

Introduction

Modelling parallel systems

Linear Time Properties

Regular Properties

Linear Temporal Logic (LTL)

Computation Tree Logic

syntax and semantics of CTL

expressiveness of CTL and LTL

CTL model checking

CTL with fairness



counterexamples/witnesses, CTL⁺ and CTL*

Equivalences and Abstraction

Complexity of CTL and LTL model checking

CTLFAIR4.4-1

LTL model checking problem:

PSPACE-complete and solvable in time

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

CTL model checking problem:

solvable in polynomial time

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

LTL model checking problem:

PSPACE-complete and solvable in time

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

CTL model checking problem:

solvable in polynomial time (even PTIME-complete)

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

LTL model checking problem:

PSPACE-complete and solvable in time

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

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

CTL model checking problem:

solvable in polynomial time (even PTIME-complete)

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

LTL model checking problem:

PSPACE-complete and solvable in time

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

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

CTL model checking problem:

solvable in polynomial time (even PTIME-complete)

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

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

Recall: LTL fairness assumptions

CTLFAIR4.4-2

Recall: LTL fairness assumptions

CTLFAIR4.4-2

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

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

where ϕ, ψ are propositional formulas

Recall: LTL fairness assumptions

CTLFAIR4.4-2

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

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

where ϕ, ψ are propositional formulas

Recall: LTL fairness assumptions

CTLFAIR4.4-2

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

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

where ϕ, ψ are propositional formulas

Reduction of \models_{fair} to \models

Recall: LTL fairness assumptions

CTLFAIR4.4-2

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

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

where ϕ, ψ are propositional formulas

Reduction of \models_{fair} to \models

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

Recall: LTL fairness assumptions

CTLFAIR4.4-2

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

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

where ϕ, ψ are propositional formulas

Reduction of \models_{fair} to \models

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

Recall: LTL fairness assumptions

CTLFAIR4.4-2

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

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

where ϕ, ψ are propositional formulas

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

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

Recall: LTL fairness assumptions

CTLFAIR4.4-2

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

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

where ϕ, ψ are propositional formulas

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

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

iff for all paths π in \mathcal{T} :

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

CTL fairness assumptions

CTL4.4-4A

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 Ψ , Φ are CTL state formulas

conjunctions of “formulas” of the type

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

where Ψ , Φ 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

CTL4.4-4A

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 Ψ , Φ are CTL state formulas

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

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

where Ψ_j , Φ_j are CTL state formulas

Satisfaction relation for CTL with fairness

CTLFAIR4.4-3

Satisfaction relation for CTL with fairness

CTLFAIR4.4-3

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

$s \models_{fair} a$ 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

CTLFAIR4.4-3

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

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

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

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

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

Satisfaction relation for CTL with fairness

CTLFAIR4.4-3

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

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

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

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

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

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

Satisfaction relation for CTL with fairness

CTLFAIR4.4-3

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

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

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

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

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

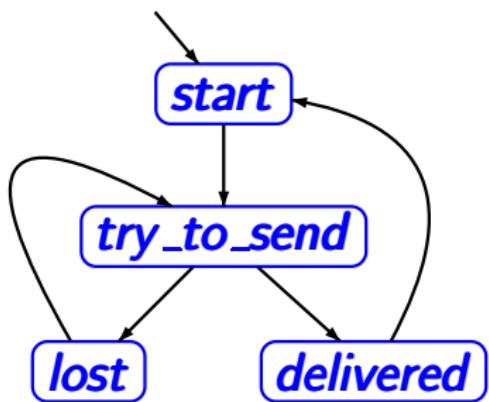
$s \models_{\text{fair}} \forall \varphi$ iff for all $\pi \in \text{Paths}(s)$:

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

e.g., $s_0 s_1 s_2 \dots \models \square \diamond \Phi$ iff $\exists^{\infty} i \geq 0$ s.t. $s_i \models \Phi$

Simple communication protocol

CTLFAIR4.4-5

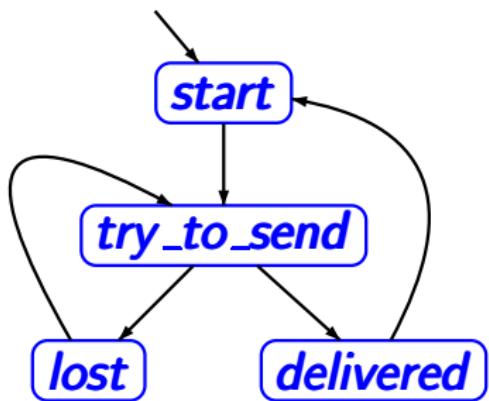


CTL formula

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

Simple communication protocol

CTLFAIR4.4-5



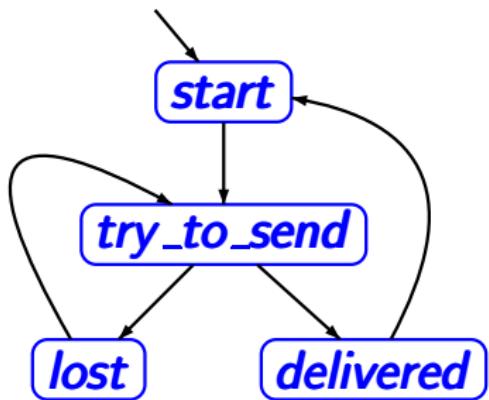
CTL formula

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

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

Simple communication protocol

CTLFAIR4.4-5



CTL formula

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

$$T \not\models \Phi$$

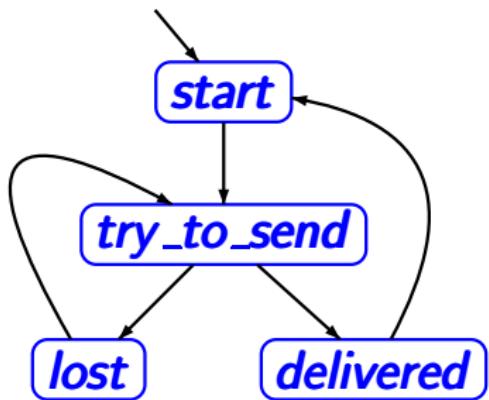
$$T \models_{ufair} \Phi$$

unconditional CTL fairness assumption:

$$ufair = \Box \Diamond \text{delivered}$$

Simple communication protocol

CTLFAIR4.4-5



CTL formula

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

$$T \not\models \Phi$$

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

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

unconditional CTL fairness assumption:

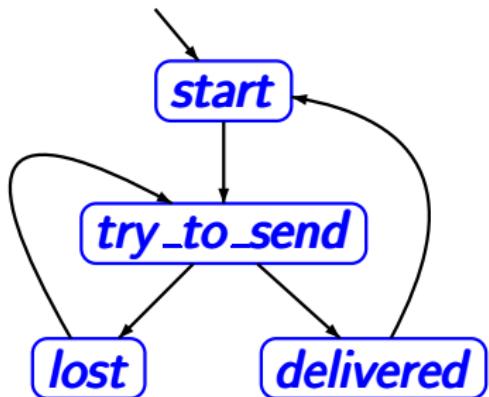
$$ufair = \Box \Diamond \text{delivered}$$

strong CTL fairness assumption:

$$sfair = \Box \Diamond \text{try_to_send} \rightarrow \Box \Diamond \text{delivered}$$

Simple communication protocol

CTLFAIR4.4-6



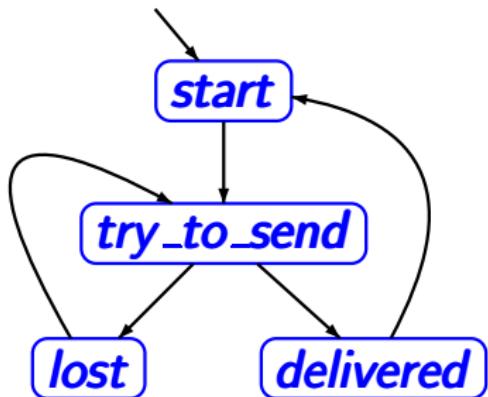
$$\Phi = \forall \Box \forall \Diamond \text{start}$$

$$T \models_{\text{ufair}} \Phi \quad ?$$

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

Simple communication protocol

CTLFAIR4.4-6



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

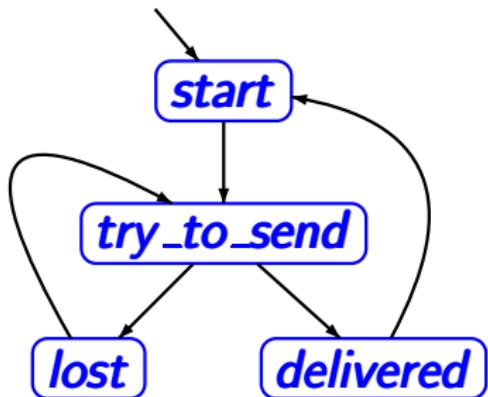
$$T \models_{ufair} \Phi \quad ?$$

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

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

Simple communication protocol

CTLFAIR4.4-6



$$\Phi = \forall \Box \forall \Diamond \text{start}$$
$$T \models_{ufair} \Phi \quad ?$$

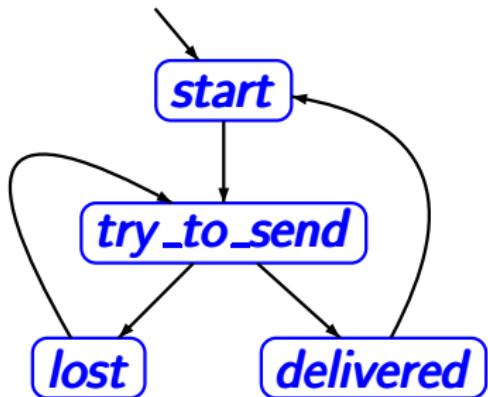
unconditional fairness: $ufair = \Box \Diamond \exists \bigcirc \text{start}$

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

$$ufair \triangleq \Box \Diamond \text{delivered}$$

Simple communication protocol

CTLFAIR4.4-6



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

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

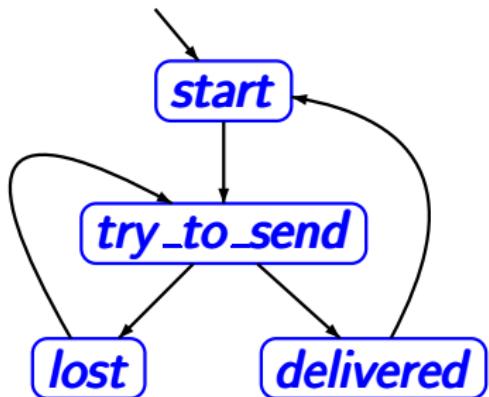
unconditional fairness: $ufair = \Box \Diamond \exists \bigcirc \text{start}$

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

$$ufair \triangleq \Box \Diamond \text{delivered}$$

Simple communication protocol

CTLFAIR4.4-6



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

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

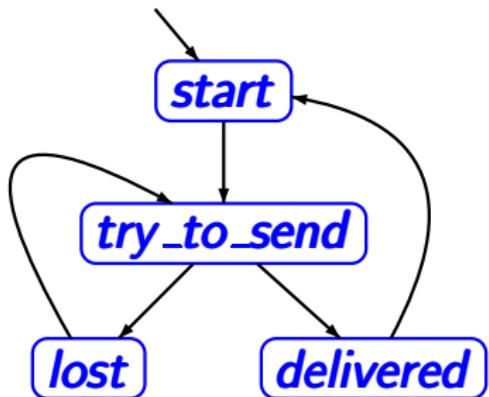
$$T \models_{\text{wfair}} \Phi \quad ?$$

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

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

Simple communication protocol

CTLFAIR4.4-6



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

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

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

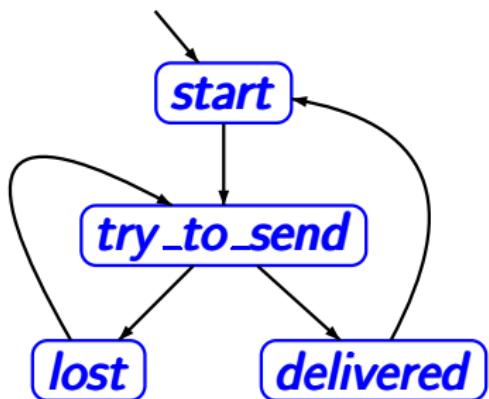
unconditional fairness: $ufair = \Box \Diamond \exists \bigcirc \text{start}$

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

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

Simple communication protocol

CTLFAIR4.4-6



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

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

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

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

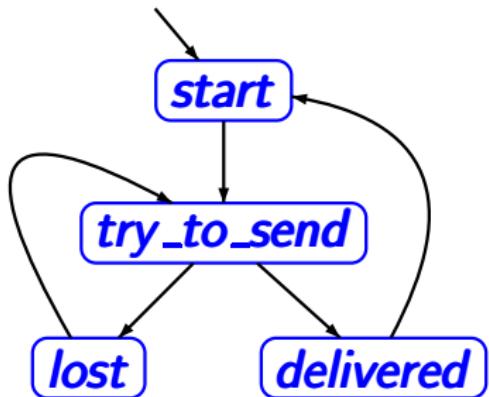
weak fairness: $\text{wfair} = \Diamond \Box \exists \Diamond \text{delivered} \rightarrow \Box \Diamond \text{delivered}$

$$\text{Sat}(\exists \Diamond \text{delivered}) = \{\text{try_to_send}\}$$

$$\text{wfair} \hat{=} \Diamond \Box \text{try_to_send} \rightarrow \Box \Diamond \text{delivered}$$

Simple communication protocol

CTLFAIR4.4-6



$$\Phi = \forall \Box A \Diamond start$$
$$T \models_{ufair} \Phi \quad \checkmark$$
$$T \models_{wfair} \Phi \quad \text{wrong}$$

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

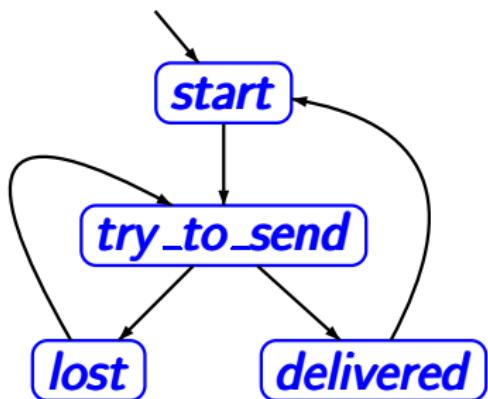
weak fairness: $wfair = \Diamond \Box \exists \bigcirc delivered \rightarrow \Box \Diamond delivered$

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

$$wfair \hat{=} \Diamond \Box try_to_send \rightarrow \Box \Diamond delivered$$

Simple communication protocol

CTLFAIR4.4-6



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

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

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

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

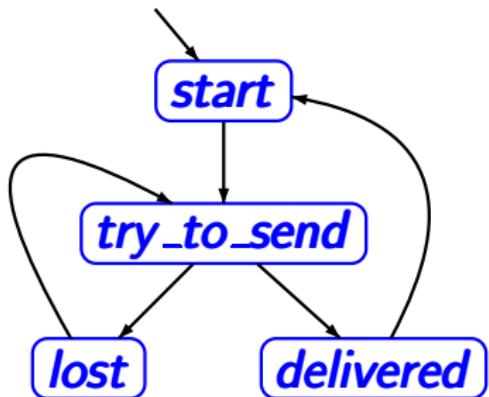
unconditional fairness: $ufair = \Box \Diamond \exists \Diamond \text{start}$

weak fairness: $wfair = \Diamond \Box \exists \Diamond \text{delivered} \rightarrow \Box \Diamond \text{delivered}$

strong fairness: $sfair = \Box \Diamond \exists \Diamond \text{delivered} \rightarrow \Box \Diamond \text{delivered}$

Simple communication protocol

CTLFAIR4.4-6



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

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

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

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

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

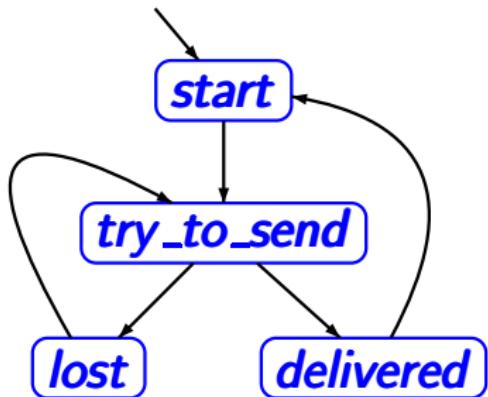
weak fairness: $wfair = \Diamond \Box \exists \Diamond \text{delivered} \rightarrow \Box \Diamond \text{delivered}$

strong fairness: $sfair = \Box \Diamond \exists \Diamond \text{delivered} \rightarrow \Box \Diamond \text{delivered}$

$$Sat(\exists \Diamond \text{delivered}) = \{\text{try_to_send}\}$$

Simple communication protocol

CTLFAIR4.4-6



$$\Phi = \Box \Diamond \text{start}$$

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

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

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

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

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

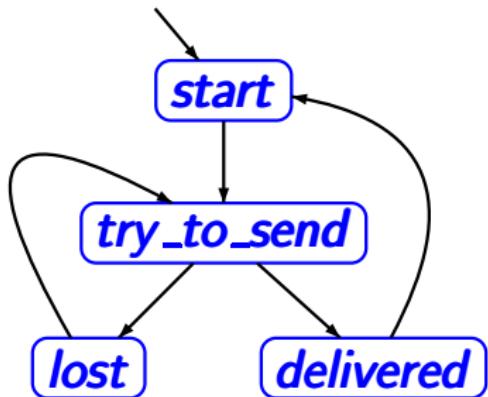
strong fairness: $sfair = \Box \Diamond \exists \bigcirc delivered \rightarrow \Box \Diamond delivered$

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

$$sfair \hat{=} \Box \Diamond try_to_send \rightarrow \Box \Diamond delivered$$

Simple communication protocol

CTLFAIR4.4-6



$$\Phi = \Box \Diamond \text{A} \Diamond \text{start}$$

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

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

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

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

weak fairness: $wfair = \Diamond \Box \exists \Diamond \text{delivered} \rightarrow \Box \Diamond \text{delivered}$

strong fairness: $sfair = \Box \Diamond \exists \Diamond \text{delivered} \rightarrow \Box \Diamond \text{delivered}$

$$Sat(\exists \Diamond \text{delivered}) = \{\text{try_to_send}\}$$

$$sfair \hat{=} \Box \Diamond \text{try_to_send} \rightarrow \Box \Diamond \text{delivered}$$

Correct or wrong?

CTLFAIR4.4-7

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

Correct or wrong?

CTLFAIR4.4-7

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

correct.

Correct or wrong?

CTLFAIR4.4-7

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

correct. Note that:

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

Correct or wrong?

CTLFAIR4.4-7

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

correct. Note that:

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

Correct or wrong?

CTLFAIR4.4-7

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

correct. Note that:

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

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

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

Correct or wrong?

CTLFAIR4.4-7

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

correct.

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

Correct or wrong?

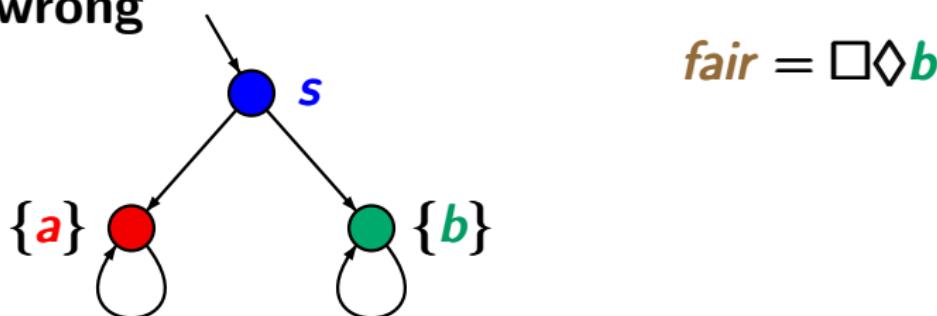
CTLFAIR4.4-7

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

correct.

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

wrong



Correct or wrong?

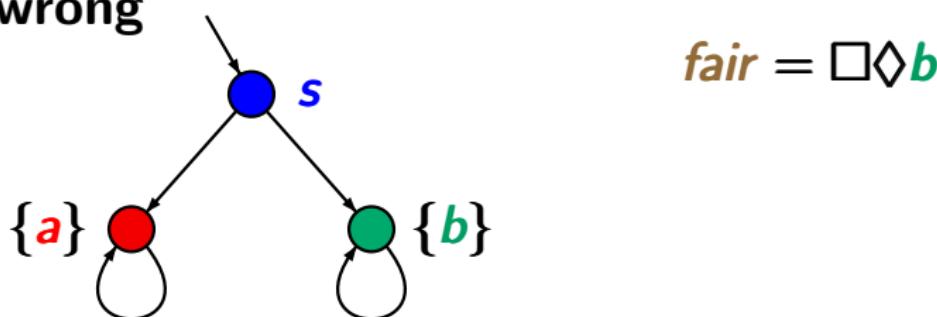
CTLFAIR4.4-7

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

correct.

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

wrong



$$fair = \Box \Diamond b$$

just one fair path



Correct or wrong?

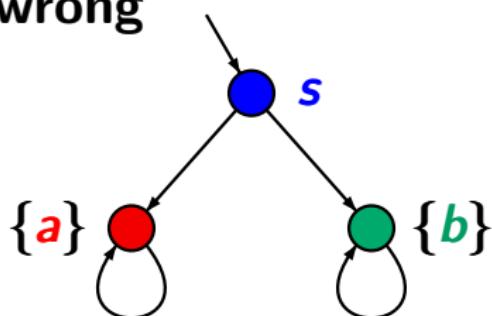
CTLFAIR4.4-7

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

correct.

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

wrong



$$fair = \Box \Diamond b$$

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

just one fair path ● ● ● ● ...

Correct or wrong?

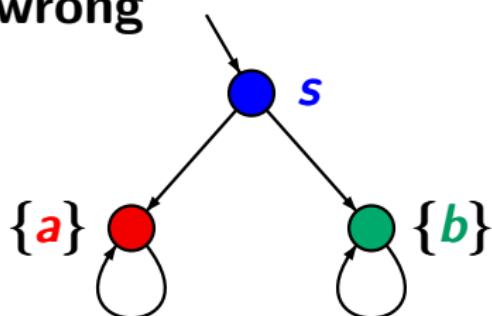
CTLFAIR4.4-7

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

correct.

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

wrong



$$fair = \Box \Diamond b$$

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

$$s \models \exists \Diamond a$$

just one fair path



Correct or wrong?

CTLFAIR4.4-7A

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

correct.

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

Correct or wrong?

CTLFAIR4.4-8

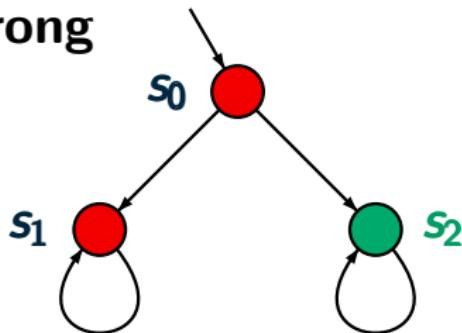
If $s \models \forall \Diamond \exists \Box a$ then $s \models_{fair} \forall \Diamond \exists \Box a$

Correct or wrong?

CTLFAIR4.4-8

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

wrong



$$\text{green circle} = \{b\}$$

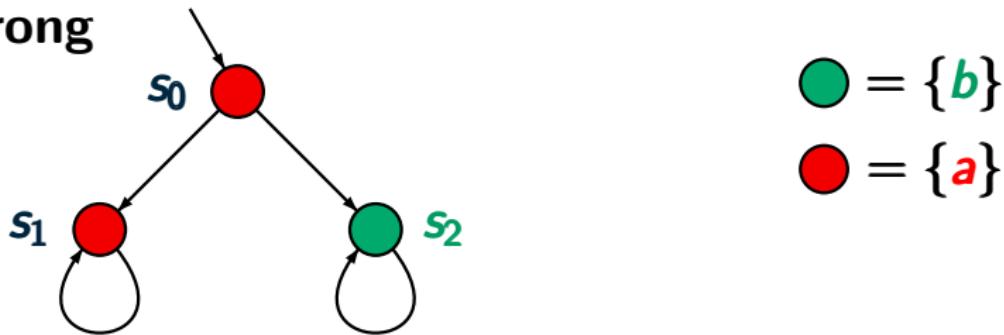
$$\text{red circle} = \{a\}$$

Correct or wrong?

CTLFAIR4.4-8

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?

CTLFAIR4.4-8

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

wrong



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

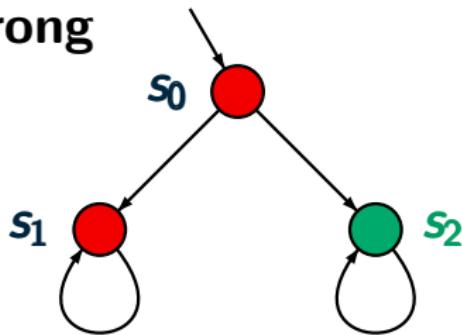
$$Sat(\forall \Diamond \exists \Box a) = \{s_0, s_1\}$$

Correct or wrong?

CTLFAIR4.4-8

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

wrong



$$\text{green circle} = \{b\}$$

$$\text{red circle} = \{a\}$$

$$fair = \Box \Diamond b$$

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

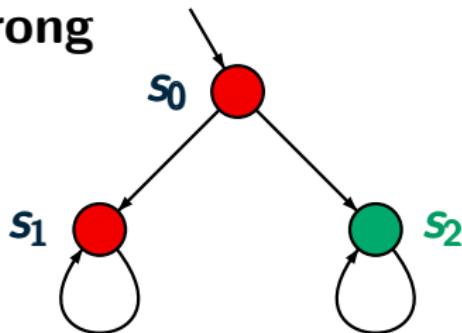
$$Sat(\forall \Diamond \exists \Box a) = \{s_0, s_1\}$$

Correct or wrong?

CTLFAIR4.4-8

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

wrong



$$\text{green circle} = \{b\}$$

$$\text{red circle} = \{a\}$$

$$fair = \Box \Diamond b$$

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

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

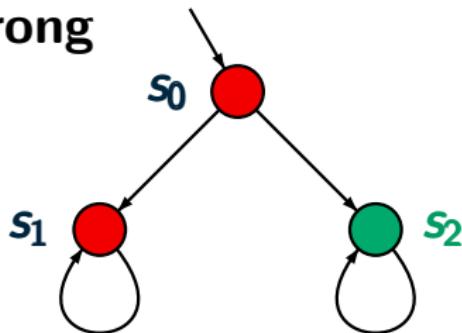
$$Sat(\forall \Diamond \exists \Box a) = \{s_0, s_1\}$$

Correct or wrong?

CTLFAIR4.4-8

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

wrong



$$\text{green circle} = \{b\}$$

$$\text{red circle} = \{a\}$$

$$fair = \Box \Diamond b$$

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

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

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

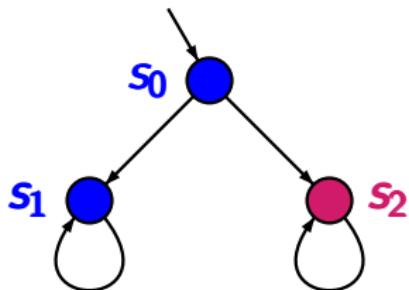
$$Sat_{fair}(\forall \Diamond \exists \Box a) = \emptyset$$

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

CTLFAIR4.4-11

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

CTLFAIR4.4-11



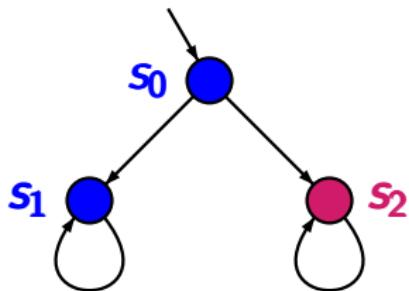
$$\text{pink circle} = \{a\}$$

$$\text{blue circle} = \emptyset$$

$$fair = \Box \Diamond a$$

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

CTLFAIR4.4-11



$$\textcolor{red}{\bullet} = \{a\}$$

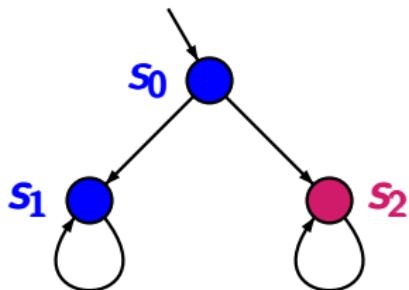
$$\textcolor{blue}{\bullet} = \emptyset$$

$$fair = \Box \Diamond a$$

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

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

CTLFAIR4.4-11



$$\textcolor{red}{\bullet} = \{a\}$$

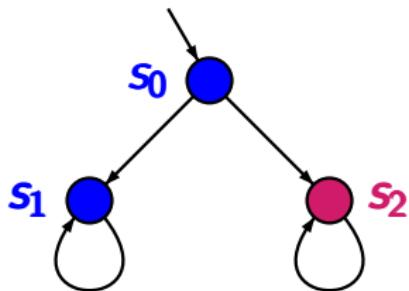
$$\textcolor{blue}{\bullet} = \emptyset$$

$$fair = \Box \Diamond a$$

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

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

CTLFAIR4.4-11



$$\textcolor{red}{\bullet} = \{a\}$$

$$\textcolor{blue}{\bullet} = \emptyset$$

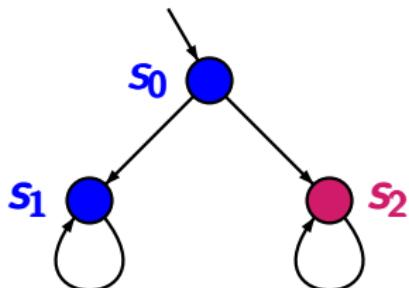
$$fair = \Box \Diamond a$$

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

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

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

CTLFAIR4.4-11



$$\textcolor{red}{\bullet} = \{a\}$$

$$\textcolor{blue}{\bullet} = \emptyset$$

$$fair = \Box \Diamond a$$

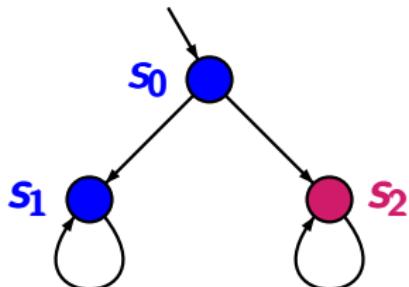
$$Sat_{fair}(\exists \Box true) = \{s_0, s_2\}$$

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

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

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

CTLFAIR4.4-11



$$\textcolor{red}{\bullet} = \{a\}$$

$$\textcolor{blue}{\bullet} = \emptyset$$

$$fair = \Box \Diamond a$$

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

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

CTLFAIR4.4-12

Model checking problem for FairCTL

CTLFAIR4.4-12

given: finite transition system \mathcal{T}

CTL formula Φ

CTL fairness assumption $fair$

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

Model checking problem for FairCTL

CTLFAIR4.4-12

given: finite transition system \mathcal{T}

CTL formula Φ

CTL fairness assumption fair , e.g.,

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

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

Model checking problem for FairCTL

CTLFAIR4.4-12

given: finite transition system \mathcal{T}

CTL formula Φ

CTL fairness assumption fair , e.g.,

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

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

for simplicity:

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

$\exists \bigcirc, \exists U, \exists \square$

given: finite transition system \mathcal{T}

CTL formula Φ in \exists -normal form

CTL fairness assumption fair , e.g.,

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

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

Preprocessing of FairCTL model checking

CTLFAIR4.4-12A

given: finite transition system \mathcal{T}

CTL formula Φ in \exists -normal form

CTL fairness assumption fair , e.g.,

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

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

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

Preprocessing of FairCTL model checking

CTLFAIR4.4-12A

given: finite transition system \mathcal{T}

CTL formula Φ in \exists -normal form

CTL fairness assumption fair , e.g.,

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

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

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

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

Preprocessing of FairCTL model checking

CTLFAIR4.4-12A

given: finite transition system \mathcal{T}

CTL formula Φ in \exists -normal form

CTL fairness assumption fair , e.g.,

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

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

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

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

Preprocessing of FairCTL model checking

CTLFAIR4.4-12A

given: finite transition system \mathcal{T}

CTL formula Φ in \exists -normal form

CTL fairness assumption fair , e.g.,

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

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

CTLFAIR4.4-12B

given: finite transition system \mathcal{T}

CTL formula Φ in \exists -normal form

CTL fairness assumption *fair*

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

1. ... preprocessing ...

Idea of FairCTL model checking

CTLFAIR4.4-12B

given: finite transition system \mathcal{T}

CTL formula Φ in \exists -normal form

CTL fairness assumption *fair*

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

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

Idea of FairCTL model checking

CTLFAIR4.4-12B

given: finite transition system \mathcal{T}

CTL formula Φ in \exists -normal form

CTL fairness assumption *fair*

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

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

Idea of FairCTL model checking

CTLFAIR4.4-12B

given: finite transition system \mathcal{T}

CTL formula Φ in \exists -normal form

CTL fairness assumption *fair*

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

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

Idea of FairCTL model checking

CTLFAIR4.4-12B

given: finite transition system \mathcal{T}

CTL formula Φ in \exists -normal form

CTL fairness assumption *fair*

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

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

recursive computation of the fair satisfaction sets:

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

recursive computation of the fair satisfaction sets:

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

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

recursive computation of the fair satisfaction sets:

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

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

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

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

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

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

Idea of FairCTL model checking

CTLFAIR4.4-12C

given: finite transition system \mathcal{T}

CTL formula Φ in \exists -normal form

CTL fairness assumption *fair*

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

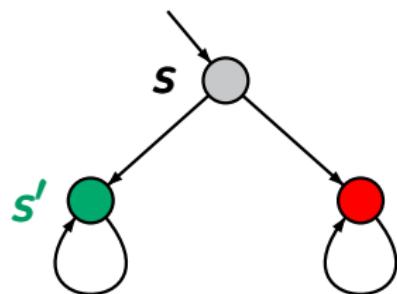
1. ... preprocessing ...
2. Build the parse tree of Φ and process it in bottom-up-manner. Treatment of:
 - *true*, $a \in AP$, \wedge , \neg : as for standard CTL
 - $\exists \bigcirc$, $\exists \mathbf{U}$: via **standard CTL** model checking
 - $\exists \square$: via analysis of SCCs

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

CTLFAIR4.4-14

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

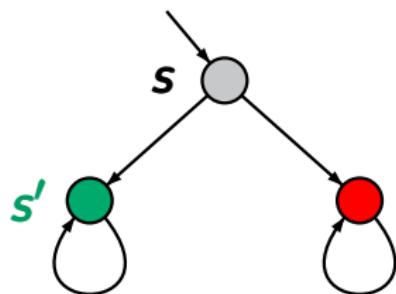
CTLFAIR4.4-14



$$fair = \Box \Diamond \text{red}$$

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

CTLFAIR4.4-14

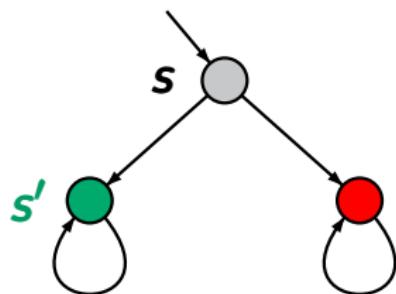


$$\textit{fair} = \square\lozenge\textcolor{red}{\text{red}}$$

$$s \not\models_{\textit{fair}} \exists\bigcirc\textcolor{teal}{\text{green}}$$

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

CTLFAIR4.4-14



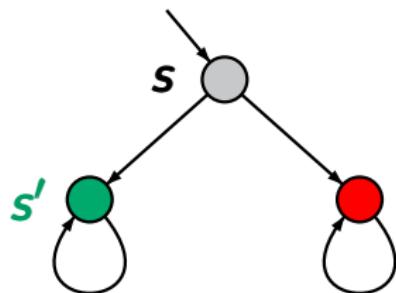
$$fair = \Box\Diamond red$$

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

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

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

CTLFAIR4.4-14



$$fair = \square\lozenge red$$

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

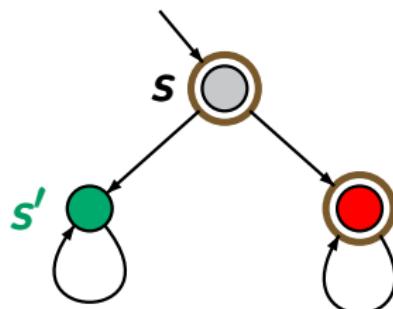
$$\text{as } s' \not\models_{fair} \exists\square true$$

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

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

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

CTLFAIR4.4-14



$$fair = \square\lozenge red$$

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

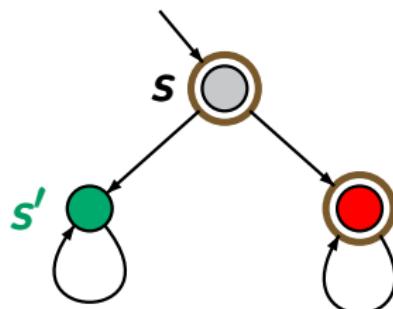
$$\text{as } s' \not\models_{fair} \exists\square true$$

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

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

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

CTLFAIR4.4-14



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

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

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

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

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

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

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

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

CTLFAIR4.4-14A

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

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

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

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

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

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

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

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

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

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

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

CTLFAIR4.4-14A

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

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

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

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

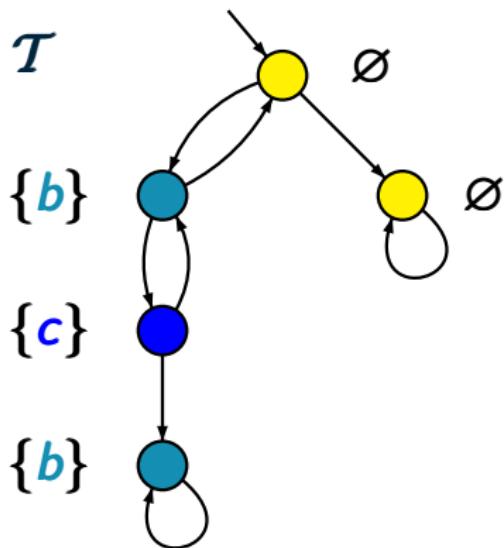
$$s \models_{fair} \exists(c \mathbf{U} b) \quad \text{iff} \quad s \models \exists(c \mathbf{U}(b \wedge a_{fair}))$$

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

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

Example: treatment of $\exists\Diamond$

CTLFAIR4.4-15

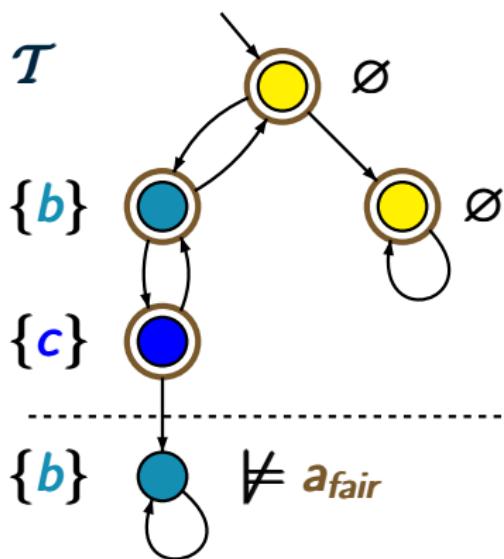


CTL formula $\exists\Diamond c$

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

Example: treatment of $\exists\Diamond$

CTLFAIR4.4-15

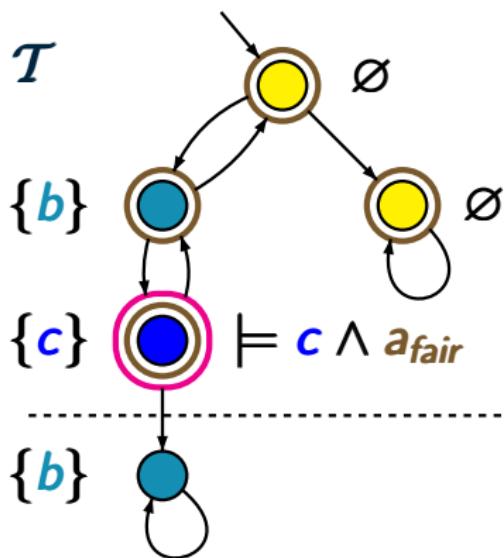


$$\begin{array}{c} \text{CTL formula } \exists\Diamond c \\ \downarrow \\ \exists\Diamond (c \wedge a_{fair}) \end{array}$$

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

Example: treatment of $\exists\Diamond$

CTLFAIR4.4-15



CTL formula $\exists\Diamond c$

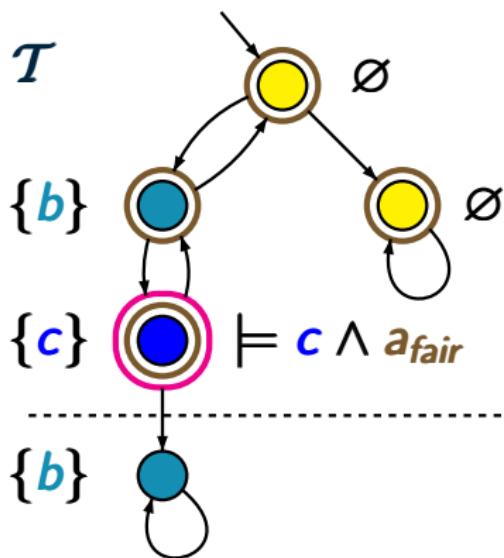
\downarrow

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

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

Example: treatment of $\exists\Diamond$

CTLFAIR4.4-15



CTL formula $\exists\Diamond c$

\downarrow

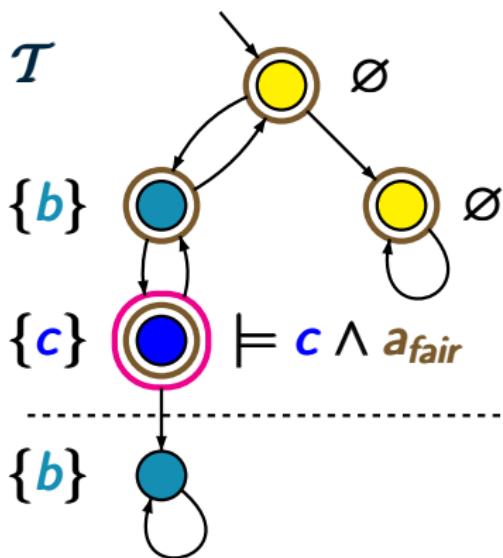
$\exists\Diamond(c \wedge a_{fair})$

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

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

Example: treatment of $\exists\Diamond$

CTLFAIR4.4-15



CTL formula $\exists\Diamond c$

\downarrow

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

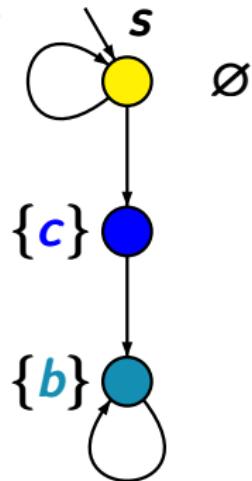
strong fairness assumption: $fair = \Box\Diamond b \rightarrow \Box\Diamond c$

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

Example: treatment of $\exists U$

CTLFAIR4.4-17

\mathcal{T} :

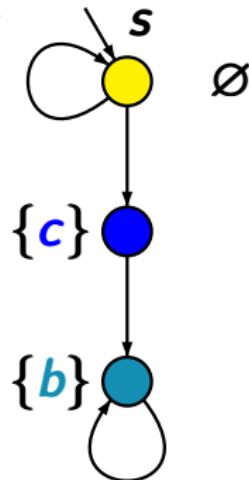


$$\mathcal{T} \models \exists(\neg b \cup c)$$

Example: treatment of $\exists U$

CTLFAIR4.4-17

\mathcal{T} :



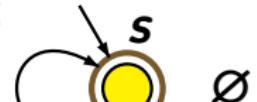
strong fairness assumption: $\text{fair} = \square \Diamond b \rightarrow \square \Diamond c$

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

Example: treatment of $\exists U$

CTLFAIR4.4-17

\mathcal{T} :



$\{c\}$ $\not\models a_{fair}$

$\{b\}$ $\not\models a_{fair}$

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

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

Example: treatment of $\exists U$

CTLFAIR4.4-17

\mathcal{T} :



$\{c\}$ $\not\models a_{fair}$

$\{b\}$ $\not\models a_{fair}$

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

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

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

Example: treatment of $\exists U$

CTLFAIR4.4-17

\mathcal{T} :



$$\{c\} \models \text{a}_{\text{fair}}$$

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

$$\{b\} \models \text{a}_{\text{fair}}$$

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



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

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

Example: treatment of $\exists U$

CTLFAIR4.4-17

\mathcal{T} :



$$\{c\} \not\models a_{fair}$$

$$\{b\} \not\models a_{fair}$$

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

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

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

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

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

Example: treatment of $\exists U$

CTLFAIR4.4-17

\mathcal{T} :



$$\{c\} \not\models a_{fair}$$

$$\{b\} \not\models a_{fair}$$

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



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



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

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

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

Correct or wrong?

CTLFAIR4.4-16

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

Correct or wrong?

CTLFAIR4.4-16

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

correct.

Correct or wrong?

CTLFAIR4.4-16

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

correct. Note that:

if $s_0 s_1 \dots s_{n-1} s_n$ is a path fragment from $s_0 = s$ s.t.

$s_n \models a_{\text{fair}}$ then $s_0, s_1, \dots, s_{n-1} \models a_{\text{fair}}$.

Correct or wrong?

CTLFAIR4.4-16

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

correct. Note that:

if $s_0 s_1 \dots s_{n-1} s_n$ is a path fragment from $s_0 = s$ s.t.

$s_n \models a_{\text{fair}}$ then $s_0, s_1, \dots, s_{n-1} \models a_{\text{fair}}$. Hence:

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

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

Correct or wrong?

CTLFAIR4.4-16

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

correct. Note that:

if $s_0 s_1 \dots s_{n-1} s_n$ is a path fragment from $s_0 = s$ s.t.

$s_n \models a_{\text{fair}}$ then $s_0, s_1, \dots, s_{n-1} \models a_{\text{fair}}$. Hence:

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

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

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

Correct or wrong?

CTLFAIR4.4-16

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

correct. Note that:

if $s_0 s_1 \dots s_{n-1} s_n$ is a path fragment from $s_0 = s$ s.t.

$s_n \models a_{\text{fair}}$ then $s_0, s_1, \dots, s_{n-1} \models a_{\text{fair}}$. Hence:

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

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

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

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

Correct or wrong?

CTLFAIR4.4-16

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

correct.

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

Correct or wrong?

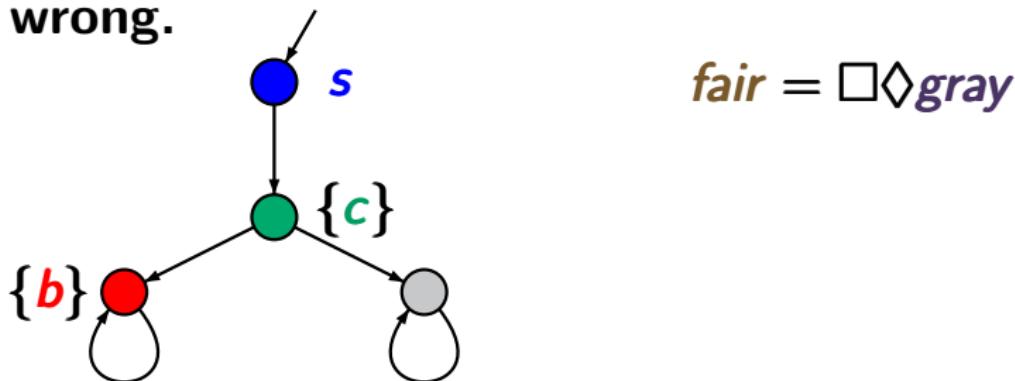
CTLFAIR4.4-16

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

correct.

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

wrong.



Correct or wrong?

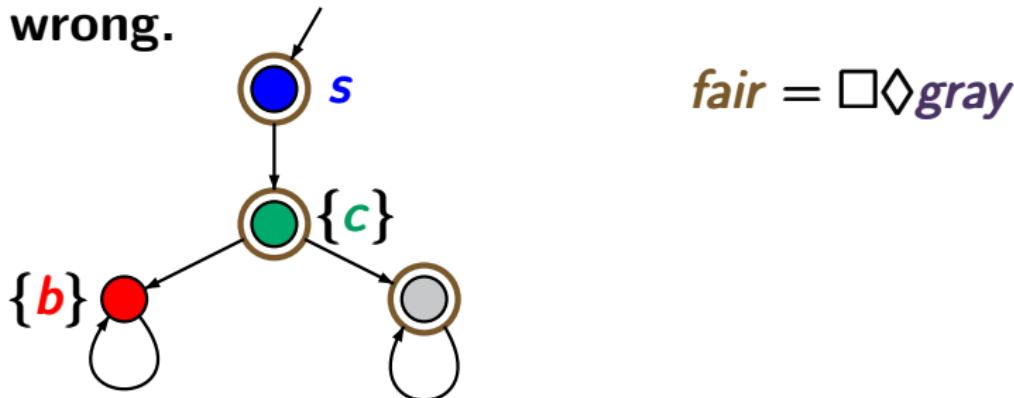
CTLFAIR4.4-16

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

correct.

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

wrong.



Correct or wrong?

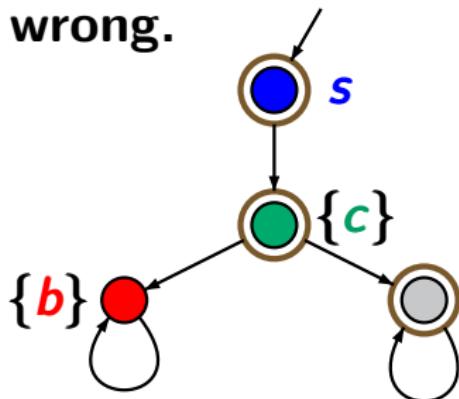
CTLFAIR4.4-16

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

correct.

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

wrong.



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

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

Correct or wrong?

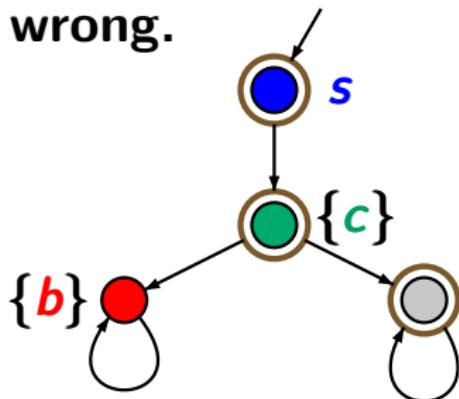
CTLFAIR4.4-16

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

correct.

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

wrong.



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

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

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

Correct or wrong?

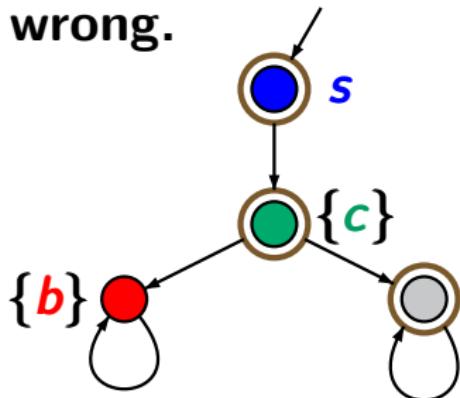
CTLFAIR4.4-16

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

correct.

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

wrong.



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

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

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

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

Correct or wrong?

CTLFAIR4.4-23

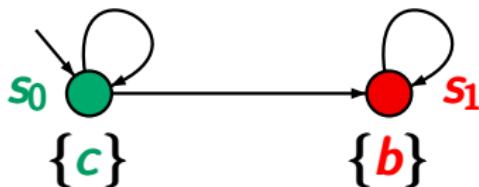
$$s \models_{fair} \exists \Box c \text{ iff } s \models \exists \Box(c \wedge a_{fair})$$

Correct or wrong?

CTLFAIR4.4-23

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

wrong.



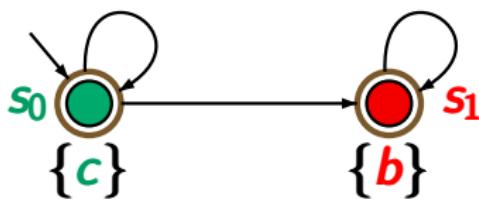
$$fair = \Box \Diamond b$$

Correct or wrong?

CTLFAIR4.4-23

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

wrong.



$$fair = \Box \Diamond b$$

$$s_0 \models a_{fair}$$

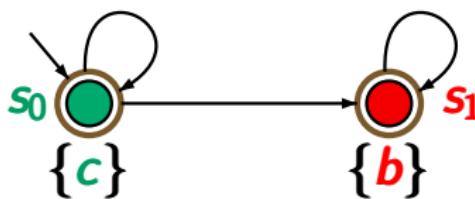
$$s_1 \models a_{fair}$$

Correct or wrong?

CTLFAIR4.4-23

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

wrong.



$$fair = \Box \Diamond b$$

$$s_0 \models a_{fair}$$

$$s_1 \models a_{fair}$$

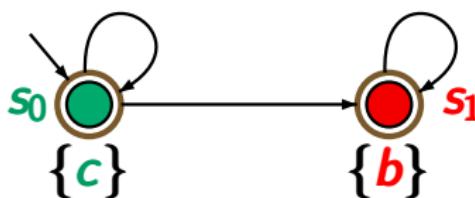
regard state $s = s_0$:

Correct or wrong?

CTLFAIR4.4-23

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

wrong.



$$fair = \Box \Diamond b$$

$$s_0 \models a_{fair}$$

$$s_1 \models a_{fair}$$

regard state $s = s_0$:

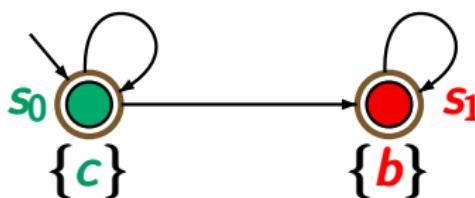
$$s \models \exists \Box(c \wedge a_{fair}),$$

Correct or wrong?

CTLFAIR4.4-23

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

wrong.



$$fair = \Box \Diamond b$$

$$s_0 \models a_{fair}$$

$$s_1 \models a_{fair}$$

regard state $s = s_0$:

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



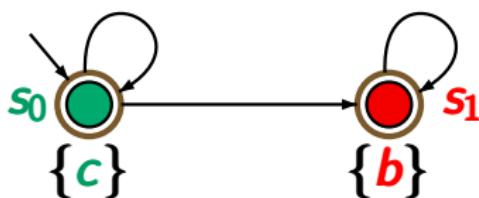
$$\text{path } \pi = s_0 s_0 s_0 s_0 \dots \models \Box(c \wedge a_{fair})$$

Correct or wrong?

CTLFAIR4.4-23

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

wrong.



$$fair = \Box \Diamond b$$

$$s_0 \models a_{fair}$$

$$s_1 \models a_{fair}$$

regard state $s = s_0$:

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



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

Idea of FairCTL model checking

CTLFAIR4.4-12D

given: finite transition system \mathcal{T}

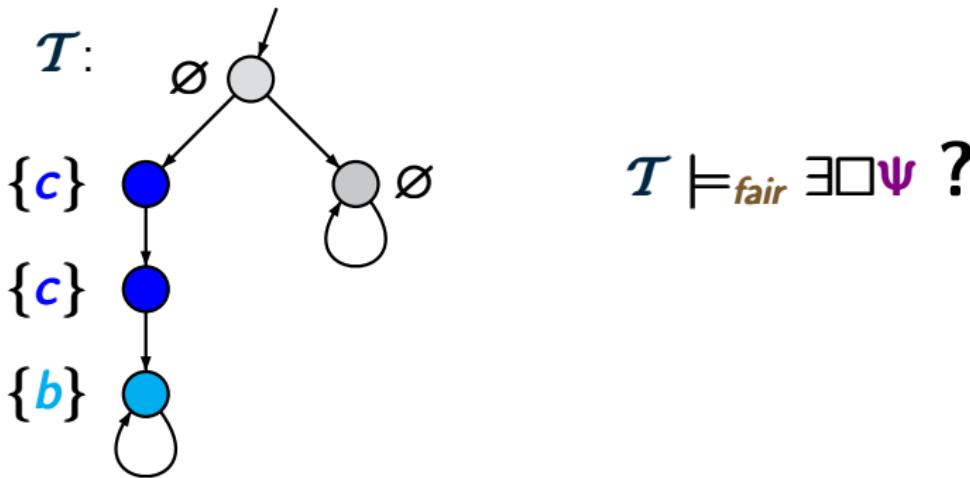
CTL formula Φ in \exists -normal form

CTL fairness assumption *fair*

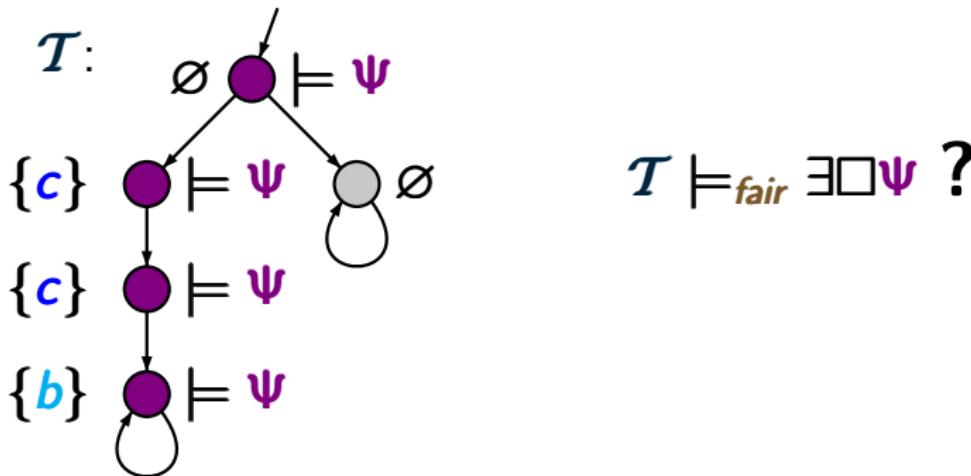
question: does $\mathcal{T} \models_{\text{fair}} \Phi$ hold ?

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

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

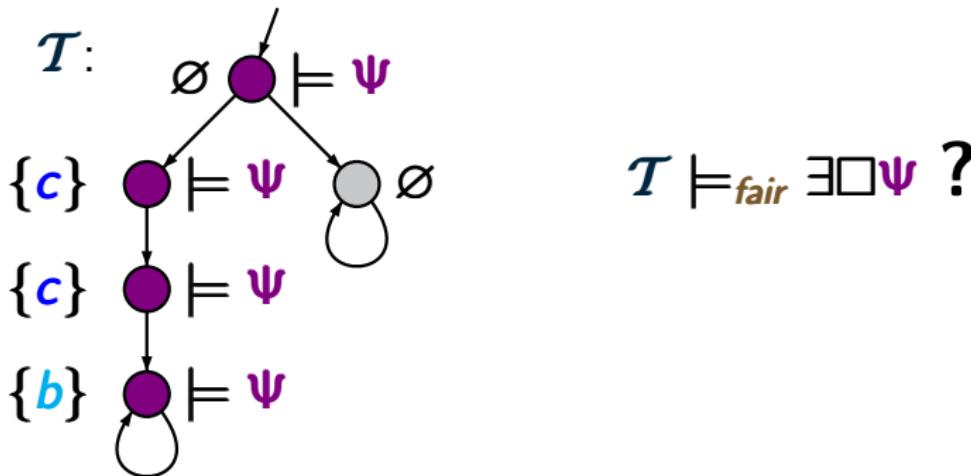


fair = $\Box \Diamond b \rightarrow \Box \Diamond c$, CTL state formula Ψ



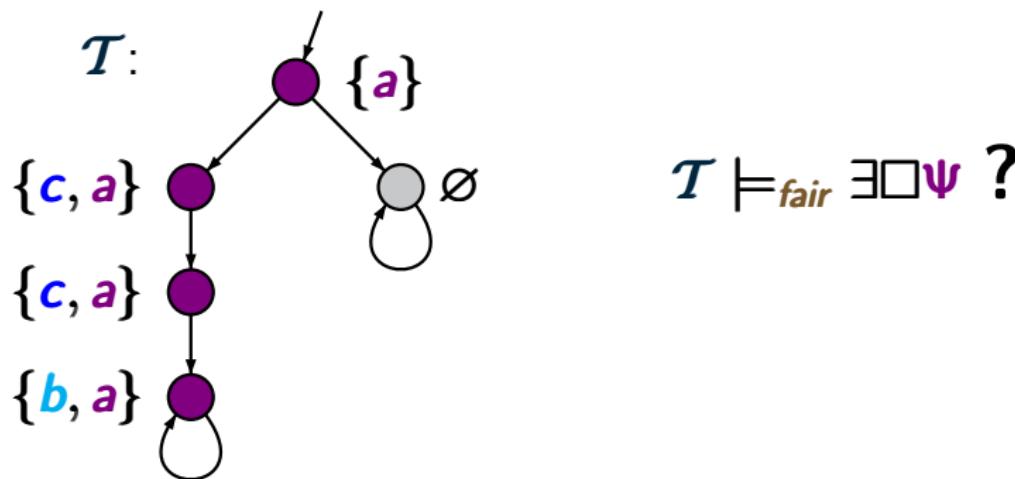
1. calculate $Sat_{\text{fair}}(\Psi)$

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



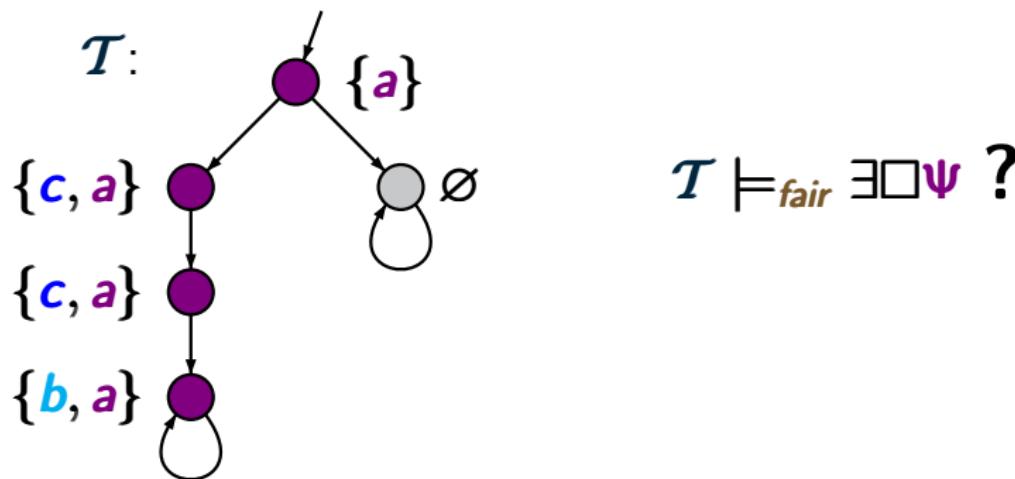
1. calculate $Sat_{\text{fair}}(\Psi)$
2. replace Ψ with a fresh atomic proposition $a = a_\Psi$

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



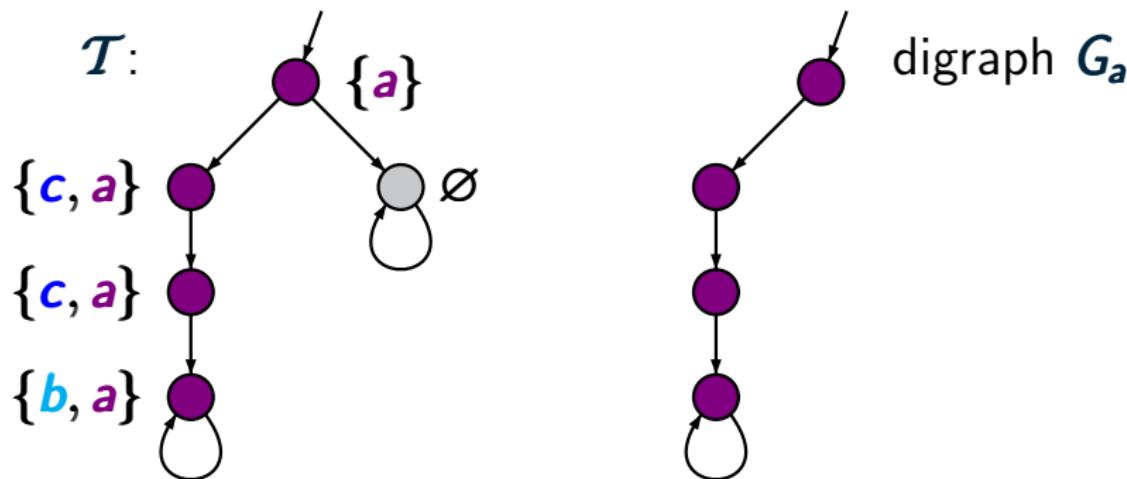
1. calculate $Sat_{\text{fair}}(\Psi)$
2. replace Ψ with a fresh atomic proposition $a = a_\Psi$

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



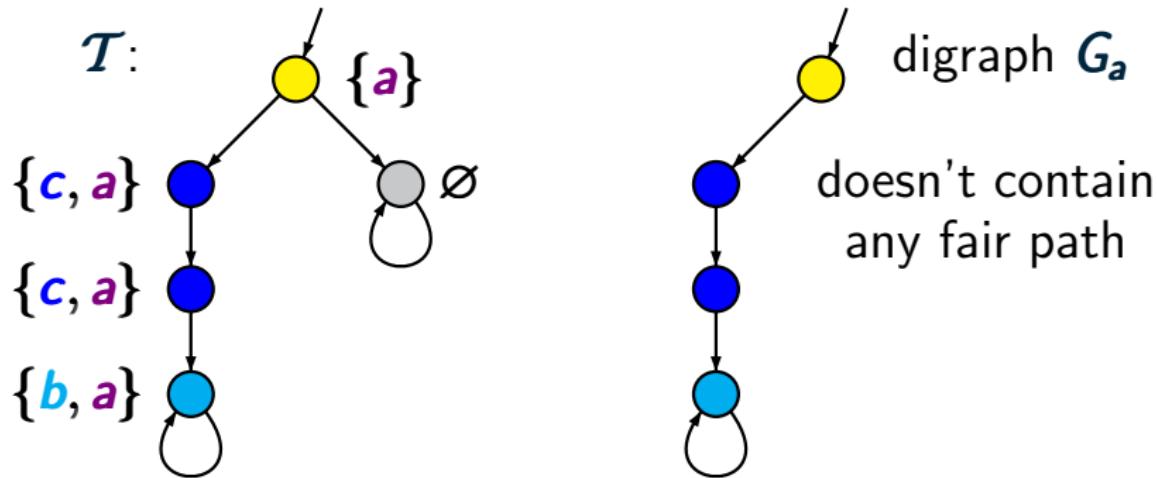
1. calculate $Sat_{\text{fair}}(\Psi)$
2. replace Ψ with a fresh atomic proposition $a = a_\Psi$
3. calculate $Sat_{\text{fair}}(\exists \Box a)$

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



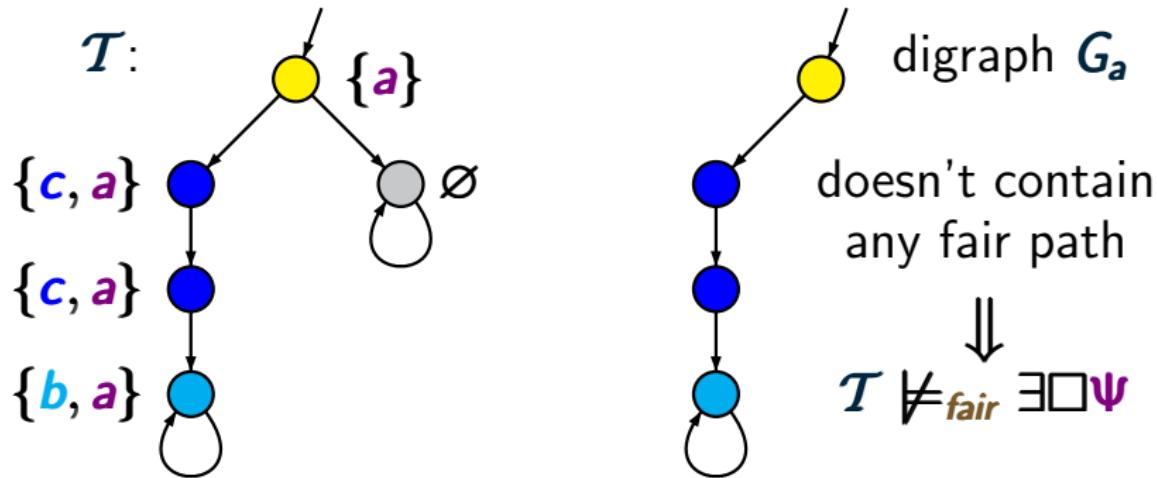
1. calculate $Sat_{fair}(\Psi)$
2. replace Ψ with a fresh atomic proposition $a = a_\Psi$
3. calculate $Sat_{fair}(\exists \Box a)$

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



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

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



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

Treatment of $\exists \Box a$ for FairCTL

CTLFAIR4.4-Box-A

given: finite TS \mathcal{T} , atomic proposition a

CTL fairness assumption $fair$

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

Treatment of $\exists \Box a$ for FairCTL

CTLFAIR4.4-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

CTLFAIR4.4-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 $Sat_{fair}(\exists \Box true)$

here: explanations only for strong fairness

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

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

$$\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond \textcolor{brown}{b}_i \rightarrow \Box \Diamond \textcolor{red}{c}_i)$$

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

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

$$\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond \textcolor{blue}{b}_i \rightarrow \Box \Diamond \textcolor{red}{c}_i)$$

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

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

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

$$\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond \textcolor{blue}{b}_i \rightarrow \Box \Diamond \textcolor{red}{c}_i)$$

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

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

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

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

$$\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond \textcolor{blue}{b}_i \rightarrow \Box \Diamond \textcolor{red}{c}_i)$$

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

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

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

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

Treatment of $\exists \Box$ under strong fairness

CTLFAIR4.4-19

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

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

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

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

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

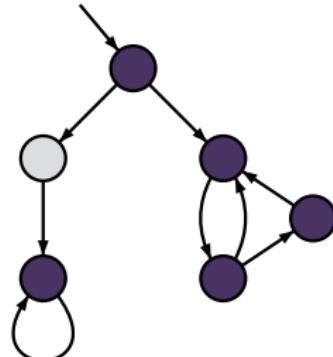
$$\{s_{n+1}, \dots, s_{n+r}\} \cap \text{Sat}(b_i) = \emptyset$$

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

$\exists \Box a$ under strong fairness

CTLFAIR4.4-19A

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

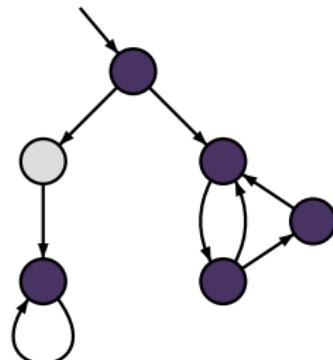


$\bullet \models a$ $\circ \not\models a$

$\exists \Box a$ under strong fairness

CTLFAIR4.4-19A

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



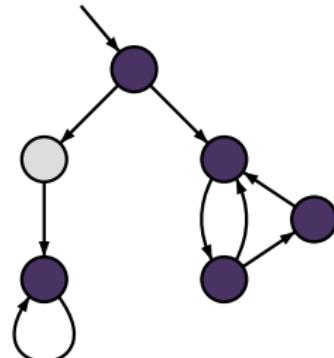
$\bullet \models a$ $\circ \not\models a$

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

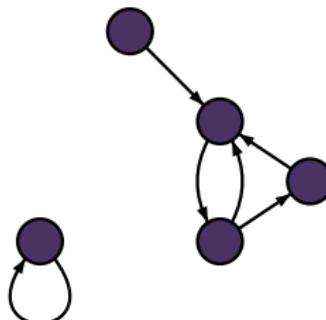
$\exists \Box a$ under strong fairness

CTLFAIR4.4-19A

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



digraph G_a



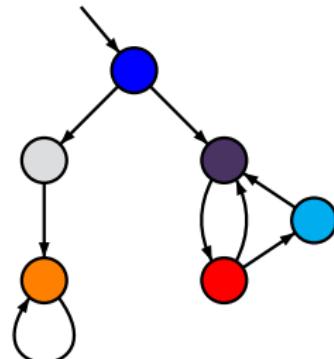
$\bullet \models a$ $\circ \not\models a$

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

$\exists \Box a$ under strong fairness

CTLFAIR4.4-19A

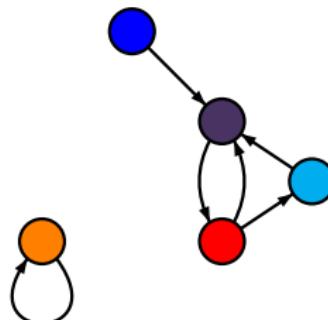
does $T \models_{fair} \exists \Box a$ hold ?



$$\bullet \hat{=} \{b_1\} \quad \bullet \hat{=} \{c_1\}$$

$$\bullet \hat{=} \{b_2\} \quad \bullet \hat{=} \{c_2\}$$

digraph G_a

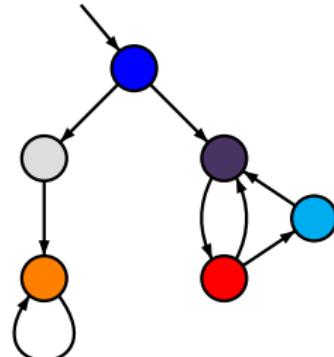


$$fair = (\Box \Diamond b_1 \rightarrow \Box \Diamond c_1) \wedge (\Box \Diamond b_2 \rightarrow \Box \Diamond c_2)$$

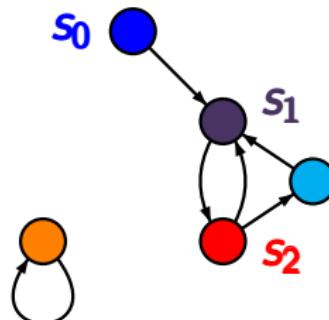
$\exists \Box a$ under strong fairness

CTLFAIR4.4-19A

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



digraph G_a



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

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

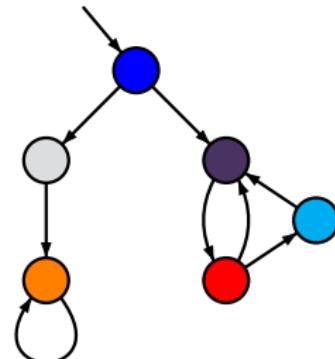
$$\text{light blue} \hat{=} \{b_2\} \quad \text{blue} \hat{=} \{c_2\}$$

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

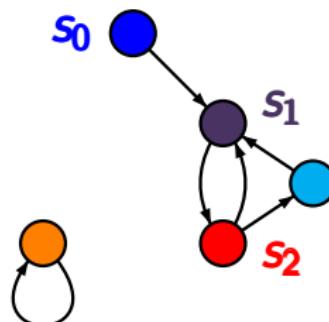
$\exists \Box a$ under strong fairness

CTLFAIR4.4-19A

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



digraph G_a



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

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

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

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

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

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

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

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

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

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

Treatment of $\exists \Box$ under strong fairness

CTLFAIR4.4-20

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

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

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

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

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



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

Treatment of $\exists \Box$ under strong fairness

CTLFAIR4.4-20

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

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

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

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

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



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

Treatment of $\exists \Box$ under strong fairness

CTLFAIR4.4-20A

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

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

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

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

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

(1) D is reachable from s

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

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

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

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

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

(1) D is reachable from s

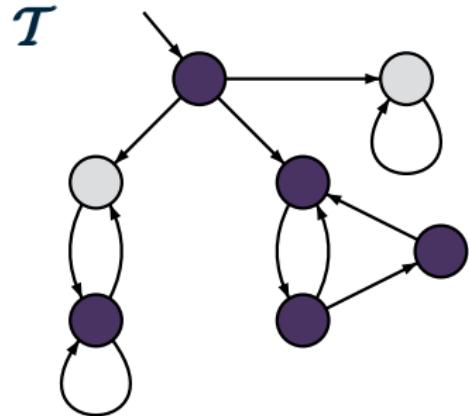
(2) for all $1 \leq i \leq k$:

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

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

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

CTLFAIR4.4-22

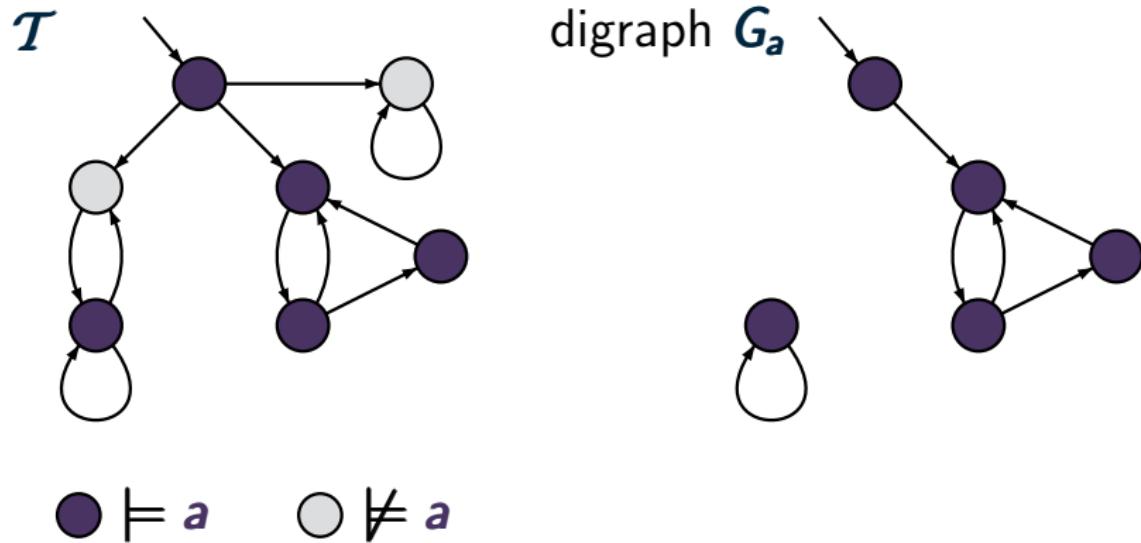


● $\models a$ ○ $\not\models a$

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

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

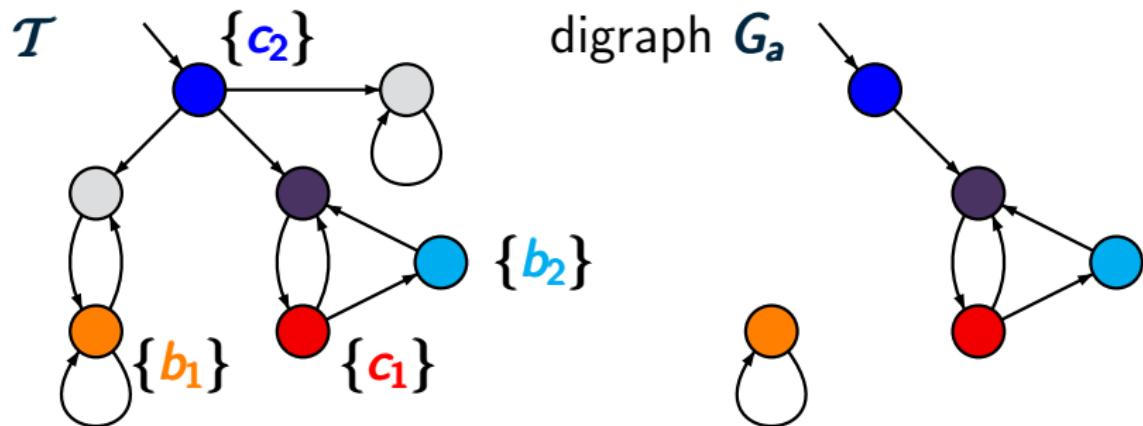
CTLFAIR4.4-22



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

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

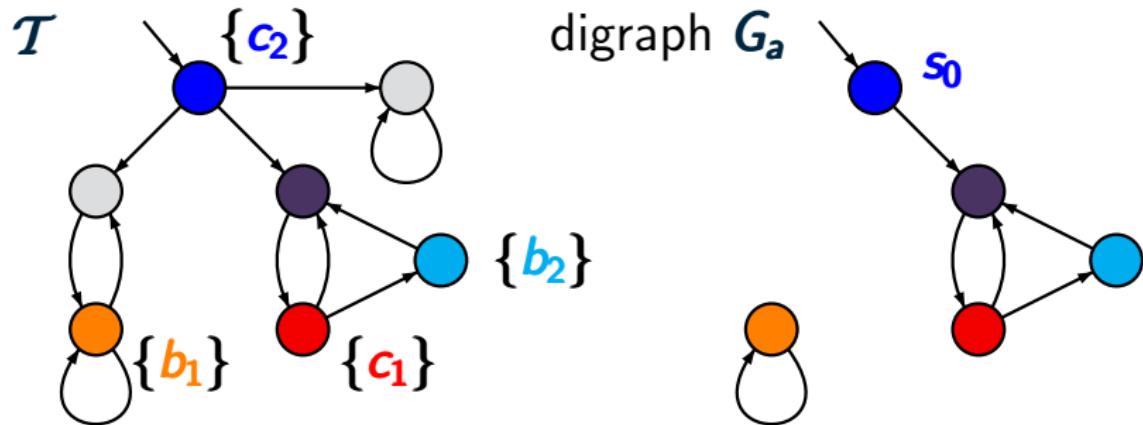
CTLFAIR4.4-22



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

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

CTLFAIR4.4-22

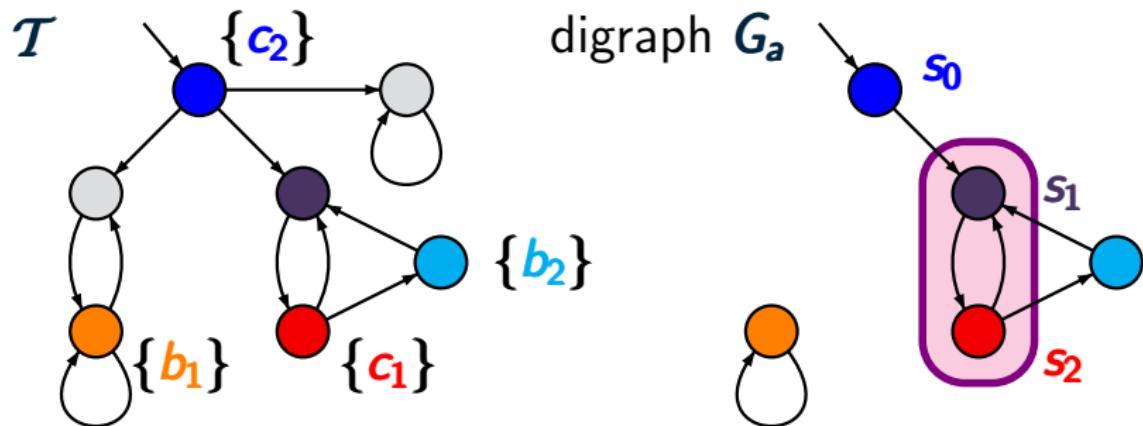


$$fair = (\Box \Diamond b_1 \rightarrow \Box \Diamond c_1) \wedge (\Box \Diamond b_2 \rightarrow \Box \Diamond c_2)$$

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

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

CTLFAIR4.4-22

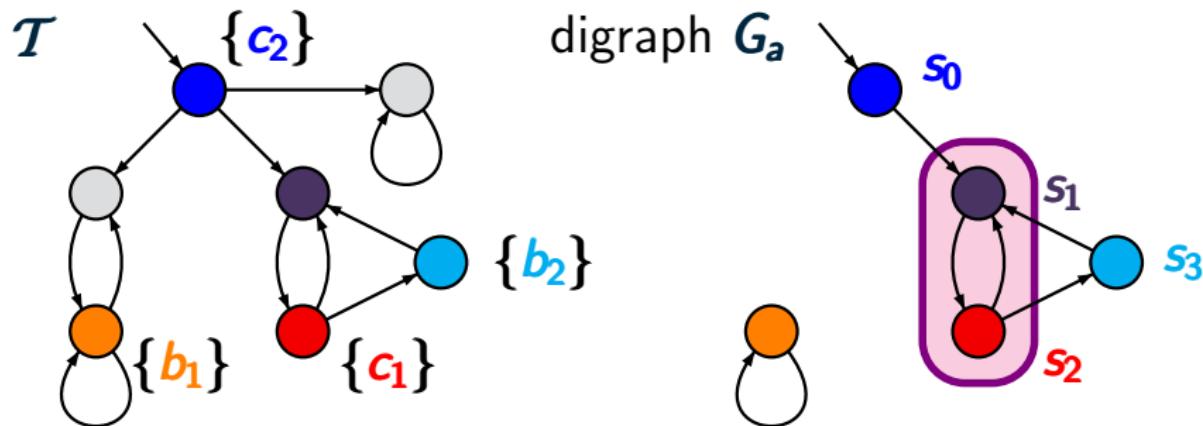


$$fair = (\Box \Diamond b_1 \rightarrow \Box \Diamond c_1) \wedge (\Box \Diamond b_2 \rightarrow \Box \Diamond c_2)$$

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

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

CTLFAIR4.4-22



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

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

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

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

CTL model checking with fairness

CTLFAIR4.4-FAIRNESS-3-CASES

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

case 3: arbitrary strong fairness assumption

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

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

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

here: explanations only for **strong** fairness

case 1: unconditional fairness

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

case 3: arbitrary strong fairness assumption

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

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

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

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

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

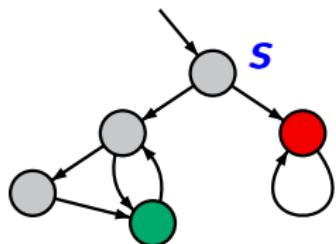
$$fair = \bigwedge_{1 \leq i \leq k} \Box \Diamond c_i$$

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

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

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

digraph G_a

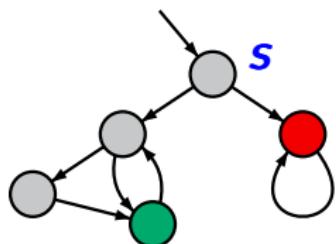


fairness assumption:
 $fair = \Box \Diamond c_1 \wedge \Box \Diamond c_2$

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

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

digraph G_a



fairness assumption:

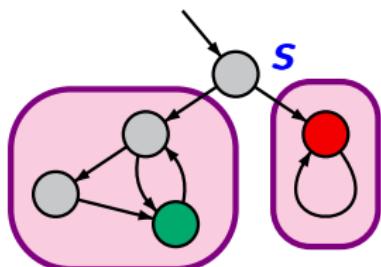
$$fair = \Box \Diamond c_1 \wedge \Box \Diamond c_2$$

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

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

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

digraph G_a

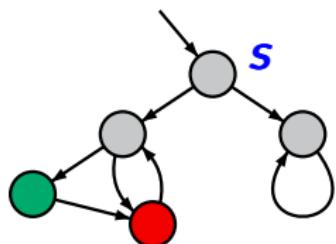


fairness assumption:
 $fair = \Box \Diamond c_1 \wedge \Box \Diamond c_2$
 $s \not\models_{fair} \exists \Box a$

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

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

digraph G_a

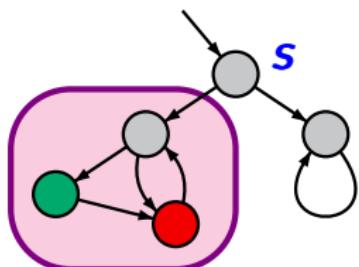


fairness assumption:
 $fair = \Box \Diamond c_1 \wedge \Box \Diamond c_2$

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

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

digraph G_a



fairness assumption:

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

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

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

here: explanations only for **strong** fairness

case 1: unconditional fairness ✓

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

case 3: arbitrary strong fairness assumption

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

CTL model checking with fairness

CTLFAIR4.4-FAIRNESS-CASE2

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

here: explanations only for **strong** fairness

case 1: unconditional fairness ✓

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

case 3: arbitrary strong fairness assumption

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

Strong fairness: 1 fairness requirement

CTLFAIR4.4-25

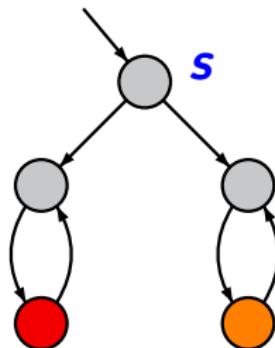
$$\text{fair} = \Box\Diamond b \rightarrow \Box\Diamond c$$

Strong fairness: 1 fairness requirement

CTLFAIR4.4-25

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

digraph G_a



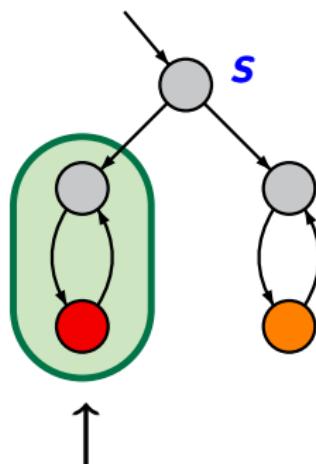
- $\hat{=} \emptyset$
- $\hat{=} \{c\}$
- $\hat{=} \{b\}$

Strong fairness: 1 fairness requirement

CTLFAIR4.4-25

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

digraph G_a



- $\hat{=} \emptyset$
- $\hat{=} \{c\}$
- $\hat{=} \{b\}$

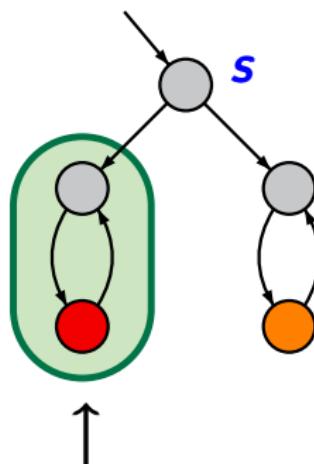
nontrivial **SCC** C of G_a with $C \cap Sat(c) \neq \emptyset$

Strong fairness: 1 fairness requirement

CTLFAIR4.4-25

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

digraph G_a



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

- $\hat{=} \emptyset$
- $\hat{=} \{c\}$
- $\hat{=} \{b\}$

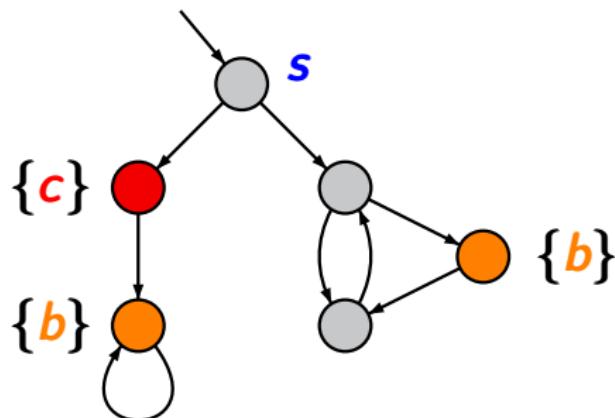
nontrivial **SCC** C of G_a with $C \cap Sat(c) \neq \emptyset$

Strong fairness: 1 fairness requirement

CTLFAIR4.4-25A

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

digraph G_a

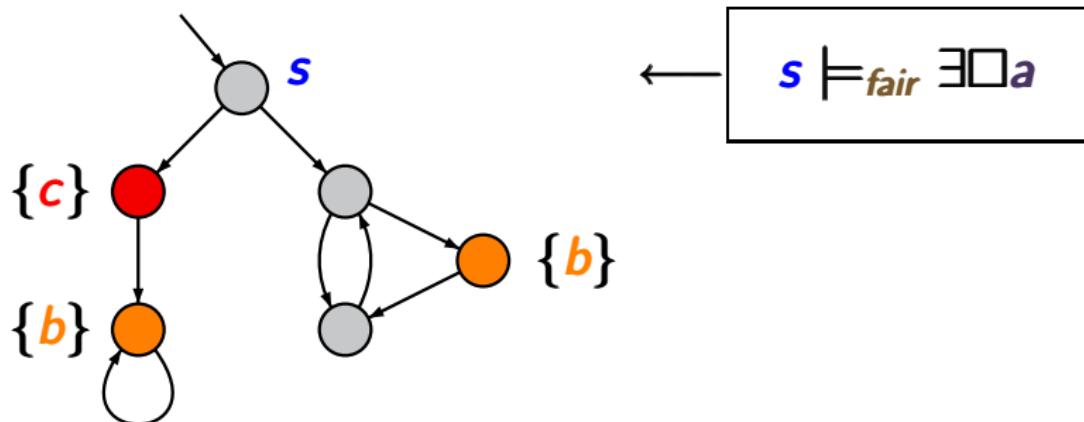


Strong fairness: 1 fairness requirement

CTLFAIR4.4-25A

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

digraph G_a

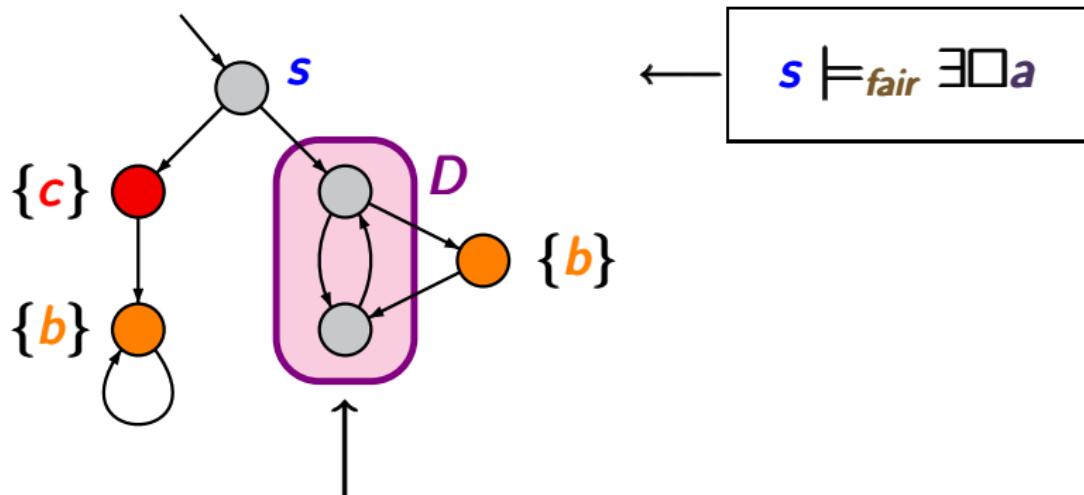


Strong fairness: 1 fairness requirement

CTLFAIR4.4-25A

$$fair = \square \lozenge b \rightarrow \square \lozenge c$$

digraph G_a



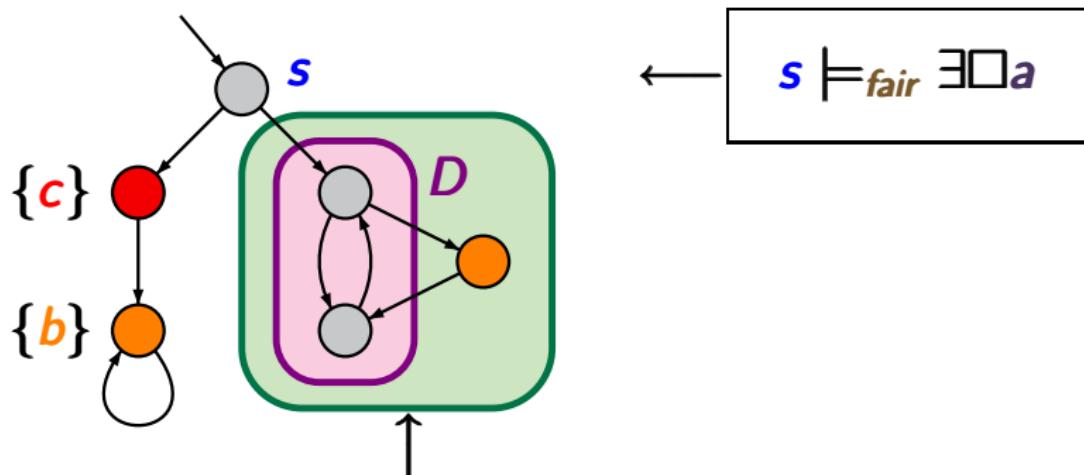
$$s \models_{fair} \exists \square a$$

Strong fairness: 1 fairness requirement

CTLFAIR4.4-25A

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

digraph G_a



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

CTL model checking with fairness

CTLFAIR4.4-FAIRNESS-CASE3

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

here: explanations only for **strong** fairness

case 1: unconditional fairness ✓

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

case 3: arbitrary strong fairness assumption

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

CTL model checking with fairness

CTLFAIR4.4-FAIRNESS-CASE3

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

here: explanations only for **strong** fairness

case 1: unconditional fairness ✓

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

case 3: arbitrary strong fairness assumption

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

Example: 2 strong fairness conditions

CTLFAIR4.4-26

Example: 2 strong fairness conditions

CTLFAIR4.4-26

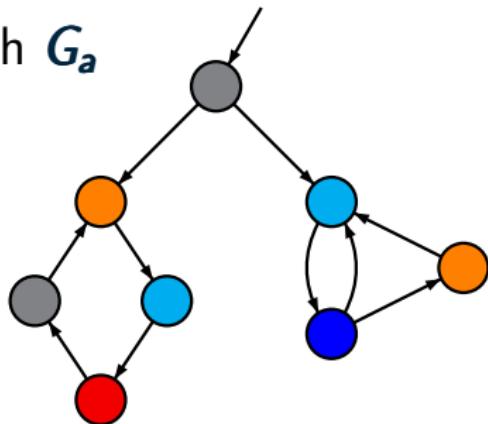
$$fair = (\Box\Diamond b_1 \rightarrow \Box\Diamond c_1) \wedge (\Box\Diamond b_2 \rightarrow \Box\Diamond c_2)$$

Example: 2 strong fairness conditions

CTLFAIR4.4-26

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

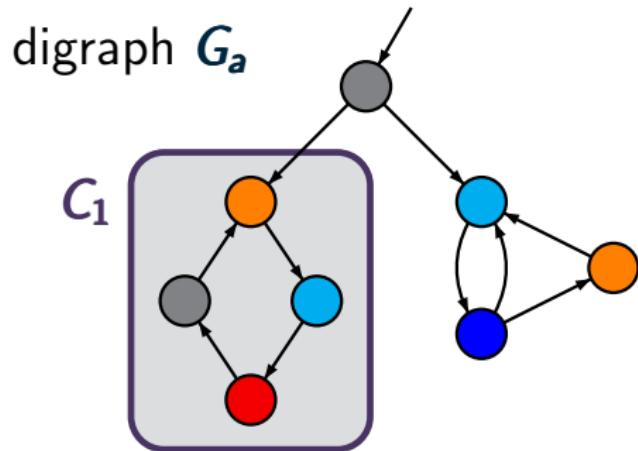
digraph G_a



Example: 2 strong fairness conditions

CTLFAIR4.4-26

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

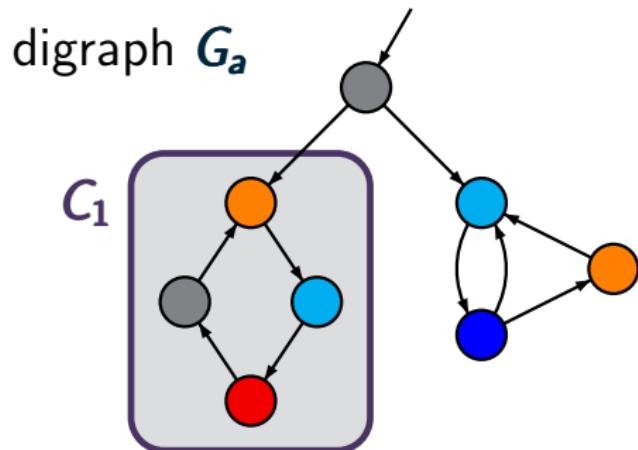


first SCC: $C_1 \cap Sat(c_2) = \emptyset$

Example: 2 strong fairness conditions

CTLFAIR4.4-26

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



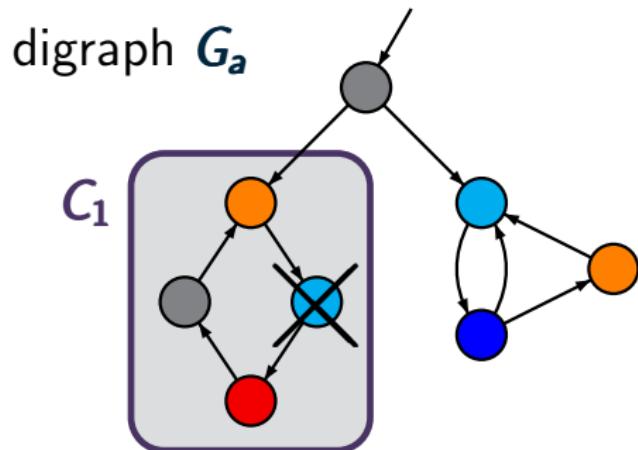
first SCC: $C_1 \cap Sat(c_2) = \emptyset$

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

Example: 2 strong fairness conditions

CTLFAIR4.4-26

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



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

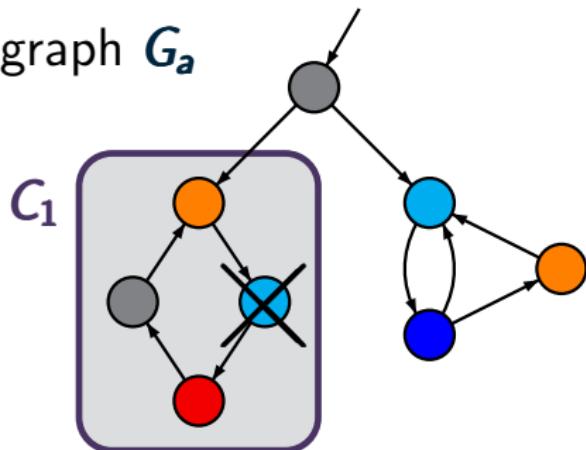
analyze $C_1 \setminus Sat(b_2)$ w.r.t. $\Box\Diamond b_1 \rightarrow \Box\Diamond c_1$

Example: 2 strong fairness conditions

CTLFAIR4.4-26

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

digraph G_a



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

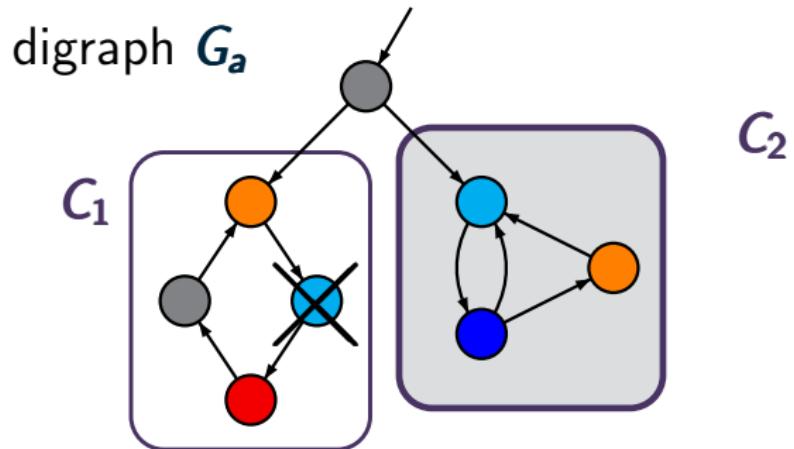
analyze $C_1 \setminus Sat(b_2)$ w.r.t. $\Box\Diamond b_1 \rightarrow \Box\Diamond c_1$

↝ there is no cycle

Example: 2 strong fairness conditions

CTLFAIR4.4-26

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

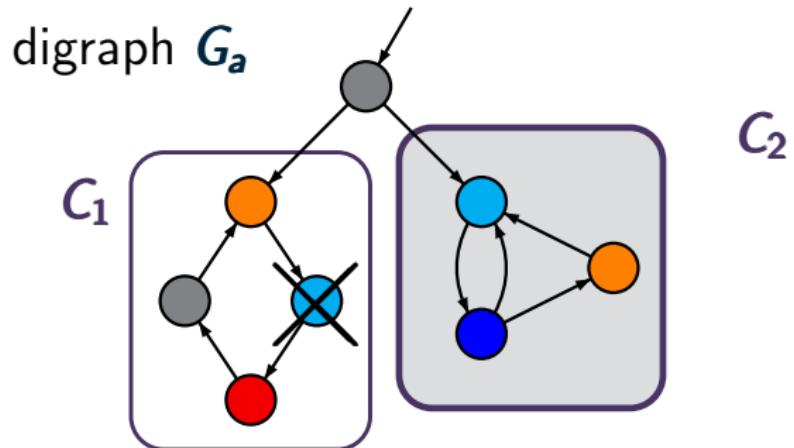


second SCC:

Example: 2 strong fairness conditions

CTLFAIR4.4-26

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

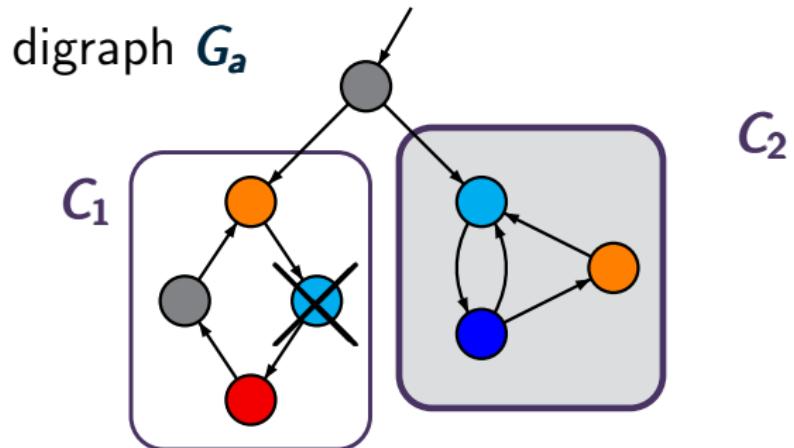


second SCC: $C_2 \cap Sat(c_1) = \emptyset$

Example: 2 strong fairness conditions

CTLFAIR4.4-26

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



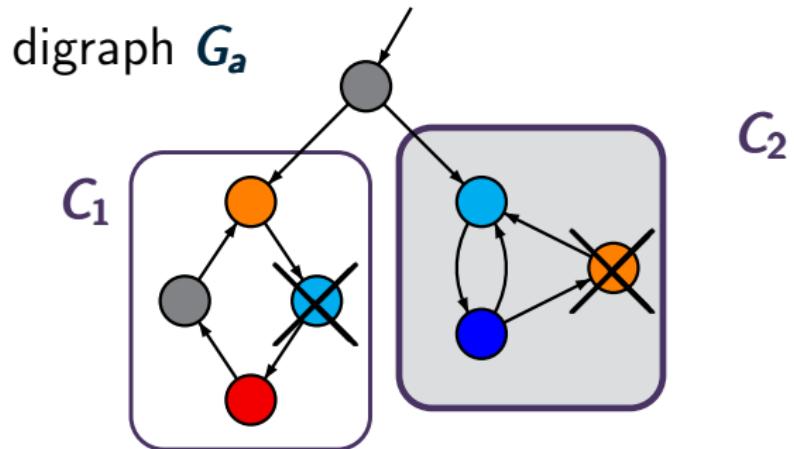
second SCC: $C_2 \cap Sat(c_1) = \emptyset$

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

Example: 2 strong fairness conditions

CTLFAIR4.4-26

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



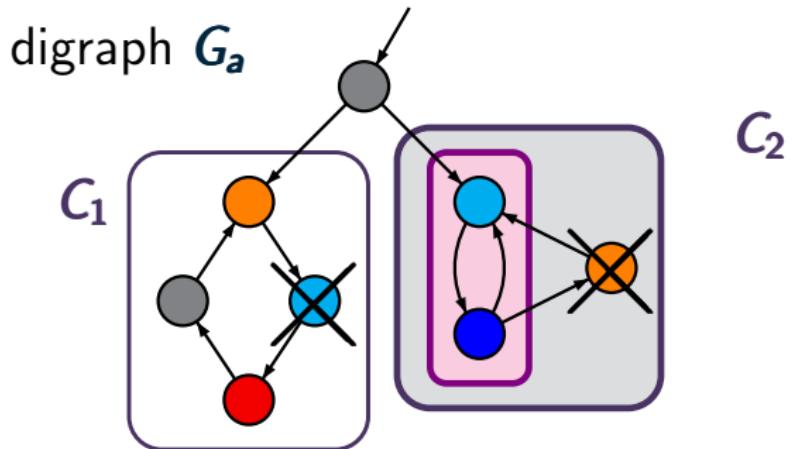
second SCC: $C_2 \cap Sat(c_1) = \emptyset$

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

Example: 2 strong fairness conditions

CTLFAIR4.4-26

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



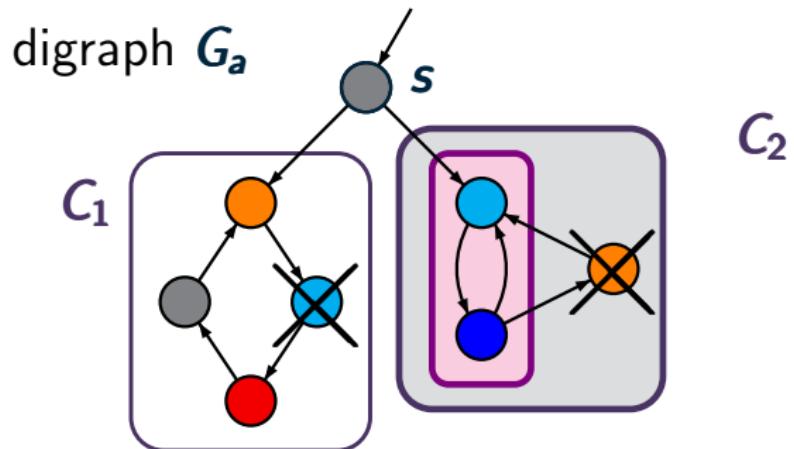
second SCC: $C_2 \cap Sat(c_1) = \emptyset$

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

Example: 2 strong fairness conditions

CTLFAIR4.4-26

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



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

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

CTLFAIR4.4-27

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

CTLFAIR4.4-27

compute the SCCs of the digraph G_a ;

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

CTLFAIR4.4-27

compute the SCCs of the digraph G_a ;

$T := \emptyset$;

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

CTLFAIR4.4-27

compute the SCCs of the digraph G_a ;

$T := \emptyset$;

FOR ALL nontrivial SCCs C of G_a DO

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

CTLFAIR4.4-27

compute the SCCs of the digraph G_a ;

$T := \emptyset$;

FOR ALL nontrivial SCCs C of G_a DO

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

OD

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

CTLFAIR4.4-27

compute the SCCs of the digraph G_a ;

$T := \emptyset$;

FOR ALL nontrivial SCCs C of G_a DO

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

OD

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

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

CTLFAIR4.4-27

compute the SCCs of the digraph G_a ;

$T := \emptyset$;

FOR ALL nontrivial SCCs C of G_a DO

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

OD

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



backward search from T

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

CTLFAIR4.4-27

compute the SCCs of the digraph G_a ;

$T := \emptyset$;

FOR ALL nontrivial SCCs C of G_a DO

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

OD

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

backward search from T

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

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

CTLFAIR4.4-27

compute the SCCs of the digraph G_a ;

$T := \emptyset$;

FOR ALL nontrivial SCCs C of G_a DO

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

OD

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

backward search from T

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

Recursive algorithm *CheckFair*(...)

CTLFAIR4.4-28

Recursive algorithm *CheckFair*(...)

CTLFAIR4.4-28

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

Recursive algorithm $\text{CheckFair}(\dots)$

CTLFAIR4.4-28

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

“true” if there exists a cyclic path fragment
 $s_0 s_1 \dots s_n$ in \mathcal{C} such that

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

“false” otherwise

Recursive algorithm *CheckFair*(...)

CTLFAIR4.4-28

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

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

Recursive algorithm $\text{CheckFair}(\dots)$

CTLFAIR4.4-28

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

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

Recursive algorithm $\text{CheckFair}(\dots)$

CTLFAIR4.4-28

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

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

Recursive algorithm $\text{CheckFair}(\dots)$

CTLFAIR4.4-28

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

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

Recursive algorithm *CheckFair*(...)

CTLFAIR4.4-28

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

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

Recursive algorithm $\text{CheckFair}(\dots)$

CTLFAIR4.4-28

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

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

Recursive algorithm $\text{CheckFair}(\dots)$

CTLFAIR4.4-28

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

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

Complexity of *CheckFair*(...)

CTLFAIR4.4-29

Complexity of *CheckFair*(...)

CTLFAIR4.4-29

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

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

Complexity of *CheckFair*(...)

CTLFAIR4.4-29

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

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

recurrence for the time complexity:

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

Complexity of *CheckFair*(...)

CTLFAIR4.4-29

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

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

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

CTL model checking with fairness

CTLFAIR4.4-30

input: finite transition system \mathcal{T}

CTL fairness assumption $fair$

CTL formula Φ

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

CTL model checking with fairness

CTLFAIR4.4-30

input: finite transition system \mathcal{T}

CTL fairness assumption $fair$

CTL formula Φ

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

here: *preprocessing*

transform Φ into an equivalent CTL formula
in **existential normal form**

CTL model checking with fairness

CTLFAIR4.4-30

input: finite transition system \mathcal{T}

CTL fairness assumption $fair$

CTL formula Φ

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

here: *preprocessing*

transform Φ into an equivalent CTL formula
in **existential normal form**



i.e., with the basic modalities $\exists\bigcirc$, $\exists\bigcup$ and $\exists\Box$

Model checking algorithm for FairCTL

CTLFAIR4.4-30

Model checking algorithm for FairCTL

CTLFAIR4.4-30

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

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

Model checking algorithm for FairCTL

CTLFAIR4.4-30

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

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

FOR ALL subformulas Ψ of Φ DO

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

OD

Model checking algorithm for FairCTL

CTLFAIR4.4-30

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

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

FOR ALL subformulas Ψ of Φ DO

CASE Ψ is:

:

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

$\exists(a_1 \bigcup a_2)$: $Sat_{fair}(\Psi)$:= $Sat(\exists(a_1 \bigcup (a_2 \wedge a_{fair})))$;

$\exists \Box a$: $Sat_{fair}(\Psi)$:= ...

OD

Model checking algorithm for FairCTL

CTLFAIR4.4-30

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

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

FOR ALL subformulas Ψ of Φ DO

CASE Ψ is:

:

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

$\exists(a_1 \bigcup a_2)$: $Sat_{fair}(\Psi) := Sat(\exists(a_1 \bigcup (a_2 \wedge a_{fair})))$;

$\exists \Box a$: $Sat_{fair}(\Psi) := ...$

replace Ψ with a fresh atomic proposition a_Ψ

OD

Model checking algorithm for FairCTL

CTLFAIR4.4-30

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

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

FOR ALL subformulas Ψ of Φ DO

CASE Ψ is:

:

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

$\exists(a_1 \bigcup a_2)$: $Sat_{fair}(\Psi) := Sat(\exists(a_1 \bigcup (a_2 \wedge a_{fair})))$;

$\exists \Box a$: $Sat_{fair}(\Psi) := ...$

replace Ψ with a fresh atomic proposition a_Ψ

OD

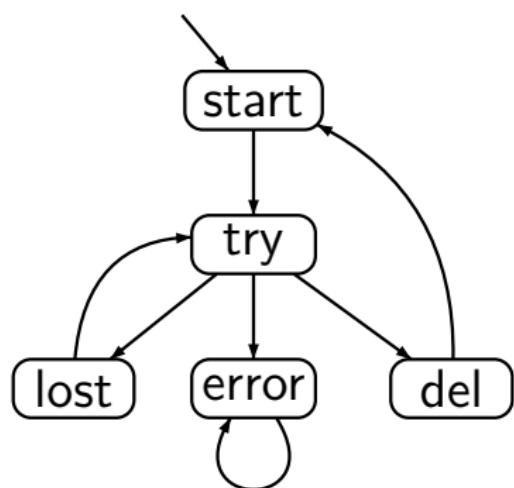
IF $S_0 \subseteq Sat_{fair}(\Phi)$ THEN return “yes”

ELSE return “no”

FI

Example: CTL model checking with fairness

CTLFAIR4.4-31

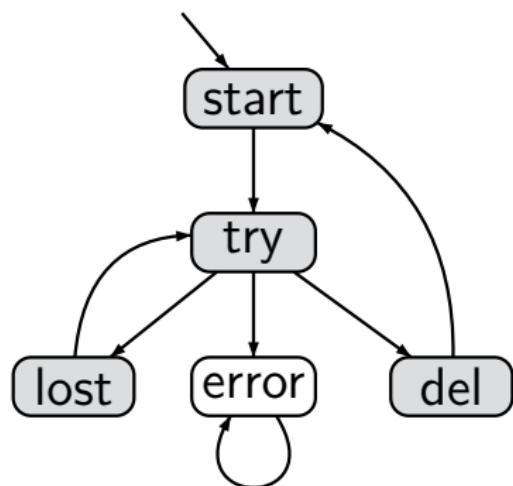


$$\Phi = \exists \Diamond \forall \bigcirc (\text{lost} \vee \text{del})$$

$$fair = \Box \Diamond \exists \Diamond \text{del}$$

Example: CTL model checking with fairness

CTLFAIR4.4-31

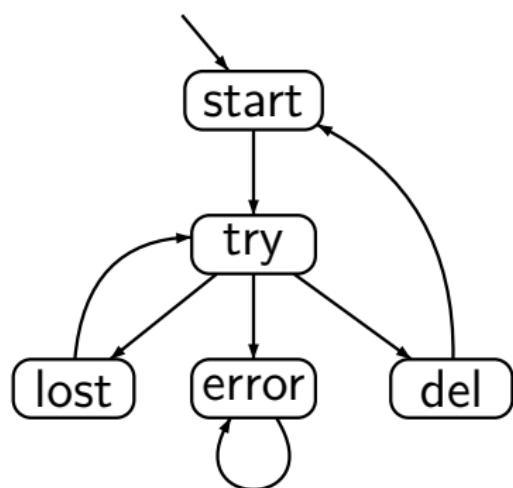


$$\Phi = \exists \Diamond \forall \bigcirc (\text{lost} \vee \text{del})$$

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

Example: CTL model checking with fairness

CTLFAIR4.4-31



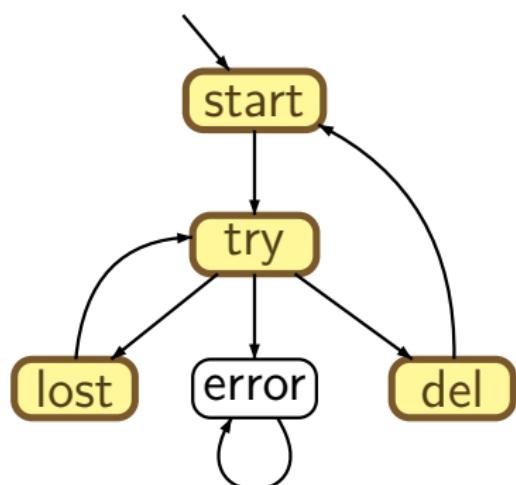
$$\Phi = \exists \Diamond \forall \bigcirc (\text{lost} \vee \text{del})$$

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

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

Example: CTL model checking with fairness

CTLFAIR4.4-31



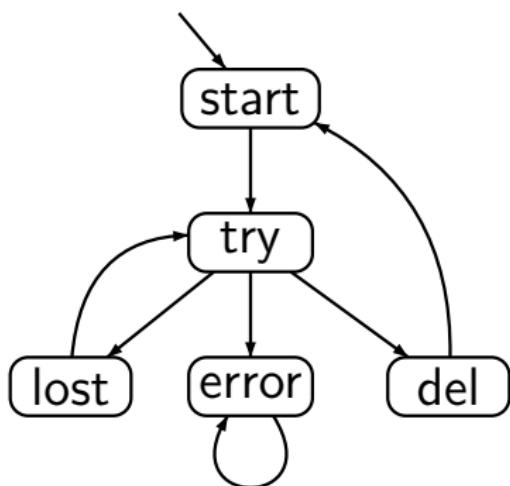
$$\Phi = \exists \Diamond \forall \bigcirc (\text{lost} \vee \text{del})$$

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

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

Example: CTL model checking with fairness

CTLFAIR4.4-31



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

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

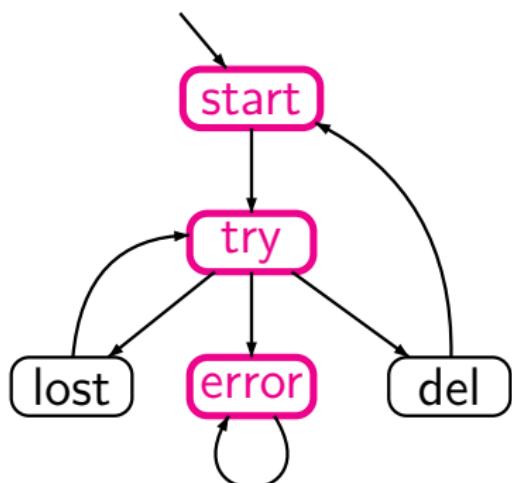
existential normal form

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

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

Example: CTL model checking with fairness

CTLFAIR4.4-31



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

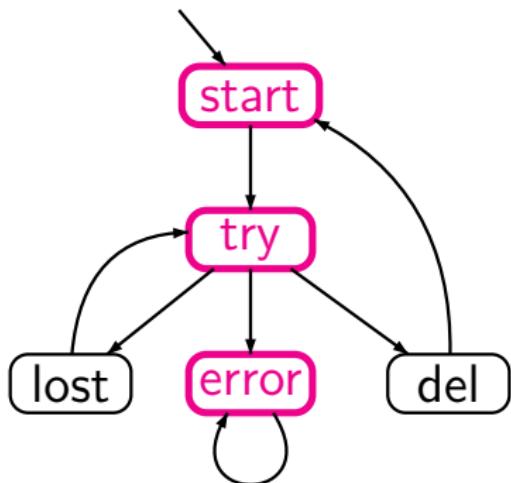
$$\equiv \exists \Diamond \neg \exists \bigcirc (\neg \text{lost} \wedge \neg \text{del})$$

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

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

Example: CTL model checking with fairness

CTLFAIR4.4-31



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

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

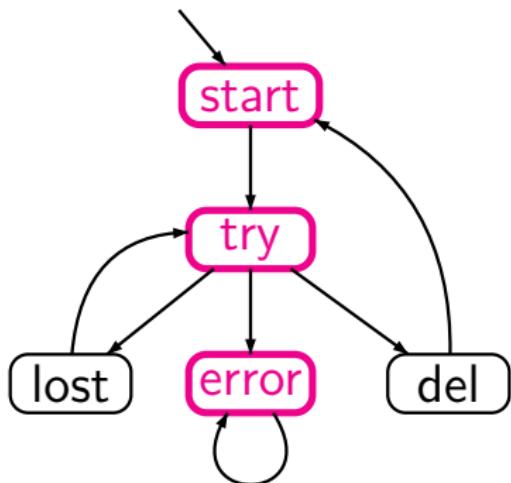
$$\rightsquigarrow \exists \Diamond \neg \exists \bigcirc a$$

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

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

Example: CTL model checking with fairness

CTLFAIR4.4-31



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

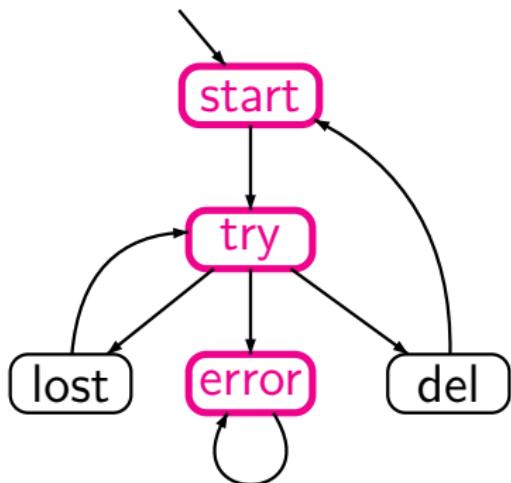
$$fair = \Box \Diamond \exists \Diamond \text{del} \rightsquigarrow \Box \Diamond c \text{ where } Sat(c) = S \setminus \{\text{error}\}$$

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

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

Example: CTL model checking with fairness

CTLFAIR4.4-31



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

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

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

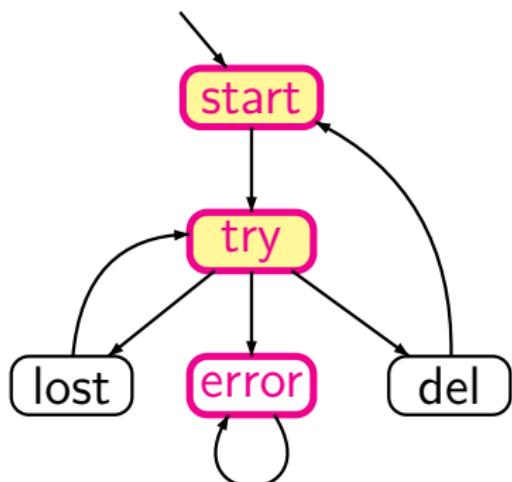
$$fair = \Box \Diamond \exists \Diamond \text{del} \rightsquigarrow \Box \Diamond c \text{ where } Sat(c) = S \setminus \{\text{error}\}$$

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

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

Example: CTL model checking with fairness

CTLFAIR4.4-31



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

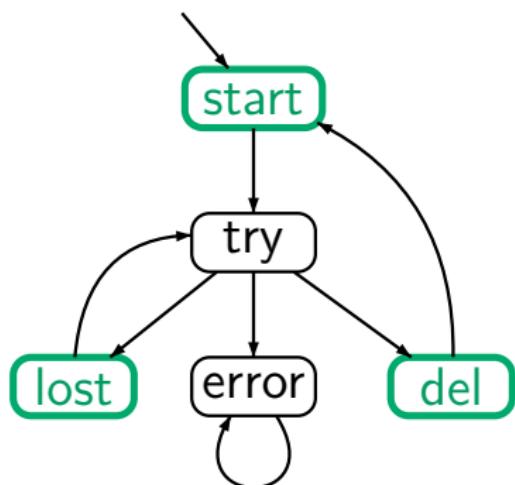
$$fair = \Box \Diamond \exists \Diamond \text{del} \rightsquigarrow \Box \Diamond c \text{ where } Sat(c) = S \setminus \{\text{error}\}$$

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

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

Example: CTL model checking with fairness

CTLFAIR4.4-31



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

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

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

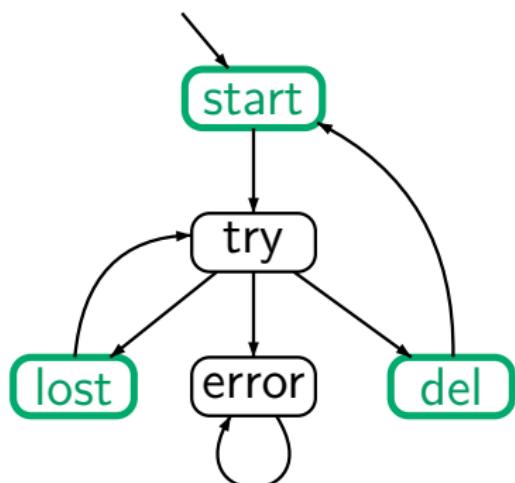
$$fair = \Box \Diamond \exists \Diamond \text{del} \rightsquigarrow \Box \Diamond c \text{ where } Sat(c) = S \setminus \{\text{error}\}$$

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

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

Example: CTL model checking with fairness

CTLFAIR4.4-31



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

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

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

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

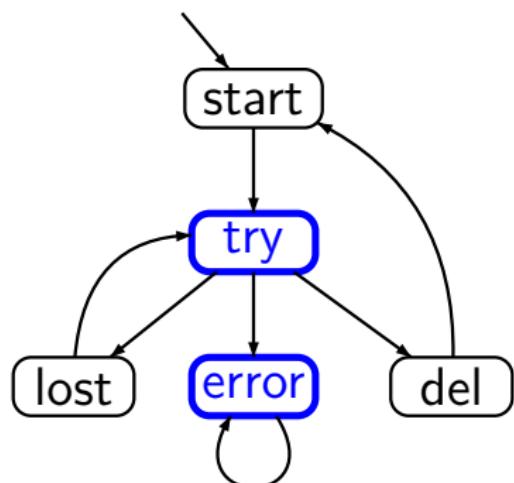
$$Sat_{fair}(\exists \Box \text{true}) = Sat(a_{fair}) = S \setminus \{\text{error}\}$$

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

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

Example: CTL model checking with fairness

CTLFAIR4.4-31



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

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

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

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

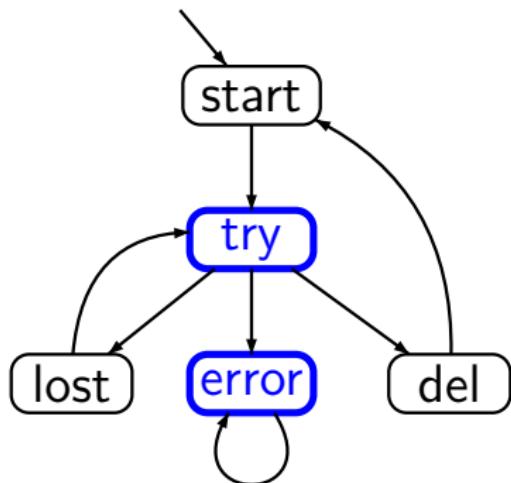
$$Sat_{fair}(\exists \Box \text{true}) = Sat(a_{fair}) = S \setminus \{\text{error}\}$$

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

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

Example: CTL model checking with fairness

CTLFAIR4.4-31



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

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

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

$$\rightsquigarrow \exists \Diamond b$$

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

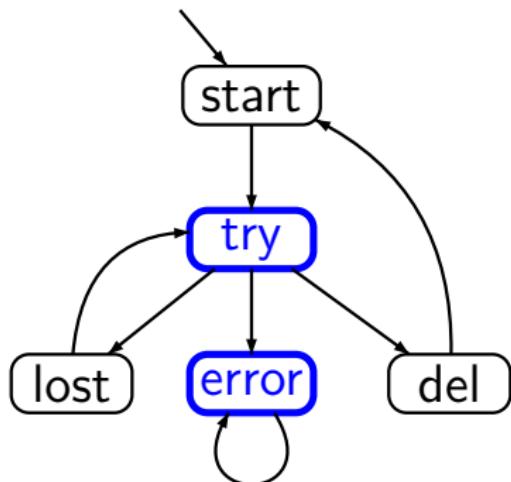
$$Sat_{fair}(\exists \Box \text{true}) = Sat(a_{fair}) = S \setminus \{\text{error}\}$$

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

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

Example: CTL model checking with fairness

CTLFAIR4.4-31



$$\begin{aligned}\Phi &= \exists \Diamond \forall \bigcirc (\text{lost} \vee \text{del}) \\ &\equiv \exists \Diamond \neg \exists \bigcirc (\neg \text{lost} \wedge \neg \text{del}) \\ &\rightsquigarrow \exists \Diamond \neg \exists \bigcirc a \\ &\rightsquigarrow \exists \Diamond b\end{aligned}$$

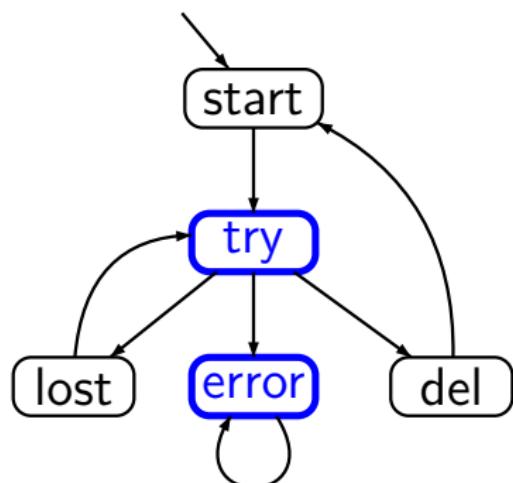
$$fair = \Box \Diamond \exists \Diamond \text{del} \rightsquigarrow \Box \Diamond c \text{ where } Sat(c) = S \setminus \{\text{error}\}$$

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

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

Example: CTL model checking with fairness

CTLFAIR4.4-31



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

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

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

$$\rightsquigarrow \exists \Diamond b$$

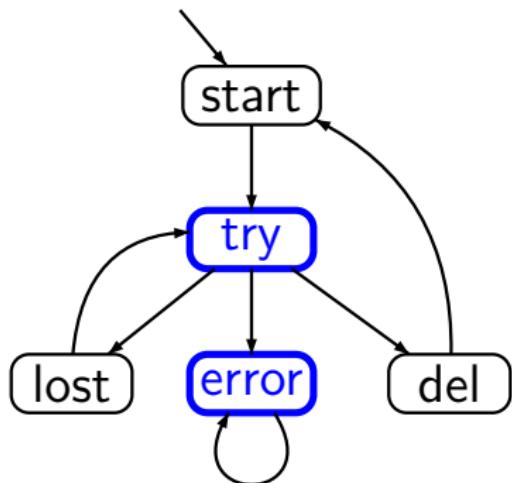
$$fair = \square \Diamond \exists \Diamond \text{del} \rightsquigarrow \square \Diamond c \text{ where } Sat(c) = S \setminus \{\text{error}\}$$

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

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

Example: CTL model checking with fairness

CTLFAIR4.4-31



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

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

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

$$\rightsquigarrow \exists \Diamond b$$

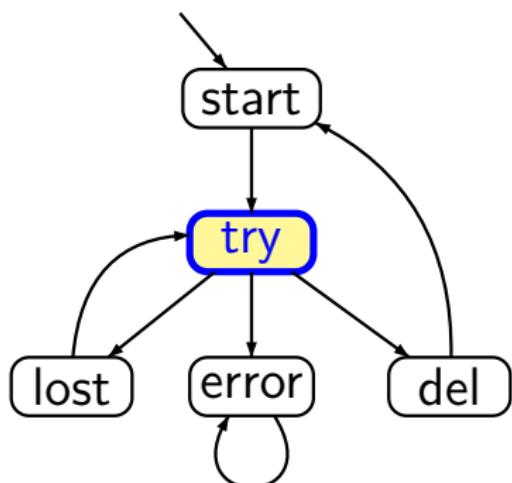
$$fair = \square \Diamond \exists \Diamond \text{del} \rightsquigarrow \square \Diamond c \text{ where } Sat(c) = S \setminus \{\text{error}\}$$

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

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

Example: CTL model checking with fairness

CTLFAIR4.4-31



$$\begin{aligned}\Phi &= \exists \Diamond \forall \bigcirc (\text{lost} \vee \text{del}) \\ &\equiv \exists \Diamond \neg \exists \bigcirc (\neg \text{lost} \wedge \neg \text{del}) \\ &\rightsquigarrow \exists \Diamond \neg \exists \bigcirc a \\ &\rightsquigarrow \exists \Diamond b\end{aligned}$$

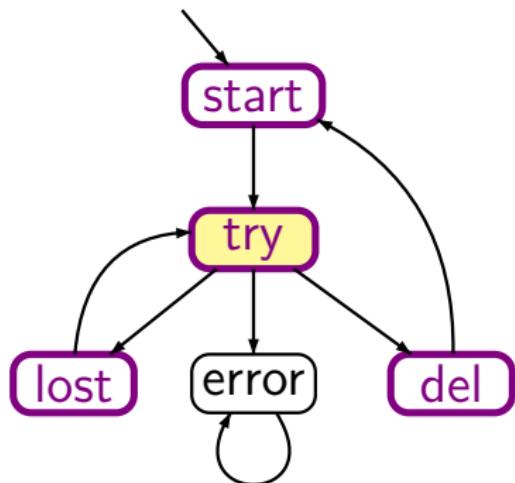
$$fair = \Box \Diamond \exists \Diamond \text{del} \rightsquigarrow \Box \Diamond c \text{ where } Sat(c) = S \setminus \{\text{error}\}$$

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

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

Example: CTL model checking with fairness

CTLFAIR4.4-31



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

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

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

$$\rightsquigarrow \exists \Diamond b$$

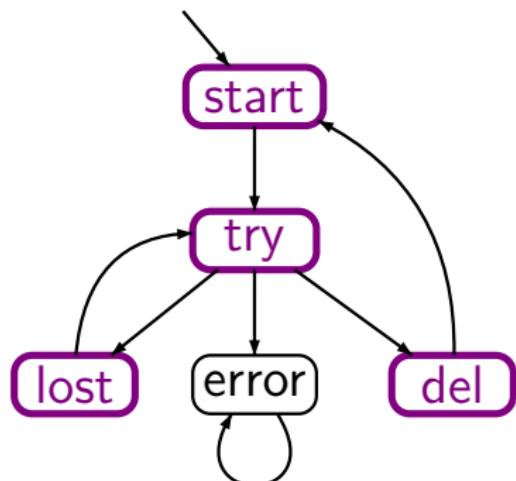
$$fair = \Box \Diamond \exists \Diamond \text{del} \rightsquigarrow \Box \Diamond c \text{ where } Sat(c) = S \setminus \{\text{error}\}$$

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

$$\begin{aligned} Sat_{fair}(\exists \Diamond b) &= Sat(\exists \Diamond (b \wedge a_{fair})) \\ &= \{\text{start}, \text{try}, \text{lost}, \text{del}\} \end{aligned}$$

Example: CTL model checking with fairness

CTLFAIR4.4-31



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

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

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

$$\rightsquigarrow \exists \Diamond b$$

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

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

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

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

Correct or wrong?

CTLFAIR4.4-32

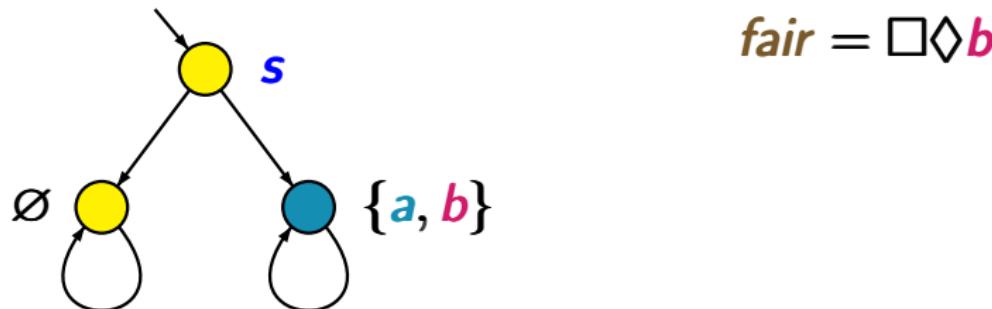
$$s \models_{\text{fair}} \forall \bigcirc a \quad \text{iff} \quad s \models \forall \bigcirc (a \wedge a_{\text{fair}})$$

Correct or wrong?

CTLFAIR4.4-32

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

wrong.

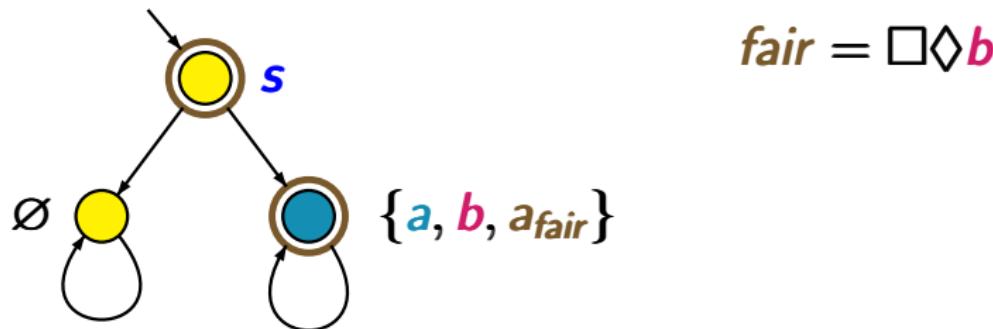


Correct or wrong?

CTLFAIR4.4-32

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

wrong.

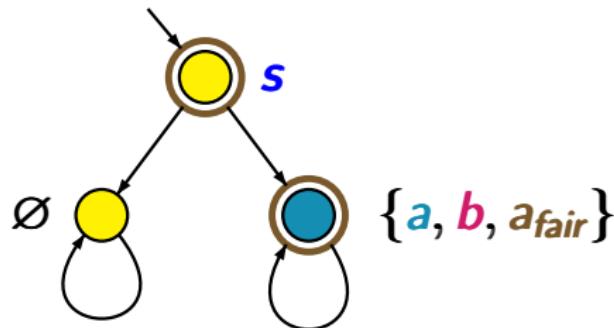


Correct or wrong?

CTLFAIR4.4-32

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

wrong.



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

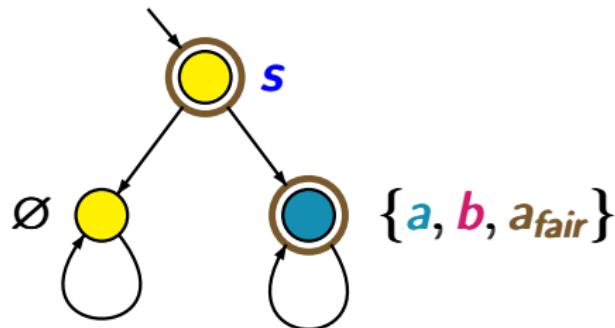
$$s \not\models \forall \bigcirc (a \wedge a_{\text{fair}})$$

Correct or wrong?

CTLFAIR4.4-32

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

wrong.



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

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

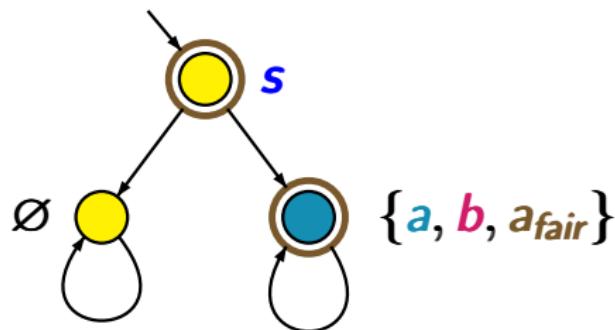
$$s \models_{\text{fair}} \forall \bigcirc a$$

Correct or wrong?

CTLFAIR4.4-32

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

wrong.



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

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

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

but correct is:

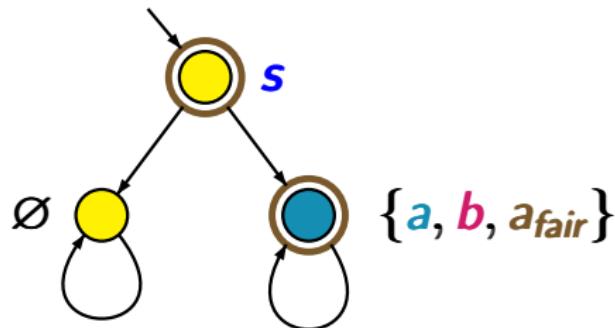
$$s \models_{\text{fair}} \forall \bigcirc a \text{ iff } ?$$

Correct or wrong?

CTLFAIR4.4-32

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

wrong.



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

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

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

but correct is:

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

Correct or wrong?

CTLFAIR4.4-32B

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

Correct or wrong?

CTLFAIR4.4-32B

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

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

Correct or wrong?

CTLFAIR4.4-32B

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

CTLFAIR4.4-32B

$s \models_{\text{fair}} \forall \Box a$ iff $s \models \forall \Box(a_{\text{fair}} \rightarrow a)$
iff there is no state s' reachable
from s with $s' \models \neg a \wedge a_{\text{fair}}$

correct

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

Correct or wrong?

CTLFAIR4.4-32B

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

Correct or wrong?

CTLFAIR4.4-32B

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

Correct or wrong?

CTLFAIR4.4-32B

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

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

correct

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

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

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

Correct or wrong?

CTLFAIR4.4-32B

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

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

correct

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

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

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

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

Correct or wrong?

CTLFAIR4.4-32B

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

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

correct

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

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

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

$$\text{iff } s \models \neg \exists \Diamond(\neg a \wedge a_{\text{fair}}) \equiv \forall \Box(a_{\text{fair}} \rightarrow a)$$

Summary

CTLFAIR4.4-32A

We just saw:

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

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

Correct or wrong?

CTLFAIR4.4-32A

We just saw:

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

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

Is the following statement correct ?

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

Correct or wrong?

CTLFAIR4.4-32A

We just saw:

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

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

Is the following statement correct ?

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

wrong.

Correct or wrong?

CTLFAIR4.4-33

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

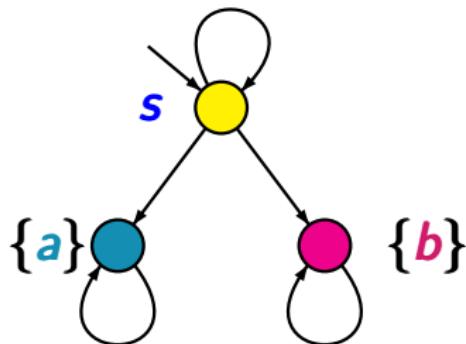
Correct or wrong?

CTLFAIR4.4-33

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

wrong.

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



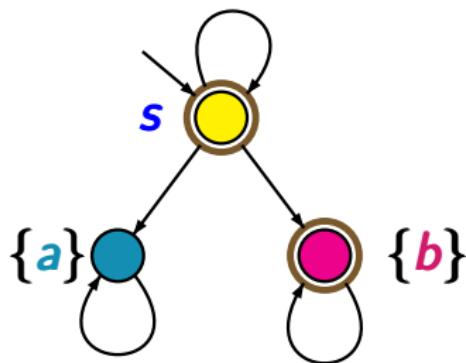
Correct or wrong?

CTLFAIR4.4-33

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

wrong.

$$\text{fair} = \Box \lozenge b$$

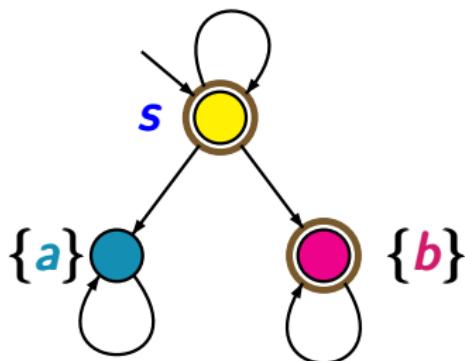


Correct or wrong?

CTLFAIR4.4-33

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

wrong.



$$\text{fair} = \Box \lozenge b$$

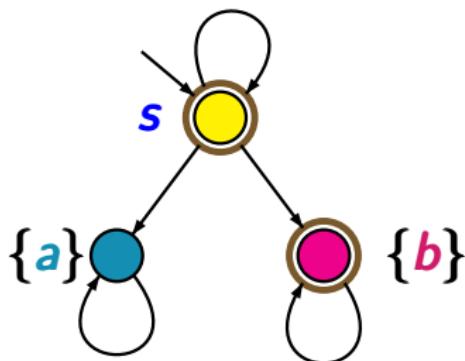
$$s \models \exists \bigcirc ((\exists \lozenge a) \wedge a_{\text{fair}})$$

Correct or wrong?

CTLFAIR4.4-33

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

wrong.



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

$$s \models \exists \bigcirc ((\exists \lozenge a) \wedge a_{\text{fair}})$$

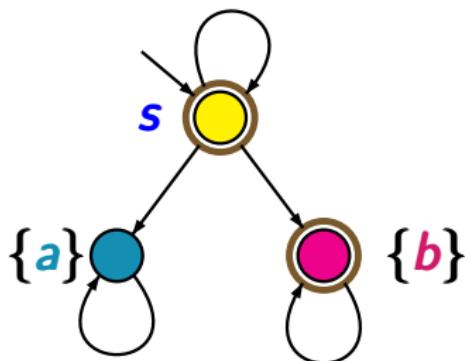
regard $s \rightarrow s$

Correct or wrong?

CTLFAIR4.4-33

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

wrong.



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

$$s \models \exists \bigcirc ((\exists \lozenge a) \wedge a_{\text{fair}})$$

regard $s \rightarrow s$

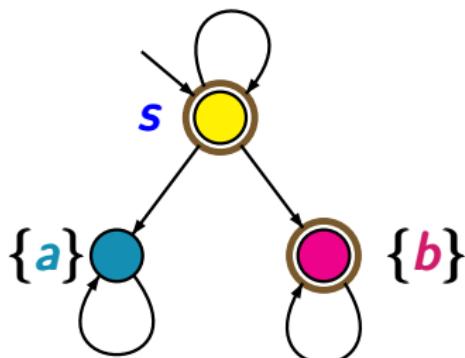
$$s \not\models_{\text{fair}} \exists \bigcirc \exists \lozenge a$$

Correct or wrong?

CTLFAIR4.4-33

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

wrong.



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

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

regard $s \rightarrow s$

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

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

Correct or wrong?

CTLFAIR4.4-33

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

wrong.

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

remind: W = weak until

Correct or wrong?

CTLFAIR4.4-33

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

wrong.

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

remind: W = weak until

wrong.

Correct or wrong?

CTLFAIR4.4-33

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

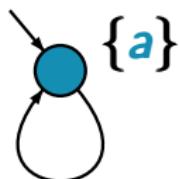
wrong.

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

remind: W = weak until

wrong.

$$\text{fair} = \Box \lozenge b$$



Correct or wrong?

CTLFAIR4.4-33

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

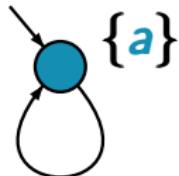
wrong.

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

remind: W = weak until

wrong.

$$\text{fair} = \Box \lozenge b$$



$$s \models \exists (a W (c \wedge a_{\text{fair}}))$$

Correct or wrong?

CTLFAIR4.4-33

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

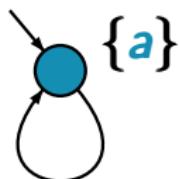
wrong.

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

remind: W = weak until

wrong.

$$\text{fair} = \Box \lozenge b$$



$$s \models \exists (a W (c \wedge a_{\text{fair}}))$$

$$s \not\models_{\text{fair}} \exists (a W c)$$

Summary: fairness in CTL

CTLFAIR4.4-34

CTL fairness assumptions: formulas similar to **LTL**

e.g., $\text{fair} = \bigwedge_{1 \leq i \leq k} (\square \lozenge \Psi_i \rightarrow \square \lozenge \Phi_i)$

CTL fairness assumptions: formulas similar to **LTL**

e.g., $\text{fair} = \bigwedge_{1 \leq i \leq k} (\square \Diamond \Psi_i \rightarrow \square \Diamond \Phi_i)$

CTL satisfaction relation with fairness:

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

CTL fairness assumptions: formulas similar to **LTL**

$$\text{e.g., } \mathbf{fair} = \bigwedge_{1 \leq i \leq k} (\square \Diamond \Psi_i \rightarrow \square \Diamond \Phi_i)$$

CTL satisfaction relation with fairness:

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

model checking for **CTL** with fairness:

CTL fairness assumptions: formulas similar to **LTL**

$$\text{e.g., } \mathbf{fair} = \bigwedge_{1 \leq i \leq k} (\square \Diamond \Psi_i \rightarrow \square \Diamond \Phi_i)$$

CTL satisfaction relation with fairness:

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

model checking for **CTL** with fairness:

- $\exists \bigcirc, \exists \mathbb{U}, \forall \bigcirc, \forall \square$ via **CTL** model checker

CTL fairness assumptions: formulas similar to **LTL**

e.g., $\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box\Diamond\Psi_i \rightarrow \Box\Diamond\Phi_i)$

CTL satisfaction relation with fairness:

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

model checking for **CTL** with fairness:

- $\exists\bigcirc, \exists\mathbb{U}, \forall\bigcirc, \forall\Box$ via **CTL** model checker
- analysis of **SCCs** for $\exists\Box, \forall\mathbb{U}$

CTL fairness assumptions: formulas similar to **LTL**

e.g., $\text{fair} = \bigwedge_{1 \leq i \leq k} (\square \lozenge \Psi_i \rightarrow \square \lozenge \Phi_i)$

CTL satisfaction relation with fairness:

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

model checking for **CTL** with fairness:

- $\exists \bigcirc, \exists \mathbf{U}, \forall \bigcirc, \forall \square$ via **CTL** model checker
- analysis of **SCCs** for $\exists \square, \forall \mathbf{U}$
- complexity: $\mathcal{O}(\text{size}(\mathcal{T}) \cdot |\Phi| \cdot |\text{fair}|)$