Overview

Complexity of CTL and LTL model checking

Complexity of CTL and LTL model checking

LTL model checking problem:

PSPACE-complete and solvable in time

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

CTL model checking problem:

solvable in polynomial time

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

Complexity of CTL and LTL model checking

LTL model checking problem:

PSPACE-complete and solvable in time

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

CTL model checking problem:

solvable in polynomial time (even PTIME-complete)

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

Complexity of CTL and LTL model checking

LTL model checking problem:

PSPACE-complete and solvable in time

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

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

CTL model checking problem:

solvable in polynomial time (even PTIME-complete)

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

Complexity of CTL and LTL model checking

LTL model checking problem:

PSPACE-complete and solvable in time

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

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

CTL model checking problem:

solvable in polynomial time (even PTIME-complete)

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

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

Recall: LTL fairness assumptions

Recall: LTL fairness assumptions

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

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

where ϕ, ψ are propositional formulas

Recall: LTL fairness assumptions

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

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

where ϕ, ψ are propositional formulas

Recall: LTL fairness assumptions

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

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

where ϕ, ψ are propositional formulas

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

Recall: LTL fairness assumptions

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

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

where 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

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 $\mathcal{T}$

iff for all paths π in $\mathcal{T}$:

$\pi \models fair \rightarrow \varphi$

Recall: LTL fairness assumptions

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

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

where ϕ, ψ are propositional formulas

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

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

iff for all paths π in $\mathcal{T}$:

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

Recall: LTL fairness assumptions

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

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

where ϕ, ψ are propositional formulas

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

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

iff for all paths π in $\mathcal{T}$:

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

CTL fairness assumptions

CTL fairness assumptions

conjunctions of "formulas" of the type

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

where Ψ, Φ are CTL state formulas

CTL fairness assumptions

conjunctions of "formulas" of the type

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

where 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

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:

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

where Ψ_j, Φ_j are CTL state formulas

Satisfaction relation for CTL with fairness

Satisfaction relation for CTL with fairness

$s \models_{fair} true$

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

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

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

Satisfaction relation for CTL with fairness

$s \models_{fair} true$

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

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

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

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

Satisfaction relation for CTL with fairness

$s \models_{fair} true$

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

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

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

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

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

Satisfaction relation for CTL with fairness

$s \models_{fair} true$

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

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

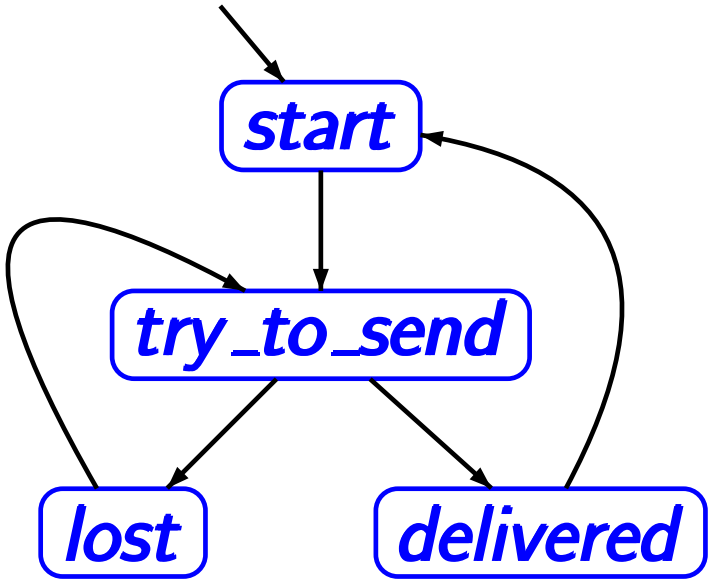
$s \models_{fair} \Phi_1 \wedge \Phi_2$ iff $s \models_{fair} \Phi_1$ and $s \models_{fair} \Phi_2$

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

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

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

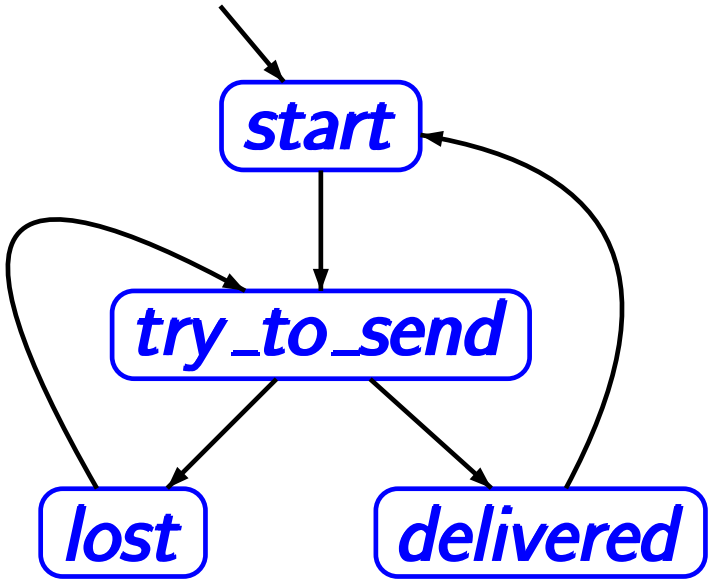
Simple communication protocol



CTL formula

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

Simple communication protocol

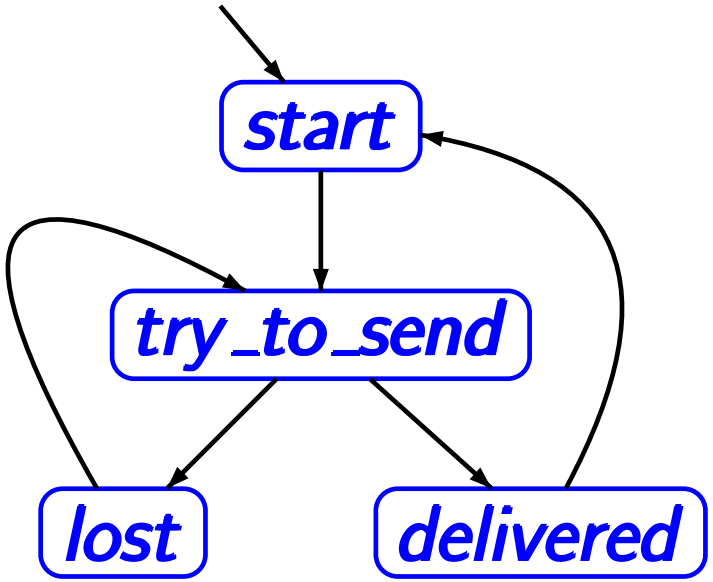


CTL formula

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

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

Simple communication protocol



CTL formula

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

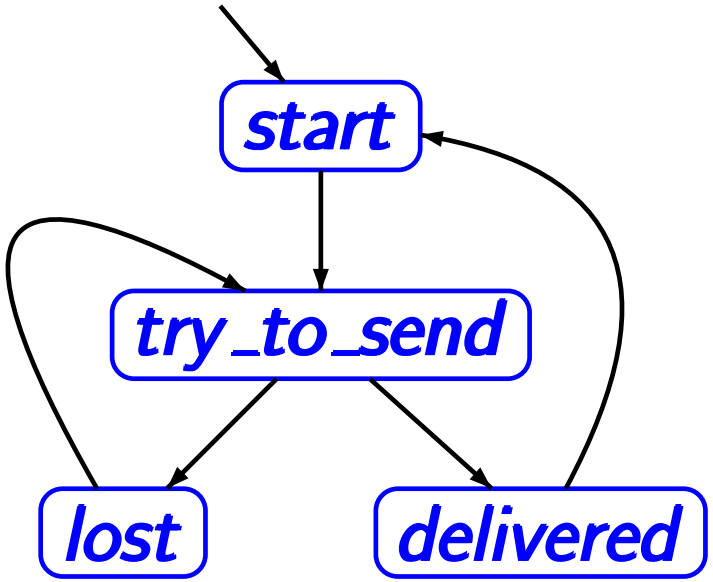
$\mathcal{T} \not\models \Phi$

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

unconditional CTL fairness assumption:

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

Simple communication protocol



CTL formula

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

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

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

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

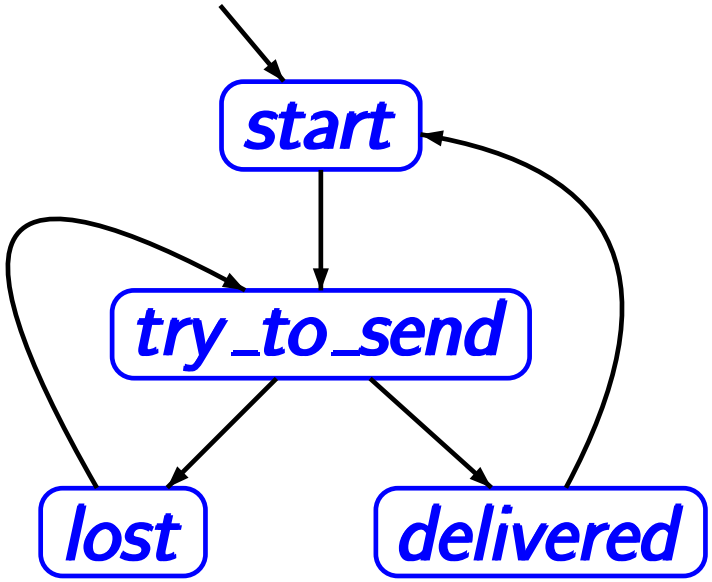
unconditional CTL fairness assumption:

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

strong CTL fairness assumption:

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

Simple communication protocol

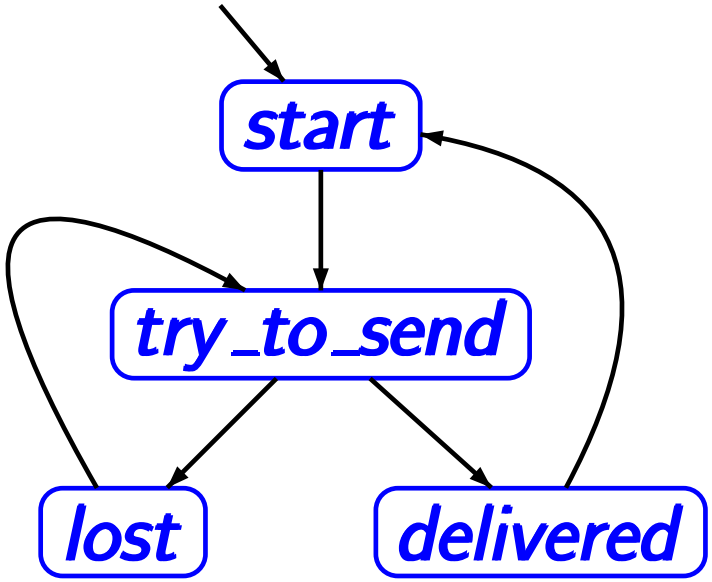


$\Phi = \forall\Box\forall\Diamond start$

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

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

Simple communication protocol



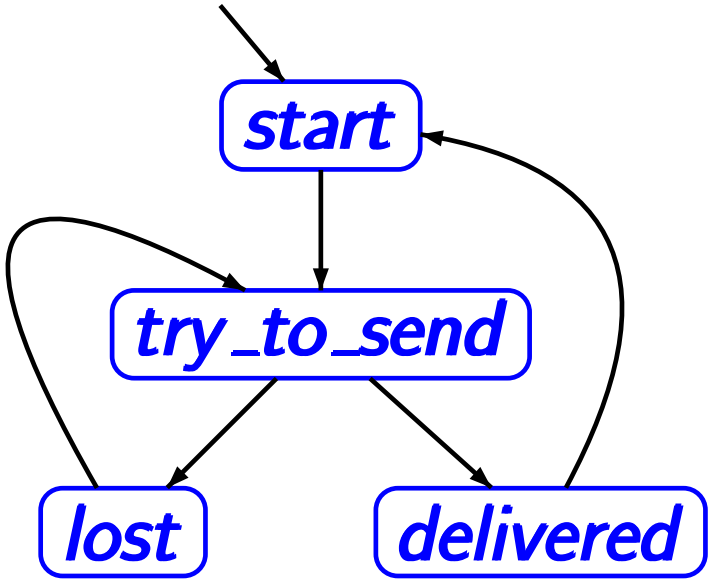
$\Phi = \forall\Box\forall\Diamond start$

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

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

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

Simple communication protocol



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

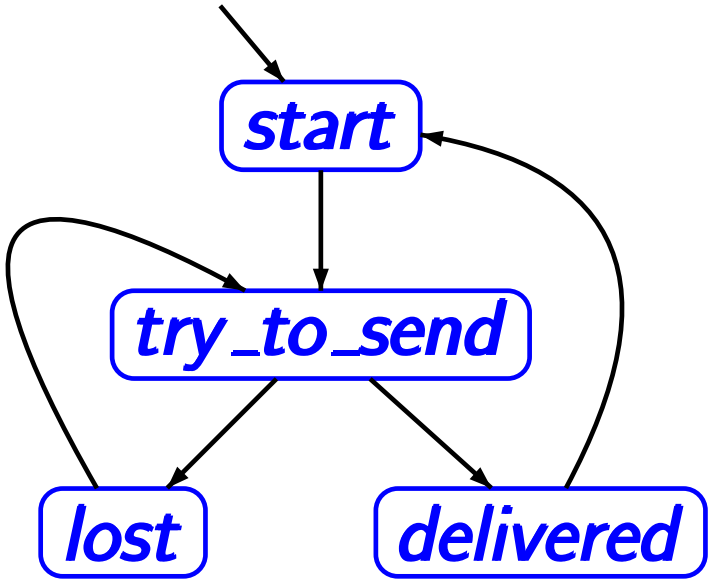
$\mathcal{T} \models_{ufair} \Phi$?

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

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

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

Simple communication protocol



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

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

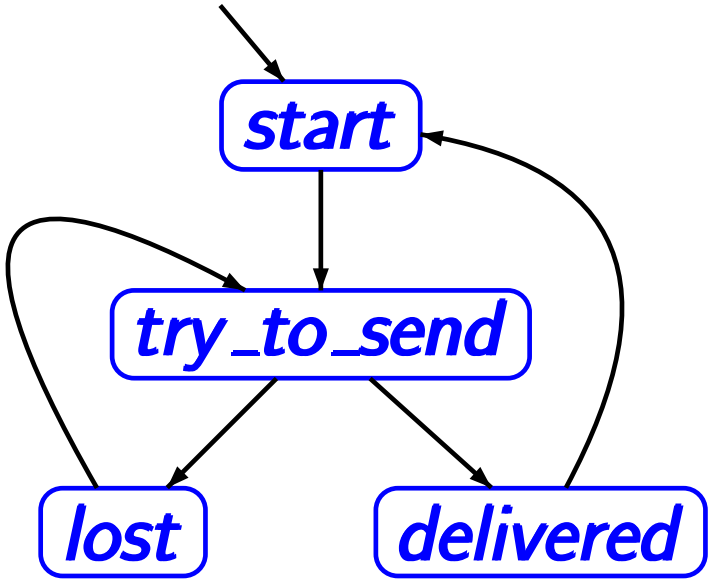
unconditional fairness: $ufair = \Box\Diamond\, \exists\bigcirc start$

$\uparrow$

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

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

Simple communication protocol



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

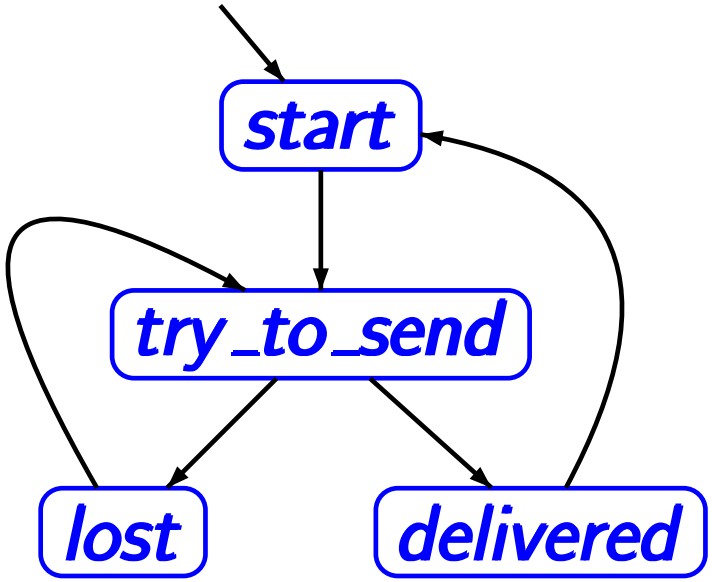
$\mathcal{T} \models_{\mathit{ufair}} \Phi$ $\surd$

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

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

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

Simple communication protocol



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

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

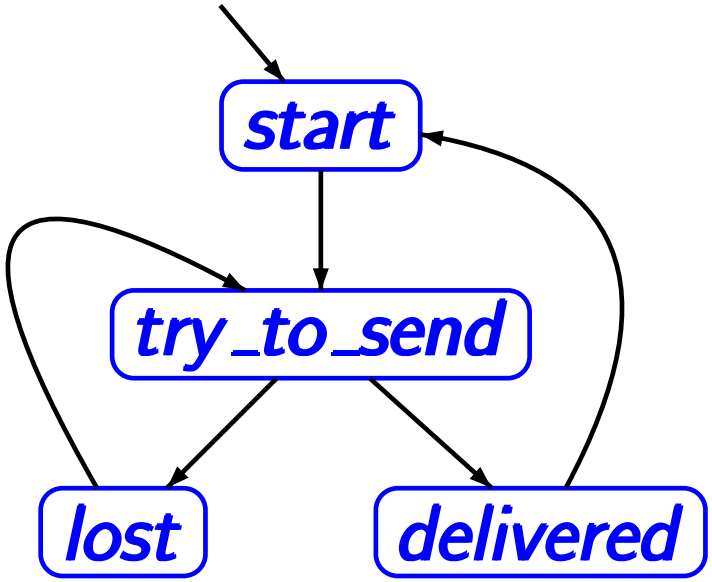
$\mathcal{T} \models_{wfair} \Phi$?

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

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

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

Simple communication protocol



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

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

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

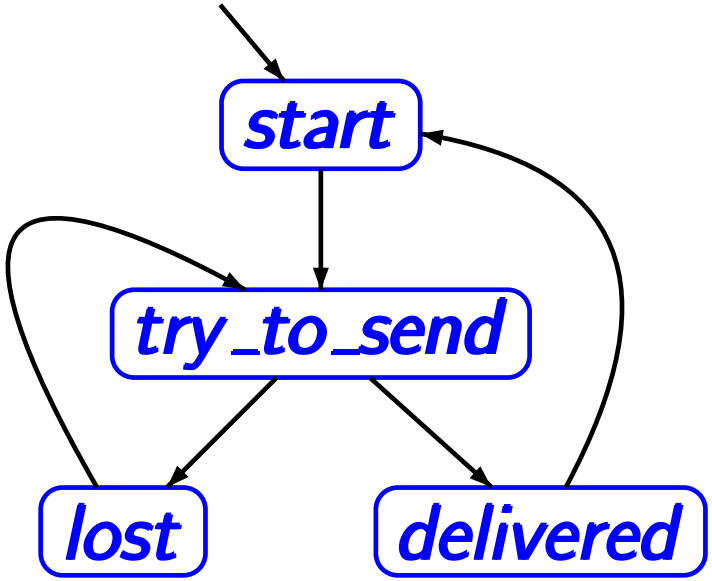
unconditional fairness: $ufair = \Box\Diamond\exists\bigcirc start$

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

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

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

Simple communication protocol



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

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

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

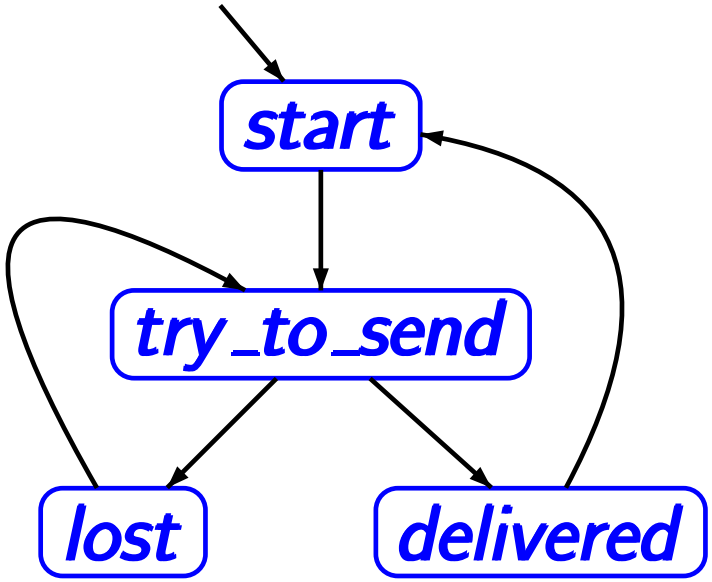
unconditional fairness: $ufair = \Box\Diamond\, \exists\bigcirc start$

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

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

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

Simple communication protocol



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

$\mathcal{T} \models_{ufair} \Phi$ ✓

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

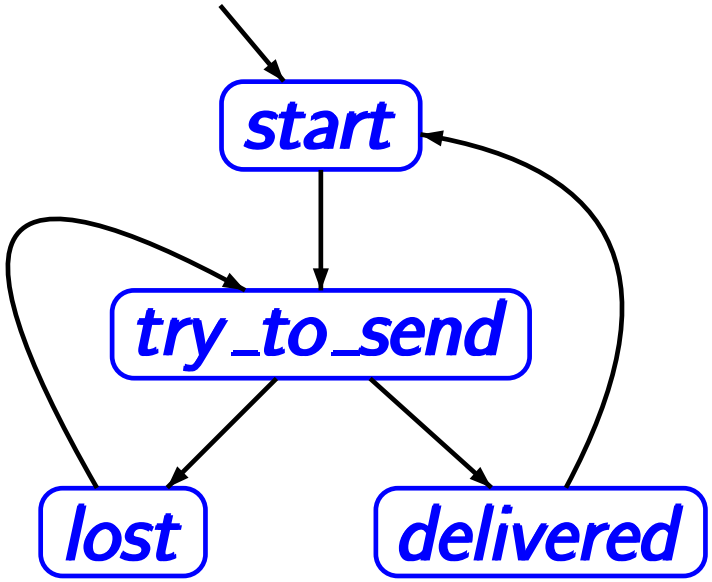
$\mathcal{T} \models_{sfair} \Phi$?

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

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

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

Simple communication protocol



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

$\mathcal{T} \models_{ufair} \Phi$ ✓

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

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

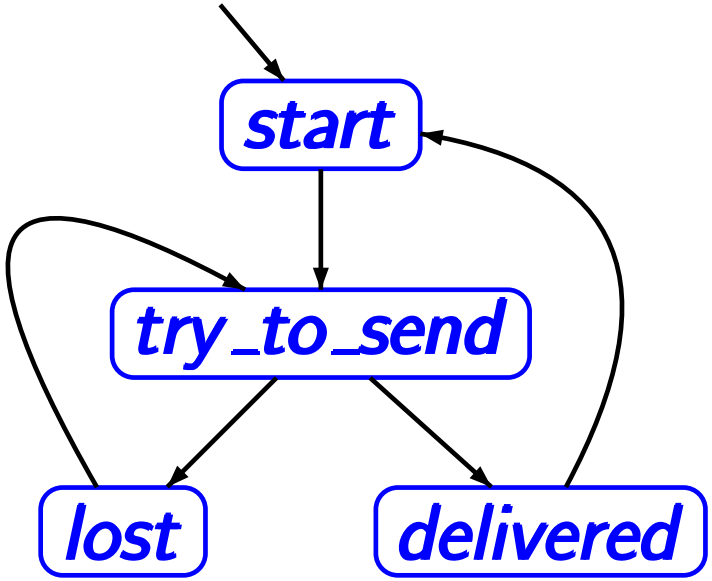
unconditional fairness: $ufair = \Box\Diamond\, \exists\bigcirc start$

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

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

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

Simple communication protocol



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

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

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

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

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

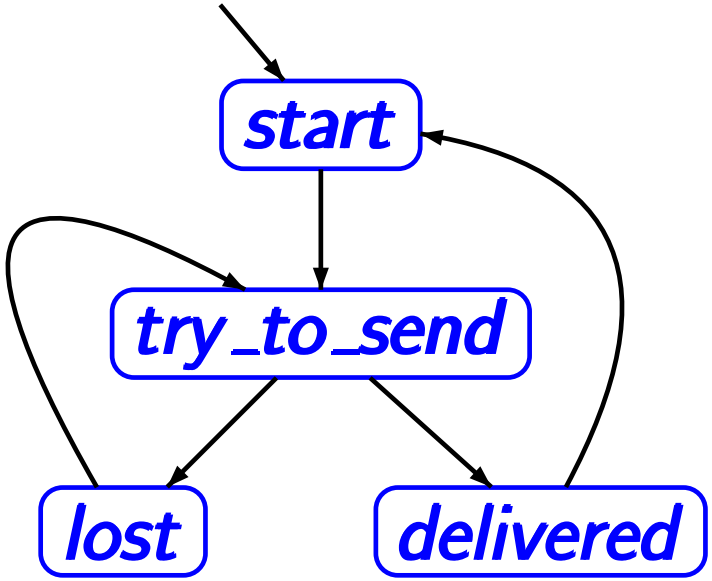
weak fairness: $wfair = \Diamond\Box\, \exists\bigcirc delivered \rightarrow \Box\Diamond delivered$

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

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

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

Simple communication protocol



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

$\mathcal{T} \models_{ufair} \Phi$ ✓

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

$\mathcal{T} \models_{sfair} \Phi$ ✓

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

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

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

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

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

Correct or wrong?

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

Correct or wrong?

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

correct.

Correct or wrong?

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

correct. Note that:

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

Correct or wrong?

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

correct. Note that:

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

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

Correct or wrong?

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

correct. Note that:

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

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

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

Correct or wrong?

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

correct.

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

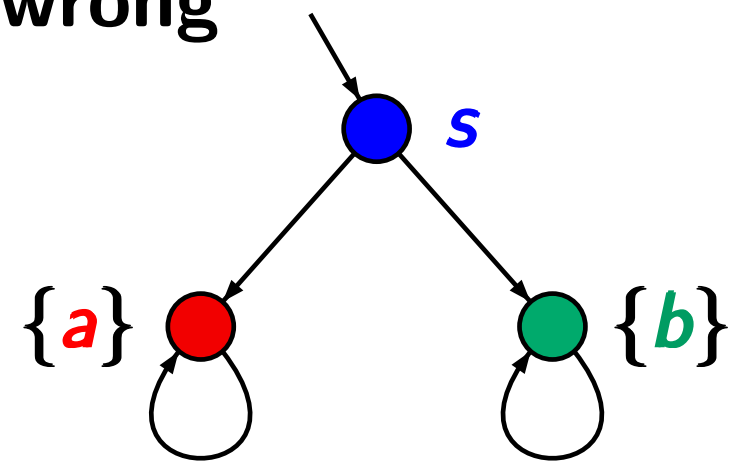
Correct or wrong?

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

correct.

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

wrong



$fair = \Box\Diamond b$

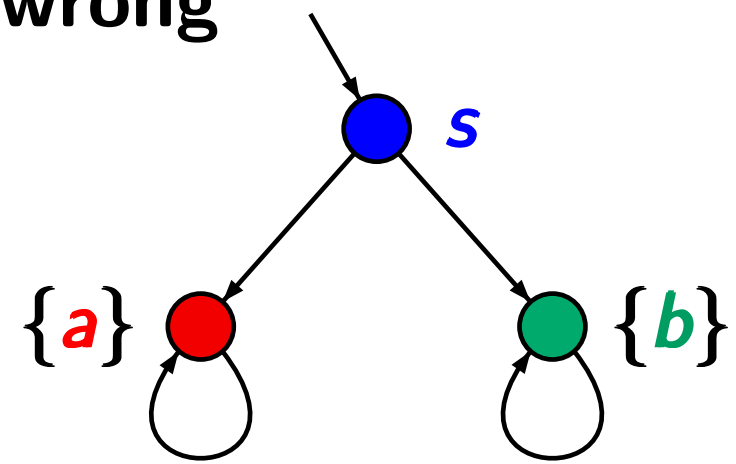
Correct or wrong?

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

correct.

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

wrong



$fair = \Box\Diamond b$

just one fair path ● ● ● ● . . .

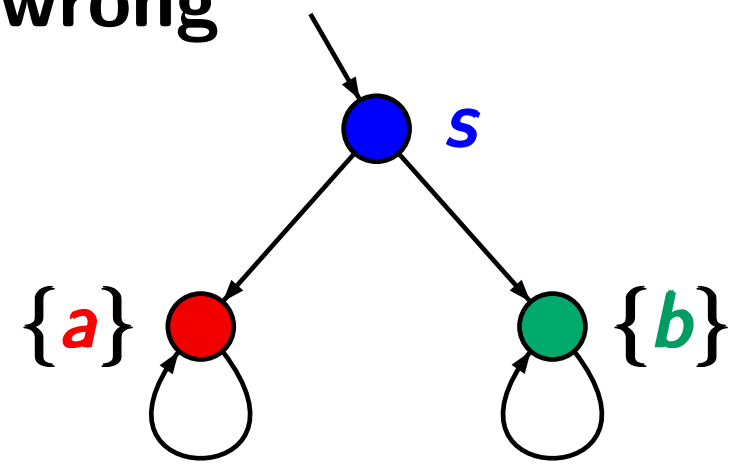
Correct or wrong?

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

correct.

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 ● ● ● ● . . .

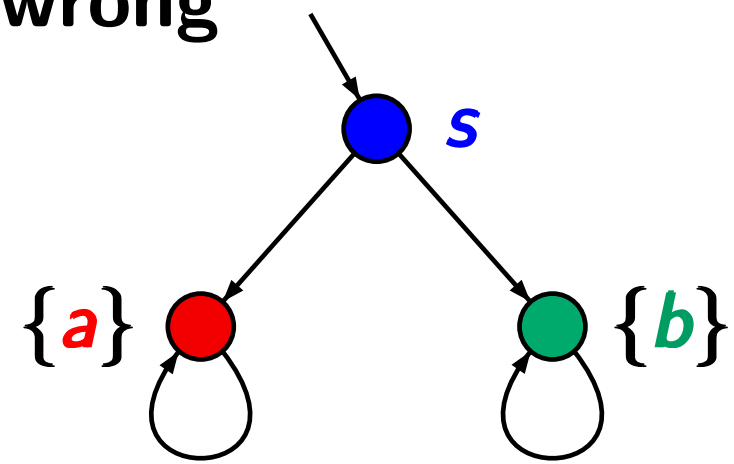
Correct or wrong?

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

correct.

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

wrong



$fair = \Box\Diamond b$

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

$s \models \exists\Diamond a$

just one fair path ● ● ● ● . . .

Correct or wrong?

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

correct.

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

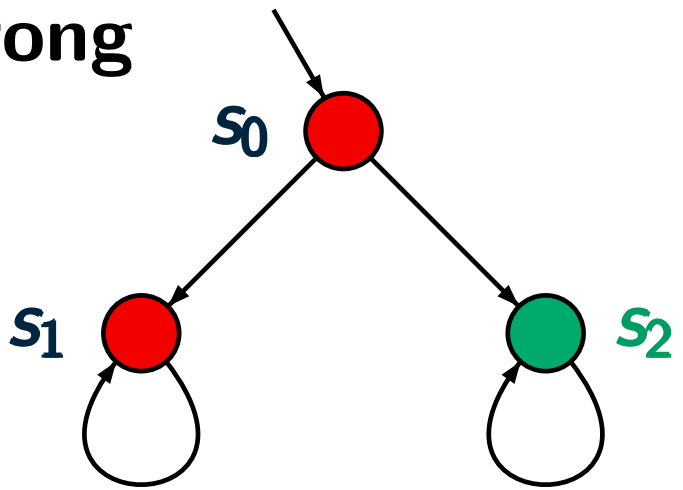
Correct or wrong?

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

Correct or wrong?

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

wrong



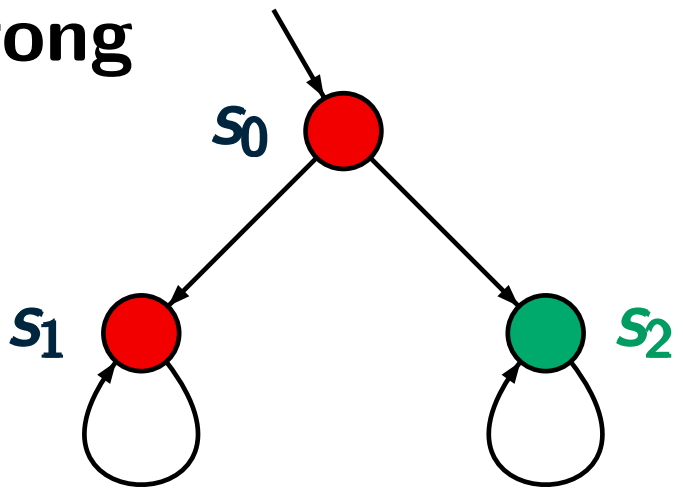
● $= \{b\}$

● $= \{a\}$

Correct or wrong?

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

wrong



● $= \{b\}$

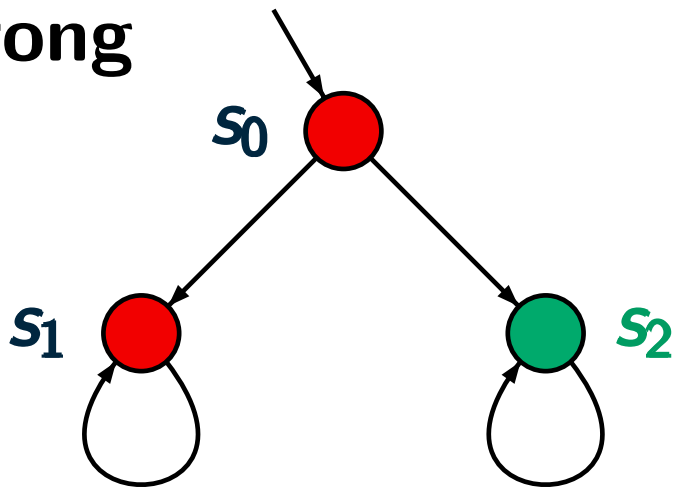
● $= \{a\}$

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

Correct or wrong?

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

wrong



● $= \{b\}$

● $= \{a\}$

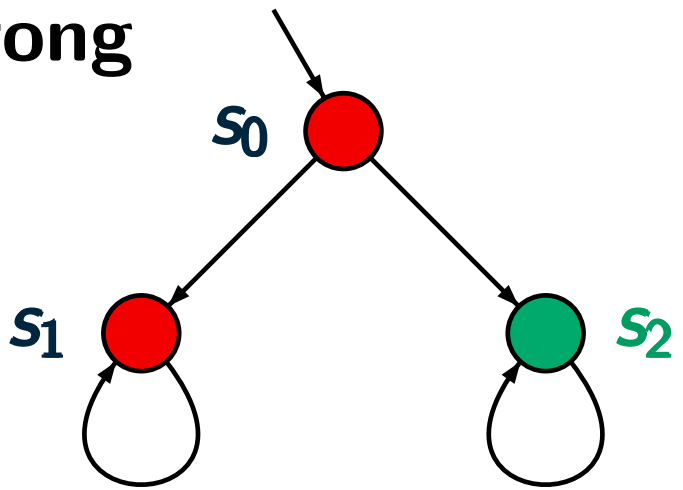
$Sat(\exists\Box a) = \{s_0, s_1\}$

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

Correct or wrong?

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

wrong



● $= \{b\}$

● $= \{a\}$

$fair = \Box\Diamond b$

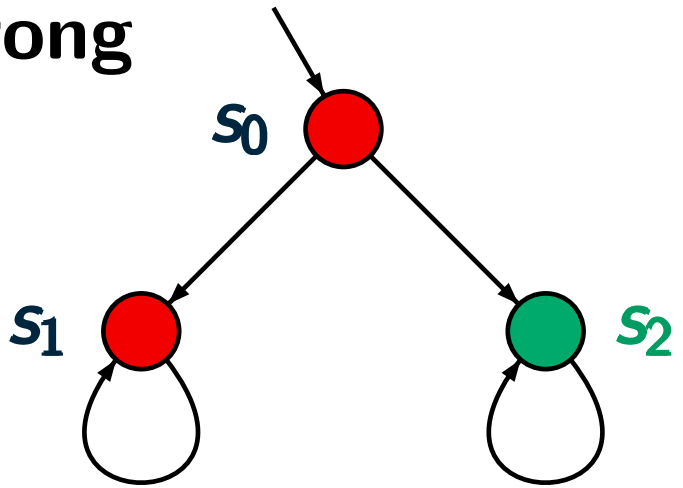
$Sat(\exists\Box a) = \{s_0, s_1\}$

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

Correct or wrong?

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

wrong



$\bigcirc = \{b\}$

$\bigcirc = \{a\}$

$fair = \Box\Diamond b$

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

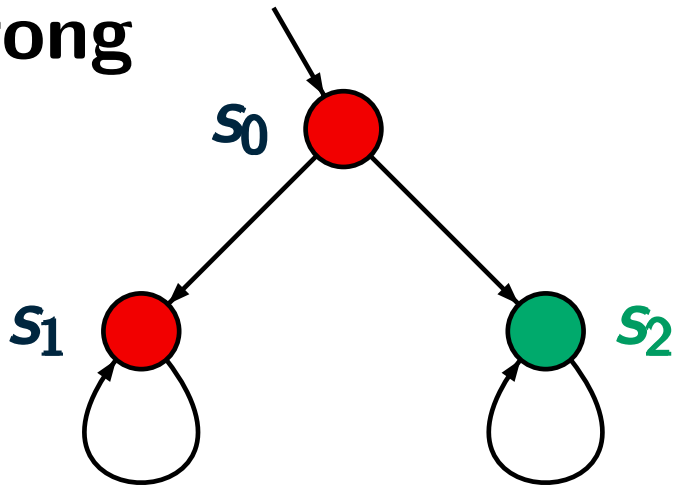
$Sat_{fair}(\exists\Box a) = \varnothing$

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

Correct or wrong?

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

wrong



$= \{b\}$

$= \{a\}$

$fair = \Box\Diamond b$

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

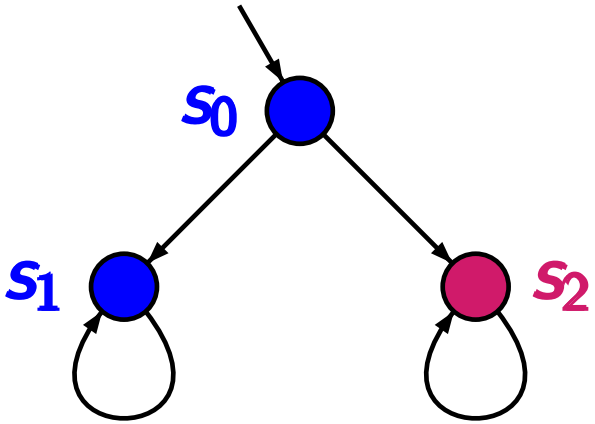
$Sat_{fair}(\exists\Box a) = \varnothing$

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

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

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

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

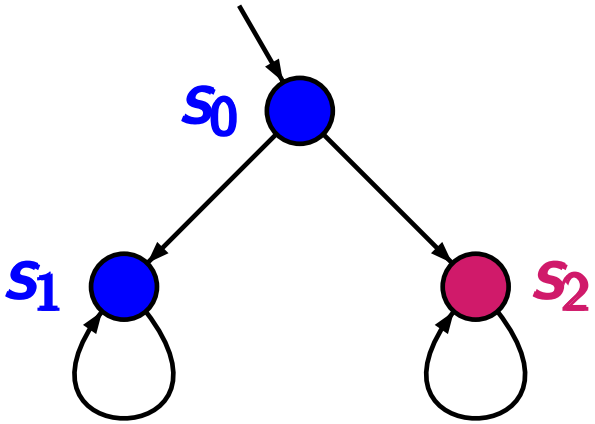


● $= \{a\}$

● $= \varnothing$

$fair = \Box\Diamond a$

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



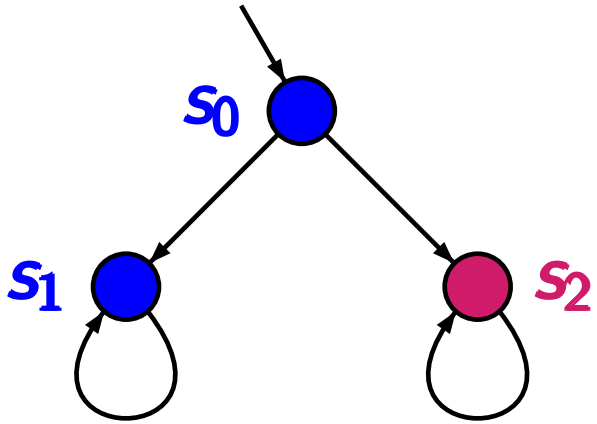
● $= \{a\}$

● $= \varnothing$

$fair = \Box\Diamond a$

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

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



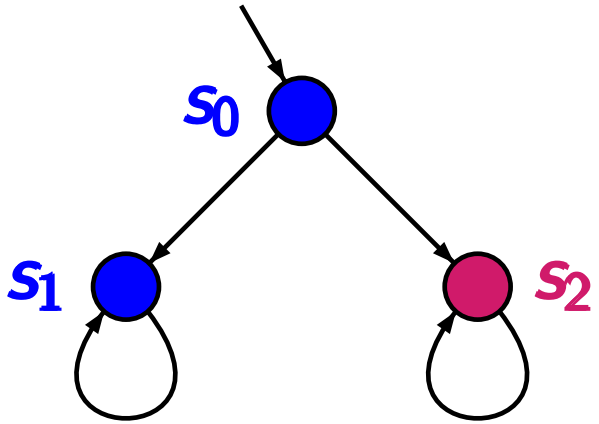
● $= \{a\}$

● $= \varnothing$

$fair = \Box\Diamond a$

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

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



● $= \{a\}$

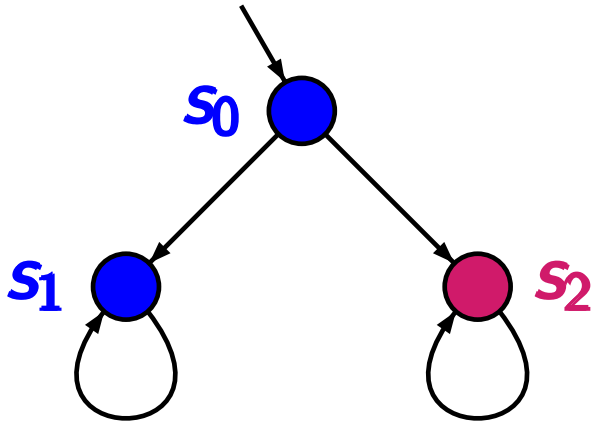
● $= \varnothing$

$fair = \Box\Diamond a$

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

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

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



● $= \{a\}$

● $= \varnothing$

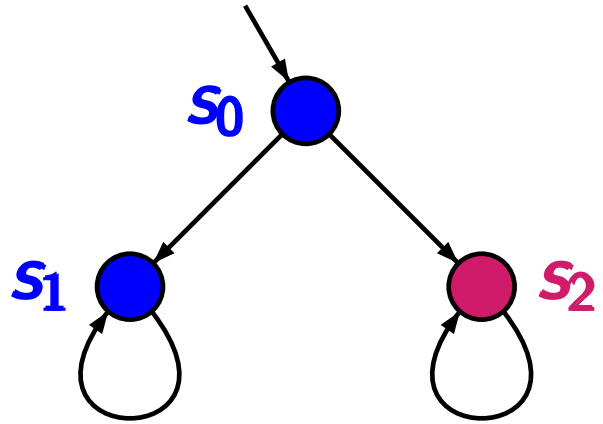
$fair = \Box\Diamond a$

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

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

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

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



● $= \{a\}$

● $= \varnothing$

$fair = \Box\Diamond a$

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

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

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

fair is realizable iff

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

Model checking problem for FairCTL

Model checking problem for FairCTL

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

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

Model checking problem for FairCTL

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

CTL formula Φ

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

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

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

Model checking problem for FairCTL

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

CTL formula Φ

CTL fairness assumption fair, e.g.,

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

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

for simplicity:

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

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

Preprocessing of FairCTL model checking

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

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

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

Preprocessing of FairCTL model checking

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

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

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

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

Preprocessing of FairCTL model checking

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

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

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

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

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

Preprocessing of FairCTL model checking

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

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

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

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

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

Preprocessing of FairCTL model checking

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

CTL formula Φ in $\exists$-normal form

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

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

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

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

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

Idea of FairCTL model checking

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

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

1. ... preprocessing ...

Idea of FairCTL model checking

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

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

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

Idea of FairCTL model checking

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

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

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

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

Idea of FairCTL model checking

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

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

recursive computation of the fair satisfaction sets:

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

recursive computation of the fair satisfaction sets:

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

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

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

Idea of FairCTL model checking

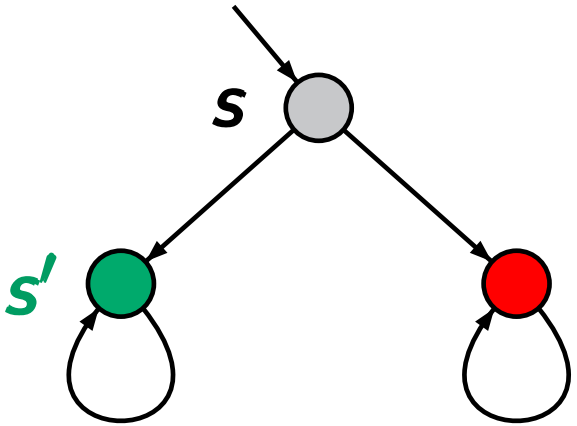
given: finite transition system $\mathcal{T}$
CTL formula Φ in $\exists$-normal form
CTL fairness assumption ***fair***

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

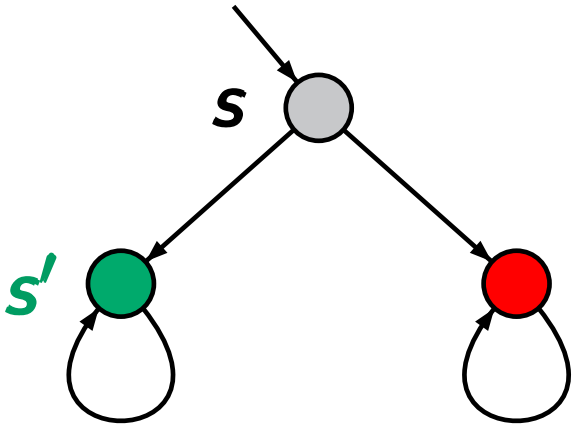
FairCTL model checking: treatment of $\exists\bigcirc$

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



$fair = \Box\Diamond red$

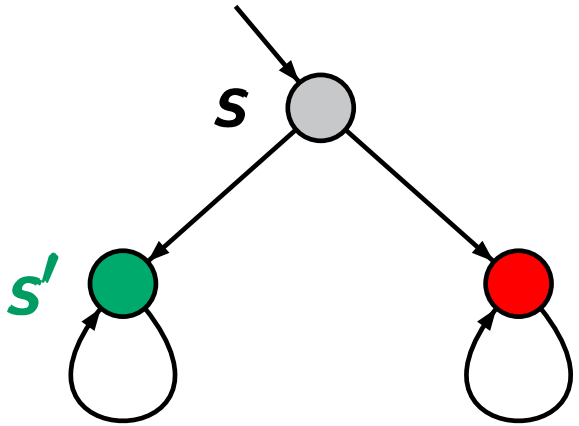
FairCTL model checking: treatment of $\exists\bigcirc$



$fair = \Box\Diamond red$

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

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

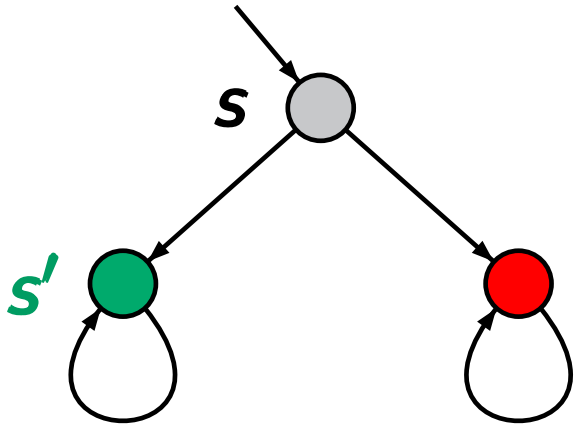


$fair = \Box\Diamond red$

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

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

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



$fair = \Box\Diamond red$

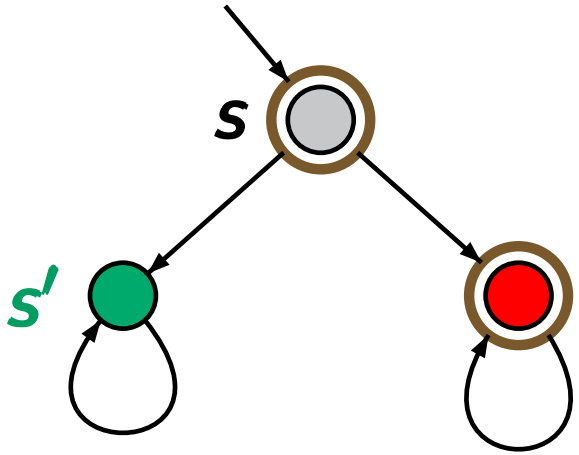
$s \not\models_{fair} \exists\bigcirc green$

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

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

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

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



$fair = \Box\Diamond red$

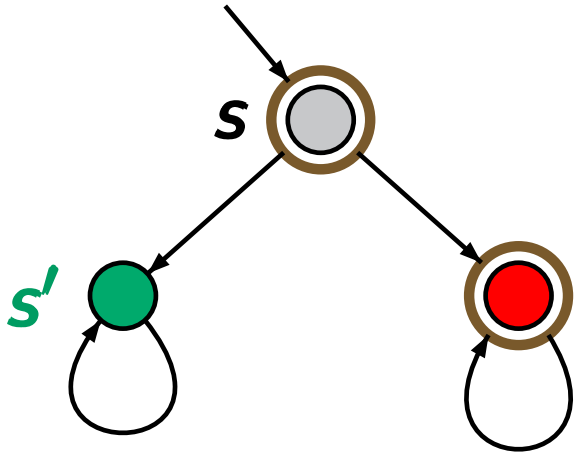
$s \not\models_{fair} \exists\bigcirc green$

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

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

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

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



$fair = \Box\Diamond red$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

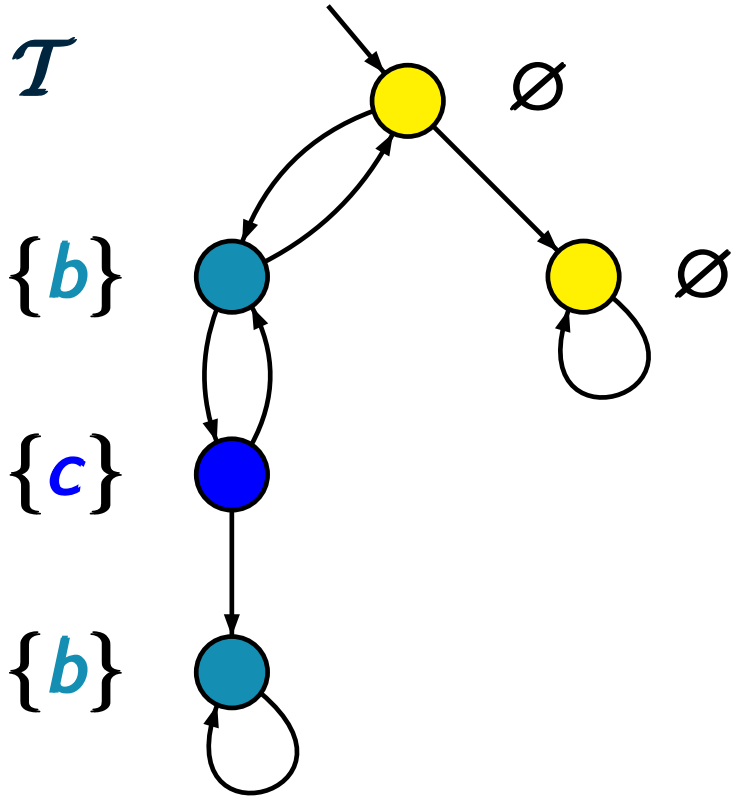
$$s \models_{fair} \exists\bigcirc b \quad \text{iff} \quad s \models \exists\bigcirc(b \wedge a_{fair})$$

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

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

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

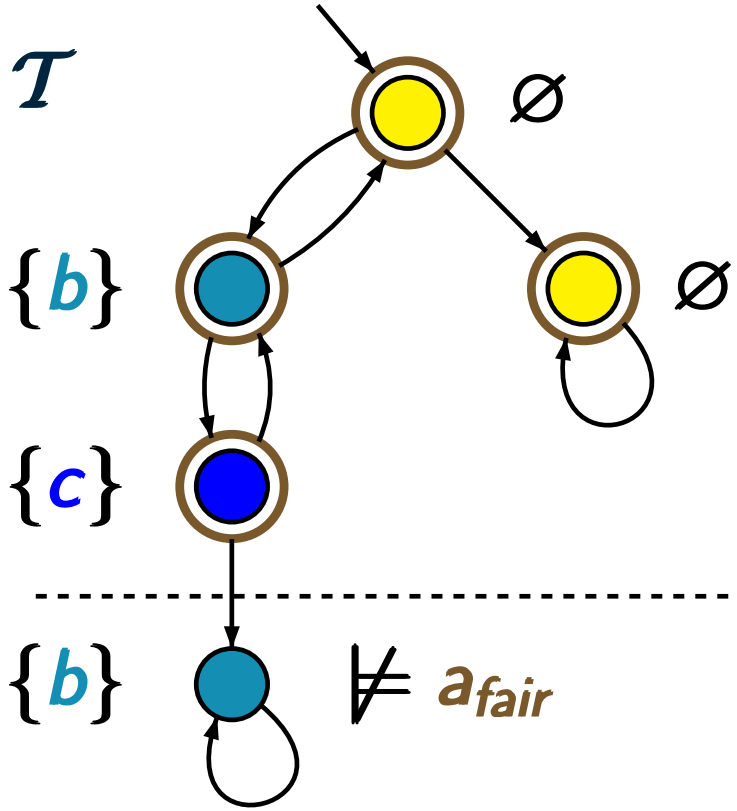
Example: treatment of $\exists\Diamond$



CTL formula $\exists\Diamond c$

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

Example: treatment of $\exists\Diamond$



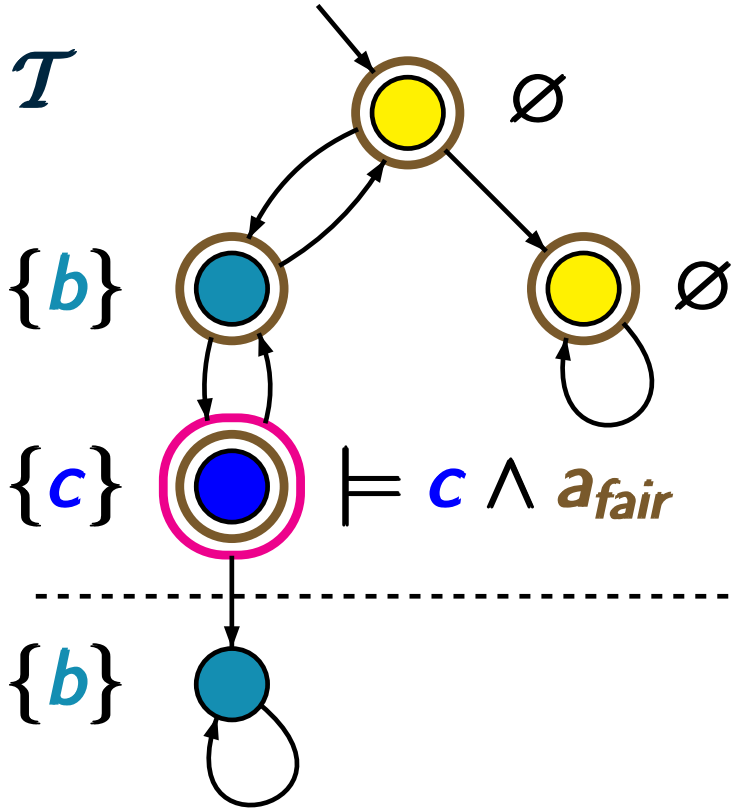
CTL formula $\exists\Diamond c$

$\downarrow$

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

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

Example: treatment of $\exists\Diamond$



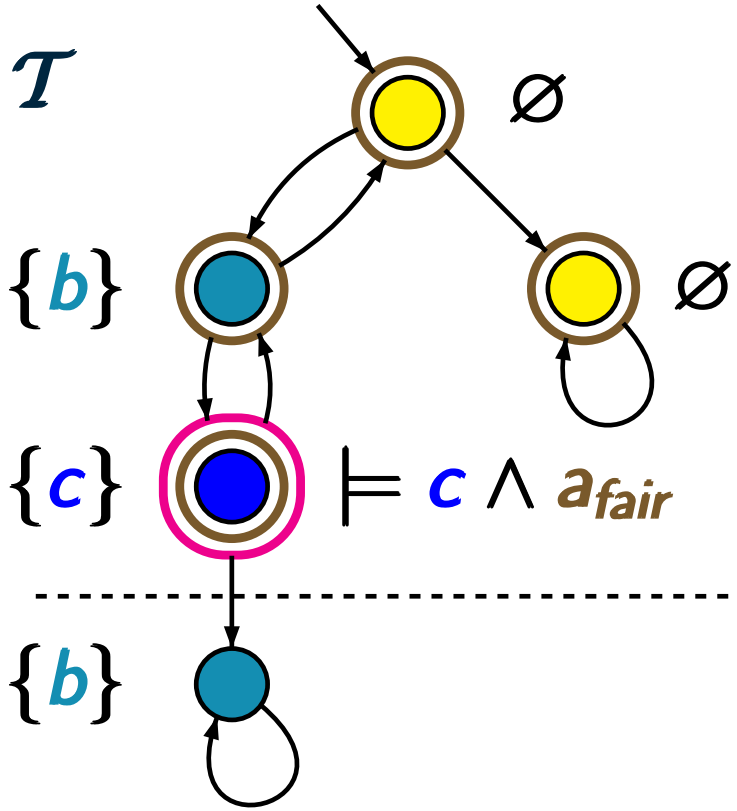
CTL formula $\exists\Diamond c$

$\downarrow$

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

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

Example: treatment of $\exists\Diamond$



CTL formula $\exists\Diamond c$

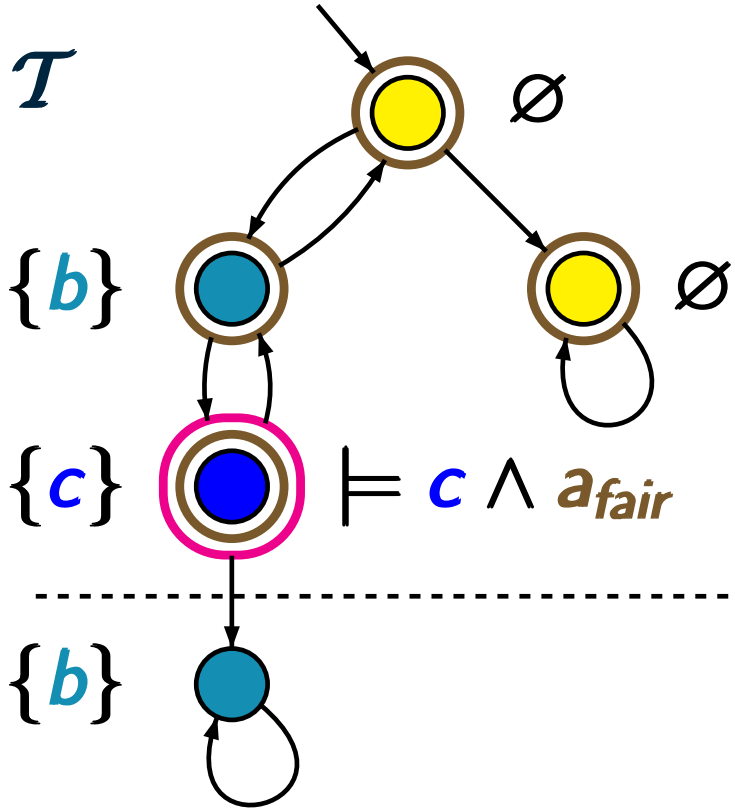
$\downarrow$

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

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

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

Example: treatment of $\exists\Diamond$



CTL formula $\exists\Diamond c$

$\downarrow$

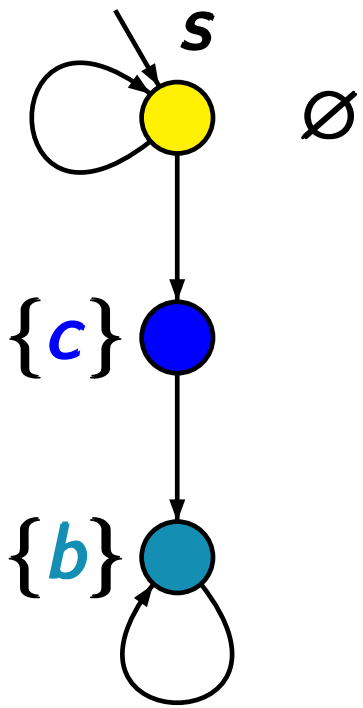
$\exists\Diamond \boxed{(c \wedge a_{fair})}$

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 $\exists \mathsf{U}$

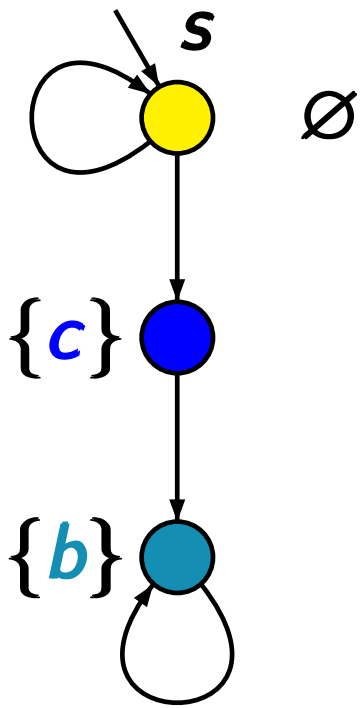
$\mathcal{T}$:



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

Example: treatment of ∃U

$\mathcal{T}$:

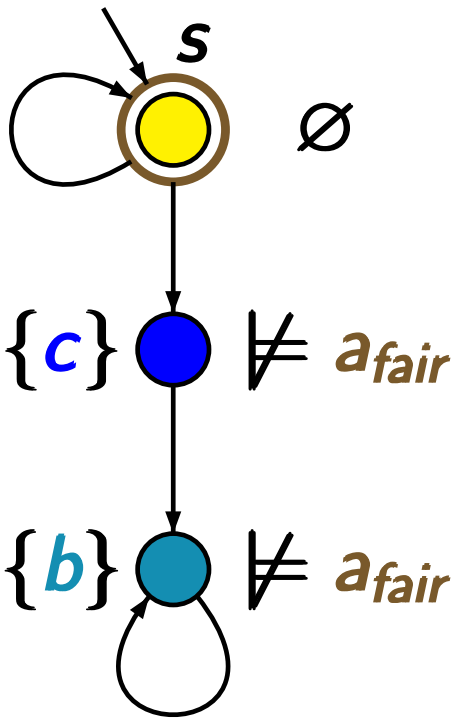


strong fairness assumption: $\mathit{fair} = \Box\Diamond b \rightarrow \Box\Diamond c$

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

Example: treatment of $\exists U$

$\mathcal{T}$:

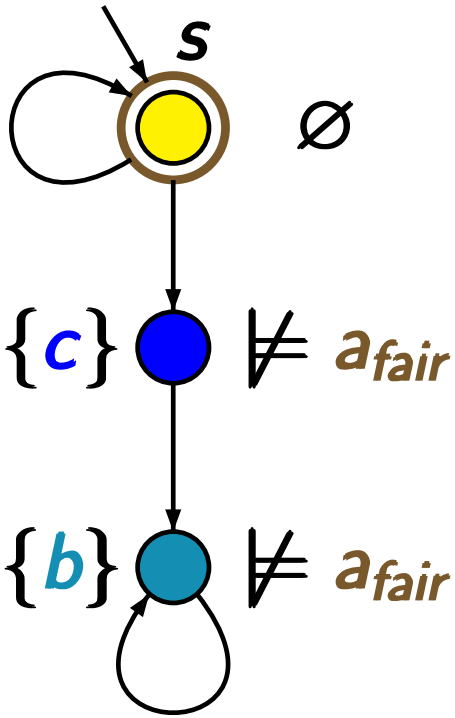


strong fairness assumption: $fair = \Box\Diamond b \rightarrow \Box\Diamond c$

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

Example: treatment of $\exists U$

$\mathcal{T}$:



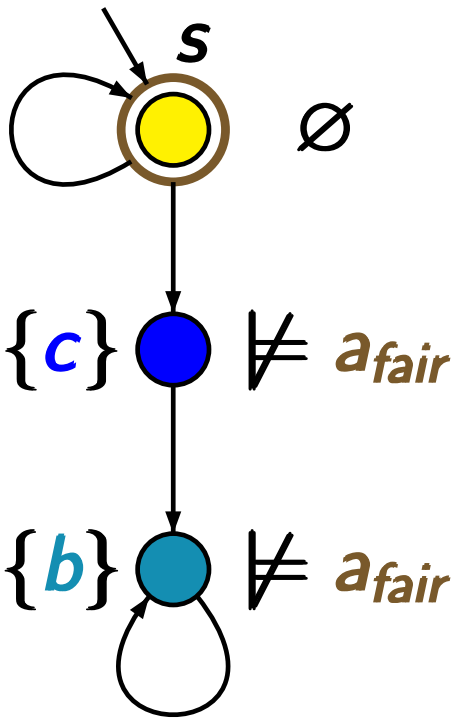
$Sat(c \wedge a_{fair}) = \emptyset$

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

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

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

$\mathcal{T}$:



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

$$\Uparrow$$

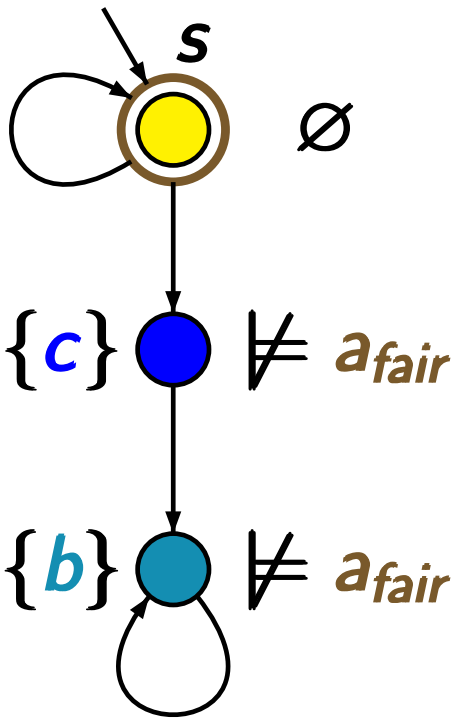
$$Sat(c \wedge a_{fair}) = \varnothing$$

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

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

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

$\mathcal{T}$:



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

$$\Uparrow$$

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

$$\Uparrow$$

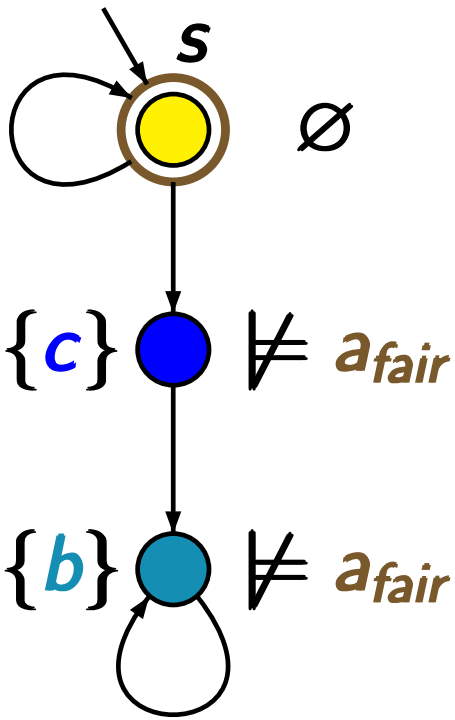
$$Sat(c \wedge a_{fair}) = \varnothing$$

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

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

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

$\mathcal{T}$:



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

$$\Uparrow$$

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

$$\Uparrow$$

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

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

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

Correct or wrong?

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

Correct or wrong?

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

correct.

Correct or wrong?

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

correct. Note that:

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

Correct or wrong?

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

correct. Note that:

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

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

Correct or wrong?

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

correct. Note that:

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

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

Correct or wrong?

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

correct. Note that:

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

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

Correct or wrong?

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

correct.

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

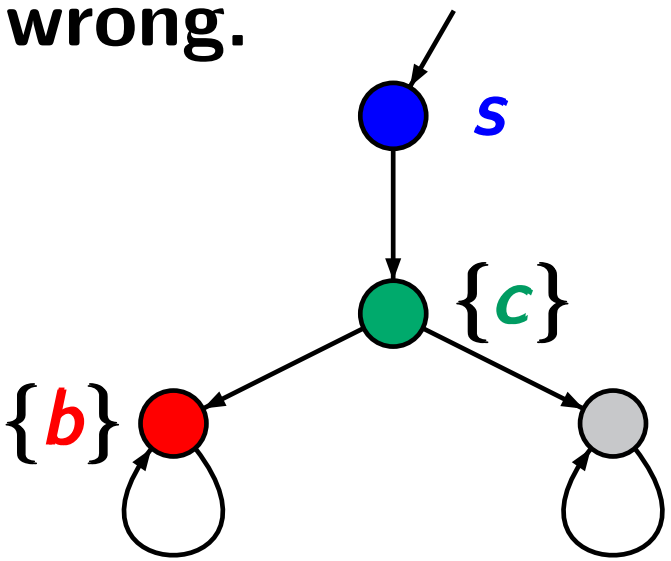
Correct or wrong?

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

correct.

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

wrong.



$$fair = \Box\Diamond gray$$

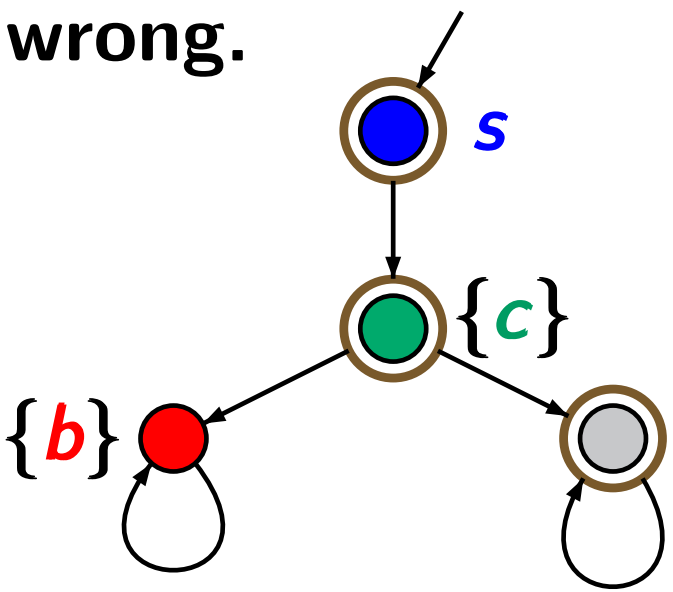
Correct or wrong?

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

correct.

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

wrong.



$$fair = \Box\Diamond gray$$

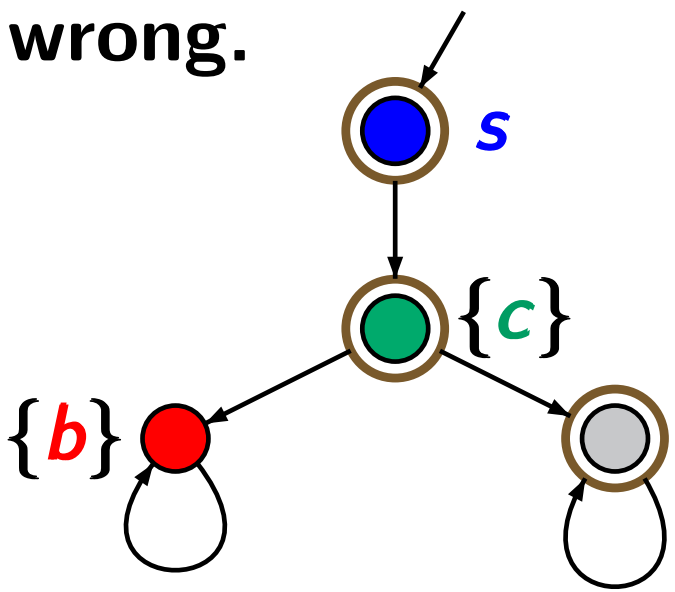
Correct or wrong?

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

correct.

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

wrong.



$$fair = \Box\Diamond gray$$

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

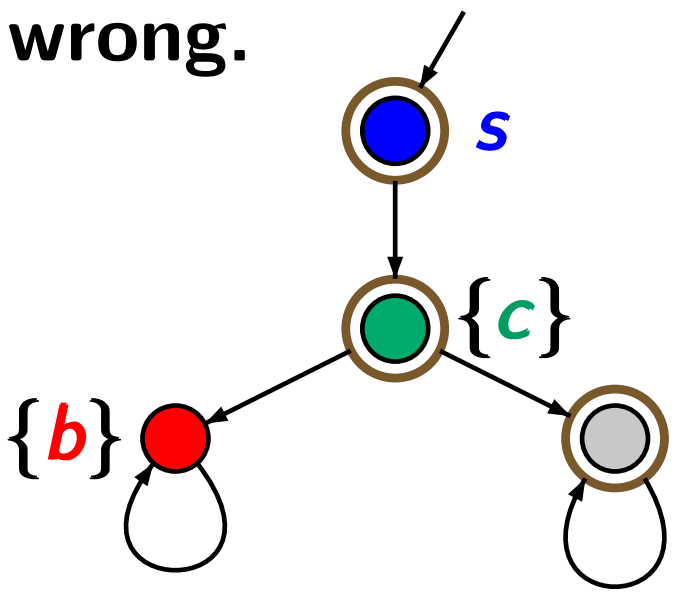
Correct or wrong?

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

correct.

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

wrong.



$$fair = \Box\Diamond gray$$

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

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

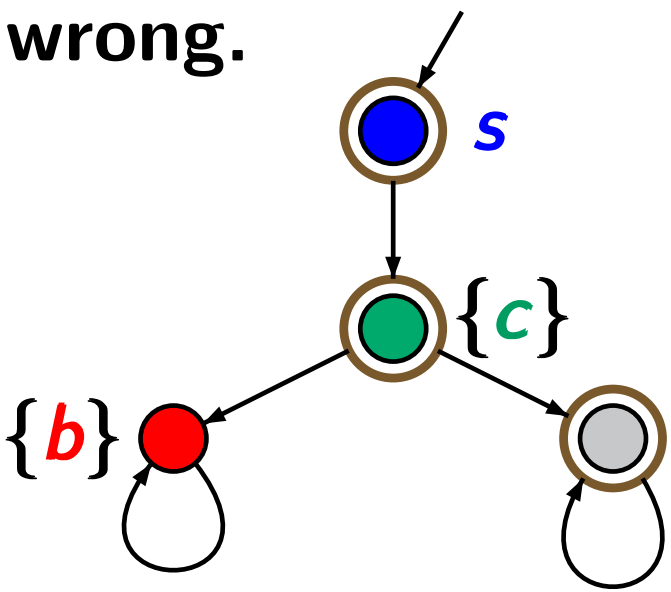
Correct or wrong?

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

correct.

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

wrong.



$$fair = \Box\Diamond gray$$

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

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

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

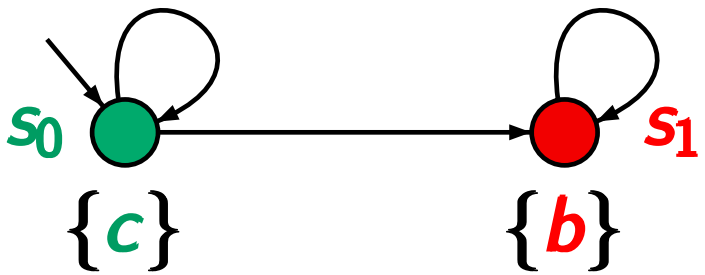
Correct or wrong?

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

Correct or wrong?

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

wrong.

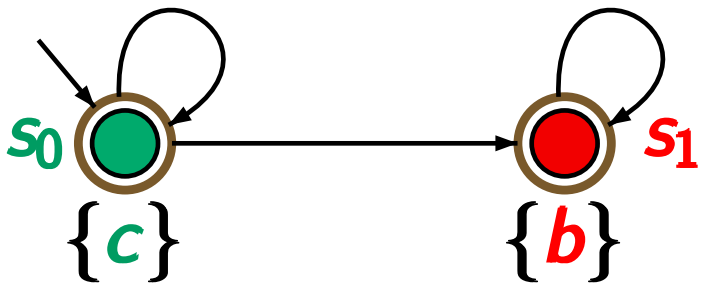


$$fair = \Box\Diamond b$$

Correct or wrong?

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

wrong.



$fair = \Box\Diamond b$

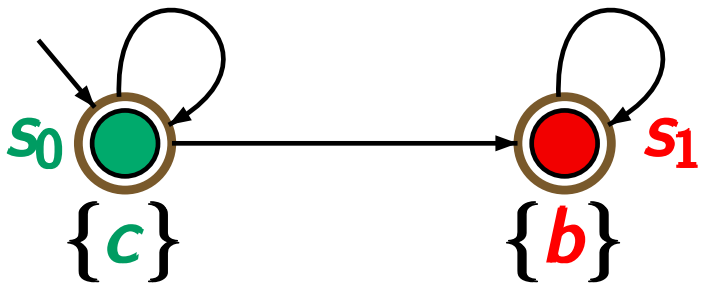
$s_0 \models a_{fair}$

$s_1 \models a_{fair}$

Correct or wrong?

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

wrong.



$fair = \Box\Diamond b$

$s_0 \models a_{fair}$

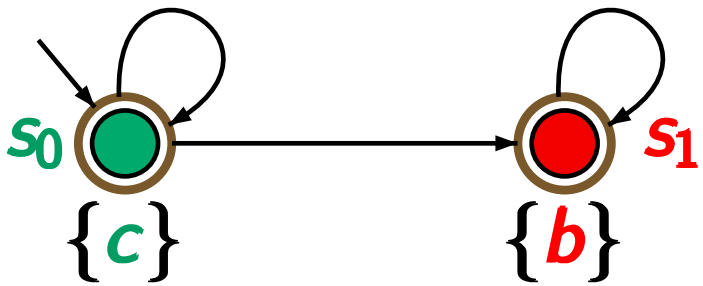
$s_1 \models a_{fair}$

regard state $s = s_0$:

Correct or wrong?

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

wrong.



$fair = \Box\Diamond b$

$s_0 \models a_{fair}$

$s_1 \models a_{fair}$

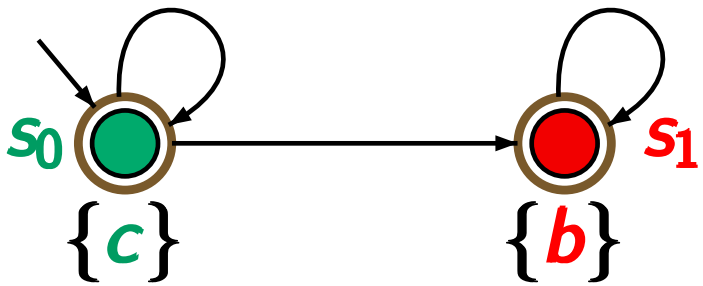
regard state $s = s_0$:

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

Correct or wrong?

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

wrong.



$fair = \Box\Diamond b$

$s_0 \models a_{fair}$

$s_1 \models a_{fair}$

regard state $s = s_0$:

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

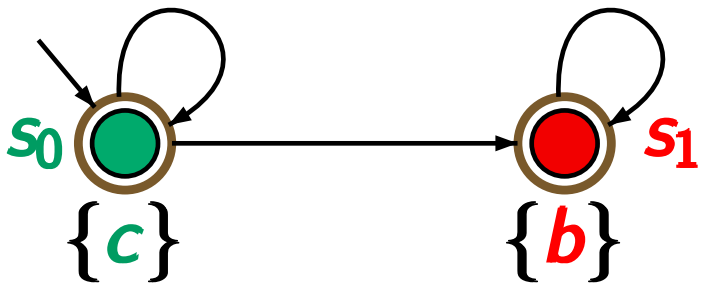
$$\uparrow$$

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

Correct or wrong?

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

wrong.



$fair = \Box\Diamond b$

$s_0 \models a_{fair}$

$s_1 \models a_{fair}$

regard state $s = s_0$:

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

$\uparrow$

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

Idea of FairCTL model checking

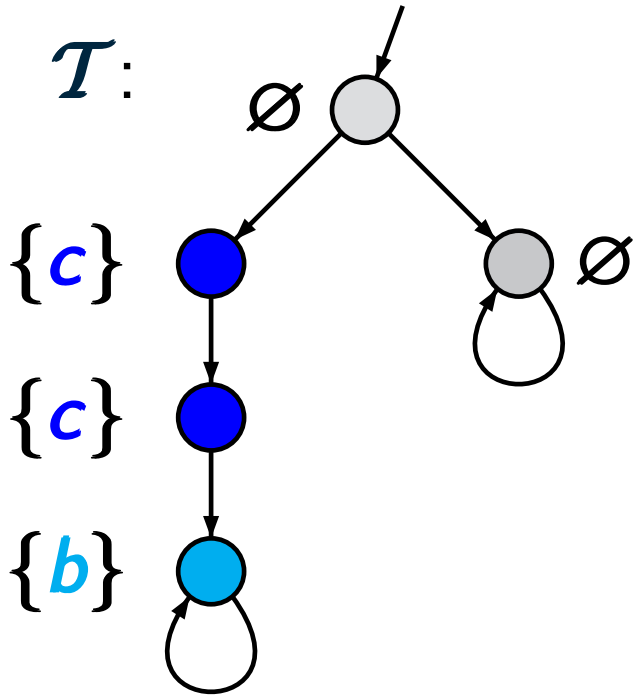
given: finite transition system $\mathcal{T}$
CTL formula Φ in $\exists$-normal form
CTL fairness assumption ***fair***

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

$\exists\Box\Psi$ under strong fairness

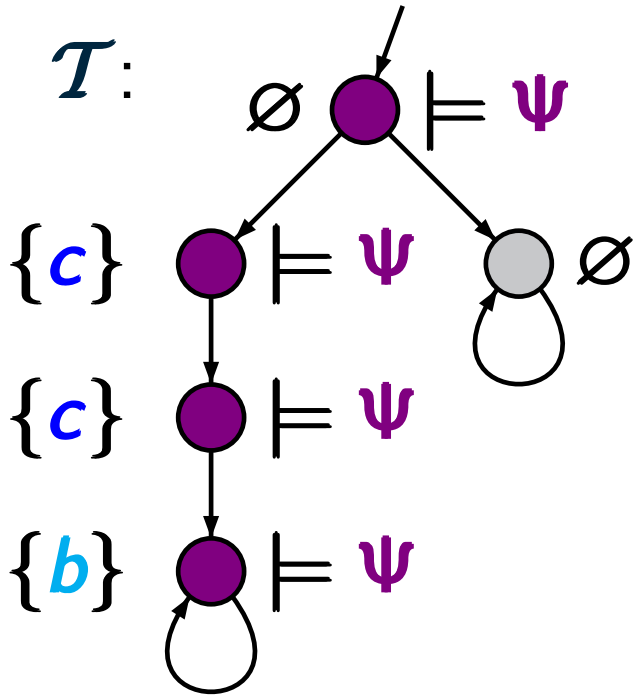
$fair = \Box\Diamond b \rightarrow \Box\Diamond c$, CTL state formula Ψ



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

$\exists\Box\Psi$ under strong fairness

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

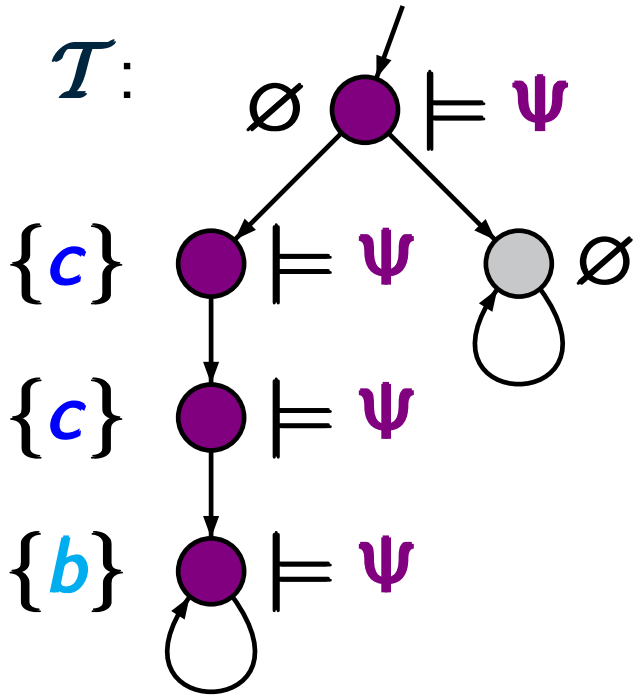


$\mathcal{T} \models_{fair} \exists\Box\Psi$?

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

$\exists\Box\Psi$ under strong fairness

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

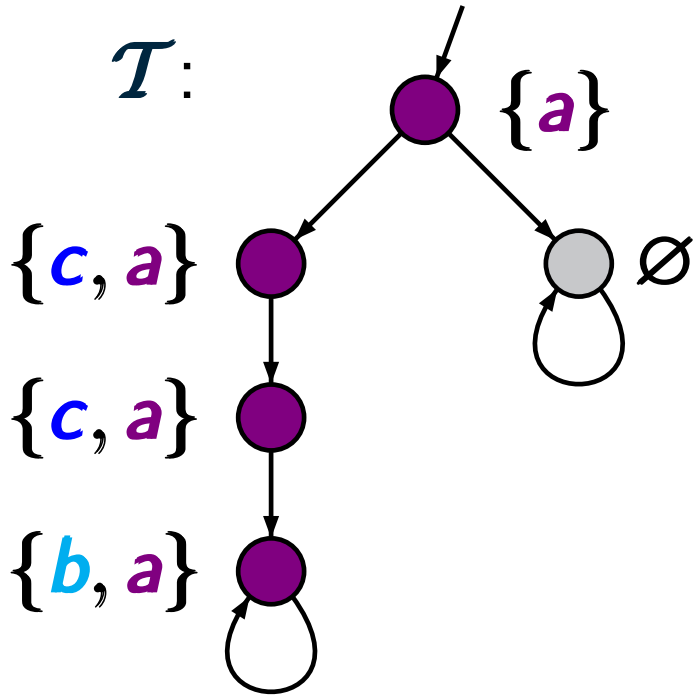


$\mathcal{T} \models_{fair} \exists\Box\Psi$?

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

$\exists\Box\Psi$ under strong fairness

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

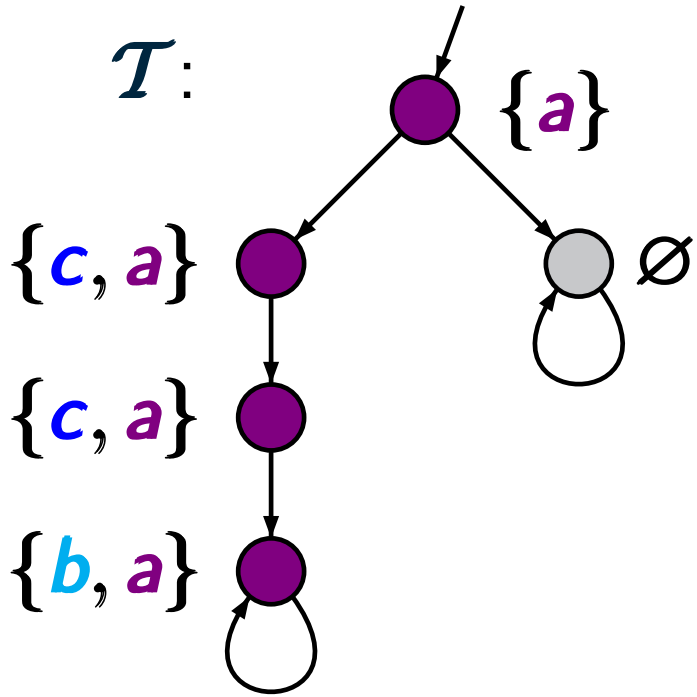


$\mathcal{T} \models_{fair} \exists\Box\Psi$?

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

$\exists\Box\Psi$ under strong fairness

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

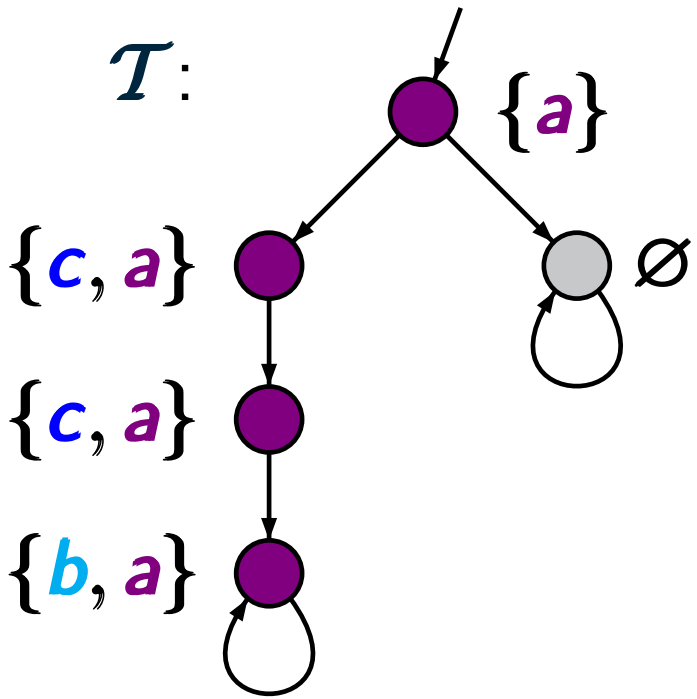


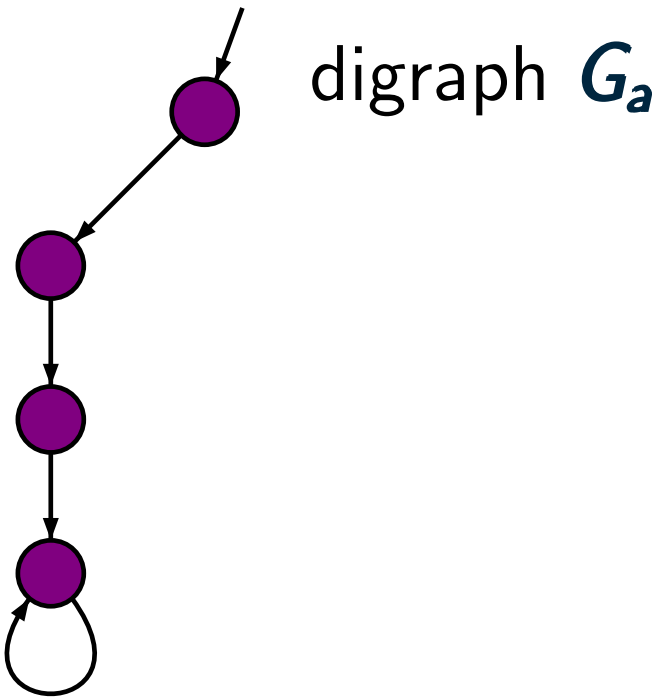
$\mathcal{T} \models_{fair} \exists\Box\Psi$?

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

$\exists\Box\Psi$ under strong fairness

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

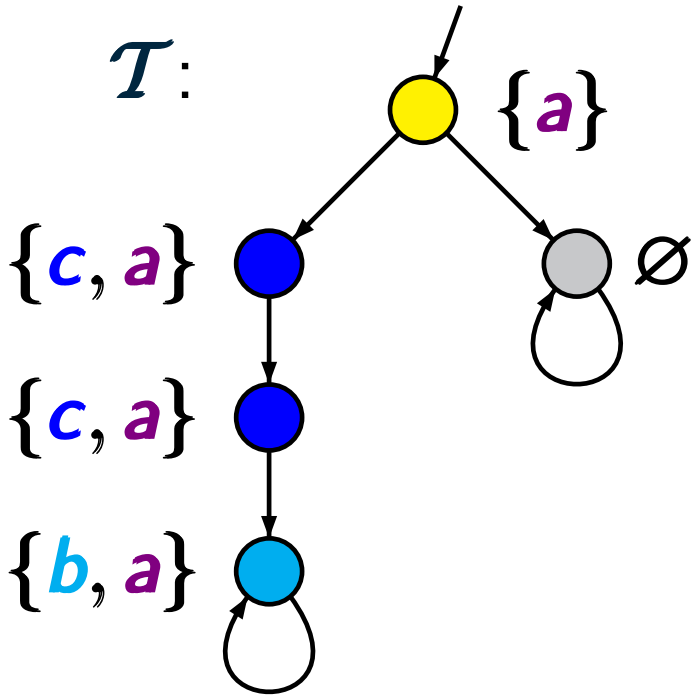


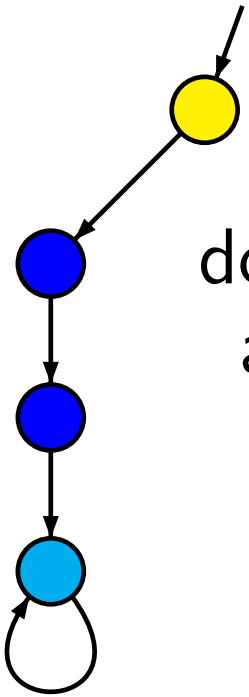


1. calculate $Sat_{fair}(\Psi)$
2. replace Ψ with a fresh atomic proposition $a = a_\Psi$
3. calculate $Sat_{fair}(\exists\Box a)$

$\exists\Box\Psi$ under strong fairness

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





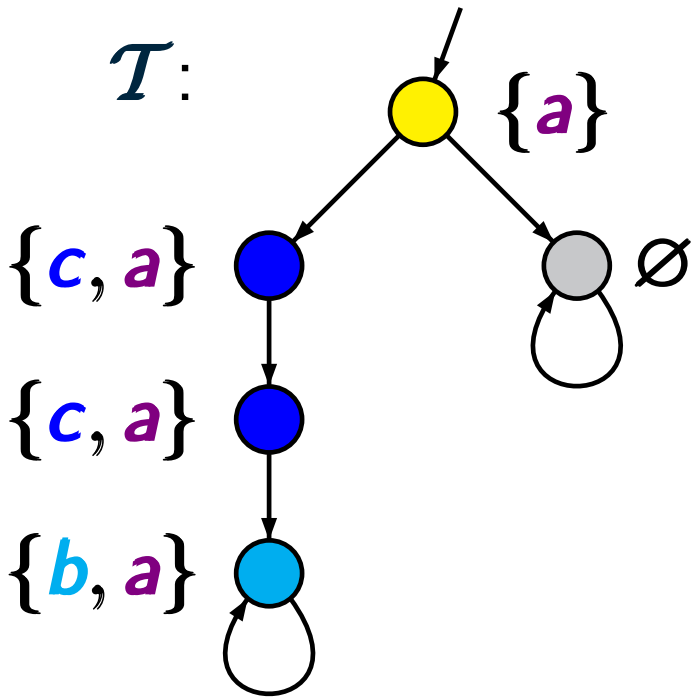
digraph G_a

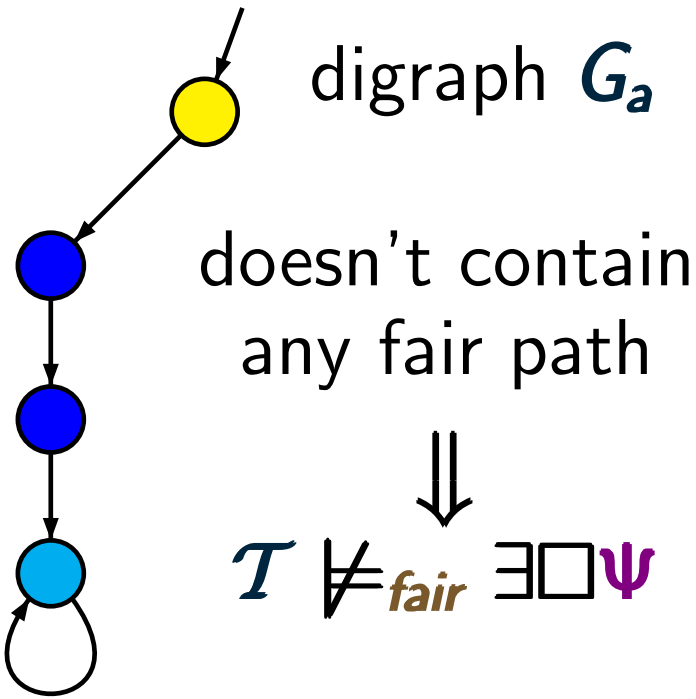
doesn't contain any fair path

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

$\exists\Box\Psi$ under strong fairness

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





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

Treatment of $\exists\Box a$ for FairCTL

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

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

Treatment of $\exists\Box a$ for FairCTL

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

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

if all states are labeled by a:

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

Treatment of $\exists\Box a$ for FairCTL

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

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

if all states are labeled by a:

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

here: explanations only for strong fairness

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

Treatment of $\exists\Box$ under strong fairness

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

Treatment of $\exists\Box$ under strong fairness

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

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

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

Treatment of $\exists\Box$ under strong fairness

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

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

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

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

Treatment of $\exists\Box$ under strong fairness

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

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

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

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

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

Treatment of $\exists\Box$ under strong fairness

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

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

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

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

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

Treatment of $\exists\Box$ under strong fairness

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

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

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

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

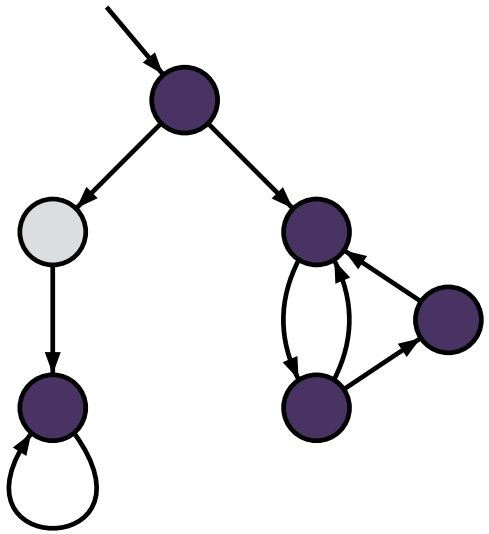
- $s_j \models a$ for all $0 \leq j \leq n + r$
- the path $s_0\, s_1 \ldots s_n (s_{n+1} \ldots s_{n+r})^\omega$ is fair, i.e., for all $1 \leq i \leq k$:

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

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

$\exists\Box a$ under strong fairness

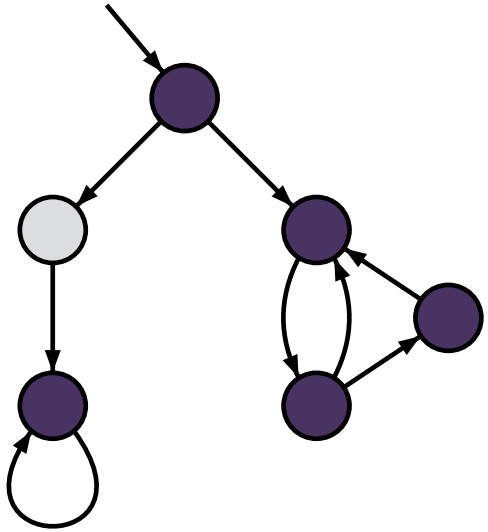
does $\mathcal{T} \models_{fair} \exists\Box a$ hold ?



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

$\exists\Box a$ under strong fairness

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



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

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