. calculate  $\text{Sat}_{\text{fair}}(\Psi)$
2. replace  $\Psi$  with a fresh atomic proposition  $a = a_{\Psi}$



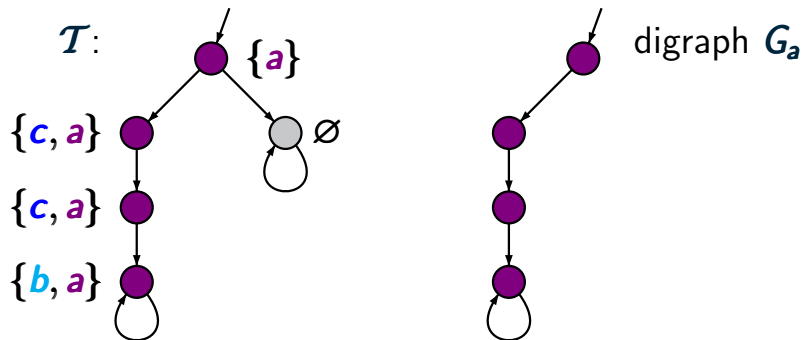
*fair* =  $\square \diamond b \rightarrow \square \diamond c$ , CTL state formula  $\Psi$



$\mathcal{T} \models_{\text{fair}} \exists \square \Psi$  ?

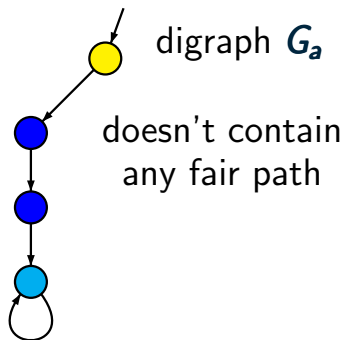
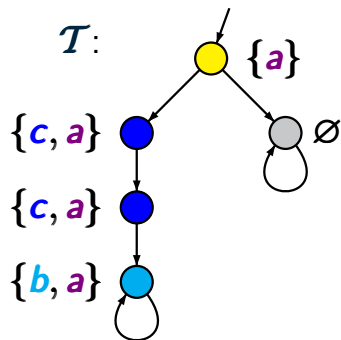
1. calculate  $\text{Sat}_{\text{fair}}(\Psi)$
2. replace  $\Psi$  with a fresh atomic proposition  $a = a_{\Psi}$
3. calculate  $\text{Sat}_{\text{fair}}(\exists \square a)$

*fair* =  $\Box \Diamond b \rightarrow \Box \Diamond c$ , CTL state formula  $\Psi$



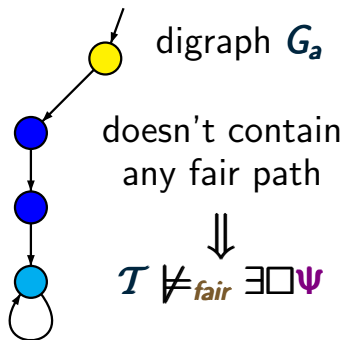
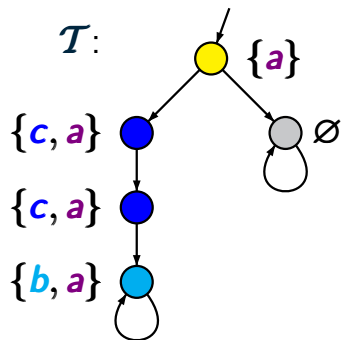
1. calculate  $Sat_{fair}(\Psi)$
2. replace  $\Psi$  with a fresh atomic proposition  $a = a_\Psi$
3. calculate  $Sat_{fair}(\exists \Box a)$

*fair* =  $\square \diamond b \rightarrow \square \diamond c$ , CTL state formula  $\Psi$



1. calculate  $Sat_{fair}(\Psi)$
2. replace  $\Psi$  with a fresh atomic proposition  $a = a_\Psi$
3. calculate  $Sat_{fair}(\exists \square a)$

*fair* =  $\square \diamond b \rightarrow \square \diamond c$ , CTL state formula  $\Psi$



1. calculate  $Sat_{\text{fair}}(\Psi)$
2. replace  $\Psi$  with a fresh atomic proposition  $a = a_\Psi$
3. calculate  $Sat_{\text{fair}}(\exists \square a) = \emptyset$

- given:* finite TS  $\mathcal{T}$ , atomic proposition  $a$   
CTL fairness assumption *fair*
- goal:* compute  $Sat_{fair}(\exists\Box a)$

*given:* finite TS  $\mathcal{T}$ , atomic proposition  $a$   
CTL fairness assumption *fair*

*goal:* compute  $Sat_{fair}(\exists\Box a)$

if all states are labeled by  $a$ :

this technique yields a method  
to compute  $Sat_{fair}(\exists\Box true)$

*given:* finite TS  $\mathcal{T}$ , atomic proposition  $a$   
CTL fairness assumption *fair*

*goal:* compute  $Sat_{fair}(\exists\Box a)$

if all states are labeled by  $a$ :

this technique yields a method  
to compute  $Sat_{fair}(\exists\Box true)$

*here:* explanations only for strong fairness

$$fair = \bigwedge_{1 \leq i \leq k} (\Box\Diamond b_i \rightarrow \Box\Diamond c_i)$$

$$\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box\Diamond b_i \rightarrow \Box\Diamond c_i)$$



$$\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box\Diamond b_i \rightarrow \Box\Diamond c_i)$$

$s \models_{\text{fair}} \exists\Box a$  iff there exists a path fragment

$$s_0 s_1 \dots s_n \dots s_{n+r}$$

$$\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box\Diamond b_i \rightarrow \Box\Diamond c_i)$$

$s \models_{\text{fair}} \exists\Box a$  iff there exists a path fragment

$$s_0 s_1 \dots s_n \dots s_{n+r}$$

such that  $r \geq 1$ ,  $s = s_0$ ,  $s_n = s_{n+r}$  and ...

$$\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box\Diamond b_i \rightarrow \Box\Diamond c_i)$$

$s \models_{\text{fair}} \exists\Box a$  iff there exists a path fragment

$$s_0 s_1 \dots s_n \dots s_{n+r}$$

such that  $r \geq 1$ ,  $s = s_0$ ,  $s_n = s_{n+r}$  and

- $s_j \models a$  for all  $0 \leq j \leq n+r$

$$\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box\Diamond b_i \rightarrow \Box\Diamond c_i)$$

$s \models_{\text{fair}} \exists\Box a$  iff there exists a path fragment

$$s_0 s_1 \dots s_n \dots s_{n+r}$$

such that  $r \geq 1$ ,  $s = s_0$ ,  $s_n = s_{n+r}$  and

- $s_j \models a$  for all  $0 \leq j \leq n+r$
- the path  $s_0 s_1 \dots s_n (s_{n+1} \dots s_{n+r})^\omega$  is fair, i.e.,

$$\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box\Diamond b_i \rightarrow \Box\Diamond c_i)$$

$s \models_{\text{fair}} \exists\Box a$  iff there exists a path fragment

$$s_0 s_1 \dots s_n \dots s_{n+r}$$

such that  $r \geq 1$ ,  $s = s_0$ ,  $s_n = s_{n+r}$  and

- $s_j \models a$  for all  $0 \leq j \leq n+r$
- the path  $s_0 s_1 \dots s_n (s_{n+1} \dots s_{n+r})^\omega$  is fair, i.e.,  
for all  $1 \leq i \leq k$ :

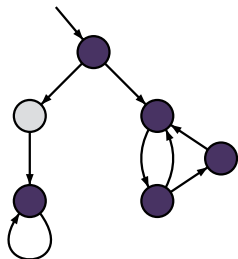
$$\{s_{n+1}, \dots, s_{n+r}\} \cap \text{Sat}(b_i) = \emptyset$$

$$\text{or } \{s_{n+1}, \dots, s_{n+r}\} \cap \text{Sat}(c_i) \neq \emptyset$$

# $\exists \Box a$ under strong fairness

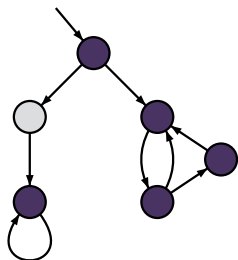
CTLFAIR4.4-19A

does  $\mathcal{T} \models_{\text{fair}} \exists \Box a$  hold ?



$\bullet \models a$      $\circ \not\models a$

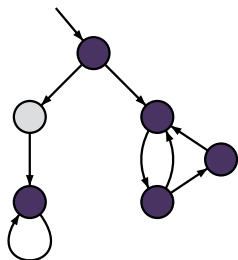
does  $\mathcal{T} \models_{\text{fair}} \exists \Box a$  hold ?



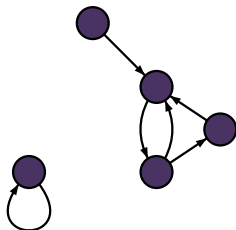
$\bullet \models a$      $\circ \not\models a$

analyze the digraph  $G_a$  that results from  $\mathcal{T}$  by removing all states  $s$  with  $s \not\models a$

does  $\mathcal{T} \models_{\text{fair}} \exists \Box a$  hold ?



digraph  $G_a$

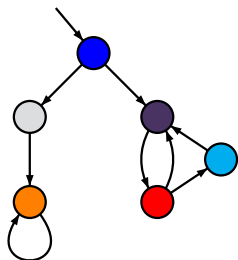


$\bullet \models a$      $\circ \not\models a$

analyze the digraph  $G_a$  that results from  $\mathcal{T}$  by removing all states  $s$  with  $s \not\models a$



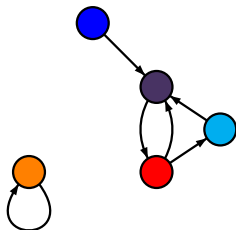
does  $\mathcal{T} \models_{\text{fair}} \exists \square a$  hold ?



$$\text{orange} \hat{=} \{b_1\} \quad \text{red} \hat{=} \{c_1\}$$

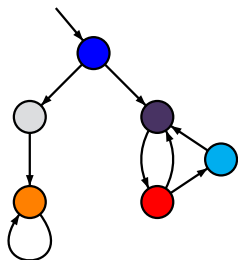
$$\text{cyan} \hat{=} \{b_2\} \quad \text{blue} \hat{=} \{c_2\}$$

digraph  $G_a$



$$\text{fair} = (\square \diamond b_1 \rightarrow \square \diamond c_1) \wedge (\square \diamond b_2 \rightarrow \square \diamond c_2)$$

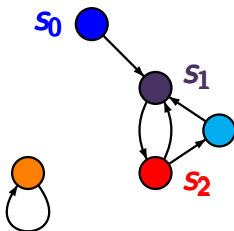
does  $\mathcal{T} \models_{\text{fair}} \exists \square a$  hold ?



$$\text{orange} \hat{=} \{b_1\} \quad \text{red} \hat{=} \{c_1\}$$

$$\text{cyan} \hat{=} \{b_2\} \quad \text{blue} \hat{=} \{c_2\}$$

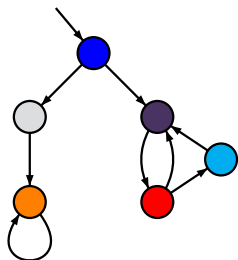
digraph  $G_a$



$$s_0 (s_1 s_2)^\omega \models \neg \square \diamond b_2 \wedge \square \diamond c_1$$

$$\text{fair} = (\square \diamond b_1 \rightarrow \square \diamond c_1) \wedge (\square \diamond b_2 \rightarrow \square \diamond c_2)$$

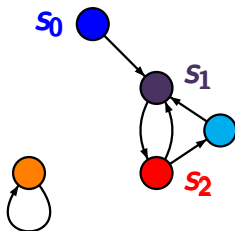
does  $\mathcal{T} \models_{\text{fair}} \exists \square a$  hold ?



$$\text{orange} \hat{=} \{b_1\} \quad \text{red} \hat{=} \{c_1\}$$

$$\text{cyan} \hat{=} \{b_2\} \quad \text{blue} \hat{=} \{c_2\}$$

digraph  $G_a$



$$s_0 (s_1 s_2)^\omega \models \neg \square \diamond b_2 \wedge \square \diamond c_1$$

$$s_0 (s_1 s_2)^\omega \models \text{fair}$$

$$\text{fair} = (\square \diamond b_1 \rightarrow \square \diamond c_1) \wedge (\square \diamond b_2 \rightarrow \square \diamond c_2)$$

$$\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box\Diamond b_i \rightarrow \Box\Diamond c_i)$$

$s \models_{\text{fair}} \exists\Box a$  iff there exists a path fragment

$$s_0 s_1 \dots s_n \dots s_{n+r}$$

such that  $r \geq 1$ ,  $s = s_0$ ,  $s_n = s_{n+r}$  and

- $s_j \models a$  for all  $0 \leq j \leq n+r$
- for all  $1 \leq i \leq k$ :  $\{s_{n+1}, \dots, s_{n+r}\} \cap \text{Sat}(b_i) = \emptyset$   
or  $\{s_{n+1}, \dots, s_{n+r}\} \cap \text{Sat}(c_i) \neq \emptyset$

$$\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box\Diamond b_i \rightarrow \Box\Diamond c_i)$$

$s \models_{\text{fair}} \exists\Box a$  iff there exists a path fragment

$$s_0 s_1 \dots s_n \dots s_{n+r}$$

such that  $r \geq 1$ ,  $s = s_0$ ,  $s_n = s_{n+r}$  and

- $s_j \models a$  for all  $0 \leq j \leq n+r$
- for all  $1 \leq i \leq k$ :  $\{s_{n+1}, \dots, s_{n+r}\} \cap \text{Sat}(b_i) = \emptyset$   
or  $\{s_{n+1}, \dots, s_{n+r}\} \cap \text{Sat}(c_i) \neq \emptyset$

Thus:  $D = \{s_{n+1}, \dots, s_{n+r}\}$  is a strongly connected node-set of the digraph  $G_a$

$$\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box\Diamond b_i \rightarrow \Box\Diamond c_i)$$

$s \models_{\text{fair}} \exists\Box a$  iff there exists a path fragment

$$s_0 s_1 \dots s_n \dots s_{n+r}$$

such that  $r \geq 1$ ,  $s = s_0$ ,  $s_n = s_{n+r}$  and

- $s_j \models a$  for all  $0 \leq j \leq n+r$
- for all  $1 \leq i \leq k$ :  $\{s_{n+1}, \dots, s_{n+r}\} \cap \text{Sat}(b_i) = \emptyset$   
or  $\{s_{n+1}, \dots, s_{n+r}\} \cap \text{Sat}(c_i) \neq \emptyset$

Thus:  $D = \{s_{n+1}, \dots, s_{n+r}\}$  is a strongly connected node-set of the digraph  $G_a$  (possibly not an SCC)

$$\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box\Diamond b_i \rightarrow \Box\Diamond c_i)$$

$s \models_{\text{fair}} \exists\Box a$  iff there exists a non-trivial  
strongly connected node-set  $D$  of  $G_a$  such that

$G_a$ : digraph that arises from  $\mathcal{T}$  by removing all  
states  $s'$  with  $s' \not\models a$

$$\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box\Diamond b_i \rightarrow \Box\Diamond c_i)$$

$s \models_{\text{fair}} \exists\Box a$  iff there exists a non-trivial strongly connected node-set  $D$  of  $G_a$  such that

(1)  $D$  is reachable from  $s$

(2) for all  $1 \leq i \leq k$ :

$$D \cap \text{Sat}(b_i) = \emptyset \quad \text{or} \quad D \cap \text{Sat}(c_i) \neq \emptyset$$

$G_a$ : digraph that arises from  $\mathcal{T}$  by removing all states  $s'$  with  $s' \not\models a$



$$\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box\Diamond b_i \rightarrow \Box\Diamond c_i)$$

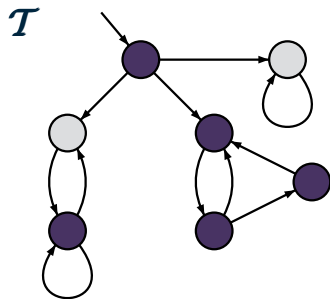
$s \models_{\text{fair}} \exists\Box a$  iff there exists a non-trivial  
strongly connected node-set  $D$  of  $G_a$  such that

(1)  $D$  is reachable from  $s$

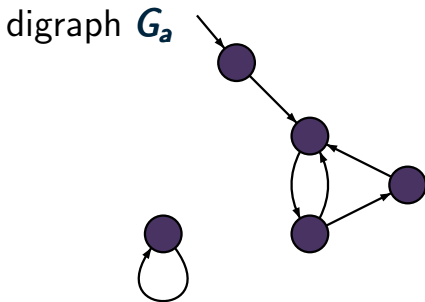
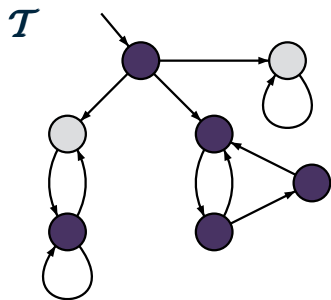
(2) for all  $1 \leq i \leq k$ :

$$D \cap \text{Sat}(b_i) = \emptyset \quad \text{or} \quad D \cap \text{Sat}(c_i) \neq \emptyset$$

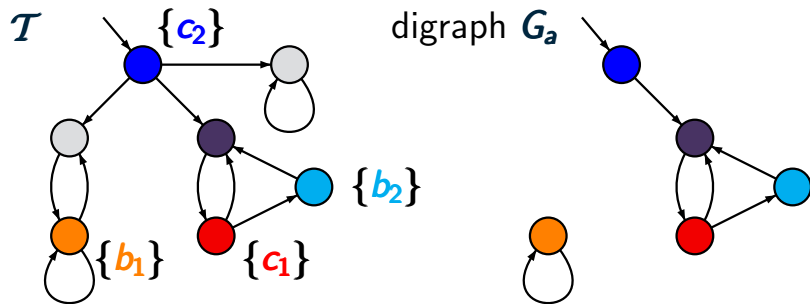
note: if  $s \models_{\text{fair}} \exists\Box a$  then there might be  
no SCC  $D$  where (1) and (2) hold



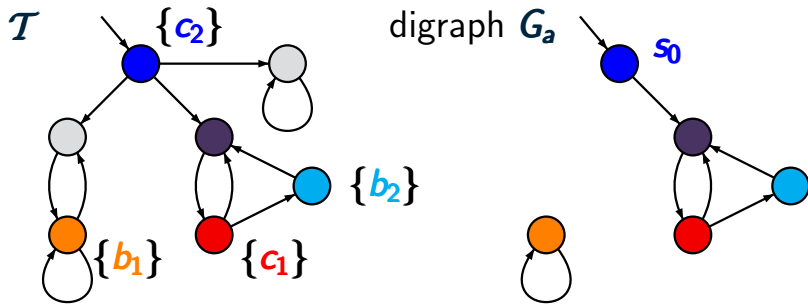
computation of  $Sat_{fair}(\exists \square a)$



computation of  $Sat_{fair}(\exists \Box a)$   
 by analyzing the digraph  $G_a$

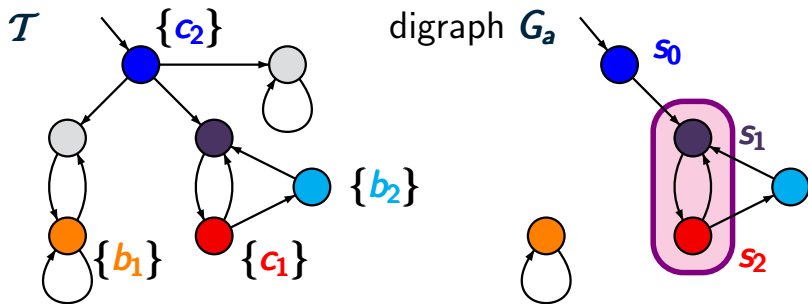


$$fair = (\Box \Diamond b_1 \rightarrow \Box \Diamond c_1) \wedge (\Box \Diamond b_2 \rightarrow \Box \Diamond c_2)$$



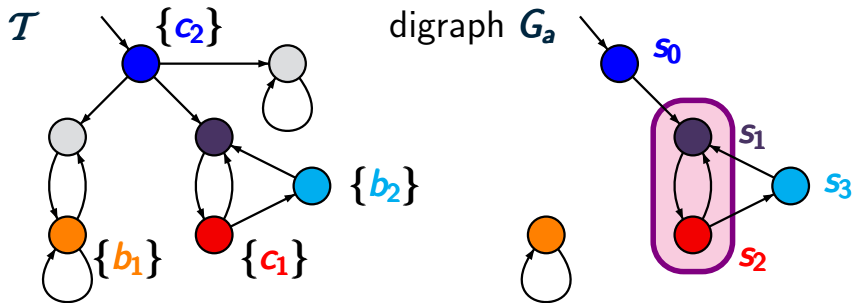
$$fair = (\square \diamond b_1 \rightarrow \square \diamond c_1) \wedge (\square \diamond b_2 \rightarrow \square \diamond c_2)$$

$$s_0 \models_{fair} \exists \square a$$



$$fair = (\square \diamond b_1 \rightarrow \square \diamond c_1) \wedge (\square \diamond b_2 \rightarrow \square \diamond c_2)$$

$$s_0 \models_{fair} \exists \square a \quad \text{as } s_0 s_1 s_2 s_1 s_2 \dots \models_{LTL} fair$$



$$fair = (\square \diamond b_1 \rightarrow \square \diamond c_1) \wedge (\square \diamond b_2 \rightarrow \square \diamond c_2)$$

$$s_0 \models_{fair} \exists \square a \quad \text{as } s_0 s_1 s_2 s_1 s_2 \dots \models_{LTL} fair$$

$$Sat_{fair}(\exists \square a) = \{s_0, s_1, s_2, s_3\}$$

treatment of  $\exists\Box$  for **CTL** with fairness



treatment of  $\exists\Box$  for **CTL** with fairness

*here:* explanations only for **strong fairness**

**weak fairness** and combinations of weak/strong fairness can be treated in an analogous way

treatment of  $\exists\Box$  for **CTL** with fairness

here: explanations only for strong fairness

case 1: unconditional fairness

case 2:  $\mathit{fair} = \Box\Diamond b \rightarrow \Box\Diamond c$

case 3: arbitrary strong fairness assumption

$$\mathit{fair} = \bigwedge_{1 \leq i \leq k} (\Box\Diamond b_i \rightarrow \Box\Diamond c_i)$$

weak fairness and combinations of weak/strong fairness can be treated in an analogous way

treatment of  $\exists\Box$  for **CTL** with fairness

here: explanations only for strong fairness

case 1: unconditional fairness

case 2:  $\text{fair} = \Box\Diamond b \rightarrow \Box\Diamond c$

case 3: arbitrary strong fairness assumption

$$\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box\Diamond b_i \rightarrow \Box\Diamond c_i)$$

weak fairness and combinations of weak/strong fairness can be treated in an analogous way

$$\mathit{fair} = \bigwedge_{1 \leq i \leq k} \Box \Diamond c_i$$

$$\text{fair} = \bigwedge_{1 \leq i \leq k} \Box \Diamond c_i$$

$s \models_{\text{fair}} \exists \Box a$  iff ?

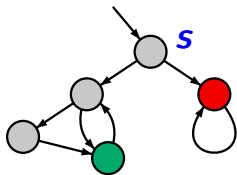
$$\text{fair} = \bigwedge_{1 \leq i \leq k} \Box \Diamond c_i$$

$s \models_{\text{fair}} \exists \Box a$  iff there exists a **nontrivial SCC**  $C$  in  $G_a$  that is reachable from  $s$  and  $C \cap \text{Sat}(c_i) \neq \emptyset$  for  $i = 1, \dots, k$

$$\text{fair} = \bigwedge_{1 \leq i \leq k} \Box \Diamond c_i$$

$s \models_{\text{fair}} \exists \Box a$  iff there exists a **nontrivial SCC**  $C$  in  $G_a$  that is reachable from  $s$  and  $C \cap \text{Sat}(c_i) \neq \emptyset$  for  $i = 1, \dots, k$

digraph  $G_a$



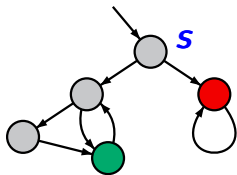
fairness assumption:

$$\text{fair} = \Box \Diamond c_1 \wedge \Box \Diamond c_2$$

$$\text{fair} = \bigwedge_{1 \leq i \leq k} \Box \Diamond c_i$$

$s \models_{\text{fair}} \exists \Box a$  iff there exists a **nontrivial SCC**  $C$  in  $G_a$  that is reachable from  $s$  and  $C \cap \text{Sat}(c_i) \neq \emptyset$  for  $i = 1, \dots, k$

digraph  $G_a$



fairness assumption:

$$\text{fair} = \Box \Diamond c_1 \wedge \Box \Diamond c_2$$

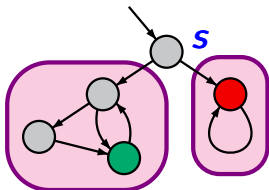
$$s \not\models_{\text{fair}} \exists \Box a$$



$$fair = \bigwedge_{1 \leq i \leq k} \Box \Diamond c_i$$

$s \models_{fair} \exists \Box a$  iff there exists a **nontrivial SCC**  $C$  in  $G_a$  that is reachable from  $s$  and  $C \cap Sat(c_i) \neq \emptyset$  for  $i = 1, \dots, k$

digraph  $G_a$



fairness assumption:

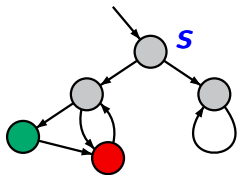
$$fair = \Box \Diamond c_1 \wedge \Box \Diamond c_2$$

$$s \not\models_{fair} \exists \Box a$$

$$\text{fair} = \bigwedge_{1 \leq i \leq k} \Box \Diamond c_i$$

$s \models_{\text{fair}} \exists \Box a$  iff there exists a **nontrivial SCC**  $C$  in  $G_a$  that is reachable from  $s$  and  $C \cap \text{Sat}(c_i) \neq \emptyset$  for  $i = 1, \dots, k$

digraph  $G_a$



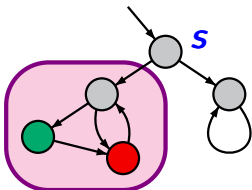
fairness assumption:

$$\text{fair} = \Box \Diamond c_1 \wedge \Box \Diamond c_2$$

$$\text{fair} = \bigwedge_{1 \leq i \leq k} \Box \Diamond c_i$$

$s \models_{\text{fair}} \exists \Box a$  iff there exists a **nontrivial SCC**  $C$  in  $G_a$  that is reachable from  $s$  and  $C \cap \text{Sat}(c_i) \neq \emptyset$  for  $i = 1, \dots, k$

digraph  $G_a$



fairness assumption:

$$\text{fair} = \Box \Diamond c_1 \wedge \Box \Diamond c_2$$

$$s \models_{\text{fair}} \exists \Box a$$

treatment of  $\exists\Box$  for CTL with fairness

here: explanations only for **strong fairness**

case 1: unconditional fairness ✓

case 2:  $\mathit{fair} = \Box\Diamond b \rightarrow \Box\Diamond c$

case 3: arbitrary strong fairness assumption

$$\mathit{fair} = \bigwedge_{1 \leq i \leq k} (\Box\Diamond b_i \rightarrow \Box\Diamond c_i)$$

treatment of  $\exists\Box$  for CTL with fairness

here: explanations only for **strong fairness**

case 1: unconditional fairness ✓

case 2: **fair** =  $\Box\Diamond b \rightarrow \Box\Diamond c$

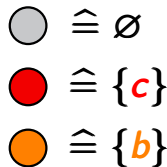
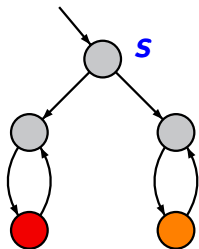
case 3: arbitrary strong fairness assumption

$$\mathbf{fair} = \bigwedge_{1 \leq i \leq k} (\Box\Diamond b_i \rightarrow \Box\Diamond c_i)$$

$$\textit{fair} = \Box \Diamond b \rightarrow \Box \Diamond c$$

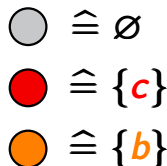
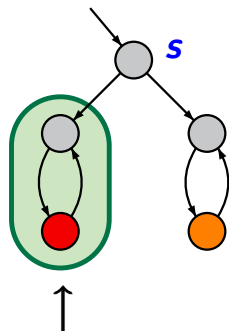
$$\text{fair} = \Box \Diamond b \rightarrow \Box \Diamond c$$

digraph  $G_a$



$$\text{fair} = \Box \Diamond b \rightarrow \Box \Diamond c$$

digraph  $G_a$

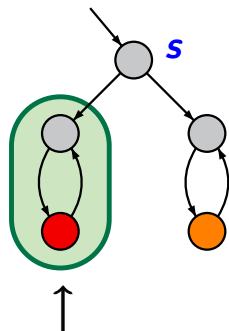


nontrivial **SCC**  $C$  of  $G_a$  with  $C \cap \text{Sat}(c) \neq \emptyset$

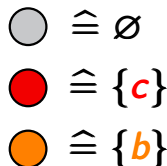


$$\text{fair} = \Box \Diamond b \rightarrow \Box \Diamond c$$

digraph  $G_a$



$$s \models_{\text{fair}} \exists \Box a$$



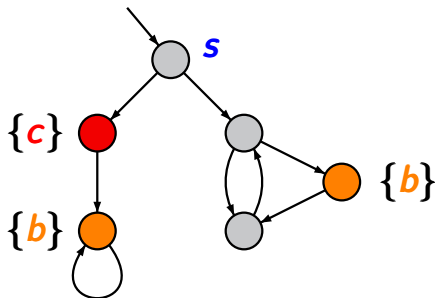
nontrivial **SCC**  $C$  of  $G_a$  with  $C \cap \text{Sat}(c) \neq \emptyset$

# Strong fairness: 1 fairness requirement

CTLFAIR4.4-25A

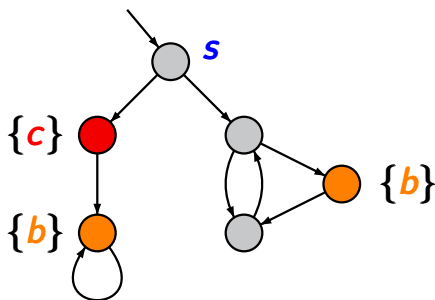
$$\text{fair} = \Box \Diamond b \rightarrow \Box \Diamond c$$

digraph  $G_a$



$$\text{fair} = \Box \Diamond b \rightarrow \Box \Diamond c$$

digraph  $G_a$



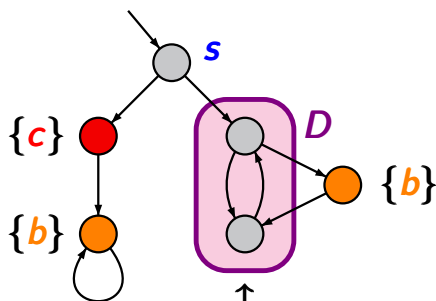
$$\leftarrow \boxed{s \models_{\text{fair}} \exists \Box a}$$

# Strong fairness: 1 fairness requirement

CTLFAIR4.4-25A

$$\text{fair} = \Box \Diamond b \rightarrow \Box \Diamond c$$

digraph  $G_a$



$$s \models_{\text{fair}} \exists \Box a$$

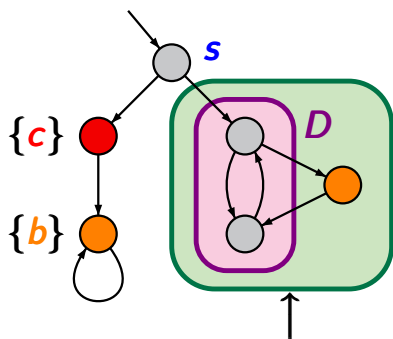
strongly connected node-set  $D$  of  $G_a$  with  
 $D \cap \text{Sat}(b) = \emptyset$

# Strong fairness: 1 fairness requirement

CTLFAIR4.4-25A

$$\text{fair} = \Box \Diamond b \rightarrow \Box \Diamond c$$

digraph  $G_a$



$$s \models_{\text{fair}} \exists \Box a$$

nontrivial **SCC**  $C$  of  $G_a$  that contains a  
nontrivial **SCC**  $D$  of  $G_a|_C \setminus \text{Sat}(b)$

treatment of  $\exists \square$  for CTL with fairness

here: explanations only for **strong fairness**

case 1: unconditional fairness ✓

case 2: **fair** =  $\square \diamond b \rightarrow \square \diamond c$  ✓

case 3: arbitrary strong fairness assumption

$$\mathbf{fair} = \bigwedge_{1 \leq i \leq k} (\square \diamond b_i \rightarrow \square \diamond c_i)$$

treatment of  $\exists\Box$  for CTL with fairness

here: explanations only for **strong fairness**

case 1: unconditional fairness ✓

case 2: **fair** =  $\Box\Diamond b \rightarrow \Box\Diamond c$  ✓

case 3: arbitrary strong fairness assumption

$$\mathbf{fair} = \bigwedge_{1 \leq i \leq k} (\Box\Diamond b_i \rightarrow \Box\Diamond c_i)$$

# Example: 2 strong fairness conditions

CTLFAIR4.4-26



## Example: 2 strong fairness conditions

CTLFAIR4.4-26

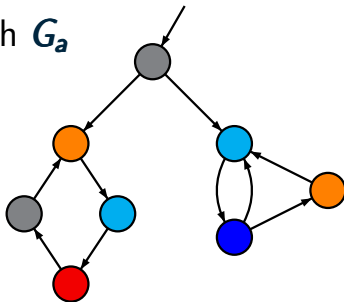
$$\mathit{fair} = (\Box\Diamond b_1 \rightarrow \Box\Diamond c_1) \wedge (\Box\Diamond b_2 \rightarrow \Box\Diamond c_2)$$

## Example: 2 strong fairness conditions

CTLFAIR4.4-26

$$\text{fair} = (\Box\Diamond b_1 \rightarrow \Box\Diamond c_1) \wedge (\Box\Diamond b_2 \rightarrow \Box\Diamond c_2)$$

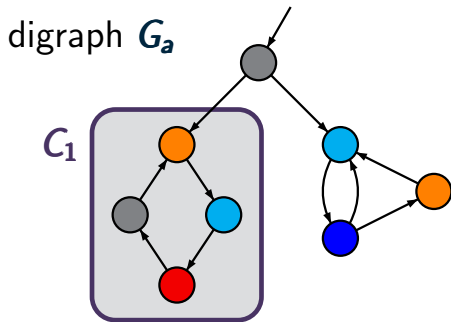
digraph  $G_a$



## Example: 2 strong fairness conditions

CTLFAIR4.4-26

$$\text{fair} = (\Box\Diamond b_1 \rightarrow \Box\Diamond c_1) \wedge (\Box\Diamond b_2 \rightarrow \Box\Diamond c_2)$$

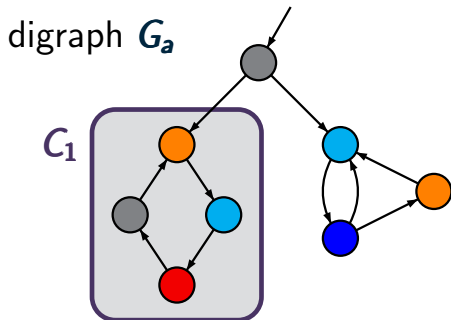


$$\text{first SCC: } C_1 \cap \text{Sat}(c_2) = \emptyset$$

## Example: 2 strong fairness conditions

CTLFair4.4-26

$$\text{fair} = (\Box\Diamond b_1 \rightarrow \Box\Diamond c_1) \wedge (\Box\Diamond b_2 \rightarrow \Box\Diamond c_2)$$



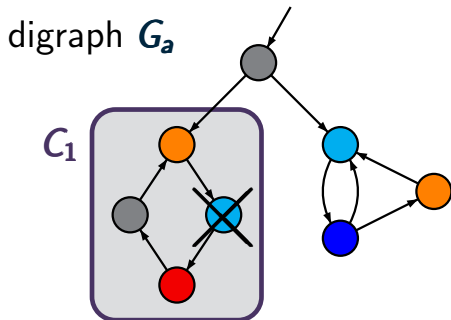
first SCC:  $C_1 \cap \text{Sat}(c_2) = \emptyset$

analyze  $C_1 \setminus \text{Sat}(b_2)$  w.r.t.  $\Box\Diamond b_1 \rightarrow \Box\Diamond c_1$

## Example: 2 strong fairness conditions

CTLFair4.4-26

$$\text{fair} = (\Box\Diamond b_1 \rightarrow \Box\Diamond c_1) \wedge (\Box\Diamond b_2 \rightarrow \Box\Diamond c_2)$$



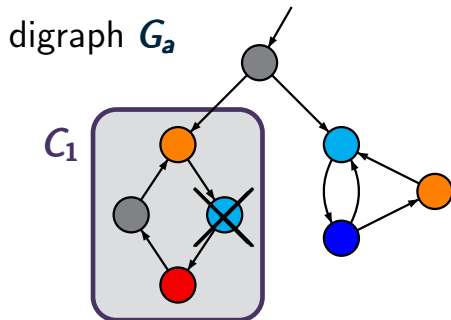
first SCC:  $C_1 \cap \text{Sat}(c_2) = \emptyset$

analyze  $C_1 \setminus \text{Sat}(b_2)$  w.r.t.  $\Box\Diamond b_1 \rightarrow \Box\Diamond c_1$

## Example: 2 strong fairness conditions

CTLFair4.4-26

$$\text{fair} = (\Box\Diamond b_1 \rightarrow \Box\Diamond c_1) \wedge (\Box\Diamond b_2 \rightarrow \Box\Diamond c_2)$$



first SCC:  $C_1 \cap \text{Sat}(c_2) = \emptyset$

analyze  $C_1 \setminus \text{Sat}(b_2)$  w.r.t.  $\Box\Diamond b_1 \rightarrow \Box\Diamond c_1$

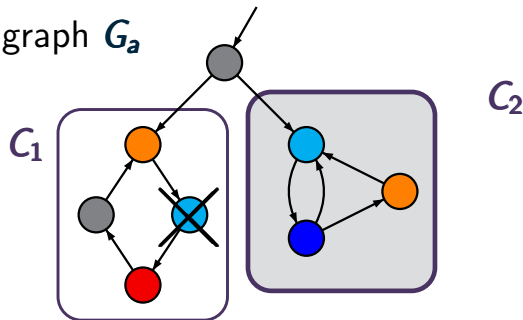
$\rightsquigarrow$  there is no cycle

# Example: 2 strong fairness conditions

CTLFAIR4.4-26

$$\text{fair} = (\Box\Diamond b_1 \rightarrow \Box\Diamond c_1) \wedge (\Box\Diamond b_2 \rightarrow \Box\Diamond c_2)$$

digraph  $G_a$



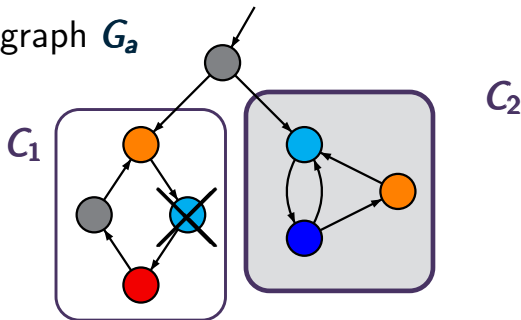
second SCC:

# Example: 2 strong fairness conditions

CTLFAIR4.4-26

$$\text{fair} = (\Box\Diamond b_1 \rightarrow \Box\Diamond c_1) \wedge (\Box\Diamond b_2 \rightarrow \Box\Diamond c_2)$$

digraph  $G_a$



second SCC:  $C_2 \cap \text{Sat}(c_1) = \emptyset$

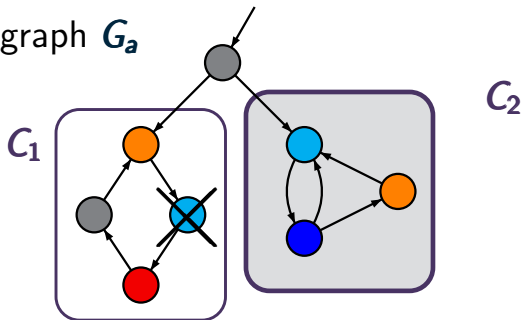


# Example: 2 strong fairness conditions

CTLFair4.4-26

$$\text{fair} = (\Box\Diamond b_1 \rightarrow \Box\Diamond c_1) \wedge (\Box\Diamond b_2 \rightarrow \Box\Diamond c_2)$$

digraph  $G_a$



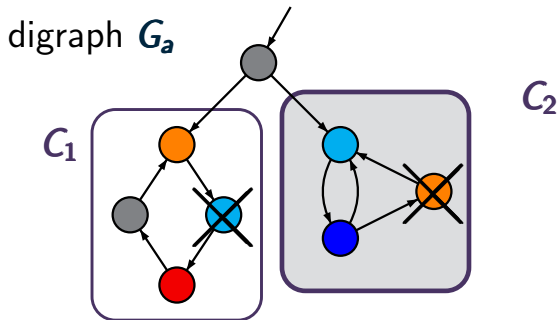
second SCC:  $C_2 \cap \text{Sat}(c_1) = \emptyset$

analyze  $C_2 \setminus \text{Sat}(b_1)$  w.r.t.  $\Box\Diamond b_2 \rightarrow \Box\Diamond c_2$

# Example: 2 strong fairness conditions

CTLFAIR4.4-26

$$\text{fair} = (\Box\Diamond b_1 \rightarrow \Box\Diamond c_1) \wedge (\Box\Diamond b_2 \rightarrow \Box\Diamond c_2)$$



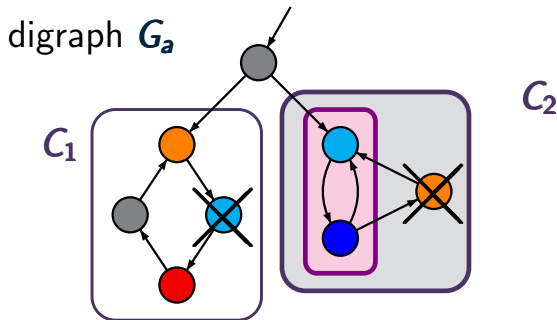
second SCC:  $C_2 \cap \text{Sat}(c_1) = \emptyset$

analyze  $C_2 \setminus \text{Sat}(b_1)$  w.r.t.  $\Box\Diamond b_2 \rightarrow \Box\Diamond c_2$

# Example: 2 strong fairness conditions

CTLFAIR4.4-26

$$\text{fair} = (\Box\Diamond b_1 \rightarrow \Box\Diamond c_1) \wedge (\Box\Diamond b_2 \rightarrow \Box\Diamond c_2)$$



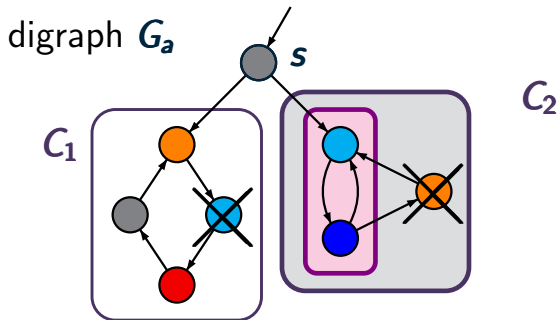
second SCC:  $C_2 \cap \text{Sat}(c_1) = \emptyset$

analyze  $C_2 \setminus \text{Sat}(b_1)$  w.r.t.  $\Box\Diamond b_2 \rightarrow \Box\Diamond c_2$

# Example: 2 strong fairness conditions

CTLFAIR4.4-26

$$\text{fair} = (\Box\Diamond b_1 \rightarrow \Box\Diamond c_1) \wedge (\Box\Diamond b_2 \rightarrow \Box\Diamond c_2)$$



second SCC:  $C_2 \cap \text{Sat}(c_1) = \emptyset$

analyze  $C_2 \setminus \text{Sat}(b_1)$  w.r.t.  $\Box\Diamond b_2 \rightarrow \Box\Diamond c_2$

hence:  $s \models_{\text{fair}} \exists\Box a$

# Calculation of $Sat_{fair}(\exists \square a)$

CTLFAIR4.4-27

compute the SCCs of the digraph  $G_a$ ;

compute the SCCs of the digraph  $G_a$ ;

$T := \emptyset$ ;

compute the SCCs of the digraph  $G_a$ ;

$T := \emptyset$ ;

FOR ALL nontrivial SCCs  $C$  of  $G_a$  DO



compute the SCCs of the digraph  $G_a$ ;

$T := \emptyset$ ;

FOR ALL nontrivial SCCs  $C$  of  $G_a$  DO

IF  $CheckFair(C, \dots)$  THEN  $T := T \cup C$  FI

OD

compute the SCCs of the digraph  $G_a$ ;

$T := \emptyset$ ;

FOR ALL nontrivial SCCs  $C$  of  $G_a$  DO

IF  $CheckFair(C, \dots)$  THEN  $T := T \cup C$  FI

OD

$Sat_{fair}(\exists \square a) := \{s \in S : Reach_{G_a}(s) \cap T \neq \emptyset\}$

compute the SCCs of the digraph  $G_a$ ;

$T := \emptyset$ ;

FOR ALL nontrivial SCCs  $C$  of  $G_a$  DO

IF  $CheckFair(C, \dots)$  THEN  $T := T \cup C$  FI

OD

$Sat_{fair}(\exists \square a) := \{s \in S : Reach_{G_a}(s) \cap T \neq \emptyset\}$

backward search from  $T$

compute the SCCs of the digraph  $G_a$ ;

$T := \emptyset$ ;

FOR ALL nontrivial SCCs  $C$  of  $G_a$  DO

IF  $CheckFair(C, \dots)$  THEN  $T := T \cup C$  FI

OD

$Sat_{fair}(\exists \square a) := \{s \in S : Reach_{G_a}(s) \cap T \neq \emptyset\}$

backward search from  $T$

time complexity:  $\mathcal{O}(size(T) \cdot |fair|)$

compute the SCCs of the digraph  $G_a$ ;

$T := \emptyset$ ;

FOR ALL nontrivial SCCs  $C$  of  $G_a$  DO

IF  $CheckFair(C, \dots)$  THEN  $T := T \cup C$  FI

OD

$Sat_{fair}(\exists \square a) := \{s \in S : Reach_{G_a}(s) \cap T \neq \emptyset\}$

backward search from  $T$

time complexity:  $\mathcal{O}(size(T) \cdot |fair|)$



algorithm *CheckFair*( $C, k, \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$ )

algorithm *CheckFair*( $C, k, \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$ ) returns

“true” if there exists a cyclic path fragment

$s_0 s_1 \dots s_n$  in  $C$  such that

$$(s_0 s_1 \dots s_{n-1})^\omega \models \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$$

“false” otherwise



## Recursive algorithm *CheckFair*(...)

CTLFAIR4.4-28

pseudo code for *CheckFair*( $C, k, \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$ )

IF  $\forall i \in \{1, \dots, k\}. C \cap \text{Sat}(c_i) \neq \emptyset$  THEN return "true" FI

## Recursive algorithm *CheckFair*(...)

CTLFAIR4.4-28

pseudo code for *CheckFair*( $C, k, \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$ )

IF  $\forall i \in \{1, \dots, k\}. C \cap \text{Sat}(c_i) \neq \emptyset$  THEN return "true" FI  
choose  $j \in \{1, \dots, k\}$  with  $C \cap \text{Sat}(c_j) = \emptyset$ ;

## Recursive algorithm *CheckFair*(...)

CTLFair4.4-28

pseudo code for *CheckFair*( $C, k, \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$ )

IF  $\forall i \in \{1, \dots, k\}. C \cap \text{Sat}(c_i) \neq \emptyset$  THEN return "true" FI  
choose  $j \in \{1, \dots, k\}$  with  $C \cap \text{Sat}(c_j) = \emptyset$ ;  
remove all states in  $\text{Sat}(b_j)$ ;

## Recursive algorithm *CheckFair*(...)

CTLFair4.4-28

pseudo code for *CheckFair*( $C, k, \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$ )

IF  $\forall i \in \{1, \dots, k\}. C \cap \text{Sat}(c_i) \neq \emptyset$  THEN return “true” FI  
choose  $j \in \{1, \dots, k\}$  with  $C \cap \text{Sat}(c_j) = \emptyset$ ;  
remove all states in  $\text{Sat}(b_j)$ ;  
IF the resulting graph  $G$  is acyclic THEN return “false” FI

## Recursive algorithm *CheckFair*(...)

CTLFair4.4-28

pseudo code for *CheckFair*( $C, k, \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$ )

IF  $\forall i \in \{1, \dots, k\}. C \cap \text{Sat}(c_i) \neq \emptyset$  THEN return “true” FI  
choose  $j \in \{1, \dots, k\}$  with  $C \cap \text{Sat}(c_j) = \emptyset$ ;  
remove all states in  $\text{Sat}(b_j)$ ;  
IF the resulting graph  $G$  is acyclic THEN return “false” FI  
FOR ALL nontrivial SCCs  $D$  of  $G$  DO  
  
OD

## Recursive algorithm *CheckFair*(...)

CTLFAIR4.4-28

pseudo code for *CheckFair*( $C, k, \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$ )

```
IF  $\forall i \in \{1, \dots, k\}. C \cap \text{Sat}(c_i) \neq \emptyset$  THEN return "true" FI
choose  $j \in \{1, \dots, k\}$  with  $C \cap \text{Sat}(c_j) = \emptyset$ ;
remove all states in  $\text{Sat}(b_j)$ ;
IF the resulting graph  $G$  is acyclic THEN return "false" FI
FOR ALL nontrivial SCCs  $D$  of  $G$  DO
  IF CheckFair( $D, k-1, \bigwedge_{i \neq j} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$ )
  THEN return "true" FI
OD
```

## Recursive algorithm *CheckFair*(...)

CTLFAIR4.4-28

pseudo code for *CheckFair*( $C, k, \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$ )

```
IF  $\forall i \in \{1, \dots, k\}. C \cap \text{Sat}(c_i) \neq \emptyset$  THEN return "true" FI
choose  $j \in \{1, \dots, k\}$  with  $C \cap \text{Sat}(c_j) = \emptyset$ ;
remove all states in  $\text{Sat}(b_j)$ ;
IF the resulting graph  $G$  is acyclic THEN return "false" FI
FOR ALL nontrivial SCCs  $D$  of  $G$  DO
  IF CheckFair( $D, k-1, \bigwedge_{i \neq j} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$ )
  THEN return "true" FI
OD
return "false"
```

# Complexity of *CheckFair*(...)

CTLFAIR4.4-29



## Complexity of *CheckFair*(...)

CTLFAIR4.4-29

pseudo code for *CheckFair*( $C, k, \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$ )

```
IF  $\forall i \in \{1, \dots, k\}. C \cap \text{Sat}(c_i) \neq \emptyset$  THEN return "true" FI
choose  $j \in \{1, \dots, k\}$  with  $C \cap \text{Sat}(c_j) = \emptyset$ ;
remove all states in  $\text{Sat}(b_j)$ ;
IF the resulting graph  $G$  is acyclic THEN return "false" FI
FOR ALL nontrivial SCCs  $D$  of  $G$  DO
  IF CheckFair( $D, k-1, \bigwedge_{i \neq j} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$ )
  THEN return "true"
OD
return "false"
```

## Complexity of *CheckFair*(...)

CTLFAIR4.4-29

pseudo code for *CheckFair*( $C, k, \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$ )

IF  $\forall i \in \{1, \dots, k\}. C \cap \text{Sat}(c_i) \neq \emptyset$  THEN return “true” FI  
choose  $j \in \{1, \dots, k\}$  with  $C \cap \text{Sat}(c_j) = \emptyset$ ;  
remove all states in  $\text{Sat}(b_j)$ ;  
IF the resulting graph  $G$  is acyclic THEN return “false” FI  
FOR ALL nontrivial SCCs  $D$  of  $G$  DO  
    IF *CheckFair*( $D, k-1, \bigwedge_{i \neq j} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$ )  
    THEN return “true”  
OD  
return “false”

recurrence for the time complexity:

$$T(n, k) = \dots \text{ where } n = \text{size}(C)$$

## Complexity of *CheckFair*(...)

CTLFAIR4.4-29

pseudo code for *CheckFair*( $C, k, \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$ )

IF  $\forall i \in \{1, \dots, k\}. C \cap \text{Sat}(c_i) \neq \emptyset$  THEN return “true” FI  
choose  $j \in \{1, \dots, k\}$  with  $C \cap \text{Sat}(c_j) = \emptyset$ ;  
remove all states in  $\text{Sat}(b_j)$ ;  
IF the resulting graph  $G$  is acyclic THEN return “false” FI  
FOR ALL nontrivial SCCs  $D$  of  $G$  DO  
    IF *CheckFair*( $D, k-1, \bigwedge_{i \neq j} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$ )  
    THEN return “true”  
OD  
return “false”

**time complexity:**  
 $\mathcal{O}(\text{size}(C) \cdot k)$

*input:* finite transition system  $\mathcal{T}$   
CTL fairness assumption *fair*  
CTL formula  $\phi$

*output:* “yes”, if  $\mathcal{T} \models_{\text{fair}} \phi$ . “no” otherwise.

*input:* finite transition system  $\mathcal{T}$   
CTL fairness assumption *fair*  
CTL formula  $\phi$

*output:* “yes”, if  $\mathcal{T} \models_{\text{fair}} \phi$ . “no” otherwise.

*here: preprocessing*

transform  $\phi$  into an equivalent CTL formula  
in **existential normal form**

*input:* finite transition system  $\mathcal{T}$   
CTL fairness assumption *fair*  
CTL formula  $\phi$

*output:* “yes”, if  $\mathcal{T} \models_{\text{fair}} \phi$ . “no” otherwise.

*here: preprocessing*

transform  $\phi$  into an equivalent CTL formula  
in **existential normal form**

↑  
i.e., with the basic modalities  $\exists O$ ,  $\exists U$  and  $\exists \square$



calculate  $Sat_{fair}(\exists \square true)$ ;

label all states in  $Sat_{fair}(\exists \square true)$  with  $a_{fair}$



calculate  $Sat_{fair}(\exists\Box true)$ ;

label all states in  $Sat_{fair}(\exists\Box true)$  with  $a_{fair}$

FOR ALL subformulas  $\Psi$  of  $\Phi$  DO

$Sat_{fair}(\Psi) := \dots$

OD

calculate  $Sat_{fair}(\exists\Box true)$ ;

label all states in  $Sat_{fair}(\exists\Box true)$  with  $a_{fair}$

FOR ALL subformulas  $\Psi$  of  $\Phi$  DO

CASE  $\Psi$  is:

$$\begin{array}{l} \vdots \\ \exists\bigcirc a : Sat_{fair}(\Psi) := Sat(\exists\bigcirc(a \wedge a_{fair})); \\ \exists(a_1 \cup a_2) : Sat_{fair}(\Psi) := Sat(\exists(a_1 \cup (a_2 \wedge a_{fair}))); \\ \exists\Box a : Sat_{fair}(\Psi) := \dots \end{array}$$

OD

calculate  $Sat_{fair}(\exists \square true)$ ;

label all states in  $Sat_{fair}(\exists \square true)$  with  $a_{fair}$

FOR ALL subformulas  $\Psi$  of  $\Phi$  DO

CASE  $\Psi$  is:

$$\begin{array}{l} \vdots \\ \exists \bigcirc a : Sat_{fair}(\Psi) := Sat(\exists \bigcirc (a \wedge a_{fair})); \\ \exists (a_1 \cup a_2) : Sat_{fair}(\Psi) := Sat(\exists (a_1 \cup (a_2 \wedge a_{fair}))); \\ \exists \square a : Sat_{fair}(\Psi) := \dots \end{array}$$

replace  $\Psi$  with a fresh atomic proposition  $a_\Psi$

OD

calculate  $Sat_{fair}(\exists\Box true)$ ;

label all states in  $Sat_{fair}(\exists\Box true)$  with  $a_{fair}$

FOR ALL subformulas  $\Psi$  of  $\Phi$  DO

CASE  $\Psi$  is:

$$\begin{array}{l} \vdots \\ \exists\bigcirc a : Sat_{fair}(\Psi) := Sat(\exists\bigcirc(a \wedge a_{fair})); \\ \exists(a_1 \cup a_2) : Sat_{fair}(\Psi) := Sat(\exists(a_1 \cup (a_2 \wedge a_{fair}))); \\ \exists\Box a : Sat_{fair}(\Psi) := \dots \end{array}$$

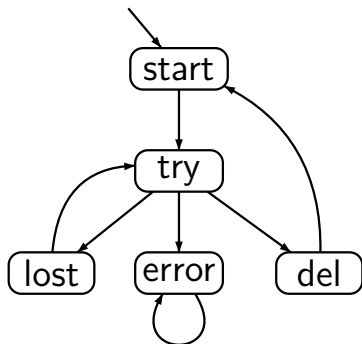
replace  $\Psi$  with a fresh atomic proposition  $a_\Psi$

OD

IF  $S_0 \subseteq Sat_{fair}(\Phi)$  THEN return “yes”

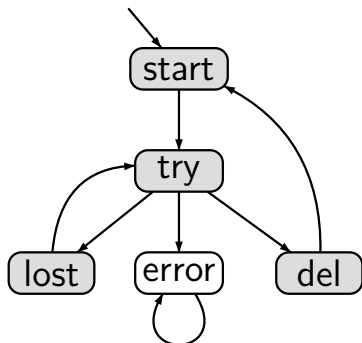
ELSE return “no”

FI



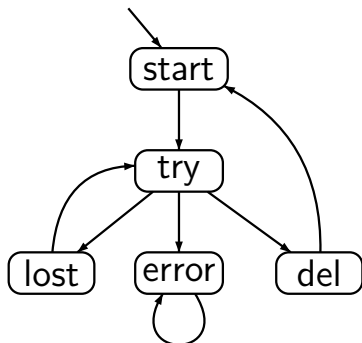
$$\Phi = \exists \diamond \forall \bigcirc (lost \vee del)$$

$$fair = \square \diamond \exists \diamond del$$



$$\Phi = \exists \diamond \forall \bigcirc (lost \vee del)$$

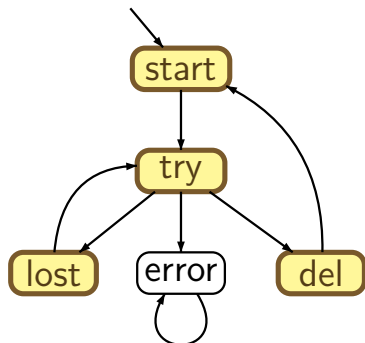
$$fair = \square \diamond \boxed{\exists \diamond del} \rightsquigarrow \square \diamond c \text{ where } Sat(c) = S \setminus \{error\}$$



$$\Phi = \exists \diamond \forall \bigcirc (lost \vee del)$$

$$fair = \square \diamond \exists \diamond del \rightsquigarrow \square \diamond c \text{ where } Sat(c) = S \setminus \{error\}$$

$$Sat_{fair}(\exists \square true)$$

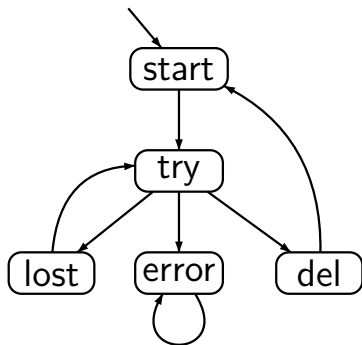


$$\Phi = \exists \diamond \forall \bigcirc (lost \vee del)$$

$$fair = \square \diamond \exists \diamond del \rightsquigarrow \square \diamond c \text{ where } Sat(c) = S \setminus \{error\}$$

$$Sat_{fair}(\exists \square true) = Sat(a_{fair}) = S \setminus \{error\}$$





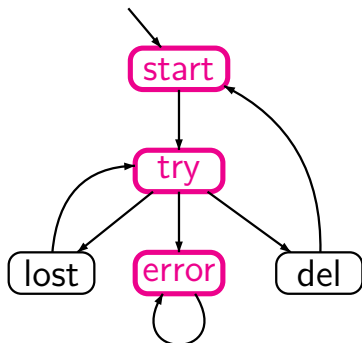
$$\Phi = \exists \Diamond \forall \bigcirc (lost \vee del)$$

$$\equiv \exists \Diamond \neg \exists \bigcirc (\neg lost \wedge \neg del)$$

existential normal form

$$fair = \square \Diamond \exists \Diamond del \rightsquigarrow \square \Diamond c \text{ where } Sat(c) = S \setminus \{error\}$$

$$Sat_{fair}(\exists \square true) = Sat(a_{fair}) = S \setminus \{error\}$$

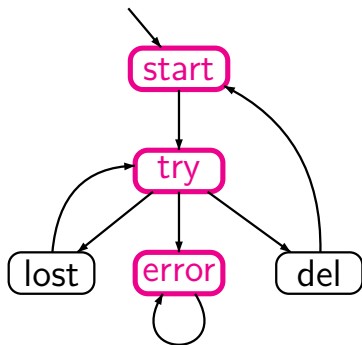


$$\Phi = \exists \diamond \forall \bigcirc (lost \vee del)$$

$$\equiv \exists \diamond \neg \exists \bigcirc (\neg lost \wedge \neg del)$$

$$fair = \square \diamond \exists \diamond del \rightsquigarrow \square \diamond c \text{ where } Sat(c) = S \setminus \{error\}$$

$$Sat_{fair}(\exists \square true) = Sat(a_{fair}) = S \setminus \{error\}$$



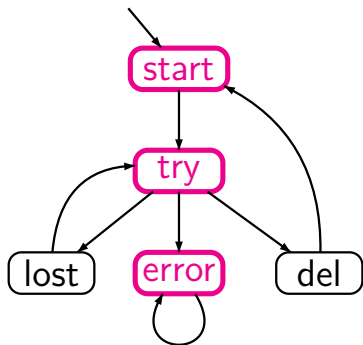
$$\Phi = \exists \diamond \forall \bigcirc (lost \vee del)$$

$$\equiv \exists \diamond \neg \exists \bigcirc (\neg lost \wedge \neg del)$$

$$\rightsquigarrow \exists \diamond \neg \exists \bigcirc a$$

$$fair = \square \diamond \exists \diamond del \rightsquigarrow \square \diamond c \text{ where } Sat(c) = S \setminus \{error\}$$

$$Sat_{fair}(\exists \square true) = Sat(a_{fair}) = S \setminus \{error\}$$



$$\Phi = \exists \Diamond \forall \bigcirc (lost \vee del)$$

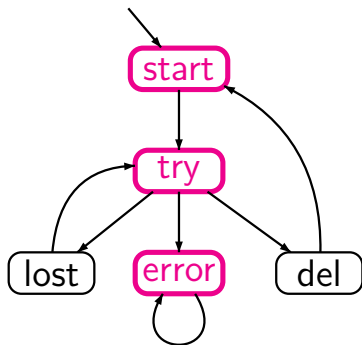
$$\equiv \exists \Diamond \neg \exists \bigcirc (\neg lost \wedge \neg del)$$

$$\rightsquigarrow \exists \Diamond \neg \boxed{\exists \bigcirc a}$$

$$fair = \square \Diamond \exists \Diamond del \rightsquigarrow \square \Diamond c \text{ where } Sat(c) = S \setminus \{error\}$$

$$Sat_{fair}(\exists \square true) = Sat(a_{fair}) = S \setminus \{error\}$$

$$Sat_{fair}(\exists \bigcirc a)$$



$$\Phi = \exists \Diamond \forall \bigcirc (lost \vee del)$$

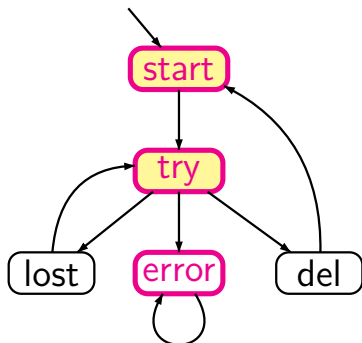
$$\equiv \exists \Diamond \neg \exists \bigcirc (\neg lost \wedge \neg del)$$

$$\rightsquigarrow \exists \Diamond \neg \boxed{\exists \bigcirc a}$$

$$fair = \square \Diamond \exists \Diamond del \rightsquigarrow \square \Diamond c \text{ where } Sat(c) = S \setminus \{error\}$$

$$Sat_{fair}(\exists \square true) = Sat(a_{fair}) = S \setminus \{error\}$$

$$Sat_{fair}(\exists \bigcirc a) = Sat(\exists \bigcirc (a \wedge a_{fair}))$$



$$\Phi = \exists \Diamond \forall \bigcirc (lost \vee del)$$

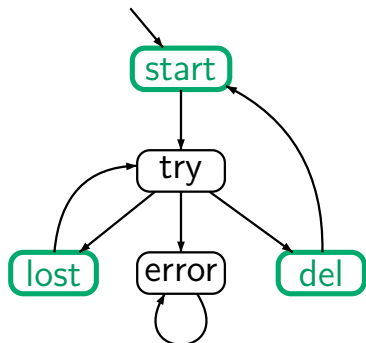
$$\equiv \exists \Diamond \neg \exists \bigcirc (\neg lost \wedge \neg del)$$

$$\rightsquigarrow \exists \Diamond \neg \boxed{\exists \bigcirc a}$$

$$fair = \square \Diamond \exists \Diamond del \rightsquigarrow \square \Diamond c \text{ where } Sat(c) = S \setminus \{error\}$$

$$Sat_{fair}(\exists \square true) = Sat(a_{fair}) = S \setminus \{error\}$$

$$Sat_{fair}(\exists \bigcirc a) = Sat(\exists \bigcirc (a \wedge a_{fair}))$$



$$\Phi = \exists \Diamond \forall \bigcirc (lost \vee del)$$

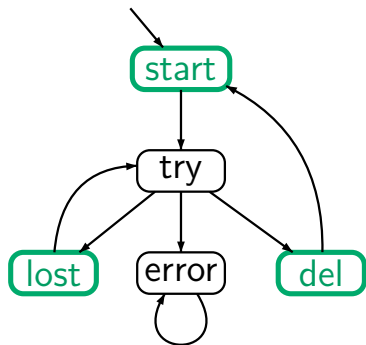
$$\equiv \exists \Diamond \neg \exists \bigcirc (\neg lost \wedge \neg del)$$

$$\rightsquigarrow \exists \Diamond \neg \boxed{\exists \bigcirc a}$$

$$fair = \Box \Diamond \exists \Diamond del \rightsquigarrow \Box \Diamond c \text{ where } Sat(c) = S \setminus \{error\}$$

$$Sat_{fair}(\exists \Box true) = Sat(a_{fair}) = S \setminus \{error\}$$

$$Sat_{fair}(\exists \bigcirc a) = Sat(\exists \bigcirc (a \wedge a_{fair})) = \{start, lost, del\}$$



$$\Phi = \exists \diamond \forall \bigcirc (lost \vee del)$$

$$\equiv \exists \diamond \neg \exists \bigcirc (\neg lost \wedge \neg del)$$

$$\rightsquigarrow \exists \diamond \boxed{\neg \exists \bigcirc a}$$

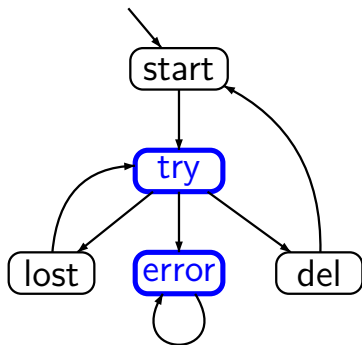
$$fair = \square \diamond \exists \diamond del \rightsquigarrow \square \diamond c \text{ where } Sat(c) = S \setminus \{error\}$$

$$Sat_{fair}(\exists \square true) = Sat(a_{fair}) = S \setminus \{error\}$$

$$Sat_{fair}(\exists \bigcirc a) = Sat(\exists \bigcirc (a \wedge a_{fair})) = \{start, lost, del\}$$

$$Sat_{fair}(\neg \exists \bigcirc a)$$





$$\Phi = \exists \Diamond \forall \bigcirc (lost \vee del)$$

$$\equiv \exists \Diamond \neg \exists \bigcirc (\neg lost \wedge \neg del)$$

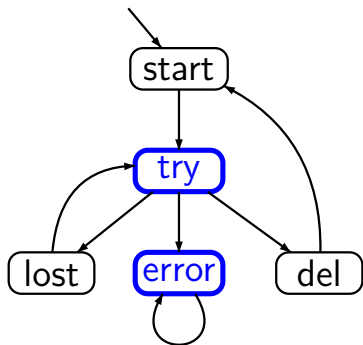
$$\rightsquigarrow \exists \Diamond \boxed{\neg \exists \bigcirc a}$$

$$fair = \square \Diamond \exists \Diamond del \rightsquigarrow \square \Diamond c \text{ where } Sat(c) = S \setminus \{error\}$$

$$Sat_{fair}(\exists \square true) = Sat(a_{fair}) = S \setminus \{error\}$$

$$Sat_{fair}(\exists \bigcirc a) = Sat(\exists \bigcirc (a \wedge a_{fair})) = \{start, lost, del\}$$

$$Sat_{fair}(\neg \exists \bigcirc a) = \{try, error\}$$



$$\Phi = \exists \diamond \forall \bigcirc (lost \vee del)$$

$$\equiv \exists \diamond \neg \exists \bigcirc (\neg lost \wedge \neg del)$$

$$\rightsquigarrow \exists \diamond \boxed{\neg \exists \bigcirc a}$$

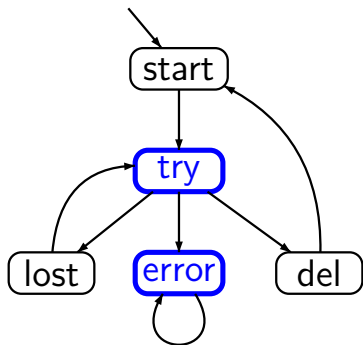
$$\rightsquigarrow \exists \diamond b$$

$$fair = \square \diamond \exists \diamond del \rightsquigarrow \square \diamond c \text{ where } Sat(c) = S \setminus \{error\}$$

$$Sat_{fair}(\exists \square true) = Sat(a_{fair}) = S \setminus \{error\}$$

$$Sat_{fair}(\exists \bigcirc a) = Sat(\exists \bigcirc (a \wedge a_{fair})) = \{start, lost, del\}$$

$$Sat_{fair}(\neg \exists \bigcirc a) = \{try, error\} = Sat(b)$$



$$\Phi = \exists \Diamond \forall \bigcirc (lost \vee del)$$

$$\equiv \exists \Diamond \neg \exists \bigcirc (\neg lost \wedge \neg del)$$

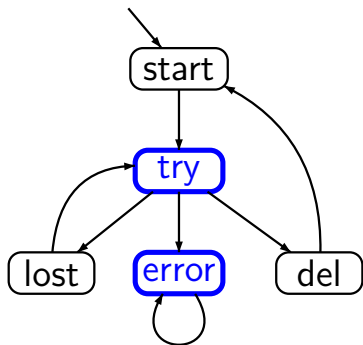
$$\rightsquigarrow \exists \Diamond \neg \exists \bigcirc a$$

$$\rightsquigarrow \exists \Diamond b$$

$$fair = \square \Diamond \exists \Diamond del \rightsquigarrow \square \Diamond c \text{ where } Sat(c) = S \setminus \{error\}$$

$$Sat_{fair}(\neg \exists \bigcirc a) = \{try, error\} = Sat(b)$$

$$Sat_{fair}(\exists \Diamond b)$$



$$\Phi = \exists \diamond \forall \bigcirc (lost \vee del)$$

$$\equiv \exists \diamond \neg \exists \bigcirc (\neg lost \wedge \neg del)$$

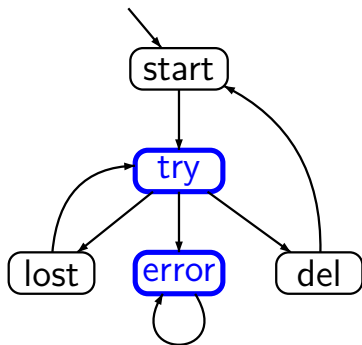
$$\rightsquigarrow \exists \diamond \neg \exists \bigcirc a$$

$$\rightsquigarrow \exists \diamond b$$

$$fair = \square \diamond \exists \diamond del \rightsquigarrow \square \diamond c \text{ where } Sat(c) = S \setminus \{error\}$$

$$Sat_{fair}(\neg \exists \bigcirc a) = \{try, error\} = Sat(b)$$

$$Sat_{fair}(\exists \diamond b) = Sat(\exists \diamond (b \wedge a_{fair}))$$



$$\Phi = \exists \diamond \forall \bigcirc (lost \vee del)$$

$$\equiv \exists \diamond \neg \exists \bigcirc (\neg lost \wedge \neg del)$$

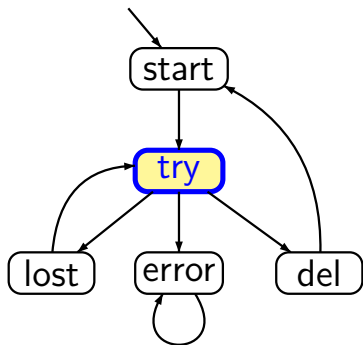
$$\rightsquigarrow \exists \diamond \neg \exists \bigcirc a$$

$$\rightsquigarrow \exists \diamond b$$

$$fair = \square \diamond \exists \diamond del \rightsquigarrow \square \diamond c \text{ where } Sat(c) = S \setminus \{error\}$$

$$Sat_{fair}(\neg \exists \bigcirc a) = \{try, error\} = Sat(b)$$

$$Sat_{fair}(\exists \diamond b) = Sat(\exists \diamond (b \wedge a_{fair}))$$



$$\Phi = \exists \Diamond \forall \bigcirc (lost \vee del)$$

$$\equiv \exists \Diamond \neg \exists \bigcirc (\neg lost \wedge \neg del)$$

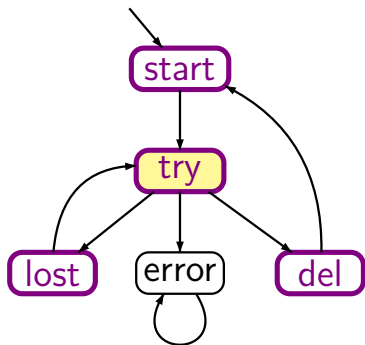
$$\rightsquigarrow \exists \Diamond \neg \exists \bigcirc a$$

$$\rightsquigarrow \exists \Diamond b$$

$$fair = \square \Diamond \exists \Diamond del \rightsquigarrow \square \Diamond c \text{ where } Sat(c) = S \setminus \{error\}$$

$$Sat_{fair}(\neg \exists \bigcirc a) = \{try, error\} = Sat(b)$$

$$Sat_{fair}(\exists \Diamond b) = Sat(\exists \Diamond (b \wedge a_{fair}))$$



$$\Phi = \exists \diamond \forall \bigcirc (lost \vee del)$$

$$\equiv \exists \diamond \neg \exists \bigcirc (\neg lost \wedge \neg del)$$

$$\rightsquigarrow \exists \diamond \neg \exists \bigcirc a$$

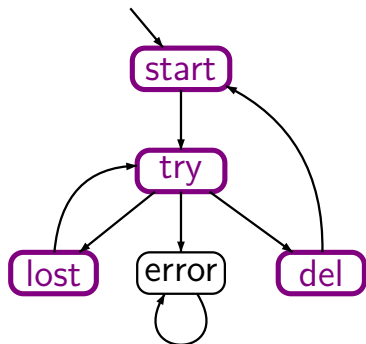
$$\rightsquigarrow \exists \diamond b$$

$$fair = \square \diamond \exists \diamond del \rightsquigarrow \square \diamond c \text{ where } Sat(c) = S \setminus \{error\}$$

$$Sat_{fair}(\neg \exists \bigcirc a) = \{try, error\} = Sat(b)$$

$$Sat_{fair}(\exists \diamond b) = Sat(\exists \diamond (b \wedge a_{fair}))$$

$$= \{start, try, lost, del\}$$



$$\Phi = \exists \diamond \forall \bigcirc (lost \vee del)$$

$$\equiv \exists \diamond \neg \exists \bigcirc (\neg lost \wedge \neg del)$$

$$\rightsquigarrow \exists \diamond \neg \exists \bigcirc a$$

$$\rightsquigarrow \exists \diamond b$$

$$fair = \square \diamond \exists \diamond del \rightsquigarrow \square \diamond c \text{ where } Sat(c) = S \setminus \{error\}$$

$$Sat_{fair}(\neg \exists \bigcirc a) = \{try, error\} = Sat(b)$$

$$Sat_{fair}(\exists \diamond b) = Sat(\exists \diamond (b \wedge a_{fair}))$$

$$= \{start, try, lost, del\}$$



# Correct or wrong?

CTLFAIR4.4-32

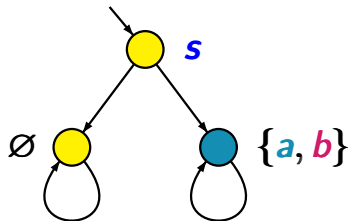
$$s \models_{\text{fair}} \forall O a \quad \text{iff} \quad s \models \forall O (a \wedge a_{\text{fair}})$$

# Correct or wrong?

CTLFAIR4.4-32

$$s \models_{\text{fair}} \forall \bigcirc a \quad \text{iff} \quad s \models \forall \bigcirc (a \wedge a_{\text{fair}})$$

wrong.



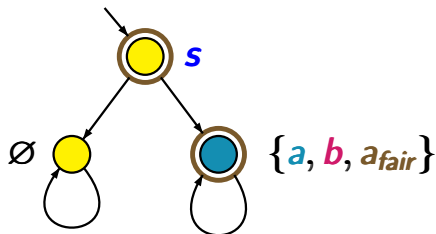
$$\text{fair} = \square \diamond b$$

# Correct or wrong?

CTLFAIR4.4-32

$$s \models_{\text{fair}} \forall \bigcirc a \quad \text{iff} \quad s \models \forall \bigcirc (a \wedge a_{\text{fair}})$$

wrong.



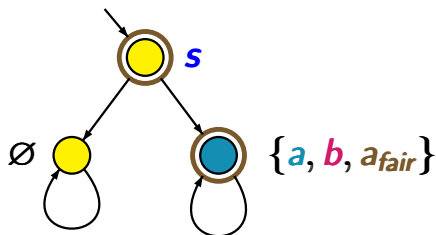
$$\text{fair} = \square \diamond b$$

# Correct or wrong?

CTLFAIR4.4-32

$$s \models_{\text{fair}} \forall \bigcirc a \quad \text{iff} \quad s \models \forall \bigcirc (a \wedge a_{\text{fair}})$$

wrong.



$$\text{fair} = \square \diamond b$$

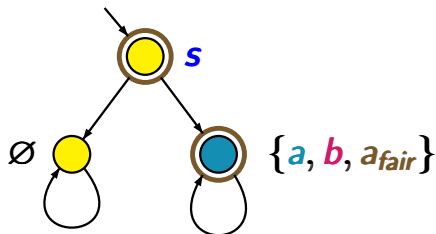
$$s \not\models \forall \bigcirc (a \wedge a_{\text{fair}})$$

# Correct or wrong?

CTLFAIR4.4-32

$$s \models_{\text{fair}} \forall \bigcirc a \quad \text{iff} \quad s \models \forall \bigcirc (a \wedge a_{\text{fair}})$$

wrong.



$$\text{fair} = \square \diamond b$$

$$s \not\models \forall \bigcirc (a \wedge a_{\text{fair}})$$

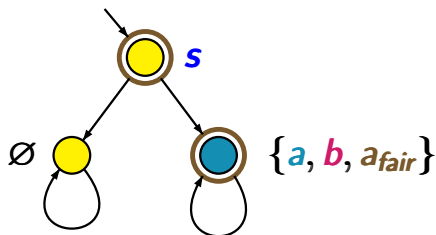
$$s \models_{\text{fair}} \forall \bigcirc a$$

# Correct or wrong?

CTLFAIR4.4-32

$$s \models_{\text{fair}} \forall \bigcirc a \text{ iff } s \models \forall \bigcirc (a \wedge a_{\text{fair}})$$

wrong.



$$\text{fair} = \square \diamond b$$

$$s \not\models \forall \bigcirc (a \wedge a_{\text{fair}})$$

$$s \models_{\text{fair}} \forall \bigcirc a$$

but correct is:

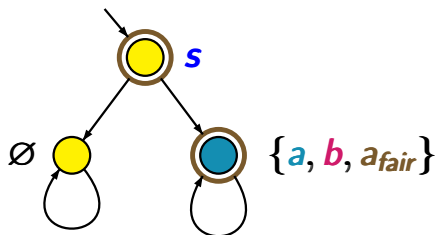
$$s \models_{\text{fair}} \forall \bigcirc a \text{ iff ?}$$

# Correct or wrong?

CTLFAIR4.4-32

$$s \models_{\text{fair}} \forall \bigcirc a \quad \text{iff} \quad s \models \forall \bigcirc (a \wedge a_{\text{fair}})$$

wrong.



$$\text{fair} = \square \diamond b$$

$$s \not\models \forall \bigcirc (a \wedge a_{\text{fair}})$$

$$s \models_{\text{fair}} \forall \bigcirc a$$

but correct is:

$$s \models_{\text{fair}} \forall \bigcirc a \quad \text{iff} \quad s \models \forall \bigcirc (a_{\text{fair}} \rightarrow a)$$

# Correct or wrong?

CTLFAIR4.4-32B

$$s \models_{\text{fair}} \forall \square a \quad \text{iff} \quad s \models \forall \square (a_{\text{fair}} \rightarrow a)$$



# Correct or wrong?

CTLFAIR4.4-32B

$s \models_{fair} \forall \square a$  iff  $s \models \forall \square (a_{fair} \rightarrow a)$   
iff there is no state  $s'$  reachable  
from  $s$  with  $s' \models \neg a \wedge a_{fair}$

# Correct or wrong?

CTLFAIR4.4-32B

$s \models_{\text{fair}} \forall \square a$  iff  $s \models \forall \square (a_{\text{fair}} \rightarrow a)$   
iff there is no state  $s'$  reachable  
from  $s$  with  $s' \models \neg a \wedge a_{\text{fair}}$

correct

# Correct or wrong?

CTLFAIR4.4-32B

$s \models_{\text{fair}} \forall \square a$  iff  $s \models \forall \square (a_{\text{fair}} \rightarrow a)$   
iff there is no state  $s'$  reachable  
from  $s$  with  $s' \models \neg a \wedge a_{\text{fair}}$

correct

$s \models_{\text{fair}} \forall \square a$

$s \models_{\text{fair}} \forall \square a$  iff  $s \models \forall \square (a_{\text{fair}} \rightarrow a)$   
iff there is no state  $s'$  reachable  
from  $s$  with  $s' \models \neg a \wedge a_{\text{fair}}$

correct

$s \models_{\text{fair}} \forall \square a$  iff  $s \models_{\text{fair}} \neg \exists \diamond \neg a$

$s \models_{\text{fair}} \forall \square a$  iff  $s \models \forall \square (a_{\text{fair}} \rightarrow a)$   
iff there is no state  $s'$  reachable  
from  $s$  with  $s' \models \neg a \wedge a_{\text{fair}}$

correct

$s \models_{\text{fair}} \forall \square a$  iff  $s \models_{\text{fair}} \neg \exists \diamond \neg a$   
iff  $s \not\models_{\text{fair}} \exists \diamond \neg a$

$s \models_{fair} \forall \square a$  iff  $s \models \forall \square (a_{fair} \rightarrow a)$   
 iff there is no state  $s'$  reachable  
 from  $s$  with  $s' \models \neg a \wedge a_{fair}$

correct

$s \models_{fair} \forall \square a$  iff  $s \models_{fair} \neg \exists \diamond \neg a$   
 iff  $s \not\models_{fair} \exists \diamond \neg a$   
 iff  $s \not\models \exists \diamond (\neg a \wedge a_{fair})$

$s \models_{\text{fair}} \forall \square a$  iff  $s \models \forall \square (a_{\text{fair}} \rightarrow a)$   
iff there is no state  $s'$  reachable  
from  $s$  with  $s' \models \neg a \wedge a_{\text{fair}}$

correct

$s \models_{\text{fair}} \forall \square a$  iff  $s \models_{\text{fair}} \neg \exists \diamond \neg a$   
iff  $s \not\models_{\text{fair}} \exists \diamond \neg a$   
iff  $s \not\models \exists \diamond (\neg a \wedge a_{\text{fair}})$   
iff  $s \models \neg \exists \diamond (\neg a \wedge a_{\text{fair}})$

$$\begin{aligned}
 s \models_{\text{fair}} \forall \square a & \text{ iff } s \models \forall \square (a_{\text{fair}} \rightarrow a) \\
 & \text{ iff there is no state } s' \text{ reachable} \\
 & \text{ from } s \text{ with } s' \models \neg a \wedge a_{\text{fair}}
 \end{aligned}$$

correct

$$\begin{aligned}
 s \models_{\text{fair}} \forall \square a & \text{ iff } s \models_{\text{fair}} \neg \exists \diamond \neg a \\
 & \text{ iff } s \not\models_{\text{fair}} \exists \diamond \neg a \\
 & \text{ iff } s \not\models \exists \diamond (\neg a \wedge a_{\text{fair}}) \\
 & \text{ iff } s \models \neg \exists \diamond (\neg a \wedge a_{\text{fair}}) \equiv \forall \square (a_{\text{fair}} \rightarrow a)
 \end{aligned}$$



We just saw:

$$s \models_{\text{fair}} \forall \bigcirc a \quad \text{iff} \quad s \models \forall \bigcirc (a_{\text{fair}} \rightarrow a)$$

$$s \models_{\text{fair}} \forall \square a \quad \text{iff} \quad s \models \forall \square (a_{\text{fair}} \rightarrow a)$$

We just saw:

$$s \models_{\text{fair}} \forall \bigcirc a \quad \text{iff} \quad s \models \forall \bigcirc (a_{\text{fair}} \rightarrow a)$$

$$s \models_{\text{fair}} \forall \square a \quad \text{iff} \quad s \models \forall \square (a_{\text{fair}} \rightarrow a)$$

Is the following statement correct ?

$$s \models_{\text{fair}} \forall (b \text{ U } a) \quad \text{iff} \quad s \models \forall (b \text{ U } (a_{\text{fair}} \rightarrow a))$$

We just saw:

$$s \models_{\text{fair}} \forall \bigcirc a \quad \text{iff} \quad s \models \forall \bigcirc (a_{\text{fair}} \rightarrow a)$$

$$s \models_{\text{fair}} \forall \square a \quad \text{iff} \quad s \models \forall \square (a_{\text{fair}} \rightarrow a)$$

Is the following statement correct ?

$$s \models_{\text{fair}} \forall (b \text{ U } a) \quad \text{iff} \quad s \models \forall (b \text{ U } (a_{\text{fair}} \rightarrow a))$$

**wrong.**

# Correct or wrong?

CTLFAIR4.4-33

$$s \models_{fair} \exists O \exists \diamond a \quad \text{iff} \quad s \models \exists O ((\exists \diamond a) \wedge a_{fair})$$

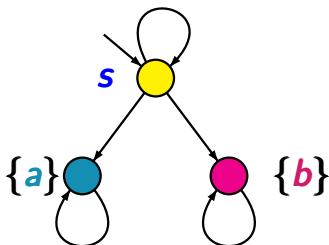
# Correct or wrong?

CTLFAIR4.4-33

$$s \models_{\text{fair}} \exists \bigcirc \exists \diamond a \quad \text{iff} \quad s \models \exists \bigcirc (\exists \diamond a) \wedge a_{\text{fair}}$$

wrong.

$$\text{fair} = \square \diamond b$$



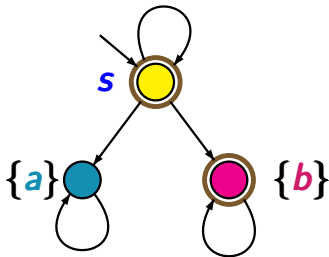
# Correct or wrong?

CTLFAIR4.4-33

$$s \models_{\text{fair}} \exists \bigcirc \exists \diamond a \quad \text{iff} \quad s \models \exists \bigcirc ((\exists \diamond a) \wedge a_{\text{fair}})$$

wrong.

$$\text{fair} = \square \diamond b$$

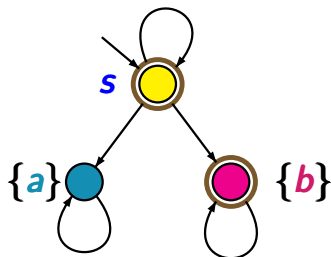


# Correct or wrong?

CTLFAIR4.4-33

$$s \models_{\text{fair}} \exists \bigcirc \exists \diamond a \quad \text{iff} \quad s \models \exists \bigcirc (\exists \diamond a) \wedge a_{\text{fair}}$$

wrong.



$$\text{fair} = \square \diamond b$$

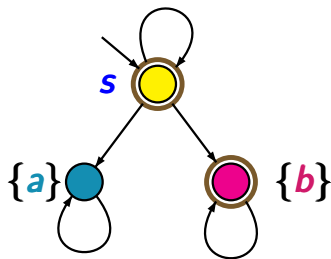
$$s \models \exists \bigcirc (\exists \diamond a) \wedge a_{\text{fair}}$$

# Correct or wrong?

CTLFAIR4.4-33

$$s \models_{\text{fair}} \exists \bigcirc \exists \diamond a \quad \text{iff} \quad s \models \exists \bigcirc (\exists \diamond a) \wedge a_{\text{fair}}$$

wrong.



$$\text{fair} = \square \diamond b$$

$$s \models \exists \bigcirc (\exists \diamond a) \wedge a_{\text{fair}}$$

regard  $s \rightarrow s$

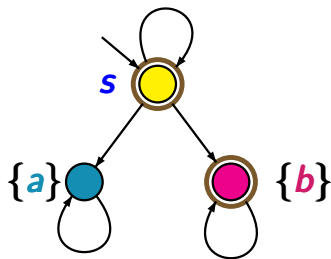


# Correct or wrong?

CTLFAIR4.4-33

$$s \models_{\text{fair}} \exists \bigcirc \exists \diamond a \quad \text{iff} \quad s \models \exists \bigcirc (\exists \diamond a) \wedge a_{\text{fair}}$$

wrong.



$$\text{fair} = \square \diamond b$$

$$s \models \exists \bigcirc (\exists \diamond a) \wedge a_{\text{fair}}$$

regard  $s \rightarrow s$

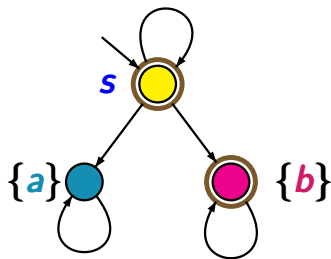
$$s \not\models_{\text{fair}} \exists \bigcirc \exists \diamond a$$

# Correct or wrong?

CTLFAIR4.4-33

$$s \models_{fair} \exists O \exists \Diamond a \text{ iff } s \models \exists O (\exists \Diamond a) \wedge a_{fair}$$

wrong.



$$fair = \Box \Diamond b$$

$$s \models \exists O (\exists \Diamond a) \wedge a_{fair}$$

regard  $s \rightarrow s$

$$s \not\models_{fair} \exists O \exists \Diamond a$$

(note  $Sat_{fair}(\exists \Diamond a) = \emptyset$ )

# Correct or wrong?

CTLFAIR4.4-33

$$s \models_{\text{fair}} \exists \bigcirc \exists \diamond a \quad \text{iff} \quad s \models \exists \bigcirc ((\exists \diamond a) \wedge a_{\text{fair}})$$

wrong.

$$s \models_{\text{fair}} \exists (a \mathbf{W} c) \quad \text{iff} \quad s \models \exists (a \mathbf{W} (c \wedge a_{\text{fair}}))$$

remind: **W** = weak until

# Correct or wrong?

CTLFAIR4.4-33

$$s \models_{\text{fair}} \exists \bigcirc \exists \diamond a \quad \text{iff} \quad s \models \exists \bigcirc ((\exists \diamond a) \wedge a_{\text{fair}})$$

wrong.

$$s \models_{\text{fair}} \exists (a \mathbf{W} c) \quad \text{iff} \quad s \models \exists (a \mathbf{W} (c \wedge a_{\text{fair}}))$$

remind: **W** = weak until

wrong.

# Correct or wrong?

CTLFAIR4.4-33

$$s \models_{\text{fair}} \exists \bigcirc \exists \diamond a \quad \text{iff} \quad s \models \exists \bigcirc ((\exists \diamond a) \wedge a_{\text{fair}})$$

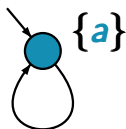
wrong.

$$s \models_{\text{fair}} \exists (a \mathbf{W} c) \quad \text{iff} \quad s \models \exists (a \mathbf{W} (c \wedge a_{\text{fair}}))$$

remind: **W** = weak until

wrong.

$$\text{fair} = \square \diamond b$$



# Correct or wrong?

CTLFAIR4.4-33

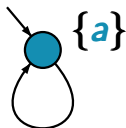
$$s \models_{\text{fair}} \exists \bigcirc \exists \diamond a \quad \text{iff} \quad s \models \exists \bigcirc ((\exists \diamond a) \wedge a_{\text{fair}})$$

wrong.

$$s \models_{\text{fair}} \exists (a \mathbf{W} c) \quad \text{iff} \quad s \models \exists (a \mathbf{W} (c \wedge a_{\text{fair}}))$$

remind: **W** = weak until

wrong.



$$\text{fair} = \square \diamond b$$

$$s \models \exists (a \mathbf{W} (c \wedge a_{\text{fair}}))$$

# Correct or wrong?

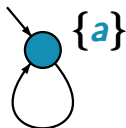
$$s \models_{\text{fair}} \exists \bigcirc \exists \diamond a \quad \text{iff} \quad s \models \exists \bigcirc ((\exists \diamond a) \wedge a_{\text{fair}})$$

wrong.

$$s \models_{\text{fair}} \exists (a \mathbf{W} c) \quad \text{iff} \quad s \models \exists (a \mathbf{W} (c \wedge a_{\text{fair}}))$$

remind: **W** = weak until

wrong.



$$\text{fair} = \square \diamond b$$

$$s \models \exists (a \mathbf{W} (c \wedge a_{\text{fair}}))$$

$$s \not\models_{\text{fair}} \exists (a \mathbf{W} c)$$





**CTL** fairness assumptions: formulas similar to **LTL**

$$\text{e.g., } \mathit{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond \Psi_i \rightarrow \Box \Diamond \Phi_i)$$

**CTL** fairness assumptions: formulas similar to **LTL**

$$\text{e.g., } \mathit{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond \Psi_i \rightarrow \Box \Diamond \Phi_i)$$

**CTL** satisfaction relation with fairness:

$$s \models_{\mathit{fair}} \exists \varphi \quad \text{iff} \quad \text{there exists } \pi \in \mathit{Paths}(s) \text{ with} \\ \pi \models_{\mathit{fair}} \varphi \text{ and } \pi \models_{\mathit{fair}} \varphi$$

**CTL** fairness assumptions: formulas similar to **LTL**

$$\text{e.g., } \mathit{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond \Psi_i \rightarrow \Box \Diamond \Phi_i)$$

**CTL** satisfaction relation with fairness:

$$s \models_{\mathit{fair}} \exists \varphi \quad \text{iff} \quad \text{there exists } \pi \in \mathit{Paths}(s) \text{ with} \\ \pi \models_{\mathit{fair}} \varphi \text{ and } \pi \models_{\mathit{fair}} \varphi$$

model checking for **CTL** with fairness:

**CTL** fairness assumptions: formulas similar to **LTL**

$$\text{e.g., } \mathit{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond \Psi_i \rightarrow \Box \Diamond \Phi_i)$$

**CTL** satisfaction relation with fairness:

$$s \models_{\mathit{fair}} \exists \varphi \quad \text{iff} \quad \text{there exists } \pi \in \mathit{Paths}(s) \text{ with} \\ \pi \models_{\mathit{fair}} \varphi \text{ and } \pi \models_{\mathit{fair}} \varphi$$

model checking for **CTL** with fairness:

- $\exists \bigcirc$ ,  $\exists \mathbf{U}$ ,  $\forall \bigcirc$ ,  $\forall \mathbf{X}$  via **CTL** model checker

**CTL** fairness assumptions: formulas similar to **LTL**

$$\text{e.g., } \mathit{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond \Psi_i \rightarrow \Box \Diamond \Phi_i)$$

**CTL** satisfaction relation with fairness:

$$s \models_{\mathit{fair}} \exists \varphi \quad \text{iff} \quad \text{there exists } \pi \in \mathit{Paths}(s) \text{ with} \\ \pi \models_{\mathit{fair}} \varphi \text{ and } \pi \models_{\mathit{fair}} \varphi$$

model checking for **CTL** with fairness:

- $\exists \bigcirc$ ,  $\exists \mathbf{U}$ ,  $\forall \bigcirc$ ,  $\forall \Box$  via **CTL** model checker
- analysis of **SCCs** for  $\exists \Box$ ,  $\forall \mathbf{U}$

**CTL** fairness assumptions: formulas similar to **LTL**

$$\text{e.g., } \mathit{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond \Psi_i \rightarrow \Box \Diamond \Phi_i)$$

**CTL** satisfaction relation with fairness:

$$s \models_{\mathit{fair}} \exists \varphi \quad \text{iff} \quad \text{there exists } \pi \in \mathit{Paths}(s) \text{ with} \\ \pi \models_{\mathit{fair}} \varphi \text{ and } \pi \models_{\mathit{fair}} \varphi$$

model checking for **CTL** with fairness:

- $\exists \bigcirc, \exists \mathbf{U}, \forall \bigcirc, \forall \Box$  via **CTL** model checker
- analysis of **SCCs** for  $\exists \Box, \forall \mathbf{U}$
- complexity:  $\mathcal{O}(\mathit{size}(\mathcal{T}) \cdot |\Phi| \cdot |\mathit{fair}|)$