# Overview



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 $\longleftarrow$
- counterexamples/witnesses, $CTL^+$ and $CTL^*$

Equivalences and Abstraction

# Complexity of CTL and LTL model checking 

# Complexity of CTL and LTL model checking 

**LTL** model checking problem:

PSPACE-complete and solvable in time

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

---

**CTL** model checking problem:

solvable in polynomial time

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

# Complexity of CTL and LTL model checking

**LTL** model checking problem:

PSPACE-complete and solvable in time

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

---

**CTL** model checking problem:

solvable in polynomial time (even PTIME-complete)

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

**LTL** model checking problem:

PSPACE-complete and solvable in time

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

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

---

**CTL** model checking problem:

solvable in polynomial time (even PTIME-complete)

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

# Complexity of CTL and LTL model checking

**LTL** model checking problem:

PSPACE-complete and solvable in time

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

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

---

**CTL** model checking problem:

solvable in polynomial time (even PTIME-complete)

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

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

# Recall: LTL fairness assumptions



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

# Recall: LTL fairness assumptions



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

# Recall: LTL fairness assumptions



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 $\models_{fair}$ to $\models$

# Recall: LTL fairness assumptions

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 $\models_{fair}$ to $\models$

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

# Recall: LTL fairness assumptions

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 $\models_{fair}$ to $\models$

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

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

$$\pi \models fair \rightarrow \varphi$$

# Recall: LTL fairness assumptions



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

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

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

$$\pi \models fair \rightarrow \varphi$$

# Recall: LTL fairness assumptions



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

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

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

$$\pi \models \; fair \rightarrow \varphi \;\equiv\; \Diamond\Box\neg a \vee \varphi$$

# CTL fairness assumptions

# CTL 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

# CTL 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

*note:* CTL fairness assumptions

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

# CTL 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:

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

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

# Satisfaction relation for CTL with fairness

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

# Satisfaction relation for CTL with fairness



$s \models_{fair} true$

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

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

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

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

# Satisfaction relation for CTL with fairness



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

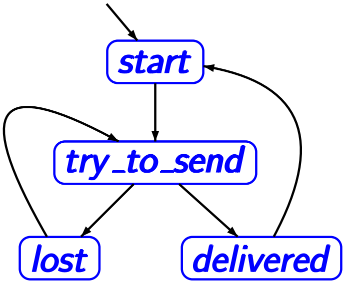
# Satisfaction relation for CTL with fairness

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

e.g., $s_0\, s_1\, s_2 \ldots \models \Box\Diamond\Phi$ iff $\overset{\infty}{\exists}\, i \geq 0$ s.t. $s_i \models \Phi$

# Simple communication protocol



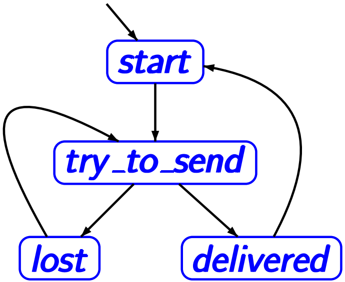



CTL formula

$\Phi = \forall\Box\forall\Diamond start$

# Simple communication protocol





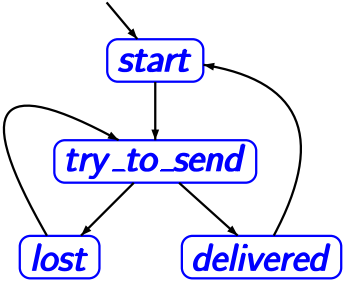

CTL formula

$\Phi = \forall\Box\forall\Diamond start$

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

# Simple communication protocol






CTL formula

$\Phi = \forall\Box\forall\Diamond\,\mathit{start}$

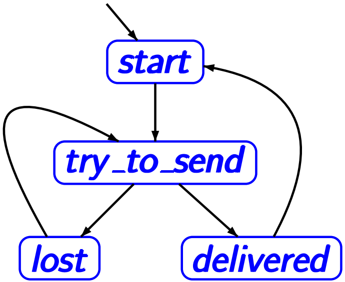
$\mathcal{T} \not\models \Phi$

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

unconditional CTL fairness assumption:

$\mathit{ufair} = \Box\Diamond\,\mathit{delivered}$

# Simple communication protocol




CTL formula

$\Phi = \forall\Box\forall\Diamond start$

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

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

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

unconditional CTL fairness assumption:

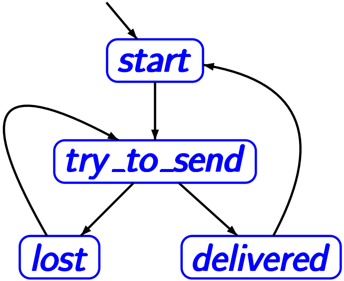
$$ufair = \Box\Diamond delivered$$

strong CTL fairness assumption:

$$sfair = \Box\Diamond try\_to\_send \rightarrow \Box\Diamond delivered$$

# Simple communication protocol

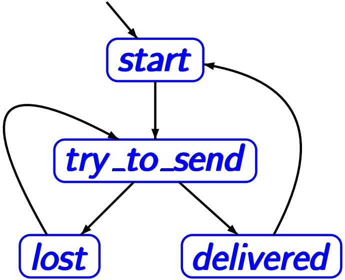





$\Phi = \forall\Box\forall\Diamond start$

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

unconditional fairness: $ufair = \Box\Diamond\, \exists\bigcirc start$




$\Phi = \forall\Box\forall\Diamond start$

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

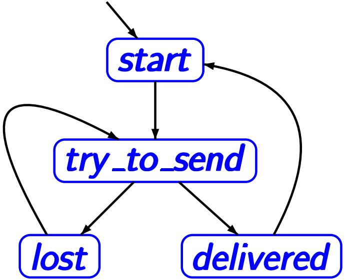
unconditional fairness: $ufair = \Box\Diamond \exists\bigcirc start$

$\uparrow$

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

# Simple communication protocol






$\Phi = \forall\Box\forall\Diamond start$

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

unconditional fairness: $ufair = \Box\Diamond \boxed{\exists\bigcirc start}$

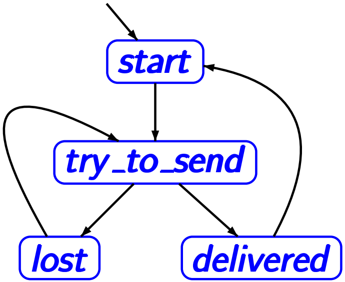
↑

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

$ufair \;\hat{=}\; \Box\Diamond delivered$

# Simple communication protocol






$\Phi = \forall\Box\forall\Diamond start$

$\mathcal{T} \models_{ufair} \Phi$ ✓

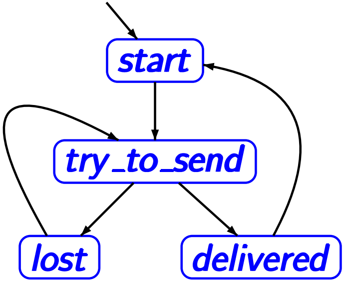
unconditional fairness: $ufair = \Box\Diamond \exists\bigcirc start$

↑

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

$ufair \;\widehat{=}\; \Box\Diamond delivered$

# Simple communication protocol




$\Phi = \forall\Box\forall\Diamond\, start$

$\mathcal{T} \models_{ufair} \Phi$ ✓

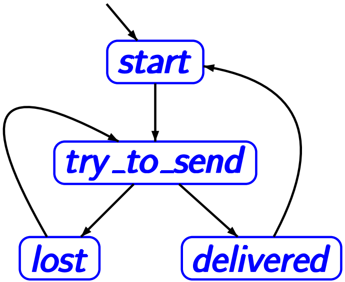
$\mathcal{T} \models_{wfair} \Phi$ **?**

unconditional fairness: $ufair = \Box\Diamond\, \exists\bigcirc start$

weak fairness: $wfair = \Diamond\Box\, \exists\bigcirc delivered \rightarrow \Box\Diamond delivered$

# Simple communication protocol






$\Phi = \forall\Box\forall\Diamond start$

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

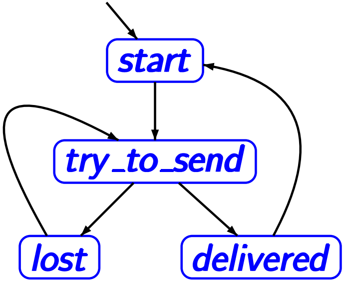
$\mathcal{T} \models_{wfair} \Phi$ ?

unconditional fairness: $ufair = \Box\Diamond\, \exists\bigcirc start$

weak fairness: $wfair = \Diamond\Box\, \exists\bigcirc delivered \longrightarrow \Box\Diamond delivered$

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

# Simple communication protocol




$\Phi = \forall\Box\forall\Diamond start$

$\mathcal{T} \models_{ufair} \Phi$ ✓

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

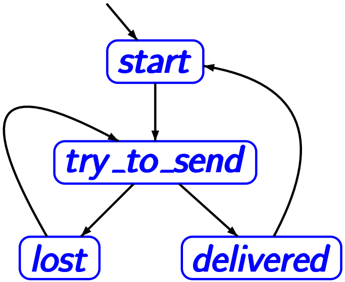
unconditional fairness: $ufair = \Box\Diamond\, \exists\bigcirc start$

weak fairness: $wfair = \Diamond\Box\, \exists\bigcirc delivered \rightarrow \Box\Diamond delivered$

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

$wfair \mathrel{\widehat{=}} \Diamond\Box try\_to\_send \rightarrow \Box\Diamond delivered$

# Simple communication protocol




$\Phi = \forall\Box\forall\Diamond start$

$\mathcal{T} \models_{ufair} \Phi$ ✓

$\mathcal{T} \models_{wfair} \Phi$ wrong

unconditional fairness: $ufair = \Box\Diamond\, \exists\bigcirc start$

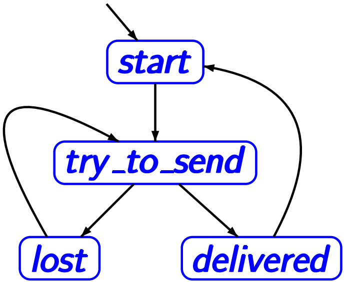
weak fairness: $wfair = \Diamond\Box\, \exists\bigcirc delivered \rightarrow \Box\Diamond delivered$

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

$wfair \mathrel{\widehat{=}} \Diamond\Box try\_to\_send \rightarrow \Box\Diamond delivered$

# Simple communication protocol






$\Phi = \forall\Box\forall\Diamond \mathit{start}$

$\mathcal{T} \models_{\mathit{ufair}} \Phi$ ✓

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

$\mathcal{T} \models_{\mathit{sfair}} \Phi$ ?

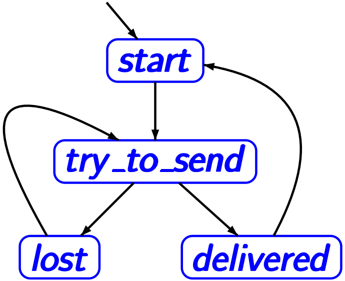
unconditional fairness: $\mathit{ufair} = \Box\Diamond\, \exists\bigcirc \mathit{start}$

weak fairness: $\mathit{wfair} = \Diamond\Box\, \exists\bigcirc \mathit{delivered} \rightarrow \Box\Diamond \mathit{delivered}$

strong fairness: $\mathit{sfair} = \Box\Diamond\, \exists\bigcirc \mathit{delivered} \rightarrow \Box\Diamond \mathit{delivered}$

# Simple communication protocol






$\Phi = \forall\Box\forall\Diamond start$

$\mathcal{T} \models_{ufair} \Phi$ ✓

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

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

unconditional fairness: $ufair = \Box\Diamond\, \exists\bigcirc start$

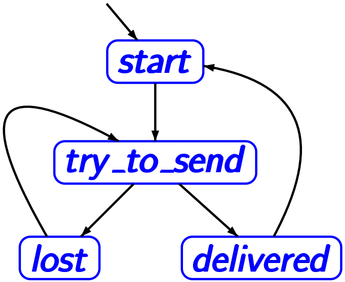
weak fairness: $wfair = \Diamond\Box\, \exists\bigcirc delivered \rightarrow \Box\Diamond delivered$

strong fairness: $sfair = \Box\Diamond\, \exists\bigcirc delivered \rightarrow \Box\Diamond delivered$

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

# Simple communication protocol






$\Phi = \forall\Box\forall\Diamond start$

$\mathcal{T} \models_{ufair} \Phi$ ✓

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

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

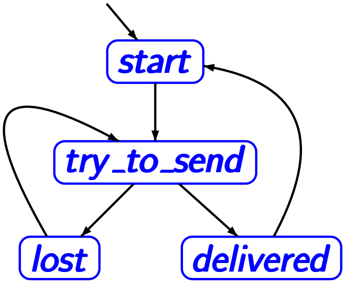
unconditional fairness: $ufair = \Box\Diamond\,\exists\bigcirc start$

weak fairness: $wfair = \Diamond\Box\,\exists\bigcirc delivered \rightarrow \Box\Diamond delivered$

strong fairness: $sfair = \Box\Diamond\,\exists\bigcirc delivered \rightarrow \Box\Diamond delivered$

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

$sfair \mathrel{\widehat{=}} \Box\Diamond try\_to\_send \rightarrow \Box\Diamond delivered$




$\Phi = \forall\Box\forall\Diamond \textit{start}$

$\mathcal{T} \models_{ufair} \Phi$ ✓

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

$\mathcal{T} \models_{sfair} \Phi$ ✓

unconditional fairness: $\textit{ufair} = \Box\Diamond\, \exists\bigcirc \textit{start}$

weak fairness: $\textit{wfair} = \Diamond\Box\, \exists\bigcirc \textit{delivered} \rightarrow \Box\Diamond \textit{delivered}$

strong fairness: $\textit{sfair} = \Box\Diamond\, \exists\bigcirc \textit{delivered} \rightarrow \Box\Diamond \textit{delivered}$

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

$\textit{sfair} \;\widehat{=}\; \Box\Diamond \textit{try\_to\_send} \rightarrow \Box\Diamond \textit{delivered}$

# Correct or wrong?



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

# Correct or wrong?



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

**correct.**

# Correct or wrong?



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

**correct.** Note that:

$$s \models \forall\varphi \quad \Longrightarrow \quad \text{for all } \pi \in Paths(s)\text{:} \;\; \pi \models \varphi$$

# Correct or wrong?



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

**correct.** Note that:

$$s \models \forall\varphi \quad \Longrightarrow \quad \text{for all } \pi \in Paths(s)\text{: } \pi \models \varphi$$

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

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

**correct.** Note that:

$$\begin{aligned} s \models \forall\varphi \quad &\Longrightarrow \quad \text{for all } \pi \in Paths(s)\text{:} \quad \pi \models \varphi \\ &\Longrightarrow \quad \text{for all } \pi \in Paths(s)\text{:} \\ &\qquad\qquad \pi \models fair \text{ implies } \pi \models \varphi \\ &\Longrightarrow \quad s \models_{fair} \forall\varphi \end{aligned}$$

# Correct or wrong?



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

**correct.**

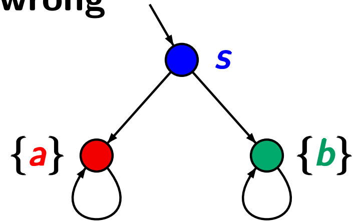
If $s \models \exists\Diamond a$ where $a \in AP$ then $s \models_{fair} \exists\Diamond a$

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**



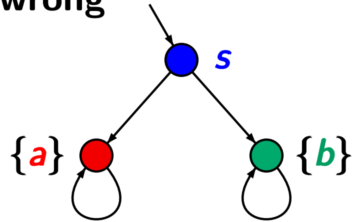

$fair = \Box\Diamond b$

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**




$fair = \Box\Diamond b$

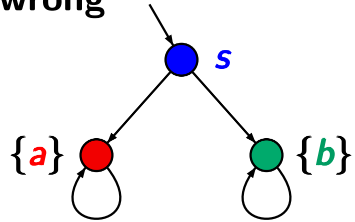
just one fair path ● ● ● ● . . .

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**




$fair = \Box\Diamond b$

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

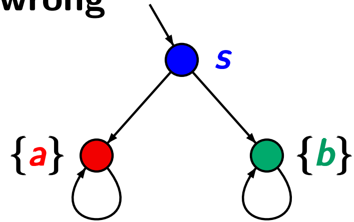
just one fair path 

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

**correct.**

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

**wrong**




$fair = \Box\Diamond b$

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

$s \models \exists\Diamond a$

just one fair path  . . .

# Correct or wrong?

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?



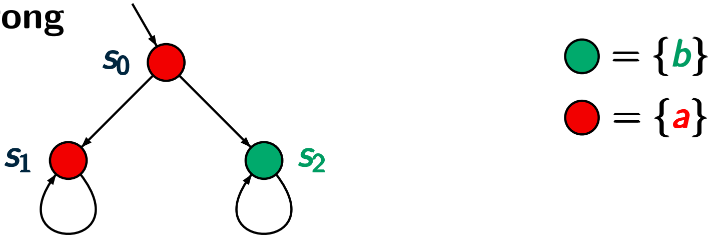
If $s \models \forall\Diamond\exists\Box a$ then $s \models_{fair} \forall\Diamond\exists\Box a$

# Correct or wrong?



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

**wrong**

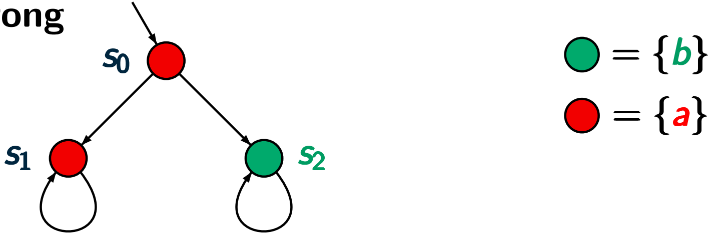


# Correct or wrong?



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

**wrong**



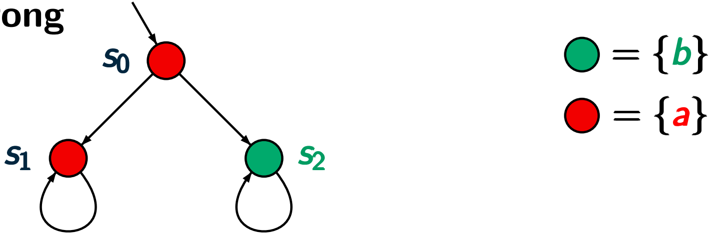

$Sat(\exists\Box a) = \{s_0, s_1\}$

# Correct or wrong?



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

**wrong**




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

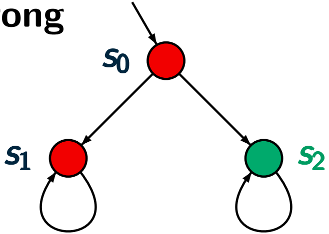
$$Sat(\forall\Diamond\exists\Box a) = \{s_0, s_1\}$$

# Correct or wrong?



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

**wrong**




$\bullet = \{b\}$ (green)

$\bullet = \{a\}$ (red)

$fair = \Box\Diamond b$

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

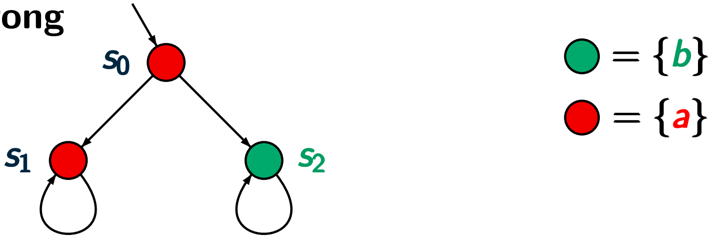
$Sat(\forall\Diamond\exists\Box a) = \{s_0, s_1\}$

# Correct or wrong?



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

**wrong**




$fair = \Box\Diamond b$

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

$Sat_{fair}(\exists\Box a) = \varnothing$

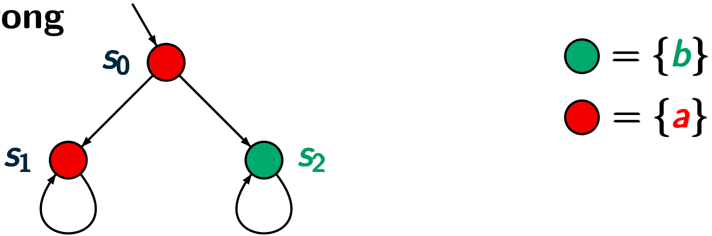
$Sat(\forall\Diamond\exists\Box a) = \{s_0, s_1\}$

# Correct or wrong?



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

**wrong**




$fair = \Box\Diamond b$

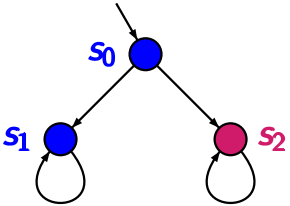
$Sat(\exists\Box a) = \{s_0, s_1\}$ $\quad$ $Sat_{fair}(\exists\Box a) = \varnothing$

$Sat(\forall\Diamond\exists\Box a) = \{s_0, s_1\}$ $\quad$ $Sat_{fair}(\forall\Diamond\exists\Box a) = \varnothing$

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

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

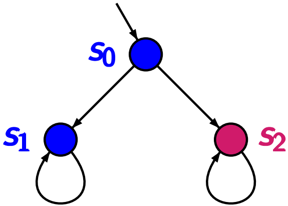





● $= \{a\}$

● $= \varnothing$

$fair = \Box\Diamond a$




$\bullet = \{a\}$ (red)

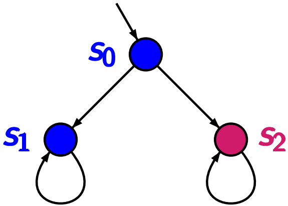
$\bullet = \varnothing$ (blue)

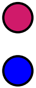
$fair = \Box\Diamond a$

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

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





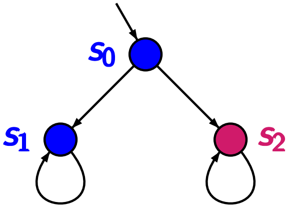




$fair = \Box\Diamond a$

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

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






$\bullet = \{a\}$ (red)

$\bullet = \varnothing$ (blue)

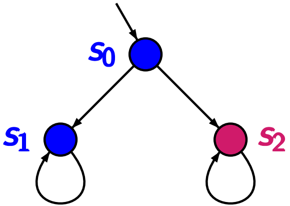
$fair = \Box\Diamond a$

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

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

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






(red circle) $= \{a\}$

(blue circle) $= \varnothing$

$fair = \Box\Diamond a$

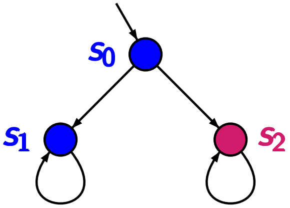
$Sat_{fair}(\exists\Box true) = \{s_0, s_2\}$

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

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

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






$\bullet = \{a\}$ (red)

$\bullet = \varnothing$ (blue)

$fair = \Box\Diamond a$

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

$Sat_{fair}(\exists\Box true)$ = 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

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

# Model checking problem for FairCTL

# Model checking problem for FairCTL



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

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

# Model checking problem for FairCTL



*given*: finite transition system $\mathcal{T}$

CTL formula $\Phi$

CTL fairness assumption *fair*, e.g.,

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

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

# Model checking problem for FairCTL



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

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

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

*for simplicity*:

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

$$\exists\bigcirc, \ \exists\mathsf{U}, \ \exists\Box$$

# Preprocessing of FairCTL model checking

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

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

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

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

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

*question*: does $\mathcal{T} \models_{fair} \Phi$ 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.,

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

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

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

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

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

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

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

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

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

# Preprocessing of FairCTL model checking



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

$$fair = \bigwedge_{1 \leq i \leq k} \Box\Diamond b_i \rightarrow \Box\Diamond c_i \text{ with } b_i, c_i \in AP$$

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

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

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

# Idea of FairCTL model checking



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

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

1. ... preprocessing ...

# Idea of FairCTL model checking



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

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

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

# Idea of FairCTL model checking



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

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

# Idea of FairCTL model checking



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

*question*: does $\mathcal{T} \models_{fair} \Phi$ 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**
   - $\exists\bigcirc$, $\exists \mathsf{U}$: via standard **CTL** model checking

# Idea of FairCTL model checking



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

*question*: does $\mathcal{T} \models_{fair} \Phi$ 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**
   - $\exists\bigcirc$, $\exists$**U**: via standard **CTL** model checking
   - $\exists\Box$: via analysis of **SCCs**

# CTL model checking with fairness



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:* $\Psi = \mathit{true}$ 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:* $\Psi = \mathit{true}$ or $\Psi = a \in AP$ or the outer most operator of $\Psi$ is a negation or conjunction:

$$\begin{aligned}
Sat_{fair}(\mathit{true}) &= S \\
Sat_{fair}(a) &= \{s \in S : \ a \in L(s)\} \\
Sat_{fair}(\neg\Psi) &= S \setminus Sat_{fair}(\Psi) \\
Sat_{fair}(\Psi_1 \wedge \Psi_2) &= Sat_{fair}(\Psi_1) \cap Sat_{fair}(\Psi_2)
\end{aligned}$$

# Idea of FairCTL model checking



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

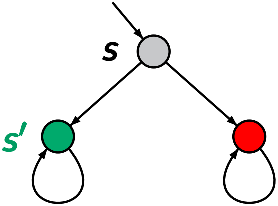
*question*: does $\mathcal{T} \models_{fair} \Phi$ hold ?

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
   - $\exists\bigcirc$, $\exists\mathsf{U}$: via standard **CTL** model checking
   - $\exists\Box$: via analysis of SCCs

# FairCTL model checking: treatment of $\exists\bigcirc$ 

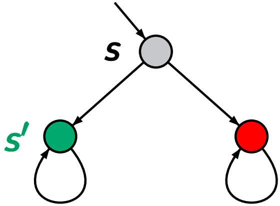
# FairCTL model checking: treatment of $\exists\bigcirc$






$fair = \Box\Diamond red$

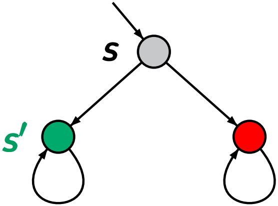
# FairCTL model checking: treatment of $\exists\bigcirc$ 




$fair = \Box\Diamond red$

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

# FairCTL model checking: treatment of $\exists\bigcirc$ 

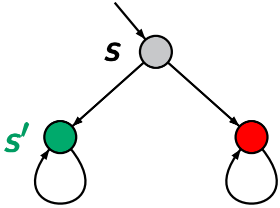



$fair = \Box\Diamond red$

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

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

# FairCTL model checking: treatment of $\exists\bigcirc$



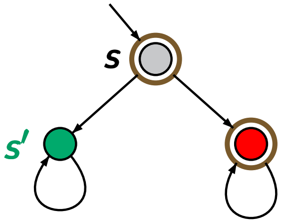

$fair = \Box\Diamond red$

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

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

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

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




$fair = \Box\Diamond red$

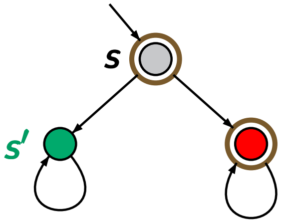
$s \not\models_{fair} \exists\bigcirc green$

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

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

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

# FairCTL model checking: treatment of $\exists\bigcirc$




$fair = \Box\Diamond red$

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

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

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

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

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

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

# FairCTL model checking: $\exists\bigcirc$ and $\exists U$



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

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

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

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

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

# FairCTL model checking: $\exists\bigcirc$ and $\exists U$ 

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

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

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

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

# FairCTL model checking: $\exists\bigcirc$ and $\exists\mathsf{U}$

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

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

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

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

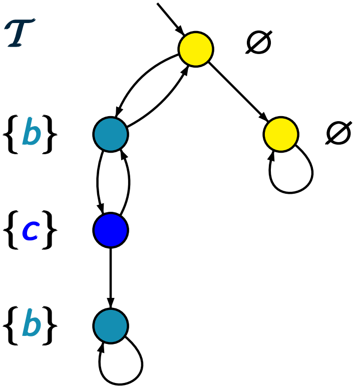
$$s \models_{fair} \exists(c \,\mathsf{U}\, b) \quad \text{iff} \quad s \models \exists(c \,\mathsf{U}(b \wedge a_{fair}))$$

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

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

# Example: treatment of $\exists\Diamond$



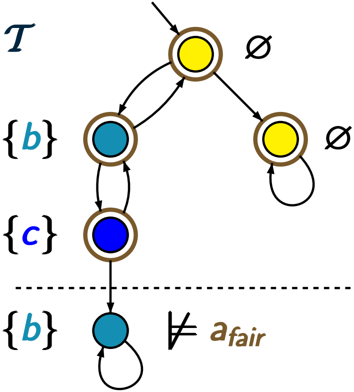



CTL formula $\exists\Diamond c$

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

# Example: treatment of $\exists\Diamond$






CTL formula $\exists\Diamond c$

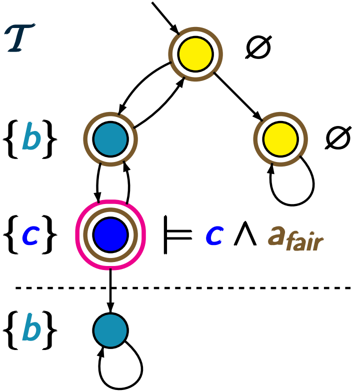
$\downarrow$

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

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

# Example: treatment of $\exists\Diamond$





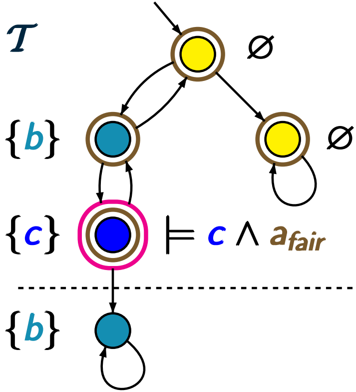

CTL formula $\exists\Diamond c$

$\downarrow$

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

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

# Example: treatment of $\exists\Diamond$




CTL formula $\exists\Diamond c$

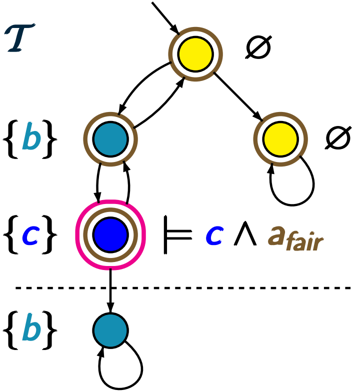
$\downarrow$

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

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

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

# Example: treatment of $\exists\Diamond$




CTL formula $\exists\Diamond c$

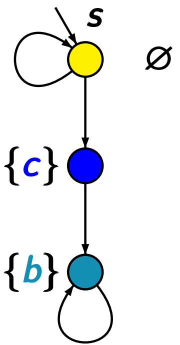
$\downarrow$

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

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

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

$\mathcal{T}$:

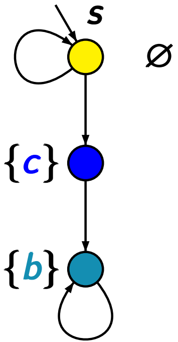



$\mathcal{T} \models \exists(\neg b \,\mathsf{U}\, c)$

# Example: treatment of ∃U



$\mathcal{T}$:

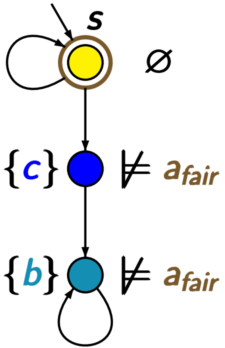



strong fairness assumption: $fair = \Box\Diamond b \rightarrow \Box\Diamond c$

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

# Example: treatment of ∃U

$\mathcal{T}$:

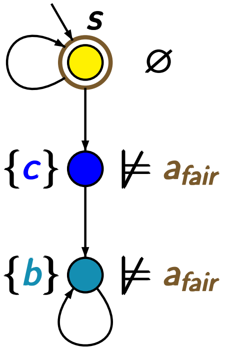



strong fairness assumption: $fair = \Box\Diamond b \to \Box\Diamond c$

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

# Example: treatment of ∃U

$\mathcal{T}$:



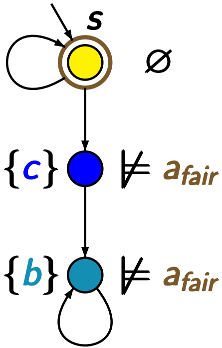

$$Sat(c \wedge a_{fair}) = \varnothing$$

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

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

# Example: treatment of ∃U

$\mathcal{T}$:




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

$$\Uparrow$$

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

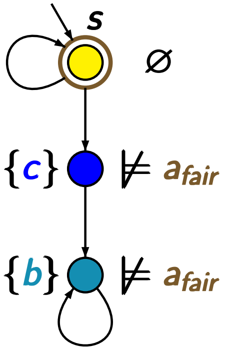
strong fairness assumption: $fair = \Box\Diamond b \rightarrow \Box\Diamond c$

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

# Example: treatment of $\exists\mathsf{U}$



$\mathcal{T}$:




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

$$\Uparrow$$

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

$$\Uparrow$$

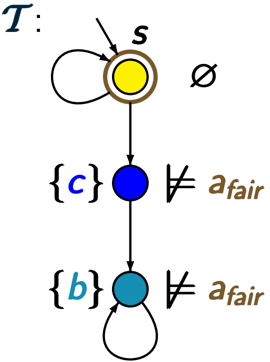
$$Sat(c \wedge a_{fair}) = \varnothing$$

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

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

# Example: treatment of ∃U






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

$$\Uparrow$$

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

$$\Uparrow$$

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

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

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

# Correct or wrong?



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

# Correct or wrong?



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

**correct.**

# Correct or wrong?



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

**correct.** Note that:

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

# Correct or wrong?



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

**correct.** Note that:

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

$$\begin{aligned} & s \models \quad \exists\bigcirc\exists(c \,\mathsf{U}(b \wedge a_{fair})) \\ \Longleftrightarrow \quad & s \models \quad \exists\bigcirc\exists((c \wedge a_{fair}) \,\mathsf{U}(b \wedge a_{fair})) \end{aligned}$$

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

**correct.** Note that:

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

$$\begin{aligned}
& s \models && \exists\bigcirc\exists(c \,\mathsf{U}(b \wedge a_{fair})) \\
\Longleftrightarrow\ & s \models && \exists\bigcirc\exists((c \wedge a_{fair}) \,\mathsf{U}(b \wedge a_{fair})) \\
\Longleftrightarrow\ & s \models && \exists\bigcirc\big(\exists(c \,\mathsf{U}(b \wedge a_{fair})) \wedge a_{fair}\big)
\end{aligned}$$

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

**correct.** Note that:

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

$$\begin{array}{rll} & s \models & \exists\bigcirc\exists(c \,\mathsf{U}(b \wedge a_{fair})) \\ \Longleftrightarrow & s \models & \exists\bigcirc\exists((c \wedge a_{fair}) \,\mathsf{U}(b \wedge a_{fair})) \\ \Longleftrightarrow & s \models & \exists\bigcirc\big(\exists(c \,\mathsf{U}(b \wedge a_{fair})) \wedge a_{fair}\big) \\ \Longleftrightarrow & s \models_{fair} & \exists\bigcirc\exists(c \,\mathsf{U}\, b) \end{array}$$

# Correct or wrong?



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

**correct.**

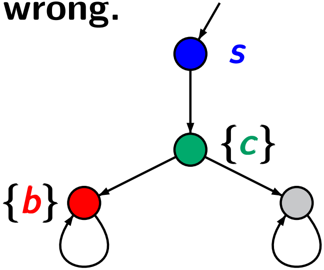
$$s \models_{fair} \exists\bigcirc\exists(c \,\mathsf{U}\, b) \quad \text{iff} \quad s \models \exists\bigcirc(\exists(c \,\mathsf{U}\, b) \wedge a_{fair})$$

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

**correct.**

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

**wrong.**



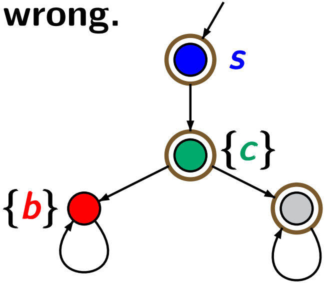

$fair = \Box\Diamond gray$

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

**correct.**

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

**wrong.**



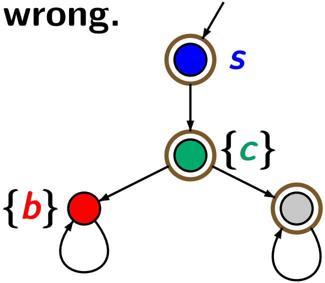

$fair = \Box\Diamond gray$

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

**correct.**

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

**wrong.**




$fair = \Box\Diamond gray$

$Sat_{fair}(\exists(c \,\mathsf{U}\, b)) = \varnothing$

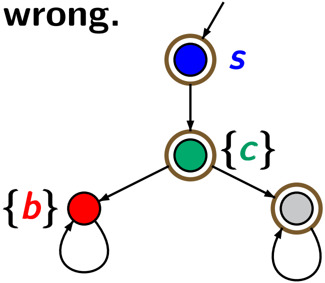
# Correct or wrong?

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

**correct.**

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

**wrong.**




$fair = \Box\Diamond gray$

$Sat_{fair}(\exists(c \,\mathsf{U}\, b)) = \varnothing$

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

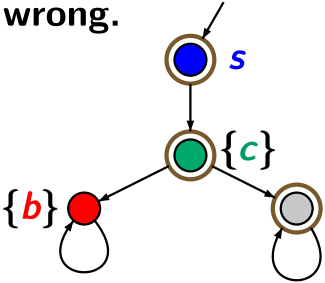
# Correct or wrong?

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

**correct.**

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

**wrong.**




$fair = \Box\Diamond gray$

$Sat_{fair}(\exists(c \,\mathsf{U}\, b)) = \varnothing$

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

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

# Correct or wrong?

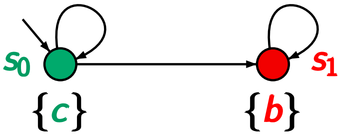


$$s \models_{fair} \exists\Box c \quad \text{iff} \quad s \models \exists\Box(c \wedge a_{fair})$$

# Correct or wrong?

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

**wrong.**



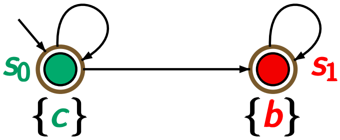

$fair = \Box\Diamond b$

# Correct or wrong?



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

**wrong.**



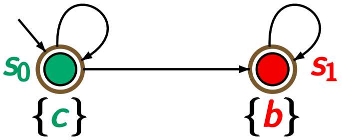

$fair = \Box\Diamond b$

$s_0 \models a_{fair}$

$s_1 \models a_{fair}$

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

**wrong.**




$fair = \Box\Diamond b$

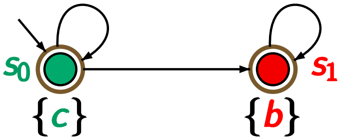
$s_0 \models a_{fair}$

$s_1 \models a_{fair}$

regard state $s = s_0$:

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

**wrong.**




$fair = \Box\Diamond b$

$s_0 \models a_{fair}$

$s_1 \models a_{fair}$

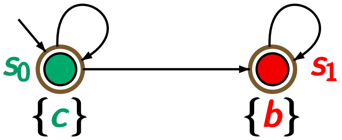
regard state $s = s_0$:

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

# Correct or wrong?

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

**wrong.**




$fair = \Box\Diamond b$

$s_0 \models a_{fair}$

$s_1 \models a_{fair}$

regard state $s = s_0$:

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

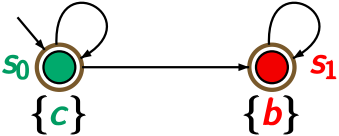
↑

path $\pi = s_0\, s_0\, s_0\, s_0 \ldots \models \Box(c \wedge a_{fair})$

# Correct or wrong?

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

**wrong.**




$fair = \Box\Diamond b$

$s_0 \models a_{fair}$

$s_1 \models a_{fair}$

regard state $s = s_0$:

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

↑

path $\pi = s_0\, s_0\, s_0\, s_0 \ldots \models \Box(c \wedge a_{fair})$

# Idea of FairCTL model checking

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

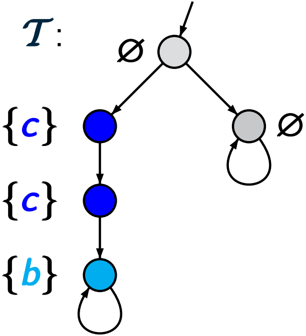
*question*: does $\mathcal{T} \models_{fair} \Phi$ hold ?

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
   - $\exists\bigcirc$, $\exists\mathsf{U}$: via standard CTL model checking
   - $\exists\Box$: via analysis of **SCCs**

# $\exists\Box\Psi$ under strong fairness



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

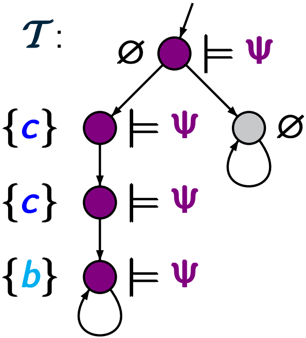



$\mathcal{T} \models_{fair} \exists\Box\Psi$ ?

# $\exists\Box\Psi$ under strong fairness



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



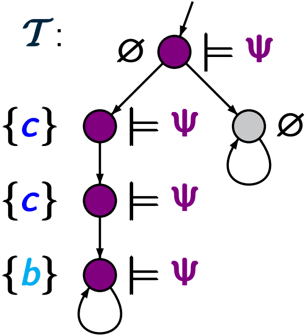

$\mathcal{T} \models_{fair} \exists\Box\Psi$ ?

1. calculate $Sat_{fair}(\Psi)$

# $\exists\Box\Psi$ under strong fairness

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

$\mathcal{T}$:



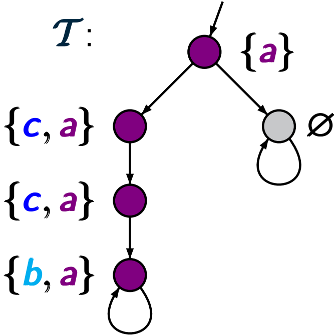

$\mathcal{T} \models_{fair} \exists\Box\Psi$ ?

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

# $\exists\Box\Psi$ under strong fairness

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

$\mathcal{T}$:



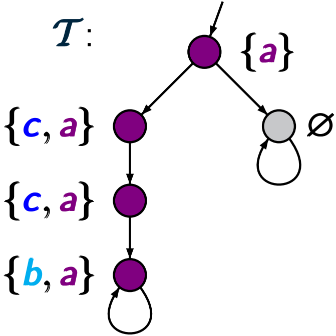

$\mathcal{T} \models_{fair} \exists\Box\Psi$ ?

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

# $\exists\Box\Psi$ under strong fairness



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

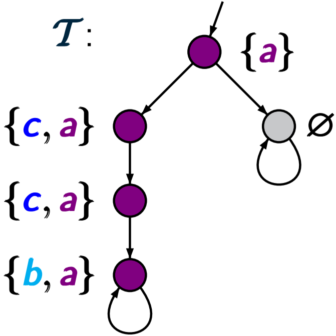


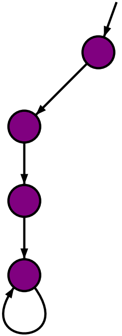

$\mathcal{T} \models_{fair} \exists\Box\Psi$ ?

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

# $\exists\Box\Psi$ under strong fairness

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

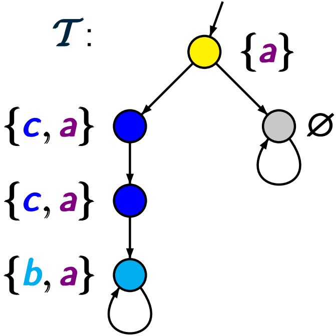


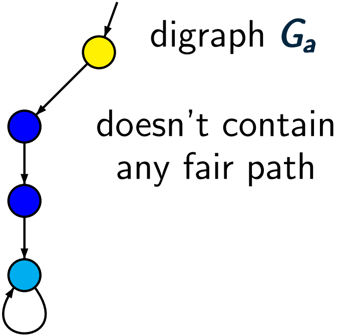




1. calculate $Sat_{fair}(\Psi)$
2. replace $\Psi$ with a fresh atomic proposition $a = a_\Psi$
3. calculate $Sat_{fair}(\exists\Box a)$

# $\exists\Box\Psi$ under strong fairness

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



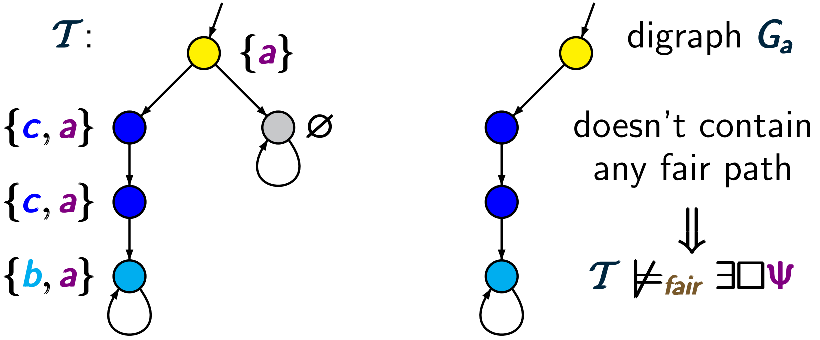




1. calculate $Sat_{fair}(\Psi)$
2. replace $\Psi$ with a fresh atomic proposition $a = a_\Psi$
3. calculate $Sat_{fair}(\exists\Box a)$

# $\exists\Box\Psi$ under strong fairness



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




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

# Treatment of $\exists\Box a$ for FairCTL



*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 $Sat_{fair}(\exists\Box true)$

# Treatment of $\exists\Box a$ for FairCTL

*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

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

# Treatment of $\exists\Box$ under strong fairness



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

# Treatment of $\exists\Box$ under strong fairness

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

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

$$s_0\, s_1 \ldots s_n \ldots s_{n+r}$$

# Treatment of $\exists\Box$ under strong fairness

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

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

$$s_0\, s_1 \ldots s_n \ldots s_{n+r}$$

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

# Treatment of $\exists\Box$ under strong fairness 

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

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

$$s_0\, s_1 \ldots s_n \ldots s_{n+r}$$

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

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

# Treatment of $\exists\Box$ under strong fairness



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

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

$$s_0\, s_1 \ldots s_n \ldots s_{n+r}$$

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 $s_0\, s_1 \ldots s_n (s_{n+1} \ldots s_{n+r})^\omega$ is fair, i.e.,

# Treatment of $\exists\Box$ under strong fairness

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

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

$$s_0\, s_1 \ldots s_n \ldots s_{n+r}$$

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 $s_0\, s_1 \ldots s_n (s_{n+1} \ldots s_{n+r})^\omega$ is fair, i.e., for all $1 \leq i \leq k$:

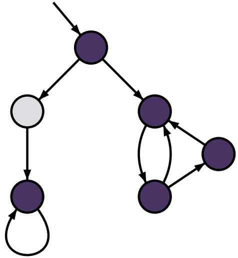
$$\{s_{n+1}, \ldots, s_{n+r}\} \cap Sat(b_i) = \varnothing$$

or $$\{s_{n+1}, \ldots, s_{n+r}\} \cap Sat(c_i) \neq \varnothing$$

# $\exists\Box a$ under strong fairness

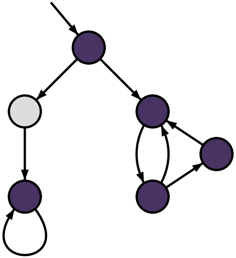


does $\mathcal{T} \models_{fair} \exists\Box a$ hold ?



# $\exists\Box a$ under strong fairness 

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



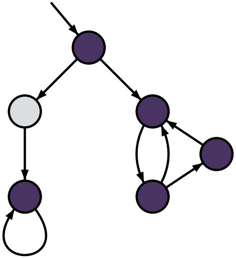
$\bullet \models a \quad \circ \not\models a$

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

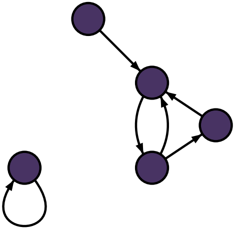
# $\exists\Box a$ under strong fairness



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



digraph $G_a$



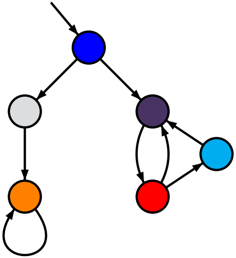
● $\models a$ ○ $\not\models a$

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

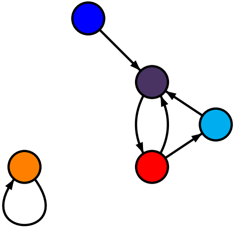
# $\exists\Box a$ under strong fairness

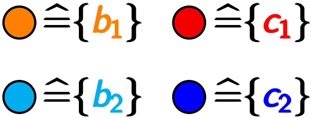


does $\mathcal{T} \models_{fair} \exists\Box a$ hold ?



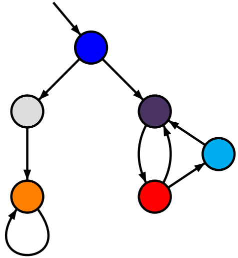
digraph $G_a$



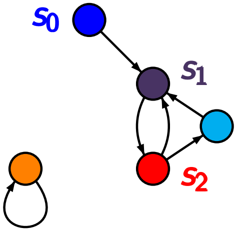



$$fair = (\Box\Diamond b_1 \rightarrow \Box\Diamond c_1) \wedge (\Box\Diamond b_2 \rightarrow \Box\Diamond c_2)$$

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



digraph $G_a$




$\widehat{=}\{b_1\}$ $\widehat{=}\{c_1\}$

$\widehat{=}\{b_2\}$ $\widehat{=}\{c_2\}$

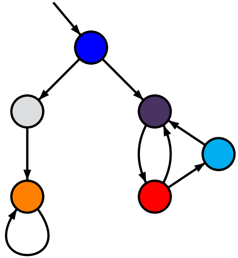
$s_0\,(s_1\,s_2)^\omega \models \neg\Box\Diamond b_2 \wedge \Box\Diamond c_1$

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

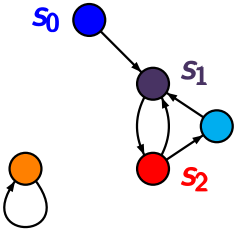
# $\exists\Box a$ under strong fairness

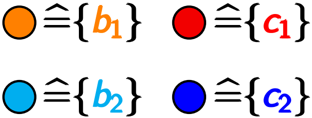


does $\mathcal{T} \models_{fair} \exists\Box a$ hold ?



digraph $G_a$




$s_0\,(s_1\,s_2)^\omega \models \neg\Box\Diamond b_2 \wedge \Box\Diamond c_1$

$s_0\,(s_1\,s_2)^\omega \models fair$

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

# Treatment of $\exists\Box$ under strong fairness



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

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

$$s_0\, s_1 \ldots s_n \ldots s_{n+r}$$

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 $1 \leq i \leq k$: $\{s_{n+1}, \ldots, s_{n+r}\} \cap Sat(b_i) = \varnothing$
  or $\{s_{n+1}, \ldots, s_{n+r}\} \cap Sat(c_i) \neq \varnothing$

# Treatment of $\exists\Box$ under strong fairness



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

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

$$s_0\, s_1 \ldots s_n \ldots s_{n+r}$$

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 $1 \leq i \leq k$: $\{s_{n+1}, \ldots, s_{n+r}\} \cap Sat(b_i) = \varnothing$
  or $\{s_{n+1}, \ldots, s_{n+r}\} \cap Sat(c_i) \neq \varnothing$

↑

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

# Treatment of $\exists\Box$ under strong fairness



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

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

$$s_0\, s_1 \ldots s_n \ldots s_{n+r}$$

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 $1 \leq i \leq k$: $\{s_{n+1}, \ldots, s_{n+r}\} \cap Sat(b_i) = \varnothing$
  or $\{s_{n+1}, \ldots, s_{n+r}\} \cap Sat(c_i) \neq \varnothing$

↑

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

# Treatment of $\exists\Box$ under strong fairness



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

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

# Treatment of $\exists\Box$ under strong fairness

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

$s \models_{fair} \exists\Box a$ 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 $1 \leq i \leq k$:

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

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

# Treatment of $\exists\Box$ under strong fairness

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

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

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

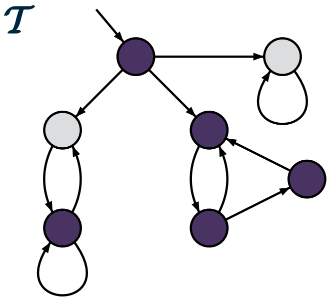
(2) for all $1 \leq i \leq k$:

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

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

# Example: computation of $Sat_{fair}(\exists\Box a)$





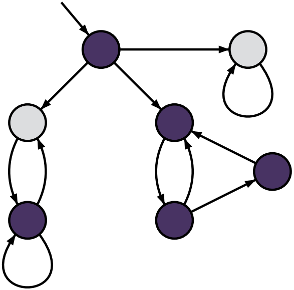

$\models a$ $\not\models a$

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

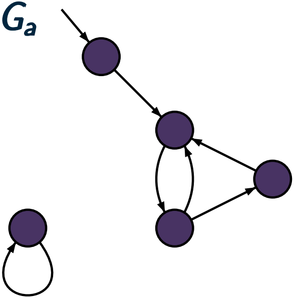
# Example: computation of $Sat_{fair}(\exists\Box a)$



$\mathcal{T}$



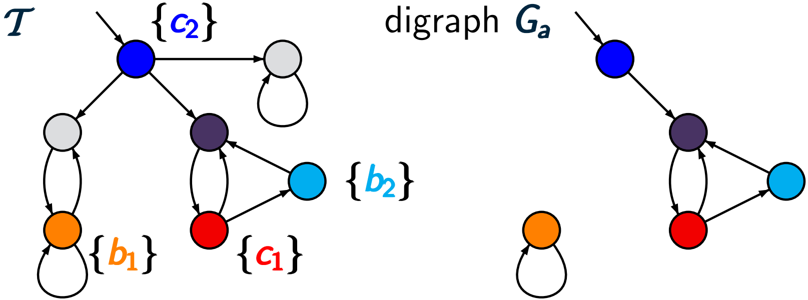
digraph $G_a$




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

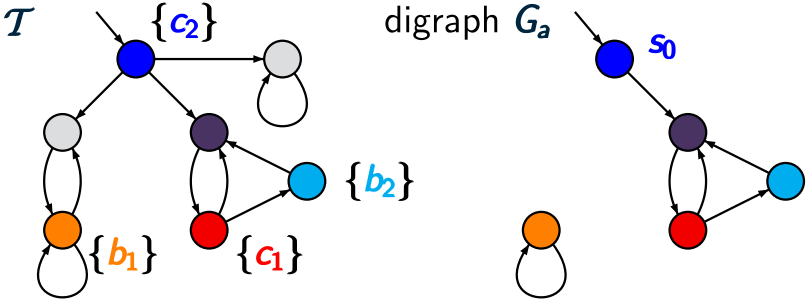
# Example: computation of $Sat_{fair}(\exists\Box a)$






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

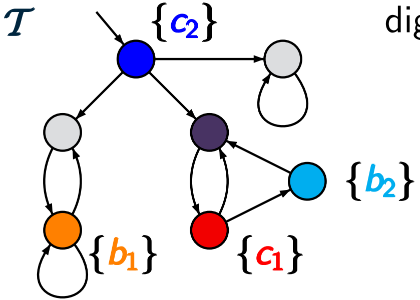
# Example: computation of $Sat_{fair}(\exists\Box a)$

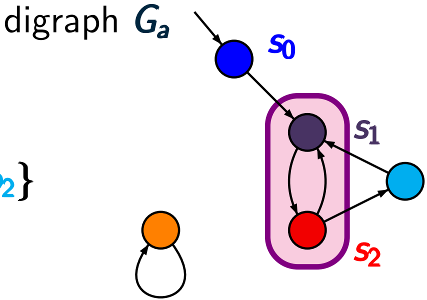



$$fair = (\Box\Diamond b_1 \rightarrow \Box\Diamond c_1) \wedge (\Box\Diamond b_2 \rightarrow \Box\Diamond c_2)$$

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

# Example: computation of $Sat_{fair}(\exists\Box a)$



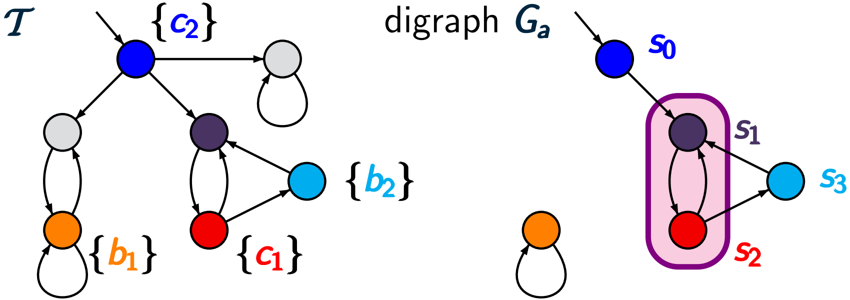




$$fair = (\Box\Diamond b_1 \rightarrow \Box\Diamond c_1) \wedge (\Box\Diamond b_2 \rightarrow \Box\Diamond c_2)$$

$s_0 \models_{fair} \exists\Box a$ as $s_0\, s_1\, s_2\, s_1\, s_2 \ldots \models_{LTL} fair$

# Example: computation of $Sat_{fair}(\exists\Box a)$






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

$s_0 \models_{fair} \exists\Box a$ as $s_0\, s_1\, s_2\, s_1\, s_2 \ldots \models_{LTL} fair$

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

# CTL model checking with fairness



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

# CTL model checking 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:* $fair = \Box\Diamond b \rightarrow \Box\Diamond c$

*case 3:* arbitrary strong fairness assumption

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

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

*case 3:* arbitrary strong fairness assumption

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

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

# $\exists\Box a$ under unconditional fairness



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

# $\exists\Box a$ under unconditional fairness



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

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

# $\exists\Box a$ under unconditional fairness



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

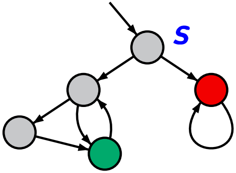
$s \models_{fair} \exists\Box a$ iff there exists a nontrivial **SCC** $C$ in $G_a$ that is reachable from $s$ and $C \cap Sat(c_i) \neq \varnothing$ for $i = 1, \ldots, k$

# $\exists\Box a$ under unconditional fairness

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

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

digraph $G_a$




fairness assumption:

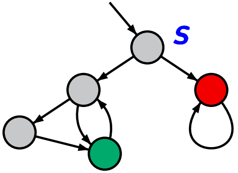
$fair = \Box\Diamond c_1 \wedge \Box\Diamond c_2$

# $\exists\Box a$ under unconditional fairness

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

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

digraph $G_a$




fairness assumption:

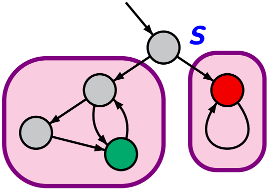
$fair = \Box\Diamond c_1 \wedge \Box\Diamond c_2$

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

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

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

digraph $G_a$




fairness assumption:

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

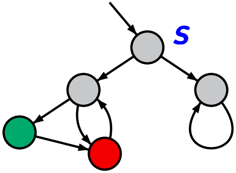
$s \not\models_{fair} \exists\Box a$

# $\exists\Box a$ under unconditional fairness

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

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

digraph $G_a$

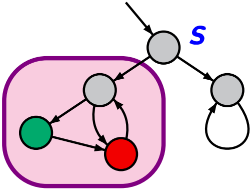



fairness assumption:
$fair = \Box\Diamond c_1 \wedge \Box\Diamond c_2$

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

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

digraph $G_a$




fairness assumption:

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

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

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

*here:* explanations only for strong fairness

*case 1*: unconditional fairness $\surd$

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

*case 3:* arbitrary strong fairness assumption

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

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

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

# Strong fairness: 1 fairness requirement

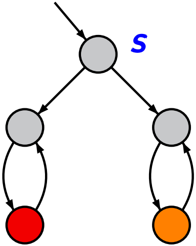


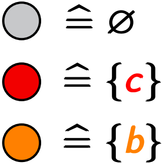
$$fair = \Box\Diamond b \rightarrow \Box\Diamond c$$

# Strong fairness: 1 fairness requirement

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

digraph $G_a$

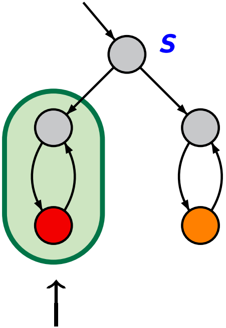


# Strong fairness: 1 fairness requirement

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

digraph $G_a$




$\widehat{=}\ \varnothing$

$\widehat{=}\ \{c\}$

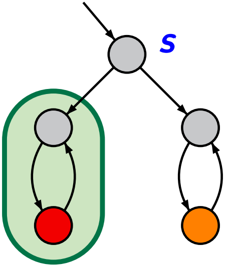
$\widehat{=}\ \{b\}$

nontrivial **SCC** $C$ of $G_a$ with $C \cap Sat(c) \neq \varnothing$

# Strong fairness: 1 fairness requirement

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

digraph $G_a$




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

$\bigcirc \mathrel{\widehat{=}} \varnothing$

$\bigcirc \mathrel{\widehat{=}} \{c\}$

$\bigcirc \mathrel{\widehat{=}} \{b\}$

$\uparrow$

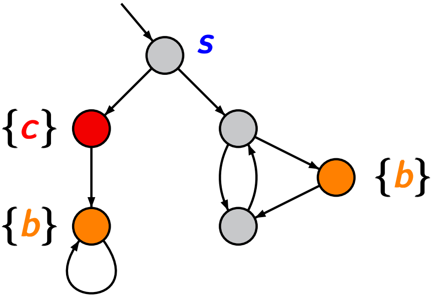
nontrivial SCC $C$ of $G_a$ with $C \cap Sat(c) \neq \varnothing$

# Strong fairness: 1 fairness requirement



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

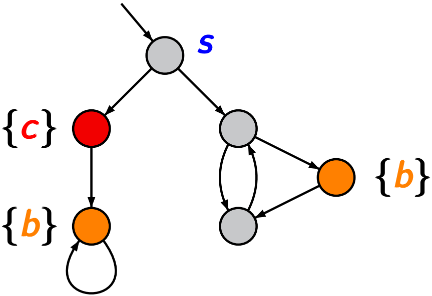
digraph $G_a$



# Strong fairness: 1 fairness requirement

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

digraph $G_a$

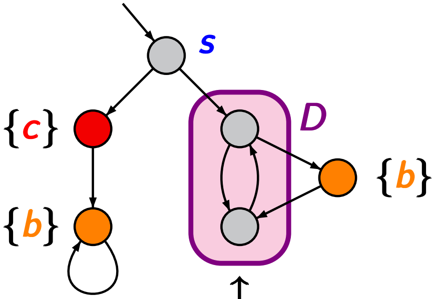



$\longleftarrow$ $s \models_{fair} \exists\Box a$

# Strong fairness: 1 fairness requirement

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

digraph $G_a$



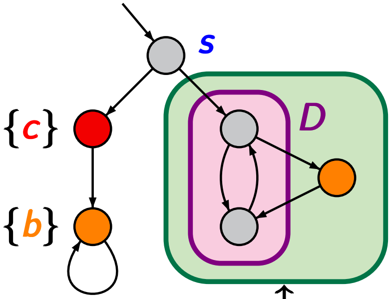

$s \models_{fair} \exists\Box a$

strongly connected node-set $D$ of $G_a$ with
$D \cap Sat(b) = \varnothing$

# Strong fairness: 1 fairness requirement

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

digraph $G_a$




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

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

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

*here:* explanations only for strong fairness

*case 1*: unconditional fairness $\surd$

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

*case 3:* arbitrary strong fairness assumption

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

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

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

# Example: 2 strong fairness conditions

# Example: 2 strong fairness conditions

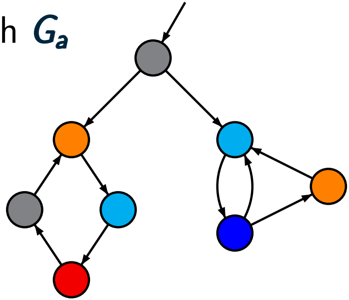


$$fair = (\Box\Diamond b_1 \rightarrow \Box\Diamond c_1) \ \wedge \ (\Box\Diamond b_2 \rightarrow \Box\Diamond c_2)$$

# Example: 2 strong fairness conditions

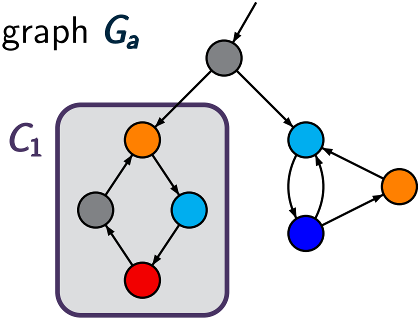
$$fair = (\Box\Diamond b_1 \to \Box\Diamond c_1) \wedge (\Box\Diamond b_2 \to \Box\Diamond c_2)$$

digraph $G_a$



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

digraph $G_a$

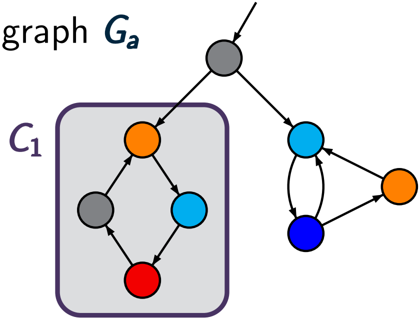



first SCC: $C_1 \cap Sat(c_2) = \varnothing$

# Example: 2 strong fairness conditions 

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

digraph $G_a$




first SCC: $C_1 \cap Sat(c_2) = \varnothing$

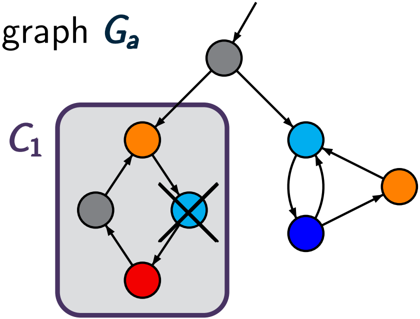
analyze $C_1 \setminus Sat(b_2)$ w.r.t. $\Box\Diamond b_1 \rightarrow \Box\Diamond c_1$

# Example: 2 strong fairness conditions



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

digraph $G_a$




first SCC: $C_1 \cap Sat(c_2) = \varnothing$

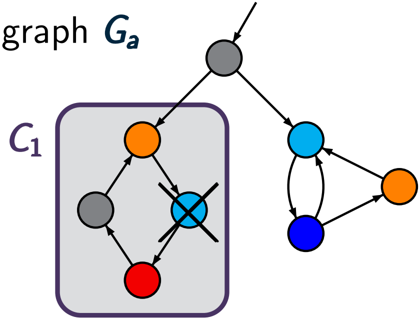
analyze $C_1 \setminus Sat(b_2)$ w.r.t. $\Box\Diamond b_1 \rightarrow \Box\Diamond c_1$

# Example: 2 strong fairness conditions



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

digraph $G_a$




first SCC: $C_1 \cap Sat(c_2) = \varnothing$

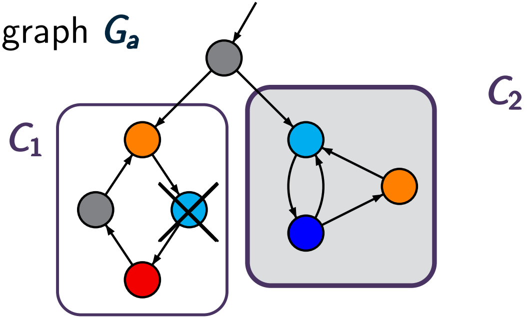
analyze $C_1 \setminus Sat(b_2)$ w.r.t. $\Box\Diamond b_1 \rightarrow \Box\Diamond c_1$

$\rightsquigarrow$ there is no cycle

# Example: 2 strong fairness conditions 

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

digraph $G_a$

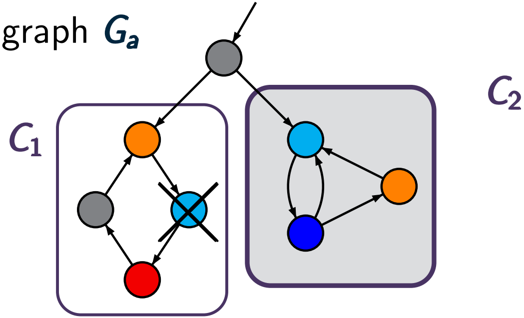



second SCC:

# Example: 2 strong fairness conditions

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

digraph $G_a$



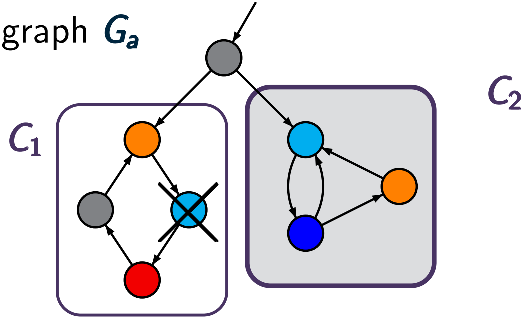

second SCC: $C_2 \cap Sat(c_1) = \varnothing$

# Example: 2 strong fairness conditions



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

digraph $G_a$




second SCC: $C_2 \cap Sat(c_1) = \varnothing$

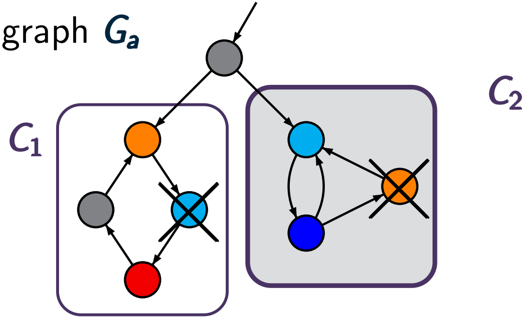
analyze $C_2 \setminus Sat(b_1)$ w.r.t. $\Box\Diamond b_2 \rightarrow \Box\Diamond c_2$

# Example: 2 strong fairness conditions



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

digraph $G_a$



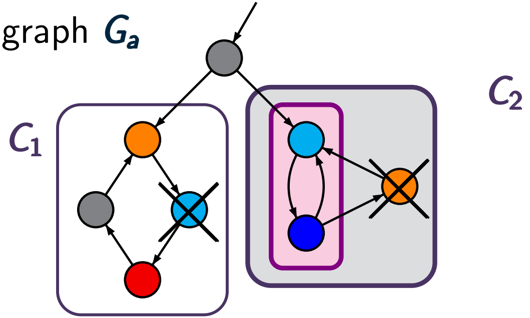

second SCC: $C_2 \cap Sat(c_1) = \varnothing$

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

# Example: 2 strong fairness conditions

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

digraph $G_a$



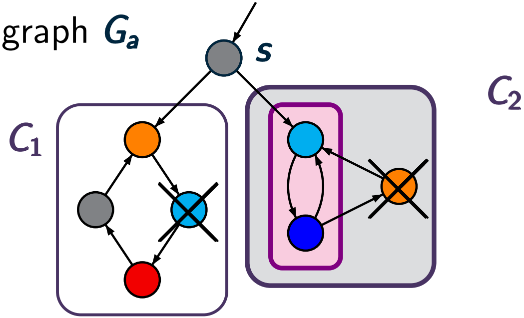

second SCC: $C_2 \cap Sat(c_1) = \varnothing$

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

# Example: 2 strong fairness conditions

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

digraph $G_a$




second SCC: $C_2 \cap Sat(c_1) = \varnothing$

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

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

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

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



compute the SCCs of the digraph $G_a$;

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



compute the SCCs of the digraph $G_a$;

$T := \varnothing$;

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



compute the SCCs of the digraph $G_a$;

$T := \varnothing$;

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

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



compute the SCCs of the digraph $G_a$;

$T := \varnothing$;

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

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

OD

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



```
compute the SCCs of the digraph G_a;
T := ∅;
FOR ALL nontrivial SCCs C of G_a DO
   IF CheckFair(C, ...) THEN T := T ∪ C FI
OD
Sat_fair(∃□a) := {s ∈ S : Reach_{G_a}(s) ∩ T ≠ ∅}
```

compute the SCCs of the digraph $G_a$;

$T := \varnothing$;

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

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

OD

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

↑ backward search from $T$

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

```
compute the SCCs of the digraph G_a;
T := ∅;
FOR ALL nontrivial SCCs C of G_a DO
  IF CheckFair(C, ...) THEN T := T ∪ C FI
OD
```

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

↑ backward search from $T$

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

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



compute the SCCs of the digraph $G_a$;

$T := \varnothing$;

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

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

OD

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

backward search from $T$

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

# Recursive algorithm *CheckFair*(...)

# Recursive algorithm *CheckFair*(...) 

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

# Recursive algorithm *CheckFair*(...)

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

"true" if there exists a cyclic path fragment $s_0\, s_1 \ldots s_n$ in $C$ such that

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

"false" otherwise

# Recursive algorithm *CheckFair*(...)



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

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

# Recursive algorithm $CheckFair(\ldots)$



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

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

choose $j \in \{1, ..., k\}$ with $C \cap Sat(c_j) = \varnothing$;

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

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

choose $j \in \{1, ..., k\}$ with $C \cap Sat(c_j) = \varnothing$;

remove all states in $Sat(b_j)$;

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

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

choose $j \in \{1, ..., k\}$ with $C \cap Sat(c_j) = \varnothing$;

remove all states in $Sat(b_j)$;

IF the resulting graph $G$ is acyclic THEN return "false" FI pseudo code for $CheckFair(C, k, \bigwedge_{1 \leq i \leq k} (\Box\Diamond b_i \rightarrow \Box\Diamond c_i))$

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

choose $j \in \{1, ..., k\}$ with $C \cap Sat(c_j) = \varnothing$;

remove all states in $Sat(b_j)$;

IF the resulting graph $G$ is acyclic THEN return "false" FI

FOR ALL nontrivial **SCCs** $D$ of $G$ DO

OD

# Recursive algorithm *CheckFair*(...)

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

```
IF ∀i ∈ {1, ..., k}. C ∩ Sat(c_i) ≠ ∅ THEN return "true" FI
choose j ∈ {1, ..., k} with C ∩ Sat(c_j) = ∅;
remove all states in 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, ⋀_{i≠j} (□◊b_i → □◊c_i))
   THEN return "true"   FI
OD
```

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

```
IF ∀i ∈ {1,...,k}. C ∩ Sat(c_i) ≠ ∅ THEN return "true" FI
choose j ∈ {1,...,k} with C ∩ Sat(c_j) = ∅;
remove all states in 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, ⋀_{i≠j} (□◊b_i → □◊c_i))
   THEN return "true"  FI
OD
return "false"
```

# Complexity of *CheckFair*(...)

# Complexity of *CheckFair*(...)



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

```
IF ∀i ∈ {1,...,k}. C ∩ Sat(c_i) ≠ ∅ THEN return "true" FI
choose j ∈ {1,...,k} with C ∩ Sat(c_j) = ∅;
remove all states in 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, ⋀_{i≠j}(□◇b_i → □◇c_i))
   THEN return "true"

OD
return "false"
```

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

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

choose $j \in \{1, ..., k\}$ with $C \cap Sat(c_j) = \varnothing$;

remove all states in $Sat(b_j)$;

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:

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

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

```
IF ∀i ∈ {1,...,k}. C ∩ Sat(c_i) ≠ ∅ THEN return "true" FI
choose j ∈ {1,...,k} with C ∩ Sat(c_j) = ∅;
remove all states in 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, ⋀_{i≠j} (□◊b_i → □◊c_i))
   THEN return "true"
OD
return "false"
```

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

# CTL model checking with fairness



| | |
|---|---|
| *input*: | finite transition system $\mathcal{T}$ |
| | CTL fairness assumption ***fair*** |
| | CTL formula $\Phi$ |
| *output*: | "**yes**", if $\mathcal{T} \models_{fair} \Phi$. "**no**" otherwise. |

| | |
|---|---|
| *input*: | finite transition system $\mathcal{T}$ |
| | CTL fairness assumption ***fair*** |
| | CTL formula $\Phi$ |
| *output*: | "**yes**", if $\mathcal{T} \models_{fair} \Phi$. "**no**" otherwise. |

*here: preprocessing*

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

# CTL model checking with fairness

| | |
|---|---|
| *input*: | finite transition system $\mathcal{T}$ |
| | CTL fairness assumption *fair* |
| | CTL formula $\Phi$ |
| *output*: | "**yes**", if $\mathcal{T} \models_{fair} \Phi$. "**no**" otherwise. |

*here: preprocessing*

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

↑

i.e., with the basic modalities $\exists\bigcirc$, $\exists\mathsf{U}$ and $\exists\Box$

# Model checking algorithm for FairCTL

# Model checking algorithm for FairCTL

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

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

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

OD

# Model checking algorithm for FairCTL



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:

$$\vdots$$

$$\begin{array}{rcrcl}
\exists\bigcirc a & : & Sat_{fair}(\Psi) & := & Sat(\exists\bigcirc(a \wedge a_{fair})); \\
\exists(a_1 \,\mathsf{U}\, a_2) & : & Sat_{fair}(\Psi) & := & Sat(\exists(a_1 \,\mathsf{U}(a_2 \wedge a_{fair}))); \\
\exists\Box a & : & Sat_{fair}(\Psi) & := & \ldots
\end{array}$$

OD

# Model checking algorithm for FairCTL

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:

⋮

$$\begin{array}{rcll}
\exists\bigcirc a & : & Sat_{fair}(\Psi) & := & Sat(\exists\bigcirc(a \wedge a_{fair})); \\
\exists(a_1 \,\mathsf{U}\, a_2) & : & Sat_{fair}(\Psi) & := & Sat(\exists(a_1 \,\mathsf{U}(a_2 \wedge a_{fair}))); \\
\exists\Box a & : & Sat_{fair}(\Psi) & := & \ldots
\end{array}$$

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:

⋮

$$\begin{array}{rcll}
\exists\bigcirc a & : & Sat_{fair}(\Psi) := & Sat(\exists\bigcirc(a \wedge a_{fair})); \\
\exists(a_1 \mathsf{U} a_2) & : & Sat_{fair}(\Psi) := & Sat(\exists(a_1 \mathsf{U}(a_2 \wedge a_{fair}))); \\
\exists\Box a & : & Sat_{fair}(\Psi) := & \ldots
\end{array}$$

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

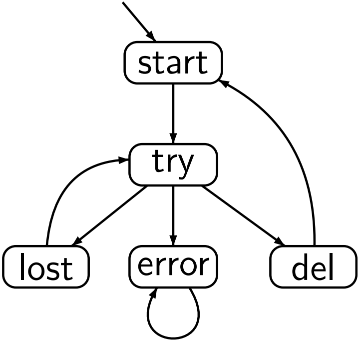
OD

IF $S_0 \subseteq Sat_{fair}(\Phi)$ THEN return "**yes**"

ELSE return "**no**"

FI

# Example: CTL model checking with fairness

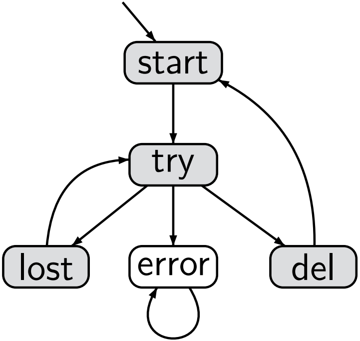



$fair = \Box\Diamond\ \exists\Diamond del$

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

# Example: CTL model checking with fairness

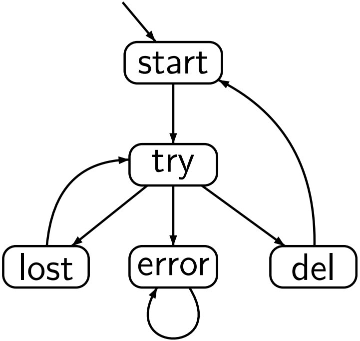





$$\Phi = \exists\Diamond\, \forall\bigcirc(\mathit{lost} \vee \mathit{del})$$

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

# Example: CTL model checking with fairness

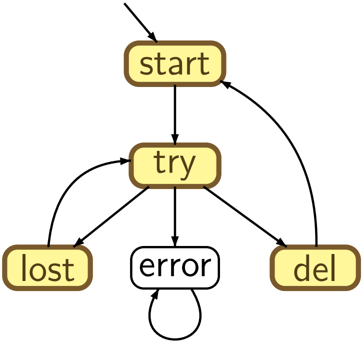



$$\Phi = \exists\lozenge\ \forall\bigcirc(lost \vee del)$$

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

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

# Example: CTL model checking with fairness

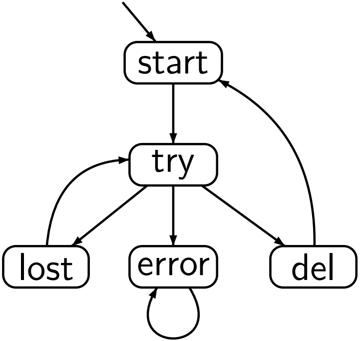



$\Phi = \exists\Diamond\ \forall\bigcirc(lost \vee del)$

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

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

# Example: CTL model checking with fairness 




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

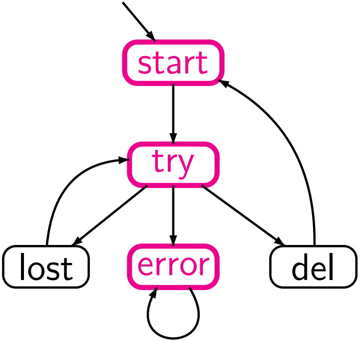
$$\equiv \exists\Diamond\ \neg\exists\bigcirc(\neg lost \wedge \neg del)$$

existential normal form

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

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

# Example: CTL model checking with fairness 




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

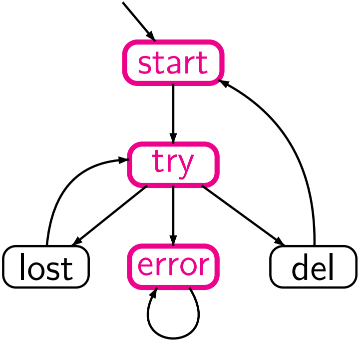
$\equiv \exists\Diamond\neg\exists\bigcirc\ (\neg lost \wedge \neg del)$

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

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

# Example: CTL model checking with fairness





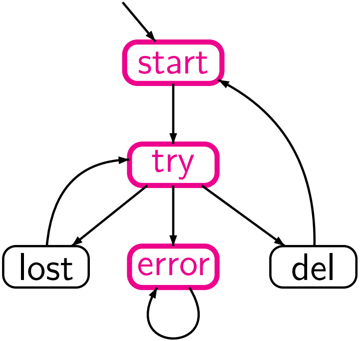

$$\Phi = \exists\Diamond\ \forall\bigcirc(lost \vee del)$$

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

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

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

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




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

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

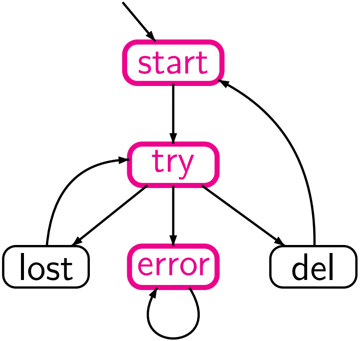
$$\rightsquigarrow \exists\Diamond\neg\boxed{\exists\bigcirc a}$$

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

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

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

# Example: CTL model checking with fairness 



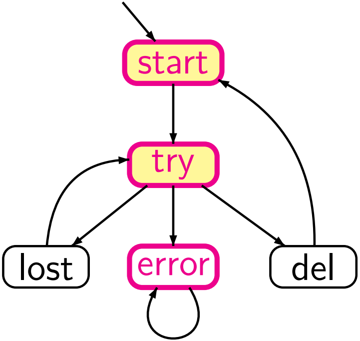

$$\Phi = \exists\Diamond\ \forall\bigcirc(lost \vee del)$$
$$\equiv \exists\Diamond\neg\exists\bigcirc\ (\neg lost \wedge \neg del)$$
$$\rightsquigarrow \exists\Diamond\neg\boxed{\exists\bigcirc a}$$

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

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

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

# Example: CTL model checking with fairness 




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

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

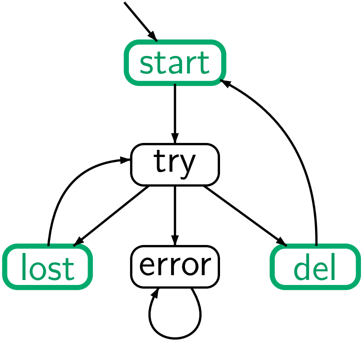
$$\rightsquigarrow \exists\Diamond\neg\boxed{\exists\bigcirc a}$$

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

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

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

# Example: CTL model checking with fairness




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

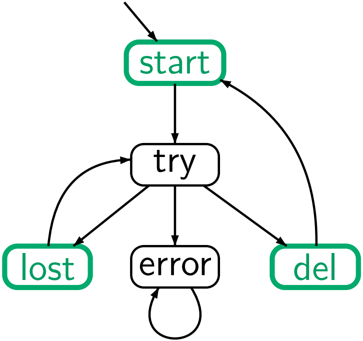
$$\equiv \exists\Diamond\neg\exists\bigcirc\ (\neg lost \wedge \neg del)$$

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

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

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

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




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

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

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

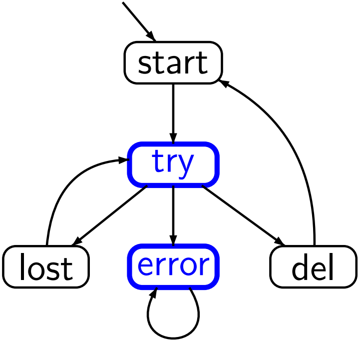
$\mathit{fair} = \Box\Diamond\ \exists\Diamond\mathit{del} \ \rightsquigarrow \Box\Diamond c$ where $\mathit{Sat}(c) = S \setminus \{\mathit{error}\}$

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

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

$\mathit{Sat}_{\mathit{fair}}(\neg\exists\bigcirc a)$

# Example: CTL model checking with fairness




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

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

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

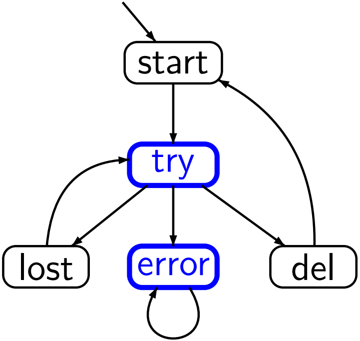
$fair = \Box\Diamond\ \exists\Diamond del \ \rightsquigarrow \Box\Diamond c$ where $Sat(c) = S \setminus \{error\}$

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

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

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

# Example: CTL model checking with fairness




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

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

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

$$\rightsquigarrow\ \exists\Diamond b$$

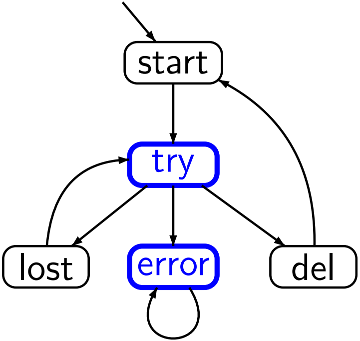
$fair = \Box\Diamond\ \exists\Diamond del\ \ \rightsquigarrow\ \Box\Diamond c$ where $Sat(c) = S \setminus \{error\}$

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

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

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

# Example: CTL model checking with fairness




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

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

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

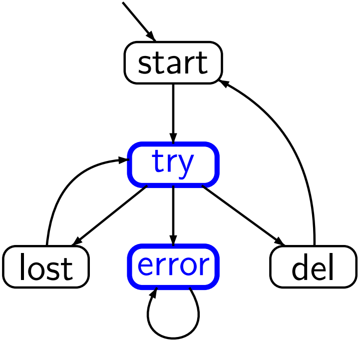
$$\rightsquigarrow \exists\Diamond b$$

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

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

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

# Example: CTL model checking with fairness 




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

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

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

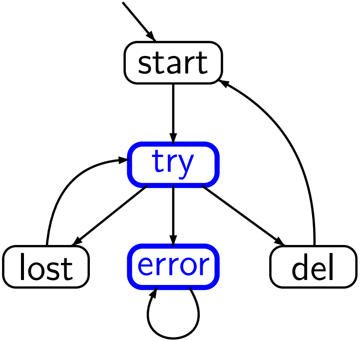
$$\rightsquigarrow \exists\Diamond b$$

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

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

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

# Example: CTL model checking with fairness




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

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

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

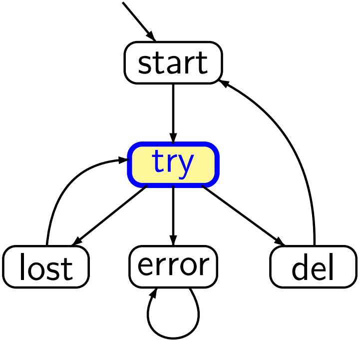
$$\rightsquigarrow \exists\Diamond b$$

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

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

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

# Example: CTL model checking with fairness




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

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

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

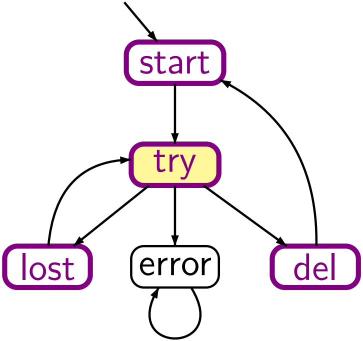
$$\rightsquigarrow \exists\Diamond b$$

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

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

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

# Example: CTL model checking with fairness




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

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

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

$$\rightsquigarrow \exists\Diamond b$$

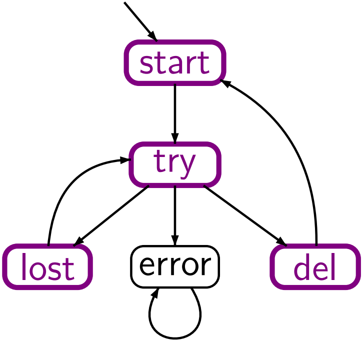
$fair = \Box\Diamond\ \exists\Diamond del \ \rightsquigarrow \Box\Diamond c$ where $Sat(c) = S \setminus \{error\}$

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

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

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

# Example: CTL model checking with fairness




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

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

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

$$\rightsquigarrow\ \exists\Diamond b$$

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

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

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

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

# Correct or wrong?

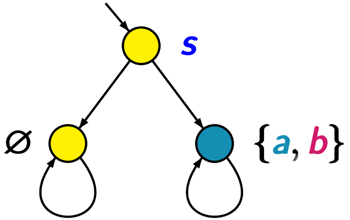


$$s \models_{fair} \forall\bigcirc a \quad \text{iff} \quad s \models \forall\bigcirc(a \wedge a_{fair})$$

# Correct or wrong?

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

**wrong.**

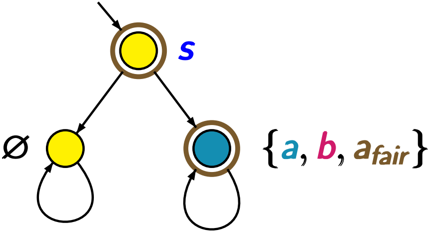



$fair = \Box \Diamond b$

# Correct or wrong? 

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

**wrong.**



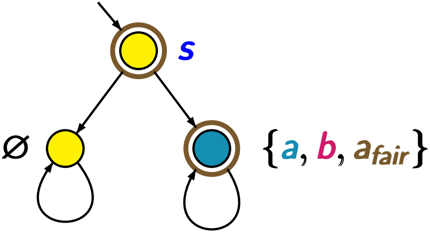

$fair = \Box\Diamond b$

# Correct or wrong?



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

**wrong.**

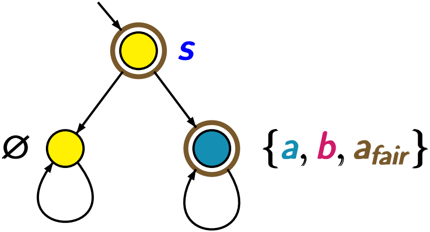



$fair = \Box\Diamond b$

$s \not\models \forall\bigcirc(a \wedge a_{fair})$

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

**wrong.**



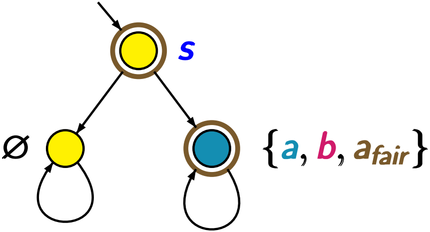

$fair = \Box\Diamond b$

$s \not\models \forall\bigcirc(a \wedge a_{fair})$

$s \models_{fair} \forall\bigcirc a$

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

**wrong.**




$fair = \Box \Diamond b$

$s \not\models \forall \bigcirc (a \wedge a_{fair})$

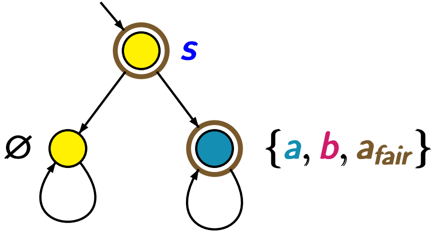
$s \models_{fair} \forall \bigcirc a$

but correct is:

$$s \models_{fair} \forall \bigcirc a \quad \text{iff} \quad ?$$

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

**wrong.**




$fair = \Box\Diamond b$

$s \not\models \forall\bigcirc(a \wedge a_{fair})$

$s \models_{fair} \forall\bigcirc a$

but correct is:

$$s \models_{fair} \forall\bigcirc a \quad \text{iff} \quad s \models \forall\bigcirc(a_{fair} \rightarrow a)$$

# Correct or wrong?



$s \models_{fair} \forall\Box a$ iff $s \models \forall\Box(a_{fair} \rightarrow a)$

# Correct or wrong?



$$s \models_{fair} \forall\Box a \quad \text{iff} \quad s \models \forall\Box(a_{fair} \rightarrow a)$$

iff there is no state $s'$ reachable from $s$ with $s' \models \neg a \wedge a_{fair}$

# Correct or wrong?



$s \models_{fair} \forall\Box a$ iff $s \models \forall\Box(a_{fair} \rightarrow a)$

iff there is no state $s'$ reachable from $s$ with $s' \models \neg a \wedge a_{fair}$

**correct**

# Correct or wrong?



$s \models_{fair} \forall\Box a$ iff $s \models \forall\Box(a_{fair} \rightarrow a)$

iff there is no state $s'$ reachable from $s$ with $s' \models \neg a \wedge a_{fair}$

**correct**

$s \models_{fair} \forall\Box a$

$s \models_{fair} \forall\Box a$ iff $s \models \forall\Box(a_{fair} \rightarrow a)$

iff there is no state $s'$ reachable from $s$ with $s' \models \neg a \wedge a_{fair}$

**correct**

$s \models_{fair} \forall\Box a$ iff $s \models_{fair} \neg\exists\Diamond\neg a$

$$s \models_{fair} \forall\Box a \quad \text{iff} \quad s \models \forall\Box(a_{fair} \rightarrow a)$$

iff there is no state $s'$ reachable from $s$ with $s' \models \neg a \wedge a_{fair}$

**correct**

$$s \models_{fair} \forall\Box a \quad \text{iff} \quad s \models_{fair} \neg\exists\Diamond\neg a$$

$$\text{iff} \quad s \not\models_{fair} \exists\Diamond\neg a$$

# Correct or wrong?



$s \models_{fair} \forall\Box a$ iff $s \models \forall\Box(a_{fair} \rightarrow a)$

iff there is no state $s'$ reachable from $s$ with $s' \models \neg a \wedge a_{fair}$

**correct**

$s \models_{fair} \forall\Box a$ iff $s \models_{fair} \neg\exists\Diamond\neg a$

iff $s \not\models_{fair} \exists\Diamond\neg a$

iff $s \not\models \exists\Diamond(\neg a \wedge a_{fair})$

$s \models_{fair} \forall\Box a$ iff $s \models \forall\Box(a_{fair} \rightarrow a)$

iff there is no state $s'$ reachable from $s$ with $s' \models \neg a \wedge a_{fair}$

**correct**

$$
\begin{aligned}
s \models_{fair} \forall\Box a \quad & \text{iff} \quad s \models_{fair} \neg\exists\Diamond\neg a \\
& \text{iff} \quad s \not\models_{fair} \exists\Diamond\neg a \\
& \text{iff} \quad s \not\models \exists\Diamond(\neg a \wedge a_{fair}) \\
& \text{iff} \quad s \models \neg\exists\Diamond(\neg a \wedge a_{fair})
\end{aligned}
$$

$s \models_{fair} \forall\Box a$ iff $s \models \forall\Box(a_{fair} \rightarrow a)$

iff there is no state $s'$ reachable from $s$ with $s' \models \neg a \wedge a_{fair}$

**correct**

$$s \models_{fair} \forall\Box a \text{ iff } s \models_{fair} \neg\exists\Diamond\neg a$$
$$\text{iff } s \not\models_{fair} \exists\Diamond\neg a$$
$$\text{iff } s \not\models \exists\Diamond(\neg a \wedge a_{fair})$$
$$\text{iff } s \models \neg\exists\Diamond(\neg a \wedge a_{fair}) \equiv \forall\Box(a_{fair} \rightarrow a)$$

# Summary



We just saw:

$$s \models_{fair} \forall \bigcirc a \quad \text{iff} \quad s \models \forall \bigcirc (a_{fair} \to a)$$

$$s \models_{fair} \forall \Box a \quad \text{iff} \quad s \models \forall \Box (a_{fair} \to a)$$

We just saw:

$$s \models_{fair} \forall \bigcirc a \quad \text{iff} \quad s \models \forall \bigcirc (a_{fair} \rightarrow a)$$

$$s \models_{fair} \forall \Box a \quad \text{iff} \quad s \models \forall \Box (a_{fair} \rightarrow a)$$

Is the following statement correct **?**

$$s \models_{fair} \forall (b \, \mathsf{U} \, a) \quad \text{iff} \quad s \models \forall \big(b \, \mathsf{U} (a_{fair} \rightarrow a)\big)$$

We just saw:

$$s \models_{fair} \forall\bigcirc a \quad \text{iff} \quad s \models \forall\bigcirc(a_{fair} \to a)$$

$$s \models_{fair} \forall\Box a \quad \text{iff} \quad s \models \forall\Box(a_{fair} \to a)$$

Is the following statement correct **?**

$$s \models_{fair} \forall(b \,\mathsf{U}\, a) \quad \text{iff} \quad s \models \forall\big(b \,\mathsf{U}(a_{fair} \to a)\big)$$

**wrong**.

# Correct or wrong?

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

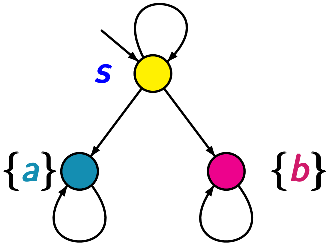
# Correct or wrong?



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

**wrong.**

$fair = \Box\Diamond b$



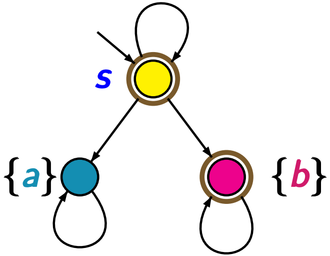
# Correct or wrong?



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

**wrong.**

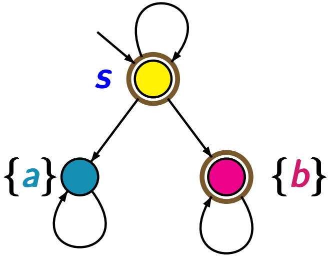
$fair = \Box\Diamond b$



# Correct or wrong?

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

**wrong.**

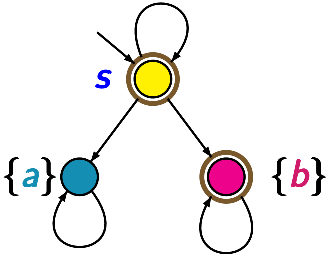



$fair = \Box\Diamond b$

$s \models \exists\bigcirc(\,(\exists\Diamond a) \wedge a_{fair})$

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

**wrong.**



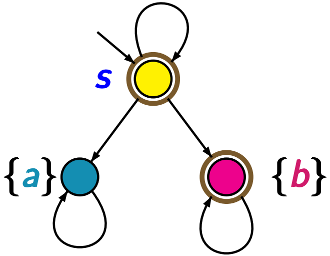

$fair = \Box\Diamond b$

$s \models \exists\bigcirc(\,(\exists\Diamond a) \wedge a_{fair}\,)$

regard $s \rightarrow s$

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

**wrong.**




$fair = \Box\Diamond b$

$s \models \exists\bigcirc\big((\exists\Diamond a) \wedge a_{fair}\big)$

regard $s \rightarrow s$

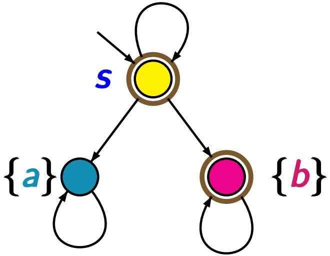
$s \not\models_{fair} \exists\bigcirc\exists\Diamond a$

# Correct or wrong?



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

**wrong.**




$fair = \Box\Diamond b$

$s \models \exists\bigcirc(\,(\exists\Diamond a) \wedge a_{fair}\,)$

regard $s \to s$

$s \not\models_{fair} \exists\bigcirc\exists\Diamond a$

(note $Sat_{fair}(\exists\Diamond a) = \varnothing$)

# Correct or wrong?

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

**wrong.**

$$s \models_{fair} \exists(a \, \mathsf{W} \, c) \quad \text{iff} \quad s \models \exists(a \, \mathsf{W}(c \wedge a_{fair}))$$

remind: $\mathsf{W}$ = weak until

# Correct or wrong?



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

**wrong.**

$$s \models_{fair} \exists(a \, \mathsf{W} \, c) \quad \text{iff} \quad s \models \exists(a \, \mathsf{W}(c \wedge a_{fair}))$$

remind: $\mathsf{W}$ = weak until

**wrong.**

# Correct or wrong?



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

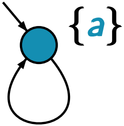
**wrong.**

$$s \models_{fair} \exists(a\,\mathsf{W}\,c) \quad \text{iff} \quad s \models \exists(a\,\mathsf{W}(c \wedge a_{fair}))$$

remind: **W** = weak until

**wrong.**

$fair = \Box\Diamond b$



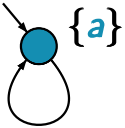
$$s \models_{fair} \exists\bigcirc\exists\lozenge a \quad \text{iff} \quad s \models \exists\bigcirc((\exists\lozenge a) \wedge a_{fair})$$

**wrong.**

$$s \models_{fair} \exists(a \,\mathsf{W}\, c) \quad \text{iff} \quad s \models \exists(a \,\mathsf{W}(c \wedge a_{fair}))$$

remind: **W** = weak until

**wrong.**




$fair = \Box\lozenge b$

$s \models \exists(a \,\mathsf{W}(c \wedge a_{fair}))$

# Correct or wrong? 

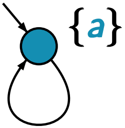
$$s \models_{fair} \exists\bigcirc\exists\Diamond a \quad \text{iff} \quad s \models \exists\bigcirc((\exists\Diamond a) \wedge a_{fair})$$

**wrong.**

$$s \models_{fair} \exists(a \, \mathsf{W} \, c) \quad \text{iff} \quad s \models \exists(a \, \mathsf{W}(c \wedge a_{fair}))$$

remind: **W** = weak until

**wrong.**




$fair = \Box\Diamond b$

$s \models \exists(a \, \mathsf{W}(c \wedge a_{fair}))$

$s \not\models_{fair} \exists(a \, \mathsf{W} \, c)$

# Summary: fairness in CTL

# Summary: fairness in CTL

**CTL** fairness assumptions: formulas similar to **LTL**

e.g., $fair = \bigwedge_{1 \leq i \leq k} (\Box\Diamond\Psi_i \to \Box\Diamond\Phi_i)$

**CTL** fairness assumptions: formulas similar to **LTL**

e.g., $fair = \bigwedge_{1 \leq i \leq k} (\Box\Diamond\Psi_i \rightarrow \Box\Diamond\Phi_i)$

**CTL** satisfaction relation with fairness:

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

**CTL** fairness assumptions: formulas similar to **LTL**

e.g., $fair = \bigwedge_{1 \leq i \leq k} (\Box\Diamond\Psi_i \rightarrow \Box\Diamond\Phi_i)$

**CTL** satisfaction relation with fairness:

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

model checking for **CTL** with fairness:

# Summary: fairness in CTL

**CTL** fairness assumptions: formulas similar to **LTL**

e.g., $fair = \bigwedge_{1 \leq i \leq k} (\Box\Diamond\Psi_i \rightarrow \Box\Diamond\Phi_i)$

**CTL** satisfaction relation with fairness:

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

model checking for **CTL** with fairness:

- $\exists\bigcirc$, $\exists$**U**, $\forall\bigcirc$, $\forall\Box$ via **CTL** model checker

# Summary: fairness in CTL

**CTL** fairness assumptions: formulas similar to **LTL**

e.g., $\mathit{fair} = \bigwedge_{1 \leq i \leq k} (\Box\Diamond\Psi_i \rightarrow \Box\Diamond\Phi_i)$

**CTL** satisfaction relation with fairness:

$s \models_{\mathit{fair}} \exists\varphi$ iff there exists $\pi \in \mathit{Paths}(s)$ with $\pi \models \mathit{fair}$ 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**

e.g., $fair = \bigwedge_{1 \le i \le k} (\Box\Diamond\Psi_i \rightarrow \Box\Diamond\Phi_i)$

**CTL** satisfaction relation with fairness:

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

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