Overview

Introduction
Modelling parallel systems
Linear Time Properties
Regular Properties
Linear Temporal Logic (LTL)

Computation Tree Logic

- syntax and semantics of CTL
- expressiveness of CTL and LTL
- CTL model checking
- CTL with fairness
- counterexamples/witnesses, CTL^+ and CTL^*

Equivalences and Abstraction
**Complexity of CTL and LTL model checking**

**LTL** model checking problem:
- PSPACE-complete and solvable in time
  \[ O(\text{size}(T) \cdot \exp(|\varphi|)) \]

**CTL** model checking problem:
- solvable in polynomial time
  \[ O(\text{size}(T) \cdot |\Phi|) \]
**LTL model checking problem:**

PSPACE-complete and solvable in time

\[ O(\text{size}(T) \cdot \exp(|\varphi|)) \]

**CTL model checking problem:**

solvable in polynomial time (even PTIME-complete)

\[ O(\text{size}(T) \cdot |\Phi|) \]
Complexity of CTL and LTL model checking

**LTL** model checking problem:

- PSPACE-complete and solvable in time
  \[ O(\text{size}(T) \cdot \exp(|\varphi|)) \]
- **LTL** with fairness:
  \[ O(\text{size}(T) \cdot \exp(|\varphi| + |\text{fair}|)) \]

**CTL** model checking problem:

- Solvable in polynomial time (even PTIME-complete)
  \[ O(\text{size}(T) \cdot |\Phi|) \]
Complexity of CTL and LTL model checking

**LTL** model checking problem:

PSPACE-complete and solvable in time

\[ O(\text{size}(T) \cdot \exp(|\varphi|)) \]

**LTL** with fairness:

\[ O(\text{size}(T) \cdot \exp(|\varphi| + |\text{fair}|)) \]

**CTL** model checking problem:

solvable in polynomial time (even PTIME-complete)

\[ O(\text{size}(T) \cdot |\Phi|) \]

**CTL** with fairness:

\[ O(\text{size}(T) \cdot |\Phi| \cdot |\text{fair}|) \]
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 $\phi$, $\psi$ are propositional formulas
Recall: LTL fairness assumptions

are conjunctions of LTL formulas of the form:

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

where $\phi$, $\psi$ are propositional formulas
Recall: LTL fairness assumptions

are conjunctions of LTL formulas of the form

- unconditional fairness \( \Box \Diamond \phi \)
- strong fairness \( \Box \Diamond \psi \rightarrow \Box \Diamond \phi \)
- weak fairness \( \Diamond \Box \psi \rightarrow \Box \Diamond \phi \)

where \( \phi, \psi \) are propositional formulas

Reduction of \( \models_{\text{fair}} \) to \( \models \)
Recall: LTL fairness assumptions

are conjunctions of LTL formulas of the form

- unconditional fairness \( \Box \Diamond \phi \)
- strong fairness \( \Box \Diamond \psi \rightarrow \Box \Diamond \phi \)
- weak fairness \( \Diamond \Box \psi \rightarrow \Box \Diamond \phi \)

where \( \phi, \psi \) are propositional formulas

Reduction of \( \models \text{fair} \) to \( \models \)

\[ T \models \text{fair} \ \varphi \ \iff \ \pi \models \varphi \ \text{for all fair paths } \pi \text{ in } T \]
Recall: LTL fairness assumptions

are conjunctions of LTL formulas of the form

- unconditional fairness $\square \diamond \phi$
- strong fairness $\square \diamond \psi \rightarrow \square \diamond \phi$
- weak fairness $\diamond \square \psi \rightarrow \square \diamond \phi$

where $\phi$, $\psi$ are propositional formulas

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

\[
\mathcal{T} \models_{fair} \varphi \iff \pi \models \varphi \text{ for all fair paths } \pi \text{ in } \mathcal{T} \\
\text{iff for all paths } \pi \text{ in } \mathcal{T}: \\
\pi \models fair \rightarrow \varphi
\]
Recall: LTL fairness assumptions

are conjunctions of LTL formulas of the form

- unconditional fairness  • unconditional fairness  • unconditional fairness  • unconditional fairness
- strong fairness  • strong fairness  • strong fairness
- weak fairness  • weak fairness  • weak fairness

where φ, ψ are propositional formulas

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

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

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

$\pi \models \text{fair} \rightarrow \varphi$
Recall: LTL fairness assumptions

are conjunctions of LTL formulas of the form

- unconditional fairness \( □♦φ \)
- strong fairness \( □♦ψ → □♦φ \)
- weak fairness \( ♦□ψ → □♦φ \)

where \( φ, ψ \) are propositional formulas

Reduction of \( \models_{\text{fair}} \) to \( \models \), e.g., for \( \text{fair} = □♦a \)

\[ \mathcal{T} \models_{\text{fair}} φ \iff \pi \models φ \text{ for all fair paths } \pi \text{ in } \mathcal{T} \]

\[ \text{iff for all paths } \pi \text{ in } \mathcal{T}: \]

\[ \pi \models \text{fair} → φ \equiv ♦□¬a \lor φ \]
CTL fairness assumptions
conjunctions of “formulas” of the type

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

where $\Psi$, $\Phi$ are CTL state formulas
conjunctions of “formulas” of the type

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

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

note: CTL fairness assumptions

- are not CTL (state or path) formulas
- just a syntactic formalism to specify fairness assumptions
conjunctions of “formulas” of the type

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

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

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

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

where $\Psi_j, \Phi_j$ are CTL state formulas
Satisfaction relation for CTL with fairness

\[ s \models_{\text{fair}} \text{true} \]

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

\[ s \models_{\text{fair}} \neg \phi \quad \text{iff} \quad s \not\models_{\text{fair}} \phi \]

\[ s \models_{\text{fair}} \phi_1 \land \phi_2 \quad \text{iff} \quad s \models_{\text{fair}} \phi_1 \quad \text{and} \quad s \models_{\text{fair}} \phi_2 \]
Satisfaction relation for CTL with fairness

\[ s \models_{\text{fair}} \text{true} \]

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

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

\[ s \models_{\text{fair}} \Phi_1 \land \Phi_2 \quad \text{iff} \quad s \models_{\text{fair}} \Phi_1 \quad \text{and} \quad s \models_{\text{fair}} \Phi_2 \]

\[ s \models_{\text{fair}} \exists \varphi \quad \text{iff} \quad \text{there exists } \pi \in \text{Paths}(s) \text{ with } \pi \models_{\text{fair}} \varphi \]
Satisfaction relation for CTL with fairness

\[ s \models_{\text{fair}} \text{true} \]
\[ s \models_{\text{fair}} a \quad \text{iff} \quad a \in L(s) \]
\[ s \models_{\text{fair}} \neg \phi \quad \text{iff} \quad s \nmodels_{\text{fair}} \phi \]
\[ s \models_{\text{fair}} \phi_1 \land \phi_2 \quad \text{iff} \quad s \models_{\text{fair}} \phi_1 \text{ and } s \models_{\text{fair}} \phi_2 \]
\[ s \models_{\text{fair}} \exists \varphi \quad \text{iff} \text{ there exists } \pi \in \text{Paths}(s) \text{ with } \pi \models_{\text{fair}} \varphi \]
\[ s \models_{\text{fair}} \forall \varphi \quad \text{iff} \text{ for all } \pi \in \text{Paths}(s): \pi \models_{\text{fair}} \text{ implies } \pi \models_{\text{fair}} \varphi \]
Satisfaction relation for CTL with fairness

\[ s \models_{\text{fair}} \text{true} \]

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

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

\[ s \models_{\text{fair}} \Phi_1 \land \Phi_2 \quad \text{iff} \quad s \models_{\text{fair}} \Phi_1 \text{ and } s \models_{\text{fair}} \Phi_2 \]

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

\[ \pi \models_{\text{fair}} \text{ and } \pi \models_{\text{fair}} \varphi \]

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

\[ \pi \models_{\text{fair}} \text{ implies } \pi \models_{\text{fair}} \varphi \]

\[ \text{e.g., } s_0 s_1 s_2 \ldots \models \square \Diamond \Phi \quad \text{iff} \quad \exists \ i \geq 0 \ \text{s.t.} \ s_i \models \Phi \]
Simple communication protocol

CTL formula
\[ \Phi = \forall \square \forall \Diamond \text{start} \]
Simple communication protocol

CTL formula
\[ \Phi = \forall \Box \forall \Diamond \text{start} \]
\[ T \not\models \Phi \]

Diagram:
- Start
- Try to send
- Lost
- Delivered
Simple communication protocol

CTL formula

\[ \Phi = \forall \Box \forall \Diamond \text{start} \]

\[ \mathcal{T} \not\models \Phi \]

\[ \mathcal{T} \models_{\text{ufair}} \Phi \]

unconditional CTL fairness assumption:

\[ \text{ufair} = \Box \Diamond \text{delivered} \]
Simple communication protocol

CTL formula

\( \Phi = \forall \Box \forall \Diamond start \)

\( \mathcal{T} \not\models \Phi \)

\( \mathcal{T} \models_{u_{fair}} \Phi \)

\( \mathcal{T} \models_{s_{fair}} \Phi \)

unconditional CTL fairness assumption:

\( u_{fair} = \Box \Diamond delivered \)

strong CTL fairness assumption:

\( s_{fair} = \Box \Diamond try\_to\_send \rightarrow \Box \Diamond delivered \)
Simple communication protocol

Unconditional fairness: $ufair = □◊ ∃◊ start$

$$Φ = ∀□∀◊ start$$

$$\mathcal{T} \models_{ufair} Φ$$?
Simple communication protocol

unconditional fairness: \( ufa\{r = \Box \Diamond \exists \Box start \)

\[ \phi = \forall \Box \forall \Diamond start \]

\[ \mathcal{T} \models_{ufair} \phi \ ? \]

\[ Sat(\exists \Box start) = \{ delivered \} \]
Simple communication protocol

\[ \Phi = \forall \Box \forall \Diamond \text{start} \]

\[ \mathcal{T} \models_{\text{ufair}} \Phi \quad ? \]

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

\[ \text{Sat} (\exists \Diamond \text{start}) = \{ \text{delivered} \} \]

\[ \text{ufair} \equiv \Box \Diamond \text{delivered} \]
Simple communication protocol

unconditional fairness: \( ufair = \Box \Diamond \exists \bigcirc start \)

\[ \Phi = \forall \Box \forall \Diamond start \]
\[ T \models_{ufair} \Phi \checkmark \]

\[ Sat(\exists \bigcirc start) = \{ delivered \} \]
\[ ufair \equiv \Box \Diamond delivered \]
Simple communication protocol

unconditional fairness: \[ ufair = \square \Diamond \exists \Diamond \text{start} \]

weak fairness: \[ wfair = \Diamond \square \exists \Diamond \text{delivered} \rightarrow \square \Diamond \text{delivered} \]
Simple communication protocol

unconditional fairness:  \( ufair = □♦∃◊start \)

weak fairness:  \( wfair = ◊□∃◊delivered \rightarrow □◊delivered \)

\[ Sat(∃◊delivered) = \{ try\_to\_send \} \]
Simple communication protocol

unconditional fairness: \( ufair = \Box \Diamond \exists \Diamond \Box start \)

weak fairness: \( wfair = \Diamond \Box \exists \Diamond delivered \rightarrow \Box \Diamond delivered \)

\[ \Phi = \forall \Box \forall \Diamond start \]
\[ T \models_{ufair} \Phi \quad \sqrt{\checkmark} \]
\[ T \models_{wfair} \Phi \quad ? \]

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

wfair \( \equiv \Diamond \Box \text{try\_to\_send} \rightarrow \Box \Diamond \text{delivered} \)
Simple communication protocol

\begin{align*}
\phi &= \forall \Box \forall \Diamond \text{start} \\
\mathcal{T} &\models_{\text{ufair}} \phi \quad \checkmark \\
\mathcal{T} &\models_{\text{wfair}} \phi \quad \text{wrong}
\end{align*}

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

weak fairness: \quad \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} \equiv \Diamond \Box \text{try_to_send} \rightarrow \Box \Diamond \text{delivered}
Simple communication protocol

\[
\Phi = \forall \Box \forall \Diamond \text{start}
\]

\[
\mathcal{T} \models_{\text{ufair}} \Phi \quad \checkmark
\]

\[
\mathcal{T} \not\models_{\text{wfair}} \Phi
\]

\[
\mathcal{T} \models_{\text{sfair}} \Phi \quad ?
\]

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

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

strong fairness: \( \text{sfair} = \Box \Diamond \exists \Box \text{delivered} \rightarrow \Box \Diamond \text{delivered} \)
Simple communication protocol

\[ \Phi = \forall \Box \forall \Diamond \text{start} \]

\[ \mathcal{T} \models_{ufair} \Phi \quad \checkmark \]

\[ \mathcal{T} \not\models_{wfair} \Phi \]

\[ \mathcal{T} \models_{sfair} \Phi \quad ? \]

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

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

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

\[
\text{Sat}(\exists \Box \Diamond \text{delivered}) = \{ \text{try\_to\_send} \}
\]
Simple communication protocol

\[ \Phi = \forall \Box \forall \Diamond \text{start} \]

\[ \mathcal{T} \models_{ufair} \Phi \quad \checkmark \]

\[ \mathcal{T} \not\models_{wfair} \Phi \]

\[ \mathcal{T} \models_{sfair} \Phi \]

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

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

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

\[ \text{Sat}(\exists \Box \Diamond \text{delivered}) = \{ \text{try_to_send} \} \]

\[ sfair \equiv \Box \Diamond \text{try_to_send} \rightarrow \Box \Diamond \text{delivered} \]
Simple communication protocol

\[ \Phi = \forall \Box \forall \Diamond \text{start} \]

\[ \mathcal{T} \models_{ufair} \Phi \quad \checkmark \]

\[ \mathcal{T} \not\models_{wfair} \Phi \]

\[ \mathcal{T} \models_{sfair} \Phi \quad \checkmark \]

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

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

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

\[
\text{Sat} (\exists \Box \text{delivered}) = \{ \text{try\_to\_send} \}
\]

\[
sfair \equiv \Box \Diamond \text{try\_to\_send} \rightarrow \Box \Diamond \text{delivered}
\]
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 \( s \models_{\text{fair}} \forall \Diamond a \)

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

correct. Note that:

$s \models \forall \varphi \implies$ for all $\pi \in Paths(s)$: $\pi \models \varphi$
Correct or wrong?

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

correct. Note that:

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

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

$\pi \models \text{fair}$ 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:

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

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

$\pi \models fair$ implies $\pi \models \varphi$

$\implies s \models_{fair} \forall \varphi$
Correct or wrong?

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

correct.

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

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

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

\[ \bullet \quad \bullet \quad \bullet \quad \bullet \quad \ldots \]
Correct or wrong?

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

correct.

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

wrong

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

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

$s \models \exists a$

just one fair path  ●  ●  ●  ●  ●  . . .
Correct or wrong?

If $s \vDash \forall \diamond a$ where $a \in AP$ then $s \vDash_{\text{fair}} \forall \diamond a$

**Correct.**

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

\[
\text{If } s \models \forall a \exists \Box a \text{ then } s \models_{\text{fair}} \forall a \exists \Box a
\]
Correct or wrong?

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

\[ s_0 \quad s_0 \]

\[ s_1 \quad s_2 \]

\[ s_1 \quad s_2 \]

wrong

\[ b \]

\[ a \]
Correct or wrong?

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

Wrong

$s_0$ $s_1$ $s_2$

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

$\bullet = \{b\}$

$\bullet = \{a\}$
Correct or wrong?

If \( s \models \forall \lozenge \exists \square a \) then \( s \models_{\text{fair}} \forall \lozenge \exists \square a \)

Wrong

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

\[ \text{Sat}(\forall \lozenge \exists \square a) = \{s_0, s_1\} \]

\[ \text{Sat}(\forall \lozenge \exists \square a) = \{s_0, s_1\} \]
Correct or wrong?

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

Wrong

\[
\begin{align*}
Sat(\exists \square a) & = \{ s_0, s_1 \} \\
Sat(\forall \diamond \exists \square a) & = \{ s_0, s_1 \}
\end{align*}
\]

\( \square_{\text{fair}} = \ \square \diamond \ b \)

\( \square = \{ b \} \)

\( \bullet = \{ a \} \)
Correct or wrong?

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

\[
\begin{align*}
\text{Sat}(\exists \square a) &= \{s_0, s_1\} \\
\text{Sat}_{\text{fair}}(\exists \square a) &= \emptyset \\
\text{Sat}(\forall \diamond \exists \square a) &= \{s_0, s_1\}
\end{align*}
\]
Correct or wrong?

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

\[
\begin{align*}
\text{Wrong} & \\
\text{sat}(\exists \square a) & = \{s_0, s_1\} \\
\text{sat}(\forall \diamond \exists \square a) & = \{s_0, s_1\}
\end{align*}
\]

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

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

$\text{sat}_{\text{fair}}(\forall \diamond \exists \square a) = \emptyset$
\( \text{Sat}_{\text{fair}}(\exists \Box \text{true}) = ? \)
\( \text{Sat}_{\text{fair}}(\exists □ \text{true}) = ? \)

\[
\begin{align*}
\text{CTLFAIR4.4-11} \\
\text{red} &= \{ a \} \\
\text{blue} &= \emptyset \\
\text{fair} &= □ □ a
\end{align*}
\]
\[ \text{Sat}_{\text{fair}}(\exists \Box \text{true}) = ? \]

CTLFAIR4.4-11

\[
\begin{align*}
\red{\bullet} &= \{a\} \\
\blue{\bullet} &= \emptyset \\
fair &= \Box \Diamond a
\end{align*}
\]

\[
\text{Sat}_{\text{fair}}(\exists \Box \text{true}) = ?
\]
$\text{Sat}_{\text{fair}}(\exists \square \text{true}) = \{s_0, s_2\}$
$\text{Sat}_{\text{fair}}(\exists\Box \text{true}) = \{s_0, s_2\}$

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

$\text{fair} = \Box\Diamond a$
\(Sat_{\text{fair}}(\exists \Box \text{true}) = ?\)
Sat_{fair}(∃□true) = ?

Sat_{fair}(∃□true) = \{s_0, s_2\}

Sat_{fair}(∃□true) = \text{set of states } s \text{ that have at least one fair path}

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

fair is realizable iff

Sat_{fair}(∃□true) \supseteq \text{set of all reachable states}
Model checking problem for FairCTL

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

question: does $T \models_{\text{fair}} \Phi$ hold?
Model checking problem for FairCTL

given: finite transition system $T$

CTL formula $\Phi$

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

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

question: does $T \models_{fair} \Phi$ hold?
Model checking problem for FairCTL

given: finite transition system $\mathcal{T}$
CTL formula $\Phi$
CTL fairness assumption $\text{fair}$, e.g.,
\[
\text{fair} = \bigwedge_{1 \leq i \leq k} \square \diamond \psi_{i,1} \rightarrow \square \square \psi_{i,2}
\]
question: does $\mathcal{T} \models_{\text{fair}} \Phi$ hold?

for simplicity:
we suppose that $\Phi$ is in existential normal form, i.e., a $\forall$-free CTL formula with temporal modalities
$\exists \circlearrowleft, \exists U, \exists \square$
Preprocessing of FairCTL model checking

given: finite transition system $\mathcal{T}$
CTL formula $\Phi$ in $\exists$-normal form
CTL fairness assumption $\text{fair}$, 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 of FairCTL model checking

given: finite transition system \( \mathcal{T} \)

CTL formula \( \Phi \) in \( \exists \)-normal form

CTL fairness assumption \( fair \), e.g.,

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

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 $\Phi$ in $\exists$-normal form

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

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

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

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

- compute $Sat(\psi_{i,1})$ and $Sat(\psi_{i,2})$
Preprocessing of FairCTL model checking

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

\[
fair = \bigwedge_{1 \leq i \leq k} \Box \Diamond \psi_{i,1} \rightarrow \Box \Diamond \psi_{i,2}
\]

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

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

- compute \(Sat(\psi_{i,1})\) and \(Sat(\psi_{i,2})\)
- replace \(\psi_{i,1}\) and \(\psi_{i,2}\) with fresh atomic propositions \(b_i\) and \(c_i\), respectively
Preprocessing of FairCTL model checking

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

- CTL formula $\Phi$ in $\exists$-normal form
- CTL fairness assumption $\text{fair}$, 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 $\text{fair}$

- 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
Idea of FairCTL model checking

**given:** finite transition system \( T \)
- CTL formula \( \Phi \) in \( \exists \)-normal form
- CTL fairness assumption \( fair \)

**question:** does \( T \models_{fair} \Phi \) hold?

1. ... preprocessing ...
Idea of FairCTL model checking

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

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

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

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

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

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

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

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

1. ... preprocessing ...

2. Build the parse tree of $\Phi$ and process it in bottom-up-manner. Treatment of:
   
   - $\text{true}$, $a \in AP$, $\land$, $\neg$: as for standard CTL
   - $\exists \bigcirc$, $\exists U$: via standard CTL model checking
Idea of FairCTL model checking

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

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

1. ... preprocessing ...

2. Build the parse tree of $\Phi$ and process it in bottom-up-manner. Treatment of:
   - $true$, $a \in AP$, $\land$, $\neg$: as for standard CTL
   - $\exists \Diamond$, $\exists U$: via standard CTL model checking
   - $\exists \square$: via analysis of SCCs
recursive computation of the fair satisfaction sets:

\[ \text{Sat}_{\text{fair}}(\psi) = \{ s \in S : s \models_{\text{fair}} \psi \} \]
recursive computation of the fair satisfaction sets:

\[ \text{Sat}_{\text{fair}}(\psi) = \{ s \in S : s \models_{\text{fair}} \psi \} \]

simple cases: \( \psi = \text{true} \) or \( \psi = a \in AP \) or the outermost operator of \( \psi \) is a negation or conjunction:
CTT model checking with fairness

recursive computation of the fair satisfaction sets:

\[ \text{Sat}_{\text{fair}}(\psi) = \{ s \in S : s \models_{\text{fair}} \psi \} \]

simple cases: \( \psi = \text{true} \) or \( \psi = a \in \text{AP} \) or the outermost operator of \( \psi \) is a negation or conjunction:

\[
\begin{align*}
\text{Sat}_{\text{fair}}(\text{true}) &= S \\
\text{Sat}_{\text{fair}}(a) &= \{ s \in S : a \in L(s) \} \\
\text{Sat}_{\text{fair}}(\neg \psi) &= S \setminus \text{Sat}_{\text{fair}}(\psi) \\
\text{Sat}_{\text{fair}}(\psi_1 \land \psi_2) &= \text{Sat}_{\text{fair}}(\psi_1) \cap \text{Sat}_{\text{fair}}(\psi_2)
\end{align*}
\]
Idea of FairCTL model checking

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

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

1. ... preprocessing ...

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

   - $\text{true}$, $a \in AP$, $\land$, $\neg$: as for standard CTL
   - $\exists \bigcirc$, $\exists U$: via standard CTL model checking
   - $\exists \Box$: via analysis of SCCs
FairCTL model checking: treatment of $\exists\bigcirc$
FairCTL model checking: treatment of $\exists \bigcirc$

\[ fair = \Box \Diamond \text{red} \]
FairCTL model checking: treatment of $\exists \Box$

\[
\text{fair} = \Box \Diamond \text{red}
\]

\[
s \nvDash_{\text{fair}} \exists \Box \text{green}
\]
FairCTL model checking: treatment of $\exists O$

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

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

as $s' \not\models_{\text{fair}} \exists \Box \text{true}$
FairCTL model checking: treatment of $\exists$  

\[ \text{Fair} = \Box \Diamond \text{red} \]

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

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

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

\[ a_{\text{fair}} \in L(s) \text{ iff } s \models_{\text{fair}} \exists \Box \text{true} \]
FairCTL model checking: treatment of \(\exists O\)

\[
\begin{align*}
\text{fair} & = \Box \Diamond \text{red} \\
\text{redfair} & = \Box \Diamond \text{redfair} = \Box \Diamond \text{red} \\
\text{greens} & \neq \text{fair} \exists O \\
\text{trues} & \neq \text{fair} \exists \Box \\
\text{true} & \\
\end{align*}
\]

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

\[
a_{\text{fair}} \in L(s) \iff s \models_{\text{fair}} \exists \Box \text{true}
\]
FairCTL model checking: treatment of $\exists \bigcirc$.

\[
\text{fair} = \Box \Diamond \text{red}
\]

\[
s \not\models_{\text{fair}} \exists \bigcirc \text{green}
\]

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

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

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

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

\[
s \models_{\text{fair}} \exists \bigcirc b \text{ iff } s \models \exists \bigcirc (b \land a_{\text{fair}})
\]
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 $s$:

$$s \models_{fair} \exists \Box b \text{ iff } s \models \exists \Box (b \land a_{fair})$$

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

$$s \models_{fair} \exists \Box b \text{ iff } s \models \exists \Box (b \land a_{fair})$$

$$s \models_{fair} \exists (c \cup b) \text{ iff } s \models \exists (c \cup (b \land a_{fair}))$$
introduce an additional atomic proposition $a_{fair}$ s.t.

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

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

$$s \models_{fair} \exists \Box b \iff s \models \exists \Box (b \land a_{fair})$$

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

**hence:** treatment of $\exists \Box$ and $\exists U$ for FairCTL via

- special methods to compute $\text{Sat}_{fair}(\exists \Box true)$
- standard CTL model checking for $\exists \Box$ and $\exists U$
Example: treatment of $\exists \diamond$

$T$

$\{b\}$

$\{c\}$

$\{b\}$

$\emptyset$

CTL formula $\exists \diamond c$

strong fairness assumption: $\textit{fair} = \Box \diamond b \rightarrow \Box \diamond c$
Example: treatment of $\exists \Diamond$

CTL formula $\exists \Diamond c$

strong fairness assumption: $fair = \Box \Diamond b \rightarrow \Box \Diamond c$
Example: treatment of $\exists \Diamond$

$\mathcal{T}$

$\{b\}$

$\{c\}$  $\models c \land a_{fair}$

$\{b\}$

CTL formula $\exists \Diamond c$

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

strong fairness assumption:  $fair = \Box \Diamond b \rightarrow \Box \Box \Diamond c$
Example: treatment of $\exists$\Diamond

$\mathcal{T}$

$\{b\}$

$\{c\}$

$\{b\}$

$\mathcal{T} \models c \land a_{fair}$

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

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

$\mathcal{T} \models \exists$\Diamond (c $\land$ $a_{fair}$)
Example: treatment of $\exists \Diamond$

CTL formula $\exists \Diamond c$

$\exists \Diamond (c \land a_{\text{fair}})$

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

$\mathcal{T} \models \exists \Diamond (c \land a_{\text{fair}}) \implies \mathcal{T} \models_{\text{fair}} \exists \Diamond c$
Example: treatment of $\exists U$

$\mathcal{T}$:

$\emptyset$

$\{c\}$

$\{b\}$

$\mathcal{T} \models \exists(\neg b U c)$
Example: treatment of $\exists U$

$\mathcal{T}$:

\[
\begin{array}{ccc}
& \xrightarrow{s} & \\
\varnothing & \downarrow & \\
& \xrightarrow{\{c\}} & \\
& \xrightarrow{\{b\}} & \\
\end{array}
\]

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

$\mathcal{T} \models \exists(\neg b \cup c)$
Example: treatment of $\exists U$

$T:$

\[
\begin{array}{c}
\{ c \} \\
\{ b \}
\end{array}
\]

$\downarrow \not\models a_{\text{fair}}$

$\emptyset$

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

$T \models \exists (\neg b \cup c)$
Example: treatment of $\exists U$

$\mathcal{T}$:

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

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

strong fairness assumption: $a_{\text{fair}} = \BoxDiamond b \rightarrow \BoxDiamond c$
Example: treatment of $\exists U$

$\mathcal{T}$:

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

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

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

$\Rightarrow$

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

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

$\mathcal{T} \models \exists(\neg b \cup c)$
Example: treatment of $\exists U$

$\mathcal{T}$:

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

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

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

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

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

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

$\mathcal{T} \models \exists (\neg b \cup c)$
Example: treatment of $\exists U$

$\mathcal{T}$:

- $s$ transitions to $\emptyset$
- $\{c\}$ transitions to $a_{\text{fair}}$
- $\{b\}$ transitions to $a_{\text{fair}}$

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

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

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

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

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

\[ s \models_{fair} \exists \Box \exists (c \cup b) \quad \text{iff} \quad s \models \exists \Box \exists (c \cup (b \land a_{fair})) \]
Correct or wrong?

\[
s \models_{\text{fair}} \exists \Box \exists (c \cup b) \quad \text{iff} \quad s \models \exists \Box \exists (c \cup (b \land a_{\text{fair}}))
\]

correct.
Correct or wrong?

\[
s \models_{\text{fair}} \exists \bigcirc \exists (c \cup b) \iff s \models \exists \bigcirc \exists (c \cup (b \land a_{\text{fair}}))
\]

correct. Note that:

if \( s_0 s_1 \ldots s_{n-1} s_n \) is a path fragment from \( s_0 = s \) s.t. \( s_n \models a_{\text{fair}} \) then \( s_0, s_1, \ldots, s_{n-1} \models a_{\text{fair}} \).
Correct or wrong?

\[
s \models_{\text{fair}} \exists \bigcirc \exists (c \cup b) \iff s \models \exists \bigcirc \exists (c \cup (b \land a_{\text{fair}}))
\]

correct. Note that:

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

\[
s \models \exists \bigcirc \exists (c \cup (b \land a_{\text{fair}})) \iff s \models \exists \bigcirc \exists ((c \land a_{\text{fair}}) \cup (b \land a_{\text{fair}}))
\]
Correct or wrong?

\[
\begin{align*}
s \models_{\text{fair}} \exists \bigcirc \exists (c \lor b) & \quad \text{iff} \quad s \models \exists \bigcirc \exists (c \lor (b \land a_{\text{fair}})) \\
\end{align*}
\]

correct. Note that:

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

\[
\begin{align*}
s \models & \quad \exists \bigcirc \exists (c \lor (b \land a_{\text{fair}})) \\
\iff & \quad s \models \exists \bigcirc \exists ((c \land a_{\text{fair}}) \lor (b \land a_{\text{fair}})) \\
\iff & \quad s \models \exists \bigcirc (\exists (c \lor (b \land a_{\text{fair}})) \land a_{\text{fair}})
\end{align*}
\]
Correct or wrong?

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

correct. Note that:

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

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

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

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

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

\[ s \models_{\text{fair}} \exists \bigcirc \exists (c \cup b) \iff s \models \exists \bigcirc \exists (c \cup (b \land a_{\text{fair}})) \]

correct.

\[ s \models_{\text{fair}} \exists \bigcirc \exists (c \cup b) \iff s \models \exists \bigcirc (\exists (c \cup b) \land a_{\text{fair}}) \]
Correct or wrong?

\[ s \models_{\text{fair}} \exists \diam \exists (c \cup b) \iff s \models \exists \diam \exists (c \cup (b \land a_{\text{fair}})) \]

correct.

\[ s \models_{\text{fair}} \exists \diam \exists (c \cup b) \iff s \models \exists \diam (\exists (c \cup b) \land a_{\text{fair}}) \]

wrong.

\[ \text{fair} = \Box \Diamond \text{gray} \]
Correct or wrong?

\[
s \models_{\text{fair}} \exists \lozenge \exists (c \cup b) \text{ iff } s \models \exists \lozenge \exists (c \cup (b \land a_{\text{fair}}))
\]

correct.

\[
s \models_{\text{fair}} \exists \lozenge \exists (c \cup b) \text{ iff } s \models \exists \lozenge (\exists (c \cup b) \land a_{\text{fair}})
\]

wrong.

\[
\text{fair} = \square \diamond \text{gray}
\]
Correct or wrong?

\[
s \models_{\text{fair}} \exists \diamond \exists (c \cup b) \iff s \models \exists \diamond \exists (c \cup (b \land a_{\text{fair}}))
\]

correct.

\[
s \models_{\text{fair}} \exists \diamond \exists (c \cup b) \iff s \models \exists \diamond (\exists (c \cup b) \land a_{\text{fair}})
\]

wrong.

\[
\text{fair} = \Box \Diamond \text{gray}
\]
\[
\text{Sat}_{\text{fair}}(\exists (c \cup b)) = \emptyset
\]
Correct or wrong?

\[ s \models_{\text{fair}} \exists \diamond \exists (c \cup b) \text{  iff  } s \models \exists \diamond \exists (c \cup (b \land a_{\text{fair}})) \]

correct.

\[ s \models_{\text{fair}} \exists \diamond \exists (c \cup b) \text{  iff  } s \models \exists \diamond (\exists (c \cup b) \land a_{\text{fair}}) \]

wrong.

\( \text{fair} = \Box \diamond \text{gray} \)

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

\[ s \not\models_{\text{fair}} \exists \diamond \exists (c \cup b) \]
Correct or wrong?

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

correct.

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

wrong.

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

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

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

$$s \models \exists \bigcirc (\exists (c \cup b) \land a_{\text{fair}})$$
Correct or wrong?

\[ s \models_{\text{fair}} \exists c \iff s \models \exists (c \land a_{\text{fair}}) \]
Correct or wrong?

\[
\begin{align*}
  s \models_{fair} \exists \Box c \text{ iff } s \models \exists \Box (c \land a_{fair})
\end{align*}
\]

wrong.

\[
\begin{align*}
  fair & = \Box \Diamond b
\end{align*}
\]
Correct or wrong?

\[ s \models_{\text{fair}} \exists c \iff s \models \exists (c \land a_{\text{fair}}) \]

drawn.

\[ \text{fair} = \Box \Diamond b \]

\[ s_0 \models a_{\text{fair}} \]

\[ s_1 \models a_{\text{fair}} \]
Correct or wrong?

\[ s \models_{\text{fair}} \exists \Box c \quad \text{iff} \quad s \models \exists \Box (c \land a_{\text{fair}}) \]

wrong.

\[ \text{fair} = \Box\Diamond b \]

\[ s_0 \models a_{\text{fair}} \quad s_1 \models a_{\text{fair}} \]

regard state \( s = s_0 \):
Correct or wrong?

\[ s \models_{\text{fair}} \exists \Box c \iff s \models \exists \Box (c \land a_{\text{fair}}) \]

Wrong.

\[ \text{fair} = \Box \Diamond b \]

\[ s_0 \models a_{\text{fair}} \]

\[ s_1 \models a_{\text{fair}} \]

regard state \( s = s_0 \):

\[ s \models \exists \Box (c \land a_{\text{fair}}), \]
Correct or wrong?

\[ s \models_{\text{fair}} \exists \Box c \iff s \models \exists \Box (c \land a_{\text{fair}}) \]

Wrong.

\[ \text{fair} = \Box \Diamond b \]

\begin{align*}
\text{s}_0 & \models a_{\text{fair}} \\
\text{s}_1 & \models a_{\text{fair}}
\end{align*}

regard state \( s = s_0 \):

\[ s \models \exists \Box (c \land a_{\text{fair}}), \]

\[ \uparrow \]

path \( \pi = s_0 s_0 s_0 s_0 \ldots \models \Box (c \land a_{\text{fair}}) \)
Correct or wrong?

\[ s \models_{\text{fair}} \exists c \quad \text{iff} \quad s \models \exists (c \land a_{\text{fair}}) \]

Wrong.

\[ \text{fair} = \Box \Diamond b \]
\[ s_0 \models a_{\text{fair}} \]
\[ s_1 \models a_{\text{fair}} \]

regard state \( s = s_0 \):

\[ s \models \exists \Box (c \land a_{\text{fair}}), \quad \text{but} \quad s \not\models_{\text{fair}} \exists \Box c \]

\[ \text{path } \pi = s_0 s_0 s_0 s_0 \ldots \models \Box (c \land a_{\text{fair}}) \]
Idea of FairCTL model checking

given: finite transition system $T$

CTL formula $\Phi$ in $\exists$-normal form

CTL fairness assumption $\text{fair}

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

1. ... preprocessing ...

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

   - $true$, $a \in AP$, $\land$, $\neg$: as for standard CTL
   - $\exists \bigcirc$, $\exists U$: via standard CTL model checking
   - $\exists \Box$: via analysis of SCCs
∃□Ψ under strong fairness

$\text{fair} = \Box \Diamond b \rightarrow \Box \Diamond c$, CTL state formula $\Psi$
Under strong fairness,

\[ \text{fair} = \square \Diamond b \rightarrow \square \Diamond c, \]

where \( \Psi \) is a CTL state formula.

1. Calculate \( \text{Sat}_{\text{fair}}(\Psi) \)
∃ψ under strong fairness

\[ fair = \Box \Diamond b \rightarrow \Box \Diamond c, \quad \text{CTL state formula } \Psi \]

1. calculate \( Sat_{\text{fair}}(\Psi) \)
2. replace \( \Psi \) with a fresh atomic proposition \( a = a_\Psi \)
∃ψ under strong fairness

\[ \text{fair} = \square \Diamond b \rightarrow \square \Diamond c, \quad \text{CTL state formula } \psi \]

\[ T: \]

\{c, a\} \rightarrow \{a\} \rightarrow \{c, a\} \rightarrow \{b, a\} \rightarrow \emptyset \]

\[ T \models_{\text{fair}} \exists \square \psi \, ? \]

1. calculate \( \text{Sat}_{\text{fair}}(\psi) \)
2. replace \( \psi \) with a fresh atomic proposition \( a = a_\psi \)
∃□Ψ under strong fairness

\[ \text{fair} = \square \Diamond b \rightarrow \square \Diamond c, \quad \text{CTL state formula } \Psi \]

1. calculate \( \text{Sat}_{\text{fair}}(\Psi) \)
2. replace \( \Psi \) with a fresh atomic proposition \( a = a_\Psi \)
3. calculate \( \text{Sat}_{\text{fair}}(\exists \Box a) \)
∃□Ψ under strong fairness

**fair** = □◊b → □◊c,  
CTL state formula Ψ

1. Calculate $Sat_{fair}(Ψ)$
2. Replace Ψ with a fresh atomic proposition $a = a_{Ψ}$
3. Calculate $Sat_{fair}(∃□a)$
∃□Ψ under strong fairness

**Fair** = □◊b → □◊c,  
CTL state formula Ψ

\[
\mathcal{I}:
\]

\[
\begin{array}{c}
\{c, a\} \\
\{c, a\} \\
\{b, a\}
\end{array}
\]


\[
\begin{array}{c}
\{a\} \\
\{a\} \\
\{a\}
\end{array}
\]

\[
\begin{array}{c}
\{c, a\} \\
\{c, a\} \\
\{c, a\}
\end{array}
\]

\[
\begin{array}{c}
\varnothing \\
\varnothing \\
\varnothing
\end{array}
\]

digraph \( G_a \)
doesn’t contain any fair path

1. calculate \( \text{Sat}_{\text{fair}}(\Psi) \)
2. replace Ψ with a fresh atomic proposition \( a = a_{\psi} \)
3. calculate \( \text{Sat}_{\text{fair}}(\exists □ a) \)
∃□Ψ under strong fairness

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

$T:$

- $\{c, a\}$
- $\{c, a\}$
- $\{b, a\}$

digraph $G_a$

doesn’t contain any fair path

$T \not\models_{\text{fair}} \exists \Box \Psi$

1. calculate $\text{Sat}_{\text{fair}}(\Psi)$
2. replace $\Psi$ with a fresh atomic proposition $a = a_\Psi$
3. calculate $\text{Sat}_{\text{fair}}(\exists \Box a) = \emptyset$
Treatment of $\exists \Box a$ for FairCTL

given: finite TS $T$, atomic proposition $a$

CTL fairness assumption $\text{fair}$

goal: compute $\text{Sat}_{\text{fair}}(\exists \Box a)$
Treatment of $\exists \Box a$ for FairCTL

given: finite TS $T$, atomic proposition $a$

CTL fairness assumption $\text{fair}$

goal: compute $\text{Sat}_{\text{fair}}(\exists \Box a)$

if all states are labeled by $a$:

this technique yields a method
to compute $\text{Sat}_{\text{fair}}(\exists \Box \text{true})$
Treatment of $\exists \Box a$ for FairCTL

given: finite TS $T$, atomic proposition $a$

CTL fairness assumption $\text{fair}$

goal: compute $\text{Sat}_{\text{fair}}(\exists \Box a)$

if all states are labeled by $a$:

this technique yields a method

to compute $\text{Sat}_{\text{fair}}(\exists \Box \text{true})$

here: explanations only for strong fairness

$$\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$$
Treatment of $\exists$ under strong fairness

\[
\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)
\]
Treatment of $\exists \Box a$ under strong fairness

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

$s \models_{\text{fair}} \exists \Box a$ iff there exists a path fragment $s_0 s_1 \ldots s_n \ldots s_{n+r}$
Treatment of $\exists \Box$ under strong fairness

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

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

\[
\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box ♦ b_i \rightarrow \Box ♦ c_i)
\]

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

\[s_0 s_1 \ldots s_n \ldots s_{n+r}\]

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

- \(s_j \models a\) for all \(0 \leq j \leq n + r\)
Treatment of $\exists \Box$ under strong fairness

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

$s \models_{fair} \exists \Box a$ iff there exists a path fragment $s_0 s_1 \ldots s_n \ldots s_{n+r}$ such that $r \geq 1$, $s = s_0$, $s_n = s_{n+r}$ and

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

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

$s \models_{\text{fair}} \exists □ a$ 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 $1 \leq i \leq k$:
  
  $\{s_{n+1}, \ldots, s_{n+r}\} \cap \text{Sat}(b_i) = \emptyset$

  or
  
  $\{s_{n+1}, \ldots, s_{n+r}\} \cap \text{Sat}(c_i) \neq \emptyset$
$\exists a$ under strong fairness

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

$\circ \models a \quad \circ \not\models a$
∃a under strong fairness

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

analyze the digraph $G_a$ that results from $\mathcal{I}$ by removing all states $s$ with $s \not\models a$
∃a under strong fairness

does \( T \models_{\text{fair}} \exists \Box a \) hold?

digraph \( G_a \)

analyze the digraph \( G_a \) that results from \( T \) by removing all states \( s \) with \( s \not\models a \)
∃ □ a under strong fairness

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

digraph $G_a$

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

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

$\text{fair} = (\Box □ b_1 \rightarrow □ □ c_1) \land (\Box □ b_2 \rightarrow □ □ c_2)$
∃□a under strong fairness

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

digraph $G_a$

\[
\begin{align*}
\hat{=} & \{b_1\} & \hat{=} & \{c_1\} \\
\hat{=} & \{b_2\} & \hat{=} & \{c_2\} \\
s_0 (s_1 s_2)^\omega & \models \neg □◊b_2 \land □◊c_1
\end{align*}
\]

$\text{fair} = (□◊b_1 \rightarrow □◊c_1) \land (□◊b_2 \rightarrow □◊c_2)$
∃□a under strong fairness

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

digraph $G_a$

$\widehat{\bullet} \equiv \{b_1\}$ \hspace{1cm} $\widehat{\bullet} \equiv \{c_1\}$

$\widehat{\bullet} \equiv \{b_2\}$ \hspace{1cm} $\widehat{\bullet} \equiv \{c_2\}$

$s_0 (s_1 s_2)^\omega \models \neg □\Diamond b_2 \land □\Diamond c_1$

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

$\text{fair} = (□\Diamond b_1 \rightarrow □\Diamond c_1) \land (□\Diamond b_2 \rightarrow □\Diamond c_2)$
Treatment of $\exists \Box$ under strong fairness

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

$s \models_{\text{fair}} \exists \Box a$ iff there exists a path fragment $s_0 \ s_1 \ldots s_n \ldots s_{n+r}$ such that $r \geq 1$, $s = s_0$, $s_n = s_{n+r}$ and

- $s_j \models a$ for all $0 \leq j \leq n + r$
- for all $1 \leq i \leq k$: $\{s_{n+1}, \ldots, s_{n+r}\} \cap \text{Sat}(b_i) = \emptyset$
  or $\{s_{n+1}, \ldots, s_{n+r}\} \cap \text{Sat}(c_i) \neq \emptyset$
Treatment of $\exists \Box$ under strong fairness

\[
\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box \diamond b_i \rightarrow \Box \diamond c_i)
\]

\[
s \models_{\text{fair}} \exists \Box a \quad \text{iff} \quad \text{there exists a path fragment}
\]
\[
s_0 \ s_1 \ldots \ s_n \ldots \ s_{n+r}
\]

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

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

- for all $1 \leq i \leq k$: \[
\{s_{n+1}, \ldots, s_{n+r}\} \cap \text{Sat}(b_i) = \emptyset \\
\text{or} \quad \{s_{n+1}, \ldots, s_{n+r}\} \cap \text{Sat}(c_i) \neq \emptyset
\]

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

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

$s \models_{\text{fair}} \exists \Box a$ iff there exists a path fragment $s_0 s_1 \ldots s_n \ldots s_{n+r}$ such that $r \geq 1$, $s = s_0$, $s_n = s_{n+r}$ and

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

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

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

$s \models_{fair} \exists \Box a$ 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 $s' \not\models a$
Treatment of $\exists \Box$ under strong fairness

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

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

1. $D$ is reachable from $s$
2. for all $1 \leq i \leq k$:
   $$D \cap Sat(b_i) = \emptyset \text{ or } D \cap Sat(c_i) \neq \emptyset$$

$G_a$: digraph that arises from $T$ by removing all states $s'$ with $s' \not\models a$
Treatment of $\exists \Box$ under strong fairness

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

$s \models_{\textit{fair}} \exists \Box a$ 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 $1 \leq i \leq k$:
   
   $D \cap \text{Sat}(b_i) = \emptyset$ or $D \cap \text{Sat}(c_i) \neq \emptyset$

Note: if $s \models_{\textit{fair}} \exists \Box a$ then there might be no SCC $D$ where (1) and (2) hold.
Example: computation of $Sat_{fair}(\exists\Box a)$

$T$

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

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

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

$\mathcal{T}$

digraph $G_a$

$fair = (\Box \Diamond b_1 \rightarrow \Box \Diamond c_1) \land (\Box \Diamond b_2 \rightarrow \Box \Diamond c_2)$
Example: computation of $\text{Sat}_{\text{fair}}(\exists \Box a)$

$\mathcal{T}$

$\text{digraph } G_a$

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

$s_0 \models \text{fair} \exists \Box a$
Example: computation of $\text{Sat}_{\text{fair}}(\exists \Box a)$

\[ \text{fair} = (\Box \Diamond b_1 \rightarrow \Box \Diamond c_1) \land (\Box \Diamond b_2 \rightarrow \Box \Diamond c_2) \]

\[ s_0 \models_{\text{fair}} \exists \Box a \quad \text{as} \quad s_0 \ s_1 \ s_2 \ s_1 \ s_2 \ldots \models_{\text{LTL}} \text{fair} \]
Example: computation of $Sat_{\text{fair}}(\exists \square a)$

$\mathcal{T}$

$\text{digraph } G_a$

\[
\begin{align*}
\text{fair} &= (\square \Diamond b_1 \rightarrow \square \Diamond c_1) \land (\square \Diamond b_2 \rightarrow \square \Diamond c_2)
\end{align*}
\]

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

$Sat_{\text{fair}}(\exists \square a) = \{s_0, s_1, s_2, s_3\}$
treatment of $\exists \Box$ for \textbf{CTL} with fairness
CTL model checking with fairness

treatment of $\exists \Box$ for $\textbf{CTL}$ 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 \textbf{CTL} with fairness

\textit{here:} explanations only for \textbf{strong fairness}

\begin{itemize}
  \item \textit{case 1:} unconditional fairness
  \item \textit{case 2:} $\text{fair} = \Box\Diamond b \rightarrow \Box\Diamond c$
  \item \textit{case 3:} arbitrary strong fairness assumption
  \begin{equation*}
  \text{fair} = \bigwedge_{1 \leq i \leq k} (\Box\Diamond b_i \rightarrow \Box\Diamond c_i)
  \end{equation*}
\end{itemize}

weak fairness and combinations of weak/strong fairness can be treated in an analogous way
treatment of $\exists \Box$ for $\text{CTL}$ with fairness

*here:* explanations only for strong fairness

<table>
<thead>
<tr>
<th>Case 1: Unconditional fairness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case 2: $\text{fair} = \Box\Diamond b \rightarrow \Box\Diamond c$</td>
</tr>
<tr>
<td>Case 3: Arbitrary strong fairness assumption</td>
</tr>
<tr>
<td>$\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box\Diamond b_i \rightarrow \Box\Diamond c_i)$</td>
</tr>
</tbody>
</table>

Weak fairness and combinations of weak/strong fairness can be treated in an analogous way.
∃a under unconditional fairness

\[ \text{fair} = \bigwedge_{1 \leq i \leq k} \Box \Diamond c_i \]
∃□a under unconditional fairness

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

\[ s \models_{\text{fair}} \exists□a \quad \text{iff} \quad ? \]
\( \exists a \) under unconditional fairness

\[
\text{fair} = \bigwedge_{1 \leq i \leq k} \lozenge \Box c_i
\]

\( s \models_{\text{fair}} \exists a \) iff there exists a nontrivial SCC \( C \) in \( G_a \) that is reachable from \( s \) and \( C \cap \text{Sat}(c_i) \neq \emptyset \) for \( i = 1, \ldots, k \)
∃a under unconditional fairness

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

\[ s \models_{\text{fair}} \exists \Box a \quad \text{iff} \quad \text{there exists a nontrivial SCC } C \]

in \( G_a \) that is reachable from \( s \) and \( C \cap \text{Sat}(c_i) \neq \emptyset \) for \( i = 1, \ldots, k \)

digraph \( G_a \)

fairness assumption:

\[ \text{fair} = \Box \Diamond c_1 \land \Box \Diamond c_2 \]
\( \exists a \) under unconditional fairness

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

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

digraph \( G_a \)

Fairness assumption:

\[
\text{fair} = \Box \Diamond c_1 \land \Box \Diamond c_2
\]

\( s \nvdash_{\text{fair}} \exists a \)
∃□a under unconditional fairness

\[
\text{fair} = \bigwedge_{1 \leq i \leq k} \Box♦c_i
\]

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

digraph \( G_a \)

fairness assumption:
\[
\text{fair} = \Box♦c_1 \land \Box♦c_2
\]

\( s \not\models_{\text{fair}} \exists□a \)
∃a under unconditional fairness

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

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

digraph \ G_a

fairness assumption:
\[ \text{fair} = \Box \Diamond c_1 \land \Box \Diamond c_2 \]
\( \exists \Box a \text{ under unconditional fairness} \)

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

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

digraph \( G_a \)

fairness assumption:
\[
\text{fair} = \Box \Diamond c_1 \land \Box \Diamond c_2
\]

\[
s \models_{\text{fair}} \exists \Box a
\]
treatment of $\exists \Box$ for CTL with fairness

*here*: explanations only for strong fairness

<table>
<thead>
<tr>
<th>Case 1: unconditional fairness</th>
<th>✓</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case 2: $\textit{fair} = \Box \Diamond b \rightarrow \Box \Diamond c$</td>
<td></td>
</tr>
<tr>
<td>Case 3: arbitrary strong fairness assumption</td>
<td></td>
</tr>
</tbody>
</table>

$$\textit{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$$
treatment of $\exists \Box$ for CTL with fairness

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

<table>
<thead>
<tr>
<th>Case</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>unconditional fairness</td>
</tr>
<tr>
<td>2</td>
<td>$fair = \Box \Diamond b \rightarrow \Box \Diamond c$</td>
</tr>
<tr>
<td>3</td>
<td>arbitrary strong fairness assumption</td>
</tr>
</tbody>
</table>

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

\[ \text{fair} = \Box \Diamond b \rightarrow \Box \Diamond c \]
Strong fairness: 1 fairness requirement

\[ \text{fair} = \square \Diamond b \rightarrow \square \Diamond c \]

digraph \( G_a \)
Strong fairness: 1 fairness requirement

\[ \text{fair} = \Box \Diamond b \rightarrow \Box \Diamond c \]

digraph \( G_a \)

nontrivial SCC \( C \) of \( G_a \) with \( C \cap \text{Sat}(c) \neq \emptyset \)
Strong fairness: 1 fairness requirement

\[ \text{fair} = \Box \Diamond b \rightarrow \Box \Diamond c \]

digraph \( G_a \)

nontrivial SCC \( C \) of \( G_a \) with \( C \cap \text{Sat}(c) \neq \emptyset \)
Strong fairness: 1 fairness requirement

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

digraph $G_a$
Strong fairness: 1 fairness requirement

\[
\text{fair} = \Box \Diamond b \rightarrow \Box \Diamond c
\]

digraph $G_a$

\[
\begin{aligned}
\{ c \} &\xrightarrow{} &\{ b \} \\
\{ b \} &\xrightarrow{} &s \\
\end{aligned}
\]

\[
\begin{aligned}
s &\xrightarrow{\text{fair}} &\exists \Box a
\end{aligned}
\]
Strong fairness: 1 fairness requirement

\[ \text{fair} = \square \diamond b \rightarrow \square \diamond c \]

digraph \( G_a \)

\[
\begin{align*}
\{c\} & \rightarrow s \\
\{b\} & \rightarrow s
\end{align*}
\]

\[ \text{strongly connected node-set } D \text{ of } G_a \text{ with } D \cap \text{Sat}(b) = \emptyset \]
Strong fairness: 1 fairness requirement

\[ \text{fair} = \Box \Diamond b \rightarrow \Box \Diamond c \]

digraph \( G_a \)

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

\( s \models_{\text{fair}} \exists \Box a \)
treatment of $\exists \Box$ for CTL with fairness

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

<table>
<thead>
<tr>
<th>Case</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case 1</td>
<td>unconditional fairness</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td>Case 2</td>
<td>$fair = \Box \Diamond b \rightarrow \Box \Diamond c$</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td>Case 3</td>
<td>arbitrary strong fairness assumption</td>
<td></td>
</tr>
</tbody>
</table>

$$fair = \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$$
treatment of $\exists \Box$ for CTL with fairness

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

<table>
<thead>
<tr>
<th>Case</th>
<th>Fairness Assumption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case 1</td>
<td>unconditional fairness</td>
</tr>
<tr>
<td>Case 2</td>
<td>$fair = \Box \Diamond b \rightarrow \Box \Diamond c$</td>
</tr>
<tr>
<td>Case 3</td>
<td>arbitrary strong fairness assumption</td>
</tr>
</tbody>
</table>

$fair = \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$
Example: 2 strong fairness conditions
Example: 2 strong fairness conditions

\[ \text{fair} = (\Box \Diamond b_1 \rightarrow \Box \Diamond c_1) \land (\Box \Diamond b_2 \rightarrow \Box \Diamond c_2) \]
Example: 2 strong fairness conditions

\[ \text{fair} = (\square\diamond b_1 \rightarrow \square\diamond c_1) \land (\square\diamond b_2 \rightarrow \square\diamond c_2) \]

digraph \( G_a \)
Example: 2 strong fairness conditions

\[ \text{fair} = (\Box\Diamond b_1 \rightarrow \Box\Diamond c_1) \land (\Box\Diamond b_2 \rightarrow \Box\Diamond c_2) \]

digraph \( G_a \)

first SCC: \( C_1 \cap \text{Sat}(c_2) = \emptyset \)
Example: 2 strong fairness conditions

\[ \text{fair} = (\Box \Diamond b_1 \rightarrow \Box \Diamond c_1) \land (\Box \Diamond b_2 \rightarrow \Box \Diamond c_2) \]

digraph \( G_a \)

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

Analyze \( C_1 \setminus \text{Sat}(b_2) \) w.r.t. \( \Box \Diamond b_1 \rightarrow \Box \Diamond c_1 \)
Example: 2 strong fairness conditions

\[
\text{fair} = (\square \diamond b_1 \rightarrow \square \diamond c_1) \land (\square \diamond b_2 \rightarrow \square \diamond c_2)
\]

digraph \( G_a \)

\[C_1 \cap \text{Sat}(c_2) = \emptyset\]

first SCC: \( C_1 \setminus \text{Sat}(b_2) \) w.r.t. \( \square \diamond b_1 \rightarrow \square \diamond c_1 \)
Example: 2 strong fairness conditions

\[
\text{fair} = (\square \diamond b_1 \rightarrow \square \diamond c_1) \land (\square \diamond b_2 \rightarrow \square \diamond c_2)
\]

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

Analyze \( C_1 \setminus \text{Sat}(b_2) \) w.r.t. \( \square \diamond b_1 \rightarrow \square \diamond c_1 \)

\( \rightsquigarrow \) there is no cycle
Example: 2 strong fairness conditions

\[
\text{fair} = (\square \diamond b_1 \rightarrow \square \diamond c_1) \land (\square \diamond b_2 \rightarrow \square \diamond c_2)
\]
Example: 2 strong fairness conditions

\[ \text{fair} = (\Box \Diamond b_1 \rightarrow \Box \Diamond c_1) \land (\Box \Diamond b_2 \rightarrow \Box \Diamond c_2) \]

digraph \ G_a

second SCC: \quad C_2 \cap \text{Sat}(c_1) = \emptyset
Example: 2 strong fairness conditions

\[ \text{fair} = (\Box ♦ b_1 \rightarrow \Box ♦ c_1) \land (\Box ♦ b_2 \rightarrow \Box ♦ c_2) \]

digraph \( G_a \)

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

analyze \( C_2 \setminus \text{Sat}(b_1) \) w.r.t. \( \Box ♦ b_2 \rightarrow \Box ♦ c_2 \)
Example: 2 strong fairness conditions

\[ \text{fair} = (\Box\Diamond b_1 \rightarrow \Box\Diamond c_1) \land (\Box\Diamond b_2 \rightarrow \Box\Diamond c_2) \]

digraph \( G_a \)

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

\[ fair = (\Box\Diamond b_1 \rightarrow \Box\Diamond c_1) \land (\Box\Diamond b_2 \rightarrow \Box\Diamond c_2) \]

digraph \( G_a \)

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

Analyze \( C_2 \setminus \text{Sat}(b_1) \) w.r.t. \( \Box\Diamond b_2 \rightarrow \Box\Diamond c_2 \)
Example: 2 strong fairness conditions

\[
\text{fair} = (\Box ♦ b_1 \rightarrow \Box ♦ c_1) \land (\Box ♦ b_2 \rightarrow \Box ♦ c_2)
\]

digraph \( G_a \)

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

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

hence: \( s \models_{\text{fair}} \exists \Box a \)
Calculation of $\text{Sat}_{\text{fair}}(\exists \Box a)$
Calculation of $\text{Sat}_{\text{fair}}(\exists \square a)$

compute the SCCs of the digraph $G_a$;
compute the SCCs of the digraph $G_a$;

$T := \emptyset$;
compute the SCCs of the digraph $G_a$;

$T := \emptyset$;

FOR ALL nontrivial SCCs $C$ of $G_a$ DO
compute the SCCs of the digraph $G_a$;

$T := \emptyset$;

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

\[ \text{IF } \text{CheckFair}(C, \ldots) \text{ THEN } T := T \cup C \text{ FI} \]

OD
compute the SCCs of the digraph $G_a$;

$T := \emptyset$;

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

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

OD

$Sat_{\text{fair}}(\exists \square a) := \{s \in S : \text{Reach}_{G_a}(s) \cap T \neq \emptyset\}$
compute the SCCs of the digraph $G_a$;

$$T := \emptyset;$$

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

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

OD

$$\text{Sat}_{\text{fair}}(\exists \Box a) := \{ s \in S : \text{Reach}_{G_a}(s) \cap T \neq \emptyset \}$$

backward search from $T$
compute the SCCs of the digraph $G_a$;

$T := \emptyset$;

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

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

OD

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

backward search from $T$

time complexity: $O(\text{size}(T) \cdot |\text{fair}|)$
compute the SCCs of the digraph $G_a$;

$T := \emptyset$;

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

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

OD

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

backward search from $T$

time complexity: $O(\text{size}(T) \cdot |\text{fair}|)$
Recursive algorithm \textit{CheckFair(\ldots)}
Recursive algorithm \textit{CheckFair}(\ldots)\

\begin{align*}
\text{algorithm } \textit{CheckFair}(C, k, \quad & \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)) \\
\end{align*}
Recursive algorithm \textit{CheckFair}(\ldots)

algorithm \textit{CheckFair}(C, k, \bigwedge_{1 \leq i \leq k} (\square \Diamond b_i \rightarrow \square \Diamond c_i)) returns

“true” if there exists a cyclic path fragment
$s_0 s_1 \ldots s_n$ in $C$ such that
\[(s_0 s_1 \ldots s_{n-1})^\omega \models \bigwedge_{1 \leq i \leq k} (\square \Diamond b_i \rightarrow \square \Diamond c_i)\]

“false” otherwise
Recursive algorithm \textit{CheckFair}(\ldots)

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

\begin{align*}
\text{IF } \forall i \in \{1, \ldots, k\}. \ C \cap \text{Sat}(c_i) \neq \emptyset \ \text{THEN return "true" FI}
\end{align*}
Recursive algorithm \texttt{CheckFair}(\ldots)

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

\begin{verbatim}
IF \forall i \in \{1, \ldots, k\}. C \cap \text{Sat}(c_i) \neq \emptyset THEN\ return \ “true” FI
choose j \in \{1, \ldots, k\} with C \cap \text{Sat}(c_j) = \emptyset;
\end{verbatim}
Recursive algorithm \textit{CheckFair( . . . )}

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

\begin{verbatim}
IF \forall i \in \{1,..., k\}. C \cap Sat(c_i) \neq \emptyset THEN return “true” FI
choose j \in \{1,..., k\} with C \cap Sat(c_j) = \emptyset;
remove all states in Sat(b_j);
\end{verbatim}
Recursive algorithm *CheckFair*(...) 

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

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

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

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

OD
\end{verbatim}
Recursive algorithm \textit{CheckFair}(...)

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

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

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

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

choose $j \in \{1, \ldots, k\}$ 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(...)
Complexity of $\text{CheckFair}(\ldots)$

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

IF $\forall i \in \{1, \ldots, k\}$. $C \cap \text{Sat}(c_i) \neq \emptyset$ THEN return “true” FI
choose $j \in \{1, \ldots, k\}$ 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 $\text{CheckFair}(...)$

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

IF $\forall i \in \{1, ..., k\}$. $C \cap \text{Sat}(c_i) \neq \emptyset$ THEN return “true” FI
choose $j \in \{1, ..., k\}$ 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”
OD
return “false”

recurrence for the time complexity:

$$T(n, k) = \ldots \text{ where } n = \text{size}(C)$$
Complexity of \texttt{CheckFair}(\ldots)

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

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

\textbf{time complexity:} \( \mathcal{O}(\text{size}(C) \cdot k) \)
CTL model checking with fairness

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

**Output:** “yes”, if $\mathcal{T} \models_{\text{fair}} \Phi$. “no” otherwise.
CTL model checking with fairness

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

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

*here: preprocessing*
transform $\Phi$ into an equivalent CTL formula
in existential normal form
CTL model checking with fairness

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

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

**here: preprocessing**
transform $\Phi$ into an equivalent CTL formula in existential normal form
i.e., with the basic modalities $\exists O$, $\exists U$ and $\exists \Box$
Model checking algorithm for FairCTL
calculate $\text{Sat}_{\text{fair}}(\exists \Box \text{true})$;
label all states in $\text{Sat}_{\text{fair}}(\exists \Box \text{true})$ with $a_{\text{fair}}$
calculate $\text{Sat}_{\text{fair}}(\exists \Box \text{true})$;

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

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

\[ \text{Sat}_{\text{fair}}(\psi) := \ldots \]

OD
Model checking algorithm for FairCTL

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

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

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

CASE $\Psi$ is:

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

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

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

OD
Model checking algorithm for FairCTL

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

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

CASE $\psi$ is:

$\exists \Box a : Sat_{\text{fair}}(\psi) := Sat(\exists \Box (a \land a_{\text{fair}}))$;
$\exists (a_1 \cup a_2) : Sat_{\text{fair}}(\psi) := Sat(\exists (a_1 \cup (a_2 \land a_{\text{fair}})))$;
$\exists \Box a : Sat_{\text{fair}}(\psi) := ...$

replace $\psi$ with a fresh atomic proposition $a_{\psi}$

OD
Model checking algorithm for FairCTL

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

FOR ALL subformulas $\psi$ of $\Phi$ DO
  CASE $\psi$ is: ................
    $\exists \Box a : Sat_{\text{fair}}(\psi) := Sat(\exists \Box (a \land a_{\text{fair}}))$;
    $\exists (a_1 \cup a_2) : Sat_{\text{fair}}(\psi) := Sat(\exists (a_1 \cup (a_2 \land a_{\text{fair}})))$;
    $\exists \Box a : Sat_{\text{fair}}(\psi) := ...$
  replace $\psi$ with a fresh atomic proposition $a_\psi$
OD

IF $S_0 \subseteq Sat_{\text{fair}}(\Phi)$ THEN return “yes”
ELSE return “no”
FI
Example: CTL model checking with fairness

\[
\Phi = \exists \Diamond \forall \circ (\text{lost} \lor \text{del})
\]

fair = \Box \Diamond \exists \Diamond \text{del}
Example: CTL model checking with fairness

\[ \varphi = \exists \diamond \forall \bigcirc (\text{lost} \lor \text{del}) \]

\[ \text{fair} = \square \diamond \exists \diamond \text{del} \leadsto \square \diamond c \text{ where } \text{Sat}(c) = S \setminus \{\text{error}\} \]
Example: CTL model checking with fairness

\[
\Phi = \exists \Diamond \, \forall \Box \, (\text{lost} \lor \text{del})
\]

\[
\text{fair} = \Box \Diamond \, \exists \Diamond \, \text{del} \iff \Box \Diamond \, c \text{ where } \text{Sat}(c) = S \setminus \{\text{error}\}
\]

\[
\text{Sat}_{\text{fair}}(\exists \Box \, \text{true})
\]
Example: CTL model checking with fairness

\[ \Phi = \exists \diamond \forall \Box (\text{lost} \lor \text{del}) \]

\[ \text{fair} = \Box \diamond \exists \diamond \text{del} \implies \Box \diamond c \text{ where } \text{Sat}(c) = S \setminus \{\text{error}\} \]

\[ \text{Sat}_{\text{fair}}(\exists \Box \text{true}) = \text{Sat}(a_{\text{fair}}) = S \setminus \{\text{error}\} \]
Example: CTL model checking with fairness

\[ \Phi = \exists \ Diamond \ \forall \ Diamond (\text{lost} \lor \text{del}) \]

\[ \equiv \exists \ Diamond \ \neg \exists \ Diamond (\neg \text{lost} \land \neg \text{del}) \]

existential normal form

\[ \text{fair} = \Box \ Diamond \ \exists \ Diamond \ \text{del} \ \leadsto \ \Box \ Diamond \ c \text{ where } \text{Sat}(c) = S \setminus \{\text{error}\} \]

\[ \text{Sat}_{\text{fair}}(\exists \Box \ true) = \text{Sat}(a_{\text{fair}}) = S \setminus \{\text{error}\} \]
Example: CTL model checking with fairness

\[
\Phi = \exists \lozenge \forall \lozenge (\text{lost} \lor \text{del})
\]

\[
\equiv \exists \lozenge \neg \exists \lozenge \neg \left( \neg \text{lost} \land \neg \text{del} \right)
\]

\[\text{fair} = \Box \lozenge \exists \lozenge \text{del} \leadsto \Box \lozenge c \text{ where } \text{Sat}(c) = S \setminus \{\text{error}\}\]

\[\text{Sat}_{\text{fair}}(\exists \Box \text{true}) = \text{Sat}(a_{\text{fair}}) = S \setminus \{\text{error}\}\]
Example: CTL model checking with fairness

\[ \Phi = \exists \diamond \Box (\text{lost} \lor \text{del}) \]

\[ \equiv \exists \diamond \neg \Box (\neg \text{lost} \land \neg \text{del}) \]

\[ \rightsquigarrow \exists \diamond \neg \Box a \]

\[ \text{fair} = \Box \exists \diamond \text{del} \rightsquigarrow \Box \exists \diamond c \text{ where } \text{Sat}(c) = S \setminus \{\text{error}\} \]

\[ \text{Sat}_{\text{fair}}(\exists \Box \text{true}) = \text{Sat}(a_{\text{fair}}) = S \setminus \{\text{error}\} \]
Example: CTL model checking with fairness

\[
\Phi = \exists \Diamond \forall \Diamond (\text{lost} \lor \text{del})
\]

\[
\equiv \exists \Diamond \neg \exists \Diamond (\neg \text{lost} \land \neg \text{del})
\]

\[
\leadsto \exists \Diamond \neg \exists \Diamond \text{a}
\]

\[
\text{fair} = \Box \Diamond \exists \Diamond \text{del} \leadsto \Box \Diamond \text{c} \text{ where } \text{Sat}(c) = S \setminus \{\text{error}\}
\]

\[
\text{Sat}_{\text{fair}}(\exists \Box \text{true}) = \text{Sat}(a_{\text{fair}}) = S \setminus \{\text{error}\}
\]

\[
\text{Sat}_{\text{fair}}(\exists \Diamond \text{a})
\]
Example: CTL model checking with fairness

\[ \Phi = \exists \Diamond \forall \Box (\text{lost} \lor \text{del}) \]
\[ \equiv \exists \Diamond \neg \exists \Box (\neg \text{lost} \land \neg \text{del}) \]
\[ \leadsto \exists \Diamond \neg \exists \Box a \]

\textit{fair} = \Box \Diamond \exists \Diamond \text{del} \leadsto \Box \Diamond c \text{ where Sat}(c) = S \setminus \{\text{error}\} \]
\[ \text{Sat}_{\text{fair}}(\exists \Box \text{true}) = \text{Sat}(a_{\text{fair}}) = S \setminus \{\text{error}\} \]
\[ \text{Sat}_{\text{fair}}(\exists \Box a) = \text{Sat}(\exists \Box (a \land a_{\text{fair}})) \]
Example: CTL model checking with fairness

\[
\Phi = \exists \Diamond \forall \Box (\text{lost} \lor \text{del})
\]

\[
\equiv \exists \Diamond \neg \exists \Box (\neg \text{lost} \land \neg \text{del})
\]

\[
\leadsto \exists \Diamond \neg \exists \Box \ a
\]

\[
\text{fair} = \Box \Diamond \exists \Diamond \text{del} \leadsto \Box \Diamond \ c \quad \text{where} \quad \text{Sat}(c) = S \setminus \{\text{error}\}
\]

\[
\text{Sat}_\text{fair}(\exists \Box \text{true}) = \text{Sat}(a_\text{fair}) = S \setminus \{\text{error}\}
\]

\[
\text{Sat}_\text{fair}(\exists \Box a) = \text{Sat}(\exists \Box (a \land a_\text{fair}))
\]
Example: CTL model checking with fairness

\[ \Phi = \exists \diamond \forall \Box (\text{lost} \lor \text{del}) \]

\[ \equiv \exists \diamond \neg \Box (\neg \text{lost} \land \neg \text{del}) \]

\[ \leadsto \exists \diamond \neg \exists \Box a \]

\[
\text{fair} = \Box \diamond \exists \diamond \text{del} \leadsto \Box \diamond c \text{ where } Sat(c) = S \setminus \{\text{error}\}
\]

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

\[
Sat_{\text{fair}}(\exists \Box a) = Sat(\exists \Box (a \land a_{\text{fair}})) = \{\text{start, lost, del}\}
\]
Example: CTL model checking with fairness

\[ \Phi = \exists \Diamond \forall \Box (\text{lost} \lor \text{del}) \]

\[ \equiv \exists \Diamond \neg \Box (\neg \text{lost} \land \neg \text{del}) \]

\[ \rightsquigarrow \exists \Diamond \neg \Box \text{a} \]

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

\[ \text{Sat}_{\text{fair}}(\exists \Box \text{true}) = \text{Sat}(a_{\text{fair}}) = S \setminus \{\text{error}\} \]

\[ \text{Sat}_{\text{fair}}(\exists \Box \text{a}) = \text{Sat}(\exists \Box (a \land a_{\text{fair}})) = \{\text{start, lost, del}\} \]

\[ \text{Sat}_{\text{fair}}(\neg \exists \Box \text{a}) \]
**Example: CTL model checking with fairness**

\[
\Phi = \exists \Diamond \forall \Box (\text{lost} \lor \text{del})
\]

\[
\equiv \exists \Diamond \neg \Box (\neg \text{lost} \land \neg \text{del})
\]

\[
\leadsto \exists \Diamond \neg \Box a
\]

\[
\text{fair} = \Box \Diamond \exists \Diamond \text{del} \leadsto \Box \Diamond c \text{ where } \text{Sat}(c) = S \setminus \{\text{error}\}
\]

\[
\text{Sat}_{\text{fair}}(\exists \Box \text{true}) = \text{Sat}(a_{\text{fair}}) = S \setminus \{\text{error}\}
\]

\[
\text{Sat}_{\text{fair}}(\exists \Diamond a) = \text{Sat}(\exists \Diamond (a \land a_{\text{fair}})) = \{\text{start, lost, del}\}
\]

\[
\text{Sat}_{\text{fair}}(\neg \exists \Diamond a) = \{\text{try, error}\}
\]
Example: CTL model checking with fairness

CTL formulae:

\[ \Phi = \exists \Diamond \ \forall \Box (\text{lost} \lor \text{del}) \]

\[ \equiv \exists \Diamond \neg \exists \Box (\neg \text{lost} \land \neg \text{del}) \]

\[ \leadsto \exists \Diamond \neg \Box a \]

\[ \leadsto \exists \Diamond b \]

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

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

\( \text{Sat}_{\text{fair}}(\exists \Box a) = \text{Sat}(\exists \Box (a \land a_{\text{fair}})) = \{\text{start}, \text{lost}, \text{del}\} \)

\( \text{Sat}_{\text{fair}}(\neg \exists \Box a) = \{\text{try}, \text{error}\} = \text{Sat}(b) \)
Example: CTL model checking with fairness

\[
\Phi = \exists \diamond \forall \bigcirc (\text{lost} \lor \text{del})
\]

\[
\equiv \exists \diamond \neg \exists \bigcirc (\neg \text{lost} \land \neg \text{del})
\]

\[
\leadsto \exists \diamond \neg \exists \bigcirc a
\]

\[
\leadsto \exists \diamond b
\]

\[
\text{fair} = \Box \diamond \exists \diamond \text{del} \leadsto \Box \diamond c \quad \text{where} \quad \text{Sat}(c) = S \setminus \{\text{error}\}
\]

\[
\text{Sat}_{\text{fair}}(\neg \exists \bigcirc a) = \{\text{try}, \text{error}\} = \text{Sat}(b)
\]

\[
\text{Sat}_{\text{fair}}(\exists \diamond b)
\]
Example: CTL model checking with fairness

\[ \Phi = \exists \Diamond \forall \Box (\text{lost} \lor \text{del}) \]
\[ \equiv \exists \Diamond \neg \exists \Box (\neg \text{lost} \land \neg \text{del}) \]
\[ \leadsto \exists \Diamond \neg \exists \Box \text{a} \]
\[ \leadsto \exists \Diamond \text{b} \]

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

\text{Sat}_{\text{fair}}(\neg \exists \Box \text{a}) = \{\text{try, error}\} = \text{Sat}(\text{b})

\text{Sat}_{\text{fair}}(\exists \Diamond \text{b}) = \text{Sat}(\exists \Diamond (\text{b} \land a_{\text{fair}})) \]
Example: CTL model checking with fairness

\[ \Phi = \exists \diamondsuit \ \forall \square (\text{lost} \lor \text{del}) \]

\[ \equiv \exists \diamondsuit \neg \square (\neg \text{lost} \land \neg \text{del}) \]

\[ \leadsto \exists \diamondsuit \neg \square a \]

\[ \leadsto \exists \diamondsuit b \]

\[ \text{fair} = \square \diamondsuit \ \exists \diamondsuit \text{del} \leadsto \square \diamondsuit c \text{ where } \text{Sat}(c) = S \setminus \{\text{error}\} \]

\[ \text{Sat}_{\text{fair}}(\neg \exists \square a) = \{\text{try, error}\} = \text{Sat}(b) \]

\[ \text{Sat}_{\text{fair}}(\exists \diamondsuit b) = \text{Sat}(\exists \diamondsuit (b \land a_{\text{fair}})) \]
Example: CTL model checking with fairness

\[ \Phi = \exists \Diamond \forall \Box (\text{lost} \lor \text{del}) \]

\[ \equiv \exists \Diamond \neg \exists \Box (\neg \text{lost} \land \neg \text{del}) \]

\[ \leadsto \exists \Diamond \neg \exists \Box a \]

\[ \leadsto \exists \Diamond b \]

\[ \text{fair} = \Box \Diamond \exists \Diamond \text{del} \leadsto \Box \Diamond c \text{ where } \text{Sat}(c) = S \setminus \{\text{error}\} \]

\[ \text{Sat}_{\text{fair}}(\neg \exists \Box a) = \{\text{try}, \text{error}\} = \text{Sat}(b) \]

\[ \text{Sat}_{\text{fair}}(\exists \Diamond b) = \text{Sat}(\exists \Diamond (b \land a_{\text{fair}})) \]
Example: CTL model checking with fairness

\[ \Phi = \exists \diamond \forall \bigcirc (\text{lost} \lor \text{del}) \]

\[ \equiv \exists \diamond \neg \exists \bigcirc (\neg \text{lost} \land \neg \text{del}) \]

\[ \leadsto \exists \diamond \neg \exists \bigcirc \text{a} \]

\[ \leadsto \exists \diamond \text{b} \]

\begin{align*}
\text{fair} &= \square \diamond \exists \diamond \text{del} \leadsto \square \diamond \text{c} \text{ where } \text{Sat}(c) = S \setminus \{\text{error}\} \\
\text{Sat}_{\text{fair}}(\neg \exists \bigcirc \text{a}) &= \{\text{try, error}\} = \text{Sat}(b) \\
\text{Sat}_{\text{fair}}(\exists \diamond \text{b}) &= \text{Sat}(\exists \diamond \left( \text{b} \land a_{\text{fair}} \right)) \\
&= \{\text{start, try, lost, del}\}
\end{align*}
Example: CTL model checking with fairness

$$\Phi = \exists \triangleright \forall \bigcirc (\text{lost} \lor \text{del})$$

$$\equiv \exists \triangleright \neg \exists \bigcirc (\neg \text{lost} \land \neg \text{del})$$

$$\leadsto \exists \triangleright \neg \exists \bigcirc a$$

$$\leadsto \exists \triangleright b$$

$$\text{fair} = \Box \triangleright \exists \triangleright \text{del} \leadsto \Box \triangleright c \quad \text{where } \text{Sat}(c) = S \setminus \{\text{error}\}$$

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

$$\text{Sat}_{\text{fair}}(\exists \triangleright b) = \text{Sat}(\exists \triangleright (b \land a_{\text{fair}}))$$

$$= \{\text{start, try, lost, del}\}$$
Correct or wrong?

\[ s \models_{\text{fair}} \forall O a \iff s \models \forall (a \land a_{\text{fair}}) \]
Correct or wrong?

\[ s \models_{\text{fair}} \forall \bigcirc a \iff s \models \forall \bigcirc (a \land a_{\text{fair}}) \]

wrong.

\[ \emptyset \]

\[ \{a, b\} \]

\[ \text{fair} = \Box \Diamond b \]
Correct or wrong?

\[ s \models_{fair} \forall \bigcirc a \iff s \models \forall \bigcirc (a \land a_{fair}) \]

Wrong.

\[ fair = \Box \Diamond b \]
Correct or wrong?

\[ s \models_{\text{fair}} \forall \bigcirc a \ \text{iff} \ s \models \forall \bigcirc (a \land a_{\text{fair}}) \]

wrong.

\[ \text{fair} = \Box \Diamond b \]

\[ s \not\models \forall \bigcirc (a \land a_{\text{fair}}) \]
Correct or wrong?

\[ s \models_{\text{fair}} \forall \Diamond a \iff s \models \forall \Diamond (a \land a_{\text{fair}}) \]

wrong.

\[ \text{fair} = \Box \Diamond b \]

\[ s \not\models \forall \Diamond (a \land a_{\text{fair}}) \]

\[ s \models_{\text{fair}} \forall \Diamond a \]
Correct or wrong?

\[ s \models _{\text{fair}} \forall \diamond a \iff s \models \forall \diamond (a \land a_{\text{fair}}) \]

wrong.

\[ \text{fair} = \square \lozenge b \]
\[ s \not\models \forall \diamond (a \land a_{\text{fair}}) \]
\[ s \models _{\text{fair}} \forall \diamond a \]

but correct is:

\[ s \models _{\text{fair}} \forall \diamond a \iff \text{?} \]
Correct or wrong?

\[ s \models \text{fair} \ \forall \Box a \quad \text{iff} \quad s \models \forall \Box (a \land a_{\text{fair}}) \]

Wrong.

\[ \emptyset \]

\[ \{a, b, a_{\text{fair}}\} \]

\[ \text{fair} = \Box \Diamond b \]

\[ s \not\models \forall \Box (a \land a_{\text{fair}}) \]

\[ s \models \text{fair} \ \forall \Box a \]

But correct is:

\[ s \models \text{fair} \ \forall \Box a \quad \text{iff} \quad s \models \forall \Box (a_{\text{fair}} \rightarrow a) \]
Correct or wrong?

\[
s \models_{fair} \forall \Box a \quad \text{iff} \quad s \models \forall \Box (a_{fair} \rightarrow a)
\]
Correct or wrong?

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

\[ \text{iff \quad there is no state } s' \text{ reachable from } s \text{ with } s' \models \neg a \land a_{\text{fair}} \]
Correct or wrong?

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

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

correct
Correct or wrong?

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

iff there is no state \( s' \) reachable from \( s \) with \( s' \models \neg a \land a_{\text{fair}} \)

\text{correct}

\[ s \models_{\text{fair}} \forall a \]
Correct or wrong?

\[ s \models_{fair} \forall a \quad \text{iff} \quad s \models \forall a(fair \to a) \]

iff there is no state \( s' \) reachable from \( s \) with \( s' \models \neg a \land fair \)

correct

\[ s \models_{fair} \forall a \quad \text{iff} \quad s \models_{fair} \neg \exists \not\Diamond \neg a \]
Correct or wrong?

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

iff there is no state \( s' \) reachable from \( s \) with \( s' \models \neg a \land a_{\text{fair}} \)

correct

\[ s \models_{\text{fair}} \forall \Box a \iff s \models_{\text{fair}} \neg \exists \Diamond \neg a \]

iff \( s \not\models_{\text{fair}} \exists \Diamond \neg a \)
Correct or wrong?

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

\[ \text{iff} \quad \text{there is no state } s' \text{ reachable from } s \text{ with } s' \models \neg a \land a_{\text{fair}} \]

correct

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

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

\[ \text{iff} \quad s \not\models \exists \Diamond (\neg a \land a_{\text{fair}}) \]
Correct or wrong?

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

iff there is no state \( s' \) reachable from \( s \) with \( s' \models \neg a \land a_{\text{fair}} \)

Correct

\[
s \models_{\text{fair}} \Box a \quad \text{iff} \quad s \models_{\text{fair}} \neg \exists \Diamond \neg a
\]

iff \( s \not\models_{\text{fair}} \exists \Diamond \neg a \)

iff \( s \not\models \exists \Diamond (\neg a \land a_{\text{fair}}) \)

iff \( s \models \neg \exists \Diamond (\neg a \land a_{\text{fair}}) \)
Correct or wrong?

\[
\begin{align*}
    s \models_{\text{fair}} \forall \square a & \iff s \models \forall \square (a_{\text{fair}} \to a) \\
    & \iff \text{there is no state } s' \text{ reachable from } s \text{ with } s' \models \neg a \land a_{\text{fair}}
\end{align*}
\]

correct

\[
\begin{align*}
    s \models_{\text{fair}} \forall \square a & \iff s \models_{\text{fair}} \neg \exists \lozenge \neg a \\
    & \iff s \not\models_{\text{fair}} \exists \lozenge \neg a \\
    & \iff s \not\models \exists \lozenge (\neg a \land a_{\text{fair}}) \\
    & \iff s \models \neg \exists \lozenge (\neg a \land a_{\text{fair}}) \equiv \forall \square (a_{\text{fair}} \to a)
\end{align*}
\]
We just saw:

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

\[ s \models_{\text{fair}} \forall \Diamond a \quad \text{iff} \quad s \models \forall \Diamond (a_{\text{fair}} \rightarrow a) \]
Correct or wrong?

We just saw:

$$\begin{align*}
  s \models_{\text{fair}} \forall \Diamond a & \iff s \models \forall \Diamond (a_{\text{fair}} \rightarrow a) \\
  s \models_{\text{fair}} \forall \Box a & \iff s \models \forall \Box (a_{\text{fair}} \rightarrow a)
\end{align*}$$

Is the following statement correct?

$$\begin{align*}
  s \models_{\text{fair}} \forall (b \cup a) & \iff s \models \forall (b \cup (a_{\text{fair}} \rightarrow a))
\end{align*}$$
Correct or wrong?

We just saw:

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

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

Is the following statement correct?

\[ s \models_{\text{fair}} \forall (b \cup a) \iff s \models \forall (b \cup (a_{\text{fair}} \rightarrow a)) \]

Wrong.
Correct or wrong?

\[ s \models_{\text{fair}} \exists \bigcirc \exists \Diamond a \iff s \models \exists \bigcirc ( (\exists \Diamond a) \land a_{\text{fair}} ) \]
Correct or wrong?

\[ s \models_{\text{fair}} \exists \Box \Diamond a \quad \text{iff} \quad s \models \exists \Box (\exists \Diamond a \land a_{\text{fair}}) \]

wrong.

\[ \text{fair} = \Box \Diamond b \]
Correct or wrong?

\[ s \models_{fair} \exists \Diamond \exists \Diamond a \text{ iff } s \models \exists \Diamond ((\exists \Diamond a) \land a_{fair}) \]

wrong.

\[ fair = \Box \Diamond b \]
Correct or wrong?

\[ s \models_{\text{fair}} \exists \Box \exists \Diamond a \quad \text{iff} \quad s \models \exists \Box (\exists \Diamond a \land a_{\text{fair}}) \]

wrong.

\[ \text{fair} = \Box \Diamond b \]

\[ s \models \exists \Box (\exists \Diamond a \land a_{\text{fair}}) \]
Correct or wrong?

\[ s \models_{\text{fair}} \exists \Diamond \exists \Diamond a \text{ iff } s \models \exists \Diamond (\exists \Diamond a \land a_{\text{fair}}) \]

Wrong.

\[ \text{fair} = \square \Diamond b \]

\[ s \models \exists \Diamond (\exists \Diamond a \land a_{\text{fair}}) \]

regard \( s \rightarrow s \)
Correct or wrong?

\[ s \models_{\text{fair}} \exists \diamond \exists \diamond a \iff s \models \exists \Box (\exists \diamond a \land a_{\text{fair}}) \]

wrong.

\[ \begin{align*}
\text{fair} &= \Box \diamond b \\
\forall s \models \exists \Box (\exists \diamond a \land a_{\text{fair}}) \\
\text{regard } s &\rightarrow s \\
\forall s \not\models_{\text{fair}} \exists \Box \diamond \diamond a
\end{align*} \]
Correct or wrong?

\[ s \models_{fair} \exists \Box \exists a \iff s \models \exists \Box (\exists a \land a_{fair}) \]

wrong.

\[ \text{fair} = \Box \diamond b \]

\[ s \models \exists \Box (\exists a \land a_{fair}) \]

regard \( s \rightarrow s \)

\[ s \not\models_{fair} \exists \Box \exists a \]

(note \( \text{Sat}_{fair}(\exists a) = \emptyset \))
Correct or wrong?

\[ s \models_{\text{fair}} \exists \Box \exists a \iff s \models \exists \Box (\exists a \land a_{\text{fair}}) \]

wrong.

\[ s \models_{\text{fair}} \exists (a \mathcal{W} c) \iff s \models \exists (a \mathcal{W} (c \land a_{\text{fair}})) \]

remind: \( \mathcal{W} = \) weak until
Correct or wrong?

\[ s \models_{\text{fair}} \exists \Box \exists \diamond a \quad \text{iff} \quad s \models \Box (\exists \diamond a \land a_{\text{fair}}) \]

Wrong.

\[ s \models_{\text{fair}} \exists (a \mathcal{W} c) \quad \text{iff} \quad s \models \exists (a \mathcal{W} (c \land a_{\text{fair}})) \]

Remind: \( \mathcal{W} = \text{weak until} \)

Wrong.
Correct or wrong?

\[ s \models_{fair} \exists \Box \exists \Diamond a \iff s \models \exists \Box (\exists \Diamond a \land a_{fair}) \]

Wrong.

\[ s \models_{fair} \exists (a \mathsf{W} c) \iff s \models \exists (a \mathsf{W} (c \land a_{fair})) \]

Remind: \( \mathsf{W} = \text{weak until} \)

Wrong.

\[ \text{fair} = \Box \Diamond b \]
Correct or wrong?

$s \models_{fair} \exists \Box \Diamond a$ iff $s \models \exists \Box (\exists \Diamond a \land a_{fair})$

Wrong.

$s \models_{fair} \exists (a W c)$ iff $s \models \exists (a W (c \land a_{fair}))$

Remind: $W =$ weak until

Wrong.

$$fair = \Box \Diamond b$$

$$s \models \exists (a W (c \land a_{fair}))$$
Correct or wrong?

\[
\begin{align*}
  s \models_{\text{fair}} \exists \Diamond \exists \Diamond a & \quad \text{iff} \quad s \models \exists \Diamond ( ( \exists \Diamond a ) \land a_{\text{fair}} ) \\
  s \models_{\text{fair}} \exists ( a W c ) & \quad \text{iff} \quad s \models \exists ( a W ( c \land a_{\text{fair}} ) )
\end{align*}
\]

wrong.

**remind:** \( W = \text{weak until} \)

wrong.

\[
\begin{align*}
  \text{fair} & = \Box \Diamond b \\
  s \models \exists ( a W ( c \land a_{\text{fair}} ) ) \\
  s \not\models_{\text{fair}} \exists ( a W c )
\end{align*}
\]
**CTL fairness assumptions**: formulas similar to **LTL**

e.g., $fair = \bigwedge_{1 \leq i \leq k} (\Box \Diamond \psi_i \rightarrow \Box \Diamond \phi_i)$
**Summary: fairness in CTL**

**CTL** fairness assumptions: formulas similar to **LTL**

\[ \text{e.g., } fair = \bigwedge_{1 \leq i \leq k} (\Box \Diamond \psi_i \rightarrow \Box \Diamond \Phi_i) \]

**CTL** satisfaction relation with fairness:

\[ s \models_{\text{fair}} \exists \varphi \iff \text{there exists } \pi \in \text{Paths}(s) \text{ with } \pi \models \text{fair} \text{ and } \pi \models_{\text{fair}} \varphi \]
**Summary: fairness in CTL**

**CTL** fairness assumptions: formulas similar to **LTL**

\[ \text{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond \psi_i \rightarrow \Box \Diamond \phi_i) \]

**CTL** satisfaction relation with fairness:

\[ s \models_{\text{fair}} \exists \phi \iff \text{there exists } \pi \in \text{Paths}(s) \text{ with } \pi \models \text{fair} \text{ and } \pi \models_{\text{fair}} \phi \]

Model checking for **CTL** with fairness:
**Summary: fairness in CTL**

**CTL** fairness assumptions: formulas similar to **LTL**

\[ \text{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond \psi_i \rightarrow \Box \Diamond \phi_i) \]

**CTL** satisfaction relation with fairness:

\[ s \models_{\text{fair}} \exists \phi \iff \text{there exists } \pi \in \text{Paths}(s) \text{ with } \pi \models \text{fair} \text{ and } \pi \models_{\text{fair}} \phi \]

model checking for **CTL** with fairness:

- \( \exists \bigcirc, \exists \mathcal{U}, \forall \bigcirc, \forall \Box \) via **CTL** model checker
Summary: fairness in CTL

CTL fairness assumptions: formulas similar to LTL

e.g., \( fair = \bigwedge_{1 \leq i \leq k} (\Box □ \psi_i \rightarrow □ \Box \phi_i) \)

CTL satisfaction relation with fairness:

\( s \models fair \exists \phi \) iff there exists \( \pi \in Paths(s) \) with

\( \pi \models fair \) and \( \pi \models_{fair} \phi \)

model checking for CTL with fairness:

- \( \exists \bigcirc, \exists U, \forall \bigcirc, \forall \Box \) via CTL model checker
- analysis of SCCs for \( \exists \Box, \forall U \)
Summary: fairness in CTL

**CTL** fairness assumptions: formulas similar to **LTL**

\[\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond \psi_i \rightarrow \Box \Diamond \Phi_i)\]

**CTL** satisfaction relation with fairness:

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

Model checking for **CTL** with fairness:

- \(\exists \bigcirc, \exists U, \forall \bigcirc, \forall \Box\) via **CTL** model checker
- Analysis of **SCCs** for \(\exists \Box, \forall U\)
- Complexity: \(O(\text{size}(T) \cdot |\Phi| \cdot |\text{fair}|)\)